Утвержден
Протоколом Правления
ООО КБ «Столичный Кредит»
от «12» декабря 2022 г.

ДОГОВОР
обмена электронными документами с использованием системы электронного банкинга «iBank 2» (физическим лицам) № ___ - ИБК2

г. Москва "____"_____20 __ г.

Общество с ограниченной ответственностью Коммерческий Банк «Столичный Кредит», именуемый в дальнейшем «Банк», имеющий Лицензию Федеральной Службы Безопасности Российской Федерации ЛСЗ № 0009116 от 11 июля 2013г., в лице _____ , действующего на основании _____, с одной стороны, и гражданин_____ , именуемый в дальнейшем «Клиент», с другой стороны, совместно именуемые «Стороны», а по отдельности – «Сторона», заключили настоящий Договор о нижеследующем:

1. Термины, применяемые в Договоре

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

1.1. Система электронного банкинга «iBank 2» (Система «iBank 2») – совокупность программно-аппаратных средств, устанавливаемых на территории Клиента и Банка, и согласовано эксплуатируемых Клиентом и Банком в соответствующих частях, а также организационных мероприятий, проводимых Клиентом и Банком, с целью предоставления Клиенту услуг по настоящему Договору.

1.2. «Электронный документ» (ЭД) – совокупность байт, содержащая финансовый документ или информационное сообщение в Системе «iBank 2».

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

1.4. «Ключ электронной подписи» (Ключ ЭП) – уникальная последовательность символов, предназначенная для создания ЭП.

1.5. «Ключ проверки электронной подписи» (Ключ проверки ЭП) – уникальная последовательность символов, однозначно связанная с Ключом ЭП и предназначенная для проверки подлинности ЭП.

1.6. «Пара ключей электронной подписи» (Пара ключей ЭП) – Ключ ЭП и соответствующий ему Ключ проверки ЭП.

1.7. «Подлинная электронная подпись» – электронная подпись в ЭД, проверка которой с использованием соответствующего ключа проверки ЭП дает положительный результат.

1.8. «Активная пара ключей ЭП» – пара ключей ЭП, зарегистрированных Банком в системе «iBank 2», и используемых Клиентом для работы в Системе «iBank 2».

1.9. «Сертификат ключа проверки электронной подписи» (сертификат ключа проверки ЭП) - электронный документ или документ на бумажном носителе, выданные удостоверяющим центром либо доверенным лицом удостоверяющего центра и подтверждающие принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи.

1.10. «Удостоверяющий центр» - юридическое лицо или индивидуальный предприниматель, осуществляющие функции по созданию и выдаче сертификатов ключей проверки электронных подписей, а также иные функции, предусмотренные Федеральным законом от 06.04.2011г. № 63-ФЗ «Об электронной подписи».

1.11. «Группа подписи ключа» – полномочия ключа электронной подписи при подписи Электронного документа. По аналогии с собственноручной подписью, образец которой есть в банковской карточке, обычно различают первую и вторую подпись (группу подписи). Электронный документ может исполняться Банком только после того, как под ним собрано столько подписей, сколько указано в Приложении 2 к настоящему Договору (по одной подписи каждой группы).

1.12. «Аппаратное средство усиленной ЭП» – специализированное аппаратное средство, предназначенное для генерации пары ключей ЭП, хранения сгенерированных ключей ЭП, формирования ЭП под документами в соответствии с утвержденными стандартами (ГОСТ Р34.10-94, ГОСТ Р34.10-2001, ГОСТ Р34.11-94) с использованием встроенного в устройство сертифицированного СКЗИ.

1.13. «Программное средство усиленной ЭП» - программный модуль, входящий в состав Системы «iBank 2», предназначенный для генерации пары ключей ЭП, формирования ЭП под документами, обеспечивающий защиту информации в соответствии с утвержденными стандартами (ГОСТ 28147-89, ГОСТ Р34.10-94, ГОСТ Р34.10-2001, ГОСТ Р34.11-94) и сертифицированный в соответствии с действующим законодательством.

1.14. «Блокировочное слово» – уникальное слово, определяемое Клиентом при регистрации в Системе «iBank 2». Блокировочное слово может быть использовано Клиентом для блокирования своей работы в Системе «iBank 2» по телефонному звонку в Банк (например, в случае компрометации ключа).

1.15. «Компрометация ключа» – утрата, хищение, несанкционированное копирование, передача закрытого ключа в линию связи в открытом виде, любые другие виды разглашения содержания ключа, а также случаи, когда нельзя

достоверно установить, что произошло с носителями, содержащими ключевую информацию (в том числе случаи, когда носитель вышел из строя и доказательно не опровергнута возможность того, что данный факт произошел в результате действий злоумышленника).

1.16. «Средство подтверждения» - электронное или иное средство, используемое для подтверждения электронных документов. Средство подтверждения считается действительным на определенный момент времени, если одновременно выполнены следующие условия: на этот момент времени между Банком и Клиентом заключено соглашение об использовании средства подтверждения (Приложение 6), срок действия средства подтверждения не истек, средство подтверждения не было отменено Клиентом или Банком.

1.17. «Одноразовый пароль» — динамическая аутентификационная информация, генерируемая для единичного использования.

1.18. «Оператор связи» - телекоммуникационная компания, осуществляющая услуги связи, в том числе услуги по доставке sms - сообщений на мобильные телефоны (устройства), в том числе Клиента.

2. Предмет Договора

2.1. Банк оказывает Клиенту услуги электронного банкинга с использованием Системы «iBank 2», позволяющей передавать Электронные документы и принимать выписки и информационные сообщения.

2.2. Настоящий Договор имеет свою юридическую силу при наличии действующего Договора банковского счёта №_____ от «___» _____20__г. заключённому Сторонами.

3. Соглашения Сторон

3.1. Стороны признают, что применяемая в Системе «iBank 2» криптографическая защита информации, обеспечивающая шифрование, контроль целостности и создание ЭП с применением Программных или Аппаратных средств усиленной ЭП достаточна для защиты информации от несанкционированного доступа, подтверждения подлинности и авторства Электронного документа.

3.2. Стороны признают, что применяемая в Системе «iBank 2» технология генерации и хранения Ключа электронной подписи, формирования ЭП под документом с использованием Аппаратного средства усиленной ЭП полностью исключает возможность получения прямого доступа к Ключу электронной подписи с целью его копирования, переноса на внешний носитель или использования для формирования ЭП вне устройства.

3.3. Аппаратные средства ЭП являются собственностью Банка и предоставляются для использования Клиенту на (без)возмездной основе.

3.4. Стороны признают, что при произвольном изменении Электронного документа, заверенного Электронной подписью, ЭП становится не подлинной, то есть проверка подлинности ЭП дает отрицательный результат.

3.5. Стороны признают, что подделка ЭП Клиента, то есть создание Подлинной ЭП в Электронном документе от имени Клиента, практически невозможно без использования ключа электронной подписи Клиента.

3.6. Стороны признают, что Электронные документы с ЭП сотрудников Клиента, полученные Банком по Системе «iBank 2», являются доказательным материалом для решения спорных вопросов в соответствии с Приложением №1 настоящего Договора («Положение о порядке проведения технической экспертизы при возникновении спорных ситуаций»). Электронные документы, не имеющие необходимого количества ЭП, при наличии спорных вопросов не являются доказательным материалом.

3.7. Стороны признают, что ключ проверки электронной подписи сотрудника Клиента, содержащийся в Сертификате ключа проверки электронной подписи, заверенном подписью руководителя и оттиском печати Клиента, инадлежит соответствующему сотруднику Клиента.

3.8. Стороны признают в качестве единой шкалы времени при работе с Системой «iBank 2» Московское поясное время. Контрольным является время системных часов аппаратных средств Банка.

3.9. Стороны признают, что применяемые в Системе «iBank 2» механизмы дополнительного подтверждения документов с помощью одноразового пароля, являются надежными. Документы, требующие подтверждения одноразовым паролем, принимаются Банком к исполнению только в случае надлежащего подтверждения одноразовым паролем, полученным со Средства подтверждения Клиента или с зарегистрированного по форме Приложения 6 мобильного телефона сотрудника Клиента.

3.10. Стороны признают, что подделка одноразового пароля, то есть подтверждение Электронного документа от имени Клиента, практически невозможна без владения Средством подтверждения или зарегистрированным в системе мобильным телефоном.

3.11. Стороны признают, что Электронные документы, заверенные необходимым количеством ЭП, юридически эквивалентны соответствующим документам на бумажном носителе, оформленным в установленном порядке (имеющим необходимые подписи и оттиск печати), обладают юридической силой и подтверждают наличие правовых отношений между Сторонами. Электронные документы без необходимого количества ЭП сотрудников Клиента не имеют юридической силы, Банком не рассматриваются и не исполняются.

3.12. Стороны признают, что для уведомления Клиента о произведенных транзакциях в Системе «iBank 2» в соответствии с Федеральным законом от 27 июня 2011 года № 161-ФЗ от «О национальной платежной системе» и Положением Банка России от 19 июня 2012 года 383-П «Положение о правилах осуществления перевода денежных средств», Банку необходимо и достаточно отправить sms-сообщение на номер мобильного телефона, зарегистрированного в Системе по Заявлению Клиента (Приложение 6). В случае получения Банком подтверждения от Оператора связи об

успешной отправке СМС-сообщения, Клиент считается уведомленным о произведенной Клиентом транзакции в системе iBank2.

3.13. Стороны признают, что, подписывая настоящий Договор они принимают Положение о порядке проведения технической экспертизы при возникновении спорных ситуаций, изложенное в Приложении 1 к настоящему Договору.

3.14. Стороны признают, что ознакомлены с информацией, указанной в Приложениях 2 и 7 к настоящему Договору.

3.15. Стороны признают, что отмена действий пары ключей ЭП сотрудника Клиента и средства подтверждения осуществляются только после письменного уведомления Банка Клиентом в установленной Банком форме (Приложение 3 и 5 соответственно к настоящему Договору).

3.16. Стороны признают, что факт передачи необходимых для работы Клиента средств фиксируется подписями Сторон в Акте передачи по форме Приложения 4 к настоящему Договору в момент передачи носителя соответствующего программного средства.

3.17. Стороны признают, что регистрация или прекращение регистрации мобильного телефона в качестве средства получения одноразовых паролей осуществляется по письменному заявлению Клиента, оформленному в соответствии с Приложением 6 к настоящему Договору.

3.18. Стороны признают, что отказом от получения одноразовых паролей на вход в Систему «iBank2», а также отказом на получение одноразовых паролей на подтверждение платежа в виде sms-сообщений Клиент увеличивает риск несанкционированного доступа в систему третьих лиц, вредоносного обеспечения и прочих фактов, приводящих к явному и/или неявному несанкционированному доступу в Систему «iBank2». Отказ от получения одноразовых паролей на вход в Систему «iBank2», а также отказ от получения одноразовых паролей на подтверждение платежа в виде sms-сообщений оформляется путем подачи заявления, установленной банком формы (Приложение 8 к настоящему Договору).

3.19. Стороны признают, что в случае проведения операций над группой документов (групповая подпись документов) Клиент увеличивает риск несанкционированного доступа в систему третьих лиц, вредоносного обеспечения и прочих фактов, приводящих к явному и/или неявному несанкционированному доступу в Систему «iBank2». Согласие на проведение операций над группой документов (отказ от подписи единичного документа) оформляется путем подачи заявления, установленной Банком формы (Приложение 9 к настоящему Договору).

3.20. Приложения 3,5,6 и 8 подписываются в соответствии с условиями, установленными пунктами 3.13 - 3.18 настоящего Договора.

4. Права и обязанности Банка

4.1. Банк обязан принимать к исполнению Электронные документы, полученные по Системе «iBank 2» от Клиента, подписанные необходимым количеством ЭП сотрудников Клиента и соответствующие действующему законодательству РФ.

4.2. Банк обязан предоставлять Клиенту необходимые рекомендации (Приложение 7) для работы с Системой «iBank 2».

4.3. Банк обязан передать Клиенту программные модули Системы «iBank 2», Программные или Аппаратные средства усиленной ЭП и средства подтверждения до начала работы Клиента в Системе «iBank 2». Факт передачи указанных средств фиксируется в Актах передачи по форме Приложения 4.

4.4. Банк обязан предоставить Клиенту не менее одного Аппаратного средства усиленной ЭП, необходимые рекомендации и системное ПО для использования устройства.

4.5. Банк обязан по письменному требованию Клиента блокировать в Системе «iBank 2» существующую Пару ключей ЭП сотрудника Клиента и регистрировать новые Ключи проверки ЭП сотрудников Клиента.

4.6. Банк обязан по телефонному звонку Клиента временно блокировать работу Клиента в Системе «iBank 2», если Клиент подтверждает свои полномочия Блокировочным словом.

4.7. Банк имеет право по своему усмотрению без уведомления Клиента блокировать Активную пару ключей ЭП Клиента и потребовать от Клиента смены Пары ключей ЭП.

4.8. При наличии обоснованных подозрений о Компрометации Ключа электронной подписи сотрудников Клиента, Банк имеет право не производить исполнение полученных от Клиента Электронных документов и требовать от Клиента предоставления оформленных в установленном порядке платежных документов на бумажном носителе. Банк обязан незамедлительно, но не позднее 24 (двадцати четырех) часов, сообщить Клиенту о возникновении подобных подозрений и необходимости предоставить платежные документы на бумажном носителе.

4.9. Банк уведомляет Клиента о проведенных транзакциях в соответствии с Федеральным законом от 27 июня 2011 года № 161-ФЗ от «О национальной платежной системе» и Положением Банка России от 19 июня 2012 года 383-П «Положение о правилах осуществления перевода денежных средств».

4.10. Банк оставляет за собой право на одностороннее расторжение Договора в случае наличия у Клиента задолженности по абонентской плате за использование данной системы за период равный одному календарному месяцу. Последующее возобновление Договора производится на общих основаниях.

4.11. Банк оставляет за собой право на приостановление действия настоящего Договора в случае, если решением/постановлением Налогового органа, Суда, или Судебного пристава-исполнителя на денежные средства Клиента, находящиеся на расчетном счете, наложен арест. В случае наложения ареста на денежные средства Клиента, находящиеся на расчетном счете, абонентская плата по Договору не взимается. По факту отмены решения о приостановлении операций по расчетному счету Клиента, действие Договора возобновляется.

4.12. Банк оставляет за собой право отказать Клиенту в приеме от него распоряжений на проведение операций по банковскому счету, подписанных аналогом собственноручной подписи, в случае:

- выявления сомнительных операций (после предварительного уведомления Клиента), установленных действующим законодательством РФ, нормативными актами о противодействии легализации (отмыванию) доходов, полученных преступным путем, финансированию терроризма и финансированию распространения оружия массового уничтожения и перейти на прием от Клиента расчетных документов только на бумажном носителе.

4.13. Банк вправе по письменному заявлению Клиента, предоставленному в Банк, с учетом технических возможностей Банка, установить в отношении операций Клиента, осуществляемых с использованием Системы «iBank 2», ограничения на осуществление операций Клиентом, либо ограничения максимальной суммы одной операции и (или) операций за определенный период времени.

5. Права и обязанности Клиента

5.1. На основании имеющихся у Банка лицензий ФСБ Клиент имеет право осуществлять эксплуатацию предоставленных Банком сертифицированных ФСБ Программных и Аппаратных средств усиленной ЭП в Системе «iBank 2».

5.2. Перед началом эксплуатации Системы «iBank 2» Клиент обязан получить в Банке и самостоятельно установить на своем рабочем месте программные модули Системы «iBank 2», Программные и Аппаратные средства усиленной ЭП.

5.3. Клиент обязуется использовать предоставленные средства усиленной ЭП только в Системе «iBank 2» без права их продажи или передачи каким-либо способом иным физическим или юридическим лицам, обеспечивать возможность контроля со стороны уполномоченных органов за соблюдением требований и условий осуществления деятельности, связанной с использованием криптографических средств.

5.4. Клиент обязан обеспечивать сохранность и целостность программного комплекса Системы «iBank 2», включая предоставленные средства усиленной ЭП. При утрате или порче Аппаратных средств усиленной ЭП, Клиент обязан возместить их стоимость в соответствии с тарифами Банка.

5.5. Клиент обязан обеспечивать информационную безопасность рабочих мест ответственных сотрудников, уполномоченных использовать Систему «iBank 2» для взаимодействия с Банком. Клиент обязан исключить или максимально ограничить доступ к этим рабочим местам лиц, чья деятельность не связана с осуществлением электронного документооборота с банком.

5.6. Клиент обязан ознакомится с описанием механизмов защиты Ситемы «iBank 2» и памяткой клиенту об обеспечении информационной безопасности своего компьютера. Описание доступно на сайте банка по адресу https://ibank.capitalkredit.ru/faq.html#security_arrangements_IB. В случае если знаний Клиента недостаточно для адекватной оценки механизмов защиты системы и (или) обеспечения информационной безопасности своего компьютера, Клиент вправе обратиться к услугам сторонних специалистов. При этом оплата услуг специалистов производится Клиентом самостоятельно.

5.7. Клиент обязан сообщать Банку об обнаружении попытки несанкционированного доступа к Системе «iBank 2» незамедлительно после момента обнаружения, любым доступным Клиенту способом, в том числе по средствам телефонной связи, электронной почты, с обязательным указанием кодового слова.

5.8. Клиент обязан незамедлительно после момента обнаружения извещать Банк обо всех случаях Компрометации ключей электронной подписи, любым доступным Клиенту способом, в том числе по средствам телефонной связи, электронной почты, с обязательным указанием кодового слова.

5.9. Клиент обязан в случае прекращения использования Системы «iBank 2» уничтожить полученные в Банке Программные средства усиленной ЭП и вернуть Аппаратные средства усиленной ЭП, предоставленные Банком.

5.10. Клиент обязан заполнять Электронные документы в Системе «iBank 2» в соответствии с действующим законодательством, в частности «Положением о правилах осуществления перевода денежных средств» от 19 июня 2012 г. № 383-П.

5.11. Клиент обязан хранить в секрете пароль к ключу электронной подписи и не передавать третьим лицам носитель с ключом электронной подписи, используемым в Системе «iBank 2».

5.12. Клиент обязан обеспечивать использование ключей электронной подписи только их владельцами (ответственными сотрудниками) в соответствии с установленными правами подписи.

5.13. Клиент обязан по требованию Банка прекратить использование указанного Банком ключа электронной подписи, сгенерировать новую Пару ключей ЭП и зарегистрировать новый Ключ проверки электронной подписи в Банке.

5.14. Клиент имеет право досрочно прекратить действие своей Активной пары ключей ЭП и потребовать от Банка блокировать эту Пару ключей ЭП, оформив уведомление по форме Приложения 3.

5.15. Клиент имеет право по своему усмотрению генерировать новые Пары ключей ЭП и регистрировать в Банке новые Ключи проверки электронной подписи.

5.16. Клиент имеет право, позвонив в Банк по телефону +7 (495) 229-00-50 (1110, 1209) и сообщив ответственному сотруднику Банка Блокировочное слово, временно блокировать свою работу в Системе «iBank 2» до момента письменного уведомления об отмене действия Пары ключей ЭП или о возобновлении работы.

5.17. Клиент имеет право отказаться от получения одноразовых паролей на вход в Систему «iBank 2», а также отказаться от получения одноразовых паролей на подтверждение платежа в виде sms-сообщений, принимая во внимание увеличение операционных рисков и возлагая на себя ответственность за причиненный в связи с этим ущерб.

5.18. Клиент имеет право на групповую подпись документов принимая во внимание увеличение операционных рисков и возлагая на себя ответственность за причиненный в связи с этим ущерб.

5.19. Клиент имеет право, при работе в Системе «iBank 2», в целях недопущения осуществления переводов денежных средств без его согласия, в заявительном порядке (заявление клиента, оформленное в письменной виде),

распорядится об установлении Банком в отношении операций, осуществляемых Клиентом с использованием удаленного доступа через Систему «iBank 2», ограничений на осуществление операций. Ограничения по операциям, осуществляемым Клиентом с использованием удаленного доступа, могут быть установлены как на все операции Клиента, так и в разрезе видов операций, исходя из технической возможности Банка, администратором Системы «iBank 2» Банка, на основании письменного заявления Клиента (Приложение № 10).

Клиент вправе отозвать заявление об установлении Банком ограничений на осуществление операций, путем направления письменного заявления на отзыв в свободной форме, либо направлением нового заявления по форме предусмотренном абзацем первым данного пункта.

6. Совместные обязательства и ответственность Сторон

6.1. Банк не несёт ответственности за ущерб, причинённый Клиенту в результате использования третьими лицами Ключа электронной подписи Клиента.

6.2. При расторжении настоящего Договора Стороны несут ответственность по всем Электронным документам, сформированным в Системе «iBank 2», в соответствии с настоящим Договором и действующим законодательством РФ.

6.3. В случае возникновении конфликтных ситуаций между Клиентом и Банком при использовании 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. Действия Сторон согласно вышеуказанному Положению являются обязательной составляющей процедуры досудебного урегулирования споров.

6.4. Стороны обязуются при разрешении экономических и иных споров, которые могут возникнуть в связи с использованием Системы «iBank 2», предоставлять в письменном виде свои оценки, доказательства и выводы по запросу заинтересованной стороны, участвующей в настоящем Договоре.

6.5. Стороны освобождаются от ответственности за частичное или полное неисполнение своих обязательств по настоящему Договору в случае возникновения обстоятельств непреодолимой силы. Обстоятельства непреодолимой силы понимаются в соответствии с п. 3 ст. 401 ГК РФ. Сторона, ссылающаяся на обстоятельства непреодолимой силы, обязана незамедлительно, но не позднее 48 (сорока восьми) часов, информировать в письменной форме другую Сторону о наступлении и прекращении подобных обстоятельств и об их влиянии на возможность исполнить обязательство. Отсутствие уведомления возлагает на нарушившую Сторону обязанность возместить другой Стороне ущерб, который в случае своевременного уведомления мог быть предотвращен.

7. Порядок обслуживания Клиента

7.1. Банк осуществляет прием Электронных документов, передаваемых по Системе «iBank 2», круглосуточно. При невозможности передачи документов в Банк с использованием Системы «iBank 2» документы могут поступить от Клиента на бумажном носителе.

7.2. Банк не несет ответственности за задержку в формировании выписок по счетам Клиента, если она связана с неполучением Банком информации о проведенных операциях по его корреспондентским счетам от банков-корреспондентов и МЦИ при Банке России.

7.3. При получении Электронного документа Банк производит в автоматизированном режиме проверку подлинности ЭП сотрудников Клиента, проверку правильности заполнения реквизитов документа, проверку на возможность возникновения дебетового сальдо на расчётном счёте Клиента. В случае отбраковки Электронный документ Банком к исполнению не принимается.

7.4. В случае отмены платежа, изменения реквизитов, назначения платежа, суммы платежа Клиент обязуется известить об этом Банк, направив электронное письмо используя систему «iBank 2», а также подтвердить вышеуказанные изменения телефонным звонком, используя кодовое слово не позднее 20 (двадцати) минут с момента выставления платежа.

7.5. Банк не несет ответственности за работу непосредственно им не контролируемых каналов и оборудования связи, при помощи которых предоставляется доступ Клиента к СЭД.

7.6. Обслуживание Клиента по Системе «iBank 2» Банк осуществляет в соответствии с тарифами, установленными Банком и акцептованными Клиентом. Банк оставляет за собой право одностороннего изменения тарифов с обязательным уведомлением об этом Клиента не менее чем за 5 (пять) дней до вступления в действие новых тарифов. Если Клиента не согласен обслуживаться в соответствии с новыми тарифами, он обязан расторгнуть данный Договор в соответствии с п. 8.3 до наступления даты ввода в действие новых тарифов.

8. Срок действия Договора

8.1. Настоящий Договор вступает в силу с момента его заключения Сторонами и считается заключенным на неопределенный срок, но не более срока действия Договора(ов) банковского счета, заключенного(ых) между Сторонами. Прекращение Договора(ов) банковского счета, заключенного(ых) между Сторонами, влечет прекращение настоящего Договора.

8.2. Любая из Сторон вправе расторгнуть Договор в одностороннем порядке не ранее, чем через месяц после письменного уведомления об этом противоположной Стороны.

9. Заключительные положения

9.1. Споры по настоящему Договору решаются путем переговоров с учетом взаимных интересов в соответствии с Приложением 1. Все неурегулированные споры, возникающие между сторонами, рассматриваются в соответствии с действующим законодательством РФ в Арбитражном суде г. Москвы.

9.2. Изменение и дополнение условий настоящего Договора и Приложений к настоящему Договору производится Банком в одностороннем порядке, при этом соответствующее изменение/дополнение оформляется в виде новой редакции настоящего Договора, которая размещается на Официальном сайте Банка по адресу: www.capitalkredit.ru. Новая редакция настоящего Договора вступает в силу через 5 (Пять) рабочих дней с даты уведомления Клиента путем размещения новой редакции Договора на Официальном сайте Банка - www.capitalkredit.ru и/или на информационных стендах Банка в местах обслуживания клиентов.

9.3. Подписав настоящий Договор, Клиент выражает свое согласие на передачу и прием электронных документов в рамках электронного банкинга с использованием системы «iBank 2» на условиях, предложенных Банком.

9.4. Настоящий Договор составлен в 2-х экземплярах, имеющих одинаковую юридическую силу, по одному для каждой Стороны.

10. Юридические адреса и реквизиты Сторон

БАНК:

Наименование:	Общество с ограниченной ответственностью Коммерческий банк «Столичный Кредит»
Юридический адрес:	105005, г.Москва, ул. Бауманская, д. 54, стр. 1
Почтовый адрес:	105005, г.Москва, ул. Бауманская, д. 54, стр. 1
Банковские реквизиты:	к/с 30101810000000000683 в ГУ Банка России по ЦФО, БИК 044525683
ИНН:	7718103767
КПП:	775001001
ОГРН:	1027739199927

КЛИЕНТ:

Фамилия, имя, отчество:	_____
Дата и место рождения	_____
Адрес места регистрации:	_____
Адрес места пребывания:	_____
Документ, удостоверяющий личность гражданина (серия, номер, кем и когда выдан, код подразделения)	_____

От БАНКА:	От КЛИЕНТА:
_____ / _____ /	_____ /_____
М.П.	

Приложение № 1 к
Договору на оказания услуг электронного банкинга в системе «iBank 2»
№_____ от «___» _____20__г.

ПОЛОЖЕНИЕ
о порядке проведения технической экспертизы при возникновении спорных ситуаций

1. В настоящем Положении под спорной ситуацией понимается существование претензий у Клиента к Банку (вместе в дальнейшем именуются Сторонами), справедливость которых может быть однозначно установлена в результате проверки Электронных подписей сотрудников Клиента в Электронных документах.

2. При возникновении спорной ситуации Клиент представляет Банку в письменном виде заявление, содержащее существо претензии с указанием на оспариваемую операцию по счёту Клиента. В заявлении также должно быть указано лицо (лица), уполномоченное представлять интересы Клиента в разрешительной комиссии.

3. Банк обязан в течение 5 (Пяти) рабочих дней с момента получения заявления Клиента сформировать разрешительную комиссию для рассмотрения заявления. В состав комиссии включаются представители Клиента и представители Банка. По согласованию Сторон в состав комиссии могут быть включены независимые эксперты. Независимый эксперт должен иметь высшее профессиональное образование в области информационной безопасности или в области информационных технологий, а также стаж работы в области информационной безопасности не менее 5 лет.

4. Банк обязан письменно, не позднее, чем за три рабочих дня до начала работы разрешительной комиссии, уведомить Клиента о назначенной дате, времени и месте начала работы комиссии.

5. Стороны обязуются способствовать работе комиссии и не допускать отказа от предоставления необходимых документов.

6. В случае если Клиент не направит своих представителей для участия в работе разрешительной комиссии, рассмотрение спорной ситуации осуществляется без представителей Клиента. В этом случае в Акте делается запись об отсутствии представителя Клиента.

7. В результате рассмотрения спорной ситуации разрешительная комиссия должна определить подлинность ЭП сотрудника Клиента в приложенном Электронном документе и обоснованность выполнения Банком операций по счету Клиента.

8. Разрешительная комиссия проводит рассмотрение заявления в срок не более пяти рабочих дней с момента формирования комиссии. Рассмотрение заявления включает следующие этапы:

8.1. Разрешительная комиссия проводит техническую экспертизу ключа (ключей) электронной подписи сотрудника(ов) Клиента.

8.1.1. С использованием штатного программного обеспечения Системы «iBank 2» АРМ «Интернет-банкинг для корпоративных клиентов» выполняется распечатка Сертификата ключа проверки ЭП сотрудника Клиента, соответствующего Ключу электронной подписи сотрудника клиента, которым был подписан спорный Электронный документ. По согласованию Сторон печатная форма Сертификата может быть получена с использованием штатного программного обеспечения Системы «iBank 2» АРМ «Администратор».

8.1.2. Распечатанный сертификат сверяется с Сертификата ключа проверки ЭП сотрудника Клиента, заверенным подписью уполномоченного лица Клиента и являющимся приложением к договору - сверяются шестнадцатеричные представления Ключей проверки ЭП. При обнаружении расхождений ситуация далее не рассматривается, комиссия составляет акт о выявленном несоответствии.

8.2. Разрешительная комиссия проводит техническую экспертизу подлинности ЭП Клиента в Электронном документе.

8.2.1. С использование штатного ПО Системы «iBank 2» АРМ «Операционист» выбирается спорный Электронный документ и выполняется операция «Проверить ЭП».

8.2.2. При невозможности получить доступ к документу через АРМ «Операционист», комиссией могут использоваться специализированные утилиты от разработчика Системы «iBank 2» для выгрузки документа из Базы данных Системы «iBank 2» и автономной проверки.

8.3. По взаимному согласию членов комиссии, автономную проверку подлинности ЭП может провести независимая организация, в том числе разработчик системы «iBank 2» - ОАО «БИФИТ». Эксперт, проводящий автономную проверку подлинности ЭП, должен иметь высшее профессиональное образование в области информационной безопасности или в области информационных технологий, а также стаж работы в области информационной безопасности не менее 5 лет.

В этом случае Банком не позднее пяти рабочих дней с момента принятия согласованного решения о проведении независимой экспертизы в независимую организацию направляются материалы для проведения проверки:

- файлы, полученные в результате выгрузки спорного документа из базы данных системы «iBank 2»;

- копии Сертификатов ключа проверки ЭП сотрудников Клиента, заверенные обеими Сторонами;

- подписанное обеими Сторонами письмо с просьбой о проведении проверки.

По результатам проверки независимая организация формирует заключение о подлинности ЭП в предоставленном документе и высылает его в адрес Банка.

Срок проведения независимой экспертизы не должен превышать одного календарного месяца с момента принятия согласованного решения о проведении независимой экспертизы.

В случае проведения независимой экспертизы подлинности ЭП в спорном электронном документе на возмездной основе, расходы по проведению экспертизы подлинности ЭП оплачивает Банк.

Если в результате проведения независимой экспертизы на возмездной основе будет подтверждена подлинность ЭП в спорном электронном документе, Клиент обязан возместить Банку стоимость проведения экспертизы подлинности ЭП на основании письменного требования Банка и выставленного счета.

8.4. На основании данных технической экспертизы разрешительная комиссия составляет акт, содержащий

– фактические обстоятельства, послужившие основанием возникновения разногласий;

– все реквизиты оспариваемого документа;

– порядок работы членов комиссии;

– вывод о подлинности ЭП в оспариваемом Электронном документе и его обоснование.

В случае если проводилась независимая проверка подлинности ЭП, к Акту прилагается подготовленное независимой организацией заключение о подлинности ЭП

Акт составляется непосредственно после завершения оценки всех обстоятельств, подлежащих установлению разрешительной комиссией, в двух экземплярах по экземпляру для каждой Стороны и подписывается всеми членами комиссии.

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

9.1. Банк не предъявляет Электронный документ, подписанный Клиентом, на основании которого Банк выполнил операции по счёту Клиента.

9.2. Банк не предъявляет Сертификаты ключа проверки ЭП сотрудников Клиента, заверенные подписью руководителя и имеющие оттиск печати Клиента, соответствующие Ключам электронной подписи сотрудников Клиента, которыми был подписан спорный Электронный документ.

9.3. Хотя бы одна ЭП Клиента в Электронном документе оказалась не подлинной.

9.4. Клиент предоставляет Уведомление об отмене действия Пары ключей ЭП сотрудника Клиента, подписанное уполномоченным должностным лицом Банка и имеющее оттиск печати Банка. При этом указанная в Уведомлении дата окончания действия Пары ключей ЭП сотрудника Клиента раньше даты подписи, указанной в рассматриваемом Электронном документе.

10. В случае, когда Банк предъявляет Электронный документ и Сертификаты ключей проверки ЭП сотрудника Клиента, подлинность ЭП Клиента в Электронном документе признана разрешительной комиссией, принадлежность Клиенту Сертификатов ключей проверки ЭП сотрудников Клиента подтверждена, Банк не несёт ответственности перед Клиентом по выполненным операциям по счёту Клиента.

11. Если Клиент настаивает на том, что данный документ он не создавал или не подписывал одной или несколькими ЭП, комиссия может вынести определение о Компрометации Ключа (ключей) электронной подписи Клиента, что не снимает с Клиента ответственности за данный документ.

Приложение № 2 к
Договору на оказания услуг электронного банкинга в системе «iBank 2»
№_____ от «___» _____20__г.

ПЕРЕЧЕНЬ

Электронных документов, передаваемых по Системе «iBank 2» и необходимое количество ЭП.

	Наименование Электронного документа	Количество ЭП
1	Платежное поручение	1 или 2
2	Заявление на перевод иностранной валюты	1 или 2
3	Поручения на продажу иностранной валюты	1 или 2
4	Поручения на покупку иностранной валюты	1 или 2
5	Поручения на конвертацию иностранной валюты	1 или 2
6	Отзыв	1 или 2
7	Письмо	1 или 2

Приложение № 3 к
Договору оказания услуг электронного банкинга в системе «iBank 2»
№_____ от «___» _____ 20_г.

УВЕДОМЛЕНИЕ
об отмене действия Пары ключей ЭП сотрудника Клиента

_____
(наименование клиента банка)

уведомляет Банк о том, что с «____» _____20__г. считать недействительным Ключ проверки электронной подписи со следующим идентификатором _____.

Соответствующий ему Ключ электронной подписи утрачивает силу для дальнейшего применения с вышеуказанной даты.

Клиент _____

Приложение № 4 к
Договору на оказания услуг электронного банкинга в системе «iBank 2»
№_____ от «___» _____20__г.

Экз. №____

АКТ № ____
передачи программных средств, средств усиленной ЭП, средств подтверждения и сопроводительной документации

Общество с ограниченной ответственностью Коммерческий банк «Столичный Кредит», именуемое в дальнейшем «Банк», в лице _____ с одной стороны, и гражданин(ка)_____, именуемый в дальнейшем «Клиент» с другой стороны, вместе в дальнейшем именуемые «Стороны», принимая во внимание Договор оказания услуг электронного банкинга в системе «iBank 2», составили настоящий акт о том, что Банком надлежаще передан, а Клиентом получен носитель Рег. № _____ со следующими программными средствами:

- дистрибутив программы для ЭВМ «РС-Банкинг»;
- программное средство усиленной ЭП СКЗИ «Крипто-КОМ 3.2» № _____;
- программное средство усиленной ЭП ПБЗИ «Крипто-Си» № _____;
- драйвер для Аппаратного средства усиленной ЭП «iBank 2»;
- документация к СКЗИ (ПБЗИ);
- средство подтверждения OTP-токен «Active Identity Mini Token» № _____;
- средство подтверждения OTP-токен «VASCO DIGIPASS GO3» № _____;
- Скрэтч-карта одноразовых паролей № _____;
- документация по использованию средств подтверждения.

Банком надлежаще переданы, а Клиентом получены со следующие аппаратные средства усиленной ЭП:

- USB-токен «iBank 2» № _____;
- Смарт-карта «iBank 2» № _____;

С момента подписания Сторонами настоящего акта Банк считается исполнившим свои обязательства по передаче необходимых для работы Клиента средств в полном объеме.

Настоящий акт составлен в двух экземплярах, имеющих равную юридическую силу, по одному экземпляру для каждой из Сторон.

БАНК	**КЛИЕНТ**
_____	_____
(Ф.И.О., подпись)	(Ф.И.О., подпись)
М. П.	

Приложение № 5 к
Договору оказания услуг электронного банкинга в системе «iBank 2»
№_____ от «___» _____ 20__г.

УВЕДОМЛЕНИЕ
об отмене действия Средства подтверждения

_____
(наименование клиента банка)

уведомляет Банк о том, что с «____» _____20__г. считать недействительным Средство подтверждения _____ Клиента, со следующим идентификатором _____, полученное от Банка на основании Акта № ___ приема-передачи от __. __.____.

Клиент_____

Приложение № 6 к
Договору оказания услуг электронного банкинга в системе «iBank 2»
№_____ от «___» _____ 20__г.

ЗАЯВЛЕНИЕ

о регистрации (прекращении регистрации) мобильного телефона в качестве средства получения одноразовых паролей

_____

(наименование клиента банка)

просит Банк, с «____» _____20__г. зарегистрировать (прекратить регистрацию) в системе «iBank 2» номер(а) мобильного телефона_____ в качестве средства получения одноразовых паролей.

Настоящим сотрудник _____ подтверждает принадлежность ему указанного номера
(наименование клиента банка)

мобильного телефона и согласие на получение в любое время суток одноразовых паролей на мобильный телефон с вышеуказанным номером.

Клиент _____

Приложение № 7 к
Договору оказания услуг электронного банкинга в системе «iBank 2»
№_____ от «___» _____ 20__г.

Рекомендации для работы с Системой «iBank 2».

Вопросы безопасности

Механизмы защиты информации в системе «iBank 2».

«iBank 2» относится к классу систем защищенного электронного документооборота.

Для обеспечения аутентичности (доказательства авторства) и целостности документа используется механизм ЭП под электронными документами.

Для обеспечения конфиденциальности используется механизм шифрования данных. При взаимодействии через Интернет осуществляется шифрование и контроль целостности передаваемой информации, проводится криптографическая аутентификация сторон.

В системе реализованы российские криптографические алгоритмы в соответствии с ГОСТ 28147-89 (шифрование, имитовставка), ГОСТ Р34.11-94 (хеш-функция) и ГОСТ Р34.10-2001 (ЭП на эллиптических кривых).

Для использования функций криптографической защиты в системе «iBank 2» встроена поддержка следующих многоплатформенных криптобиблиотек, сертифицированных ФСБ:

- ПБЗИ «Крипто-Си Версия 2.0» компании «КриптоЭкс» (сертификат соответствия ФСБ РФ рег. № СФ/114-1614 от 28 февраля 2011 года);
- СКЗИ «Крипто-КОМ 3.2» компании «Сигнал-КОМ» (сертификаты соответствия ФСБ РФ рег. № СФ/124-1337 от 5 июня 2009 года, № СФ/114-1170 от 15 июля 2008 года, № СФ/114-1551, № СФ/114-1552, № СФ/124-1553, № СФ/124-1554 от 7 ноября 2010 года).

В системе «iBank 2» ведутся контрольные архивы, в которых хранятся все электронные документы с ЭП для разрешения конфликтных ситуаций. В системе ведется история документов - кем и когда документ был создан, отредактирован, подписан, исполнен или отвернут.

Дополнительные механизмы безопасности корпоративных клиентов.

- SMS-информирование клиентов о входе в систему, о поступлении в банк платежных документов, о движении средств по счетам клиентов.
- Расширенная многофакторная аутентификация при входе в систему с использованием одноразовых паролей.
- Механизм дополнительного подтверждения платежных поручений одноразовыми паролями (дополнительно к ЭП).

В качестве источников одноразовых паролей в системе «iBank 2» используются SMS-сообщения и OTP-токены.

Какие меры безопасности необходимо соблюдать при работе в Internet-Банкинге?

Меры безопасности при работе с ЭП:

- Для защиты ключей ЭП от хищения вредоносными программами рекомендуется использовать USB-токен или смарт-карту «iBank 2 Key»;
- В случае отсутствия «iBank 2 Key» файл-хранилище ключей сохраните на отчуждаемом носителе (USB-накопитель). Не допускается сохранять его в местах, где к нему может получить доступ кто-либо, кроме Вас. Отчуждаемый носитель с хранилищем ключей необходимо тщательно оберегать от несанкционированного доступа;
- Пароль на доступ к ключу ЭП должен быть известен только Вам как владельцу;
- Не допускайте постоянного и бесконтрольного подключения к компьютеру USB-токена и смарт-карты «iBank 2 Key»;
- Не передавайте «iBank 2 Key» с ключами ЭП никому;
- Не пользуйтесь Internet-Банкингом в Интернет-кафе, а также там, где Вы не уверены в безопасности компьютеров;
- При увольнении ответственного сотрудника, имевшего доступ к ключу ЭП, обязательно сообщите в Банк и заблокируйте ключ;
- При возникновении любых подозрений на компрометацию ключей ЭП или компрометацию среды исполнения (наличие в компьютере вредоносных программ) – обязательно сообщить в Банк и заблокировать ключи ЭП.

Меры по защите компьютера, с которого осуществляется работа в Internet-Банкинге:

- Соблюдайте регламент ограниченного физического доступа к данному компьютеру. Должен быть утвержден список сотрудников организации, включая ответственных сотрудников и технический персонал, которым разрешен доступ к компьютерам, с которых осуществляется работа в Internet-Банкинге.
- Рекомендуется использовать отдельный компьютер исключительно для работы в Internet-Банкинге. Другие действия (работа с другими программами, работа с электронной почтой, посещение сайтов в Интернете) с этого компьютера осуществляться не должны.
- Используйте в работе только лицензионное ПО. Не загружайте и не устанавливайте ПО полученное из непроверенных источников.

- Старайтесь использовать современные операционные системы (ОС). Данные системы являются более защищенными, в отличие от предыдущих, зачастую устаревших версий. Своевременно устанавливайте исправления и обновления для ОС. Включите автоматическое обновление ОС, которое будет устанавливать последние исправления, тем самым ликвидируя уязвимости ОС.
- Используйте системное и прикладное ПО только из доверенных источников, гарантирующих отсутствие вредоносных программ. При этом необходимо обеспечить целостность получаемых на носителях или загружаемых из Интернета обновлений.
- Используйте и оперативно обновляйте специализированное ПО для защиты информации — антивирусное ПО, персональные межсетевые экраны, средства защиты от несанкционированного доступа и пр.
- Не подключайте к компьютеру непроверенные на наличие вирусов отчуждаемые носители.
- Регулярно проверяйте Ваш компьютер на вирусы, как минимум раз в неделю.

Правила безопасной работы в Интернете:

- Не нажимайте на всплывающие окна, которые содержат рекламу. Желательно настроить Ваш браузер на автоматическую блокировку таких окон.
- Не посещайте непроверенные и небезопасные сайты. Вы можете непреднамеренно загрузить на свой компьютер вирусы и шпионские программы.
- Не читайте подозрительных электронных писем от незнакомых людей, они могут содержать вирусы. Читайте темы сообщений внимательно, если не уверены, что письмо пришло из надежного источника, не открывайте его. Не доверяйте дружественному тону сообщений или срочности содержащейся в них просьбы. В подозрительных письмах не нажимайте на содержащиеся в письме ссылки, а также не открывайте вложенные файлы, особенно если в письме указано, что проблема безотлагательная, и при этом просят срочно открыть приложенный файл, который имеет файловое расширение "exe".
- Максимально ограничьте использование Интернет-пейджеров (ICQ и пр.).
- Будьте внимательнее к странным или непонятным сообщениям об ошибках браузера. В случае возникновения подозрений просканируйте свой компьютер на наличие вирусов или шпионского ПО.

Документация

Следующие руководства пользователей Вы можете получить через службу опровождения компании ООО КБ «Столичный Кредит»:

- Руководство по работе с USB-токенами и смарт-картами «iBank 2 Key» - *iBank_2_Key_Guide.pdf*
- Руководство пользователя Internet-Банкинг для юридических лиц - *Corporate_Internet-Banking_Guide.pdf*
- Руководство пользователя PC-Банкинг для юридических лиц – *Corporate_PC-Banking_Guide.pdf*
- Руководство пользователя Internet-Банкинг для физических лиц - *iBank2_Private_Internet_Banking.pdf*
- Интеграция с программой «1С:Предприятие 7.7 и 8.1» - *Corporate_iBank2-Format_Guide.pdf*

Приложение № 8 к
Договору оказания услуг электронного банкинга в системе «iBank 2»

№_____ от «___»_____ 20_ г.

Заявление

_____,
(наименование клиента Банка)

в лице

_____
(Ф.И.О.)

отказывается от получения одноразовых паролей на вход в систему «iBank 2», одноразовых паролей на подтверждение платежа в виде SMS-сообщений, и в этой связи

_____
(наименование клиента Банка)

соглашается с увеличением степени риска несанкционированного доступа в систему третьих лиц, а также внедрения вредоносного программного обеспечения и прочих фактов, приводящих к явному и/или неявному несанкционированному доступу к системе управления счетами «iBank2».

В связи с этим _____
(наименование клиента Банка)

принимает ответственность за причиненный ущерб на себя.

Клиент_____

Приложение № 9 к
Договору оказания услуг электронного банкинга в системе «iBank 2»

№_____ от «___»_____ 20__г.

Заявление

От _____,
(наименование клиента Банка)
в лице_____
(должность, Ф.И.О.)

прошу предоставить возможность одновременного подписания нескольких документов (одно уведомление на подпись одного пакета документов) в системе «iBank2», и в этой связи

_____
(наименование клиента Банка)
соглашаюсь с увеличением риска несанкционированного доступа в систему третьих лиц, вредоносного программного обеспечения и прочих фактов, приводящих к явному и/или не явному несанкционированному доступу в системе iBank2».

В случае несоблюдения _____
(наименование клиента Банка)
требований по обеспечению безопасности ключевой информации указанных в п. 6.1 Договора СЭД, Банк не несет ответственности за ущерб, причиненный _____,
(наименование клиента Банка)
а также за возникновение чрезвычайных ситуаций и несанкционированного доступа третьих лиц к системе управления счетами _____ в системе «iBank2».
(наименование клиента Банка)

Руководитель _____ _____ _____
(наименование клиента банка) (ФИО руководителя) (подпись)

От имени Клиента

Приложение № 10 к
Договору оказания услуг электронного банкинга в системе «iBank 2»

№_____ от «___»_____ 20__г.

ЗАЯВЛЕНИЕ НА УСТАНОВЛЕНИЕ ОГРАНИЧЕНИЙ ПО ПАРАМЕТРАМ ОПЕРАЦИЙ С ИСПОЛЬЗОВАНИЕМ СИСТЕМЫ ДИСТАНЦИОННОГО БАНКОВСКОГО ОБСЛУЖИВАНИЯ

_____
(ФИО Клиента)

_____
(паспортные данные)

_____
(адрес места нахождения Клиента)

ИНН _____

в целях осуществления электронного документооборота с Банком прошу установить ограничения по параметрам операций по счету:
№ _____

№ п/п	ТИП ОГРАНИЧЕНИЙ ПО ПАРАМЕТРАМ ОПЕРАЦИЙ	СУММА ОГРАНИЧЕНИЙ (в валюте счета)	ПЕРИОД ВРЕМЕНИ
1.	На **общую сумму переводов (платежей)**, совершенных с использованием системы дистанционного банковского обслуживания iBank2 **за сутки в общей сумме:** **в т.ч.:** ☐ **внутренний перевод на свой счет** ☐ **перевод клиенту Банка** ☐ **перевод на карту (любую)** ☐ **валютный перевод**	_____ _____ _____ _____ _____ _____	**За 1 сутки (с 0:00 до 23:59)**
2.	На **общую сумму переводов (платежей)**, совершенных с использованием системы дистанционного банковского обслуживания iBank2 **за месяц в т.ч.:** ☐ **внутренний перевод на свой счет** ☐ **перевод клиенту Банка** ☐ **перевод на карту (любую)** ☐ **валютный перевод**	_____ _____ _____ _____ _____	**За 1 месяц (с 1-го по последнее число месяца)**

_____ _____
(ФИО Клиента) (подпись)

Дата: _____

В случае получения Банком настоящего Заявления от Клиента до 15:00 текущего операционного дня ограничения по счету устанавливаются Банком не позднее 9:00 следующего операционного дня. В случае получения Банком настоящего Заявления от Клиента после 15:00 текущего операционного дня, ограничения по счету устанавливаются Банком не позднее 12:00 следующего операционного дня.

Настоящее Заявление действует до момента его отзыва Клиентом.

Заполняется сотрудником Банка

Заявление на установление ограничений по параметрам операций с использованием системы дистанционного банковского обслуживания получено Банком, предоставленные Клиентом сведения проверил:

_____ _____ _____
(наименование должности сотрудника) (подпись) (ФИО)