У С Л О В И Я
дистанционного обслуживания КЛИЕНТОВ
с использованием Системы «iBank 2»

Международный коммерческий инвестиционный БАНК "РОССИТА-БАНК" Общество с ограниченной ответственностью (МКИБ «РОССИТА-БАНК» ООО или БАНК), оказывает КЛИЕНТАМ, юридическим лицам, индивидуальным предпринимателям, физическим лицам, занимающимся в установленном законодательством Российской Федерации порядке частной практикой, обслуживающимся по Договору расчетно-кассового обслуживания в МКИБ «РОССИТА-БАНК» ООО на публичных условиях (далее – Договор РКО), в соответствии с Тарифами БАНКА, услугу по дистанционному распоряжению денежными средствами на счете(-тах) КЛИЕНТА с использованием электронного средства платежа (ЭСП), а также обмену электронными документами (ЭД), (далее – Услуга) по системе «iBank 2», далее – по тексту «Система» или «iBank 2».

Услуга распространяется на все счета КЛИЕНТА, подключенные к Системе «iBank 2».

Использование КЛИЕНТОМ клиентской части Системы «iBank 2» допускается путем ее установки на компьютер пользователя или сетевой компьютер.

КЛИЕНТУ предоставляется неисключительное право на использование клиентской части Системы «iBank 2» на срок действия Договора РКО.

Неисключительное право на использование клиентской части Системы «iBank 2» не включает права на:

- декомпилирование, изучение кода, модификацию и изменение клиентского модуля или любой его части;
- передачу полученного права третьим лицам;
- изготовление не предусмотренных руководством пользователя экземпляров Системы «iBank 2», за исключением резервных, используемых в архивных целях.

БАНК гарантирует, что он вправе передавать КЛИЕНТУ неисключительные права на использование клиентской части Системы «iBank 2» и что такое предоставление не повлечет предъявления к КЛИЕНТУ исков со стороны третьих лиц.

Для подключения Услуги по дистанционному обслуживанию с использованию Системы «iBank 2», КЛИЕНТУ необходимо ознакомиться с Правилами использования Системы «iBank 2» (**Приложение № 1** к настоящим Условиям), Требованиями по обеспечению безопасности при работе с Системой «iBank 2» (**Приложение № 2** к настоящим Условиям), Требованиями по защите от Вредоносного кода рабочего места Системы «iBank 2» (**Приложение № 3** к настоящим Условиям). Услуга предоставляется КЛИЕНТУ на основании Заявления о подключении Услуги по дистанционному обслуживанию с использованием Системы «iBank 2» (**Приложение № 5** к настоящим Условиям). После прохождения КЛИЕНТОМ регистрации в Системе «iBank 2» в порядке, предусмотренном **Приложением № 4** к настоящим Условиям, КЛИЕНТ получает по Акту передачи аппаратные средства усиленной электронной подписи, сопроводительную документацию, и приступает к работе в Системе «iBank 2».

1. Термины и определения, применяемые в настоящих Условиях

1.1. **Электронное средство платежа (ЭСП)** – средство и (или) способ, позволяющие КЛИЕНТУ составлять, удостоверять и передавать распоряжения в целях осуществления перевода денежных средств в рамках применяемых форм безналичных расчетов с использованием информационно-коммуникационных технологий, электронных носителей информации, также иных технических устройств.

1.2. **Система «iBank 2» (Система)** – совокупность программно-аппаратных средств, устанавливаемых на территории КЛИЕНТА и БАНКА, и согласовано эксплуатируемых КЛИЕНТОМ и БАНКОМ в соответствующих частях с целью осуществления переводов денежных средств. В рамках настоящих Условий Система «iBank 2» является электронным средством платежа.

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

1.3.1. **Платежные ЭД** – финансовый документ, распоряжение КЛИЕНТА на расходную операцию;

1.3.2. **Неплатежные ЭД** – документы, имеющие информационный характер, не подразумевающие распоряжение КЛИЕНТА на расходные операции по Счету(-там).

Перечень ЭД, которые могут быть направлены через Систему «iBank 2» представлен в **Приложении № 9** к настоящим Условиям.

1.4. **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.

1.5. **Ключ электронной подписи (Ключ ЭП)** – уникальная последовательность символов, предназначенная для создания ЭП.

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

1.7. **Пара ключей электронной подписи (Пара ключей ЭП)** – Ключ ЭП и соответствующий ему Ключ проверки ЭП.

1.8. **Подлинная электронная подпись (Подлинная ЭП)** – ЭП в ЭД, проверка которой с использованием соответствующего Ключа проверки ЭП дает положительный результат.

1.9. **Активная пара ключей электронной подписи (Активная пара ключей ЭП)** – пара ключей ЭП, зарегистрированных БАНКОМ в Системе «iBank 2», и используемых сотрудником КЛИЕНТА для работы в Системе «iBank 2».

1.10. **Сертификат ключа проверки электронной подписи (Сертификат)** – документ на бумажном носителе, выданный удостоверяющим центром, заверенный подписью владельца ключа проверки ЭП, подписью руководителя и оттиском печати КЛИЕНТА. Сертификат является приложением к **Заявлению о подключении Услуги по дистанционному обслуживанию с использованием Системы «iBank 2» (Приложение № 5** к настоящим Условиям).

1.11. **Удостоверяющий центр** – юридическое лицо или индивидуальный предприниматель, осуществляющие функции по созданию и выдаче Сертификатов, а также иные функции, предусмотренные Федеральным законом Российской Федерации от 6 апреля 2011 г. N 63-ФЗ «Об электронной подписи». В рамках настоящих Условий функции удостоверяющего центра выполняются БАНКОМ.

1.12. **Аппаратное средство усиленной электронной подписи (Аппаратное средство усиленной ЭП)** – специализированное аппаратное средство, предназначенное для генерации Пары ключей ЭП, хранения сгенерированных Ключей ЭП, формирования ЭП в документах в соответствии с утвержденными стандартами с использованием встроенного в устройство сертифицированного средства криптографической защиты информации. Аппаратное средство усиленной ЭП могут получить только лица, указанные в карточке с образцами подписей и оттиском печати.

1.13. **Программное средство усиленной электронной подписи (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 и сертифицированный в соответствии с действующим законодательством РФ.

1.14. **Ключевое слово** – уникальное слово, определяемое КЛИЕНТОМ при регистрации в Системе «iBank 2», сообщаемое сотруднику БАНКА в рамках телефонного звонка, используемое КЛИЕНТОМ для блокирования (например, в случае компрометации Ключа ЭП) своей работы в Системе «iBank 2»;

КЛИЕНТ несет полную ответственность за разглашение Ключевого слова, а также за последствия такого разглашения.

1.15. **Компрометация Средства подтверждения –** утрата/хищение Средства подтверждения, несанкционированное копирование Ключа ЭП, передача Ключа ЭП по открытым каналам связи, любые другие признаки осуществления несанкционированных действий в системе «iBank 2», а также случаи, когда нельзя достоверно установить, что произошло со Средством подтверждения.

1.16. **Средство подтверждения** – электронное или иное средство, используемое для подписи/подтверждения ЭД. В качестве средства подтверждения могут использоваться, включая, но не ограничиваясь: Аппаратное средство усиленной ЭП с ключами ЭП, файловое хранилище ключей ЭП, зарегистрированный в Системе мобильный телефон.

1.17. **Одноразовый пароль** – динамическая аутентификационная информация, генерируемая для единичного использования, в целях дополнительного подтверждения КЛИЕНТОМ платежа.

1.18. **Вредоносный код** – компьютерная программа, предназначенная для внедрения в автоматизированные системы, программное обеспечение, средства вычислительной техники, телекоммуникационное оборудование БАНКА и/или КЛИЕНТА, приводящего к уничтожению, созданию, копированию, блокированию, модификации и (или) передаче информации, а также к созданию условий для такого уничтожения, создания, копирования, блокирования, модификации и (или) передачи.

1.19. **Автоматизированное Рабочее место Клиента (АРМ Клиента)** - индивидуальный программно-технический комплекс, предназначенный для дистанционного взаимодействия КЛИЕНТА с БАНКОМ по системе «iBank 2».

1.20. **Протоколы операций** — файлы или записи базы данных, содержащие в хронологическом порядке сведения о действиях пользователя и иных событиях в системе «iBank 2».

1.21. **Система криптозащиты (СКЗИ)** – функция программы, предназначенная для обеспечения подлинности и авторства документов, обрабатываемых в электронной форме с помощью вычислительной техники.

1.22. **IP-фильтрация** – ограничение доступа к удаленному компьютеру только с указанных IP адресов и сетей.

1.23. **Многофакторная аутентификация** - расширенная **аутентификация**, метод контроля доступа к компьютеру, в котором пользователю для получения доступа к информации необходимо предъявить более одного «доказательства механизма **аутентификации**».

1.24. **Файловое хранилище** – аппаратное устройство, предназначенное для хранения файлов (флэш-накопитель, диск, мобильное устройство и др.)

1.25. **Владелец ЭП без права подписи** – лица, обладающие ЭП только для входа в Систему «iBank 2», получения доступа к информации, отображаемой в Системе «iBank 2», для создания в Системе «iBank 2» платёжных ЭД и (или) неплатёжных ЭД, но не обладающие правом их подписывать и направлять в Банк.

1.26. **Сервис «Мобильный банк»** – дополнительный в рамках Услуги «iBank 2» информационный сервис для пользователей Системы «iBank 2», обеспечивающий КЛИЕНТУ возможность через мобильное приложение просматривать информацию по Счетам и выполнять действия, предусмотренные п. 3 **Приложения № 13** к настоящим Условиям.

Описание сервиса и процедура подключения приведены в **Приложении № 13** к настоящим Условиям.

2. Соглашения СТОРОН

2.1. 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 ЭД.

2.2. Стороны признают, что применяемая в Аппаратных средствах усиленной ЭП технология генерации и хранения Ключа ЭП, формирования ЭП под документом с использованием Аппаратного средства усиленной ЭП полностью исключает возможность получения прямого доступа к Ключу ЭП с целью его копирования, переноса на внешний носитель или использования для формирования ЭП вне устройства.

2.3. Аппаратные средства усиленной ЭП являются собственностью БАНКА и предоставляются для использования КЛИЕНТУ на возмездной основе.

2.4. Стороны признают, что при произвольном изменении ЭД, заверенного ЭП, ЭП становится не подлинной, то есть проверка подлинности ЭП дает отрицательный результат.

2.5. Стороны признают, что подделка ЭП сотрудника КЛИЕНТА, то есть создание Подлинной ЭП в ЭД от имени сотрудника КЛИЕНТА, невозможна без использования Ключа ЭП сотрудника КЛИЕНТА.

2.6. Стороны признают, что ЭД с ЭП сотрудников КЛИЕНТА, полученные БАНКОМ по Системе «iBank 2», являются доказательным материалом для решения спорных вопросов в соответствии с **Положением о процедуре разбора конфликтных ситуаций (Приложение № 9** к настоящим Условиям). Электронные документы, не имеющие необходимого количества ЭП, при наличии спорных вопросов не являются доказательным материалом.

2.7. Стороны признают, что Ключ проверки ЭП сотрудника КЛИЕНТА, содержащийся в Сертификате, принадлежит соответствующему сотруднику КЛИЕНТА, наделенному правом подписи финансовых документов. Права подписи и возможные сочетания подписей должны соответствовать сведениям, указанным в карточке с образцами подписей и оттиском печати и Соглашению о количестве подписей, необходимых для подписания платежных документов и их возможных сочетаниях (Приложение № 5 к Договору РКО).

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

2.9. 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 с зарегистрированного мобильного телефона, указанного КЛИЕНТОМ в **Заявлении о подключении Услуги по дистанционному обслуживанию с использованием системы «iBank2» (Приложение № 5** к настоящим Условиям).

2.10. Стороны признают, что подделка Одноразового пароля, то есть подтверждение ЭД от имени КЛИЕНТА, практически невозможна без владения соответствующим Средством подтверждения.

2.11. Стороны признают, что ЭД должны быть подписаны не менее чем двумя ЭП, необходимыми для подписания финансовых документов, если иное количество подписей не определено **Соглашением о количестве подписей, необходимых для подписания платежных документов, и их возможных сочетаниях (Приложение № 5 к Договору РКО).**

БАНК принимает Неплатежные документы по Системе «iBank 2» за одной ЭП любого лица, включенного в карточку с образцами подписей и оттиска печати.

2.12. Стороны признают, что ЭД, 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. ЭД без необходимого количества ЭП сотрудников КЛИЕНТА не имеют юридической силы, БАНКОМ не рассматриваются и не исполняются.

2.13. Стороны признают, что возможность воспроизведения в электронном виде и на бумажных носителях принятого к исполнению и исполненного платежного распоряжения с отметками БАНКА осуществляется с использованием системы «iBank 2». Получение платежного распоряжения на бумажном носителе с отметками БАНКА может осуществляться также в офисе БАНКА в соответствии с графиком работы БАНКА.

2.14. Стороны признают надлежащим уведомление КЛИЕНТА о совершенных операциях с использованием ЭСП хотя бы одним из способов, установленных **Положением о порядке и способах информирования КЛИЕНТА о совершенных операциях с использованием электронного средства платежа (Приложение № 11** к настоящим Условиям).

2.15. Стороны признают, что Протоколы операций, заполняемые посредством системы «iBank 2», могут использоваться в качестве доказательства авторства проводимых КЛИЕНТОМ операций, а также в качестве доказательства нарушения КЛИЕНТОМ **Требований по защите от Вредоносного кода рабочего месте Системы «iBank 2» (Приложение № 3** к настоящим Условиям).

2.16. Срок хранения ключей ЭП, с истекшим сроком действия, определяется БАНКОМ самостоятельно в соответствии с требованиями документации на СКЗИ, но не менее 3 (трех) лет.

2.17. Стороны пришли к соглашению, что платежные поручения на сумму, превышающую 100 000 (Сто тысяч) рублей, требуют подтверждение одноразовым паролем. Пароль автоматически высылается на мобильный телефон, указанный в **Заявлении о подключении Услуги по дистанционному обслуживанию с использованием системы «iBank2» (Приложение № 5** к настоящим Условиям), после подписания платежного поручения.

3. Права КЛИЕНТА

3.1. На основании имеющихся у БАНКА лицензий ФСБ РФ КЛИЕНТ имеет право осуществлять эксплуатацию предоставленных БАНКОМ сертифицированных ФСБ РФ Программных и Аппаратных средств усиленной ЭП в Системе «iBank 2».

3.2. КЛИЕНТ имеет право досрочно прекратить действие своей Активной пары ключей ЭП и потребовать от БАНКА блокировать эту Пару ключей ЭП, оформив **Уведомление о прекращении действия средства подтверждения в связи с утратой средства подтверждения / использования ЭСП без согласия Клиента (Приложение № 7** к настоящим Условиям).

3.3. КЛИЕНТ имеет право по своему усмотрению генерировать новые Пары ключей ЭП и регистрировать в БАНКЕ новые Ключи проверки ЭП.

3.4. КЛИЕНТ имеет право установить / отключить IP-фильтрацию при работе в Системе, подключить / отключить многофакторную аутентификацию с использованием одноразовых паролей при входе в Систему, заполнив соответствующие графы в **Заявлении о подключении Услуги по дистанционному обслуживанию с использованием системы «iBank2» (Приложение № 5** к настоящим Условиям).

3.5. В случае если КЛИЕНТУ необходимо заменить средство подтверждения, установить / отключить IP-фильтрацию и иное) КЛИЕНТ повторно подписывает **Заявление о подключении Услуги по дистанционному обслуживанию с использованием системы «iBank2» (Приложение № 5** к настоящим Условиям), отметив в соответствующем поле, что Заявление – «корректирующее», и вносит изменения только в те графы, в которых будет меняться соответствующая информация.

3.6. В случае необходимости КЛИЕНТ вправе приостановить действие Системы «iBank2», предоставив в БАНК **Уведомление о приостановлении использования Услуги по дистанционному обслуживанию с использованием Системы «iBank2»** (Приложение № 8 к настоящим Условиям).

4. Обязанности КЛИЕНТА

4.1. Перед началом эксплуатации Системы «iBank 2» КЛИЕНТ обязан получить в БАНКЕ и самостоятельно установить на своем рабочем месте Программные и Аппаратные средства усиленной ЭП.

Для хранения ЭП с правом подписания и отправки в Банк платёжных и других документов Клиент обязан использовать только Аппаратные средства усиленной ЭП.

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

4.3. КЛИЕНТ обязан обеспечивать сохранность и целостность программного комплекса Системы «iBank 2», включая предоставленные Средства усиленной ЭП.

4.4. КЛИЕНТ обязан обеспечивать информационную безопасность (в том числе защиту от Вредоносного кода) 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.

4.5. КЛИЕНТ обязан ознакомиться с описанием механизмов защиты Системы «iBank 2» - **Требованиями по обеспечению безопасности при работе с системой дистанционного банковского обслуживания «iBank2» (Приложение № 2** к настоящим Условиям). 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.

4.6. КЛИЕНТ обязан в случае прекращения использования Системы «iBank 2» вернуть полученные в БАНКЕ Программные и аппаратные средства усиленной ЭП, о чем делается соответствующая отметка в Акте передачи аппаратных средств усиленной электронной подписи и сопроводительной документации (Приложение № 6 к настоящему Договору).

4.7. КЛИЕНТ обязан заполнять ЭД в Системе «iBank 2» в соответствии с действующим Положением БАНКА России от 19 июня 2012 г. № 383-П «О правилах осуществления перевода денежных средств» или аналогичным документом, утвержденным вместо указанного Положения.

4.8. КЛИЕНТ обязан хранить в секрете пароль к Ключу ЭП и не передавать третьим лицам Средство подтверждения, используемое в Системе «iBank 2», а также обеспечить защиту Ключа ЭП и Средства подтверждения от несанкционированного использования третьими лицами.

4.9. КЛИЕНТ обязан обеспечивать использование Ключей ЭП только их владельцами (ответственными сотрудниками) в соответствии с установленными правами подписи.

4.10. КЛИЕНТ обязан по требованию БАНКА прекратить использование указанного БАНКОМ Ключа ЭП, сгенерировать новую Пару ключей ЭП и зарегистрировать новый Ключ проверки ЭП в БАНКЕ.

4.11. КЛИЕНТ обязан предоставить БАНКУ достоверную информацию для связи и информирования о совершении операций.

4.12. В случае изменения информации для связи и информирования КЛИЕНТ обязан своевременно предоставить БАНКУ обновленную информацию в соответствии с п. 3.6. настоящих Условий. Обязанность БАНКА по направлению КЛИЕНТУ уведомлений о совершении операций считается исполненной при направлении уведомления в соответствии с имеющейся у БАНКА информацией для связи с КЛИЕНТОМ.

4.13. В случае компрометации Средства подтверждения КЛИЕНТ обязан незамедлительно проинформировать БАНК в соответствии с **Положением о порядке действий сторон в случае компрометации средства подтверждения (Приложение № 12** к настоящим Условиям»).

4.14. КЛИЕНТ обязан исполнять обязательства, возникшие до момента приостановления или прекращения использования КЛИЕНТОМ ЭСП.

4.15. КЛИЕНТ обязан перед подключением к Системе, а также по запросу БАНКА подтверждать выполнение **Требований по защите от Вредоносного кода (Приложение № 3** к настоящим Условиям**)** с указанием конкретных средств защиты от Вредоносного кода и проведенных мероприятий.

4.16. КЛИЕНТ обязан уведомить БАНК о прекращении/изменении полномочий лиц, имеющих действующие сертификаты ключа ЭП, в возможно короткий срок, но не позднее 5 (Пяти) рабочих дней с даты внесения соответствующих записей в Единый государственный реестр юридических лиц/индивидуальных предпринимателей (далее «ЕГРЮЛ/ЕГРИП»).

В случае невыполнения указанной обязанности КЛИЕНТ несет полную ответственность за неблагоприятные последствия, связанные с получением информации по счетам КЛИЕНТА, а также созданием и подписью ЭД такими лицами после прекращения/изменения их полномочий.

4.17. КЛИЕНТ обязан при работе с Программными и Аппаратными средствами усиленной ЭП выполнять требования законодательных актов Российской Федерации, регламентирующих использование средств криптографической защиты информации.»

4.18. КЛИЕНТ обязан в случае компрометации средств подтверждения и/или поступления платежного поручения по Системе «iBank 2» без ведома КЛИЕНТА / совершения платежа без согласия КЛИЕНТА, о котором БАНК уведомил КЛИЕНТА в соответствии с настоящими Условиями, наличия подозрения, что Системой «iBank 2» могут воспользоваться третьи лица, утраты/завладения Аппаратными средствами усиленной электронной подписи, иное, совершать действия, предусмотренные **Положением о порядке действий сторон в случае компрометации средства подтверждения (Приложение № 12** к настоящим Условиям)

5. Права БАНКА

5.1. БАНК имеет право отказать КЛИЕНТУ в подключении Услуги по дистанционному обслуживанию с использованием Системы «iBank 2».

5.2. БАНК имеет право по своему усмотрению без уведомления КЛИЕНТА блокировать Активную пару ключей ЭП КЛИЕНТА и потребовать от КЛИЕНТА смены Пары ключей ЭП.

5.3. При наличии обоснованных подозрений о нарушении КЛИЕНТОМ порядка использования ЭСП, БАНК имеет право не производить исполнение полученных от КЛИЕНТА ЭД, заблокировать

использование ЭСП и требовать от КЛИЕНТА предоставления оформленных в установленном порядке платежных документов на бумажном носителе. БАНК обязан незамедлительно, но не позднее 24 (Двадцати четырех) часов, любым способом сообщить КЛИЕНТУ о возникновении подобных подозрений и необходимости предоставить платежные документы на бумажном носителе.

5.4. При нарушении КЛИЕНТОМ обязанности по предоставлению БАНКУ достоверной информации для связи с КЛИЕНТОМ или обновленной информации в случае ее изменения, БАНК вправе приостановить использование КЛИЕНТОМ ЭСП до получения от КЛИЕНТА достоверной информации. При этом БАНК прекращает обработку всех ЭД, полученных от КЛИЕНТА.

5.5. БАНК имеет право не возмещать КЛИЕНТУ сумму операции, совершенной без согласия КЛИЕНТА при условиях:

5.5.1. БАНК исполняет обязанность по информированию КЛИЕНТА о совершении операций;

5.5.2. КЛИЕНТ не направил БАНКУ **Уведомление о прекращении действия средства подтверждения в связи с утратой средства подтверждения / использования ЭСП без согласия Клиента (Приложение № 7** к настоящим Условиям) на бумажном носителе за подписью руководителя КЛИЕНТА и оттиском печати в случае утраты Ключей ЭП и/или Средства подтверждения и/или об утрате Аппаратного средства усиленной ЭП или Средства подтверждения и/или об использовании Системы «iBank 2» без согласия КЛИЕНТА в установленные настоящими Условиями сроки.

5.6. В случае возникновения у БАНКА технических неисправностей или других обстоятельств, препятствующих использованию КЛИЕНТОМ ЭСП, БАНК имеет право в одностороннем порядке приостановить до момента устранения неисправности использование ЭСП КЛИЕНТОМ. Все документы в этом случае должны передаваться сторонами на бумажных носителях.

5.7. БАНК имеет право разрабатывать, внедрять и предоставлять КЛИЕНТУ для последующего использования и применения:

новые версии Системы «iBank 2»;

новые средства электронной подписи (аппаратные, программные) и средства подтверждения, используемые в Системе «iBank 2»;

новую техническую и регламентную документацию по Системе «iBank 2»;

новые механизмы защиты от Вредоносного кода, используемые в Системе «iBank 2».

6. Обязанности БАНКА

6.1. БАНК обязан принимать к исполнению ЭД, полученные по Системе «iBank 2» от КЛИЕНТА , соответствующие требованиям настоящих Условий, действующему законодательству РФ, подписанные необходимым количеством ЭП сотрудников КЛИЕНТА в соответствии с Карточкой с образцами подписей и оттиском печати / Карточкой с образцами подписей и оттиском печати и Соглашением о количестве подписей, необходимых для подписания платежных документов и их возможных сочетаниях (Приложение № 5 к Договору РКО) в случае его заключения.

6.2. БАНК обязан информировать КЛИЕНТА о совершении операциях с использованием электронного средства платежа способами, установленными **Положением о порядке и способах информирования КЛИЕНТА о совершенных операциях с использованием системы «iBank 2» (Приложение № 11** к настоящим Условиям).

6.3. БАНК обязан предоставлять КЛИЕНТУ необходимые рекомендации для работы с Системой «iBank 2».

6.4. БАНК обязан передать КЛИЕНТУ необходимые для работы программные модули системы «iBank 2», аппаратные средства усиленной электронной подписи, сопроводительную документацию до начала работы КЛИЕНТА в Системе «iBank 2». Факт передачи указанных средств фиксируется в **Акте передачи аппаратных средств усиленной электронной подписи и сопроводительной документации (Приложение № 6** к настоящим Условиям).

6.5. БАНК обязан после принятия от КЛИЕНТА **Уведомления о прекращении действия средства подтверждения в связи с утратой средства подтверждения / использования ЭСП без согласия Клиента,** на бумажном носителе, подписанного руководителем КЛИЕНТА и с оттиском печати **(Приложение № 7** к настоящим Условиям) незамедлительно заблокировать все ключи ЭП/Средства подтверждения и прекратить обработку ЭД, подписанных/подтвержденных указанными средствами, в случае если имеется техническая возможность остановить совершение платежа КЛИЕНТА, имеющегося в БАНКЕ в момент получения вышеуказанного Уведомления на обработке.

6.6. В случае получения от КЛИЕНТА **Уведомления о прекращении действия средства подтверждения в связи с утратой средства подтверждения / использования ЭСП без согласия Клиента (Приложение № 7** к настоящим Условиям) **на бумажном носителе** в случаях и срок, установленные **Положением о порядке действий сторон в случае компрометации средства подтверждения (Приложение № 12** к настоящим Условиям), БАНК обязан возместить КЛИЕНТУ сумму операции, совершенной без согласия КЛИЕНТА после получения указанного Уведомления.

6.7. Возмещение КЛИЕНТУ суммы операции производится на указанный КЛИЕНТОМ счет в срок не более 30 (тридцати) дней, а также не более 60 дней в случае использования электронного средства

платежа для осуществления трансграничного перевода денежных средств, после проведения разбора конфликтной ситуации в соответствии с действующим на момент рассмотрения конфликтной ситуации **Положением о процедуре разбора конфликтных ситуаций (Приложение № 9** к настоящему Договору) при условии подтверждения по результатам работы комиссии факта получения БАНКОМ соответствующего Уведомления КЛИЕНТА и совершения операции без согласия КЛИЕНТА.

6.8. В случае неисполнения БАНКОМ обязанности по информированию КЛИЕНТА о совершенной операции, БАНК обязан возместить КЛИЕНТУ сумму операции, о которой КЛИЕНТ не был проинформирован и которая была совершена без согласия КЛИЕНТА.

6.9. Возмещение КЛИЕНТУ суммы операции производится на указанный КЛИЕНТОМ счет в срок не более 30 (тридцати) дней, а также не более 60 дней в случае использования электронного средства платежа для осуществления трансграничного перевода денежных средств, после проведения разбора конфликтной ситуации в соответствии с действующим на момент рассмотрения конфликтной ситуации **Положением о процедуре разбора конфликтных ситуаций (Приложение № 9** к настоящим Условиям) при условии подтверждения по результатам работы комиссии факта неисполнения БАНКОМ обязанности по информированию КЛИЕНТА об оспариваемой операции.

6.10. БАНК обязан фиксировать полученные от КЛИЕНТА **Уведомления о прекращении действия средства подтверждения в связи с утратой средства подтверждения / использования ЭСП без согласия Клиента (Приложение № 7** к настоящим Условиям) и подтверждать получение указанного Уведомления, полученного на бумажном носителе, путем проставления на клиентском экземпляре соответствующих подписей уполномоченных лиц Банка и оттиска печати.

6.11. БАНК обязан хранить полученные от КЛИЕНТА **Уведомления о прекращении действия средства подтверждения в связи с утратой средства подтверждения / использования ЭСП без согласия Клиента (Приложение № 7** к настоящим Условиям) на бумажном носителе не менее трех лет.

7. Совместные обязательства и ответственность СТОРОН

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

7.2. БАНК не несёт ответственности за ущерб, причинённый КЛИЕНТУ в результате использования третьими лицами Ключа ЭП КЛИЕНТА.

7.3. При отключении Услуги «iBank 2» Стороны несут ответственность по всем ЭД, сформированным в Системе «iBank 2», в соответствии с настоящими Условиями и действующим законодательством РФ.

7.4. В случае возникновении конфликтных ситуаций между КЛИЕНТОМ и БАНКОМ при использовании Системы «iBank 2», СТОРОНЫ обязуются участвовать в рассмотрении споров в соответствии с действующим **Положением о процедуре разбора конфликтных ситуаций (Приложение № 9** к настоящим Условиям), выполнять требования указанные в данном Положении и нести ответственность согласно выводам по рассмотрению конфликтной ситуации. Действия СТОРОН согласно указанному Положению являются обязательной составляющей процедуры досудебного урегулирования споров.

7.5. СТОРОНЫ обязуются при разрешении экономических и иных споров, которые могут возникнуть в связи с использованием ЭСП, предоставлять в письменном виде свои оценки, доказательства и выводы по запросу заинтересованной СТОРОНЫ.

7.6. В случае недостижения СТОРОНЫ согласия, споры решаются в судебном порядке в Арбитражном суде г. Москвы.

7.7. СТОРОНЫ освобождаются от ответственности за частичное или полное неисполнение своих обязательств, принятых в соответствии с настоящими Условиями в случае возникновения обстоятельств непреодолимой силы. Обстоятельства непреодолимой силы понимаются в соответствии с пунктом 3 статьи 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.

7.8. БАНК не несёт ответственности за ущерб, причинённый КЛИЕНТУ в результате нарушения или ненадлежащего исполнения КЛИЕНТОМ **Требований по защите от Вредоносного кода рабочего места Системы «iBank2» (Приложение № 3** к настоящим Условиям).

7.9. В случае нарушения КЛИЕНТОМ условий использования полученного в рамках настоящих Условий программного обеспечения (в том числе, но не ограничиваясь случаями тиражирования и (или) передачи программного обеспечения третьим лицам, вскрытия технологии и (или) деассемблирования и (или) декомпиляции программного продукта), и предъявления третьими лицами требований к БАНКУ, КЛИЕНТ обязуется возместить БАНКУ убытки в полном объеме.

8. Процедуры приема к исполнению, отзыва, возврата (аннулирования) распоряжений и порядок их выполнения

8.1. БАНК осуществляет прием ЭД, передаваемых по Системе «iBank2», круглосуточно. При невозможности передачи ЭД в БАНК с использованием Системы «iBank2» КЛИЕНТ может подать документы в БАНК на бумажном носителе.

8.2. ЭД считается полученным БАНКОМ после присвоения ему в Системе «iBank2» статуса «Доставлен».

8.3. При получении от КЛИЕНТА ЭД, содержащего распоряжение, БАНК производит следующие процедуры:

8.3.1. В автоматизированном режиме производится проверка подлинности ЭП сотрудника(-ов) КЛИЕНТА в ЭД. При необходимости подтверждения ЭД Одноразовым паролем, БАНК в автоматизированном режиме проверяет правильность Одноразового пароля.

При положительном результате проверок распоряжение считается совершенным уполномоченным лицом (лицами). Целостность распоряжения считается подтвержденной.

8.3.2. В автоматизированном режиме производится структурный контроль распоряжения и проверка правильности заполнения реквизитов распоряжения в соответствии с действующим законодательством РФ и нормативными актами БАНКА России.

8.3.3. В автоматизированном режиме производится проверка достаточности денежных средств на расчётном счёте КЛИЕНТА.

8.4. В случае положительного результата проведения проверок, указанных в пункте 8.3. настоящего Раздела, распоряжение принимается БАНКОМ к исполнению.

8.5. Распоряжение не принимается БАНКОМ к исполнению в случае отбраковки такого ЭД по критериям, указанным в пункте 8.3. настоящих Условий, ЭД при этом аннулируется БАНКОМ.

8.6. Стороны признают надлежащим способ уведомления КЛИЕНТА об аннулировании БАНКОМ распоряжений и иных ЭД путем присвоения статуса «Отвергнут», присвоенного ЭД в Системе «iBank 2». В электронной форме документа КЛИЕНТУ доступна информация, позволяющая идентифицировать аннулируемое распоряжение, дату его аннулирования и причину.

8.7. ЭД считается принятым БАНКОМ к исполнению после присвоения ему в Системе «iBank 2» статуса «На обработке» («На исполнении»).

8.8. ЭД считается исполненным БАНКОМ после присвоения ему в Системе «iBank 2» статуса «Исполнен».

8.9. СТОРОНЫ признают надлежащим способ уведомления КЛИЕНТА о получении и/или исполнении БАНКОМ распоряжений и иных ЭД путем присвоения соответствующего статуса ЭД в системе «iBank 2». В электронной форме документа КЛИЕНТУ доступна информация, содержащая реквизиты БАНКА, идентификатор системы «iBank 2», вид операции, дату операции, сумму операции, идентификатор операции с использованием системы «iBank 2», а также электронные отметки БАНКА об исполнении ЭД.

8.10. Характеристики переводов денежных средств: безотзывность, безусловность и окончательность трактуются в соответствии с действующим законодательством РФ. Данные характеристики переводов денежных средств, осуществляемых БАНКОМ на основании распоряжений КЛИЕНТОВ, имеют следующие особенности:

8.10.1. Безотзывность перевода денежных средств наступает с момента списания денежных средств со счета плательщика.

8.10.2. Безусловность перевода денежных средств означает отсутствие условий или выполнение всех условий для осуществления перевода денежных средств в определенный момент времени.

Безусловность перевода денежных средств наступает:

- при расчетах платежными требованиями - в случае предоставления КЛИЕНТОМ АКЦЕПТА;

- при расчетах инкассовыми поручениями - в случае наличия в Договоре РКО между КЛИЕНТОМ и БАНКОМ условия о списании денежных средств со счета КЛИЕНТА и представлении КЛИЕНТОМ в БАНК сведений о получателе средств, имеющем право предъявлять инкассовые поручения к счету КЛИЕНТА.

8.11.3. Окончательность перевода денежных средств наступает:

- при переводе денежных средств на счет получателя, открытый в БАНКЕ - в момент зачисления денежных средств на счет получателя средств;

- при переводе на счета, открытые в иных банках, - в момент зачисления денежных средств на счет банка получателя денежных средств.

8.12. КЛИЕНТ вправе совершить отзыв распоряжения о переводе денежных средств до наступления момента безотзывности перевода, предоставив в БАНК электронное заявление об отзыве распоряжения по форме, предусмотренной настройками системы «iBank 2», с возможностью указания причины отзыва документа. Заявление об отзыве служит основанием для отзыва БАНКОМ распоряжения.

8.13. Способом уведомления КЛИЕНТА об отзыве распоряжения Стороны признают присвоенный ЭД в Системе «iBank 2» статус «Отвергнут». В электронной форме документа КЛИЕНТУ доступна

информация, позволяющая идентифицировать аннулируемое распоряжение, дату его аннулирования и причину.

9. Стоимость услуг и порядок оплаты

9.1. Стоимость использования КЛИЕНТОМ ЭСП рассчитывается согласно Тарифам БАНКА, размещенным на общедоступных ресурсах БАНКА (информационных стендах в операционных залах и/или сайте БАНКА **www.russitabank.ru)**.

9.2. Оплата Услуги «iBank 2» в соответствии с настоящими Условиями производится путём списания денежных средств с расчетного счёта КЛИЕНТА на основании п. 5.2.3. Договора РКО.

9.3. В случае неоплаты КЛИЕНТОМ в срок стоимости Услуги «iBank 2» БАНК вправе заблокировать использование ЭСП КЛИЕНТОМ без предварительного уведомления.

9.4. В случае блокирования БАНКОМ использования ЭСП КЛИЕНТОМ по основаниям, предусмотренным пунктом 9.3. настоящих Условий, повторное предоставление КЛИЕНТУ возможности использования ЭСП производится после оплаты КЛИЕНТОМ задолженности по предоставленной Услуге.

10. Иные условия

10.1. Настоящие Условия дистанционного обслуживания с использованием Системы «iBank 2», принятые КЛИЕНТОМ, вступают в силу со дня предъявления в БАНК **Заявления о подключении Услуги по дистанционному обслуживанию с использованием Системы «iBank 2» (Приложению № 5** к настоящим Условиям) и действуют до момента расторжения Договора РКО или до момента отключении БАНКОМ КЛИЕНТУ Услуги «iBank 2» в одностороннем порядке или отключения Услуги КЛИЕНТОМ на основании заявления в свободной форме.

10.2. С момента расторжения Договора расчетно-кассового обслуживания в МКИБ «РОССИТА-БАНК» ООО на публичных условиях **Условия дистанционного обслуживания с использованием системы «iBank 2»** автоматически прекращают свое действие, БАНК блокирует доступ КЛИЕНТА к банковской части Системы «iBank 2».

10.3. Стороны вправе по обоюдному согласию вносить изменения и дополнения к настоящим Условиям в виде заключения дополнительных соглашений, которые будут вступать в силу с момента их подписания обеими Сторонами.

Приложение № 1
к Условиям дистанционного обслуживания
клиентов с использованием Системы «iBank 2»

ПРАВИЛА
использования Системы «iBank 2»

В настоящих Правилах понятия Рабочее место и Вредоносный код используются в соответствии с терминологией Условий дистанционного обслуживания клиентов по системе «iBank 2».

Во исполнение пункта 3 статьи 9 Федерального закона «О национальной платежной системе» БАНК настоящим информирует КЛИЕНТА о следующем:

1. Использование клиентской части Системы «iBank 2» (далее – Система) допускается из любых мест и любыми возможными способами с учетом указанных ниже ограничений.

2. Использование Системы не рекомендуется в следующих случаях (включая, но не ограничиваясь):

2.1. КЛИЕНТОМ не выполнены Требования по защите от Вредоносного кода; Требования по обеспечению безопасности при работе с системой дистанционного банковского обслуживания «iBank2».

2.2. На Рабочем месте КЛИЕНТА не установлены полученные из доверенных источников сертифицированные ФСБ средства криптографической защиты информации (СКЗИ);

2.3. КЛИЕНТ не обеспечил надежное хранение и защиту от компрометации средств, использующихся для дистанционного распоряжения счетом КЛИЕНТА (Средства подтверждения

2.4. КЛИЕНТ не ознакомился с правилами работы с Системой и правилами работы с СКЗИ;

2.5. КЛИЕНТ не обеспечил периодическую (но не реже 1 раза в год) смену паролей для доступа к своему Рабочему месту или к ключу ЭП;

2.6. КЛИЕНТОМ был обнаружен отказ специализированного ПО, используемого для защиты информации, или отказ клиентской части Системы;

2.7. КЛИЕНТОМ не обеспечен запрет использования на Рабочем месте средств удаленного управления (R-Admin, TeamViewer и аналоги), администрирования и модификации ОС и её настроек (службы терминалов, удаленных рабочих столов и аналоги);

2.8. У КЛИЕНТА не настроены минимум два канала оповещения о совершении операций.

3.КЛИЕНТ уведомлен, что при использовании Системы он несет повышенные риски, связанные с несанкционированным списанием средств КЛИЕНТА неуполномоченными лицами, в том числе и с использованием Вредоносного кода. Начиная работать с Системой, КЛИЕНТ подтверждает, что он полностью принимает на себя указанные риски.

4. КЛИЕНТ несет полную ответственность за действия, совершенные третьими лицами, в случае передачи КЛИЕНТОМ Средств подтверждения указанным лицам и/или в случае создания КЛИЕНТОМ условий для несанкционированного использования третьими лицами Средств подтверждения. КЛИЕНТ также несет полную ответственность за ущерб, причиненный БАНКУ, указанными действиями или бездействием.

5. КЛИЕНТ согласен с использованием логов (журналов) Системы и журналов модуля Системы по детектированию вредоносного программного обеспечения в качестве доказательства при разбирательстве по факту нарушений настоящих Правил и требований по защите от Вредоносного кода.

6. КЛИЕНТ уведомлен, что при использовании одного Аппаратного средства усиленной ЭП для хранения Ключей ЭП нескольких сотрудников он несет повышенные риски, связанные с несанкционированным списанием средств КЛИЕНТА неуполномоченными лицами, в том числе и с использованием Вредоносного кода. БАНК рекомендует КЛИЕНТУ использовать Аппаратное средство усиленной ЭП для хранения одного Ключа ЭП одного сотрудника. Начиная работать с Системой, КЛИЕНТ подтверждает, что он полностью принимает на себя указанные риски.

7. КЛИЕНТ уведомлен и согласен, что ключи ЭП различных сотрудников КЛИЕНТА, имеющих право подписи платежных документов должны создаваться и храниться на отдельных Аппаратных средствах усиленной ЭП.

Приложение № 2
к Условиям дистанционного обслуживания
клиентов с использованием Системы «iBank 2»

ТРЕБОВАНИЯ
по обеспечению безопасности при работе с Системой «iBank2».

Настоящие Требования разработаны в целях:

- Предотвращения хищения денежных средств, находящихся на банковских счетах Клиента при осуществлении расчётов с использованием Системы «iBank 2» (далее – «iBank 2»).

- Минимизации рисков проведения злоумышленниками несанкционированных платежей и других вредоносных действий с использованием Системы «iBank 2».

1. В целях обеспечения безопасности электронного устройства, на котором производится работа с Системой «iBank 2»:

- Используйте для работы в Системе «iBank 2» специально выделенное для этих целей исправное электронное устройство (компьютер/ноутбук/планшет/смартфон, далее по тексту - ЭУ);
- Исключите возможность несанкционированного доступа к ЭУ;
- На ЭУ должна быть установлена только одна операционная система;
- На ЭУ должна быть установлена парольная защита для входа в BIOS и в операционную систему. Пароли должны иметь высокий уровень сложности и меняться не реже одного раза в месяц;
- На ЭУ не должны устанавливаться средства разработки и откладки программного обеспечения;
- Крайне желательно опечатывать корпус и неиспользуемые разъёмы ЭУ с целью исключения несанкционированного подключения и установки аппаратных закладок;
- Применяйте на ЭУ только лицензионное системное, прикладное и антивирусное программное обеспечение (далее - ПО);
- Своевременно устанавливайте на ЭУ необходимые обновления системы безопасности, обновления системного, прикладного и антивирусного ПО, обновления модулей и баз антивирусного ПО;
- Еженедельно осуществляйте полную проверку ЭУ на наличие/отсутствие вредоносного кода (вирусов);
- Применяйте на ЭУ специализированные программные средства безопасности – персональные межсетевые экраны (firewall), а также средние или высокие параметры безопасности и конфиденциальности установленного на ЭУ Интернет – браузера;
- Во время работы в сети Интернет никогда не соглашайтесь на установку каких-либо дополнительных программ или компонентов, если неизвестно для чего это нужно;
- При работе с электронной почтой не открывайте письма и вложенные в них файлы, полученные от неизвестных отправителей, не переходите по содержащимся в таких письмах ссылкам;
- Исключите посещение Интернет-сайтов, за исключением сайтов банков и сайтов обновлений систем безопасности разработчиков системного, прикладного и антивирусного ПО с данного ЭУ;
- Отключайте устройства беспроводного доступа (Wi-Fi и Bluetooth), когда в них нет необходимости.

2. В целях исключения доступа посторонних лиц к ЭУ, на котором производится работа с системой «iBank 2»:

- Назначьте ответственное лицо, имеющее право использовать Систему «iBank 2»;
- Определите порядок доступа и порядок работы на данном ЭУ, исключающий доступ к данному ЭУ неуполномоченных лиц;
- Исключите обслуживание данного ЭУ нештатными специалистам.

3. В целях исключения возможности удалённого подключения к ЭУ:

- На ЭУ, предназначенном для работы в Системе «iBank 2», не должно быть установлено программ он-лайн общения (ICQ, Skype и т.п.), программ удалённого администрирования и программ удаленного доступа к данному ЭУ;
- При обычной работе на ЭУ входите в Систему «iBank 2» под учётной записью с правами ограниченного доступа (как обычный пользователь), не имеющего неограниченные права администратора системы;
- Учётная запись «Гость», в операционной системе ЭУ, должна быть выключена.

4. В целях защиты ключа электронной подписи от хищения и копирования:

- Храните USB-токен/файловое хранилище на котором содержится ключ электронной подписи в надёжном месте;
- Подключайте USB-токен/файловое хранилище и к компьютеру только на время работы с Системой «iBank 2». Отключайте и извлекайте USB-токены в то время, когда они не используются для работы с Системой «iBank 2»;

- Определите порядок доступа и места хранения USB-токенов, исключающие их несанкционированное использование неуполномоченными работниками и третьими лицами;
- Никогда не передавайте USB-токены/файловые хранилища каким-либо специалистам для проверки работы Системы «iBank 2», проверки настроек взаимодействия с Банком и т.п. При необходимости таких проверок только ответственный за работу с Системой «iBank 2» должен подключить USB-токен к ЭУ и лично ввести пароль доступа, исключая его подсматривание;
- При увольнении работника, ответственного за USB-токен/файловое хранилище, при переводе такого работника на другую должность и в других случаях, когда работник прекращает работать с USB-токеном/файловым хранилищем, незамедлительно обратитесь в Банк с просьбой временной блокировки данной учётной записи в Системе «iBank 2», сгенерируйте новые ключи электронной подписи и зарегистрируйте их в БАНКЕ.

5. В целях сохранности пароля доступа к ключу электронной подписи:

- Запомните пароль к ключу электронной подписи, который находится на USB-токене/файловом хранилище;
- Никогда не записывайте его в местах, доступных посторонним лицам;
- Периодически (желательно – 1 раз в месяц) меняйте пароль доступа к ключу электронной подписи;
- Никому и никогда не сообщайте сведения о пароле, включая работников Банка. Банк никогда не запрашивает данную информацию.

6. При работе с Системой «iBank 2» и СМС-подтверждениями платежей:

- Ограничьте доступ к телефону на номер которого приходят СМС с ключами подтверждения платежей и ключами доступа к Системе «iBank 2»;
- Перед вводом СМС ключа для подтверждения платежа, убедитесь, что информация, полученная в СМС, соответствует фактическим реквизитам платежа.

7. Будьте осторожны и внимательны при работе в Системе «iBank 2»:

- Внимание! Если возникло подозрение, что компьютер заражён (неадекватная реакция на действия пользователя, непонятные окна и сообщения, получение незапрашиваемых СМС с ключом для входа или для проведения операции и т.п.) - немедленно прекратите работу в Системе «iBank 2», извлеките USB-токен/файловое хранилище и обратитесь к ИТ-специалисту для выяснения причин происходящего.
- Не пользуйтесь Системой «iBank 2» до выяснения причин происходящего.
- Не пользуйтесь Системой «iBank 2» через публичные компьютерные сети (интернет-кафе, компьютерные салоны, и любые другие общественные места);
- Особое внимание следует обратить на недопустимость использования Системы «iBank 2» через публичные Wi-Fi сети;
- Не работайте с Системой «iBank 2», используя чужие ЭУ;
- Прежде чем ввести пароль в Системе «iBank 2», убедитесь, что соединение установлено именно с сервером БАНКА - в адресной строке должен отображаться адрес **https://ibank.russitabank.ru/**. Злоумышленники часто используют похожие сайты, например, https://ibank.rositabank.ru/;
- Если при подключении к Системе «iBank 2» появляется предупреждение Интернет-браузера о перенаправлении на другой сайт, немедленно прекратите все операции и обратитесь в службу технической поддержки БАНКА по телефону +7 (495) 933-46-00;
- Обращайте особое внимание на любые изменения в привычных процессах установления соединения с Системой «iBank 2». При возникновении любых сомнений в правильном функционировании Системы «iBank 2», немедленно обращайтесь по телефону +7 (495) 933-46-00 в службу технической поддержки БАНКА;
- Регулярно контролируйте состояние своих счетов в Системе «iBank 2» и незамедлительно сообщайте работникам Банка по телефону +7 (495) 933-46-00 обо всех подозрительных или несанкционированных финансовых операциях;
- При возникновении любых подозрений на компрометацию ключа электронной подписи или на наличие в ЭУ вредоносных программ – незамедлительно заблокируйте Вашу учетную запись в Системе «iBank 2», сгенерируйте новые ключи электронной подписи и зарегистрируйте их в БАНКЕ;
- В случае обнаружения на ЭУ посторонних, незнакомых и необычных программ, нарушения целостности программного обеспечения либо выявления факта повреждения печатей на системных блоках все работы на данном ЭУ должны быть прекращены;
- В случае сбоев в работе ЭУ, его поломки во время работы с Системой «iBank 2», или сразу после сеанса работы (проблемы с загрузкой операционной системы, выход из строя жесткого диска, и т.п.), немедленно обратитесь в Банк по телефону +7 (495) 933-46-00 и убедитесь, что от имени вашей организации не производились несанкционированные переводы денежных средств;
- В случае утери, хищения или повреждения USB-токена/файлового хранилища немедленно свяжитесь с БАНКОМ.

8. Пользователю системы «iBank 2» запрещается:

- обрабатывать предоставленными Банком ключами электронной подписи информацию, содержащую государственную тайну;
- после ввода ключевой информации либо иной конфиденциальной информации оставлять без контроля ЭУ, на которых ведётся работа с системой «iBank 2»;
- разглашать содержимое USB-токенов или передавать USB-токены/файловые хранилища лицам, к ним не допущенным, выводить ключевую информацию на дисплей, принтер и иные средства отображения информации (за исключением случаев, предусмотренных соответствующими соглашениями между Банком и Клиентом);
- использовать USB-токены/файловые хранилища в режимах, не соответствующих соглашениям между Банком и Клиентом;
- записывать на ключевые носители постороннюю информацию;
- производить дублирование ключевых носителей.

9. Общие рекомендации по использованию и хранению USB-токенов:

- Необходимо оберегать USB-токены от сильных механических воздействий (падения с высоты, сотрясения, вибрации, удары);
- USB-токены необходимо оберегать от воздействия высоких и низких температур;
- При резкой смене температур (вносе охлажденного устройства с мороза в теплое помещение) не рекомендуется использовать USB-токен в течение 3 часов во избежание повреждений из-за сконденсированной на электронной схеме влаги;
- Необходимо оберегать USB-токены от попадания на них прямых солнечных лучей;
- Необходимо оберегать USB-токены от воздействия влаги и агрессивных сред;
- Недопустимо воздействие на USB-токены сильных магнитных, электрических или радиационных полей, высокого напряжения и статического электричества;
- При подключении USB-токена к компьютеру не прилагайте излишних усилий;
- USB-токен в нерабочее время необходимо всегда держать закрытым во избежание попадания на разъем USB-токена пыли, грязи и влаги;
- При засорении разъема токена нужно принять меры для его очистки. Для очистки корпуса и разъема используйте сухую ткань. Использование воды, растворителей и прочих жидкостей недопустимо;
- Не разбирайте USB-токены;
- Необходимо избегать скачков напряжения питания ЭУ ;
- Не извлекайте USB-токен из USB-порта во время записи и считывания;
- В случае неисправности или неправильного функционирования USB-токенов обращайтесь в Банк.

10. Важно! Обратите внимание!

- МКИБ "РОССИТА-БАНК" ООО не имеет доступа к секретным ключам клиентов;
- У МКИБ "РОССИТА-БАНК" ООО отсутствует возможность подписания документов электронной подписью от имени какого-либо клиента;
- В МКИБ "РОССИТА-БАНК" ООО хранятся только сертификаты открытого ключа электронной подписи клиентов, сформированные и переданные клиентами в Банк при подключении к системе «iBank 2». Данные сертификаты пригодны только для проверки электронной подписи платежных документов, полученных от клиентов;
- МКИБ "РОССИТА-БАНК" ООО никогда не запрашивает у клиентов конфиденциальную информацию, информацию о паролях и ключах;
- МКИБ "РОССИТА-БАНК" ООО не несёт ответственности за сохранность ключевой информации клиентов (она хранится только у клиентов и только клиент является её единственным владельцем), а также за возможный ущерб, который может понести клиент в случае исполнения МКИБ "РОССИТА-БАНК" ООО платёжных документов, инициированных неуполномоченными лицами, но подписанных действительной электронной подписью клиента.

Приложение № 3
к Условиям дистанционного обслуживания
клиентов по Системе «iBank 2»

ТРЕБОВАНИЯ
по защите от Вредоносного кода рабочего места Системы «iBank 2»

1. К средствам защиты от Вредоносного кода относятся средства, используемые для:
   - выявления и обезвреживания Вредоносного кода (антивирусы);
   - межсетевого экранирования Рабочего места или корпоративной сети;
   - Web-фильтрации;
   - обнаружения и предотвращения вторжений;
   - контроля выполнения приложений.
2. Для обеспечения надлежащей защиты от вредоносного кода КЛИЕНТ обязан:
   - обеспечить непрерывное использование средств защиты от Вредоносного кода;
   - обеспечить периодический контроль целостности системного, прикладного и специального программного обеспечения;
   - ежедневно осуществлять проверку Рабочего места на наличие Вредоносного кода;
   - обеспечить регулярное обновление средств защиты от Вредоносного кода, обновление прикладного программного обеспечения, установку пакетов обновления безопасности операционной системы;
   - использовать лицензионное программное обеспечение или программное обеспечение, полученное исключительно из доверенных источников;
   - использовать для работы в Системе учетную запись, не входящую в группу «Локальные администраторы» или аналогичную группу пользователей;
   - осуществлять вход в сеть Интернет с Рабочего места исключительно для подключения к сайту БАНКА или обновления антивирусной программы, прикладного или системного программного обеспечения.
   - предварительно на выделенном компьютере проверять съемные носители информации на наличие Вредоносного кода перед использованием на Рабочем месте.

Приложение № 4

к Условиям дистанционного обслуживания
клиентов по Системе «iBank 2»

Порядок регистрации Клиента в Системе «iBank 2»

Регистрация в офисе клиента

Предварительная регистрация производится после подписания Заявления о присоединении к Условиям дистанционного обслуживания клиентов по Системе «iBank 2» и получения usb-токена.

1. Зайдите на страницу https:// ibank.russitabank.ru;
2. Нажмите на кнопку «Регистрация»;
3. Пройдите процедуру регистрации нового клиента.

Обратите внимание:

- Процедура регистрации подробно описана в Руководстве пользователя. Руководство пользователя находится на компакт-диске, переданном при заключении договора. Также, Руководство доступно по ссылке «Документация» на главной странице Системы «iBank 2» - https://ibank.russitabank.ru.
- В начале регистрации браузер может потребовать разрешение на установку программного обеспечения (расширение, плагин) BIFIT Signer. Необходимо согласиться. Могут потребоваться права администратора.
- Во время предварительной регистрации в Системе «iBank 2» usb-токен или файловое хранилище («флешка») должны быть подключены к компьютеру.
- Если для хранения ключей используется файловое хранилище, необходимо ознакомиться с разделом Руководства «Использование СКЗИ «Крипто-КОМ».

После завершения процедуры регистрации необходимо распечатать сертификат ключа проверки ЭП в **трёх** экземплярах.

- Один экземпляр сертификата не заполняется. Он используется в качестве контрольного и остаётся у Клиента;
- Два других экземпляра необходимо заполнить, проставить подписи и печати в соответствующих местах.

На этом процесс предварительной регистрации клиента считается завершённым. Для окончательной регистрации необходимо лично явиться в офис Банка

Внимание!
Информация о зарегистрированном Клиенте сохраняется в системе в течение 30 дней. Если к моменту окончания этого срока Клиент не прошёл окончательную регистрацию в офисе Банка, то информация о Клиенте удаляется из системы.

Регистрация клиента в офисе банка

Для окончательной регистрации Клиенту необходимо лично явиться в офис Банка, имея при себе:

- два распечатанных и заполненных экземпляра сертификата ключа проверки ЭП клиента, заверенных подписями и печатью организации;
- документ об удостоверении личности;
- другие документы, требуемые банком при заключении договора с клиентом.

Внимание!
Сертификат ключа проверки электронной подписи должен предоставлять именно тот сотрудник Клиента, который зарегистрирован как владелец ключа.

Сотрудники Банка выполнят проверку сертификата на правильность заполнения, сверят ключ проверки ЭП. В случае корректности сертификата ключ электронной подписи будет активирован.

После активации сертификат заверяется печатью Банка. Один экземпляр остается в Банке, второй возвращается Клиенту.

После завершения процедуры регистрации в офисе Банка Клиент может полноценно работать в Системе «iBank 2».

Приложение № 5
к Условиям дистанционного обслуживания
клиентов с использованием Системы «iBank 2»

Заявление о подключении Услуги по дистанционному обслуживанию с использованием системы «iBank 2»	№					/		

☐ первоначальное ☐ корректирующее ☐ повторное

1. Полное наименование клиента (далее – Клиент) _____

_____

ИНН															
ОГРН															

Клиент в лице _____,

действующего(-щей) на основании _____,

заявляет о своем присоединении к Условиям дистанционного обслуживания клиентов по Системе «iBank 2» (далее – «Условия») в соответствии со ст. 428 ГК РФ.

Клиент подтверждает, что ознакомился с Условиями (включая все приложения), выражает своё согласие с ними и обязуется выполнять.
Клиент подтверждает, что ознакомился с Тарифами Банка.

2. Прошу подключить Услугу по дистанционному обслуживанию с использованием Системы «iBank 2» (далее – «Услуга») по всем счетам в рублях РФ и/или иностранной валюте, открытым в МКИБ «РОССИТА-БАНК» ООО.

3. Прошу использовать следующий номер телефона для информирования о совершении операций.

Номер мобильного телефона:	+	7										

4. Прошу предоставить доступ к Системе «iBank 2» следующим сотрудникам Клиента. Подтверждаю их полномочия, корректность номеров телефонов[3] и ознакомление с Требованиями по безопасности использования Системы «iBank 2» (Приложение № 2 к Условиям)

Фамилия, имя, отчество сотрудника	Номер мобильного телефона												Без права подписи[1]	Мобильный банк[2]
_____	+	7											☐	☐
_____	+	7											☐	☐
_____	+	7											☐	☐
_____	+	7											☐	☐

[1] *Владелец ЭП без права подписи может осуществлять вход в Систему «iBank 2», получать доступ к информации, отображаемой в Системе «iBank 2», создавать в Системе «iBank 2» платёжные ЭД и (или) неплатёжные ЭД, но не может их подписывать и направлять в Банк.*
[2] *Отметьте для подключения сервиса Мобильный банк. Описание сервиса и процедура подключения приведены в Приложении № 13.*
[3] *Мобильный телефон используется КЛИЕНТОМ для получения одноразовых паролей и для Мобильного банка.*

5. Настоящим Клиент подтверждает, что для отправки в Банк электронных платёжных документов (в том числе платёжных поручений) требуются электронно-цифровые подписи в количестве (указать):	_____ (цифрой)	_____ (прописью)

6. Клиент соглашается с тем, что электронный платёжный документ не будет доставлен в Банк в случае несоответствия фактического числа подписей под документом количеству, установленному настоящим Заявлением.
Клиент соглашается с тем, что конкретное сочетание подписей под электронным документом определяется Приложением № 5 к Договору РКО (при его наличии).

7. Клиент соглашается с тем, что для подписания неплатёжных электронных документов (см. Приложение № 10) достаточно любой одной электронно-цифровой подписи с правом подписи.

8. Клиент соглашается с тем, что платёжные поручения на сумму, превышающую 100000 (сто тысяч) рублей, требуют подтверждения одноразовым паролем. Пароль автоматически высылается по SMS после подписания платёжного поручения.

_____ (Подпись Клиента)

_____ (Подпись сотрудника Банка)

9. Прошу при каждом входе в Систему «iBank 2» запрашивать дополнительное подтверждение. Дополнительное подтверждение производится одноразовым паролем, направляемым по SMS. Вход в систему будет возможен только после ввода одноразового пароля.	
☐ **ДА**	☐ **НЕТ**

11. Прошу ☐ подключить услугу IP-фильтрации для следующих IP-адресов:

№ п/п	IP-адрес (Может быть указан либо IP-адрес(-а), либо маска IP-адреса(-ов), с которого(-ых) будет осуществляться соединение по Системе «iBank 2»)				Маска IP-адреса
1					
2					
3					
4					

При попытке входа в систему с компьютера, IP-адрес которого отличается от указанного в заявлении, система проинформирует о невозможности соединения с Банком, даже если при попытке входа будет использован зарегистрированный ключ.

Использование IP-фильтрации не позволит работать с «iBank 2» через любое подключение к интернету, но исключит использование злоумышленником похищенного секретного ключа электронной подписи клиента.

12. ☐ Настоящим отказываюсь от осуществления IP-фильтрации. Возможные риски, связанные с таким отказом, мне разъяснены

_____ (должность)	_____ (фамилия, имя, отчество)	_____ (подпись)

13. Прошу использовать следующее кодовое слово для экстренной блокировки операций по счетам Клиента с использованием Системы «iBank 2». Блокировка производится путём обращения по телефону Банка. Кодовое слово предназначено только для указанной блокировки и не позволяет запрашивать какую-либо информацию или услуги.

Кодовое слово:															

14. С Требованиями по защите от Вредоносного кода рабочего места Системы «iBank 2» (Приложение № 3 к Условиям) и с Требованиями по обеспечению безопасности при работе с Системой «iBank2» (Приложение № 2 к Условиям) ознакомлен и обязуюсь выполнять

_____ (должность)	_____ (фамилия, имя, отчество)	_____ (подпись)

17. Подпись Клиента (представителя)

_____ (должность)	_____ (фамилия, имя, отчество)	_____ (подпись)
		М. П.

18. Отметки УФМ Банка

Настоящее Заявление принято Банком «_____» _____ 201___ года в г. Москве.

_____ (должность)	_____ (фамилия, имя, отчество)	_____ (подпись)
Примечания _____ _____		**М. П.**

19. Отметки УИТ Банка

Информация внесена в Систему «iBank 2» в ___:___ «_____» _____ 201___ года.

_____ (должность)	_____ (фамилия, имя, отчество)	_____ (подпись)

Приложение № 6
к Условиям дистанционного обслуживания
клиентов с использованием системы «iBank 2»

АКТ № _____
передачи аппаратных средств усиленной электронной подписи и сопроводительной документации

г. Москва «_____» _____ 201__ г.

МКИБ «РОССИТА-БАНК» ООО, именуемый в дальнейшем «**Банк**», в лице _____, действующего(-ей) на основании _____, с одной стороны, и _____, именуемое в дальнейшем «**Клиент**», в лице _____действующего(-ей) на основании _____, с другой стороны, совместно именуемые – «Стороны», а по отдельности – «Сторона», принимая во внимание Условия дистанционного обслуживания клиентов с использованием Системы «iBank 2» и Заявление КЛИЕНТА о присоединении № _____ от «_____» _____ 201__ г., составили настоящий Акт о нижеследующем:

Банком надлежащим образом передан(ы), а **Клиентом** получен(ы) средство(а) усиленной электронной подписи:

USB-токен «MS_KEY K» – «АНГАРА» в количестве ____ (_____) шт.

Идентификационный номер(-а)_____.

Гарантийный срок эксплуатации Аппаратных средств усиленной ЭП «MS_KEY K» – «АНГАРА» составляет шесть месяцев со дня предоставления Банком Клиенту.

Банком надлежаще передан, а **Клиентом** получен компакт-диск № _____ со следующими программными средствами и документацией:

- Документация по Системе «iBank 2»;
- Документация к СКЗИ «MS_KEY K» – «АНГАРА»;

☐ С правилами пользования Средством криптографической защиты информации «MS_KEY K» – «АНГАРА» ознакомлен и согласен выполнять.

.

_____ (_____)
(подпись) (Ф.И.О.)

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

Банк

_____ (_____)
(подпись) (Ф.И.О.)

М.П.

Клиент

_____(_____)
(подпись) (Ф.И.О.)

М. П.

Отметка о возврате USB-токенов в количестве в количестве ____ (_____) шт.
Идентификационный номер(-а)_____.

Банк принял

_____(_____)
(подпись) (Ф.И.О.)

М. П.

Клиент передал

_____(_____)
(подпись) (Ф.И.О.)

М. П.

Приложение № 7
к Условиям дистанционного обслуживания
с использованием Системы «iBank2»

УВЕДОМЛЕНИЕ
о прекращении действия средства подтверждения в связи с утратой средства подтверждения / использованием ЭСП без согласия Клиента

Наименование Клиента:	
ИНН:	

«Клиент», в лице _____, действующего на основании _____, настоящим уведомляет Банк о:

☐ об утрате/компрометации средства подтверждения

☐ об использовании ЭСП без согласия Клиента подтверждения

☐ иные обстоятельства: _____
(указать обстоятельства)
_____
_____
_____

Прошу с ___ : ___ «___» _____ 20__ г. заблокировать указанные ниже средства подтверждения, использовавшиеся в рамках Условий дистанционного обслуживания клиентов по Системе «iBank2» согласно Заявлению о подключении Услуги по дистанционному обслуживанию с использованием системы «iBank2» № _____ от " _____ " _____ 201_ г., и остановить обработку ЭД, подписанных/подтвержденных указанными средствами:

Ф.И.О. владельца	USB-токен №	Идентификатор ключа проверки ЭП	Номер мобильного телефона, используемого для подтверждения платежей

До момента постановки отметки об исполнении на письменном уведомлении Банк не несет ответственности за возможные убытки, возникшие у Клиента в результате незаконного использования Ключей ЭП и (или) Средства подтверждения.

_____ _____ (_____)
(должность руководителя) (подпись) (Ф.И.О.)

«_____» _____ 20__ г.

М.П.

Отметка Банка:

Уведомление принято к исполнению в Банке " _____ " _____ 201_ г.

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

М.П.

Уведомление исполнено УИТ " _____ " _____ 201___ г. в ___ : ____

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

М.П.

Приложение № 8
к Условиям дистанционного обслуживания
с использованием Системы «iBank 2»

УВЕДОМЛЕНИЕ
о приостановлении использования Услуги по дистанционному обслуживанию с использованием системы «iBank 2»

Наименование Клиента:	
ИНН:	

«Клиент», в лице _____, действующего на основании _____, уведомляет Банк о приостановлении использования Услуги по дистанционному обслуживанию с использованием системы «iBank 2» использовавшихся в рамках Условий дистанционного обслуживания клиентов по Системе «iBank 2» согласно заявлению о присоединении № _____ от " _____ " _____ 201_ г.

Прошу с __:__ " _____ " _____ 201_ г. по " _____ " _____ 201_ г. заблокировать все ключи ЭП и Средства подтверждения и прекратить обработку электронных документов, подписанных/подтвержденных указанными средствами.

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

«_____» _____ 20__ г.

М.П.

Отметка Банка:

Уведомление принято к исполнению в Банке " _____ " _____ 201_ г.

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

М.П.

Уведомление исполнено УИТ " _____ " _____ 201___ г. в ___ : ____

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

М.П.

Приложение № 9
к Условиям дистанционного обслуживания
клиентов с использованием Системы «iBank 2»

ПОЛОЖЕНИЕ
о процедуре разбора конфликтной ситуации в рамках дистанционного обслуживания с использованием Системы «iBank 2»

Настоящее положение о процедуре разбора конфликтной ситуации в рамках дистанционного обслуживания с использованием Системы «iBank 2» (далее — Положение) в соответствии с ГК РФ, ФЗ «О национальной платежной системе» и ФЗ «Об электронной подписи», является порядком досудебного урегулирования споров между БАНКОМ и КЛИЕНТОМ возникающих из Условий дистанционного обслуживания с использованием Системы «iBank 2» в рамках Договора РКО.

Раздел 1. Термины, применяемые в Положении

1.1. В рамках настоящего Положения используются понятия Электронное средство платежа (далее – ЭСП), Перевод денежных средств в соответствии с Федеральным Законом от 27 июня 2011 года № 161-ФЗ «О национальной платежной системе».

1.2. В рамках настоящего Положения используются понятия Электронная подпись (далее – ЭП), Ключ электронной подписи (далее – Ключ ЭП), Ключ проверки электронной подписи (далее – Ключ проверки ЭП), Электронный документ (далее – ЭД) в соответствии с Федеральным Законом от 6 апреля 2011 года № 63-ФЗ «Об электронной подписи».

1.3. В рамках настоящего Положения используются понятия Сертификат ключа проверки электронной подписи (далее – Сертификат), Система «iBank 2», Пара ключей электронной подписи (далее – Пара ключей ЭП) в соответствии с Условиями дистанционного обслуживания с использованием Системы «iBank 2»Термины, применяемые в рамках настоящего Положения, используются в следующих значениях:

- Конфликтная ситуация – спор между КЛИЕНТОМ и БАНКОМ по причине перевода денежных средств, в рамках которого КЛИЕНТОМ оспаривается подлинность электронной подписи в электронном документе и (или) факт уведомления о совершении операции, возникшие в результате воздействия Вредоносного кода или по иным причинам.
- Разрешительная комиссия – орган, формируемый в соответствии с настоящим Положением с целью разбора Конфликтной ситуации по существу и документального оформления результатов работы.

Раздел 2. Состав Разрешительной комиссии

2.1. В обязательном порядке в состав Комиссии включаются представители КЛИЕНТА и представители БАНКА.

2.2. По требованию КЛИЕНТА и (или) БАНКА к работе Разрешительной комиссии может быть привлечен эксперт.

2.3. Эксперт может участвовать в работе Разрешительной комиссии непосредственно (лично). При этом эксперт включается в состав Разрешительной комиссии.

2.4. При невозможности непосредственного (личного) участия эксперта в работе Разрешительной комиссии, эксперт на основании полученных от БАНКА материалов проводит экспертизу подлинности ЭП или анализ архивов на предмет подтверждения факта уведомления КЛИЕНТА. При этом эксперт не включается в состав Разрешительной комиссии.

2.5. Требования к эксперту определены в Разделе 8 настоящего Положения.

2.6. В качестве эксперта к работе Разрешительной комиссии может быть привлечен представитель разработчика Системы «iBank 2».

Раздел 3. Порядок формирования Разрешительной комиссии

3.1. При возникновении Конфликтной ситуации, КЛИЕНТ направляет в БАНК заявление в письменном виде в свободной форме, которое должно содержать:

- дата и номер заявления;
- дата и номер заявления о подключении Услуги дистанционного обслуживания с использованием Системы «iBank 2;
- реквизиты КЛИЕНТА (ИНН, адрес места нахождения, номер банковского(-их) счета(-ов));
- суть претензии с подробным изложением обстоятельств, на которых основана претензия, и сведений о подтверждающих ее доказательствах;
- обоснованный расчет заявленных в претензии требований;
- нормы законодательных и иных нормативных правовых актов, на которых основывается претензия;
- перечень прилагаемых к заявлению документов, составляющих доказательную базу (при наличии);

- список лиц, выступающих от лица КЛИЕНТА в качестве членов Разрешительной комиссии.
- требование о привлечении к работе Разрешительной комиссии эксперта (при необходимости).

3.2. В случае привлечения по требованию КЛИЕНТА к работе Разрешительной комиссии эксперта, БАНК не позднее 2 (Двух) рабочих дней высылает в экспертную организацию запрос, содержащий:

- требования к экспертной организации;
- требования к эксперту;
- вопросы, поставленные перед экспертом;
- требуемый срок проведения экспертизы.

3.3. Экспертная организация в разумный срок ответ БАНКУ. В случае получения в указанный срок ответа от экспертной организации о соответствии предъявленным требованиям и возможности проведения экспертизы в указанный срок, БАНК привлекает к работе Разрешительной комиссии указанного эксперта.

3.4. В случае неполучения от экспертной организации положительного ответа в указанный срок, БАНК привлекает к работе Разрешительной комиссии представителя разработчика Системы «iBank 2».

БАНК в течение 5 (Пяти) рабочих дней с момента получения заявления КЛИЕНТА:

- определяет дату, время и место работы Разрешительной комиссии;
- формирует состав Разрешительной комиссии с учетом требований КЛИЕНТА;
- информирует КЛИЕНТА о назначенной дате, времени, месте работы Разрешительной комиссии и о ее составе.

3.5. Заседание Разрешительной комиссии должно быть организовано БАНКОМ не позднее 10 (Десяти) рабочих дней с момента получения заявления КЛИЕНТА. В случае привлечения к работе Разрешительной комиссии эксперта, срок организации заседания Разрешительной комиссии продлевается на срок, необходимый эксперту для проведения экспертизы подлинности ЭП или анализа архивов на предмет подтверждения факта уведомления КЛИЕНТА.

3.6. В случае если КЛИЕНТ не направит своих представителей для участия в работе Разрешительной комиссии, разбор Конфликтной ситуации осуществляется без представителей КЛИЕНТА.

3.7. Срок предоставления КЛИЕНТУ результатов рассмотрения его заявления в общем случае – не более 30 дней, при использовании ЭСП для трансграничного перевода денежных средств – не более 60 дней. В случае препятствования КЛИЕНТОМ работе Разрешительной комиссии, указанный срок может быть увеличен.

Раздел 4. Разбор Конфликтной ситуации, в рамках которой оспаривается подлинность электронной подписи

4.1. При возможности доступа в ходе работы Разрешительной комиссии к базе данных системы «iBank 2», описанные ниже действия осуществляются с использованием штатного программного обеспечения Системы «iBank 2» АРМ «Операционист» и/или АРМ «Администратор».

4.2. При невозможности доступа в ходе работы Разрешительной комиссии к базе данных системы «iBank 2», описанные ниже действия осуществляются с использованием материалов, предварительно полученных (распечатанных, выгруженных) БАНКОМ из базы данных Системы «iBank 2».

Этап 1:

1. БАНК предъявляет на обозрение Разрешительной комиссии выписку по счету КЛИЕНТА.
2. КЛИЕНТ с помощью выписки по счету определяет оспариваемый перевод денежных средств.
3. БАНК предъявляет ЭД, на основании которого совершен оспариваемый перевод денежных средств.
4. Разрешительная комиссия делает запись о факте предъявления/не предъявления БАНКОМ ЭД, при этом:

- В случае если БАНК предъявляет ЭД, Конфликтная ситуация рассматривается далее по существу. Разрешительная комиссия переходит к Этапу 2 настоящего Раздела.
- В случае если БАНК не предъявляет ЭД, Конфликтная ситуация далее по существу не рассматривается. Разрешительная комиссия переходит к Разделу 6 настоящего Положения.

Этап 2:

5. Разрешительная комиссия определяет Ключ ЭП, посредством которого был подписан ЭД.
6. БАНК предъявляет на обозрение Разрешительной комиссии Сертификат, соответствующий вышеуказанному Ключу ЭП КЛИЕНТА.
7. Разрешительная комиссия делает запись о факте предъявления/не предъявления БАНКОМ Сертификата, при этом:

- В случае если БАНК предъявляет Сертификат, Конфликтная ситуация рассматривается далее по существу. Разрешительная комиссия переходит к Этапу 3 настоящего Раздела.
- В случае если БАНК не предъявляет Сертификат Конфликтная ситуация далее по существу не рассматривается. Разрешительная комиссия переходит к Разделу 6 настоящего Положения.

Этап 3:

8. Разрешительная комиссия просматривает ключ проверки ЭП, использующийся при проверке ЭП в ЭД, на основании которого совершен оспариваемый перевод денежных средств.
9. Разрешительная комиссия производит сверку шестнадцатеричного представления Ключа проверки ЭП, содержащегося в Сертификате, с шестнадцатеричным представлением Ключа проверки ЭП, использующегося при проверке ЭП.
10. Разрешительная комиссия делает запись о факте наличия/отсутствия расхождения между шестнадцатеричным представлением Ключа проверки ЭП в Сертификате, и шестнадцатеричным представлением Ключа проверки ЭП, использующегося при проверке ЭП, при этом:

- В случае если между шестнадцатеричными представлениями Ключей проверки ЭП расхождение не обнаружится, Конфликтная ситуация рассматривается далее по существу. Разрешительная комиссия переходит к Этапу 4 настоящего Раздела.
- В случае если обнаружится расхождение между шестнадцатеричными представлениями Ключей проверки ЭП, Конфликтная ситуация далее по существу не рассматривается. Разрешительная комиссия переходит к Разделу 6 настоящего Положения.

Этап 4:

11. КЛИЕНТ предъявляет на обозрение Разрешительной комиссии уведомление о прекращении действия средства подтверждения и (или) об утрате средства подтверждения и (или) об использовании ЭСП без согласия КЛИЕНТА (при наличии).
12. Разрешительная комиссия определяет действительность Сертификата на момент получения БАНКОМ перевода денежных средств:

- Сертификат сверяется с оспариваемым переводом денежных средств. Предметом сверки выступают даты начала и окончания действия Сертификата и дата получения БАНКОМ от КЛИЕНТА распоряжения на осуществление перевода денежных средств. При необходимости может учитываться и время указанных событий.
- Уведомление о прекращении действия средства подтверждения и (или) об утрате средства подтверждения и (или) об использовании ЭСП без согласия КЛИЕНТА (при наличии) сверяется с оспариваемым переводом денежных средств. Предметом сверки выступают дата отметки о принятии (об исполнении) БАНКОМ указанного уведомления и дата получения БАНКОМ от КЛИЕНТА распоряжения на осуществление перевода денежных средств. При необходимости может учитываться и время указанных событий, а также время, необходимое БАНКУ на исполнение указанного уведомления.

13. Разрешительной комиссией делается запись о действительности/недействительности Сертификата на момент получения БАНКОМ от КЛИЕНТА распоряжения на перевод денежных средств, при этом:

- В случае действительности Сертификата на момент получения БАНКОМ от КЛИЕНТА распоряжения на осуществление перевода денежных средств, Конфликтная ситуация рассматривается далее по существу. Разрешительная комиссия переходит к Этапу 5 настоящего Раздела.
- В случае недействительности Сертификата на момент получения БАНКОМ от КЛИЕНТА распоряжения на осуществление перевода денежных средств, Конфликтная ситуация далее по существу не рассматривается. Разрешительная комиссия переходит к Разделу 6 настоящего Положения.

Этап 5:

14. Разрешительная комиссия проводит проверку подлинности ЭП в ЭД.
15. Разрешительной комиссией может использоваться специализированная утилита от разработчика Системы «iBank 2» для автономной проверки подлинности ЭП.
16. Разрешительной комиссией делается запись о подлинности/нарушении подлинности ЭП в ЭД, при этом Разрешительная комиссия переходит к Разделу 6 настоящего Положения.

Раздел 5. Разбор Конфликтной ситуации, в рамках которой оспаривается факт уведомления о переводе денежных средств (о совершенной операции)

Этап 1:

1. БАНК предъявляет на обозрение Разрешительной комиссии выписку по счету КЛИЕНТА.
2. КЛИЕНТ с помощью выписки по счету определяет оспариваемый перевод денежных средств.
3. БАНК предъявляет Разрешительной комиссии архивы уведомлений, переданных в период, включающий дату получения БАНКОМ от КЛИЕНТА распоряжения на осуществление перевода денежных средств. БАНКОМ могут по его усмотрению и в зависимости от технической возможности использоваться архивы уведомлений, хранящиеся в базе данных и журналах Системы «iBank 2», и (или) архивы уведомлений, полученные от оператора связи, предоставляющего услугу по передаче уведомлений.
4. БАНК определяет в архиве уведомление, соответствующее рассматриваемому переводу денежных средств.
5. Комиссия определяет реквизиты, по которым было направлено уведомление. При использовании для информирования КЛИЕНТА изменения поля «Статус» и выписки в Системе по счету КЛИЕНТА, данный пункт не рассматривается.

6. БАНК предъявляет действовавший на момент осуществления перевода и заверенный КЛИЕНТОМ документ, в котором указаны реквизиты для информирования КЛИЕНТА (информация для связи с КЛИЕНТОМ).
7. КЛИЕНТ предъявляет действовавший на момент осуществления перевода документ с отметкой БАНКА, в котором указаны реквизиты для информирования КЛИЕНТА (информация для связи с КЛИЕНТОМ) при наличии такого документа.
8. Разрешительная комиссия делает запись о факте соответствия/не соответствия реквизитов, по которым было отправлено уведомление, реквизитам, указанным КЛИЕНТОМ для осуществления информирования:

- В случае если реквизиты, по которым было совершено информирование КЛИЕНТА, соответствуют реквизитам, указанным КЛИЕНТОМ для осуществления информирования, Конфликтная ситуация рассматривается далее по существу. Разрешительная комиссия переходит к Этапу 2 настоящего Раздела.
- В случае если реквизиты не соответствуют, Конфликтная ситуация далее по существу не рассматривается. Разрешительная комиссия переходит к Разделу 6 настоящего Положения.

Этап 2:

9. Комиссия определяет срок отправки уведомления. При рассмотрении архивов, хранящихся в базе данных Системы «iBank 2», может использоваться АРМ «Операционист».
10. В случае использования для информирования КЛИЕНТА изменения поля «Статус», по истории документа определяется момент присвоения ЭД статуса «На обработке»/«На исполнении».
11. В случае использования для информирования КЛИЕНТА выписки в Системе по счету КЛИЕНТА, по распечатанной проводке определяется момент подписи проводки (информации об операции), который соответствует моменту появления данной информации в выписке по счету КЛИЕНТА.
12. Разрешительная комиссия делает запись о соблюдении/не соблюдении срока отправки уведомления (информирования КЛИЕНТА), при этом Разрешительная комиссия переходит к Разделу 6 настоящего Положения.

Раздел 6. Подведение итогов разбора Конфликтной ситуации

6.1. По результатам работы Разрешительной комиссии составляется акт, в котором содержится краткое изложение выводов комиссии и решение комиссии по рассматриваемому разногласию.

6.2. Помимо изложения выводов и решения Разрешительной комиссии в акте должны содержаться:

- состав Разрешительной комиссии;
- дата и место составления акта;
- дата, время начала и окончания работы Разрешительной комиссии;
- фактические обстоятельства, послужившие основанием возникновения претензии;
- краткий перечень мероприятий, проведенных Разрешительной комиссией;
- реквизиты оспариваемого ЭД;
- вывод о подлинности/нарушении подлинности ЭП в оспариваемом ЭД и его обоснование – в случае оспаривания КЛИЕНТОМ подлинности ЭП;
- вывод об уведомлении/не уведомлении КЛИЕНТА о совершенной операции – в случае оспаривания КЛИЕНТОМ факта уведомления о переводе денежных средств;
- указание на особое мнение члена Разрешительной комиссии (при наличии);
- собственноручные подписи членов Разрешительной комиссии.

6.3. В случае если проводилась экспертиза подлинности ЭП или анализ архивов на предмет подтверждения факта уведомления КЛИЕНТА, к акту прилагается подготовленное экспертом заключение о подлинности ЭП или результат анализа архивов соответственно.

6.4. Акт составляется непосредственно после завершения оценки всех обстоятельств, подлежащих установлению Разрешительной комиссией, в двух экземплярах по экземпляру для КЛИЕНТА и БАНКА и подписывается всеми членами Разрешительной комиссии. В случае включения в состав Разрешительной комиссии эксперта, акт составляется в трех экземплярах.

6.5. Решение Разрешительной комиссии по результатам разбора Конфликтной ситуации, в рамках которой оспаривается подлинность электронной подписи:

6.6. Разрешительная комиссия признает БАНК исполнившим платеж без согласия КЛИЕНТА, и БАНК несет ответственность перед КЛИЕНТОМ в случае, когда имела место хотя бы одна из следующих ситуаций:

- БАНК не предъявляет ЭД, подписанный КЛИЕНТОМ, на основании которого БАНК совершил перевод денежных средств КЛИЕНТА.
- БАНК не предъявляет Сертификат, соответствующий Ключу ЭП КЛИЕНТА, которым был подписан ЭД.
- В случае обнаружения расхождения между шестнадцатеричным представлением Ключа проверки ЭП в Сертификате, и шестнадцатеричным представлением Ключа проверки ЭП, использующегося при проверке ЭП.

- Сертификат был недействительным на момент получения БАНКОМ от КЛИЕНТА распоряжения на осуществление перевода денежных средств.
- Хотя бы одна ЭП КЛИЕНТА в ЭД оказалась не подлинной.

6.7. В иных случаях, за исключением определенных в пункте 5.1 настоящего Раздела, БАНК не несет ответственности перед КЛИЕНТОМ за совершение перевода денежных средств.

6.8. Решение Разрешительной комиссии по результатам разбора Конфликтной ситуации, в рамках которой оспаривается факт уведомления о переводе денежных средств (о совершенной операции):

6.9. Разрешительная комиссия признает БАНК не исполнившим обязанность по информированию КЛИЕНТА о совершенной операции, и БАНК несет ответственность перед КЛИЕНТОМ в случае, когда имела место хотя бы одна из следующих ситуаций:

- БАНК осуществил информирование КЛИЕНТА о платеже (операции) по реквизитам, не соответствующим реквизитам, указанным КЛИЕНТОМ в Заявлении о подключении Услуги по дистанционному обслуживанию с использованием Системы «iBank 2» (Приложение № 5 дистанционному обслуживанию с использованием Системы «iBank 2») для осуществления информирования;
- БАНК осуществил информирование КЛИЕНТА о платеже (операции) в срок, превышающий срок, установленный в Договоре.

6.10. В иных случаях, за исключением определенных в пункте 6.1 настоящего Раздела, БАНК признается Разрешительной комиссией исполнившим обязанность по информированию КЛИЕНТА не несет ответственности перед КЛИЕНТОМ за совершение перевода денежных средств.

6.11. Расходы по формированию и работе Разрешительной комиссии, исключая расходы КЛИЕНТА, связанные с привлечением им в одностороннем порядке независимых экспертов, возлагаются на БАНК. В случае признания Разрешительной комиссией требований КЛИЕНТА необоснованными, КЛИЕНТ обязан в течение 7 рабочих дней с даты составления Акта возместить БАНКУ все указанные расходы. КЛИЕНТ предоставляет БАНКУ право (дает акцепт) при нарушении КЛИЕНТОМ указанного выше условия, БАНК вправе взыскать указанные расходы с любого счета КЛИЕНТА, открытого в БАНКЕ, без его дополнительного распоряжения.

Раздел 7. Проверка подлинности электронной подписи экспертом

7.1. По требованию КЛИЕНТА и (или) БАНКА проведение проверки подлинности ЭП в ЭД может быть поручено экспертной организации.

7.2. При наличии требования о проверке подлинности ЭП в ЭД экспертной организацией БАНК в течение (Пяти) рабочих дней с момента получения заявления КЛИЕНТА или с момента принятия решения о проведении экспертизы по собственной инициативе, направляет эксперту следующие материалы:

- файлы, полученные в результате выгрузки спорного ЭД из базы данных Системы «iBank 2»;
- заверенную копию Сертификата;
- в случае проведения экспертизы по инициативе КЛИЕНТА – копию заявления КЛИЕНТА, указанного в пункте 1 Раздела 2 настоящего Положения.

7.3. По результатам экспертизы подлинности ЭП организация формирует заключение о подлинности ЭП в предоставленном ЭД и высылает его в адрес БАНКА.

7.4. Срок проведения экспертизы подлинности ЭП не должен превышать 10 (Десяти) рабочих дней с момента получения экспертной организацией всех необходимых материалов.

7.5. В случае принятия решения о проведении экспертизы подлинности ЭП в ЭД экспертом, срок организации заседания Разрешительной комиссии увеличивается на срок, необходимый эксперту для проведения экспертизы подлинности ЭП.

Раздел 8. Требования к эксперту, экспертной организации и экспертному заключению

8.1. Экспертная организация должна:

- использовать на законных основаниях для проверки сертифицированные ФСБ РФ ЭП шифровальные (криптографические) средства, реализующие криптографические процедуры проверки ЭП и криптографическую процедуру вычисления хеш-функции по действующим ГОСТам Российской Федерации;
- использовать на законных основаниях для проверки ЭП программное обеспечение, разработанное организацией имеющей лицензию ФСБ РФ на разработку защищенных с использованием шифровальных (криптографических) средств информационных систем, если для проверки ЭП используется Программное обеспечение разработанное сторонней организацией, и (или) иметь лицензию ФСБ России на разработку защищенных с использованием шифровальных (криптографических) средств информационных систем, если для проверки ЭП используется программное обеспечение собственной разработки.

Эксперт должен:

- иметь высшее профессиональное образование в области информационной безопасности или пройти переподготовку по одной из специальностей этого направления в объеме не менее 500 часов;
- иметь стаж работы в области информационной безопасности не менее 5 (Пяти) лет.
- Заключение о проверке подлинности должно:
- быть оформленным в форме экспертного заключения;
- содержать сведения об Экспертной организации: фирменное наименование, место нахождения, ИНН, КПП, ОГРН;
- содержать контактные данные Экспертной организации: телефон, факс, e-mail;
- содержать дату оформления (составления);
- содержать время и дату проведения исследования, адрес места проведения исследования, основание проведения исследования;
- содержать перечень вопросов поставленных на разрешение эксперту;
- содержать перечень объектов исследования представленных эксперту;
- содержать методику исследования;
- содержать результаты исследования;
- содержать выводы эксперта;
- быть заверенным подписью эксперта, подписью единоличного исполнительного органа экспертной организации и печатью экспертной организации.

Приложение № 10
к Условиям дистанционного обслуживания
клиентов с использованием Системы «iBank 2»

ПЕРЕЧЕНЬ
электронных документов передаваемых по Системе «iBank 2»

Наименование Электронного документа	
Платежные документы	
1.	Платежное поручение
2.	Инкассовое поручение
3.	Заявление на аккредитив
4.	Заявление об отказе от акцепта
5.	Заявление на перевод в иностранной валюте
6.	Акцепт
7.	Заявление на покупку/ продажу / конвертацию иностранной валюты
8.	Распоряжение о перечислении средств с транзитного валютного счета
9.	Заявление на выдачу наличных денежных средств
10.	Иные документы
Неплатежные документы	
1.	Справка о валютных операциях
2.	Справка о подтверждающих документах
3.	Паспорт сделки по контракту
4.	Паспорт сделки по кредитному договору
5.	Заявление на переоформление паспорта сделки
6.	Заявление о закрытии паспорта сделки
7.	Отзыв
8.	Зарплатный реестр
9.	Реестр переданных на инкассо расчетных документов
10.	Отзыв
11.	Письмо
12.	Заявление
13.	Уведомление
14.	Внутренние документы КЛИЕНТА (приказы, протоколы, договора и/или соглашения с контрагентами и иное)
15.	Заявления (письма) о готовящихся изменениях в организации с обязательным последующем предоставлением документов на бумажных носителях
16.	Документы, подтверждающие операции КЛИЕНТА в соответствии с требованиями 115-ФЗ
17.	Подтверждающие документы по валютному контролю
18.	Иные документы

Приложение № 11
к Условиям дистанционного обслуживания
клиентов с использованием Системы «iBank 2»

ПОЛОЖЕНИЕ
о порядке и способах информирования КЛИЕНТА о совершении операций с использованием Системы «iBank2»

Раздел 1. Способы информирования КЛИЕНТА

В целях исполнения требований Федерального закона от 27.06.2011 г. № 161-ФЗ «О национальной платежной системе» БАНК осуществляет информирование КЛИЕНТА о совершении операций посредством направления уведомлений следующими способами:

1. Путем отправки SMS-сообщения на указанный КЛИЕНТОМ в Заявлении по форме Приложения № 5 к Условиям дистанционного обслуживания с использованием Системы «iBank2» номер мобильного телефона, зарегистрированного в РФ. При формировании текста SMS-сообщения может использоваться транслитерация.
   БАНК направляет SMS-сообщение КЛИЕНТУ в момент принятия БАНКОМ по Системе «iBank 2» распоряжения КЛИЕНТА на расходную операцию. Обязанность БАНКА по информированию КЛИЕНТА считается исполненной БАНКОМ при направлении SMS-сообщения о совершении операции на номер мобильного телефона, указанный КЛИЕНТОМ. Уведомление считается полученным КЛИЕНТОМ по истечении одной минуты с момента отправки БАНКОМ SMS-сообщения.
   БАНК не несет ответственности за неполучение КЛИЕНТОМ SMS-сообщений от БАНКА по причинам поломки, отключения телефонного аппарата, смены сим-карт, нахождения вне доступа сети, отсутствия денежных средств на счету телефона, а также в случае, когда SMS-сообщений от БАНКА поступило на мобильный телефон КЛИЕНТА, а КЛИЕНТ по каким-либо причинам его не открыл/не прочитал и т.д., и иных подобных причин.
2. Путем изменения статуса соответствующего электронного документа в Системе «iBank 2». Присвоение электронному документу в Системе «iBank 2» статуса «Доставлен» подтверждает получение БАНКОМ распоряжения КЛИЕНТА. Присвоение электронному документу в Системе «iBank 2» статуса «На обработке»/«На исполнении» подтверждает прием БАНКОМ распоряжения КЛИЕНТА к исполнению. Присвоение электронному документу статуса «Исполнено» подтверждает исполнение БАНКОМ распоряжения КЛИЕНТА. Присвоение электронному документу статуса «Отвергнут» подтверждает аннулирование БАНКОМ распоряжения КЛИЕНТА.
   Обязанность БАНКА по информированию КЛИЕНТА считается исполненной БАНКОМ при изменении статуса электронного документа в Системе «iBank 2». Уведомление считается полученным КЛИЕНТОМ по истечении одной минуты с момента изменении статуса электронного документа в Системе «iBank 2».
3. Путем предоставления выписки по счету в Системе «iBank 2», запрашиваемой КЛИЕНТОМ в Системе «iBank 2». Уведомление считается полученным КЛИЕНТОМ по истечении одного часа с момента появления в выписке информации об операции по счету.
4. БАНК обязан проинформировать КЛИЕНТА о совершении операций с использованием ЭСП незамедлительно, но не позднее, чем через 24 часа после совершения соответствующей операции.
5. Способ информирования, указанный в пункте 1 настоящего Раздела, применяются БАНКОМ для информирования КЛИЕНТА о получении БАНКОМ распоряжения КЛИЕНТА на осуществление перевода денежных средств;
6. Способ информирования, указанный в пункте 2 настоящего Раздела, применяется БАНКОМ для информирования КЛИЕНТА о:
   - получении БАНКОМ распоряжения на осуществление перевода денежных средств при информировании КЛИЕНТА о получении ЭД статуса «Доставлен»;
   - принятии БАНКОМ распоряжения на осуществление перевода денежных средств к исполнению при информировании КЛИЕНТА о получении ЭД статуса «На обработке»/«На исполнении;
   - исполнении БАНКОМ распоряжения на осуществление перевода денежных средств при информировании КЛИЕНТА о получении ЭД статуса «Исполнен»;
   - аннулировании БАНКОМ распоряжения на осуществление перевода денежных средств при информировании КЛИЕНТА о получении ЭД статуса «Отвергнут».
7. Способ информирования, указанный в пункте 3 настоящего Раздела, применяется БАНКОМ для информирования КЛИЕНТА об исполнении БАНКОМ распоряжения КЛИЕНТА на осуществление перевода денежных средств.
8. Получение Уведомления считается подтвержденным КЛИЕНТОМ в случае отсутствия сообщений от КЛИЕНТА о неполучении уведомления в срок не позднее двух часов после совершения операции.

Раздел 2. Порядок информирования КЛИЕНТА

1. При информировании КЛИЕНТА путем отправки SMS-сообщений Стороны руководствуются приведенными ниже положениями.
2. Уведомление в виде SMS-сообщения может включать:
   - наименование БАНКА
   - идентификатор электронного средства платежа
   - вид операции
   - дата операции
   - сумма операции
   - валюта операции
   - дополнительная информация о контрагенте
   - идентификатор устройства при его применении для осуществления операции с использованием электронного средства платежа
   - иная информация.
3. При получении от КЛИЕНТА информации о номере мобильного телефона БАНК отправляет КЛИЕНТУ тестовое SMS-сообщение для проверки правильности указания КЛИЕНТОМ номера мобильного телефона. КЛИЕНТ обязан уведомить БАНК при неполучении указанного сообщения по истечении одного рабочего дня. При отсутствии уведомления КЛИЕНТОМ БАНКА о факте неполучения указанного сообщения по истечении двух рабочих дней после его отправки, указанная КЛИЕНТОМ контактная информация считается достоверной, а услуга информирования оказываемой надлежащим образом.

Раздел 3. Права и обязанности Сторон

1. КЛИЕНТ обязан предоставить БАНКУ достоверную информацию для связи с КЛИЕНТОМ.
2. КЛИЕНТ обязан предоставить в БАНК новое Заявление по форме Приложения № 5 к Условиям дистанционного обслуживания с использованием Системы «iBank 2» на бумажном носителе за подписью руководителя КЛИЕНТА и оттиска печати в случае изменения номера мобильного телефона для получения SMS-сообщения. Все риски, связанные с несвоевременным предоставлением информации об изменении номера мобильного телефона несет КЛИЕНТ. Обязанность БАНКА по информированию КЛИЕНТА считается исполненной надлежащим образом при направлении сообщений на ранее известный номер мобильного телефона, если на дату отправки таких сообщений БАНК не получил вышеуказанного Заявления от КЛИЕНТА с измененным номером мобильного телефона.
3. КЛИЕНТ обязан не реже одного раза в сутки проверять поступающие на номер мобильного телефона SMS-сообщения о совершении операции, проверять информацию о статусе операции («Доставлен», «на обработке/на исполнении», «исполнено», «отвергнуто»), размещаемом БАНКОМ в Системе «iBank 2», получать выписки о совершенных операциях в подразделении БАНКА.
4. КЛИЕНТ обязан самостоятельно обеспечить поддержку функции приема SMS-сообщений на своем мобильном телефоне.
5. КЛИЕНТ обязан самостоятельно и за свой счет поддерживать баланс средств на лицевом счете у оператора мобильной связи, необходимый для обеспечения непрерывности получения SMS-сообщений о совершении операций.
6. КЛИЕНТ обязан самостоятельно обеспечить доступность получения SMS-сообщений у своего оператора мобильной связи при нахождении мобильного телефона в междугороднем или международном роуминге.
7. КЛИЕНТ обязан в рабочее время БАНКА просматривать список ЭД в системе «iBank 2» не реже, чем один раз в час. Просмотр рекомендуется осуществлять с рабочего места, отличного от рабочего места, с которого производится подписание ЭД.
8. КЛИЕНТ обязан в рабочее время БАНКА запрашивать в системе «iBank 2» выписки за текущий и предыдущий день по открытым в БАНКЕ счетам не реже, чем один раз в час. Просмотр рекомендуется осуществлять с рабочего места, отличного от рабочего места, с которого производится подписание ЭД.
9. КЛИЕНТ вправе в любой момент изменить номер телефона, на который осуществляется уведомление в виде SMS-сообщения, предоставив БАНКУ обновленную информацию для связи с КЛИЕНТОМ и направления ему уведомлений, установленным БАНКОМ способом.

Раздел 4. Ответственность сторон

1. В случае не предоставления КЛИЕНТОМ в БАНК достоверной информации о номере мобильного телефона, КЛИЕНТ признается не предоставившим надлежащим образом информацию для связи с КЛИЕНТОМ, и БАНК вправе заблокировать доступ КЛИЕНТА к Системе «iBank2» и/или отключить Услугу дистанционного обслуживания с использованием Системы «iBank2».

2. В случае если КЛИЕНТ предоставил неверные сведения о номере мобильного телефона для осуществления БАНКОМ информирования о совершении операций и/или номер мобильного телефона не используется (блокирован/отключен/не доступен и др.), БАНК не несет ответственности за неисполнение обязанности по направлению уведомления КЛИЕНТУ.
3. БАНК не несет ответственности в случае неполучения КЛИЕНТОМ SMS-сообщения о совершении операции, не осуществления просмотра КЛИЕНТОМ в Системе «iBank 2» списка ЭД и(или) выписок за текущий и предыдущий день по открытым в БАНКЕ счетам.

Раздел 5. Иные условия

1. КЛИЕНТ согласен на передачу информации, связанной с операциями по его счету(-там), путем отправки SMS-сообщений. КЛИЕНТ дает свое согласие на передачу информации о номере мобильного телефона третьим лицам в целях информирования о совершении операций.

Приложение № 12
к Условиям дистанционного обслуживания
клиентов с использованием Системы «iBank 2»

ПОЛОЖЕНИЕ
о порядке действий сторон в случае компрометации средства подтверждения

1. События, которые могут быть расценены как компрометация Средства подтверждения:
   1.1. утрата/хищение Средства подтверждения;
   1.2. несанкционированное копирование ключа ЭП;
   1.3. передача ключа ЭП по открытым каналам связи;
   1.4. случаи, когда нельзя достоверно установить, что произошло со Средством подтверждения (в том числе случаи, когда Средство подтверждения вышло из строя и доказательно не опровергнута возможность того, что, данный факт произошел в результате несанкционированных действий злоумышленника);
   1.5. любые другие признаки осуществления несанкционированных действий в системе «iBank 2».

2. Решение о компрометации Средства подтверждения может быть принято владельцем ключа ЭП или руководителем организации.

3. **В случае компрометации Средства подтверждения и обнаружения факта несанкционированного списания средств КЛИЕНТУ необходимо:**
   3.1. немедленно прекратить любые действия с Рабочим местом Системы «iBank2», обесточить его и отключить от информационных сетей или перевести в режим гибернации;
   3.2. произвести фотосъемку Рабочего места, обеспечить его сохранность, поместив в место с ограниченным доступом и обеспечив при этом защиту от вскрытия. При необходимости ведения хозяйственной деятельности - задействовать другое Рабочее место;
   3.3. обратиться в БАНК с **Уведомлением о прекращении действия средства подтверждения в связи с утратой средства подтверждения / использованием ЭСП без согласия Клиента (Приложение № 7** к настоящим Условиям), далее – «Уведомление по форме Приложения № 7», **на бумажном носителе** за подписью руководителя КЛИЕНТА и оттиском печати, не позднее дня, следующего за днем получения от БАНКА уведомления о совершении операции, и просьбой заблокировать указанные Средства подтверждения и остановить обработку ЭД, подписанных/подтвержденных указанными Средства подтверждения;
   3.4. обратиться в иные банки, которые предоставляют КЛИЕНТУ услуги электронного банкинга, с просьбой о внеплановой замене ключей ЭП в их информационных системах;
   3.5. 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 за максимальный период времени;
   3.6. провести сбор записей с межсетевых экранов и других средств защиты информации, коммуникационного оборудования и устройств, которые могут использоваться для удаленного управления Рабочим местом;
   3.7. обратиться с письменным заявлением к своему Интернет-провайдеру или оператору связи для получения в электронной форме журналов соединений Рабочего места или локальной вычислительной сети компании с сетью Интернет;
   3.8. не предпринимать никаких действий для поиска и удаления компьютерных вирусов, восстановления работоспособности Рабочего места, не отправлять Рабочее место в сервисные службы для восстановления работоспособности;
   3.9. зафиксировать в протокольной форме значимые действия и события, в том числе имена лиц, имеющих доступ к Рабочему месту, предпринимаемые действия с Рабочим местом, подготовить объяснения ответственных сотрудников в случае использования Рабочего места в целях, отличных от осуществления операций в системе электронного банкинга, посещаемых сайтах, перебоях в работе или отказах Рабочего места, обращениях в службы сопровождения, в БАНК, о сторонних лицах, побывавших в месте расположения Рабочего места и т.д.
   3.10. все действия с Рабочим местом производить коллегиально, протоколировать и документировать, в том числе с использованием фотосъемки.

4. **В случае компрометации Средства подтверждения, если факт несанкционированного списания средств не обнаружен, КЛИЕНТУ необходимо:**
Обратиться в БАНК с **Уведомлением по форме Приложения № 7 на бумажном носителе** не позднее дня, следующего за днем обнаружения факта компрометации, и просьбой заблокировать указанные Средства подтверждения и остановить обработку ЭД, подтвержденных указанными Средствами подтверждения.

5. **О компрометации ключа ЭП КЛИЕНТ уведомляет БАНК следующими способами:**
5.1. **по телефону БАНКА 8(495)933-46-00** (Управление информационных технологий Банка), назвав Кодовое слово, с последующим предоставлением **Уведомлением по форме Приложения № 7 на бумажном носителе,** в срок, предусмотренный п. 3.3. настоящего Приложения.
5.2. направить **Уведомление по форме Приложения № 7** в виде скан-копии на электронную почту БАНКА ibank@russitabank.ru, с последующим предоставлением **Уведомлением по форме Приложения № 7 на бумажном носителе,** в срок, предусмотренный п. 4. настоящего Приложения.
5.3. предоставить **Уведомление по форме Приложения № 7** на бумажном носителе в БАНК. Указанное Уведомление предоставляется руководителем КЛИЕНТА или лицом, имеющим соответствующую доверенность на подачу в БАНК вышеуказанного Уведомления.
Уведомление по форме Приложения № 7 на бумажном носителе, предусмотренное настоящий пунктом должно быть подписано руководителем КЛИЕНТА с проставлением оттиском печати и предоставлено в БАНК руководителем КЛИЕНТА или лицом, имеющим соответствующую доверенность на подачу в БАНК вышеуказанного Уведомления.
Уведомление по форме Приложения № 7 на бумажном носителе от КЛИЕНТА считается принятым БАНКОМ с момента проставления уполномоченными лицами Банка соответствующих отметок, подписей и печати на экземпляре КЛИЕНТА указанного Уведомления.

6. БАНК не позднее 1 (Одного) часа с момента получения Уведомления КЛИЕНТА, способами, предусмотренными п. 5 настоящего Приложения, и подтверждения полномочий КЛИЕНТА, останавливает обработку ЭД, подписанных ключами ЭП КЛИЕНТА, и блокирует ключи ЭП КЛИЕНТА.

7. Во всех случаях отключения КЛИЕНТОМ Системы «iBank 2», предусмотренных п. 5 настоящего Приложения, дальнейшее подключение КЛИЕНТОМ Системы «iBank 2» осуществляется заново с предоставлением в БАНК Заявления о подключении Услуги по дистанционному обслуживанию с использованием системы «iBank 2» (Приложение № 5 к настоящим Условиям) и взиманием комиссии согласно Тарифам БАНКА.

8. В случае получения SMS-Сообщения от БАНКА о принятии от КЛИЕНТА по Системе «iBank 2» платежного поручения на расходную операцию и несогласия с указанной операцией КЛИЕНТ обязан незамедлительно с момента поступления указанного SMS-сообщения уведомить БАНК способами, предусмотренными п. 5.1.-5.3. настоящего Приложения, о своем несогласии и обратиться с просьбой предотвратить совершение планируемой расходной операции.
В случае поступления в БАНК от КЛИЕНТА по Системе «iBank 2» платежного поручения на расходную операцию и отсутствия в соответствии с настоящим Приложением Уведомления от КЛИЕНТА свидетельствуют о согласии КЛИЕНТА с расходной операцией по Счету. В указанном случае БАНК не несет ответственности за совершение несанкционированной расходной операции по Счету(-там) КЛИЕНТА.

9. Электронные документы, находящиеся на момент получения/исполнения **Уведомление по форме Приложения № 7** на бумажном в статусе «На обработке»/«На исполнении» отзыву не подлежат. При наличии в вышеуказанном случае технической возможности БАНК вправе остановить обработку и исполнение ЭД.

Приложение № 13
к Условиям дистанционного обслуживания
клиентов с использованием Системы «iBank 2»

СЕРВИС «МОБИЛЬНЫЙ БАНК»

1. Сервис Мобильный банк – дополнительный информационный сервис для пользователей Системы «iBank 2»в рамках Услуги дистанционного обслуживания по Системе «iBank2 и обеспечивает Клиенту возможность через мобильное приложение просматривать информацию по Счетам и выполнять действия, предусмотренные п. 3 настоящего Приложения.

2. Сервис Мобильный банк предназначен только для пользователей Системы «iBank2».

3. Сервис Мобильный банк позволяет Клиенту при помощи мобильного телефона осуществлять следующие действия:

- **просматривать список Счетов Клиента;**
- **просматривать остатки по Счетам Клиента;**
- **получать выписки по Счетам Клиента;**
- **просматривать список платежных поручений;**
- **просматривать выбранное платежное поручение;**
- **просматривать банковские реквизиты Счетов Клиента;**
- **печатать выбранное платежное поручение.**

4. Доступ к сервису Мобильный банк реализуется путём установки приложения на мобильный телефон Клиента. Мобильный телефон должен работать под управлением операционной системы:

- Android (версия 4.1 и выше);
- IOS (версия 8.0 и выше).
- Мобильный телефон должен иметь доступ к сети интернет.

5. Для подключения сервиса Мобильный банк необходимо:

Предоставить в банк **Заявление о подключении Услуги по дистанционному обслуживанию с использованием системы «iBank 2» (Приложение № 5** к Условиям дистанционного обслуживания клиентов по Системе «iBank 2») с отмеченной опцией «Мобильный банк» для тех сотрудников (уполномоченных представителей Клиента), кому это необходимо.

6. Для отключения, а также изменения номеров телефонов сотрудников Клиента, которым предоставлен доступ к сервису Мобильный банк необходимо использовать также **Заявление о подключении Услуги по дистанционному обслуживанию с использованием системы «iBank 2» (Приложение № 5** к Условиям дистанционного обслуживания клиентов по Системе «iBank 2»), указав, что заявление корректирующее – и внести соответствующие изменения.

7. Процедура установки приложения Мобильный банк

Не ранее следующего рабочего дня после подачи заявления Уполномоченный представитель Клиента скачивает и устанавливает мобильное приложение «Мобильный банк РОССИТА-БАНК» на свой мобильный телефон (через сервисы приложений Google Play или AppStore) и выполняет регистрацию в Мобильном банке следующим образом:

- Необходимо пройти идентификацию в мобильном приложении по номеру телефона (при первом входе на стартовой странице указывается номер телефона, для которого будет создана учетная запись);
- Необходимо создать для входа в мобильное приложение «Мобильный банк РОССИТА-БАНК» код доступа, который представляет собой последовательность цифр, которая будет использоваться для аутентификации Уполномоченного представителя Клиента.

После окончания процедуры подключения Мобильного банка Клиенту становится доступно выполнение действий, указанных в п. 3 настоящего Приложения.

7. Особые условия

7.1. Клиент уведомлен о необходимости самостоятельной установки мобильного приложения Мобильный банк на мобильный телефон с соответствующей операционной системой.

7.2. Клиент уведомлён о том, что сервис Мобильный банк доступен только тем сотрудникам (Уполномоченным лицам) Клиента, которые получили в Банке электронную цифровую подпись для работы в системе «iBank 2».

7.3. Клиент предупрежден о том, что в целях соблюдения мер безопасности, необходимо каждый раз после завершения работы в Мобильном банке - выполнять выход из мобильного приложения (меню-выход).

7.4. Клиент предупрежден о том, что утрата мобильного телефона может позволить третьим лицам получить информацию о состоянии Счета Клиента.

7.5. Клиент соглашается с тем, что Банк не несет ответственности за утечку информации по каналам связи сотового оператора.

7.6. Клиент соглашается с тем, что Банк не несет ответственности в случае невозможности получения Клиентом информации через Мобильный банк, обусловленной техническими проблемами, в том числе возникшими по вине провайдера сети интернет или оператора сотовой связи.