

ДОГОВОР
обмена электронными документами
с использованием системы дистанционного банковского
обслуживания «iBank 2» (для физических лиц)
№ ___ - ПЭП

г. Москва

"___" _____ 20__ г.

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

1. Термины, применяемые в Договоре

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

1.1. **Система дистанционного банковского обслуживания «iBank 2» (Система ДБО, Система ДБО «iBank2»)** – совокупность программно-аппаратных средств, устанавливаемых на территории Клиента и Банка, и согласовано эксплуатируемых Клиентом и Банком в соответствующих частях, а также организационных мероприятий, проводимых Клиентом и Банком, позволяющая осуществлять обмен электронными документами и информацией в электронном виде между ее участниками, и предназначенная для предоставления Клиентам – физическим лицам возможности получать информационные услуги и совершать банковские операции посредством сети Интернет, с целью предоставления Клиенту услуг по настоящему Договору. В Системе ДБО Клиентом может использоваться только встроенный в Систему ДБО механизм простой электронной подписи (ПЭП). Помимо наименования Система ДБО «iBank 2», Система «iBank 2» в тексте документации разработчика может также использоваться тождественное наименование – «Система iBank для жизни».

1.2. **Авторизация** – процедура подтверждения полномочий Клиента на получение услуг в Системе ДБО. Авторизация проводится после проведения идентификации и аутентификации путем ввода Клиентом авторизационных данных (Логина, Первичного пароля, Пароля, Кода доступа). Авторизация проводится при каждом входе Клиента в Систему ДБО.

1.3. **Аутентификация** – выполняемая средствами Системы ДБО процедура установления принадлежности Клиенту используемого им способа идентификации для авторизации, поддерживаемого системой ДБО (логин и пароль, отпечаток пальца (fingerprint), распознавание лица (FaceID)).

1.4. **Банк** – Общество с ограниченной ответственностью Коммерческий Банк «Столичный Кредит», ООО КБ «Столичный Кредит».

1.5. **Блокировочное слово** – уникальное слово, определяемое Клиентом при регистрации в Системе ДБО. Блокировочное слово может быть использовано Клиентом для блокирования своей работы в Системе ДБО по телефонному звонку в Банк (например, в случае компрометации ключа).

1.6. **Браузер** - используемое Клиентом для работы с Системой ДБО прикладное программное обеспечение, предназначенное для: просмотра веб-сайтов, содержания веб-документов, компьютерных файлов и их каталогов; управления веб-приложениями; запроса веб-страниц, их обработки, вывода и перехода от одной страницы к другой; а также для решения других задач. Разрешенные для использования Клиентом при работе с Системой ДБО наименования браузеров, а также их версии приведены в Приложении №4 настоящего Договора.

1.7. **Вредоносный код (ВК)** – компьютерная программа, предназначенная для внедрения в автоматизированные системы, программное обеспечение, средства вычислительной техники, телекоммуникационное оборудование 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.

1.8. **Договор обмена электронными документами с использованием системы дистанционного банковского обслуживания «iBank 2» (для физических лиц) (далее – Договор)** - настоящий документ, являющийся одновременно публичным договором и договором присоединения, а также Заявление, надлежащим образом заполненное и подписанное Клиентом и Банком, Тарифы и комиссии ООО КБ «Столичный Кредит».

1.9. **Договор банковского счета** – совокупность документов: Правила, Тарифы и комиссии, каждое Заявление, надлежащим образом заполненное и подписанное Клиентом и Банком, на основании которого Клиенту открыт банковский счет.

1.10. **Долговременный пароль** – секретная, известная только Клиенту последовательность алфавитно-цифровых символов, соответствующая Логину Клиента многократно используемая в совокупности с Логинном для аутентификации Клиента при авторизации в Системе ДБО. При регистрации в Системе ДБО Клиент самостоятельно создает и с необходимой регулярностью, а также по мере необходимости в любой момент времени самостоятельно изменяет Долговременный пароль посредством Системы ДБО.

1.11. **Защита от ВК** – организованная деятельность по защите автоматизированных систем, программного обеспечения, средств вычислительной техники, телекоммуникационного оборудования от атак ВК и устранению их последствий.

1.12. **Интернет-Банк** – канал обслуживания (интерфейс, модуль) Системы ДБО предназначенный для использования Клиентом посредством персональных компьютеров.

1.13. **Информационная безопасность** – состояние сохранности информации, информационных ресурсов и информационных систем, при котором с требуемой вероятностью обеспечивается защита информации (данных) от утечки, хищения, утраты, несанкционированного уничтожения, искажения, модификации (подделки), копирования, блокирования и т.п., состояния защищенности информации, обрабатываемой средствами вычислительной техники или автоматизированной системы, от внутренних или внешних угроз.

1.14. **Клиент** – физическое лицо, находящееся на обслуживании в Банке, на имя которого на момент заключения настоящего Договора открыт Счет.

1.15. **Код подтверждения** – одноразовая цифровая последовательность символов, генерируемая Системой ДБО, направляемая Банком на зарегистрированный в Системе телефонный номер Мобильного устройства Клиента посредством SMS-сообщения на номер мобильного телефона или в сообщении на адрес электронной почты Клиента, указанные в Заявлении на присоединение.

1.16. **Код доступа** – уникальная цифровая последовательность, устанавливаемая Клиентом, которая известна только Клиенту в Мобильном приложении и предназначенная для аутентификации в мобильной версии Системы ДБО.

На устройствах, оснащенных соответствующими датчиками, в качестве Кода доступа может использоваться отпечаток пальца (fingerprint) или распознавание лица (FaceID). При этом для обработки информации содержащей сведения об отпечатке пальца или распознавании лица используются средства операционной системы Мобильного устройства, а информация об отпечатке пальца или распознавании лица не покидает пределов Мобильного устройства. Банком при этом не осуществляется обработка биометрических персональных данных. Поддерживаются технологии идентификации пользователя по отпечатку пальца или распознаванию лица операционных систем Android и iOS.

1.17. **Компрометация** – утрата, хищение, несанкционированное копирование, либо разглашение авторизационных данных, Кодов подтверждения, утрата Мобильного устройства, передача закрытого ключа в линию связи в открытом виде, любые другие виды разглашения содержания ключа, кодов подтверждения, а также случаи, когда нельзя достоверно установить, что произошло с носителями, содержащими ключевую информацию (в том числе случаи, когда носитель вышел из строя и доказательно не опровергнута возможность того, что данный факт произошел в результате действий злоумышленника), авторизационными данными, Кодом подтверждения, Мобильным устройством, любые другие аналогичные признаки, явившиеся причиной осуществления несанкционированных действий в Системе ДБО.

1.18. **Логин** – имя учетной записи Клиента в виде уникальной комбинации символов, служащее для идентификации Клиента. Присваивается Клиенту при регистрации в Системе ДБО.

1.19. **Мобильное приложение** – переносное устройство Клиента, такое как смартфон, планшетный компьютер, мобильный телефон и/или другие устройства Клиента, на которых есть возможность установки Мобильного приложения и доступ в Интернет, используемое для оказания услуг дистанционного банковского обслуживания посредством канала обслуживания, а также для оперативной мобильной связи с Клиентом, отправки Банком Клиенту Кодов подтверждения, SMS-уведомлений и иных SMS-сообщений от Системы ДБО.

1.20. **Мобильное приложение** – специализированное программное обеспечение, устанавливаемое Клиентом на его Мобильное устройство с официального ресурса распространения программного обеспечения. Официальными ресурсами являются: для операционной системы Android – магазин приложений Google Play, для операционной системы iOS – магазин приложений App Store. В перечисленных выше магазинах приложений мобильное приложение Банка размещено под названием «Банк Столичный Кредит». Разработчиком мобильного приложения является АО «БИФИТ».

1.21. **Мобильный Банк** – канал обслуживания (интерфейс, модуль) Системы ДБО, предназначенный для использования Клиентом посредством Мобильных устройств. Для использования данного модуля требуется установка Мобильного приложения на Мобильное(-ые) устройство(-а) Клиента.

1.22. **Многофакторная аутентификация** – метод аутентификации Клиента, при котором требуются, по крайней мере, два и более различных фактора аутентификации (обязательные: Логин, Долговременный пароль; дополнительные: Код подтверждения).

1.23. **Одноразовый пароль** – уникальная последовательность символов, направляемая Клиенту посредством SMS-сообщения на зарегистрированный в Системе телефонный номер Мобильного устройства, указанный в Заявлении на присоединение, и используемая Клиентом в качестве Пароля для единичного использования.

1.24. **Операция** – действия, осуществляемые Банком на основании Электронного документа, переданного Клиентом в Банк с использованием Системы ДБО в порядке, установленном настоящим Договором.

1.25. **Пароль** – уникальная последовательность символов, созданная Клиентом самостоятельно в Системе ДБО.

1.26. **Первичный пароль** – уникальная последовательность символов, направляемая Клиенту посредством SMS-сообщения на зарегистрированный в Системе телефонный номер Мобильного устройства или в сообщении на адрес электронной почты Клиента, указанные в Заявлении на присоединение, и используемая Клиентом в качестве Пароля при первой регистрации в Системе ДБО.

1.27. **Платежный документ, Платеж** – расчетные (платежные) документы, такие как платежное поручение, инкассовое поручение, платежное требование, платежный ордер, банковский ордер, платежное распоряжение имеющие реквизиты для их последующей обработки.

1.28. **Протоколы операций** – файлы и/или записи в базе данных Системы ДБО, содержащие в хронологическом порядке сведения о действиях Клиента и иных событиях, возникающих в ходе работы Системы ДБО.

1.29. **Простая электронная подпись (ПЭП)** – электронная подпись, которая посредством использования кодов, паролей или иных средств подтверждает факт формирования электронной подписи Клиентом. Для создания ПЭП используется Код подтверждения.

1.30. **Рабочее место** – совокупность программного и аппаратного средства (компьютер или Мобильное устройство), с которого осуществляется доступ Клиентом к Системе ДБО.

1.31. **Рабочий день** – день, который в соответствии с законодательством Российской Федерации не является выходным и (или) нерабочим праздничным днем.

1.32. **Статус ЭД** – реквизит Электронного документа, характеризующий стадию его обработки Банком и отображающийся в Системе ДБО. Возможны следующие статусы электронных документов: «Принят», «На обработке», «На исполнении», «Исполнен», «Отвергнут».

1.33. **Стороны** – Банк и Клиент при совместном упоминании.

1.34. **Счет** – текущий счет/счет по вкладу, открытый на имя Клиента в Банке, по которому Клиент совершает Операции и получает информацию в рамках настоящего Договора.

1.35. **Тарифы Банка** – официальный документ Банка, устанавливающий размер и порядок оплаты комиссий, услуг Банка.

1.36. **Электронный документ (ЭД)** – документированная финансовая информация с платежными данными или информационным сообщением, представленная в электронной форме в виде, пригодном для обработки Системой ДБО, подготовленная с использованием Рабочего места Клиента, для передачи по сети Интернет в Системе ДБО.

1.37. **Электронная подпись (далее - 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. Обслуживание Клиентов с использованием Системы ДБО осуществляется с применением Простой электронной подписи (ПЭП).

1.38. **SMS-уведомление** – сообщение, содержащее информацию об Операции, совершенной по Счету / Платежной карте с использованием Системы ДБО, направляемое Банком Клиенту в электронном виде на номер мобильного телефона, указанный в Заявлении на присоединение.

2. Предмет Договора

2.1. Банк оказывает Клиенту услуги дистанционного банковского обслуживания с использованием Системы ДБО «iBank2», позволяющей передавать Электронные документы и принимать выписки и информационные сообщения.

2.2. Настоящий Договор имеет свою юридическую силу при наличии действующего Договора банковского счёта № _____ от «__» _____ 20__ г. заключённого Сторонами.

2.3. Настоящий Договор распространяются на Счета Клиента, подключенные к Системе ДБО «iBank2».

3. Соглашения Сторон

3.1. Стороны признают, что аутентификация Клиента в Системе ДБО проводится методом Многофакторной аутентификации.

3.2. Стороны признают, что применяемые в Системе ДБО механизмы ПЭП являются надежными. Документы, подписанные ПЭП, принимаются Банком к исполнению только в случае осуществления подписи с использованием Кода подтверждения, направленного Банком на зарегистрированный в Системе ДБО телефонный номер Мобильного устройства, предоставленный Клиентом при открытии Счета в Банке, также указанный по форме в соответствии с Приложением № 5 настоящего Договора.

3.3. Стороны признают, что применяемая в Системе ДБО система подтверждения Электронного документа ПЭП достаточна для защиты информации от несанкционированного доступа, подтверждения подлинности и авторства ЭД.

3.4. Стороны признают, что ЭД, подписанный ПЭП, является ЭД равнозначным документу на бумажном носителе подписанному собственноручной подписью.

3.5. Стороны признают, что зарегистрированным в Системе ДБО телефонным номером Мобильного устройства, является номер, предоставленный Клиентом при открытии Счета в Банке, также указанный по форме в соответствии с Приложением № 5 настоящего Договора.

3.6. Стороны признают, что подтверждение электронного документа ПЭП от имени Клиента практически невозможно без владения Мобильным устройством Клиента и/или знания Кода подтверждения.

3.7. Стороны признают, что подделка ЭП Клиента (то есть создание ПЭП в Электронном документе от имени Клиента) практически невозможно без владения Мобильным устройством Клиента и/или знания Кода подтверждения.

3.8. Стороны признают, что Электронные документы, подтвержденные ПЭП Клиента, полученные Банком по Системе ДБО, являются доказательным материалом для решения спорных вопросов в соответствии с Приложением №1 настоящего Договора («Положение о порядке проведения технической экспертизы при возникновении спорных ситуаций»). ЭД Клиента, не подтвержденные ПЭП, при наличии спорных вопросов не являются доказательным материалом.

3.9. Стороны признают, что в Системе ДБО каждая ПЭП однозначно соответствует одному ЭД Клиента.

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

3.11. Стороны признают, что применяемые в Системе ДБО 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 в Системе ДБО телефонного номера Мобильного устройства Клиента, указанного по форме в соответствии с Приложением №5 настоящего Договора.

3.12. Перечень ЭД Клиента, передаваемых по Системе ДБО, приведен в Приложении №2 к настоящему Договору.

3.13. Стороны признают, что ЭД Клиента, подтвержденные ПЭП, юридически эквивалентны соответствующим документам на бумажном носителе, оформленным в установленном порядке, обладают юридической силой и подтверждают наличие правовых отношений между Сторонами. Электронные документы Клиента, не подтвержденные ПЭП Клиента, не имеют юридической силы, Банком не рассматриваются и не исполняются.

3.14. Стороны признают, что для уведомления Клиента о произведенных транзакциях в Системе ДБО в соответствии с Федеральным законом от 27 июня 2011 года № 161-ФЗ от «О национальной платежной системе» и Положением Банка России от 29 июня 2021 года 762-П «О правилах осуществления перевода денежных средств», Банку необходимо и достаточно отправить SMS-сообщение на номер Мобильного телефона Клиента, зарегистрированного в Системе ДБО по Заявлению Клиента (Приложение №5). В случае получения Банком подтверждения от оператора связи об успешной отправке SMS-сообщения, Клиент считается уведомленным о произведенной Клиентом транзакции в Системе ДБО «iBank2».

3.15. Стороны признают, что, подписывая настоящий Договор они принимают Положение о порядке проведения технической экспертизы при возникновении спорных ситуаций, изложенное в Приложении №1 к настоящему Договору.

3.16. Стороны признают, что ознакомлены с информацией, указанной в Приложениях №3 и №4 к настоящему Договору.

3.17. Стороны признают, что Протоколы операций Системы ДБО, могут использоваться в качестве доказательства авторства проводимых Клиентом операций, а также в качестве доказательства нарушения Клиентом правил безопасной работы в Системе ДБО.

3.18. Стороны признают, что регистрация или прекращение регистрации Мобильного устройства Клиента в качестве средства получения, кодов подтверждения, первичных паролей осуществляется по письменному заявлению Клиента, оформленному в соответствии с Приложениями №5 и №6 к настоящему Договору.

3.19. Приложения к настоящему договору подписываются в соответствии с условиями, установленными пунктами 3.1 - 3.19 настоящего Договора.

4. Права и обязанности Банка

4.1. Банк обязан принимать к исполнению ЭД Клиента, полученные по Системе ДБО от Клиента, подтвержденные ПЭП Клиента, соответствующие требованиям настоящего Договора и действующего законодательства Российской Федерации.

4.2. Банк обязан информировать Клиента о совершенных операциях с использованием Системы ДБО одним из способов, установленных в Положении о порядке и способах информирования Клиента о совершенных операциях с использованием Системы ДБО (Приложение № 3 к настоящему Договору).

4.3. Банк обязан предоставить Клиенту необходимые рекомендации для работы с Системой ДБО «iBank2» (Приложение №7 к настоящему Договору).

4.4. В случае выявления Банком операций, соответствующих признакам осуществления перевода денежных средств без согласия клиента, при наличии технической возможности Банк, до осуществления списания денежных средств со Счета Клиента, обязан приостановить исполнение таких ЭД.

4.4.1. Банк предоставляет Клиенту информацию о совершении им действий, предусмотренных п. 4.4 настоящего Договора и запрашивает у Клиента подтверждение возобновления исполнения ЭД.

4.4.2. При получении от Клиента подтверждения, указанного в п. 4.4.1 настоящего Договора, Банк возобновляет исполнение ЭД. При неполучении от Клиента подтверждения, Банк возобновляет исполнение ЭД по истечении двух рабочих дней после дня совершения им действий, предусмотренных п. 4.4 настоящего Договора.

4.5. Банк обязан соблюдать конфиденциальность созданных для Клиента Логина, Первичного пароля, Кодов подтверждения.

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

4.7. Банк обязан в случае получения от Клиента телефонного звонка и сообщения Блокировочного слова или получения надлежащим образом оформленного уведомления о прекращении действия телефонного номера Мобильного устройства и/или сообщения Клиента о Компрометации, и/или об использовании Системы ДБО без согласия Клиента заблокировать доступ Клиента к Системе ДБО и прекратить обработку ЭД, подписанных ПЭП Клиента.

4.8. Банк уведомляет Клиента о проведенных транзакциях в соответствии с Федеральным законом от 27 июня 2011 года №161-ФЗ «О национальной платежной системе», Положением Банка России от 29 июня 2021 года №762-П «О правилах осуществления перевода денежных средств».

4.9. Банк имеет право отказать Клиенту в заключении Договора.

4.10. При наличии обоснованных подозрений в нарушении Клиентом порядка использования Системы ДБО, Правил Безопасности, либо если у Банка имеются основания предполагать, что доступ к Системе ДБО от имени Клиента осуществляется неуполномоченным лицом и/или имеет место Компрометация, Банк имеет право не производить исполнение полученных от Клиента ЭД, заблокировать использование Клиентом Системы ДБО и требовать от Клиента предоставления оформленных в установленном порядке платежных документов на бумажном носителе. Банк незамедлительно любым способом сообщит Клиенту о возникновении подобных подозрений и необходимости предоставить платежные документы на бумажном носителе.

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

4.12. Банк оставляет за собой право на приостановление действия настоящего Договора в случае, если решением/постановлением налогового органа, суда, или судебного пристава-исполнителя на денежные средства Клиента, находящиеся на банковском счете, наложен арест. В случае наложения ареста на денежные средства Клиента, находящиеся на банковском счете, абонентская плата по настоящему Договору не взимается. По факту отмены решения о приостановлении операций по банковскому счету Клиента, действие настоящего Договора возобновляется.

4.13. 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 Системы ДБО до получения от Клиента достоверной информации. При этом Банк прекращает обработку всех ЭД, полученных от Клиента с момента выявления факта предоставления Клиентом недостоверной информации или отсутствия уведомления об изменении информации. Банк незамедлительно любым способом сообщает Клиенту о приостановлении использования Системы ДБО и прекращении обработки его ЭД.

4.14. Банк оставляет за собой право отказать Клиенту в приеме от него распоряжений на проведение операций по банковскому счету, подписанных ПЭП, в случае:

- выявления сомнительных операций (после предварительного уведомления Клиента), установленных действующим законодательством РФ,

- нормативными актами о противодействии легализации (отмыванию) доходов, полученных преступным путем, финансированию терроризма и финансированию распространения оружия массового уничтожения и перейти на прием от Клиента расчетных документов только на бумажном носителе.

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

4.16. Банк вправе определять перечень разрешенных для использования Клиентом поддерживаемых Банком каналов обслуживания (интерфейсов, модулей) Системы «iBank для жизни». Если Банк разрешает Клиенту одновременно использовать несколько каналов обслуживания (интерфейсов, модулей) Системы «iBank для жизни», то Клиент вправе по своему усмотрению использовать любой(-ые) из них с учетом всех возможностей, особенностей и рисков, указанных в настоящем Договоре и в соответствующих руководствах пользователя по использованию каждого из каналов обслуживания (интерфейсов, модулей) Системы «iBank для жизни». Разрешенными для использования Клиентами Банка каналами обслуживания (интерфейсами, модулями) Системы «iBank для жизни», являются: «Интернет-Банк» и «Мобильный Банк».

4.17. Банк вправе запросить у Клиента документы, информацию и сведения, необходимые для исполнения Банком требований Федерального закона от 07.08.2001 № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма», иных действующих нормативных актов Российской Федерации, в том числе раскрывающие экономический смысл Операций, проводимых посредством Системы ДБО. Предоставление документов осуществляется в сроки и в порядке, установленные запросом Банка. Выполнение данного требования является условием исполнения Банком ЭД Клиента

5. Права и обязанности Клиента

5.1. Клиент имеет право зарегистрировать новый телефонный номер Мобильного устройства, оформив заявление по форме в соответствии с Приложением № 5 настоящего Договора, предварительно отменив действие ранее зарегистрированного телефонного номера Мобильного устройства, оформив соответствующее уведомление по форме в соответствии с Приложением № 6 настоящего Договора.

5.2. Клиент обязан использовать для получения SMS-уведомлений и иных SMS-сообщений от Системы ДБО номер мобильного телефона, зарегистрированный за Клиентом у оператора, оказывающего услуги мобильной связи.

5.3. Перед началом эксплуатации Системы ДБО Клиент получает и самостоятельно устанавливает на своем рабочем месте программные модули Системы ДБО.

5.4. Клиент имеет право самостоятельно изменять пароль в Системе ДБО неограниченное количество раз.

5.5. Клиент имеет право пользоваться услугами Системы ДБО с учетом ограничений, установленных настоящим Договором, Тарифами Банка и техническими возможностями Системы ДБО.

5.6. Клиент имеет право приостановить или отказаться от услуг Системы ДБО, уведомив Банк письменно.

5.7. Клиент обязан до начала работы в Системе ДБО ознакомиться с описанием механизмов защиты Системы ДБО (Приложение №7 настоящего Договора) и памяткой клиенту об обеспечении информационной безопасности своего Рабочего места (Приложение №9 настоящего Договора), которые также размещены на сайте Банка в сети Интернет.

5.8. В случае если знания Клиента недостаточно для адекватной оценки механизмов защиты системы и (или) обеспечения информационной безопасности своего Рабочего места, Клиент вправе обратиться к услугам сторонних специалистов. При этом оплата услуг специалистов производится Клиентом самостоятельно.

5.9. Клиент обязан сообщать Банку об обнаружении попытки несанкционированного доступа к Системе ДБО незамедлительно после момента обнаружения, любым доступным Клиенту способом, в том числе по средствам телефонной связи, электронной почты, с обязательным указанием Блокировочного слова.

5.10. Клиент обязан обеспечивать информационную безопасность своих Рабочих мест, используемых для взаимодействия с Банком, в том числе соблюдая правила, перечисленные в Приложении № 7, 9 настоящего Договора.

5.11. Клиент предупрежден, что при невыполнении данного условия у него могут возникнуть неблагоприятные последствия в виде несанкционированного списания денежных средств с его Счетов третьими лицами. Клиент обязан исключить или максимально ограничить доступ к своим Рабочим местам посторонних лиц.

5.12. Клиент обязан заполнять Электронные документы в Системе ДБО в соответствии с действующим законодательством РФ, в частности Положением Банка России от 29 июня 2021 г. № 762-П «О правилах осуществления перевода денежных средств».

5.13. Клиент обязан хранить в секрете и не передавать третьим лицам авторизационные данные. Запрещается хранить авторизационные данные на Рабочем месте, а также в открытом доступе. Разглашение Клиентом данных о его счетах, логине, пароле и кодах является нарушением условий настоящего Договора со стороны Клиента и негативные последствия, наступившие в их результате, возлагаются на Клиента.

5.14. Клиент обязан соблюдать конфиденциальность полученных/созданных паролей, Кодов доступа и Кодов подтверждения.

5.15. Клиент обязуется не передавать третьим лицам авторизационные данные, Мобильное устройство, Коды подтверждения и обеспечить защиту Рабочего места от несанкционированного использования третьими лицами.

5.16. Клиент обязан предоставлять Банку документы и информацию, необходимые для осуществления операций по Счету и контроля за проведением Клиентом операций в порядке, предусмотренном законодательством Российской Федерации и нормативными актами Банка России.

5.17. Клиент обязан оплачивать услуги Банка по настоящему Договору на основании утвержденных Тарифов Банка.

5.18. Клиент обязан в случае указания неверного номера Мобильного телефона для получения SMS-сообщений - компенсировать Банку выплаты по претензии владельца неверно указанного номера Мобильного телефона, если таковые выплаты имелись и подтверждены Банком документально.

5.19. Клиент имеет право, при работе в Системе ДБО, в целях недопущения осуществления переводов денежных средств без его согласия, в заявительном порядке (заявление клиента, оформленное в письменном виде), распорядится об установлении Банком в отношении операций, осуществляемых Клиентом с использованием Системы ДБО, ограничений на осуществление операций. Ограничения по операциям, осуществляемым Клиентом с использованием Системы ДБО, могут быть установлены как на все операции Клиента, так и в разрезе видов операций, исходя из технической возможности Банка, администратором Системы ДБО Банка, на основании письменного заявления Клиента (Приложение №8).

5.20. Клиент вправе отозвать заявление об установлении Банком ограничений на осуществление операций, путем направления письменного заявления на отзыв в свободной форме, либо направлением нового заявления по форме в соответствии с Приложением №8 настоящего Договора.

5.21. Клиент обязан в случае подозрения на кражу или потерю мобильного устройства незамедлительно обратиться в Банк для временной блокировки доступа в Систему ДБО (до восстановления SIM-карты) или изменения номера мобильного телефона.

5.22. Клиент обязан исключить возможность получения доступа в Систему ДБО посредством браузера с Рабочего места, в том числе Мобильного устройства содержащего вредоносный или модифицированный код.

5.23. Клиент обязан исключить возможность пользования Мобильным устройством, которое может содержать не предусмотренное разработчиками и/или не сертифицированное производителем мобильного устройства программное обеспечение, прошло модификацию операционной системы, Мобильного приложения или иного программного обеспечения, не предусмотренную разработчиками программного обеспечения и/или не сертифицированную производителем Мобильного устройства.

5.24. Клиент проинформирован, что использование Системы ДБО с персонального компьютера, размещенного в общественном или ином общедоступном месте имеет повышенный риск несанкционированного доступа в Систему ДБО.

5.25. Клиент обязан принять факт, того что Интернет не является безопасным каналом связи и передачи информации, и осознает риски, связанные с возможным нарушением конфиденциальности и целостности информации при работе через Сеть Интернет, и иные риски, возникающие вследствие использования такого канала доступа.

5.26. Клиент обязан не допускать переполнение памяти Мобильных устройств, предназначенных для приема и хранения SMS-сообщений, что может являться препятствием для приема SMS – подтверждений и SMS, e-mail – уведомлений.

6. Совместные обязательства и ответственность Сторон

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

6.2. Банк не несёт ответственности за ущерб, причинённый Клиенту в результате использования третьими лицами авторизационных данных, Кодов подтверждения и паролей Клиента.

6.3. При расторжении настоящего Договора Стороны несут ответственность по всем Электронным документам, сформированным в Системе ДБО, в период действия настоящего Договора, в соответствии с настоящим Договором и действующим законодательством РФ.

6.4. В случае возникновения конфликтных ситуаций между Клиентом и Банком при использовании Системы ДБО, Стороны обязуются участвовать в рассмотрении конфликтов в соответствии с «Положением о порядке проведения технической экспертизы при возникновении спорных ситуаций» (Приложение №1), выполнять требования указанного Положения и нести ответственность согласно выводам по рассмотрению конфликтной ситуации. Действия Сторон согласно вышеуказанному Положению являются обязательной составляющей процедуры досудебного урегулирования споров.

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

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

6.7. Банк не несет ответственности за техническое состояние оборудования и Рабочего места Клиента, возможные помехи на линии связи, плохое соединение или невозможность установить соединение, отключение электроэнергии и другие, не зависящие от Банка неисправности, делающие невозможным обмен ЭД.

6.8. Банк не несет ответственности за обеспечение информационной безопасности на Рабочем месте Клиента. Ответственность за обеспечение информационной безопасности на Рабочем месте Клиента несет сам Клиент.

6.9. Банк не несёт ответственности за ущерб, причинённый Клиенту в результате нарушения или ненадлежащего исполнения Клиентом настоящего Договора, правил и рекомендаций для работы в Системе ДБО.

6.10. Клиент несет ответственность за:

- обеспечение информационной безопасности своего Рабочего места;
- несвоевременное и/или неполное письменное уведомление Банка об обстоятельствах, предусмотренных настоящим Договором, в том числе о компрометации/подозрении на компрометацию и/или о несанкционированном доступе к Системе ДБО/подозрении на несанкционированный доступ к Системе ДБО, об изменении ранее сообщенных Банку сведений о себе;
- убытки, возникшие у Банка в результате исполнения распоряжений, переданных в Банк от имени Клиента неуполномоченным лицом, при условии, что это стало возможно по вине Клиента;
- конфиденциальность, сохранность и целостность авторизационных данных и Кодов подтверждения;
- полноту и правильность данных, указанных в ЭД, оформляемых в рамках настоящего Договора.
- недостоверность информации, указанной в соответствующих ЭД, которая может служить отказом Банка в их исполнении;
- правильность и актуальность всех документов (иной информации), предоставляемых им в Банк при заключении и исполнении настоящего Договора.

7. Порядок обслуживания Клиента

7.1. Банк осуществляет прием ЭД, передаваемых по Системе ДБО, круглосуточно. При невозможности передачи документов в Банк с использованием Системы ДБО документы могут поступить от Клиента на бумажном носителе в офис Банка по месту обслуживания Счета Клиента в соответствии с графиком работы Банка.

7.2. При получении от Клиента ЭД, содержащего распоряжение денежными средствами, находящимися на счете Клиента Банк производит в автоматизированном режиме проверку подлинности ПЭП Клиента, проверку полноты и правильности заполнения реквизитов документа, проверку на возможность возникновения дебетового сальдо на расчётном счёте Клиента, и проверка на выполнение условий по ограничениям, установленным Тарифами Банка. В случае отбраковки Электронный документ Банком к исполнению не принимается.

7.3. В случае отмены платежа, изменения реквизитов, назначения платежа, суммы платежа Клиент обязуется известить об этом Банк, направив электронное письмо используя Систему ДБО, а также подтвердить вышеуказанные изменения телефонным звонком, используя Блокировочное слово не позднее 20 (двадцати) минут с момента выставления платежа.

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

7.5. Обслуживание Клиента по Системе ДБО Банк осуществляет в соответствии с тарифами, установленными Банком и акцептованными Клиентом. Банк оставляет за собой право одностороннего изменения тарифов с обязательным уведомлением об этом Клиента не менее чем за 10 (десять) дней до вступления в действие новых тарифов. Если Клиент не согласен обслуживаться в соответствии с новыми тарифами, он обязан расторгнуть настоящий Договор в порядке, предусмотренном разделом 8 настоящего Договора.

8. Срок действия Договора

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

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

8.3. Договор считается расторгнутым автоматически в случае прекращения действия (расторжения) всех Договоров банковского счета, заключенных между Клиентом и Банком, без письменного уведомления Банком Клиента или без письменного заявления Клиента.

9. Заключительные положения

9.1. Споры по настоящему Договору решаются путем переговоров с учетом взаимных интересов в соответствии с Приложением №1 настоящего Договора. Все нерегулируемые споры, возникающие между сторонами, рассматриваются в соответствии с действующим законодательством РФ в Арбитражном суде г. Москвы.

9.2. Внесение изменений и/или дополнений в настоящий Договор (включая все приложения) и/или Тарифы Банка, в том числе утверждение Банком новой редакции настоящего Договора, производится по инициативе Банка в порядке, предусмотренном настоящим разделом.

9.3. Банк информирует Клиента об изменениях и/или дополнениях, вносимых в настоящий Договор и/или Тарифы Банка, в том числе об утверждении Банком новой редакции настоящего Договора, не позднее, чем за 10 (Десять) календарных дней до вступления их в силу одним из способов, обеспечивающих возможность ознакомления с этой информацией Клиентов, в том числе:

- размещения информации на интернет-сайте Банка;
- размещения информации в операционных залах Банка (дополнительных офисах и других структурных подразделениях Банка, осуществляющих обслуживание Клиентов);

- рассылки информационных сообщений по Системе ДБО;

- иными способами, позволяющими Клиенту получить информацию и установить, что она исходит от Банка.

9.4. В случае несогласия Клиента с изменениями и/или дополнениями, внесенными Банком в настоящий Договор и/или Тарифы Банка, Клиент имеет право расторгнуть настоящий Договор в порядке, предусмотренном разделом 8 настоящего Договора.

9.5. Подписав настоящий Договор, Клиент выражает свое согласие на передачу и прием электронных документов в рамках дистанционного банковского обслуживания с использованием Системы ДБО «iBank2» на условиях, предложенных Банком.

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

10. Юридические адреса и реквизиты Сторон

БАНК:

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

КЛИЕНТ:

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

От БАНКА:

_____/_____/_____
М.П.

От КЛИЕНТА:

_____/_____/_____

ПОЛОЖЕНИЕ **о порядке проведения технической экспертизы при возникновении спорных ситуаций**

1. В настоящем «Положении о порядке проведения технической экспертизы при возникновении спорных ситуаций» (далее – Положение) под спорной ситуацией понимается существование претензий у Клиента к Банку (вместе в дальнейшем именуется Сторонами), справедливость которых может быть однозначно установлена в результате проверки Электронных документов, подписанных ПЭП.

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

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

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

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

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

7. В результате рассмотрения спорной ситуации разрешительная комиссия должна определить подлинность и принадлежность Клиенту ПЭП в приложенном Электронном документе и обоснованность выполнения Банком операций по счёту Клиента.

8. Разрешительная комиссия проводит рассмотрение заявления в срок не более пяти рабочих дней с момента формирования комиссии.

9. Разрешительная комиссия проводит проверку подлинности и принадлежности Клиенту ПЭП в оспариваемом документе.

10. На основании данных проверки разрешительная комиссия составляет акт, содержащий

– фактические обстоятельства, послужившие основанием возникновения разногласий;

– все реквизиты оспариваемого документа;

– порядок работы членов комиссии;

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

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

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

13. В случае, когда Банк предъявляет Электронный документ, а также подлинность и принадлежность Клиенту ПЭП, которая признана разрешительной комиссией, Банк не несёт ответственности перед Клиентом по выполненным операциям по счёту Клиента.

14. Если Клиент настаивает на том, что данный документ он не создавал или не подписывал ПЭП, разрешительная комиссия может вынести определение о Компрометации ПЭП Клиента, что не снимает с Клиента ответственности за данный документ.

ПЕРЕЧЕНЬ¹

Электронных документов, передаваемых по Системе ДБО

1. Платежное поручение;
2. Заявление на перевод иностранной валюты;
3. Поручения на продажу иностранной валюты;
4. Поручения на покупку иностранной валюты;
5. Поручения на конвертацию иностранной валюты;
6. Отзыв;
7. Письмо.

¹ Перечень может быть дополнен при заключении договора.

ПОЛОЖЕНИЕ о порядке и способах информирования клиента о совершенных операциях с использованием Системы ДБО «iBank2»

1. Способы информирования Клиента.

1.1. В целях исполнения требований Федерального закона от 27.06.2011 г. № 161-ФЗ «О национальной платежной системе» Банк осуществляет информирование Клиента о совершенных операциях одним или несколькими из указанных ниже способов:

1.2. Путем отправки SMS-сообщения на указанный Клиентом телефонный номер Мобильного устройства, зарегистрированного в Российской Федерации. Обязанность Банка по информированию Клиента считается исполненной Банком при направлении SMS-сообщения о совершенной операции на телефонный номер Мобильного устройства, указанный Клиентом.

1.3. Путем отправки сообщения электронной почты на указанный Клиентом адрес электронной почты. Обязанность Банка по информированию Клиента считается исполненной Банком при направлении сообщения электронной почты о совершенной операции на адрес электронной почты, указанный Клиентом.

1.4. Путем изменения статуса, соответствующего ЭД в Системе «iBank2». Присвоение ЭД в Системе ДБО статуса «Доставлен» подтверждает получение Банком распоряжения Клиента. Присвоение ЭД в Системе ДБО статуса «На обработке» / «На исполнении» подтверждает прием Банком распоряжения денежными средствами, находящими на счете Клиента к исполнению. Присвоение ЭД статуса «Исполнен» подтверждает исполнение Банком распоряжения денежными средствами, находящими на счете Клиента. Присвоение ЭД статуса «Отвергнут» подтверждает отказ Банка в принятии к исполнению распоряжения денежными средствами, находящими на счете Клиента. Обязанность Банка по информированию Клиента считается исполненной Банком при изменении статуса ЭД в Системе ДБО.

1.5. Банк обязан проинформировать Клиента о совершенных операциях с использованием электронного средства платежа не позднее, чем через 24 (Двадцать четыре) часа после совершения соответствующей операции.

1.6. Способ информирования, указанный в п. 1.1 Положения, является основным способом и применяется Банком для информирования Клиента о:

- получении Банком распоряжения денежными средствами, находящими на счете для осуществления перевода денежных средств [при информировании Клиента о получении ЭД и установке статуса «Доставлен»];
- принятии Банком распоряжения денежными средствами, находящими на счете для осуществления перевода денежных средств к исполнению [при информировании Клиента о получении ЭД и установке статуса «На обработке» / «На исполнении»];
- исполнении Банком распоряжения денежными средствами, находящими на счете для осуществления перевода денежных средств [при информировании Клиента о получении ЭД и установке статуса «Исполнен»];
- аннулировании Банком распоряжения денежными средствами, находящими на счете для осуществления перевода денежных средств [при информировании Клиента о получении ЭД статуса «Отвергнут»].

1.7. Способ информирования, указанный в п. 1.2 Положения, является дополнительным способом информирования Клиента об исполнении Банком распоряжения денежными средствами, находящими на счете для осуществления перевода денежных средств.

1.8. Указанные способы информирования осуществляются Банком в случае, если Клиентом в Системе ДБО выбран (ы) необходимый (ые) способ (ы) уведомления (sms, e-mail). Изменение статуса ЭД производится автоматически.

2. Состав информации при информировании Клиента.

2.1. Уведомление в виде SMS-сообщения и/или сообщения электронной почты может включать следующие реквизиты:

- наименование Банка,
- идентификатор Клиента,
- вид операции,
- дата операции,
- сумма операции,
- валюта операции,
- дополнительная информация о контрагенте,
- идентификатор устройства при его применении для осуществления операции с использованием ЭСП,
- иная информация при наличии технической возможности.

3. Права и обязанности Сторон.

3.1. Клиент обязан предоставить Банку достоверную информацию для связи с ним.

3.2. Клиент обязан предоставить в Банк письменное заявление в случае изменения телефонного номера Мобильного устройства и/или адреса электронной почты, на которые Банком направляются уведомления о совершенных операциях. Все риски, связанные с несвоевременным предоставлением информации об изменении телефонного номера мобильного устройства и/или адреса электронной почты, несет Клиент.

3.3. Обязанность Банка по информированию Клиента считается исполненной надлежащим образом при направлении сообщений на известный Банку телефонный номер мобильного устройства и/или адрес электронной почты, если на дату отправки таких сообщений Банк не получил заявление Клиента об изменении номера мобильного устройства/адреса электронной почты.

3.4. Клиент обязан не реже одного раза в сутки проверять поступающие на номер мобильного устройства SMS-сообщения и/или сообщения электронной почты, проверять информацию об операциях, размещаемую Банком в Системе ДБО.

3.5. Клиент обязан самостоятельно обеспечить поддержку функции приема SMS-сообщений на своем мобильном телефоне, работоспособность своей электронной почты.

3.6. 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 совершенных операциях.

3.7. Клиент обязан самостоятельно обеспечить доступность получения SMS-сообщений у своего оператора мобильной связи при нахождении мобильного устройства в междугороднем или международном роуминге.

3.8. Клиент вправе в любой момент изменить телефонный номер телефона, на который осуществляется уведомление в виде SMS-сообщения или адрес электронной почты, предоставив Банку обновленную информацию, установленным Банком способом.

3.9. Банк имеет право проводить работы по техническому обслуживанию Системы ДБО, программно-аппаратных средств, систем, обеспечивающих отправку ЭД. На период проведения указанных мероприятий работа Клиента с Системой может быть приостановлена.

4. Ответственность Сторон.

4.1. В случае не предоставления Клиентом в Банк достоверной информации о номере мобильного устройства и/или адресе электронной почты, Клиент признается не предоставившим надлежащим образом информацию для связи с Клиентом, и Банк вправе заблокировать доступ Клиента к Системе ДБО и/или расторгнуть Договор с Клиентом.

4.2. В случае если Клиент предоставил неверные сведения о номере мобильного устройства и/или адресе электронной почты для осуществления Банком информирования о совершенных операциях и/или номер мобильного устройства и/или адрес электронной почты не используется (блокирован/отключен и др.), Банк не несет ответственности за неисполнение обязанности по направлению уведомления Клиенту этими способами.

4.3. Банк не несет ответственности в случае неполучения Клиентом SMS-сообщения и/или сообщения электронной почты о совершенной операции, за неосуществление просмотра Клиентом списка операций в Системе ДБО «iBank2».

4.4. Для получения SMS – сообщений Клиент самостоятельно обеспечивает поддержку функции SMS на своем мобильном телефоне, а также подписку на услугу SMS у своего оператора мобильной связи. В случае неполучения SMS -сообщения не по вине Банка, Банк не несет ответственности за неполучение SMS-сообщения (отключение данной услуги соответствующим оператором мобильной связи, недоставка сообщения оператором мобильной связи, изменение номера телефона Клиентом без соответствующего уведомления Банка и т.д.). То же в отношении сообщений электронной почты.

5. Иные условия.

5.1. Клиент согласен на передачу информации, связанной с операциями по его Счету, путем отправки SMS-сообщений и/или сообщений электронной почты. Клиент дает свое согласие на передачу информации о номере мобильного устройства и адресе электронной почты третьим лицам (провайдерам услуг) в целях информирования Клиента о совершенных операциях.

Требования Системы ДБО «iBank2»

Для работы с Системой «Интернет-Банк iBank 2» пользователю необходимы:

1. Любой современный компьютер с объемом свободной оперативной памяти не менее 128 Мбайт.
2. Любая современная операционная система: Windows, Mac OS X, Linux и др. (Далее ОС).
3. Любой современный web-браузер: Microsoft Internet Explorer, Mozilla Firefox, Opera, Google Chrome, Safari.
4. Доступ в сеть Интернет.

ЗАЯВЛЕНИЕ

о регистрации телефонного номера Мобильного устройства
(в качестве средства получения кодов подтверждения, паролей)

Ф.И.О. Клиента: _____

Данные документа, удостоверяющего личность: _____

Прошу ООО КБ «Столичный Кредит» с «__» _____ 20__ г. **зарегистрировать** в Системе ДБО «iBank2» телефонный номер мобильного устройства (____) ____ - ____ - ____ в качестве средства получения Кодов подтверждения.

Настоящим подтверждаю принадлежность мне указанного телефонного номера Мобильного устройства и согласие на получение Кодов подтверждения на указанный номер.

_____ (_____)

(подпись) (Ф.И.О.)

«__» _____ 20__ г.

Отметка Банка:

Заявление принято к исполнению в ООО КБ «Столичный Кредит» " ____ " _____ 20__ г. в ____ : ____

_____ (_____)

(подпись) (Ф.И.О.)

Уведомление

о прекращении регистрации телефонного номера Мобильного устройства
(в качестве средства получения кодов подтверждения, паролей)

Ф.И.О. Клиента: _____

Данные документа, удостоверяющего личность: _____

Прошу ООО КБ «Столичный Кредит» с «__» _____ 20__ г. **прекратить регистрацию** в Системе ДБО «iBank2» телефонного
номер мобильного устройства (____) ____ - ____ - ____ в качестве средства получения Кодов подтверждения.

Настоящим подтверждаю принадлежность мне указанного телефонного номера Мобильного устройства и согласие на прекращение
регистрации указанного телефонного номера в Системе ДБО «iBank2».

_____ (_____)

(подпись) (Ф.И.О.)

«__» _____ 20__ г.

Отметка Банка:

Заявление принято к исполнению в ООО КБ «Столичный Кредит» " ____ " _____ 20__ г. в __ : ____

_____ (_____)

(подпись) (Ф.И.О.)

Рекомендации для работы с Системой ДБО «iBank 2»

1. Механизмы защиты информации в Системе ДБО:

- 1.1. Система ДБО «iBank 2» относится к классу систем защищенного электронного документооборота.
- 1.2. Для обеспечения аутентичности (доказательства авторства) и целостности документа используется механизм ПЭП электронных документов.
- 1.3. Для обеспечения конфиденциальности используется механизм шифрования данных. При взаимодействии через Интернет осуществляется шифрование и контроль целостности передаваемой информации, проводится криптографическая аутентификация сторон.
- 1.4. В Системе ДБО ведутся контрольные архивы, в которых хранятся все электронные документы с ЭП для разрешения конфликтных ситуаций. В системе ведется история документов - кем и когда документ был создан, отредактирован, подписан, исполнен или отвергнут.

2. Механизмы безопасности клиентов:

- 2.1. SMS-информирование клиентов о входе в Систему ДБО, о поступлении в Банк платежных документов, о движении средств по счетам клиентов.
- 2.2. Расширенная многофакторная аутентификация при входе в Систему ДБО с использованием одноразовых паролей.
- 2.3. Механизм дополнительного подтверждения платежных поручений одноразовыми паролями.
- 2.4. В качестве источников одноразовых паролей в Системе ДБО используются SMS-сообщения.

3. Меры безопасности при работе с ЭП:

- 3.1. Не допускается сохранять данные для подписи ПЭП в местах, где к ним может получить доступ кто-либо, кроме Вас;
- 3.2. Данные для подписи ПЭП должны быть известны только Вам как владельцу;
- 3.3. Не пользуйтесь Системой ДБО в Интернет-кафе, а также там, где Вы не уверены в безопасности компьютеров;
- 3.4. При возникновении любых подозрений на компрометацию ПЭП или компрометацию среды исполнения (наличие в компьютере вредоносных программ) – обязательно сообщить в Банк и заблокировать использование ПЭП.

4. Меры по защите компьютера, с которого осуществляется работа в Системе ДБО:

- 4.1. Соблюдайте регламент ограниченного физического доступа к данному компьютеру.
- 4.2. Рекомендуется использовать отдельный компьютер исключительно для работы в Системе ДБО. Другие действия (работа с другими программами, работа с электронной почтой, посещение сайтов в Интернете) с этого компьютера осуществляться не должны.
- 4.3. Используйте в работе только лицензионное ПО. Не загружайте и не устанавливайте ПО полученное из непроверенных источников.
- 4.4. Старайтесь использовать современные операционные системы (ОС). Данные системы являются более защищенными, в отличие от предыдущих, зачастую устаревших версий. Своевременно устанавливайте исправления и обновления для ОС. Включите автоматическое обновление ОС, которое будет устанавливать последние исправления, тем самым ликвидируя уязвимости ОС.
- 4.5. Используйте системное и прикладное ПО только из доверенных источников, гарантирующих отсутствие вредоносных программ. При этом необходимо обеспечить целостность получаемых на носителях или загружаемых из Интернета обновлений.
- 4.6. Используйте и оперативно обновляйте специализированное ПО для защиты информации - антивирусное ПО, персональные межсетевые экраны, средства защиты от несанкционированного доступа и пр.
- 4.7. Не подключайте к компьютеру непроверенные на наличие вирусов отчуждаемые носители.
- 4.8. Регулярно проверяйте Ваш компьютер на вирусы, как минимум раз в неделю.

5. Правила безопасной работы в Интернете:

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

6. Меры по безопасному использованию ПЭП:

- 6.1. При использовании web-браузера в качестве интерфейса для осуществления доступа к сервису ПЭП отключите функции автоматического сохранения пароля и логина. *(По умолчанию эта опция может быть включена во многих популярных браузерах, служит она для повышения удобства, однако в ущерб безопасности).*
- 6.2. Используйте и оперативно обновляйте специализированное ПО для защиты информации - антивирусное ПО, персональные межсетевые экраны, средства защиты от несанкционированного доступа и пр. *(По мимо стандартного функционала защиты компьютера от вирусов, во многие современные антивирусные продукты встроены дополнительные фичи безопасности, как то модули анти-фишинга, контроля целостности настроек браузера, проверка защищенных соединений. возможности вводить пароль используя виртуальную клавиатуру, которая появляется на странице авторизации. Это обеспечивает защиту от кейлоггеров и троянов – программ, записывающих и отправляющих злоумышленнику данные введенные пользователями с клавиатуры).*
- 6.3. Убедитесь в том, что на страничке авторизации используется защищенный протокол HTTPS, обеспечивающий шифрованную передачу данных от пользователя к серверу. Так же обращайте внимание на сертификат сайта, подтверждающий его легитимность. *(как правило это выглядит в виде небольшой иконки с изображением зеленого замочка рядом с URL-адресом открытой страницы, щелкнув по которому можно получить дополнительную информацию).*
- 6.4. При использовании смартфонов, планшетов как средства доступа будьте уверены в том, что вы не используете «рутованную» версию прошивки Android или установленный Jailbreak для гаджетов от Apple. Модифицированные и не поддерживаемые официальным производителем прошивки для смартфонов могут содержать в себе закладки или недокументированные возможности, которые злоумышленник при определенных условиях с успехом сможет использовать. Не устанавливайте приложения из посторонних источников, а по возможности вообще минимизируйте список софта, который у вас будет установлен на телефоне или планшете.
- 6.5. Не при каких обстоятельствах никогда не сообщайте посторонним лицам, в том числе работникам Банка или службе поддержке, никаких кодов, SMS-сообщений, парольных и контрольных фраз. Все действия, предусмотренные услугой (сервисом), которые вы можете делать должны выполнять только лично Вами без каких-либо посредников. Исключение составляет только первичная идентификация вас как клиента, к примеру, по паспортным данным и ключевой фразе.
- 6.6. Руководства пользователя по использованию ПО и ДБО, а также можно получить в службе поддержки Банка, в электронном виде в Системе ДБО и на официальном сайте Банка www.capitalkredit.ru.

От имени Клиента

Приложение № 8
к Договору обмена электронными документами
с использованием системы дистанционного банковского
обслуживания «iBank 2» (для физических лиц)
№ _____ от «__» _____ 20__ г

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

(ФИО Клиента)

(паспортные данные)

(адрес места нахождения Клиента)

ИНН _____

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

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

(ФИО Клиента) _____
(подпись)

Дата: _____

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

Настоящее Заявление действует до момента его отзыва Клиентом.

Заполняется работником Банка

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

(наименование должности работника Банка) _____
(подпись) _____
(ФИО)

Памятка Клиенту об обеспечении информационной безопасности

Следуя приведенным ниже рекомендациям, Вы максимально обезопасите себя от действий злоумышленников и вредоносного программного обеспечения.

1. Необходимо соблюдать принципы обеспечения информационной безопасности с целью защиты информации от воздействия вредоносного кода и исключения случаев несанкционированного доступа к счетам Клиента, с целью недопущения осуществления переводов денежных средств лицами, не обладающими правом распоряжения этими денежными средствами.

2. Средства и методы защиты информации, применяемые в Банке, позволяют обеспечить необходимый уровень безопасности при осуществлении переводов денежных средств и предотвратить мошеннический вывод денежных средств со счетов клиентов при условии выполнения Клиентами рекомендаций, изложенных в данном документе.

3. Операционные системы устройств, расположенных на Рабочем месте Клиента (совокупность программного и аппаратного средства (компьютер или Мобильное устройство), с которого осуществляется доступ Клиентом к Системе ДБО) и приложения на сегодняшний день, имеют различные инструменты для защиты персональных данных и денежных средств, но ключевая роль в обеспечении безопасной работы принадлежит пользователю.

4. Установите лицензионное средство защиты от вредоносного кода или защитное программное обеспечение и регулярно обновляйте его.

5. Скачивайте и устанавливайте лицензионное программное обеспечение из проверенных источников (рекомендованных производителями устройств, в том числе мобильных).

6. Используйте только последние версии браузера. Регулярно (не реже чем ежедневно) в автоматическом режиме производите обновление браузера.

7. На устройствах, используемых для работы с приложением, не рекомендуется выполнять процедуры получения доступа к файловой системе устройства (Jailbreak, Rooting). Такие операции наносят существенный ущерб системе безопасности, предоставленной производителем устройства.

8. Скачивайте и устанавливайте приложение "iBank для жизни" только из официальных магазинов приложений Google Play, App Store. Разработчик приложения должен быть указан как "БИФИТ".

9. Не записывайте и не сохраняйте свой код доступа к приложению, долговременный пароль и данные учетной записи.

10. Не сообщайте код доступа третьим лицам, в том числе работникам Банка.

11. При получении любых сообщений или писем, связанных с работой приложения, обращайтесь к отправителю. Подобные сообщения должны поступать только с официального сервисного номера или адреса электронной почты вашего Банка. Банк не осуществляет рассылку электронных писем с просьбой прислать логин, долговременный пароль, код подтверждения и никогда не запрашивает у Клиентов эту информацию.

12. Запрещается выполнять указания, в случае получения Клиентом такого письма от имени Банка, содержащего ссылку на установку программы, программу для установки или запрос на предоставление логина, долговременного пароля, кода подтверждения, используемых Клиентом в Системе ДБО. О произошедшем необходимо незамедлительно сообщить в ваш Банк по предоставленным им номерам телефонов, также обозначенными на сайте Банка.

13. Не переходите по ссылкам и не открывайте вложения из писем от подозрительных или неизвестных отправителей.

14. После завершения работы с документами и банковскими счетами каждый раз выполняйте выход из приложения (Меню → Выход).

15. При подозрении, что ваш код доступа к приложению стал известен посторонним лицам или при получении уведомлений об операциях по счету, которых Вы не совершали, немедленно обратитесь в Банк и заблокируйте свою учетную запись.

16. Не назначать долговременный пароль, используемый в Системе ДБО, в любых других системах и сервисах.

17. Пароль должен состоять из комбинации следующих символов: прописные и строчные латинские буквы, цифры. Необходимо выбирать трудно подбираемые пароли. При выборе паролей не должна использоваться какая-либо «система»: новый пароль не должен быть прогнозируемым на основе знаний о предыдущих паролях, датах их смены. Новый пароль не должен совпадать ни с одним из предыдущих паролей. Новый пароль должен отличаться от предыдущего не менее чем в четырех символах. Включать в пароль ассоциируемую с Клиентом или Рабочим местом информацию, которую легко узнать: Ф.И.О. Клиента или его ближайших родственников, марку автомобиля, кличку домашнего животного, название в локальной сети, полное или сокращенное наименование Банка, название сервера.

18. Исключите доступ к Рабочему месту лиц, не имеющих отношения к работе с Системой ДБО.

19. Не устанавливайте на Рабочем месте средства разработки программного обеспечения и отладчики программного обеспечения.

20. В случае передачи (списания, утилизации и т.п.) сторонним лицам стационарного Рабочего места, ноутбука или мобильного устройства, на котором ранее была установлена Система ДБО, необходимо гарантированно удалить с него всю информацию, использование которой третьими лицами может потенциально нанести вред Вашей финансовой деятельности как Клиента.

21. На Рабочем месте установите только одну операционную систему.

22. Не используйте Рабочее место в публичных (проводных/беспроводных) сетях, предоставляющих доступ к сети Интернет, для исключения значительного повышения риска компрометации логина и долговременного пароля, используемых в Системе ДБО.

23. Не допускайте установку на Рабочее место никаких программ для удаленного управления (Team Viewer, Ammyu Admin, AnyDesk, VNC и т.п.), заблокируйте на нем работу встроенного сервиса удаленного доступа к рабочему столу.

Прошито, пронумеровано и скреплено печатью
17 (семнадцать) листов

Председатель Правления


И.В. Чурюмов

