

ДОГОВОР

на обслуживание Клиента в системе дистанционного банковского обслуживания «Клиент-Банк» (ТИПОВАЯ ФОРМА)

1. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

В целях исполнения настоящего Договора применяемые в нем термины и определения будут иметь следующие значения:

«Банк» - Братский Акционерный Народный коммерческий Банк (Акционерное общество) (сокращенное наименование – «Братский АНКБ» АО).

«Клиент» - юридическое лицо, индивидуальный предприниматель, физическое лицо, занимающееся в установленном законодательством порядке частной практикой, находящееся на обслуживании в Банке на основании Договора банковского счета, использующие электронный документооборот системы «Клиент-Банк» в соответствии с законодательством и настоящим Договором.

«Система «Клиент-Банк» (СКБ) – система дистанционного банковского обслуживания, предназначенная для удаленного обслуживания Клиента с использованием сети Интернет, представляющая собой совокупность программно-аппаратных средств, устанавливаемых на территории Клиента и Банка и согласованно эксплуатируемых Клиентом и Банком в соответствующих частях, а также организационных мероприятий, проводимых Клиентом и Банком, с целью предоставления Клиенту услуг по настоящему Договору.

«Банковская часть СКБ» - Сервер Приложения iBank2 с необходимыми серверными модулями и Сервер БД iBank2.

«Клиентская часть СКБ» - web-приложение, запускаемое в браузере на компьютере пользователя и/или приложение РС-Банкинг для работы офлайн.

«Средство криптографической защиты информации Крипто-Ком 3.4 (СКЗИ)» - аппаратно–программные средства разработки ЗАО «Сигнал-КОМ» предназначенные для выполнения следующих операций:

- выработки ключей шифрования и электронной (цифровой) подписи (ЭП);
- шифрования и имитозащиты данных;
- обеспечения целостности и подлинности информации.

«Электронный документ» (ЭД) – документ, представленный в электронном виде (файл-документ) и подписанный Электронной подписью (ЭП) Клиента, имеющий равную юридическую силу с расчётными или иными документами на бумажных носителях, собственноручно подписанными уполномоченными лицами согласно карточки образцов подписей и заверенными оттиском печати. Электронный документ может быть платёжным (в этом случае он является основанием для совершения операций по счетам Клиента, открытым в Банке), либо служебно-информационным.

«Счет» – банковский счет, открываемый Клиенту в Банке на основании соответствующего договора банковского счета, заключаемого между Клиентом и Банком.

«Электронный платёжный документ (Платёжный ЭД)» – направляемый Клиентом в Банк посредством СКБ для последующего исполнения документ (платежное поручение, инкассовое поручение, платежное требование, поручение на покупку/продажу иностранной валюты, заявление на перевод иностранной валюты, распоряжение на обязательную продажу иностранной валюты, поручение на конвертацию иностранной валюты и иные платежные документы согласно требованиями действующего Положения о правилах осуществления перевода денежных средств, утвержденного Банком России 19.06.2012 N 383-П), подписанный необходимым Сочетанием ЭП Клиента.

«Служебно-информационный документ» – направляемый Клиентом в Банк посредством СКБ документ, не содержащий распоряжение Клиента о перечислении денежных средств со Счета, подписанный корректной ЭП Владельца Ключа. К таким документам относятся:

- письмо;
- заявления на акцепт и на отзыв заявления на акцепт;
- справка о подтверждающих документах;
- сведения о валютных операциях;
- заявление о постановке на учет контракта (кредитного договора);
- заявление о снятии с учета контракта (кредитного договора);
- заявление о внесении изменений в I раздел ведомости банковского контроля;
- иные документы и информация, требование о представлении (направлении) которых предусмотрено законодательством Российской Федерации, в том числе нормативными актами Банка России и техническими возможностями установленной версии СКБ.

«Электронная подпись» (ЭП) – специальный уникальный код, добавляемый в файл-документ, являющийся средством защиты информации от несанкционированного доступа. ЭП используется для подтверждения аутентичности (подтверждение авторства и целостности) электронного документа. ЭП является аналогом печати и собственноручной подписи Клиента при бумажном делопроизводстве. ЭД, подписанный ЭП в соответствии с настоящим Договором, считается подписанным усиленной неквалифицированной электронной подписью.

«Усиленная электронная подпись» – неквалифицированная электронная подпись, которая:

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

«Пара ключей ЭП Клиента» – секретный ключ ЭП Клиента и соответствующий ему Открытый ключ ЭП Клиента.

«Секретный ключ ЭП Клиента» – ключ (последовательность байт), генерируемый Клиентом с использованием средств СКБ, и предназначенный для формирования Клиентом ЭП ЭД. Термин «секретный ключ электронной подписи» соответствует термину «ключ электронной подписи», определенному в п.5 ст.2 Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи» (далее – Федеральный закон № 63-ФЗ).

«Открытый ключ ЭП Клиента» – ключ (последовательность байт), зависящий от секретного ключа ЭП Клиента, самостоятельно генерируемый Клиентом с использованием средств СКБ, и предназначенный для проверки Банком корректности ЭП ЭД, сформированного Клиентом. Термин «открытый ключ электронной подписи» соответствует термину «ключ проверки электронной подписи», определенному в п.6 ст.2 Федерального закона № 63-ФЗ.

«Владелец ключа» - физическое лицо, указанное Клиентом в Сертификате открытого ключа ЭП Клиента, уполномоченное Клиентом подписывать Электронные документы Клиента в объеме и порядке, определенным Клиентом. Владельцы Ключа ЭП наделяются правом подписи Платёжных документов Клиента при условии внесения их в Карточку с образцами подписей и оттиска печати Клиента, либо в соответствии с п.6.29 настоящего Договора владельцу ключа предоставляется доступ к выпискам по счету Клиента. Каждый Владелец Ключа ЭП, надлежащим образом наделенный правом подписи Платёжных документов Клиента, имеет право единолично подписывать Неплатёжные документы Клиента.

«Корректная электронная подпись Клиента» – ЭП ЭД Клиента, дающая положительный результат его проверки с открытым ключом ЭП Клиента.

«Сертификат открытого ключа ЭП Клиента» (Сертификат) – бумажный документ с представленным в шестнадцатеричном виде открытым ключом ЭП Клиента, датой начала и окончания действия открытого ключа ЭП Клиента, заверенный подписью (подписями) уполномоченных лиц и скрепленный печатью Клиента.

«Активный открытый ключ ЭП Клиента» - открытый ключ ЭП Клиента, зарегистрированный Банком в СКБ, и используемый Клиентом в текущее время для работы в СКБ.

«Карточка с образцами подписей» - карточка с образцами подписей лиц, имеющих право подписывать расчётные документы Клиента, и оттиском печати Клиента (при наличии), предоставляемая в Банк Клиентом в соответствии с условиями соответствующего договора банковского счёта.

«Сочетание ЭП Клиента» – количество и комбинация корректных ЭП Владельцев Ключей, внесенных в Карточку с образцами подписей и оттиска печати, необходимое для принятия Банком к исполнению расчётных (платёжных) документов Клиента. Сочетание ЭП Клиента устанавливается Сторонами Соглашением о возможных сочетаниях собственноручных подписей.

«Соглашение о возможных сочетаниях собственноручных подписей» – соглашение о возможных сочетаниях собственноручных подписей лиц, наделенных правом подписи расчетных (платёжных) документов Клиента, необходимых для подписания документов, содержащих распоряжение Клиента (по форме Банка), заключаемое между Сторонами. Данное Соглашение предусматривает количество и комбинацию собственноручных подписей лиц, внесенных в Карточку с образцами подписей и оттиска печати Клиента, необходимых для принятия Банка к исполнению Расчетных документов Клиента.

«Блокировочное слово» – уникальное слово, определяемое Клиентом при регистрации в Системе «Клиент-Банк», для блокирования работы Клиента по телефонному звонку в Банк.

«Многофакторная аутентификация» – дополнительная проверка подлинности Клиента, проводимая с использованием разового пароля, полученного посредством короткого сообщения (SMS), либо аппаратного устройства (MAC-токен). В зависимости от выбранного Клиентом метода многофакторной аутентификации, проверка осуществляется при входе Клиента в СКБ, а так же

при передаче Клиентом посредством СКБ отдельного платёжного поручения или пакета/ группы платёжных поручений.

«MAC-токен» (Средство хранения ключей ЭП Клиента и средство подтверждения ЭП Клиента) - аппаратное устройство, позволяющие генерировать одноразовые пароли для дополнительной аутентификации Клиента при входе в систему «Клиент-Банк» и/или подтверждения Клиентом совершения расходных операций по счету. Предоставляется Банком Клиенту во временное пользование на период действие настоящего Договора.

(USB-токен) (Средство хранения ключей ЭП Клиента) – компактное устройство в виде USB – брелока, служащее для авторизации Клиента в СКБ, с неизвлекаемым хранением ключей ЭП, генерирующее ключи ЭП внутри себя, обеспечивающее их защищенное неизвлекаемое хранение в защищенной долговременной памяти и формирующее усиленную ЭП под электронными документами внутри устройства. Предоставляется Банком Клиенту во временное пользование на период действие настоящего Договора.

«Носитель ключевой информации (НКИ)» - MAC-токен или USB-токен.

«Автоматизированное рабочее место Клиента (АРМ Клиента)» – аппаратно-программные средства, средства вычислительной техники, телекоммуникационное оборудование Клиента, используемое им для работы с СКБ в рамках настоящей Оферты.

«Компрометация ключа ЭП» - утрата доверия к тому, что используемый ключ ЭП (пара ключей ЭП) обеспечивает безопасность информации. К событиям, связанным с компрометацией ключа ЭП (пары ключей ЭП), относятся, в том числе, следующие события:

- утрата НКИ;
- утрата НКИ с последующим обнаружением;
- нарушение правил хранения НКИ;
- несанкционированное копирование ключа ЭП по вине клиента (при такой возможности);
- случаи, когда нельзя достоверно установить, что произошло с ключом ЭП (в том числе случаи, когда ключ ЭП вышел из строя и доказательно не опровергнута возможность того, что данный факт произошел в результате несанкционированных действий злоумышленника);
- возникновение подозрений на утечку информации или ее искажение в системе «Клиент-Банк»;
- доступ посторонних лиц к НКИ;
- иные обстоятельства, прямо или косвенно свидетельствующие о наличии возможности несанкционированного доступа третьих лиц к ключу ЭП.

«Пакет/группа электронных платёжных поручений» - ЭД, к которому присоединены один или несколько связанных между собой платёжных ЭД. При подписании пакета (группы) документов ЭП, каждый из присоединенных платёжных ЭД, составляющих пакет, считается подписанным ЭП, которой подписан пакет документов.

Иные, не урегулированные настоящим разделом Договора на обслуживание Клиента в системе дистанционного банковского обслуживания «Клиент-Банк» термины и понятия, используемые в тексте настоящего Договора, применяются в соответствии с терминологией, определённой Федеральным законом от 06.04.2001 № 63-ФЗ «Об электронной подписи».

2. ОБЩИЕ ПОЛОЖЕНИЯ

2.1. Настоящий Договор на обслуживание Клиента в системе дистанционного банковского обслуживания «Клиент-Банк» (далее – Договор) является Договором присоединения, регулирующим отношения по обслуживанию Клиента в системе дистанционного банковского обслуживания «Клиент-Банк» в Банке.

2.2. Опубликование Договора, включая распространение его текста и приложений к нему на официальном сайте Банка www.aikb.ru, необходимо рассматривать как публичное предложение (оферта) Банка, адресованное Клиенту, заключить Договор на предлагаемых условиях в соответствии со ст.428 Гражданского Кодекса РФ.

2.3. Предметом настоящего Договора является установление между Банком и Клиентом (далее - Стороны):

- порядка обмена платёжными ЭД при осуществлении расчётов через Банк;
- порядка обмена электронными служебно-информационными документами и документами, предоставляемыми в целях валютного контроля;
- прав и обязанностей Сторон для работы в СКБ, в том числе обязанностей по обеспечению информационной безопасности при обмене ЭД с использованием СКБ.

2.4. Банк осуществляет подключение Клиента к СКБ с предоставлением Клиенту консультаций по вопросам подключения и работы Клиента в СКБ.

2.5. Настоящий Договор распространяется на все счета Клиента, зарегистрированные в системе «Клиент-Банк».

2.6. Заключение Договора между Сторонами производится путем присоединения Клиента к условиям настоящего Договора (акцепта Договора) в следующем порядке: Клиент представляет в Банк подписанное со своей стороны Заявление о присоединении к Договору на бумажном носителе в двух экземплярах, составленном по форме Приложения № 1 к Договору.

В случае если Клиент уже осуществляет электронный документооборот с Банком посредством СКБ на основании соответствующего договора, заключенного между Банком и Клиентом, Клиент вправе присоединиться к условиям настоящего Договора, предоставив в Банк Заявление о присоединении к Договору на бумажном носителе в двух экземплярах, составленном по форме Приложения № 1 к Договору при этом:

- договор, применяемый до введения настоящего Договора, считается измененным и изложенным в редакции настоящего Договора, со дня принятия Банком Заявления Клиента о присоединении;
- комиссия за подключение не взимается.

2.7. Доступ Клиента к СКБ предоставляется через сеть Интернет. Способ, которым Клиент получает доступ к сети Интернет, не является предметом Договора на обслуживание Клиента по СКБ.

2.8 Стороны принимают на себя обязательства не разглашать полученные в ходе исполнения Договора сведения, составляющие банковскую и иную конфиденциальную информацию каждой из Сторон.

2.9 Под сведениями, составляющими банковскую тайну, понимаются сведения, указанные в статье 26 Федерального закона «О банках и банковской деятельности».

Под сведениями, составляющими конфиденциальную информацию, в Договоре понимаются не являющиеся общедоступными сведения о применяемых технологиях, а также об управлении, финансовой и иной деятельности каждой из Сторон, разглашение которых может привести к возникновению убытков и/или негативно повлиять на деловую репутацию любой из Сторон, включая, но не ограничиваясь:

- информацией о технических и программных возможностях Сторон (сетевые адреса, пароли, используемые пакеты прикладных программ и т.п.);
- информацией о тарифной политике Сторон;
- - сведениями о методике и содержании информационного обмена между Сторонами.

2.10 Стороны обязуются сохранять конфиденциальность в отношении условий Договора и не разглашать их любым третьим лицам, за исключением случаев письменного разрешения другой Стороны, а также случаев, предусмотренных законодательством Российской Федерации.

3. СОГЛАШЕНИЯ СТОРОН

3.1. Стороны признают, что используемое в СКБ средство криптографической защиты информации Кристо-Ком 3.4, которое обеспечивает шифрование, контроль целостности электронного документа и электронную подпись, достаточно для защиты информации от несанкционированного доступа, подтверждения подлинности и авторства ЭД, а также разбора конфликтных ситуаций.

3.2. Стороны признают, что при произвольном изменении ЭД, заверенного ЭП, ЭП становится некорректной, то есть проверка ЭП дает отрицательный результат.

3.3. Стороны признают, что подделка ЭП Клиента, то есть создание корректной ЭП ЭД от имени Клиента, невозможно без знания секретного ключа ЭП Клиента.

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

3.5. Стороны признают, что ЭД с ЭП Клиента, создаваемые СКБ в Банке, являются доказательным материалом для решения спорных вопросов в соответствии с Приложением № 4 – «Порядок проведения технической экспертизы при возникновении спорных ситуаций» – настоящего Договора. ЭД, не имеющие необходимого количества ЭП, при наличии спорных вопросов не являются доказательным материалом.

3.6. Стороны признают, что открытый ключ ЭП Клиента, указанный в заверенном подписью руководителя и оттиском печати Клиента Сертификате открытого ключа ЭП Клиента, принадлежит Клиенту.

3.7. Стороны признают, что способом уведомления Клиента о состоянии ЭД являются следующие статусы:

- «На обработке» - о получении Банком ЭД;
- «В картотеке» - о помещении Банком ЭД в очередь распоряжений;
- «Исполнен» - об исполнении Банком ЭД;
- «Отвергнут» - об аннулировании Банком ЭД.

В системе «Клиент-Банк» Клиенту доступна информация, содержащая реквизиты Банка, вид операции, дату операции, сумму операции, идентификатор операции, статус ЭД, а так же информация, позволяющая идентифицировать аннулируемый ЭД, дату его аннулирования и причину.

3.8. Дата отправления/принятия ЭД, переданного с использованием СКБ, регистрируется системой и признается Сторонами фактической датой получения/отправки этого ЭД. Данные по проведенным операциям текущего операционного дня по счету Клиента отражаются в выписке. Обновление данных в СКБ осуществляется непрерывно.

3.9. Стороны признают, что Банк осуществляет обработку полученных от Клиента персональных данных в соответствии с Федеральным законом от 27.07.2006 г. № 152-ФЗ «О персональных данных» (далее – Федеральный закон «О персональных данных»). Согласно Федеральному закону «О персональных данных» к персональным данным физического лица относятся его фамилия, имя, отчество, дата и место рождения, гражданство, адрес, реквизиты документа, удостоверяющего личность, и другая информация об указанном лице, полученная Банком. Обработка персональных данных осуществляется Банком только в целях исполнения настоящего Договора. Сроки обработки персональных данных определяются Договором и регламентирующими документами к нему.

3.10. Стороны признают в качестве единой шкалы времени при работе с СКБ Иркутское поясное время. Контрольным является время системных часов аппаратных средств Банка.

4. ПОРЯДОК ПОДКЛЮЧЕНИЯ, ПОЛУЧЕНИЯ ДОСТУПА КЛИЕНТА К СИСТЕМЕ «КЛИЕНТ-БАНК» И ИСПОЛЬЗОВАНИЯ ЭЛЕКТРОННОЙ ПОДПИСИ

4.1. Порядок подключения и получения доступа Клиента к системе «Клиент-Банк» основан на использовании электронной подписи в соответствии с законодательством, Руководством пользователя Системы «Клиент-Банк» для корпоративных клиентов и настоящим Договором.

4.2. В целях подключения Клиента к системе «Клиент-Банк» Клиенту следует:

4.2.1. Ознакомиться с размещенными на общедоступных ресурсах Банка (информационных стендах в операционных залах и на сайте Банка <http://www.ankb.ru/>) документами:

- Настоящим Договором и всеми приложениями, в т.ч. памяткой клиенту о возможных угрозах хищения денежных средств с использованием системы «iBank 2» и способах защиты (Приложение № 5 к настоящему Договору);
- Руководством пользователя Системы «Клиент-Банк» для корпоративных клиентов, содержащим условия использования СКБ;
- Тарифами Банка.

4.2.2. Предоставить в Банк Заявление о присоединении по форме Приложения № 1 к настоящему Договору (в двух экземплярах). Документы предоставляются в Банк на бумажном носителе, подписанные собственноручной подписью уполномоченного лица и скрепленные оттиском печати Клиента (при наличии).

4.2.3. Оплатить комиссию за установку автоматизированного рабочего места Клиента в соответствии с Тарифами Банка.

4.2.4. Получить USB-токен/MAC-токен. Факт приема - передачи USB-токена/MAC-токена подтверждается Актом приема-передачи USB-токена/MAC-токена, оформляемым Банком по форме Приложения № 2 к настоящему Договору.

4.2.5. Пройти процедуру предварительной регистрации в СКБ. Указанная процедура осуществляется Клиентом самостоятельно на сервере СКБ в соответствии с «Инструкцией по регистрации для клиента системы «Клиент-Банк», размещенной на сайте Банка в разделе Главная/Клиент-Банк/Документация. В результате предварительной регистрации Клиента в СКБ формируются ключ ЭП и ключ проверки ЭП. После формирования и сохранения ключа проверки ЭП на НКИ, необходимо распечатать его сертификат в двух экземплярах на бумажный носитель.

4.2.6. Предоставить в Банк указанный в подпункте 4.2.5. настоящего Договора Сертификат ключа проверки ЭП Клиента на бумажном носителе в 2 (Двух) экземплярах, подписанных собственноручной подписью уполномоченного лица и скрепленные оттиском печати Клиента (при наличии) для окончательной регистрации Банком Клиента в СКБ.

4.2.7. Банк производит регистрацию Клиента в системе «Клиент-Банк» в срок не позднее следующего рабочего дня, после прохождения процедур, указанных в пункте 4.2. Договора.

4.3. После исполнения процедур, указанных в пункте 4.2. настоящего Договора, Клиенту следует получить свои экземпляры следующих документов:

- Заявление о присоединении по форме Приложения № 1 к настоящему Договору с отметкой Банка о его принятии;
- Сертификат ключа проверки ЭП;
- Акт приема-передачи USB-токена/MAC-токена по форме Приложения № 2 к настоящему Договору.

- Памятка для работы с sms-подтверждением Приложение № 7 к настоящему Договору.

4.4. После завершения процедур подключения Клиента к СКБ и оформления пакета документов, указанных в настоящем пункте, Клиент производит тестовый (проверочный) сеанс связи по СКБ с передачей тестового документа и получением выписки по счетам. После тестового сеанса связи Клиент направляет по СКБ подтверждение (письмо в свободной форме) о своей готовности работать по ней.

4.5. В случае утраты или порчи Клиентом НКИ Банк отключает его от обслуживания в СКБ в соответствии с пунктами 5.8. или 5.11 Договора. Повторное подключение Клиента производится в рамках настоящего Договора после уплаты Клиентом комиссионного вознаграждения в соответствии с пунктом 4.2.3. Договора.

5. ОБЯЗАННОСТИ И ПРАВА БАНКА

Банк обязан:

5.1. Консультировать Клиента по вопросам эксплуатации системы «Клиент-Банк» и ее настройке, в том числе, размещая актуальную информацию на общедоступных ресурсах Банка (информационных стендах в операционных залах и на сайте Банка <http://www.ankb.ru/>).

5.2. Осуществлять обеспечение полной защиты банковской части СКБ от несанкционированного доступа третьих лиц.

5.3. Обеспечить сопровождение СКБ, включая обновление её версий, в течение срока действия настоящего Договора.

5.4. Регистрировать в течение 3 (трех) рабочих дней новый ключ ЭП Клиента на основании предоставленного Сертификата ключа проверки ЭП.

5.5. Принимать к исполнению ЭД, полученные по СКБ от Клиента, подписанные необходимым количеством ЭП сотрудников Клиента, соответствующие требованиям настоящего Договора и действующему законодательству РФ.

5.6. Принимать по требованию Клиента расчётные (платёжные) и служебно-информационные документы Клиента и передавать сведения по счетам не только в электронной форме, но и обычным путем в установленном порядке.

5.7. Блокировать по требованию Клиента в СКБ существующие активные открытые ключи ЭП Клиента и зарегистрировать новые открытые ключи ЭП Клиента.

5.8. Временно блокировать работу Клиента в СКБ по телефонному звонку Клиента после произнесения Клиентом блокировочного слова и до получения от Клиента письменного уведомления о начале работы в СКБ.

5.9. Сохранять сертификаты выведенных из действия открытых ключей ЭП Клиента в течение сроков хранения ЭД, в которых использовались данные ключи.

5.10. В случае заявления Клиентом своих IP-адресов Банк обязан осуществлять обмен электронными документами с Клиентом с использованием только заявленных Клиентом IP-адресов.

5.11. Немедленно приостанавливать операции по счёту Клиента с использованием СКБ при потере контроля над СКЗИ и/или ЭП Клиента.

Банк имеет право:

5.12. По своему усмотрению без уведомления Клиента блокировать активный открытый ключ ЭП Клиента, и потребовать от Клиента смены пары ключей ЭП Клиента.

5.13. Осуществлять автоматизированную обработку персональных данных, содержащихся в Сертификатах открытых ключей ЭП Клиентов. Банк имеет право на сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (предоставление надзорным органам, доступ сотрудникам Банка для исполнения ими своих должностных обязанностей), обезличивание, блокирование, удаление, уничтожение персональных данных на период действия Договора, а также в течение срока хранения электронных документов, при оформлении которых использовались данные Сертификатов Клиента. Банком не допускается публичное обнародование персональных данных, указанных в Сертификатах, в средствах массовой информации, а также размещение в информационно-телекоммуникационных сетях.

5.14. Потребовать от Клиента оформления расчетного (платёжного) документа на бумажном носителе за подписью лиц, заявленных в карточке с образцами подписей и оттиска печати, скрепленного печатью Клиента, приостановив исполнение Платёжного документа, полученного по СКБ, сообщив об этом Клиенту не позднее следующего рабочего дня со дня получения соответствующего платёжного документа по СКБ.

5.15. В случае возникновения у Банка технических неисправностей или других обстоятельств, препятствующих использованию Клиентом ЭП, Банк имеет право в одностороннем порядке приостановить до момента устранения неисправности использование ЭП Клиентом, уведомив об этом Клиента (письменно и/или по телефону). Все документы в этом случае должны передаваться

сторонами на бумажных носителях в общем порядке.

5.16. Не исполнять ЭД Клиента, если они не соответствуют требованиям законодательства к их оформлению, не содержащих ЭП и иных необходимых реквизитов.

5.17. Не принимать ЭД Клиента, если они не прошли дополнительную проверку подлинности Клиента, проводимую с использованием разового пароля (некорректно/неверно/несвоевременно введен пароль, полученный посредством короткого сообщения (SMS) или аппаратным устройством (MAC-токен)).

5.18. Отказать в доступе Клиента в систему «Клиент-Банк» в случае не подтверждения Клиентом входа в систему одноразовым (некорректно/неверно/несвоевременно введен пароль, полученный посредством короткого сообщения (SMS) или аппаратным устройством (MAC-токен)).

5.19. Списывать со счета (счетов) Клиента плату за подключение и обслуживание в СКБ на условиях заранее данного Клиентом акцепта.

5.20. В одностороннем порядке вводить, отменять или изменять тарифы, определяющие стоимость предоставляемых Банком услуг по СКБ.

5.21. В случае недостаточности денежных средств на счете Клиента для оплаты за обслуживание в СКБ в соответствии с Тарифами Банка, Банк прекращает предоставление соответствующей услуги Клиенту по истечении 15 календарных дней с момента возникновения задолженности Клиента.

5.22. Требовать от Клиента предоставления документов и сведений, необходимых в соответствии с требованиями законодательства в области противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма. В случае не предоставления вышеуказанных документов отказать Клиенту в приеме от него распоряжений, подписанных ЭП Клиента, и принимать от Клиента только надлежащим образом оформленные расчетные документы на бумажном носителе. При этом Банк не несёт ответственности по исполнению взятых по настоящему Договору обязательств, и ранее внесённая плата за право пользования СКБ не возвращается.

5.23. Отказать клиенту в заключении Договора на обслуживание в СКБ.

5.24. Отключить Клиента от СКБ при невыполнении Клиентом условий настоящего договора.

6. ОБЯЗАННОСТИ И ПРАВА КЛИЕНТА

Клиент обязан:

6.1. Самостоятельно устанавливать на своем рабочем месте необходимое программное обеспечение и самостоятельно осуществлять предварительную регистрацию в СКБ в соответствии с предоставленными Банком инструкциями.

6.2. Допускать к эксплуатации СКБ только сотрудников, имеющих соответствующую подготовку.

6.3. Обеспечивать информационную безопасность АРМ Клиента. Клиент обязан исключить или максимально ограничить доступ к АРМ Клиента лиц, чья деятельность не связана с осуществлением электронного документооборота с Банком.

6.4. Обеспечивать сохранность и целостность клиентской части программного комплекса СКБ, сохранять конфиденциальность и подлинность секретных ключей ЭП.

6.5. Хранить в секрете и не передавать третьим лицам пароль к секретному ключу ЭП Клиента и НКИ, используемые в СКБ.

6.6. Обеспечить защиту Ключей ЭП Клиента и НКИ от несанкционированного использования третьими лицами.

6.7. Хранить в секрете разовый пароль, полученный посредством короткого сообщения (SMS) или аппаратным устройством MAC-токен, не передавать третьим лицам аппаратное устройство MAC-токен или телефон, на который поступают разовые пароли посредством SMS (Средство подтверждения). Обеспечить защиту разового пароля и Средства подтверждения от несанкционированного использования третьими лицами.

6.8. Обеспечить использование Ключей ЭП только их владельцами (ответственными сотрудниками) в соответствии с установленными правами подписи.

6.9. По требованию Банка сгенерировать новую пару ключей ЭП Клиента и зарегистрировать новый открытый ключ ЭП Клиента в Банке.

6.10. Ознакомиться с памяткой клиенту описанием о возможных угрозах хищения денежных средств с использованием СКБ и способах защиты (Приложение 5 к настоящему Договору). В случае если знаний сотрудников Клиента недостаточно для адекватной оценки механизмов защиты Системы «iBank 2» и/или обеспечения информационной безопасности рабочих мест ответственных сотрудников, Клиент вправе обратиться к услугам сторонних специалистов. Оплата услуг специалистов производится Клиентом самостоятельно.

6.11. Сообщать Банку об обнаружении попытки несанкционированного доступа к СКБ не позднее следующего дня с момента обнаружения, а также извещать Банк обо всех случаях подозрений в компрометации секретных ключей ЭП СКБ не позднее следующего дня с момента

возникновения одним из следующих способов:

- посредством телефонной связи по телефону (3953) 41-49-70, используя для идентификации Клиента «Блокировочное слово» в целях приостановления Банком использования Клиентом системы «Клиент-Банк»;
- путем направления соответствующего сообщения по адресу электронной почты Банка: soft@ankb.ru;
- с помощью факсимильной связи по телефону (3953) 41-65-82 с обязательным последующим направлением в Банк не позднее следующего операционного дня письменного уведомления в произвольной форме, заверенного подписью уполномоченного лица и оттиском печати Клиента (при наличии).

6.12. Соблюдать определенный порядок действий в случае выявления хищения денежных средств в СКБ (Приложение № 6 к настоящему Договору).

6.13. Исполнять обязательства, возникшие до момента приостановления или прекращения использования Клиентом ЭП.

6.14. В случае прекращения использования СКБ вернуть Банку НКИ, уничтожить программное обеспечение СКБ и официально уведомить об этом Банк.

6.15. Представить в Банк персональные данные Владельца Сертификата (Владельца ЭП Клиента) и согласия на обработку (включая автоматизированную обработку) персональных данных Владельцев Сертификатов по форме, установленной Банком.

6.16. Предоставить Банку достоверную информацию для связи и для передачи SMS-сообщений, содержащих одноразовые коды подтверждения ЭД, переданных с использованием СКБ. В случае изменения информации для связи Клиент обязан своевременно предоставить Банку обновленную информацию. Обязанность Банка по информированию Клиента считается исполненной при направлении уведомления в соответствии с имеющейся у Банка информацией для связи с Клиентом.

6.17. Незамедлительно заявить по форме Приложения № 3 к данному Договору о смене телефонных номеров, используемых Банком для передачи SMS-сообщений, содержащих одноразовые коды подтверждения электронных документов, переданных с использованием СКБ.

6.18. Производить плановую смену пары ключей ЭП Клиента до истечения срока их действия (срок действия пары Ключей ЭП Клиента составляет 1 год).

6.19. Производить внеплановую смену Ключа ЭП в случаях:

- компрометации Ключей ЭП Клиента;
- выхода из строя НКИ;
- истечение срока действия ЭП Клиента;
- изменение данных владельцев Ключей ЭП Клиента.

6.20. На регулярной основе принимать в системе «Клиент-Банк» информацию (выписки по счетам, сообщения свободного формата, иные документы), переданную Банком, и производить сверку платежей.

6.21. Заполнять ЭД в СКБ в соответствии с действующим Положением Банка России от 19.06.2012 г. № 383-П «О правилах осуществления перевода денежных средств» или аналогичным документом, утвержденным вместо указанного Положения.

6.22. Руководствоваться актуальной информацией по работе в системе «Клиент-Банк», размещенной на общедоступных ресурсах Банка (информационных стендах в операционных залах и/или на сайте Банка <http://www.ankb.ru/>). Периодически ознакомляться с размещенными на общедоступных ресурсах Банка (информационных стендах в операционных залах и/или на сайте Банка <http://www.ankb.ru/> документами и информацией.

6.23. Своевременно осуществлять оплату за подключение и обслуживание в СКБ в соответствии с разделом 9 настоящего Договора.

Клиент имеет право:

6.24. Осуществлять эксплуатацию предоставленного Банком в составе программного обеспечения сертифицированного СКЗИ в СКБ в соответствии с его функциональным назначением.

6.25. Заявить (в письменном виде в свободной форме с подписью руководителя и оттиском печати) действующие IP-адреса Клиента, с использованием которых будет осуществляться обмен ЭД в рамках настоящего Договора.

6.26. Требовать от Банка предоставления экземпляров расчетных документов на бумажном носителе с отметкой Банка об исполнении в день проведения операции Банком.

6.27. Досрочно прекратить действие своего активного открытого ключа ЭП и потребовать от Банка заблокировать этот активный открытый ключ ЭП Клиента.

6.28. По своему усмотрению генерировать новые пары ключей ЭП Клиента и регистрировать в Банке новые открытые ключи ЭП Клиента.

6.29. По своему усмотрению предоставлять лицам, имеющим соответствующую подготовку для работы в СКБ, доступ к своим выпискам в СКБ. Для этого Клиенту необходимо сгенерировать пару ключей ЭП для просмотра выписок. Регистрация открытого ключа ЭП Клиента, в этом случае, производится после получения Банком письма в произвольной форме на бумажном носителе либо по СКБ о регистрации в Банке новых открытых ключей ЭП Клиента для просмотра выписок. В письме указывается ФИО владельца ключа ЭП и идентификационный номер ключа ЭП.

6.30. Дать Банку указание на временное блокирование операций Клиента в СКБ, позвонив по телефону администратору СКБ в Банк и произнеся блокировочное слово. Восстановление работы Клиента в СКБ производится Банком после получения письменного уведомления Клиента о начале работы в СКБ не позднее следующего операционного дня.

6.31. Приостановить действие настоящего Договора по письменному заявлению на срок не более 6 (шести) месяцев. Приостановление действия Договора производится Банком не позднее следующего операционного дня в случае оплаты Клиентом причитающегося к уплате на дату предоставления заявления комиссионного вознаграждения Банка согласно тарифам.

6.32. Отозвать свой ЭД в порядке, предусмотренном настоящим Договором.

6.33. Предоставлять документы и информацию в Банк на бумажном носителе в случае невозможности использования СКБ.

7. СОВМЕСТНЫЕ ОБЯЗАТЕЛЬСТВА И ОТВЕТСТВЕННОСТЬ СТОРОН

7.1. Ответственность за достоверность информации и подлинность ЭП в ЭД несет Сторона, отправившая ЭД.

7.2. Операция и выписка по счету считаются подтвержденными Клиентом, если он не представит свои замечания в течение 10 календарных дней от даты проведения операции.

7.3. ЭД порождает обязательства Сторон по Договору, если он надлежащим образом оформлен передающей Стороной, заверен ЭП и передан по СКБ, а принимающей Стороной получен, проверен и расшифрован.

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

7.5. Банк и Клиент все уведомления осуществляют в установленный Сторонами срок, в письменной форме, за подписями уполномоченных лиц, с оттиском печати и обязательным требованием отметки о приеме. В случае необходимости принятия экстренных мер допускается также высылка копии уведомления по факсимильной связи с обязательным последующим предоставлением оригинала противоположной Стороне в течение установленного срока.

7.6. В случае поступления от противоположной Стороны официального письменного уведомления, полученного, в том числе, и по факсимильной связи, касающегося компрометации или прекращения действия ключей и/или средств ЭП, получившая такое уведомление Сторона обязана немедленно прекратить все операции, производимые с их применением, и не позднее следующего рабочего дня предоставить противоположной Стороне официальное письменное уведомление о прекращении действия соответствующих ключей ЭП.

7.7. До истечения установленного срока допустимого использования своих секретных ключей ЭП Сторона должна уведомлять об этом противоположную Сторону в произвольной форме, в том числе по телефонной или факсимильной связи.

7.8. В случае истечения установленного срока допустимого использования своих секретных ключей ЭП, Стороны обязуются немедленно прекращать все операции, производимые с их участием.

7.9. В случае предоставления противоположной Стороной письменных документов, относящихся к сфере действия настоящего Договора, и требующих обязательной отметки о приеме, вернуть противоположной Стороне ее экземпляры этих документов с соответствующей отметкой о дате приема в течение установленного срока с момента поступления документа.

7.10. Клиент полностью принимает на себя ответственность:

- За правильность и достоверность заполнения ЭД, переданного им и принятого Банком;
- За корректность передачи ЭД в случае компьютерного, механического или электрического сбоя, или обстоятельств, находящихся вне зоны ответственности Банка;
- За соблюдение режима конфиденциального доступа к АРМ Клиента и НКИ;
- За действия сотрудников Клиента, имеющих доступ к СКБ, электронным документам и ЭП;
- Любые риски наступления неблагоприятных последствий вследствие нарушения Клиентом условий Договора, в том числе обязанности, предусмотренной пунктом 6.11.

7.11. Банк принимает на себя ответственность:

- За правильность заполнения и оформления ЭД, заверенных подписью Банка;
- За своевременность исполнения ЭД в соответствии с действующим законодательством;

7.12. Банк не несет ответственности:

- за убытки, понесенные Клиентом вследствие ошибок, отказов и несвоевременных

действий лиц, в пользу которых осуществляется расчетная операция по поручению Клиента;

- за сбои в СКБ, если они происходят по вине или в силу неквалифицированной работы с пакетом программ сотрудников Клиента;
- за исполнение ЭД, заверенных ЭП Клиента, сформированной утерянным, украденным или скопированным у Клиента программными средствами и/или ключами, если клиент не уведомил Банк о их компроментации, до момента проведения операции;
- за возникновение нештатных ситуаций на АРМ Клиента при использовании последним нелегального программного обеспечения;
- за частичную или полную потерю работоспособности клиентской части СКБ по вине Клиента (из-за переустановки или замены Операционной системы, изменения конфигурации оборудования, настроек программно-аппаратных средств АРМ, установка другого программного обеспечения изменяющего настройки АРМ).

7.13. При прекращении настоящего Договора Стороны несут ответственность по всем электронным документам с ЭП Клиента, сформированным в СКБ, в соответствии с действующим законодательством РФ.

7.14. Стороны обязуются при разрешении экономических и иных споров, которые могут возникнуть в связи с использованием СКБ, предоставлять в письменном виде свои оценки, доказательства и выводы по запросу заинтересованной Стороны, участвующей в настоящем Договоре.

7.15. Стороны освобождаются от ответственности за неисполнение или ненадлежащее исполнение принятых 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 СКБ, круглосуточно. При невозможности передачи документов в Банк с использованием СКБ, документы могут поступить от Клиента на бумажном носителе.

8.2. Документы, поступившие до 17-45, Банк принимает к исполнению в день поступления; документы, поступившие позже указанного времени - на следующий рабочий день.

8.3. Клиент поручает Банку дальнейшее оформление платёжных ЭД, переданных в Банк по СКБ.

8.4. При получении ЭД Банк производит проверку корректности ЭП Клиента с помощью Открытого ключа ЭП Клиента, дополнительную аутентификации Клиента, проверку правильности заполнения реквизитов документа в соответствии с действующим законодательством, банковскими правилами, настоящим Договором, ЭД, не прошедшие контроль, Банком к исполнению не принимаются.

8.5. Формирование Клиентом в СКБ и прием Банком к исполнению платёжных поручений/пакета (группы) платёжных поручений, переданных Клиентом в Банк с использованием СКБ, осуществляется Банком при выполнении следующих процедур:

- удостоверение права распоряжения денежными средствами;
- контроль целостности распоряжений Клиента;
- контроль структуры и значений реквизитов;
- контроль достаточности денежных средств на счете Клиента, в том числе проверку на возможность возникновения дебетового сальдо на расчётном счёте Клиента.

В случае нарушения хотя бы одной процедуры проверки, проверяемый платёжный ЭД отвергается СКБ.

8.5.1 Удостоверение права распоряжения денежными средствами и контроль целостности распоряжений Клиента Банк осуществляет посредством проверки ЭП Клиента и Многофакторной аутентификации.

Процедура проверки ЭП включает:

- проверку соответствия и подлинности ЭП;
- определение ключа проверки ЭП, соответствующего ключу ЭП, с использованием которого подписан платёжный ЭД;
- проверку целостности и неизменности платёжный ЭД (в том числе, реквизитов платёжный ЭД), созданного Клиентом и поступившего для исполнения в Банк.

Процедура Многофакторной аутентификации включает проверку корректности/правильности/своевременности введенного пароля, полученного посредством короткого сообщения (SMS) или аппаратным устройством (MAC-токен).

8.5.2. При получении от Клиента платёжного ЭД системой «Клиент-Банк» автоматически осуществляется процедура контроля структуры и значений реквизитов, посредством проверки соответствия реквизитов платёжного ЭД, сформированных Клиентом в СКБ, требованиям законодательства.

8.5.3. При получении от Клиента платёжного ЭД, Банком осуществляется контроль достаточности денежных средств на счете Клиента с учетом ограничений на распоряжение денежными средствами на счете, установленных законодательством, и с учетом поступления денежных средств на счет Клиента в течение текущего операционного дня.

8.5.4. Платёжные ЭД Клиента исполняются Банком в порядке поступления в Банк (получения акцепта от Клиента) в пределах остатка денежных средств на счете Клиента.

8.5.5. При выявлении недостаточности денежных средств на счете Клиента, поступившие платёжные ЭД Клиента не принимаются Банком к исполнению (отвергаются) за исключением:

- платёжные ЭД, которые в соответствии с очередностью, установленной законодательством, помещаются в очередь не исполненных в срок для дальнейшего осуществления контроля достаточности денежных средств на счете Клиента-плательщика (распоряжения о переводе денежных средств в бюджеты бюджетной системы Российской Федерации и распоряжений этой же, либо предыдущей очередности списания денежных средств, установленной законодательством);
- а также платёжные ЭД, принимаемых Банком к исполнению в соответствии с Договором банковского счета, заключенным с Клиентом.

В случае нарушения хотя бы одной процедуры проверки, проверяемый платёжный ЭД отвергается СКБ.

8.5. Помещение Банком платёжных ЭД Клиента в очередь, не исполненных в срок, по причине недостаточности денежных средств на счете Клиента-плательщика, либо ожидающих разрешения на проведение операций, не является отрицательным результатом процедуры приема платёжного ЭД к исполнению.

8.6. Клиент вправе совершить отзыв ЭД до наступления момента безотзывности перевода, предоставив в Банк электронное заявление об отзыве ЭД по форме, предусмотренной в СКБ, с указанием причины отзыва документа. Заявление об отзыве служит основанием для возврата (аннулирования) Банком ЭД Клиента.

8.7. Клиент самостоятельно контролирует статусы состояния ЭД по их статусам в СКБ в соответствии с п. 3.7 настоящего Договора.

9. ПОРЯДОК ОПЛАТЫ

9.1. Оплата за подключение и обслуживание в СКБ производится в соответствии с действующими Тарифами за расчетно-кассовое обслуживание, установленными Банком.

9.2. Плата за подключение к СКБ списывается Банком со счета Клиента, открытого в Банке на условиях заранее данного акцепта или производится Клиентом самостоятельно посредством перечисления с любого другого счета или внесения в кассу Банка в день заключения настоящего Договора.

9.3. В период действия настоящего Договора Банк, на условиях заранее данного акцепта, списывает со счета Клиента абонентскую плату за пользование СКБ в размере и в сроки, установленные действующими в Банке на момент оплаты Тарифами.

9.4. В случае прекращения настоящего Договора, Банк в последний день действия Договора на условиях заранее данного акцепта списывает со счета Клиента абонентскую плату за последний месяц пользования Клиентом СКБ в полном объеме, независимо от того, сколько дней обслуживался Клиент в СКБ с начала оплачиваемого месяца при условии, что оплата за текущий месяц не взималась.

10. ПОРЯДОК ИЗМЕНЕНИЯ И РАСТОРЖЕНИЯ ДОГОВОРА, СРОК ДЕЙСТВИЯ ДОГОВОРА

10.1. Настоящий Договор считается заключенным и вступает в силу с даты проставления Банком отметки о принятии на Заявлении о присоединении и считается заключенным на неопределенный срок.

10.2. Внесение изменений и/или дополнений в настоящий Договор и/или Тарифы Банка, в том числе утверждение Банком новой редакции настоящего Договора, производится Банком в одностороннем порядке.

10.3. Банк уведомляет Клиента об изменениях и/или дополнениях, вносимых в настоящий Договор и/или Тарифы Банка, в том числе об утверждении Банком новой редакции настоящего Договора, за 5 (пять) календарных дней до даты введения изменений путем размещения их на

общедоступных ресурсах Банка (информационных стендах в операционных залах и/или официальном сайте Банка www.ankb.ru), а так же посредством отправки информационного уведомления в СКБ.

10.4. Каждая из Сторон вправе отказаться от Договора в одностороннем порядке, направив другой Стороне письменное уведомление в срок не позднее чем за 10 календарных дней до предполагаемой даты прекращения Договора.

10.5. Настоящий Договор прекращается вне зависимости от волеизъявления сторон в день закрытия Клиентом последнего из открытых в Банке расчетных счетов.

11. ПОРЯДОК РАЗРЕШЕНИЯ СПОРОВ

11.1. Все споры и разногласия, возникшие в результате исполнения условий настоящего Договора, разрешаются путем переговоров.

11.2. В случае возникновения спорных ситуаций между Клиентом и Банком при использовании СКБ Стороны обязуются участвовать в рассмотрении споров в соответствии с Порядком проведения технической экспертизы при возникновении спорных ситуаций (Приложение № 4 к настоящему Договору), выполнять требования указанного Положения и нести ответственность согласно выводам по рассмотрению спорной ситуации.

11.3. Споры и разногласия, которые не могут быть урегулированы путем взаимных переговоров Сторон, подлежат рассмотрению в Арбитражном суде по месту нахождения ответчика.

12. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

12.1. Стороны обязуются незамедлительно сообщать друг другу информацию, необходимую для исполнения обязательств по настоящему Договору, в том числе об изменении юридического статуса и реквизитов.

12.2. Невозможность выполнения каких-либо условий Договора в результате изменений законодательства, произошедших после его заключения, не влияет на обязательность исполнения Сторонами остальных условий Договора.

12.3. Настоящий Договор содержит следующие Приложения, являющиеся его неотъемлемой частью:

- Приложение № 1 – Заявление о присоединении к Договору на обслуживание Клиента в системе дистанционного банковского обслуживания «Клиент-Банк»;
- Приложение № 2 – Акт приема-передачи USB-токена/MAC-токена;
- Приложение № 3 – Заявка на изменение телефонных номеров, используемых Банком для передачи SMS-сообщений, содержащих одноразовые коды подтверждения электронных документов, переданных с использованием Системы «Клиент-Банк»;
- Приложение № 4 – Порядок проведения технической экспертизы при возникновении спорных ситуаций;
- Приложение № 5 – Памятка Клиенту о возможных угрозах хищения денежных средств с использованием системы «Клиент-Банк» и способах защиты;
- Приложение № 6 – Порядок действий Сторон в случае выявления хищения денежных средств в системе «Клиент-Банк»;
- Приложение № 7 – Памятка для работы с SMS-подтверждением.

13. АДРЕСА И РЕКВИЗИТЫ БАНКА

Полное наименование: Братский Акционерный Народный коммерческий Банк (Акционерное общество)

Сокращенное наименование: «Братский АНКБ» АО ИНН 3803202031 КПП 380401001

ОГРН 1023800000069, ОКПО 39092538

Место нахождения: 665717, г. Братск, ул. Комсомольская, д. 43

БИК 042520842, Корреспондентский счет 30101810850042520842 в Отделении г.Иркутска

Телефон: (3953) 41-63-64, Факс: (3953) 41-65-82, E-mail: post@ankb.ru

WWW:<http://ankb.ru>

Уважаемые Клиенты, обращаем Ваше внимание!

Консультирование по вопросам электронного документооборота в системе «Клиент-Банк» осуществляется по следующим телефонам:

+7(3953) 414-970 по вопросам технического подключения и использования системы «Клиент-Банк»;

+7(3953) 413-058 по вопросам заключения/изменения/расторжения настоящего Договора;

+7(3953) 413-058 по вопросам оформления электронных документов;

+7(3953) 413-107 по вопросам предоставления документов, связанных с проведением Клиентом валютных операций, подтверждающих (дополнительных) документов, предоставления консультаций по вопросам валютного контроля.

Консультирование осуществляется по телефонам Банка в рабочее время Банка, в соответствии с установленным режимом работы Банка (Подразделений Банка).

**Заявление
о присоединении к Договору на обслуживание Клиента в системе
дистанционного банковского обслуживания «Клиент-Банк»**

«___» _____ 20__ г.

Настоящим заявлением Клиент

Полное наименование Клиента:	
Сокращенное наименование Клиента:	
ИНН/КИО:	
ОГРН/ОГРНИП:	
Адрес места нахождения:	
Адрес фактического местонахождения:	
Контактная информация:	

1. Присоединяется полностью и безусловно к действующей в «Братском АНКБ» АО редакции Договора на обслуживание Клиента в системе дистанционного банковского обслуживания «Клиент-Банк» в порядке, предусмотренном ст. 428 Гражданского кодекса Российской Федерации, и обязуется соблюдать все положения (условия) Договора на обслуживание Клиента в системе дистанционного банковского обслуживания «Клиент-Банк» со дня принятия настоящего заявления «Братским АНКБ» АО (далее - Банк).

2. Подтверждает, что ознакомлен и согласен со всеми положениями (условиями) действующей в Банке редакции Договора на обслуживание Клиента в системе дистанционного банковского обслуживания «Клиент-Банк» (включая все Приложения и Тарифы Банка), их содержание и смысл понятны.

3. Информация об уполномоченных лицах Клиента:

	№ п/п	Фамилия, Имя, Отчество	Должность
С правом подписи и отправки документов*	1.		
	2.		
	3.		
Без права подписи и отправки документов**	1.		
	2.		

4. Средства и способы получения одноразовых паролей контроля входа в систему «Клиент-Банк» и подтверждения платежных поручений:

АКТ приема-передачи USB-токена/MAC-токена

«___» _____ 20____ г.

Братский Акционерный Народный коммерческий Банк» (Акционерное общество), именуемое в дальнейшем «Банк», в лице **Председателя Правления** _____, действующего на основании Устава, с одной стороны, и _____, именуемый(ое) в дальнейшем «Клиент», в лице _____, действующего на основании _____ с другой стороны, совместно именуемые «Стороны», подписали настоящий Акт приема-передачи USB-токена/MAC-токена (далее – Акт) о том, что:

1. Банк передал, а Клиент получил нижеследующее устройства:

- USB- токен, в количестве _____ шт.
 MAC-токен, в количестве _____ шт.

Серийный номер (Идентификатор) USB-токена:

№ п/п	Серийный номер (Идентификатор) USB-токена

2. Клиент подтверждает, что каждое полученное аппаратное устройство не имеет видимых признаков повреждения и взлома.

3. Клиент обязуется использовать средства электронной подписи в соответствии с Договором на обслуживание Клиента в системе дистанционного банковского обслуживания «Клиент-Банк».

4. В случае повторной выдачи USB-токена/MAC-токена по причине его утраты или порчи, Банком производится повторная процедура подключения Клиента к СКБ при этом с Клиента взымается оплата в соответствии с пунктом 4.2.3. Договора .

5. Настоящий Акт составлен в двух экземплярах по одному для каждой из Сторон.

БАНК

КЛИЕНТ

_____/_____/_____
М.П.

_____/_____/_____
М.П.

Приложение № 3
к Договору на обслуживание в Системе «Клиент-Банк»
№ _____ от «___» _____ г.

ЗАЯВКА

«___» _____ 20__ г.

на изменение средств (номеров средств) получения одноразовых паролей контроля входа в систему «Клиент-Банк» и подтверждения платежных поручений

(наименование, ИНН Клиента)

поручает Банку в рамках Договора на обслуживание Клиента в системе дистанционного банковского обслуживания «Клиент-Банк» № _____ от «___» _____ 20__ г. не позднее рабочего дня, следующего за днем предоставления в Банк настоящей Заявки, осуществлять передачу одноразовых паролей контроля входа в систему «Клиент-Банк» и подтверждения платежных поручений следующими средствами*:

□ № моб. телефона	□ № OTP-токена	□ № MAC-токена
1. _____	1. _____	1. _____
2. _____	2. _____	2. _____
3. _____	3. _____	3. _____
4. _____	4. _____	4. _____

_____/_____
(подпись, ФИО уполномоченного представителя клиента)
М.П.

* Клиент может указать в настоящей Заявке не более 4 (четырёх) номеров каждого вида средств получения одноразовых паролей.

**ПОРЯДОК
проведения технической экспертизы при возникновении спорных ситуаций**

1. В настоящем Порядке под спорной ситуацией понимается существование претензий у Клиента к Банку, справедливость которых может быть однозначно установлена по результату проверки ЭП Клиента под электронным документом.
 2. Клиент в соответствии с действующим Порядком Работы Банка с обращениями клиентов, размещённом на сайте Банка (<http://www.ankb.ru/>) направляет в Банк письменное обращение, содержащее существо претензии с указанием на электронный документ с ЭП, на основании которого Банк выполнил операции по счету Клиента.
 3. Банк обязан в течение не более пяти рабочих дней от даты подачи заявления Клиента сформировать разрешительную комиссию для рассмотрения заявления. В состав комиссии включаются представители Клиента и представители Банка, 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, на которую возлагается ответственность согласно выводу об истинности ЭП Клиента под спорным электронным документом.
 5. Разрешительная комиссия в течение не более пяти рабочих дней проводит рассмотрение заявления Клиента. Рассмотрение заявления включает следующие этапы:
 - 5.1. Разрешительная комиссия проводит техническую экспертизу с целью установления:
 - электронного документа, заверенного ЭП Клиента, на основании которого Банком выполнены оспариваемые Клиентом действия со счетом Клиента;
 - ключа проверки ЭП Клиента, периода действия и статуса ключа проверки ЭП Клиента, и его принадлежности Клиенту;
 - корректности ЭП Клиента в электронном документе.
 - Техническая экспертиза проводится с использованием специального программного обеспечения для рассмотрения спорных ситуаций, предоставленного компанией – разработчиком системы «Клиент-Банк» - АО «БИФИТ».
 - 5.2. По требованию одной из Сторон к проведению технической экспертизы может быть привлечена компания – разработчик системы «Клиент-Банк» - АО «БИФИТ».
 - 5.3. На основании данных технической экспертизы разрешительная комиссия составляет акт.
6. Банк несет ответственность перед Клиентом в случае, когда имела место хотя бы одна из следующих ситуаций:
7. Банк не предъявляет электронного документа, переданного Клиентом, на основании которого Банк выполнил операции по счету Клиента.
8. ЭП Клиента в электронном документе оказалась некорректной.
9. Клиент предоставляет уведомление об отмене действия ключа ЭП и соответствующего ему ключа проверки ЭП Клиента, подписанное должностным лицом Банка и имеющим оттиск печати Банка. При этом указанная в уведомлении дата окончания действия пары ключей ЭП Клиента раньше даты, указанной в рассматриваемом электронном документе.
10. В случае, когда Банк предъявляет электронный документ, корректность ЭП Клиента признана разрешительной комиссией, принадлежность Клиенту ключа проверки ЭП Клиента подтверждена, Банк перед Клиентом по выполненным операциям по счету Клиента ответственности не несёт.

**ПАМЯТКА КЛИЕНТУ
О ВОЗМОЖНЫХ УГРОЗАХ ХИЩЕНИЯ ДЕНЕЖНЫХ СРЕДСТВ С ИСПОЛЬЗОВАНИЕМ СИСТЕМЫ
«КЛИЕНТ-БАНК» И СПОСОБАХ ЗАЩИТЫ**

Хищение денежных средств с расчетных счетов возможно при получении злоумышленниками доступа к Секретным ключам ЭП и паролям. Для того, чтобы предотвратить хищение и использование Вашего Секретного ключа ЭП Банк настоятельно рекомендует придерживаться приведенных ниже правил:

Для хранения файлов с секретными ключами ЭП использовать внешние носители: дискеты, флеш-диски, специализированные устройства – USB-токены. При этом владелец такого внешнего носителя должен хранить его в условиях, исключающих доступ к нему третьих лиц, например, личный сейф.

Использовать IP-фильтрацию - дополнительный сервис, запрещающий пользование ключами ЭП на компьютерах вне вашего офиса. IP-фильтрация позволяет быть уверенным в том, что информация, передаваемая в банк, будет обработана только в случае совпадения IP-адреса передающего компьютера с IP-адресом клиента, хранящимся в базе данных банка;

Использовать SMS-Банкинг. Сервис позволяет оперативно получать информацию о входе в систему, о поступлении платежных поручений, о движении средств и т.д. При получении сообщения о несанкционированной операции Вы должны связаться с Банком для ее приостановки.

Не хранить на носителях с ключами ЭП какую-либо другую информацию.

Не допускать использования «пустых» или простых паролей, например 123456, «qwerty», для всех учетных записей, имеющих право входа в Windows. Осуществлять периодическую смену паролей, рекомендуемая частота смены паролей - 1 раз в месяц.

Не передавать ключи ЭП ИТ-сотрудникам для проверки работы СКБ и проверки настроек взаимодействия с Банком. При необходимости проведения проверок владелец ключа ЭП должен лично подключить носитель к компьютеру, убедиться, что пароль доступа к ключу вводится в интерфейс клиентского АРМа СКБ, и ввести пароль, исключая умышленное наблюдение посторонними лицами;

Не передавать ключи ЭП замещающим сотрудникам (заместителям, временно исполняющим обязанности). Для таких сотрудников необходимо получить персональные ЭП и внести их в банковскую карточку.

При увольнении ответственного или технического сотрудника, имевшего доступ к Секретному ключу ЭП, обязательно заблокировать его ключ ЭП.

При увольнении ИТ-специалиста, осуществлявшего обслуживание компьютеров, используемых для работы с СКБ, проверить их на отсутствие вредоносных программ.

В случае если работа в системе Интернет-банкинг продолжительна, отключать и извлекать носители с ключами ЭЦП, если они не используются для работы. Носители с ключами ЭП должны находиться в компьютере только в момент подписания документов, и извлекаться сразу после подписания документов.

Выделить отдельный компьютер, который будет использоваться только для работы с СКБ и не выполнять на этом компьютере никакие другие задачи.

Ограничить доступ к компьютерам, используемым для работы с СКБ и исключить к ним доступ персонала, не работающего с СКБ.

Исключить обслуживание компьютеров, используемых для работы с СКБ, нелицензионными ИТ-сотрудниками.

При обслуживании компьютера ИТ-сотрудниками, обеспечивать контроль над выполняемыми ими действиями.

На компьютерах, используемых для работы с СКБ, исключить посещение Интернет-сайтов сомнительного содержания, загрузку и установку нелицензионного программного обеспечения и т. п. По возможности, полностью запретить все соединения (входящие и исходящие) с сетью Интернет, разрешив только доступ к необходимым ресурсам.

Использовать только лицензионное программное обеспечение, обеспечив автоматическое обновление системного и прикладного программного обеспечения.

Применять на рабочем месте лицензионные средства антивирусной защиты, обеспечив возможность автоматического обновления антивирусных баз, а также еженедельную полную антивирусную проверку.

Применять на рабочем месте специализированные программные средства безопасности: персональные фаерволы, антишпионское программное обеспечение и т.п.

Осуществлять антивирусную проверку любых файлов и программ, загружаемых из сети Интернет, полученных по электронной почте или на внешних носителях (дискеты, флеш-накопители, CD/DVD и др.).

Проводить полную антивирусную проверку после любых действий внештатных ИТ-специалистов или других сотрудников, выполнявших операции на компьютере, используемом для работы с системой. например, решение технических проблем: подключения к сети Интернет, установки или обновления бухгалтерских и информационно-правовых программ.

Не допускать работу под учетной записью Windows, имеющей права администратора. Необходимо использовать учетную запись с ограниченными правами в операционной системе Windows, установленной на компьютере.

Запрещать использование любых средств удаленного (дистанционного) доступа, которые обычно используется ИТ-специалистами для удаленной поддержки. Заблокировать возможность использования таких средств с помощью фаервола (программного и/или аппаратного).

При возникновении подозрений на копирование Секретных ключей ЭП или наличие в компьютере вредоносных программ – обязательно заблокировать ключи ЭП.

Если Вы заметили проявление необычного поведения программного обеспечения СКБ или какие-то изменения в интерфейсе программы – позвонить в Банк и выяснить, не связаны ли такие изменения с обновлением версии программного обеспечения. Если нет – заблокировать ключи ЭП.

Хищение денежных средств с расчетных счетов при получении злоумышленниками доступа к Секретным ключам ЭП и паролям с целью направления в Банк платежных поручений, заверенных от Вашего лица похищенным ключом ЭП предположительно могут осуществить:

- ответственные сотрудники Вашей организации, ранее имевшие доступ к Секретным ключам ЭП;
- штатные ИТ-сотрудники Вашей организации, имеющие или имевшие технический доступ к носителям (дискеты, флеш-носители, жесткие диски и пр.) с Секретными ключами ЭП, а также доступ к компьютерам организации, с которых осуществлялась работа по СКБ;
- нештатные, приходящие по вызову, ИТ-специалисты, обслуживающие компьютеры Вашей организации, осуществляющие профилактику и подключение к Интернету, установку и обновление бухгалтерских и информационно-правовых программ (другого программного обеспечения) на компьютеры, с которых осуществлялась или осуществляется работа по СКБ;
- другие злоумышленники путем заражения через Интернет Ваших компьютеров вредоносными программами, через уязвимости системного и прикладного программного обеспечения с последующим дистанционным хищением Секретных ключей ЭП и паролей.

Таким образом, в Банк могут поступать не вызывающие подозрений платежи, направленные злоумышленниками с использованием действующих Секретных ключей ЭП, имеющие обычные реквизиты получателей и типовые назначения платежа.

Банк напоминает Вам о том, что:

- не имеет доступа к Вашим Секретным ключам ЭП и не может от Вашего имени сформировать корректную ЭП под ЭД;
- не осуществляет рассылку электронных писем с просьбой прислать Ваш Секретный ключ ЭП или пароль;
- Банк не рассылает по электронной почте программы для установки на Ваши компьютеры. В случае если Вы получили подобное письмо от имени Банка, содержащее программу для установки или запрос на предоставление ключей ЭП и/или паролей, необходимо незамедлительно сообщить об этом в Службу технической поддержки клиентов Банка;
- ответственность за конфиденциальность Ваших Секретных ключей ЭП лежит на Вас, как единственных владельцах Секретных ключей ЭП;
- если Вы сомневаетесь в конфиденциальности своих Секретных ключей ЭП или есть подозрение в их компрометации (копировании), Вы должны незамедлительно заблокировать Ваши ключи ЭП;
- изменение пароля доступа к Секретному ключу ЭП не защищает Вас от использования злоумышленниками ранее похищенного ключа;

Для получения дополнительной информации по техническим вопросам Вы можете обратиться в Отдел автоматизации и ДБО (3953) 41-49-70

ПОРЯДОК ДЕЙСТВИЙ КЛИЕНТА В СЛУЧАЕ ВЫЯВЛЕНИЯ ХИЩЕНИЯ ДЕНЕЖНЫХ СРЕДСТВ В СИСТЕМЕ «Клиент - Банк»

В случае выявления хищения денежных средств в СКБ Клиенту (пострадавшему) необходимо:

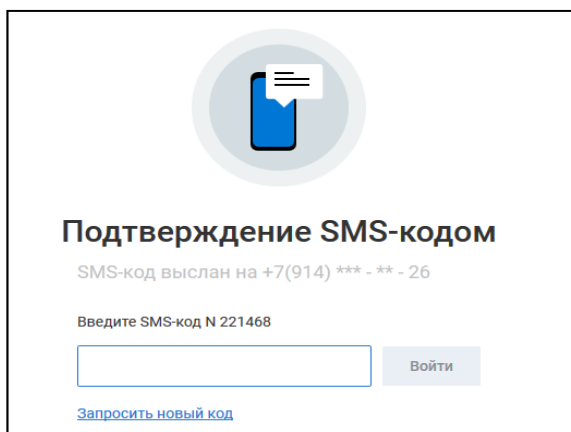
1. Немедленно прекратить любые действия с электронным устройством (далее - ЭУ), подключенным к СКБ, обесточить и отключить от информационных сетей (если было подключение, например, по Ethernet, USB, Wi-Fi, Dial-Up и др.) или перевести в режим гибернации ("спящий" режим).
2. При отсутствии возможности обесточивания ЭУ, осуществить отключение по штатной процедуре и запротоколировать указанный факт.
3. При наличии технической возможности отозвать перевод с использованием иного ЭУ, после чего принять меры к блокировке ключа ЭП, любым из способов, указанных в пункте 6.11 Договора.
4. При отсутствии технической возможности отозвать перевод по СКБ немедленно обратиться Банк с заявлением о блокировке ключа ЭП, приостановке исполнения платежа и возврате средств, любым из способов, указанных в пункте 6.11 Договора.
5. Произвести фотосъемку ЭУ, рабочего места и его расположения в помещении. Обеспечить сохранность (целостность) ЭУ как возможного средства совершения преступления, поместив его в место с ограниченным доступом, обеспечив при этом защиту от вскрытия (стикеры, наклейки, пластилин, мастичная печать, пломбы и т.п.) и по возможности зафиксировать средства контроля целостности фотографированием со всех ракурсов. Если позволяют размеры ЭУ, следует поместить его в непрозрачный пакет (мешок) и заклеить горловину. При необходимости ведения хозяйственной деятельности - задействовать другое ЭУ.
6. Дополнительно к п. 1, 2 обратиться в Банк с письменным заявлением об отзыве платежа, возврате средств и блокировании доступа к СКБ, а также о компрометации ключей и необходимости смены ключей ЭП. Копия заявления должна быть направлена в банк плательщика незамедлительно по факсу или по электронной почте (скан-копия). Оригинал заявления должен быть доставлен в Банк течение одного дня.
7. Проинформировать все банки, с которыми клиент имеет договорные отношения, предусматривающие использование ДБО, о факте хищения денежных средств и обратиться с просьбой о внеплановой замене ключевой информации.
8. При наличии необходимой информации обратиться в банк получателя или к оператору соответствующей платежной системы с письменным заявлением о приостановлении платежа и возврате денежных средств.
9. Предпринять меры для обеспечения сохранности и неизменности записей с внутренних и внешних камер систем видеонаблюдения, журналов систем контроля доступа, средств обеспечения и разграничения доступа в сеть Интернет (при наличии таковых) за максимальный период времени, как до, так и после даты совершения хищения денежных средств.
10. Провести сбор записей с межсетевых экранов и других средств защиты информации, серверов баз данных и иных компонент клиентского приложения системы ДБО, систем авторизации пользователей (AD, NDS и т.д.), коммуникационного оборудования (включая АТС), ЭУ, используемых для управления денежными средствами через СКБ Банка, устройств, которые могут использоваться для удаленного управления указанными ЭУ.
11. При возможности оперативно обратиться с письменным заявлением к своему Интернет-провайдеру или оператору связи для получения в электронной форме журналов соединений с Интернет с электронного устройства клиента или из его локальной вычислительной сети (далее - ЛВС) как минимум за три месяца, предшествовавшие факту хищения денежных средств.
12. Не предпринимать никаких действий для самостоятельного или с привлечением сторонних ИТ-специалистов поиска и удаления компьютерных вирусов, восстановления работоспособности ЭУ, не отправлять ЭУ в сервисные службы ИТ для восстановления работоспособности.

13. Зафиксировать в протокольной форме значимые действия и события, в том числе имена лиц, имеющих доступ к ЭУ, действия с ЭУ, подключенным к СКБ, предшествовавшие факту хищения денежных средств, подготовить объяснения клиента (работников клиента) об использовании ЭУ в целях, отличных от осуществления операций в СКБ, посещаемых сайтах, о странностях при работе ЭУ, перебоях или отказах ЭУ, обращениях в ИТ-службы, в Банк, о сторонних лицах, побывавших в месте расположения ЭУ и т.д.
14. Все действия, указанные в пунктах 1, 4, 8, 9, 12 настоящего Приложения, производить коллегиально, протоколировать и документировать, в т.ч. с использованием фотосъемки.
15. При невозможности осуществления коллегиальных действий (для индивидуальных предпринимателей или физических лиц, занимающихся частной практикой) отдельно зафиксировать данный факт.
16. Оперативно обратиться с заявлением в правоохранительные органы о возбуждении уголовного дела по факту хищения денежных средств (глава 21 УК РФ).
17. Оперативно обратиться в суд с исковым заявлением в отношении получателя денежных средств (указав все известные реквизиты получателя) о взыскании неосновательно полученного обогащения и процентов за пользование денежными средствами (глава 60 ГК РФ), а также с ходатайством о принятии судом мер по обеспечению иска в виде ареста денежных средств на счете получателя в сумме неосновательно полученного обогащения. К исковому заявлению необходимо приложить копию заявления о возбуждении уголовного дела либо копию талона, содержащего порядковый номер из книги учета сообщений о преступлениях (далее - КУСП) содержащую отметку правоохранительного органа о его приеме.
18. Копии вышеуказанных документов, направить в Банк с приложением Справки по факту инцидента информационной безопасности в СКБ.

ПАМЯТКА ДЛЯ РАБОТЫ С SMS-ПОДТВЕРЖДЕНИЕМ

Для предотвращения хищения средств с расчетного счета клиента используется механизма расширенной аутентификации с использованием одноразового пароля, полученного с помощью SMS.

Для входа в систему «Клиент-Банк» с помощью механизма расширенной аутентификации с применением SMS уведомлений после ввода пароля к ключу ЭП необходимо ввести код подтверждения в окно подтверждения.



Подтверждение SMS-кодом

SMS-код выслан на +7(914) *** - ** - 26

Введите SMS-код N 221468

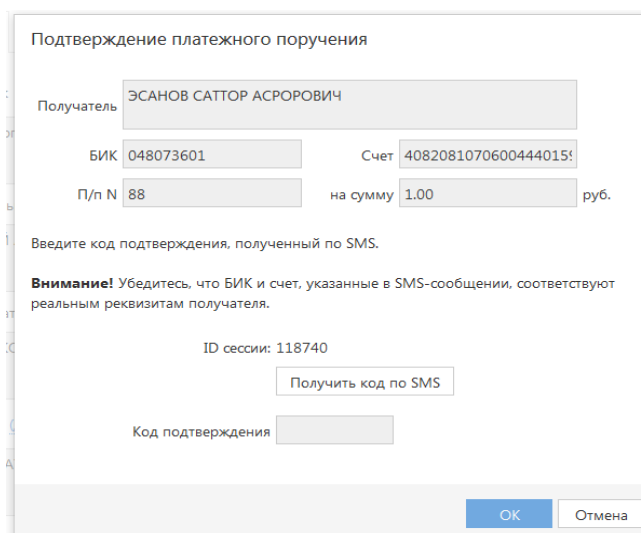
Войти

[Запросить новый код](#)

Рис. 1 Окно подтверждения.

В том случае, если одноразовый пароль был введен верно, будет произведен вход в систему.

Механизм подтверждения платежных поручений с помощью одноразового пароля является дополнительным подтверждением клиента под документом. После подписания платежного поручения ЭП и при превышении пороговой суммы (которая указана в пункте 4 Заявления о присоединении к Договору на обслуживание в СКБ) документ переходит в статус «Требуется подтверждение». Для доставки в Банк такого документа необходимо ввести одноразовый пароль (см. Рис.2)



Подтверждение платежного поручения

Получатель ЭСАНОВ САТТОР АСРОРОВИЧ

БИК 048073601 Счет 4082081070600444015!

П/п N 88 на сумму 1.00 руб.

Введите код подтверждения, полученный по SMS.

Внимание! Убедитесь, что БИК и счет, указанные в SMS-сообщении, соответствуют реальным реквизитам получателя.

ID сессии: 118740

Получить код по SMS

Код подтверждения

ОК Отмена

Рис. 2 Подтверждение платежного поручения одноразовым паролем

Для группового подтверждения необходимо выделить группу (пакет) документов и нажать кнопку: «Подтвердить»

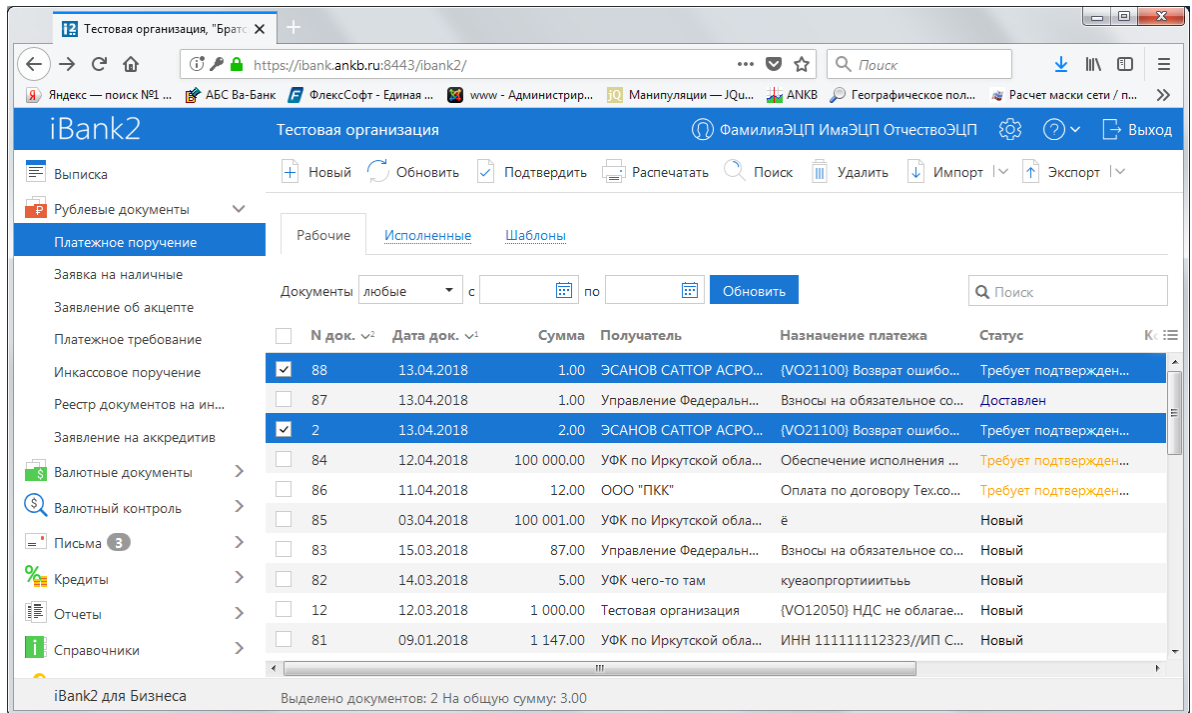


Рис. 3 Выделение группы документов

Подтверждение платежных поручений

Количество п/п Общая сумма руб.

Введите код подтверждения, полученный по SMS.

ID сессии: 138041

Код подтверждения

Рис. 4 Подтверждение группы документов