

ДОГОВОР № _____

на обслуживание клиентов в системе "iBank 2"
(с использованием аппаратного криптопровайдера)

г. Москва

" ____ " _____ 20__ г

Закрытое акционерное общество Коммерческий банк "Универсальные финансы", именуемое в дальнейшем "БАНК", в лице _____, действующего на основании _____ с одной стороны, и _____, именуемое(ый) в дальнейшем "КЛИЕНТ", в лице _____, действующего(ей) на основании _____ с другой стороны, именуемые в дальнейшем СТОРОНЫ, заключили настоящий Договор о нижеследующем:

1. ТЕРМИНЫ, ПРИМЕНЯЕМЫЕ В ДОГОВОРЕ

- 1.1. Термины, применяемые в тексте настоящего Договора, используются в следующем значении:
- 1.2. Система "iBank 2" – совокупность программно-аппаратных средств, устанавливаемых на территории КЛИЕНТА и БАНКА, и согласовано эксплуатируемых КЛИЕНТОМ и БАНКОМ в соответствующих частях, а также организационных мероприятий, проводимых КЛИЕНТОМ и БАНКОМ, с целью предоставления КЛИЕНТУ услуг по настоящему Договору.
- 1.3. "Электронный документ" – документ, представленный в электронной форме, то есть совокупность байт в виде файла или в виде одной или нескольких записей в базе данных, подготовленный с помощью программного обеспечения системы "iBank 2", и содержащий платежное поручение или другую информацию КЛИЕНТА.
- 1.4. "Электронная цифровая подпись" (ЭЦП) – реквизит электронного документа в виде совокупности байт, формируемый КЛИЕНТОМ с помощью криптографического преобразования, реализованного в системе "iBank 2", и однозначно сопоставляемый электронному документу и используемый для аутентификации (подтверждение авторства и целостности) электронного документа. Электронная цифровая подпись однозначно увязывает в одно целое содержание документа и секретный ключ подписывающего и делает невозможным изменение документа без нарушения подлинности данной подписи.
- 1.5. "Секретный ключ ЭЦП Клиента" - ключ (последовательность байт), самостоятельно генерируемый КЛИЕНТОМ с использованием средств системы "iBank 2", и предназначенный для формирования КЛИЕНТОМ электронной цифровой подписи электронных документов.
- 1.6. "Открытый ключ ЭЦП Клиента" - ключ (последовательность байт), однозначно зависящий от секретного ключа ЭЦП Клиента, и автоматически формируемый системой "iBank 2" при изготовлении КЛИЕНТОМ секретного ключа ЭЦП Клиента, и предназначенный для проверки БАНКОМ корректности электронной цифровой подписи электронного документа, сформированного КЛИЕНТОМ.
- 1.7. "Корректная электронная цифровая подпись Клиента" - электронная цифровая подпись электронного документа КЛИЕНТА, дающая положительный результат ее проверки с открытым ключом ЭЦП Клиента.
- 1.8. "Сертификат открытого ключа ЭЦП Клиента" - бумажный документ, с представленным в шестнадцатеричном виде открытым ключом ЭЦП Клиента, датой начала и окончания действия открытого ключа ЭЦП Клиента, заверенный подписью руководителя и имеющий оттиск печати КЛИЕНТА.
- 1.9. "Активный открытый ключ ЭЦП Клиента" - открытый ключ ЭЦП Клиента, зарегистрированный БАНКОМ в системе "iBank 2", и используемый КЛИЕНТОМ в текущее время для работы в системе "iBank 2".
- 1.10. "Пара ключей ЭЦП Клиента" - секретный ключ ЭЦП Клиента и соответствующий ему открытый ключ ЭЦП Клиента.
- 1.11. "Блокировочное слово" - уникальное слово, определяемое КЛИЕНТОМ при регистрации в системе "iBank 2", для блокирования работы КЛИЕНТА или отмены услуги IP-фильтрации по телефонному звонку в Банк.

КЛИЕНТ _____

БАНК _____

- 1.12. Компрометация ключа – утрата доверия к тому, что используемые ключи обеспечивают безопасность информации. К событиям, связанным с компрометацией ключей относятся, включая, но не ограничиваясь, следующие:
 - 1.12.1. Утрата ключевых элементов;
 - 1.12.2. Утрата ключевых элементов с последующим обнаружением;
 - 1.12.3. Увольнение сотрудников, имевших доступ к ключевой информации;
 - 1.12.4. Нарушение правил хранения и уничтожения (после окончания срока действия) секретного ключа;
 - 1.12.5. Несанкционированное копирование или подозрение на копирование файла с секретными ключами;
 - 1.12.6. Возникновение подозрений на утечку информации или ее искажение в системе конфиденциальной связи;
 - 1.12.7. 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).
- 1.13. "Карточка с образцами подписей" - карточка с образцами подписей лиц имеющих право подписывать расчетные документы КЛИЕНТА и с оттиском печати, предоставляемая в БАНК КЛИЕНТОМ в соответствии с договором банковского счета;
- 1.14. "СКЗИ" - Средства криптографической защиты информации;
- 1.15. "Персональный аппаратный криптопровайдер" – специальное устройство, необходимое для работы в системе "iBank 2", реализованное в виде смарт-карты или USB-токена, содержащее программное обеспечение, предназначенное для выработки и хранения секретного ключа ЭЦП Клиента и формирования ЭЦП Клиента под документами внутри самого устройства, и обеспечивающее неизвлекаемость (невозможность считывания) секретного ключа ЭЦП Клиента. В программное обеспечение Персонального аппаратного криптопровайдера встроено СКЗИ сертифицированное ФСБ РФ.

2. ПРЕДМЕТ ДОГОВОРА

- 2.1. Предметом настоящего Договора является предоставление БАНКОМ КЛИЕНТУ услуг по обмену электронными документами, подписанными электронной цифровой подписью, в соответствии с "Порядком обслуживания КЛИЕНТА" (раздел 8 настоящего Договора) с применением Системы "iBank 2".
- 2.2. БАНК предоставляет клиенту Персональный аппаратный криптопровайдер со встроенным программным средством криптографической защиты информации, необходимый для работы с системой "iBank 2". Персональный аппаратный криптопровайдер является собственностью БАНКА и подлежит возвращению в БАНК при прекращении действия настоящего договора.
- 2.3. БАНК регистрирует КЛИЕНТА в системе "iBank 2" с предоставлением КЛИЕНТУ консультаций по вопросам подключения и работы КЛИЕНТА в системе "iBank 2".
- 2.4. БАНК предоставляет услуги по обслуживанию счетов КЛИЕНТА, открытых в КБ "Унифин" ЗАО, с использованием системы "iBank 2" на основании заявления КЛИЕНТА (Приложение №3 к настоящему Договору). Обслуживание счетов КЛИЕНТА с использованием системы "iBank 2" осуществляется на условиях и в соответствии с договорами банковского счета, на основании которых они открыты.
- 2.5. Доступ КЛИЕНТА к системе "iBank 2" предоставляется через публичную сеть "Интернет". Способ, которым КЛИЕНТ получает доступ к сети "Интернет", не является предметом настоящего Договора.

3. СОГЛАШЕНИЯ СТОРОН

- 3.1. СТОРОНЫ признают метод электронной цифровой подписи, функционирующий в соответствии со стандартами ГОСТ Р34.10-94, ГОСТ Р34.11-94 и ГОСТ Р34.10-2001 и используемый в системе "iBank 2" при передаче электронных документов от КЛИЕНТА в БАНК.
- 3.2. СТОРОНЫ признают, что при произвольном изменении электронного документа, заверенного электронной цифровой подписью, ЭЦП становится некорректной, то есть проверка ЭЦП дает отрицательный результат.

- 3.3. СТОРОНЫ признают, что подделка ЭЦП Клиента, то есть создание корректной электронной цифровой подписи электронного документа от имени КЛИЕНТА, практически невозможна без знания секретного ключа ЭЦП Клиента.
- 3.4. СТОРОНЫ признают, что электронные документы, создаваемые системой "iBank 2", заверенные корректной электронной цифровой подписью (подписями) КЛИЕНТА, юридически эквивалентны соответствующим документам на бумажном носителе, имеющим оттиск печати КЛИЕНТА и подписанным лицами, имеющими право подписывать расчетные документы КЛИЕНТА, обладают юридической силой и подтверждают наличие правовых отношений между СТОРОНАМИ. Электронные документы без ЭЦП Клиента не имеют юридической силы, БАНКОМ не рассматриваются и не исполняются.
- 3.5. СТОРОНЫ признают, что электронные документы с электронной цифровой подписью КЛИЕНТА, создаваемые системой "iBank 2" в БАНКЕ, являются доказательным материалом для решения спорных вопросов в соответствии с Приложением №1 "Положение о порядке проведения технической экспертизы при возникновении спорных ситуаций" - настоящего Договора. Электронные документы, не имеющие электронной цифровой подписи, при наличии спорных вопросов, не являются доказательствами при разрешении спорной ситуации.
- 3.6. СТОРОНЫ признают, что открытый ключ ЭЦП Клиента, указанный в Сертификате открытого ключа ЭЦП Клиента, заверенном подписями лиц, имеющих право подписывать расчетные документы КЛИЕНТА и оттиском печати КЛИЕНТА, принадлежит КЛИЕНТУ.
- 3.7. СТОРОНЫ признают в качестве единой шкалы времени при работе с системой "iBank 2" Московское поясное время. Контрольным является время системных часов аппаратных средств БАНКА.

4. ПРАВА И ОБЯЗАННОСТИ БАНКА

- 4.1. БАНК обязан по письменному уведомлению КЛИЕНТА (Приложение №5 настоящего Договора) блокировать в системе "iBank 2" существующий активный открытый ключ ЭЦП Клиента.
- 4.2. БАНК обязан по телефонному звонку КЛИЕНТА после произношения КЛИЕНТОМ блокировочного слова, впредь до письменного уведомления, временно блокировать работу КЛИЕНТА в системе "iBank 2".
- 4.3. БАНК имеет право не принимать к регистрации Сертификат открытого ключа ЭЦП Клиента, который был выработан без использования Персонального аппаратного криптопровайдера, полученного в БАНКЕ.
- 4.4. БАНК имеет право по своему усмотрению без уведомления КЛИЕНТА блокировать активный открытый ключ ЭЦП Клиента, и потребовать от КЛИЕНТА смены пары ключей ЭЦП Клиента.
- 4.5. БАНК имеет право вносить изменения в порядок обслуживания КЛИЕНТА в системе "iBank 2", закрепленный в разделе 8 настоящего Договора, с обязательным предварительным уведомлением КЛИЕНТА, через доступные каналы связи, в том числе и путем размещения соответствующей информации на Интернет сайте БАНКА по адресу <http://www.unifinbank.ru>.
- 4.6. БАНК имеет право в случае необходимости затребовать от КЛИЕНТА оформления бумажного платежного документа, оформленного в соответствии с требованиями Банка России и не производить платеж до предоставления данного документа, о чем БАНК обязан сообщить КЛИЕНТУ в однодневный срок со дня получения документа в электронной форме.
- 4.7. БАНК имеет право отказывать КЛИЕНТУ в приеме от него распоряжений на проведение операций по банковскому счету, подписанных аналогом собственноручной подписи, в случае выявления сомнительных операций КЛИЕНТА.
- 4.8. БАНК имеет право не исполнять поступившие от Клиента электронные документы, оформленные с нарушением требований действующего законодательства РФ, нормативных документов Банка России и условий настоящего Договора, а также при отсутствии или некорректности ЭЦП КЛИЕНТА.

5. ПРАВА И ОБЯЗАННОСТИ КЛИЕНТА

- 5.1. КЛИЕНТ обязан для выработки и хранения секретных ключей ЭЦП Клиента использовать Персональный аппаратный криптопровайдер, полученный в БАНКЕ.
- 5.2. КЛИЕНТ обязан самостоятельно зарегистрироваться в системе "iBank 2" через модуль "Регистратор", ука-

зывая требуемые регистрационные данные, выработать необходимое количество Пар ключей ЭЦП Клиента, используя для генерации и хранения секретных ключей ЭЦП Клиента Персональный аппаратный криптопровайдер, полученный в БАНКЕ и распечатать сертификат открытого ключа ЭЦП Клиента на каждый открытый ключ ЭЦП Клиента. Образец сертификата представлен в Приложении № 4 настоящего Договора.

- 5.3. КЛИЕНТ обязан создать вторую Пару ключей ЭЦП Клиента, при наличии в штате организации КЛИЕНТА лица, которому предоставлено право второй подписи под расчетными документами КЛИЕНТА.
- 5.4. КЛИЕНТ обязан заверять передаваемый в БАНК Сертификат открытого ключа ЭЦП Клиента двумя подписями (первой и второй) лиц, имеющих право подписывать расчетные документы КЛИЕНТА, или одной подписью (при отсутствии в штате организации КЛИЕНТА лица, которому может быть предоставлено право второй подписи), и оттиском печати, указанных в карточке с образцами подписей.
 - 5.4.1. КЛИЕНТ обязан в поле "Группа подписи" сертификата открытого ключа ЭЦП Клиента указать тип подписи "ПЕРВАЯ", "ВТОРАЯ" или "БЕЗ ПРАВА ПОДПИСИ".
 - 5.4.2. Владельцем ЭЦП с группой подписи "ПЕРВАЯ" или "ВТОРАЯ" может быть только лицо, имеющее соответствующее право подписи, указанное в карточке с образцами подписей.
- 5.5. КЛИЕНТ обязан заверять создаваемые им электронные документы двумя ЭЦП Клиента "ПЕРВОЙ" и "ВТОРОЙ", при наличии в штате организации КЛИЕНТА лица, которому предоставлено право второй подписи.
- 5.6. КЛИЕНТ обязан заполнять электронные документы в системе "iBank 2" в соответствии с требованиями действующего законодательства РФ и нормативных документов Банка России.
- 5.7. КЛИЕНТ обязан следовать порядку обмена электронными документами закрепленному в разделе 8 настоящего Договора.
- 5.8. КЛИЕНТ обязан хранить в секрете и не передавать третьим лицам пароли, файлы и носители с секретными ключами ЭЦП Клиента, используемые в электронной системе "iBank 2", а также блокировочное слово.
- 5.9. КЛИЕНТ обязан по требованию БАНКА сгенерировать новую Пару ключей ЭЦП Клиента, используя Персональный аппаратный криптопровайдер, полученный в БАНКЕ, и зарегистрировать новый открытый ключ ЭЦП Клиента в БАНКЕ.
- 5.10. Срок действия ключей ЭЦП ограничен двумя годами. КЛИЕНТ обязан по истечении срока действия ключа ЭЦП сгенерировать новую Пару ключей ЭЦП Клиента и зарегистрировать новый открытый ключ ЭЦП Клиента в Банке.
- 5.11. В случае изменения в составе руководства КЛИЕНТА (смена руководителя, гл. бухгалтера) КЛИЕНТ обязан, сгенерировать новые Пары ключей ЭЦП и зарегистрировать новые открытые ключи ЭЦП в Банке.
- 5.12. КЛИЕНТ обязан немедленно сообщать БАНКУ об обнаружении попытки несанкционированного доступа к электронной системе "iBank 2".
- 5.13. КЛИЕНТ обязан в случае компрометации своих ключей незамедлительно позвонить в БАНК для принятия мер по блокированию скомпрометированных ключей, и в кратчайшие сроки направить в БАНК письменное уведомление о блокировании своих ключей согласно Приложению №5 настоящего Договора.
- 5.14. КЛИЕНТ имеет право досрочно прекратить действие своего активного открытого ключа ЭЦП и потребовать от БАНКА блокировать этот активный открытый ключ ЭЦП Клиента, передав в БАНК уведомление согласно Приложению №5 настоящего Договора.
- 5.15. КЛИЕНТ имеет право по своему усмотрению генерировать новые пары ключей ЭЦП Клиента, используя Персональный аппаратный криптопровайдер, полученный в БАНКЕ, и регистрировать в БАНКЕ новые открытые ключи ЭЦП Клиента.
- 5.16. КЛИЕНТ имеет право, позвонив в Банк, и произнеся блокировочное слово, впредь до письменного уведомления, временно заблокировать свою работу в системе "iBank 2".
- 5.17. КЛИЕНТ имеет право, позвонив в Банк, и произнеся блокировочное слово отменить заказанную ранее услугу IP-фильтрации.

6. СОВМЕСТНЫЕ ОБЯЗАТЕЛЬСТВА И ОТВЕТСТВЕННОСТЬ СТОРОН

- 6.1. БАНК не несёт ответственности за ущерб, причинённый КЛИЕНТУ в результате использования третьими лицами секретного ключа ЭЦП Клиента, принадлежащего КЛИЕНТУ.
- 6.2. При расторжении настоящего Договора СТОРОНЫ несут ответственность в соответствии с действующим законодательством РФ по всем электронным документам с ЭЦП Клиента, сформированным в период действия настоящего Договора.
- 6.3. В случае возникновения конфликтных ситуаций между КЛИЕНТОМ и БАНКОМ при использовании электронной системы "iBank 2" СТОРОНЫ обязуются участвовать в рассмотрении конфликтов в соответствии с "Положением о порядке проведения технической экспертизы при возникновении спорных ситуаций" (Приложение №1 настоящего Договора), выполнять требования указанного Положения и нести ответственность согласно выводам по рассмотрению конфликтной ситуации.
- 6.4. СТОРОНЫ обязуются при разрешении экономических и иных споров, которые могут возникнуть в связи с использованием электронной системы "iBank 2", предоставлять в письменном виде свои оценки, доказательства и выводы по запросу заинтересованной стороны, участвующей в настоящем Договоре.
- 6.5. СТОРОНЫ освобождаются от ответственности за неисполнение или ненадлежащее исполнение взятых по настоящему Договору обязательств в случае возникновения обстоятельств непреодолимой силы (форс-мажор), 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 органов федеральных или местных органов власти (включая Центральный банк РФ) и обязательных для исполнения одной из сторон, прямо или косвенно запрещающих указанные в Договоре виды деятельности или препятствующие выполнению сторонами своих обязательств по Договору, если сторона, пострадавшая от их влияния, доведет до сведения другой стороны известие о случившемся в возможно короткий срок после возникновения этих обстоятельств.

7. ПОРЯДОК ПРЕДОСТАВЛЕНИЯ И ОПЛАТЫ УСЛУГ

- 7.1. БАНК взимает плату с КЛИЕНТА в соответствии с Тарифами Банка.
- 7.2. БАНК имеет право в безакцептном порядке списывать со счета КЛИЕНТА комиссионные вознаграждения, предусмотренные Тарифами БАНКА, в соответствии с перечнем заказанных услуг (Приложение №3) и в порядке, определенном настоящим договором.
- 7.3. БАНК производит регистрацию незарегистрированного ранее в системе "iBank 2" КЛИЕНТА в день передачи КЛИЕНТУ Персональных аппаратных криптопровайдеров.
- 7.4. БАНК производит безакцептное списание комиссионного вознаграждения за услуги, предусмотренные п.2.2. и п.2.3 настоящего Договора, в день передачи КЛИЕНТУ Персональных аппаратных криптопровайдеров и регистрации БАНКОМ КЛИЕНТА в системе "iBank 2". При этом составляется акт сдачи-приемки оказанных услуг.
- 7.5. После самостоятельной регистрации КЛИЕНТА в системе "iBank 2" и генерации КЛИЕНТОМ необходимого количества Пар ключей ЭЦП, КЛИЕНТ предоставляет в БАНК сертификаты открытых ключей ЭЦП, заверенные в соответствии с пунктом 5.4 настоящего договора. БАНК регистрирует ключи ЭЦП КЛИЕНТА и составляет акт о вводе в эксплуатацию системы "iBank 2".
- 7.6. Услуги по обслуживанию счетов КЛИЕНТА (п.2.4) настоящего Договора предоставляются бесплатно до конца первого календарного месяца с даты подписания акта о вводе в эксплуатацию системы "iBank 2", а в дальнейшем при достаточности средств на счете КЛИЕНТА для списания комиссионного вознаграждения в сроки предусмотренные пунктом 7.7. настоящего договора.
- 7.7. БАНК списывает комиссионное вознаграждение за услуги по обслуживанию счетов КЛИЕНТА (п.2.4) настоящего Договора в течение первых 5-ти рабочих дней текущего месяца (кроме первого месяца предоставления услуг).
- 7.8. КЛИЕНТ обязан обеспечить остаток денежных средств на счете достаточный для списания комиссионных вознаграждений, предусмотренных настоящим договором, на даты указанные в пунктах 7.4 и 7.7 настоящего договора.
- 7.9. В случае недостаточности средств на счете КЛИЕНТА в течение первых 5-ти рабочих дней текущего месяца (кроме первого месяца предоставления услуг) для списания предоплаты за предоставление услуг по обслуживанию расчетного счета КЛИЕНТА (п.2.4) настоящего Договора, предоставление услуг приостанавливается.

- 7.10. Предоставление услуг в текущем месяце возобновляется при достаточности средств на счете КЛИЕНТА для списания оплаты за текущий месяц кроме случая расторжения Договора согласно пункту 9.3 настоящего Договора.

8. ПОРЯДОК ОБСЛУЖИВАНИЯ КЛИЕНТА

- 8.1. БАНК осуществляет прием документов, передаваемых по электронной системе "iBank 2", круглосуточно. Активной стороной в установлении соединения и в процессе приема-передачи электронных документов, их статусов, выписок и сообщений является КЛИЕНТ. При невозможности передачи документов в БАНК с использованием электронной системы "iBank 2", документы могут поступить от КЛИЕНТА в виде подлинника на бумажном носителе.
- 8.2. Электронные документы КЛИЕНТА, подписанные необходимым количеством ЭЦП Клиента, считаются доставленными в БАНК и принимают статус "доставлен".
- 8.3. Доставленные по системе "iBank 2" электронные документы проходят дальнейшую автоматическую проверку в БАНКЕ только в течение операционного дня. По результатам этой проверки КЛИЕНТУ выдается окончательное решение о приеме в обработку или об отбраковке документа.
- 8.4. При получении электронного документа, БАНК производит проверку корректности ЭЦП Клиента, проверку правильности заполнения реквизитов документа, проверку на возможность возникновения дебетового сальдо на расчётном счёте КЛИЕНТА. В случае отбраковки, документ БАНКОМ не принимается, о чем в статусе электронного документа, запрашиваемого КЛИЕНТОМ, делается отметка "отвергнут" с указанием причины.
- 8.5. Электронные документы "Платежное поручение", полностью прошедшие автоматическую проверку в БАНКЕ и поступившие на обработку получают статус "на обработке". Документы, принятые на обработку до 15:00, БАНК принимает к исполнению в тот же день; документы, принятые на обработку позже указанного времени, принимаются к исполнению БАНКОМ на следующий рабочий день, о чем делается отметка в описании статуса электронного документа. Окончательное решение о приеме документа к исполнению принимает операционист БАНКА. Документ, принятый к исполнению операционистом БАНКА получает статус "на исполнении".
- 8.6. Электронный документ, поступивший в БАНК и имеющий статус "доставлен" или "на обработке", может быть отозван КЛИЕНТОМ, путем формирования специального электронного документа "Отзыв". Электронный документ "отзыв" должен быть подписан ЭЦП Клиента. В случае успешного отзыва документ "Отзыв" принимает статус "исполнен", а отозванный документ - "Платежное поручение" принимает статус "отвергнут". Электронный документ, имеющий статус "на исполнении", не может быть отозван КЛИЕНТОМ.
- 8.7. КЛИЕНТ поручает БАНКУ дальнейшее оформление платежных документов, переданных в БАНК по электронной системе "iBank 2".
- 8.8. Документы, исполненные БАНКОМ и проведенные по выписке КЛИЕНТА, принимают статус "исполнен".
- 8.9. Выписку за текущий операционный день КЛИЕНТ может запрашивать в любое время, но полнота выписки гарантируется БАНКОМ только после закрытия операционного дня с 10:00 следующего банковского дня.

9. СРОК ДЕЙСТВИЯ ДОГОВОРА, ПОРЯДОК И УСЛОВИЯ ЕГО ИЗМЕНЕНИЯ И ПРЕКРАЩЕНИЯ

- 9.1. Настоящий Договор вступает в силу с момента его подписания обеими сторонами и заключается на неопределенный срок.
- 9.2. СТОРОНЫ вправе по своему усмотрению расторгнуть Договор в одностороннем порядке не ранее, чем через 30 дней после письменного уведомления об этом противоположной стороны.
- 9.3. БАНК имеет право расторгнуть настоящий Договор в одностороннем порядке с последующим уведомлением КЛИЕНТА в случае
- 9.3.1. невозможности подписания акта о вводе в эксплуатацию системы "iBank 2" в течение 3-х месяцев с да-

ты подписания договора.

- 9.3.2. задержки в течение 3 (трех) месяцев поступления денежных средств на счет КЛИЕНТА, необходимых для списания оплаты за предоставление услуги.
- 9.3.3. систематического нарушения КЛИЕНТОМ правил использования системы "iBank 2".
- 9.4. Настоящий Договор подлежит расторжению в случае расторжения всех договоров банковского счета, указанных в п.2.4 настоящего Договора.

10. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

- 10.1. С даты подписания акта о вводе в эксплуатацию по настоящему Договору, настоящий Договор заменяет предыдущие соглашения в отношении системы iBank и прекращает действие ранее заключенного Договора на обслуживание клиентов в системе "iBank 2" (в случае если такой договор был заключен между Сторонами).
- 10.2. Споры по настоящему Договору решаются путем переговоров с учетом взаимных интересов в соответствии с Приложением №1 к настоящему Договору, а при не достижении соглашения - в судебном порядке.
- 10.3. Все Приложения, изменения, дополнения и особые условия к настоящему Договору оформляются в письменном виде, подписываются полномочными представителями сторон и являются неотъемлемой его частью.
- 10.4. Настоящий Договор составлен в 2-х экземплярах, имеющих одинаковую юридическую силу, по одному для каждой стороны.

11. АДРЕСА И ПОДПИСИ СТОРОН

11.1. БАНК:

Юридический адрес: 127051, г. Москва, 1-ый Колобовский пер., д.11

Фактический адрес: 127051, г. Москва, 1-ый Колобовский пер., д.11

тел. 771-75-07

Реквизиты для расчетов: БИК 044585423, К/С 30101810400000000423 в отделении №2 Московского ГТУ Банка России.

11.2. КЛИЕНТ:

Юридический адрес: _____

Фактический адрес _____

Реквизиты: расчетный счет _____ в КБ "Унифин" ЗАО,

БИК 044585423, К/С 30101810400000000423 в отделении №2 Московского ГТУ Банка России.

Телефоны: _____

e-mail: _____

КЛИЕНТ

БАНК

(Ф.И.О., подпись)

(Ф.И.О., подпись)

М. П.

М. П.

ПОЛОЖЕНИЕ

о порядке проведения технической экспертизы при возникновении спорных ситуаций

1. В настоящем Положении под спорной ситуацией понимается существование претензий у КЛИЕНТА к БАНКУ, связанных с подлинностью электронных документов, **исполненных** в Системе "iBank 2", справедливость которых может быть однозначно установлена по результату проверки ЭЦП Клиента под электронным документом.
2. КЛИЕНТ представляет БАНКУ заявление, содержащее существо претензии с указанием на документ с электронной цифровой подписью, на основании которого БАНК выполнил операции по счёту КЛИЕНТА.
3. БАНК обязан в течение не более пяти дней от даты подачи заявления КЛИЕНТА сформировать разрешительную комиссию для рассмотрения заявления. В состав комиссии включаются представители КЛИЕНТА, представители БАНКА и при необходимости – независимые эксперты. Выбор членов комиссии осуществляется по согласованию со всеми участниками.
4. Результатом рассмотрения спорной ситуации разрешительной комиссией является определение стороны, несущей ответственность согласно выводу об истинности электронной цифровой подписи Клиента под приложенным документом.
5. Разрешительная комиссия в течение не более пяти дней проводит рассмотрение заявления. Рассмотрение заявления включает следующие этапы:
 - 5.1. Разрешительная комиссия проводит техническую экспертизу электронного документа, заверенного электронной цифровой подписью Клиента, на основании которого БАНКОМ выполнены оспариваемые КЛИЕНТОМ действия с его счетом.
 - 5.2. Разрешительная комиссия проводит техническую экспертизу открытого ключа ЭЦП Клиента, период действия и статус открытого ключа ЭЦП Клиента, и установление его принадлежности КЛИЕНТУ.
 - 5.3. Разрешительная комиссия проводит техническую экспертизу корректности электронной цифровой подписи Клиента в электронном документе.
 - 5.4. На основании данных технической экспертизы разрешительная комиссия составляет акт.
6. БАНК несет ответственность перед КЛИЕНТОМ в случае, когда имело место хотя бы одна из следующих ситуаций:
 - 6.1. БАНК не предъявляет электронного документа, переданного КЛИЕНТОМ, на основании которого БАНК выполнил операции по счёту КЛИЕНТА.
 - 6.2. Электронная цифровая подпись Клиента в электронном документе оказалась некорректной.
 - 6.3. КЛИЕНТ предоставляет Уведомление об отмене действия секретного и соответствующего ему открытого ключей ЭЦП Клиента (Приложение №5 настоящего Договора), подписанное должностным лицом БАНКА, с указанием момента времени приема Уведомления БАНКОМ и имеющим оттиск печати БАНКА. При этом указанный в Уведомлении момент времени окончания действия пары ключей ЭЦП Клиента и момент времени приема Уведомления БАНКОМ раньше момента времени, указанного в рассматриваемом электронном документе.
7. В случае, когда БАНК предъявляет электронный документ, корректность ЭЦП Клиента признана разрешительной комиссией, принадлежность КЛИЕНТУ открытого ключа ЭЦП Клиента подтверждена, БАНК перед КЛИЕНТОМ по выполненным операциям со счётом КЛИЕНТА ответственности не несёт.

КЛИЕНТ

БАНК

(Ф.И.О., подпись)

(Ф.И.О., подпись)

М. П.

М. П.

ТРЕБОВАНИЯ
по обеспечению безопасности использования программного обеспечения со
встроенными средствами криптографической защиты информации.

Для криптографической защиты информации в систему "iBank 2" встроены сертифицированные ФСБ РФ криптобиблиотеки.

Средства криптографической защиты информации (СКЗИ) предназначены для защиты конфиденциальной информации от угроз нарушения конфиденциальности и целостности.

При работе с программным и аппаратным обеспечением, в которое встроены СКЗИ необходимо соблюдать следующие правила:

- Автоматизированные рабочие места с СКЗИ должны располагаться в помещениях, обеспечивающих невозможность несанкционированного доступа к СКЗИ.
- Правом доступа к рабочим местам с СКЗИ должны обладать только лица, ознакомленные с правилами безопасного использования СКЗИ.
- На технических средствах, предназначенных для работы с СКЗИ, разрешено использовать только лицензионное программное обеспечение фирм-изготовителей.
- На ПЭВМ должна быть установлена только одна операционная система.
- На ПЭВМ должна быть установлена парольная защита на вход в BIOS и в операционную систему. При выборе пароля для операционной системы, BIOS или ключа ЭЦП необходимо следовать следующим рекомендациям:
 - пароль должен содержать не менее 7 символов;
 - не использовать в качестве пароля имя, фамилию, день рождения и другие памятные даты, номер телефона, автомобиля, адрес местожительства и другие данные, которые могут быть подобраны злоумышленником путем анализа информации об администраторе или пользователе;
 - не использовать в качестве пароля один и тот же повторяющийся символ либо повторяющуюся комбинацию из нескольких символов;
 - не использовать в качестве пароля комбинацию символов, набираемых в закономерном порядке на клавиатуре (например, "1234567" или "1йфячыц2" и т. п.);
 - использовать в качестве пароля комбинацию знаков, смысл последовательности которых трудно определить.
- На ЭВМ с СКЗИ не должны устанавливаться средства разработки и отладки программного обеспечения.
- Системный блок и разъемы ЭВМ с СКЗИ должны опечатываться сотрудником службы безопасности компании, при каждом включении ЭВМ должна проверяться их целостность.
- В случае обнаружения "посторонних" (незарегистрированных) программ, нарушения целостности программного обеспечения либо выявления факта повреждения печатей на системных блоках все работы на данном рабочем месте должны быть прекращены.
- Необходимо организовать и использовать комплекс мероприятий антивирусной защиты.
- Необходимо регулярно устанавливать пакеты обновления безопасности Операционной системы, обновлять антивирусные базы;
- При использовании СКЗИ на ЭВМ, подключенных к общедоступным сетям связи (таким как Интернет), с целью исключения возможности несанкционированного доступа к системным ресурсам используемых операционных систем, к программному обеспечению, в окружении которого функционируют СКЗИ, и к компонентам СКЗИ со стороны указанных сетей, должны использоваться дополнительные методы и средства защиты (например: установка межсетевых экранов, организация VPN и т.п.).

Пользователю СКЗИ запрещается:

- обрабатывать предоставленными Банком СКЗИ информацию, содержащую государственную тайну;
- оставлять без контроля вычислительные средства, на которых эксплуатируется СКЗИ, после ввода ключевой информации либо иной конфиденциальной информации;
- разглашать содержимое носителей ключевой информации или передавать сами носители лицам, к ним не допущенным, выводить ключевую информацию на дисплей, принтер и иные средства отображения информации;
- использовать ключевые носители в режимах, не предусмотренных функционированием СКЗИ;
- записывать на ключевые носители постороннюю информацию;
- производить несанкционированное копирование СКЗИ.
- подключать к ЭВМ дополнительные устройства и соединители, не предусмотренные штатной комплектацией;
- осуществлять несанкционированное вскрытие системных блоков ЭВМ;

КЛИЕНТ

(Ф.И.О., подпись)

М. П.

ЗАЯВЛЕНИЕ № _____ от "___" _____ 20__ г.

Настоящим

(КЛИЕНТ)

просит Закрытое акционерное общество Коммерческий банк "Универсальные Финансы" (БАНК):

предоставить следующие услуги:

Наименование услуги	Потребность в услуге
Предоставить Персональные аппаратные криптопровайдеры в количестве:	_____(шт.)
Подключить к системе "iBank 2" следующие счета:	Номера счетов _____ _____ _____ _____ _____ _____
Отключить от системы "iBank 2" следующие счета:	Номера счетов _____ _____
Подключить IP-фильтрацию по следующими IP-адресам (подсетям IP-адресов) (доступ к системе будет возможен только с этих IP-адресов. Для оперативной отмены IP-фильтрации можно использовать блокировочное слово):	IP-адрес (подсеть IP-адресов) _____ _____ _____
Отключить IP-фильтрацию по следующим IP-адресам (подсетям IP-адресов)	IP-адрес (подсеть IP-адресов) _____

КЛИЕНТ

(Ф.И.О., подпись)

М. П.

Отметки Банка

**СЕРТИФИКАТ ОТКРЫТОГО КЛЮЧА ЭЦП СОТРУДНИКА КЛИЕНТА
В СИСТЕМЕ "IBANK 2"
ЗАО КБ "УНИВЕРСАЛЬНЫЕ ФИНАНСЫ"**

1. Наименование организации _____
2. Юридический адрес _____
3. ОГРН _____ дата внесения в ЕГРЮЛ (ЕГРИП) "___" "___" _____ 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 _____
10. Примечания* _____
* обязательно 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 "iBank2"
№ _____ от "___" "___" _____ 20__ г.

Группа подписи _____

(указать в соответствии с должностью сотрудника, владельца ключа ЭЦП)

Достоверность приведенных данных подтверждаю

Руководитель организации

подпись / ф.и.о.

Сверено с юридическим досье

подпись / ф.и.о.

Главный бухгалтер

подпись / ф.и.о.

Оттиск печати
Банка

Дата приема сертификата
открытого ключа ЭЦП
"___" _____ 20__ г.

Оттиск печати

Администратор безопасности системы

подпись / ф.и.о.

Дата регистрации сертификата
открытого ключа ЭЦП
"___" _____ 20__ г.

УВЕДОМЛЕНИЕ

об отмене действия секретного и соответствующего ему открытого ключей ЭЦП Клиента

(КЛИЕНТ)

уведомляет Закрытое акционерное общество Коммерческий банк "Универсальные Финансы" (БАНК) о том, что с "___" _____ 20__ г. _____ часов _____ минут считать недействительным открытый ключ ЭЦП Клиента со следующим

идентификатором: _____
(см. в сертификате открытого ключа ЭЦП клиента поле - "Идентификатор")

Соответствующий ему секретный ключ ЭЦП Клиента утрачивает силу для дальнейшего применения с вышеуказанного момента времени.

"_____" _____ 200__ г

КЛИЕНТ

(Ф.И.О., подпись)
М. П.

М.П.

Отметки Банка

Принято Банком: "___" _____ 20__ года _____ часов _____ минут.

Операционист _____ (_____)
Ф.И.О. подпись

Администратора системы "iBank 2"

Открытый ключ ЭЦП Клиента с идентификатором _____

блокирован в системе "iBank 2" с "___" _____ 20__ года _____ часов _____ минут.

Администратор системы "iBank 2" _____ (_____)
Ф.И.О. подпись

М.П.

АКТ
сдачи-приемки услуг
по Договору на обслуживание клиентов
в системе "iBank 2" № _____ от "___" _____ 20__ г.
в дальнейшем "ДОГОВОР"

г. Москва

"___" _____ 20__ г

Закрытое акционерное общество Коммерческий банк "Универсальные финансы", именуемое в дальнейшем "БАНК", в лице _____, действующего на основании _____ с одной стороны, и _____, именуемое(ый) в дальнейшем "КЛИЕНТ", в лице _____, действующего(ей) на основании _____ с другой стороны, именуемые в дальнейшем СТОРОНЫ, составили настоящий акт о нижеследующем:

БАНК оказал, а КЛИЕНТ принял следующие услуги в соответствии с ДОГОВОРОМ.

Номер	Наименование услуг	Цена(руб.)	Количество	Стоимость (руб.)
1	Предоставление КЛИЕНТУ Персонального аппаратного криптопровайдера со встроенным программным средством криптографической защиты (СКЗИ) "Криптомодуль-С" (сертификат соответствия ФСБ РФ Рег. № СФ/114-1009 от 14.05.2007г.), необходимого для работы с системой "iBank 2". Номера Экземпляров: _____	1500	_____	_____
2	Регистрация КЛИЕНТА в системе "iBank 2"	1500	_____	_____
Итого:				_____

Итого оказано услуг на сумму _____ руб. _____ коп.

(_____) НДС не облагается.

Вышеперечисленные услуги оказаны полностью, СТОРОНЫ друг к другу претензий не имеют.

КЛИЕНТ

БАНК

(Ф.И.О., подпись)

(Ф.И.О., подпись)

М. П.

М. П.

Я, представитель КЛИЕНТА _____, Ф.И.О. _____, действующая на основании _____, документ _____, указанные Выше Персональные аппаратные криптопровайдеры получил в количестве _____ штук.

(подпись)

(дата)

_____ 20__ г.

АКТ
о вводе в эксплуатацию системы "iBank 2"
по Договору на обслуживание клиентов
в системе "iBank 2" № _____ от "___" _____ 20__ г.
в дальнейшем "ДОГОВОР"

г. Москва

"___" _____ 20__ г

Закрытое акционерное общество Коммерческий банк "Универсальные финансы", именуемое в дальнейшем "БАНК", в лице _____, действующего на основании _____ с одной стороны, и _____, именуемое(ый) в дальнейшем "КЛИЕНТ", в лице _____ действующего(ей) на основании _____ с другой стороны, именуемые в дальнейшем СТОРОНЫ, составили настоящий акт о нижеследующем:

Сторонами проведены следующие мероприятия по подключению Клиента к системе "iBank 2":

- Банком переданы и Клиентом получены Персональные аппаратные криптопровайдеры со встроенным программным средством криптографической защиты информации, необходимыми для подключения и работы в системе "iBank 2";
- На автоматизированном рабочем месте Клиентом проведена установка и настройка программного обеспечения, необходимого для подключения и работы в системе "iBank 2"
- Клиентом приняты меры по обеспечению безопасности функционирования средств криптографической защиты информации в соответствии с настоящим договором и инструкцией, доступной на сайте Банка, по работе с Персональным аппаратным криптопровайдером;
- Клиентом сгенерированы и зарегистрированы в Банке криптографические ключи должностных лиц Клиента, уполномоченных подписывать электронными цифровыми подписями, передаваемые в Банк электронные документы;
- Мероприятия по подключению к системе "iBank 2" выполнены Сторонами в полном объеме, система "iBank 2" полностью работоспособна и вводится в эксплуатацию с момента подписания настоящего Акта.

КЛИЕНТ

БАНК

(Ф.И.О., подпись)

(Ф.И.О., подпись)

М. П.

М. П.