

ДОГОВОР № _____
на обслуживание Клиента по системе «iBank 2»

г. Москва

«___» _____ 20 г.

КБ «КБР БАНК» (ООО), именуемый в дальнейшем «Банк», имеющий Лицензии Центра по лицензированию, сертификации и защите государственной тайны ФСБ России ЛЗ № 0003170 от 09.08.2007г. на техническое обслуживание шифровальных средств, ЛЗ № 0002171 от 09.08.2007г. на распространение шифровальных средств, и ЛЗ № 0002172 от 09.08.2007г. на предоставление услуг в области шифрования информации, в лице _____

_____, действующего (-ей) на основании _____, с одной стороны, и _____, именуемое в дальнейшем «Клиент», в лице _____,

действующего на основании _____, с другой стороны, вместе в дальнейшем именуемые «Сторонами», заключили настоящий Договор о нижеследующем:

1. Термины, применяемые в Договоре

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

1.1. 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.

1.2. «Электронный документ» – совокупность байт, содержащая финансовый документ или информационное сообщение Клиента.

1.3. «Электронная цифровая подпись» (ЭЦП) – совокупность байт, формируемая Клиентом, однозначно сопоставляемая электронному документу и используемая для аутентичности (подтверждение авторства и целостности) электронного документа. Количество ЭЦП, необходимое для электронных документов описано в Приложении № 3 к данному договору.

1.4. «Секретный ключ ЭЦП Клиента» – ключ (последовательность байт), генерируемый Клиентом с использованием средств системы «iBank 2», и предназначенный для формирования Клиентом электронной цифровой подписи электронных документов.

1.5. «Открытый ключ ЭЦП Клиента» – ключ (последовательность байт), зависящий от секретного ключа ЭЦП Клиента, самостоятельно генерируемый Клиентом с использованием средств системы «iBank 2», и предназначенный для проверки Банком корректности электронной цифровой подписи электронного документа, сформированного Клиентом.

1.6. «Корректная электронная цифровая подпись Клиента» – электронная цифровая подпись электронного документа Клиента, дающая положительный результат ее проверки с открытым ключом ЭЦП Клиента.

1.7. «Сертификат открытого ключа ЭЦП Клиента» – бумажный документ, с представленным в шестнадцатеричном виде открытым ключом ЭЦП Клиента, датой начала и окончания действия

От Банка _____

От Клиента _____

открытого ключа ЭЦП Клиента, заверенный подписью руководителя и имеющий оттиск печати Клиента.

1.8. «Владелец сертификата» – физическое лицо, на имя которого оформлен, зарегистрирован и заверен Банком документ на бумажном носителе - сертификат регистрации открытого ключа ЭЦП, и которое владеет соответствующим закрытым ключом ЭЦП, позволяющим с помощью встроенных в Систему средств электронной цифровой подписи создавать свою ЭЦП в ЭД (подписывать (заверять) ЭД).

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. «Группа подписи» – очередность формирования ЭЦП. В случае, когда электронный документ требует более одной электронной цифровой подписи (см. Приложение № 3) очередность формирования ЭЦП определяется группой подписи: для формирования первой ЭЦП используется секретный ключ ЭЦП клиента из первой группы подписи, для формирования второй ЭЦП используется секретный ключ ЭЦП клиента из второй группы подписи и так далее.

1.12. «Компрометация ключа ЭЦП» – утрата доверия к тому, что используемые ключи обеспечивают безопасность информации. К событиям, связанным с компрометацией ключей, относятся следующие (включительно, но не ограничиваясь):

- утрата ключевых элементов;
- утрата ключевых элементов с последующим обнаружением;
- несанкционированное копирование или подозрение на копирование носителя электронного ключа;
- нарушение правил хранения и уничтожения (после окончания срока действия) секретного ключа ЭЦП;
- возникновение подозрений на утечку информации или ее искажение в Системе;
- 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. «Программная библиотека защиты информации «Агава-С» и «Средство криптографической защиты информации «Крипто-КОМ 3.2» – программные модули, именуемые в дальнейшем «Средство криптографической защиты информации, или СКЗИ, входящие в состав системы «iBank 2», обеспечивающие защиту информации по уровню «КС1», соответствующий требованиям ГОСТ 28147-89, ГОСТ Р34.10-94, ГОСТ Р34.10-2001, ГОСТ Р34.11-94 и требованиям ФАПСИ к стойкости средств криптографической защиты информации Класса КНВ-2.99. СКЗИ «Агава-С» имеет Сертификат соответствия ФСБ РФ рег. № СФ/114-1171 от 01.09.2008. СКЗИ «Крипто-КОМ 3.2» - Сертификат соответствия ФСБ РФ рег. № СФ/114-1068 от 07.11.2007 и № СФ/124-1070 от 15.07.2008г.

1.14. «Блокировочное слово» – уникальное слово, определяемое Клиентом при регистрации в системе «iBank 2», для блокирования работы Клиента по телефонному звонку в Банк.

1.15. «ДБО» - дистанционное банковское обслуживание.

2. Предмет Договора

2.1. Банк осуществляет обслуживание расчётного счёта № _____

Клиента с использованием системы «iBank 2», позволяющей передавать электронные документы, и принимать выписки и информационные сообщения.

2.2. Настоящий Договор носит аксессуарный характер и действует в связи с «Договором на расчётно-кассовое обслуживание» банковского счёта № _____ от «__» _____ 20__ г. заключённого Сторонами.

3. Соглашения Сторон

3.1. Стороны признают, что электронная цифровая подпись в электронном документе равнозначна собственноручной подписи в документе на бумажном носителе при одновременном соблюдении следующих условий:

- сертификат ключа подписи, относящийся к этой электронной цифровой подписи, не утратил силу (действует) на момент проверки или на момент подписания электронного документа при наличии доказательств, определяющих момент подписания;

- подтверждена подлинность электронной цифровой подписи в электронном документе;

- электронная цифровая подпись используется в соответствии со сведениями, указанными в сертификате ключа подписи.

3.2. Стороны признают, что электронные документы, заверенные электронной цифровой подписью Клиента, обладают юридической силой и подтверждают возникновение правовых отношений между Сторонами, а в случае расторжения договора банковского счёта на основании заявления, подписанного электронной цифровой подписью, прекращение правовых отношений.

3.3. Стороны признают, что используемые в системе «iBank 2» средства криптографической защиты информации, которое обеспечивает шифрование, контроль целостности и электронную цифровую подпись, достаточно для защиты информации от несанкционированного доступа, подтверждения подлинности и авторства электронных документов, а также разбора конфликтных ситуаций.

3.4. Стороны признают, что при произвольном изменении электронного документа, заверенного электронной цифровой подписью, ЭЦП становится некорректной, то есть проверка ЭЦП дает отрицательный результат.

3.5. 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.

3.7. Стороны признают, что электронные документы с электронными цифровыми подписями 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 необходимого количества электронных цифровых подписей, при наличии спорных вопросов, не являются доказательным материалом.

3.8. Стороны признают, что открытый ключ ЭЦП Клиента, указанный в заверенном подписью руководителя и оттиском печати Клиента Сертификате открытого ключа ЭЦП Клиента, принадлежит уполномоченному сотруднику Клиента.

3.9. 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 предоставлять Клиенту необходимые рекомендации для работы с системой «iBank 2».

4.2. Банк обязан передать Клиенту СКЗИ до начала работы Клиента в системе «iBank 2». Факт передачи фиксируется Актом передачи СКЗИ (см. Приложение № 4 и Приложение № 4 (дополнительное) к данному договору).

4.3. Банк обязан по требованию Клиента блокировать в системе «iBank 2» существующие активные открытые ключи ЭЦП Клиента и зарегистрировать новые открытые ключи ЭЦП Клиента.

4.4. Банк обязан по телефонному звонку Клиента после произношения Клиентом блокировочного слова, впредь до письменного уведомления, временно блокировать работу Клиента в системе «iBank 2».

4.5. Банк имеет право по своему усмотрению без уведомления Клиента блокировать активный открытый ключ ЭЦП Клиента, и потребовать от Клиента смены пары ключей ЭЦП Клиента.

4.6. Банк имеет право, в случае некорректной электронной цифровой подписи, отказать Клиенту в исполнении платежа и затребовать от него оформления платежного документа на бумажном носителе (подлинника) с подписью руководителя и оттиском печати Клиента. Вместе с тем, Банк имеет право потребовать от Клиента сменить ключи ЭЦП и временно, до получения Клиентом новых ключей, блокировать работу Клиента в системе «iBank 2»

4.7. Банк имеет право отказать Клиенту в приеме от него расчетных (платежных) документов, подписанных ЭЦП, в случае выявления Банком сомнительных операций, проводимых Клиентом предварительно уведомив об этом Клиента. При возникновении такой ситуации Банк принимает надлежащим образом оформленные расчетные (платежные) документы на бумажном носителе и **ПИСЬМО-ОБЪЯСНЕНИЕ**.

4.8. Банк имеет право отключить систему «iBank 2» при неполучении от Клиента до окончания текущего месяца ежемесячной абонентской платы за предыдущий месяц за обслуживание системы. В случае если абонентская плата не уплачивается Клиентом, настоящий Договор подлежит расторжению в одностороннем порядке по инициативе Банка

4.9. Банк имеет право произвести блокировку электронно-цифровой подписи в случае непредоставления Клиентом документов, подтверждающих полномочия лиц, обладающих правом электронно-цифровой подписи, а также в других случаях, предусмотренных действующим законодательством Российской Федерации.

5. Права и обязанности Клиента

5.1. На основании имеющихся у Банка лицензий ФСБ России Клиент имеет право осуществлять эксплуатацию, предоставленного Банком сертифицированного средства криптографической защиты информации в системе «iBank 2» без получения собственной лицензии.

5.2. Перед началом эксплуатации системы «iBank 2» Клиент обязан:

- самостоятельно зарегистрироваться в Системе на сайте Банка <https://ib.kbrbank.ru>;

- сгенерировать открытый и закрытый ключи ЭЦП для каждого из уполномоченных на подпись банковских документов сотрудников Клиента (в случае использования электронного носителя ключей ЭЦП, носитель необходимо заранее приобрести в Банке);

- распечатать сертификат ЭЦП в 2-х экземплярах (в соответствии с пошаговой инструкцией к «iBank 2», размещённой на сайте Банка) (Приложение № 2 к Договору);

- при генерации ЭЦП Клиент должен определить и ввести в Систему блокировочное слово, предназначенное для голосовой идентификации Клиента во время телефонных переговоров Клиента с сотрудником Центра дистанционного обслуживания Банка с целью экстренной блокировки доступа к Системе для данного Клиента в случае такой необходимости;

- представитель Клиента должен прийти в Банк и заключить Договор. При визите в Банк представитель Клиента должен иметь следующие документы:

а) документ, удостоверяющий личность;

б) документы, подтверждающие его полномочия;

в) два распечатанных экземпляра сертификата ЭЦП для каждого из уполномоченных на подпись банковских документов сотрудника Клиента;

г) договор на обслуживание Клиента по системе «iBank 2» .

5.3. Перед началом эксплуатации системы «iBank 2» Клиент обязан получить в Банке и самостоятельно установить на своем рабочем месте СКЗИ.

5.4. Клиент обязуется использовать предоставленное СКЗИ только в системе «iBank 2», без права их продажи или передачи каким-либо другим способом иным физическим или юридическим лицам, обеспечивать возможность контроля со стороны федеральных органов правительственной связи и информации за соблюдением требований и условий осуществления лицензионной деятельности.

5.5. Клиент обязан допускать к эксплуатации системы «iBank 2» только сотрудников, имеющих соответствующую подготовку.

5.6. Клиент обязан обеспечивать сохранность и целостность программного комплекса системы «iBank 2», включая СКЗИ. Сохранять конфиденциальность и подлинность секретных ключей ЭЦП. Выполнять правила изложенные в Порядке формирования, хранения, смены и блокировки ЭЦП (Приложение 6 к Договору).

5.7. Клиент обязан обеспечивать безопасность и целостность среды исполнения на своем компьютере (защиту от вирусов, программ-закладок, шпионских программ и другого вредоносного программного обеспечения), также неукоснительно выполнять все пункты документа «Правила доступа клиентов КБ «КБР БАНК» (ООО) к услугам ДБО с указанием мер информационной безопасности» (Приложение 7 к Договору).

5.8. Клиент обязан сообщать Банку об обнаружении попытки несанкционированного доступа к системе «iBank 2», не позднее следующего дня с момента обнаружения.

5.9. Клиент обязан извещать Банк обо всех случаях компрометации секретных ключей ЭЦП.

5.10. Клиент обязан в случае прекращения использования системы «iBank 2» уничтожить программное обеспечение системы «iBank 2», включая СКЗИ и официально уведомить об этом Банк.

5.11. Клиент обязан заполнять электронные документы в системе «iBank 2» в соответствии с действующим «Положением о безналичных расчётах в Российской Федерации».

5.12. Клиент обязан хранить в секрете и не передавать третьим лицам пароль и носитель с секретным ключом ЭЦП Клиента, используемые в системе «iBank 2».

5.13. Клиент обязан по требованию Банка сгенерировать новую пару ключей ЭЦП Клиента и зарегистрировать новый открытый ключ ЭЦП сотрудника Клиента в Банке.

5.14. Клиент обязан подтвердить права лиц, использующих ЭЦП, в соответствии с Приложением № 5 к настоящему Договору.

5.15. Клиент имеет право требовать от Банка предоставление оригиналов платёжных поручений с исполнением в день проведения операции Банком (во второй половине дня).

5.16. Клиент имеет право досрочно прекратить действие своего активного открытого ключа ЭЦП и потребовать от Банка заблокировать этот активный открытый ключ ЭЦП Клиента.

5.17. Клиент имеет право по своему усмотрению генерировать новые пары ключей ЭЦП Клиента и регистрировать в Банке новые открытые ключи ЭЦП Клиента.

5.18. Клиент имеет право, позвонив телефону (495) 380-08-97 в Банк, и произнеся блокировочное слово, впредь до письменного уведомления, временно заблокировать свою работу в системе «iBank 2».

6. Условия расчетов

6.1. За оказанные услуги Клиент уплачивает Банку ежемесячную абонентскую плату в соответствии с Тарифами Банка.

6.2. Оплата оказанных Банком услуг производится путем безакцептного списания денежных средств с расчетного счета Клиента. При этом Клиент обязуется обеспечить на период списания, с 25 числа и до конца текущего месяца, остаток на расчетном счете в размере, достаточном для оплаты оказанных Банком услуг. В противном случае Банк имеет право в одностороннем порядке и без предварительного уведомления прекратить доступ Клиенту к пользованию системой «iBank 2».

6.3. При прекращении оказания услуг на основании п.п. 4.9, 6.2 настоящего Договора абонентская плата продолжает начисляться и уплачиваться Клиентом.

7. Совместные обязательства и ответственность Сторон

7.1. Банк не несёт ответственности за ущерб, причинённый Клиенту в результате использования третьими лицами секретного ключа ЭЦП Клиента.

7.2. При расторжении настоящего Договора Стороны несут ответственность по всем электронным документам с электронными цифровыми подписями Клиента, сформированным в системе «iBank 2», в соответствии с действующим законодательством РФ.

7.3. 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), выполнять требования указанного Положения и нести ответственность согласно выводам по рассмотрению конфликтной ситуации.

7.4. Банк не несет ответственности за ущерб, возникший вследствие нарушения Системы защиты информации не по вине Банка.

7.5. В случае несоблюдения Клиентом п. 5.6 настоящего Договора Банк не несет ответственности за возможные негативные последствия.

7.6. 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.

7.7. Стороны освобождаются от ответственности за неисполнение или ненадлежащее исполнение взятых по настоящему Договору обязательств в случае возникновения обстоятельств непреодолимой силы, к которым относятся: стихийные бедствия, пожары, аварии, отключения электроэнергии, повреждение линий связи, массовые беспорядки, забастовки, военные действия, противоправные действия третьих лиц, вступление в силу законодательных актов, актов органов федеральных или местных органов власти и обязательных для исполнения одной из сторон, прямо или косвенно запрещающих указанные в Договоре виды деятельности или препятствующие выполнению сторонами своих обязательств по Договору, если сторона, пострадавшая от их влияния, доведет до сведения другой стороны известие о случившемся в возможно короткий срок после возникновения этих обстоятельств.

8. Порядок обслуживания Клиента

8.1. Банк осуществляет прием документов, передаваемых по электронной системе «iBank 2», круглосуточно. 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. Документы, поступившие до 15:30, Банк принимает к исполнению в тот же день; документы, поступившие позже указанного времени – на следующий рабочий день.

8.3. Клиент поручает Банку дальнейшее оформление платежных документов, переданных в Банк по электронной системе «iBank 2».

8.4. При получении электронного документа Банк производит проверку корректности электронных цифровых подписей Клиента, проверку правильности заполнения реквизитов документа, проверку на возможность возникновения дебетового сальдо на расчетном счете Клиента. В случае отбраковки документ Банком не принимается.

9. Срок действия Договора

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

9.2. Стороны вправе расторгнуть Договор в одностороннем порядке не ранее, чем через месяц после письменного уведомления об этом противоположной стороны.

9.3. В случае если абонентская плата не уплачивается Клиентом, настоящий Договор подлежит расторжению в одностороннем порядке по инициативе Банка.

9.4. Настоящий Договор подлежит немедленному расторжению в случае расторжения «Договора на расчетно-кассовое обслуживание».

10. Заключительные положения

10.1. Споры по настоящему Договору решаются путем переговоров с учетом взаимных интересов в соответствии с Приложением № 1, а при не достижении соглашения - в судебном порядке.

10.2. Все Приложения, изменения, дополнения и особые условия к настоящему Договору оформляются в письменном виде, подписываются полномочными представителями сторон и являются неотъемлемой его частью.

10.3. Настоящий Договор составлен в 2-х экземплярах по одному для каждой стороны, причем оба экземпляра имеют одинаковую силу.

11. Юридические адреса Сторон

Банк	Клиент
КБ «КБР БАНК» (ООО)	_____
Адрес: 117556, г. Москва, ул. Фруктовая, д. 5А	Адрес _____
к/с 30101810500000000427 в Отделении № 3	_____
Московского ГТУ Банка России	_____
БИК 044599427 ИНН 7744000729	_____
_____	_____
(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, справедливость которых может быть однозначно установлена по результату проверки электронных цифровых подписей Клиента под электронным документом.

2. Клиент представляет Банку заявление, содержащее существо претензии с указанием на электронный документ, на основании которого Банк выполнил операции по счёту Клиента.

3. Банк обязан в течение пяти дней от даты подачи заявления Клиента сформировать разрешительную комиссию для рассмотрения заявления. В состав комиссии включаются представители Клиента, представители Банка, представители компании-разработчика системы «iBank 2» – ООО «БИФИТ», и при необходимости – независимые эксперты. Выбор членов комиссии осуществляется по согласованию со всеми участниками. При невозможности согласованного выбора, последний проводится случайно (по жребию).

4. Результатом рассмотрения спорной ситуации разрешительной комиссией является определение стороны, несущей ответственность согласно выводу об истинности электронных цифровых подписей 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 необходимыми количеством электронных цифровых подписей Клиента, на основании которого Банком выполнены оспариваемые Клиентом действия с его счетом.
- 5.2. Разрешительная комиссия проводит техническую экспертизу открытых ключей ЭЦП Клиента, период действия и статус открытых ключей ЭЦП Клиента, и установление их принадлежности Клиенту.
- 5.3. Разрешительная комиссия проводит техническую экспертизу корректности электронных цифровых подписей 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. Хотя бы одна 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, подписанное должностным

лицом Банка и имеющим оттиск печати Банка. При этом указанная в Уведомлении дата окончания действия пары ключей ЭЦП Клиента раньше даты, указанной в рассматриваемом электронном документе.

7. В случае, когда Банк предъявляет электронный документ, корректность электронных цифровых подписей Клиента признана разрешительной комиссией, принадлежность Клиенту открытых ключей Клиента подтверждена, Банк перед Клиентом по выполненным операциям со счётом Клиента ответственности не несёт.

Банк

Клиент

(Ф.И.О., подпись)

(Ф.И.О., подпись)

М. П.

М. П.

Приложение № 3 к
Договору на обслуживание Клиента в системе
«iBank 2» № _____ от
«__» _____ 20__ г.

ПЕРЕЧЕНЬ

электронных документов передаваемых по системе «iBank 2» и необходимое количество ЭЦП.
(при наличии в штате должности Руководителя и Главного бухгалтера - 2)

	Наименование электронного документа	Количество ЭЦП
1. Рублевые документы		
1.1.	Платежное поручение	
1.2.	Заявление на аккредитив	
1.3.	Платежное требование	
1.4.	Инкассовое поручение	
1.5.	Заявление об акцепте	
1.6.	Заявка на выдачу наличных денежных средств	
1.7.	Реестр документов на инкассо	
2. Валютные документы		
2.1.	Заявление на перевод	
2.2.	Межбанковский перевод	
2.3.	Поручение на покупку иностранной валюты	
2.4.	Поручение на продажу иностранной валюты	
2.5.	Поручение на обратную продажу иностранной валюты	
2.6.	Распоряжение на обязательную продажу иностранной валюты	
2.7.	Распоряжение на списание с транзитного счета	
2.8.	Поручение на конвертацию иностранной валюты	
2.9.	Паспорт сделки по контракту	
2.10.	Паспорт сделки по кредитному договору	
2.11.	Справка о валютных операциях	
2.12.	Справка о поступлении валюты РФ	
2.13.	Справка о подтверждающих документах	
3. Прочие документы		
3.1.	Отзыв	
3.2.	Письмо*	

* сообщение в свободной форме и/или с прикрепленным файлом. В данном документе возможно отправление заявления на закрытие расчетного счета по форме Банка (по предварительному согласованию с Банком).

Банк

Клиент

(Ф.И.О., подпись)
М. П.

(Ф.И.О., подпись)
М. П.

Приложение № 4 к
Договору на обслуживание Клиента в системе
«iBank 2» № _____ от
«__» _____ 20__ г.

АКТ

КБ «КБР БАНК» (ООО), имеющий Лицензию Центра по лицензированию, сертификации и защите государственной тайны ФСБ России ЛЗ № 0002171 от 09 августа 2007 года на распространение шифровальных (криптографических) средств, в лице

_____,
передал а _____, в
лице _____ получил
носитель CD регистрационный № _____ с встроенным и поставляемым в
составе ПрЭВМ «iBank2» криптобиблиотеки (Программы для ЭВМ):

- Программная библиотека защиты информации «Агава-С» (версия 5.0)
- Средство криптографической защиты информации «Крипто-КОМ 3.2»

Встроенная в ПрЭВМ «iBank2» программа для ЭВМ «Программная библиотека защиты информации «Агава-С» (версия 5.0)», все исключительные имущественные права на которую принадлежат ООО «Р-Альф», имеет Сертификат соответствия ФСБ РФ рег. № СФ/114-1171 от 01.09.2008 и поставляется в составе ПрЭВМ «iBank2» на основании Договора № ЛД 1479 от 02.08.2010 между КБ «КБР БАНК» (ООО) и ООО «БИФИТ», и Договора № 01/02-06Агава от 23.06.2006г. между ООО «БИФИТ» и ООО «Р-Альф». Регистрационный номер эталонного экземпляра криптобиблиотеки, переданной Клиенту в составе ПрЭВМ «iBank2» - 341С-001016/1847.

Встроенная в ПрЭВМ «iBank2» программа для ЭВМ «Средство криптографической защиты информации «Крипто-КОМ 3.2», все исключительные имущественные права на которую принадлежат ООО «Сигнал-КОМ», имеет Сертификат соответствия ФСБ РФ рег. № СФ/114-1068 от 07.11.2007 и № СФ/124-1070 от 15.07.2008г., и поставляется в составе ПрЭВМ «iBank2» на основании Договора № ЛД 1479 от 02.08.2010 между КБ «КБР БАНК» (ООО) и ООО «БИФИТ», и Договора № СО-401-06 от 16.06.2006г. между ООО «БИФИТ» и ООО «Сигнал-КОМ». Регистрационный номер эталонного экземпляра криптобиблиотеки, переданной Клиенту в составе ПрЭВМ «iBank2» - 508-001114/1847.

Банк

Клиент

(Ф.И.О., подпись)

(Ф.И.О., подпись)

М. П.

М. П.

Приложение № 4 (дополнение) к
 Договору на обслуживание Клиента в системе
 «iBank 2» № _____ от
 «__» _____ 20__ г.

Приложение
к АКТУ
(прикладные библиотеки защиты информации (опись CD))

Имя	Контрольная сумма (SH1)	Описание
/		
shalsum.exe	d8b9542dd46057db29bbff4146dbbb8f7e8261a2	Утилита для вычисления контрольной суммы
lib/linux-i586/ libibank2agava.so	5585282f99a1ebca770de42e94e8f143944f4d62	Модуль ПБЗИ «Агава-С» (вер. 5.0) для ОС Linux (платформа x86)
libibank2ccom.so	7caa264c480a72cfb882177b19a7eaa486733fb0	Модуль ПБЗИ «Крипто-КОМ 3.2» для ОС Linux (платформа x86)
lib/linux-x86_64/ libccom.so.0	b8b86a80d6202b42a4fc7f655487e673fb48dd92	Модуль ПБЗИ «Крипто-КОМ 3.2» для ОС Linux (платформа x86, 64 бит)
libccom.so.0.sig	a17d94d927d780ff5858ee67328b83a66dbbc106	
libibank2ccom.so	54268797c0b50ab05a0539c6a51a14d4bfa99c39	
lib/solaris-x86_64/ libccom.so.0	c32e35eb95a4388229c9e05dc4f3b64452f864b2	Модуль ПБЗИ «Крипто-КОМ 3.2» для ОС Solaris (платформа x86, 64 бит)
libccom.so.0.sig	8d55386d96c0fdfacefbc816984101b61558958	
libibank2ccom.so	bed1e07b85d76d3749b640221d8374d6744d7159	
lib/win32/ ibank2agava.dll	2322c9395716b1d6c91ba77520a4910066edc282	Модуль ПБЗИ «Крипто-КОМ 3.2» для ОС Windows
ibank2ccom.dll	a98521ffd2a84491d470045b70b9de697c411b9c	Модуль ПБЗИ «Агава-С» (вер. 5.0) для ОС Windows
lib/freebsd-i586/ libibank2agava.so	752642e6c406a8fa7c9c534761706c14f7099f8b	Модуль ПБЗИ «Агава-С» (вер. 5.0) для ОС FreeBSD

Руководитель Банка

_____ / _____

АНКЕТА

Заявка по настройке параметров безопасности ДБО «iBank 2»

Параметры настройки ДБО, обеспечивающие	
максимальное удобство пользования и <u>очень низкий уровень безопасности</u>	обеспечивающие более высокий уровень безопасности.
Носитель ключей ЭЦП	
<input type="checkbox"/> На диске	<input type="checkbox"/> USB – токен «iBank 2 Key» или <input type="checkbox"/> смарт-карта «iBank 2 Key»
Аутентификации	
<input type="checkbox"/> Однофакторная аутентификации <input type="checkbox"/> Не использовать подтверждение документов	<input type="checkbox"/> Многофакторная аутентификации <input type="checkbox"/> Подтверждение ОТП документов на сумму свыше _____ <input type="checkbox"/> с помощью SMS тел.: _____ <input type="checkbox"/> с помощью ОТП – токена
Использование IP фильтра	
<input type="checkbox"/> Не использовать	<input type="checkbox"/> Указать конкретный IP адрес или сеть где будет установлена система ДБО _____ <input type="checkbox"/> Указать доверенный регион _____ <input type="checkbox"/> Автоматическая настройка IP фильтра
Уведомление о событиях в системе	
<input type="checkbox"/> Не использовать	<input type="checkbox"/> Использовать
Фильтры платежей*	
<input type="checkbox"/> По умолчанию (платежи на счета физ. лиц и в платежные системы с электронными кошельками)	<input type="checkbox"/> счет получателя 30301 (БК СБРФ) <input type="checkbox"/> счет получателя 30232 (БК БМ и д.р.) <input type="checkbox"/> счет получателя 47422 (БК ВТБ 24)
Кодовое слово	
Ответственное лицо	
Контактная информация по ответственному лицу	
Телефон:	Е-Mail:

Руководитель Клиента

_____ / _____
(должность)

М.П.

_____ / _____
(подпись) (Ф.И.О.)

Предупреждение!

Уважаемый Клиент, выбирая те или иные настройки безопасности, Вы должны хорошо себе представлять уровень риска, которому Вы подвержены используя систему ДБО работающую через публичные сети передачи данных. Сочетание тех или иных настроек безопасности «iBank 2» в комплексе с выполнением норм «Правил доступа клиентов кредитной организации к услугам ДБО с указанием мер информационной безопасности» должно обеспечить должный уровень безопасности и удобства пользования системой «iBank 2».

Выбранные настройки безопасности системы «iBank 2» соответствуют требованиям _____ по уровню безопасности при работе с системами ДБО работающим через публичные сети передачи данных. С рисками связанными с использованием систем ДБО, публичных сетей передачи данных и не соблюдением мер «Правил доступа клиентов кредитной организации к услугам ДБО с указанием мер информационной безопасности» ознакомлен, претензий к Банку по обеспечению информационной безопасности при работе с системой ДБО «iBank 2» не имею.

Руководитель Клиента

_____ / _____
(должность)

М.П.

_____ / _____
(подпись) (Ф.И.О.)

Приложение № 6 к

1. Порядок формирования, хранения, смены и блокировки ЭЦП

1.1. В процессе предварительной регистрации Клиент самостоятельно создает секретный ключ ЭЦП и парный ему открытый ключ ЭЦП. При формировании ключей ЭЦП Клиент вводит блокировочное слово, предназначенное для голосовой аутентификации (подтверждения подлинности) Клиента для экстренной блокировки доступа к Системе.

В связи с распространением шпионских программ, приводящих к краже или компрометации секретных ключей пользователей систем интернет-банкинга, Банк настоятельно рекомендует в качестве носителя ключевой информации использовать специализированный аппаратный ключ, выполненный в виде USB-ключа. Данное аппаратное решение распространяется за отдельную плату согласно тарифам и может быть использовано для хранения нескольких секретных ключей одновременно.

1.2. Секретный ключ ЭЦП Клиента сохраняется в файле на носителе Клиента или USB-ключе, а открытый ключ посредством сети Интернет передается в Банк (открытый ключ регистрируется в Банке).

1.3. Также открытый ключ ЭЦП распечатывается Клиентом на бумажном носителе в виде Сертификата регистрации открытого ключа ЭЦП в двух экземплярах и заверяется подписью Клиента. Распечатка Сертификата регистрации открытого ключа ЭЦП хранится в Банке и у Клиента, а ее электронный аналог находится в каталоге ключей Банка и Клиента.

1.4. Секретный ключ ЭЦП защищается паролем и данный пароль является конфиденциальной информацией Клиента.

1.5. Владелец Сертификата регистрации открытого ключа ЭЦП несет персональную ответственность за обеспечение сохранности ключевой информации и защиту ключевых файлов (элементов) от несанкционированного доступа.

1.6. Все процедуры окончательной регистрации и проверки открытого ключа ЭЦП происходят в помещении, на программном обеспечении и оборудовании Банка.

1.7. При регистрации открытого ключа Клиента в Банке производится сверка открытого ключа Клиента с открытым ключом, напечатанным в Сертификате регистрации открытого ключа ЭЦП, и проверка данных Клиента, на имя которого сформирован ключ ЭЦП.

1.8. Ключ ЭЦП активизируется только после получения заверенного Клиентом Сертификата ключа подписи и положительных результатов проверки Сертификата.

2. Порядок хранения и смены ключей ЭЦП

2.1. Клиент обеспечивает сохранность, неразглашение и нераспространение своего секретного ключа ЭЦП.

2.2. Срок действия ключей ЭЦП устанавливается в течение одного календарного года с момента их изготовления.

2.3. Смена ключей ЭЦП (т.е. формирование новой пары ключей ЭЦП) может быть произведена в следующих случаях:

- истечение срока действия ключей ЭЦП;
- компрометация ключей ЭЦП.

2.4. Срок хранения открытого ключа ЭЦП (в бумажном и электронном виде), выведенного из употребления, соответствует сроку хранения документов, подписанных и зашифрованных ключами ЭЦП.

3. Порядок блокировки ключей ЭЦП

3.1. Блокировка ключей ЭЦП может осуществляться по инициативе Банка или Клиента (по телефонному звонку) в случае подозрения в компрометации ключа ЭЦП.

3.2. Блокирование скомпрометированного ключа ЭЦП на основании телефонного звонка Клиента в Банк осуществляется с применением блокировочного слова, подтверждающего подлинность Клиента.

3.3. Банк может блокировать ключ ЭЦП самостоятельно, в случае подозрения в его компрометации, уведомляя об этом Клиент

3.4. В случае блокирования ключа ЭЦП прием и обработка ЭД, подписанных данным ключом ЭЦП, не осуществляется.

3.5. Снятие блокировки скомпрометированного ключа ЭЦП осуществляется на основании письменного заявления Клиента, представленного им в Банк при личной явке представителя Клиента.

Руководитель Клиента

_____ /
(должность)

М.П.

_____ /
(подпись)

_____ /
(Ф.И.О.)

Правила доступа клиентов кредитной организации к услугам ДБО с указанием мер информационной безопасности

Для снижения рисков, возникающих при дистанционном банковском обслуживании, особенно с применением интернет-технологий, КБ «КБР БАНК» (ООО) настоятельно рекомендует Вам выполнять следующие требования:

Общие требования безопасности при работе в сети интернет:

- При работе с электронной почтой не открывать письма и вложения к ним, полученные от неизвестных отправителей, не переходить по содержащимся в таких письмах ссылкам.

- Своевременно обновлять операционную систему (установка патчей, критических обновлений).

- Не использовать права администратора при отсутствии необходимости. В повседневной работе входить в систему как пользователь, не имеющий прав администратора.

- Периодически просматривать журнал событий операционной системы и реагировать на ошибки.

- Установить и своевременно обновлять на компьютере антивирусное программное обеспечение (ПО) (AVAST, NOD32, Kaspersky, Symantec AntiVirus и т.д.).

- Антивирусное ПО должно быть запущено постоянно с момента загрузки компьютера. Рекомендуется полная еженедельная проверка компьютера на наличие вирусов, удаление обнаруженного вредоносного ПО.

- При выходе в Интернет использовать сетевые экраны (встроенный в MS Windows, аппаратные межсетевые экраны, Kerio winroute, Outpost firewall и т.д.), разрешив доступ только к доверенным ресурсам сети Интернет.

- Не давать разрешения неизвестным программам выходить в сеть Интернет.

- При работе в интернет не соглашаться на установку каких-либо дополнительных программ.

Требования к персональному компьютеру, используемому при работе в системе «Клиент-Банк»:

- Должен быть установлен и обновлен антивирус.

- Должен быть установлен и настроен межсетевой экран.

- Пароли учетных записей, обладающих правами администратора, должны быть сложными (содержать заглавные и строчные буквы, цифры, спецсимволы, длина не менее 8 символов).

- Учетная запись «Гость» должна быть выключена.

- Не должно быть учетных записей с пустыми паролями.

- Должны быть установлены все критические обновления к установленной операционной системе.

- Воздерживаться от использования программ онлайн-общения (таких, как ICQ) на компьютере, используемом для работы в системе «Банк-Клиент».

Комплекс мер безопасности при работе в системе «Клиент-Банк»:

Ключевая информация – это аналог *Вашей личной подписи*, при ее использовании соблюдайте следующие правила:

- После выработки *рабочих ключей ЭЦП* необходимо создать резервную копию ключевого носителя, хранимую в сейфе;

- Ключевой носитель с *рабочими ключами ЭЦП* нельзя передавать третьим лицам, оставлять без присмотра, хранить в доступном месте.

- Ключевой носитель должен использоваться только владельцем сертификата ключевой информации, либо лицом, уполномоченным на использование ЭЦП.

- На электронном носителе (дискета, флеш-карта, CD), на котором расположены ключи ЭЦП, не должно быть *другой информации*;

- Хранение закрытого ключа ЭЦП на жёстком диске **НЕДОПУСТИМО**.

- Для просмотра выписки использовать систему "*Выписка on-line*", не требующую использования ключей ЭЦП.

- По истечении срока действия ключа ЭЦП, необходимо провести его плановую замену.

- Настоятельно не рекомендуется использовать компьютер, на котором установлена система ДБО для выполнения поиска в сети интернет, посещения развлекательных и прочих ресурсов, официальный владелец которых не известен или не вызывает доверия.

- Работа с системой ДБО с гостевых рабочих мест (интернет-кафе и т.д.) значительно увеличивает риск хищения и дальнейшего неправомерного использования ключей ЭЦП и другой аутентификационной информации.

- Должен быть исключен доступ (физический и/или удаленный) к компьютеру лиц, не имеющих полномочий для работы в системе «Клиент-Банк».

- В случае передачи (списания) компьютера (ноутбука), на котором ранее была установлена система «Клиент-Банк», необходимо гарантированно удалить с него всю информацию, использование которой третьими лицами может потенциально нанести вред финансовой деятельности или имиджу Вашей организации, в том числе следы работы в системе «Клиент-Банк».

- Настоятельно рекомендуем, при работе с системой «Клиент-Банк» использовать USB-Токе-

ны. Защищенное хранение и неизвлекаемость секретного ключа ЭЦП при использовании USB-токена делает невозможным хищение секретных ключей ЭЦП, используемых при работе в системе.

- Сменный носитель с ключевой информацией должен быть установлен в считывающее устройство компьютера только на время проведения платежной операции и операций обмена с Банком. Размещение сменного носителя в считывателе на продолжительное время существенно повышает риск несанкционированного доступа к ключевой информации третьими лицами.

Регулярно меняйте пароль для работы в системе «Клиент-Банк». Используйте сложные пароли, чтобы длина Вашего пароля была не менее 8 символов, и представлял собой сочетание заглавных и прописных букв, цифр и, если возможно, спецсимволов. Мы крайне не рекомендуем Вам использовать простые пароли (например, имена, фамилии, номера телефонов, года рождения и т.д.).

При смене, увольнении лица, имеющего, даже потенциально, доступ к ключевому носителю (например, системного администратора), необходимо незамедлительно:

- Сменить пароль доступа;
- Произвести регенерацию ключей ЭЦП при содействии сотрудников Банка.

Для дополнительной защиты Ваших денежных средств настоятельно рекомендуем как можно чаще контролировать состояние счёта (путем просмотра выписки) при помощи систем "Выписка on-line" или "Телефон-Клиент".

Просим вас незамедлительно обращаться в банк при возникновении следующих ситуаций:

- На компьютере, используемом для работы в интернет-банке, обнаружено вредоносное ПО (вирусы, «трояны» и т.д.);

- Обнаружены факты проникновения в систему посторонних лиц;
- В выписке обнаружены несанкционированные Вами расходные операции;
- У Вас не работает система «Банк-Клиент» по неизвестным причинам.

Обращаем Ваше внимание, что **своевременное** обращение в Банк позволит принять оперативные меры по предотвращению мошенничества. Сотрудники Отдела автоматизации готовы оказать помощь по вопросам соблюдения требований безопасности при работе в сети Интернет и использования систем ДБО «Клиент-Банк» и «Интернет-Клиент».

Руководитель Клиента

_____ / _____
(должность)

М.П.

_____ / _____
(подпись)

_____ / _____
(Ф.И.О.)

Телефон службы технической поддержки КБ «КБР БАНК» (ООО) – (495) 380-0897