УТВЕРЖДЕНО
Совет директоров
ООО КБ «Столичный Кредит»
Протокол от «26» июля 2022г.

Правила электронного документооборота в системе электронного банкинга «iBank2» ООО КБ «Столичный кредит».

г. Москва
2022 г.

Содержание

1. **ОБЩИЕ ПОЛОЖЕНИЯ** 2
2. **ЭЛЕКТРОННЫЙ ДОКУМЕНТ** 6
3. **ОРГАНИЗАЦИЯ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА** 7
4. **ПОРЯДОК ОБМЕНА ЭЛЕКТРОННЫМИ ДОКУМЕНТАМИ И ИНФОРМАЦИЕЙ В СИСТЕМЕ ДБО «IBANK2** 9
5. **ПОРЯДОК ИНФОРМИРОВАНИЯ КЛИЕНТОВ О СОВЕРШЕННИИ ОПЕРАЦИЙ В СИСТЕМЕ ДБО «IBANK2»** 11
6. **СИСТЕМА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ** 12
7. **ЧРЕЗВЫЧАЙНЫЕ СИТУАЦИИ ПРИ ОСУЩЕСТВЛЕНИИ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА** 13
8. **ПОРЯДОК РАЗРЕШЕНИЯ КОНФЛИКТНЫХ СИТУАЦИЙ И СПОРОВ, ВОЗНИКШИХ В СВЯЗИ С ОСУЩЕСТВЛЕНИЕМ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА В СИСТЕМЕ ДБО «IBANK2»** 15
9. **ИНЫЕ ПОЛОЖЕНИЯ**..... 16

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящий документ определяет: правила обмена электронными документами в рамках дистанционного банковского обслуживания при работе в системе электронного банкинга «iBank2» (далее по тексту Система ДБО «iBank2»).

1.2. Текст настоящих Правил публикуется на официальном сайте Банка по адресу www.capitalkredit.ru (далее – официальный сайт Банка) и размещается на информационных стендах в офисах Банка и может быть выдан Клиенту на бумажном носителе при личном обращении Клиента в Банк.

1.3. **Термины и определения**

АБС – автоматизированная банковская система, используемая Банком

Аутентификация – выполняемая средствами Системы ДБО «iBank2» процедура проверки подлинности и принадлежности Клиенту введенного им имени пользователя (задействованного ключа ЭП) и пароля в Системе ДБО «iBank2». Банком обеспечивается аутентификация входящих электронных документов и взаимная (двусторонняя) аутентификация Банка и Клиента.

Банк – Общество с ограниченной ответственностью Коммерческий Банк «Столичный кредит» (ООО КБ «Столичный Кредит»).

Банковский счет – счет, открытый Клиенту на основании договора банковского счета в валюте Российской Федерации или иностранной валюте для осуществления операций, разрешенных действующим законодательством РФ.

Владелец открытого ключа электронной подписи – лицо, на имя которого Банком зарегистрирован открытый ключ электронной подписи и которое владеет соответствующим закрытым ключом электронной подписи, позволяющим создавать свою электронную подпись в электронных документах (подписывать электронные документы электронной подписью).

Договор обмена электронными документами с использованием системы электронного банкинга "iBank2"(для юридических лиц и индивидуальных предпринимателей) (далее - Договор) – договор между Банком и Клиентом об использовании Системы ДБО «iBank2», включающий в качестве составных и неотъемлемых частей Тарифы и комиссии Банка.

Защита информации – комплекс организационно-технических мероприятий, проводимых Банком с целью предотвращения утечки, хищения, утраты, несанкционированного уничтожения, изменения, модификации (подделки), несанкционированного копирования, блокирования информации.

Заявление - Заявление о подключении к системе iBank2 (Приложение №1 к Договору обмена электронными документами с использованием системы электронного банкинга "iBank2")

Информация – сведения, сообщения, данные, обрабатываемые в Системе ДБО «iBank2».

Клиент (корпоративный клиент) – юридическое лицо, индивидуальный предприниматель, физическое лицо, занимающееся в установленном законодательством Российской Федерации порядке частной практикой (нотариус, адвокат), физическое лицо, находящиеся на обслуживании в Банке и имеющие на момент присоединения к Правилам открытые Банковские счета.

Ключ проверки ЭП – (открытый ключ) – уникальная последовательность символов, однозначно связанная с ключом электронной подписи и предназначенная для проверки подлинности электронной подписи (далее - проверка электронной подписи). В целях настоящих Правил - ключ (последовательность байт), зависящий от Ключа ЭП Клиента, самостоятельно формируемый Клиентом в Системе ДБО «iBank2» с использованием СКЗИ (средства криптографической защиты информации) или с использованием защищенных ресурсов (облачное хранилище), и предназначенный для проверки Банком подлинности ЭП в документе, сформированном Клиентом.

Ключ ЭП – (закрытый ключ) – уникальная последовательность символов, предназначенная для создания электронной подписи. В целях настоящих Правил - ключ (последовательность байт), самостоятельно формируемый Клиентом с использованием программных средств Системы ДБО «iBank2» и предназначенный для авторизации в Системе ДБО «iBank2» и формирования Клиентом электронной подписи в документах.

Ключевой носитель - физический носитель определенной структуры, предназначенный для размещения на нем ключевой информации (исходной ключевой информации) (USB-токен, смарт-карта).

Код подтверждения – одноразовый код, используемый в целях аутентификации Клиента при осуществлении переводов денежных средств с использованием Системы ДБО «iBank2», а также при подтверждении Клиентом права доступа к Системе ДБО «iBank2», который действителен на протяжении ограниченного периода времени. Код подтверждения используется для подтверждения Клиентом права доступа к Системе ДБО «iBank2» или для подтверждения распоряжения (нескольких распоряжений) о переводе денежных средств. Код подтверждения однозначно соответствует сеансу использования Системы ДБО «iBank2» или распоряжению (распоряжениям, договору), подтверждаемому (подтверждаемым) Клиентом с использованием Системы ДБО «iBank2». Код подтверждения доводится до Клиента по альтернативному к Системе ДБО «iBank2» каналу связи. В Системе ДБО «iBank2» применяется одноразовая динамическая последовательность цифровых символов (от 4 до 6) которая направляется Клиенту посредством SMS-сообщения на номера мобильных телефонов, указанных в Заявлении о присоединении к Правилам; Срок действия Кода подтверждения составляет 5 (пять) минут, по истечении указанного срока Код подтверждения становится недействительным. В сообщении, передаваемом для подтверждения распоряжения о переводе денежных средств, содержатся сведения о сумме и получателе денежных средств.

Компрометация Ключа ЭП (нарушение конфиденциальности Ключа ЭП) – констатация обстоятельств, при которых возможно несанкционированное использование Ключа ЭП неуполномоченными лицами и/или произошла утрата доверия к тому, что используемый Ключ ЭП обеспечивает безопасность информации. В частности, к событиям, связанным с компрометацией Ключа ЭП, относятся следующие события:

- утрата ключевого носителя, в том числе с его последующим обнаружением;
- увольнение или перевод в другое подразделение сотрудников Клиента, имевших доступ к ключевому носителю;
- нарушение правил хранения Ключа ЭП;
- возникновение подозрений, что Ключ ЭП стал доступен третьим лицам, а также об утечке информации или ее искажении в системе конфиденциальной связи;
- случаи, когда нельзя достоверно установить, что произошло с ключевыми носителями (в том числе случаи, когда ключевой носитель вышел из строя и достоверно не опровергнута возможность того, что данный факт произошел в результате несанкционированных действий злоумышленника);
- факт или попытка несанкционированного списания денежных средств со счета Клиента с использованием рабочих пары ключей ЭП;
- факты или попытки информирования посторонних лиц о кодах, смс-сообщений, парольных и контрольных фраз при использовании облачной подписи. Выполнение действий, предусмотренных услугой (сервисом) посторонними лицами;
- иные обстоятельства, прямо или косвенно свидетельствующие о доступе или возможности доступа к содержимому ключа ЭП неуполномоченных лиц.

Операционное время – время, в течение которого поступившие от Клиента по Системе ДБО «iBank2» платежные документы принимаются Банком в обработку, исполняются и отражаются по счетам бухгалтерского учета. Для различных Операций, осуществляемых с использованием Системы ДБО «iBank2», Операционное время может отличаться. Информацию об установленном Операционном времени Банк указывает в Тарифах, размещенных на официальном сайте www.capitalkredit.ru.

Операция – действия, осуществляемые Банком с денежными средствами Клиента на его Банковских счетах на основании электронного документа, переданного Клиентом в Банк с использованием Системы ДБО «iBank2» в порядке, установленном настоящими Правилами, и содержащего указание на распоряжение денежными средствами Клиента.

Платежные документы - платежные поручения, инкассовые поручения, платежные требования, платежные ордера, банковские ордера, составленные в соответствии с «Положением о правилах осуществления перевода денежных средств» (утв. Банком России 29.06.2021 N 762- П).

Платежный ЭД – платежный документ, оформленный в виде электронного документа.

Послеоперационное время – время, в течение которого поступившие от Клиента по Системе ДБО «iBank2» ЭД по определенным типам Операций принимаются Банком в обработку, но исполняются не в день получения, а на следующий рабочий день.

Признаки осуществления перевода денежных средств без согласия клиента – совокупность признаков, при наличии которых Банк имеет основания заподозрить, что перевод денежных средств осуществляется без ведома и согласия Клиента. Признаки осуществления перевода денежных средств без согласия клиента устанавливаются Банком России (Приказ Банка России от 27 сентября 2018 года N ОД-2525) и размещаются на его официальном сайте в информационно-телекоммуникационной сети Интернет. Банк в рамках реализуемой им системы управления рисками определяет в документах, регламентирующих процедуры управления рисками, процедуры выявления операций, соответствующих признакам осуществления переводов денежных средств без согласия клиента, на основе анализа характера, параметров и объема совершаемых его клиентами операций (осуществляемой клиентами деятельности).

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

Распоряжения - распоряжения о переводе денежных средств, составляемые плательщиками, получателями средств, а также лицами, органами, имеющими право на основании закона предъявлять распоряжения к банковским счетам плательщиков (далее - взыскатели средств), банками.

Сертификат ключа проверки электронной подписи (СКП ЭП) – электронный документ или документ на бумажном носителе, выданный уполномоченными организациями, осуществляющими функции по созданию и выдаче сертификатов ключей проверки электронных подписей, и подтверждающие принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи. В целях настоящих Правил - электронный документ и соответствующий ему документ на бумажном носителе, заверенный подписью руководителя Клиента и оттиском печати в соответствии с указанными в карточке с образцами подписей и оттиска печати Клиента с одной стороны и Уполномоченными сотрудниками Банка с другой. Сертификат ключа проверки ЭП Клиента содержит информацию:

- о номере ключа ЭП;
- о дате начала и окончания срока его действия;
- о наименовании и месте регистрации Клиента;
- о Владельце ключа ЭП (ФИО, должность, паспортные данные);
- о стандартах, требованиям которых соответствует пара ключей (ключ ЭП и ключ проверки ЭП).

Система дистанционного банковского обслуживания «iBank2» (далее – Система ДБО «iBank2») – система дистанционного банковского обслуживания «Банк-Клиент «iBank2», представляющая собой комплекс программно-аппаратных средств, устанавливаемых, и согласовано эксплуатируемых Клиентом и Банком, обеспечивающих подготовку, защиту, передачу Клиентом в Банк ЭД, обработку Банком ЭД, формирования Банком и предоставления Клиенту выписок о

движении денежных средств и прочих сообщений с использованием электронно-вычислительных средств обработки информации.

Средства криптографической защиты информации (СКЗИ) – совокупность программно-технических средств, обеспечивающих применение ЭП и шифрования при организации электронного документооборота. В качестве СКЗИ могут применятся аппаратные Ключевые носители, обеспечивающие генерацию Ключа ЭП Клиента по российскому криптографическому алгоритму ГОСТ Р34.10-2012 непосредственно внутри самого устройства и неизвлекаемость (невозможность считывания) закрытого ключа ЭП клиента.

Статус ЭД – реквизит ЭД, характеризующий стадию его обработки Банком и отображающийся в Системе ДБО «iBank2». Например, «Новый», «Доставлен», «Принят», «На обработке», «На исполнении», «Исполнен», «Отвергнут» и другие.

Стороны – Банк и Клиент при совместном упоминании.

Электронный документ (далее - ЭД) – документ, представленный в электронной форме, подписанный ЭП, подготовленный и переданный с использованием программного обеспечения Системы ДБО «iBank2» и СКЗИ в соответствии со всеми процедурами защиты информации.

Электронный документооборот (ЭДО) – обмен электронными документами в соответствии с настоящими Правилами.

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. ЭП подтверждает авторство ЭД, созданного в Системе ДБО «iBank2», и является средством проверки неизменности его содержания, так как любое изменение ЭД после его подписания ЭП нарушает целостность ЭП.

Электронная подпись в облаке (Облачная электронная подпись, ОЭП) – вычислительная система, предоставляющая через сеть доступ к возможностям создания, проверки ЭП и интеграции этих функций в бизнес-процессы других систем. Для целей настоящих правил понятие ЭП используется как в первом (электронная подпись), так и во втором (облачная электронная подпись) случае.

SMS-сообщение – сообщение, содержащее информацию для Клиента Банка о различных событиях, связанных с работой Системы ДБО «iBank2», об Операциях, совершенных по Банковскому счету/Платежной карте с использованием Системы ДБО «iBank2», а также сообщения для подтверждения идентификации (аутентификации), и другую информацию, направляемую Банком Клиенту в электронном виде на номер мобильного телефона, указанный в Заявлении о присоединении.

1.4. Регулирование электронного документооборота в системе ДБО «iBank2 осуществляется настоящими Правилами и приложениями к ним.

1.5. Клиент допускается к осуществлению документооборота в системе ДБО «iBank2 после выполнения им всей совокупности следующих действий:

- заключения Договора обмена электронными документами с использованием системы электронного банкинга "iBank2";
- установки необходимых аппаратных средств, клиентского программного и информационного обеспечения (в случае использования клиентом аппаратных ключевых носителей), или генерации ОЭП;
- получения необходимых паролей и идентификаторов для доступа к ДБО у Банка;
- выработки криптографических ключей Клиента;
- регистрации отрытого ключа электронной подписи для уполномоченного лица Клиента.

1.6. Банк вправе вносить изменения в настоящие Правила в одностороннем порядке, о чем сообщает Клиентам не позднее, чем за 5 (пять) календарных дней до даты введения в действие изменений, путем уведомления Клиентов по Системе ДБО «iBank2» и публикации информации на

официальном сайте Банка *(capitalkredit.ru*) и в офисах Банка, за исключением изменений, обусловленных требованиями законодательства Российской Федерации, более ранний срок вступления которых в силу определяется нормативными и правовыми актами Российской Федерации.

1.7. При невозможности обмена ЭД между Банком и Клиентом по Системе ДБО «iBank2» (сбои в работе оборудования, средств связи, приостановление работы Клиента в Системе ДБО «iBank2», отключение Клиента от Системы ДБО «iBank2» и т.п.) расчетно-кассовое обслуживание Клиента осуществляется путем обмена документами на бумажных носителях в соответствии с Договором банковского счета.

1.8. Все Приложения к настоящим Правилам являются его неотъемлемой частью.

2. ЭЛЕКТРОННЫЙ ДОКУМЕНТ

2.1. **Требования, предъявляемые к электронному документу**. Электронный документ, сформированный в Системе ДБО «iBank2», имеет юридическую силу и влечет предусмотренные для данного документа правовые последствия в соответствии с настоящими Правилами. Электронный документ считается надлежащим образом оформленным, при условии его соответствия законодательству Российской Федерации, в том числе нормативным актам Банка России, настоящим Правилам, а также иным договорам, заключаемым между Банком и Клиентом. Электронное сообщение приобретает правовой статус электронного документа при его соответствии настоящим Правилам, а также иным договорам, заключаемым между Банком и Клиентом. Электронный документ должен быть сформирован в одном из форматов, определенных в настоящих Правилах или Приложениям к ним, и подписан электронной подписью. Электронный документ, имеющий формат, не отвечающий установленным правилам, в качестве электронного документа в соответствии с настоящими Правилами не рассматривается.

2.2. **Использование электронной подписи и шифрования в электронном документообороте**. Электронный документ может быть подписан только тем закрытым ключом электронной подписи, для которого Банком зарегистрирован открытый ключ электронной подписи уполномоченного лица Клиента. Электронный документ считается подписанным уполномоченным лицом, если он подписан тем закрытым ключом электронной подписи, для которого Банком зарегистрирован открытый ключ электронной подписи уполномоченного лица Клиента. Замена закрытых ключей электронной подписи не влияет на юридическую силу электронного документа, если он был подписан действующим на момент подписания закрытым ключом электронной подписи в соответствии с настоящими Правилами. У каждого Клиента имеются индивидуальные закрытые ключи электронной подписи, при помощи которых он подписывает ЭД своей электронной подписью. ЭД, содержащий конфиденциальную информацию, подлежит шифрованию. Конфиденциальность ЭД определяется отправителем. При получении зашифрованного ЭД, он расшифровывается в соответствии с применяемой технологией, затем проверяется электронная подпись ЭД. Предусмотренные для данного документа правовые последствия могут наступить, только если получен положительный результат проверки электронной подписи. С целью уменьшения объемов передаваемой информации при транспортировке электронных документов могут использоваться специальные алгоритмы сжатия информации. В случае необходимости, может выполняться шифрование сжатого электронного документа.

2.3. **Использование электронного документа**. Все юридические действия, оформляемые посредством электронных документов в соответствии с настоящими Правилами, а также внутренними нормативными документами Банка, признаются совершенными в письменной форме и не могут быть оспорены только на том основании, что они совершены в электронном виде.

2.4. **Подлинник электронного документа**. Электронный документ может иметь неограниченное количество экземпляров, в том числе выполненных на машиночитаемых носителях различного типа. Для создания дополнительного экземпляра существующего электронного документа осуществляется воспроизводство содержания документа вместе с электронной подписью. Все экземпляры электронного документа являются подлинниками данного электронного документа. Электронный документ не может иметь копий в электронном виде. Подлинник электронного документа считается не существующим в случаях если:

- не существует ни одного учтенного Банком экземпляра данного электронного документа и восстановление таковых невозможно;
- не существует способа установить подлинность электронной подписи, которой подписан данный документ.

2.5. **Копии электронного документа на бумажном носителе**. Копии электронного документа могут быть изготовлены (распечатаны) на бумажном носителе и должны быть заверены собственноручной подписью лица, уполномоченного Банком или Клиентом, являющимся отправителем или получателем ЭД. Копии ЭД на бумажном носителе должны соответствовать требованиям действующего законодательства и государственным стандартам. Электронный документ и его копии на бумажном носителе должны быть аутентичными. Программные средства, осуществляющие преобразование ЭД для изготовления (распечатки) в виде бумажного документа, являются составной частью программного обеспечения, используемого в Системе ДБО «iBank2».

3. ОРГАНИЗАЦИЯ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА.

3.1. Электронный документооборот включает следующие этапы:

1) формирование электронного документа;
2) отправку и доставку электронного документа;
3) проверку электронного документа;
4) подтверждение получения электронного документа;
5) отзыв электронного документа;
6) учет электронных документов (регистрацию входящих и исходящих ЭД);
7) хранение электронных документов (ведение архивов ЭД);
8) создание дополнительных экземпляров электронного документа;
9) создание бумажных копий электронного документа.

3.2. Система ДБО «iBank2» автоматически отображает сведения о текущем этапе (стадии) обработки Клиентом и/или Банком ЭД посредством присвоения ЭД определенного статуса. Статус каждого ЭД, однозначно отражающий текущий этап его обработки Банком, автоматически отслеживается программными средствами Системы ДБО «iBank2» во время сеансов связи, проводимых Клиентом. Свидетельством того, что ЭД принят Банком для проведения процедуры приема к исполнению в соответствии с законодательством РФ и утвержденным в Банке порядком, является присвоение ему в Системе статуса «Доставлен».

3.3. **Формирование электронного документа** осуществляется в следующем порядке:

- ЭД формируется путем заполнения стандартной формы, предусмотренной в Системе ДБО «iBank2» или при загрузке файлов соответствующего формата, сформированных внешними программами. При формировании ЭД Система ДБО «iBank2» осуществляет автоматический контроль присутствия обязательной информации в соответствующих полях формы документа. Ключевыми полями ЭД являются все обязательные для данного вида ЭД реквизиты, без наличия которых надлежащее исполнение ЭД является невозможным.
- Возможно формирование ЭД, не являющегося платежным, в виде текстового (в формате DOC, RTF, TXT и др.) или графического (в форматах PDF, JPEG/JPG, TIF и др.) документа для дальнейшей пересылки в Банк в виде вложения в ЭД «Письмо» или в другие виды ЭД, в которых предусмотрена возможность присоединения файлов.
- Сформированный ЭД подписывается ЭП в количестве и сочетаниях, указанных в Приложении №1 к Договору обмена электронными документами с использованием системы электронного банкинга "iBank2". ЭП подтверждает авторство ЭД, созданного в Системе ДБО «iBank2», и является средством проверки неизменности его содержания. При подписи ЭД с вложенными файлами одновременно подписываются присоединенные к ЭД файлы. ЭД с присоединенными файлами представляет собой единое целое.

3.4. **Отправка и доставка электронного документа**. В отношениях между отправителем и получателем ЭД считается исходящим от Клиента, если электронный документ отправлен:

- самим отправителем;
- лицом, уполномоченным действовать от имени отправителя в отношении данного ЭД;

– информационной системой, используемой отправителем и действующей автоматически.
– подписан с использованием Ключей ЭП Клиента;
– срок действия сертификатов Ключей ЭП, использованных для подписания ЭД не истек;
– Банк не уведомлен о Компрометации ключей ЭП Клиента;
– срок действия полномочий Владельцев ключей ЭП, указанный в документах, представленных Клиентом, и хранящихся в Юридическом деле, не истек;
– ЭД передан в Банк средствами Системы ДБО «iBank2».

ЭД не считается исходящим от отправителя, если:

– получатель знал или должен был знать, в том числе в результате выполнения проверки, о том, что ЭД не исходит от отправителя;
– получатель знал или должен был знать, в том числе в результате выполнения проверки, о том, что получен искаженный ЭД.

В случае положительного результата проверки ЭД присваивается статус «Доставлен» или «На обработке» и он принимается к исполнению. В случае отрицательного результата проверки, ЭД не может быть принят к исполнению и ЭД присваивается статус «Отвергнут».

3.5. Проверка подлинности доставленного электронного документа Проверка электронного документа включает:

– проверку электронного документа на соответствие установленному для него формату;
– проверку подлинности всех электронных подписей электронного документа. В случае положительного результата проверки ЭД, данный электронный документ принимается к исполнению или подлежит дальнейшей обработке. В противном случае данный ЭД считается не полученным, о чем получатель должен послать уведомление отправителю. При получении зашифрованного ЭД, для проведения проверки подлинности ЭД сначала выполняется расшифрование электронного документа. В случае невозможности расшифрования электронного документа получатель должен послать уведомление отправителю с указанием причины неполучения документа.
– проверку соответствия параметров ЭД требованиям Договоров, заключенных между Банком и Клиентом, а также действующему законодательству РФ и нормативным актам Банка России.

3.6. **Подтверждение получения ЭД**. При использовании Клиентом механизма подтверждения ЭД, или, если при анализе поручения выявлены признаки повышенного риска проведения платежа, то для доставки в Банк такого документа Клиенту необходимо указывать Код подтверждения. Код подтверждения может быть получен в SMS-сообщении на номер мобильного телефона, зарегистрированный в Банке, согласно Заявлению о присоединении. ЭД, ожидающий ввода Кода подтверждения, приобретает статус «Требует подтверждения». После успешного ввода Клиентом полученного Кода подтверждения, статус ЭД меняется на «Доставлен».

3.7. **Отзыв электронного документа**. Клиент вправе отозвать отправленный электронный документ путем отправки получателю электронного документа “Уведомление об отзыве”. “Уведомление об отзыве” является документом той же категории, что и отзываемый документ. В “Уведомлении об отзыве” должно указываться основание отзыва электронного документа. Электронный документ может быть отозван отправителем только до начала его исполнения получателем. Порядок отзыва и формат электронного документа, уведомляющего об отзыве ЭД, устанавливается настоящими Правилами.

3.8. **Учет электронных документов**. Учет электронных документов осуществляется путем ведения электронных журналов учета. Технология ведения электронных журналов учета должна включать программно-технологические процедуры заполнения и администрирования электронных журналов и средства хранения этой информации. Программные средства ведения электронных журналов учета являются составной частью программного обеспечения, используемого для организации электронного документооборота. Для выполнения текущих работ по ведению учета электронных документов Системы ДБО «iBank2» Банк и Клиент назначают ответственных лиц.

При учете исходящего электронного документа Банк должен обеспечить учет следующих данных:

– уникальный идентификатор документа;

- идентификатор составителя документа;
- дата и время проставления электронной подписи составителя документа;
- тип и формат документа, определенные в соответствии с Приложениями к настоящим правилам;
- отметка о доставке документа (дата и время доставки документа);
- иные данные по усмотрению Банка.

При учете входящего электронного документа Банк должен обеспечить учет следующих данных:

- уникальный идентификатор документа; – уникальный идентификатор документа при регистрации в Системе ДБО «iBank2»;
- идентификатор составителя документа;
- дата и время проставления электронной подписи составителя документа;
- дата и время получения документа
- тип и формат документа, определенные в соответствии с настоящими правилами;
- иные данные по усмотрению Банка.

Банк должен обеспечить защиту от несанкционированного доступа и непреднамеренного уничтожения и/или искажения учетных данных, содержащихся в электронных журналах учета электронных документов. Срок хранения учетных данных не может быть менее 5 лет.

3.9. **Хранение электронных документов.** Все электронные документы, учтенные в Системе ДБО «iBank2», должны храниться в течение сроков, предусмотренных нормативными документами Банка. Электронные документы должны храниться либо в электронных архивах, либо в виде копий электронных документов на бумажных носителях, заверенных уполномоченным лицом. Электронные документы должны храниться в том же формате, в котором они были сформированы, отправлены или получены. Срок хранения электронных документов не может быть менее 5 (пяти) лет. Хранение электронных документов должно сопровождаться хранением соответствующих электронных или бумажных журналов учета, сертификатов ключей электронной подписи и программного обеспечения, обеспечивающего возможность работы с электронными журналами и проверки электронной подписи хранимых электронных документов. Закрытые ключи шифрования должны храниться в электронных архивах только в случае хранения электронных документов в зашифрованном на этих ключах виде. Хранение электронных документов должно сопровождаться хранением соответствующих открытых ключей электронной подписи для проведения процедуры разрешения конфликтных ситуаций. Обязанности хранения электронных документов и открытых ключей электронной подписи возлагаются на Банк. Для выполнения текущих работ по ведению электронных архивов в подсистемах обработки данных Системы ДБО «iBank2» Банк и Клиенты назначают ответственных лиц. Электронные архивы и архивы бумажных копий электронных документов подлежат защите от несанкционированного доступа и непреднамеренного уничтожения и/или искажения.

4. ПОРЯДОК ОБМЕНА ЭЛЕКТРОННЫМИ ДОКУМЕНТАМИ И ИНФОРМАЦИЕЙ В СИСТЕМЕ ДБО «IBANK2»

4.1. Система ДБО «iBank2» позволяет:

- осуществлять прием от Клиента созданных, подписанных ЭП и отправленных в Банк Платежных ЭД Клиента;
- осуществлять прием от Клиента подписанных ЭП ЭД свободного формата (заявлений, справок, уведомлений, реестров и проч.);
- получать и просматривать информацию (выписки Банка) об Операциях, иные уведомления и извещения, в том числе, направление которых для Банка является обязательным в соответствии с законодательством Российской Федерации;
- осуществлять просмотр информации о ЭД, поступивших в Банк в целях осуществления перевода денежных средств со счетов Клиента, о статусах ЭД, просмотр уведомлений об их исполнении (неисполнении);
- получить доступ к регулярно обновляемым Банком Справочникам кодов SWIFT, БИК и других, используемых в Системе ДБО «iBank2».

4.2. В рамках Системы ДБО «iBank2» Клиент и Банк обмениваются следующими видами ЭД:

- Платежное поручение;
- Платежное требование;
- Инкассовое поручение;
- Заявление об акцепте, отказе от акцепта;
- Заявление о заранее данном акцепте, отмене заранее данного акцепта;
- Заявка на наличные;
- Входящие платежные требования и инкассовые поручения;
- Заявление на перевод валюты;
- Поручение на покупку иностранной валюты;
- Поручение на продажу иностранной валюты;
- Распоряжение на обязательную продажу иностранной валюты;
- Распоряжение на списание с транзитного счета;
- Поручение на конвертацию валюты;
- Запрос на отзыв ЭД;
- Документы, перечисленные в Инструкции Банка России от 16.08.2017 № 181-И «О порядке представления резидентами и нерезидентами уполномоченным банкам подтверждающих документов и информации при осуществлении валютных операций, о единых формах учета и отчетности по валютным операциям, порядке и сроках их представления»;
- Уведомление о зачислении иностранной валюты на транзитный валютный счет Клиента;
- Документы, установленные внутренними Порядками Банка, в целях осуществления контроля за операциями с денежными средствами и иным имуществом, предусмотренными Федеральным законом от 07.08.2001 № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» (далее – Федеральный закон № 115-ФЗ);
- Документы свободного формата (запросы, тексты, сообщения свободного формата);
- Прочие документы и приложения к ним, определенные заключенными сторонами договорами или соглашениями.

4.3. Перечень документов, передаваемых по Системе ДБО «iBank2», Банк вправе изменять в одностороннем порядке, о чем сообщает Клиентам в порядке, установленном п. 1.6. настоящих Правил.

4.4. В Системе ДБО «iBank2» возможно присвоение следующих статусов ЭД:

- «Новый»: присваивается при создании и сохранении нового ЭД, при редактировании и сохранении существующего ЭД, а также при импорте ЭД из файла. ЭД со статусом «Новый» Банк не рассматривает и не обрабатывает;
- «Подписан»: присваивается в случае, если ЭД подписан, но число подписей под документом меньше необходимого. При внесении изменений в документ с таким статусом и его последующем сохранении статус ЭД меняется на «Новый»;
- «Требует подтверждения»: присваивается ЭД после получения необходимого количества подписей в случае использования дополнительных мер защиты для ЭД. Если Клиентом используется механизм подтверждения ЭД, то для доставки в Банк такого документа Клиенту необходимо указывать Код подтверждения. Код подтверждения может быть получен в SMS-сообщении на номер, зарегистрированный в Системе ДБО «iBank2»;
- «Доставлен»: присваивается ЭД, когда число подписей под документом соответствует необходимому для рассмотрения документа Банком, и Клиентом указан верный Код подтверждения, если это требуется в соответствии с настроенными правилами контроля. Статус «Доставлен» является для Банка указанием начать обработку ЭД (исполнить или отвергнуть);
- «На обработке»: присваивается ЭД при его выгрузке в АБС после прохождения всех ее проверок;
- «На исполнении»: присваивается при принятии ЭД к исполнению (проведении Банком процедуры приема к исполнению в соответствии с действующим законодательством РФ и порядком, утвержденном в Банке);

- «В картотеке»: присваивается ЭД при недостаточности средств на Банковском счете. Порядок обработки таких Платёжных ЭД определён действующим договором Банковского счета, законодательством РФ и соответствующими нормативными документами Банка России;
- «На акцепт»: присваивается входящему платежному требованию, когда для его исполнения требуется получение акцепта плательщика;
- «Не акцептован»: присваивается платежному требованию, если Клиентом создано и подписано Заявление об отказе от акцепта;
- «Исполнен»: присваивается ЭД непосредственно после отражения документа в балансе Банка;
- «Отвергнут»: присваивается ЭД, не прошедшему проверку АБС, либо последующую проверку по причине его несоответствия требованиям, установленным действующим законодательством РФ или настоящими Правилами, а также в иных случаях на усмотрение Банка. Клиент может создать новый ЭД на основе отвергнутого или удалить ЭД (статус изменится на «удален»);
- «Удален»: присваивается ЭД, удаленному пользователем. Удалению подлежат только ЭД в статусе «Новый», «Подписан» или «Отвергнут». ЭД в статусе «Новый» и «Подписан» удаляются из системы ДБО «iBank2» безвозвратно. ЭД, удаленные из системы после отвержения, можно просмотреть, используя фильтр в информационной панели интерфейса.

4.5. В отношении платежных ЭД Клиента Банк дополнительно проводит процедуры приема к исполнению, установленные законодательством РФ, правилами осуществления перевода денежных средств и Договором банковского счета.

4.6. Клиент может отозвать отправленный ЭД со статусом «Доставлен», «На обработке» или «На исполнении», направив в Системе ДБО «iBank2» запрос на отзыв с указанием причины отзыва. Отзыв ЭД, подлежащих валютному контролю возможен только в случае, если на момент поступления запроса на отзыв ЭД в подразделение валютного контроля Банка ЭД не принят Банком в соответствии с требованиями валютного законодательства.

4.7. Клиент обязан по рабочим дням, до момента получения информации об исполнении либо об отказе в исполнении ЭД, отслеживать информацию об этапах и результатах обработки ЭД в соответствующих разделах Системы ДБО «iBank2».

4.8. При отсутствии изменения статуса ЭД в течение 2 (двух) часов с момента отправки ЭД в Банк Клиент обязан уведомить Банк о данном факте в день отправки ЭД любым доступным способом, позволяющим идентифицировать Клиента Банка. Банк не несет ответственности за неисполнение неполученных или непринятых ЭД.

4.9. Ответственность за риски, возникающие в случае отсутствия или несвоевременного контроля Клиентом за результатами обработки ЭД, несет Клиент.

4.10. Свидетельством того, что ЭД исполнен Банком, является присвоение ему в Системе ДБО «iBank2» статуса «исполнен». После присвоения статуса «исполнен» ЭД отражается в электронной выписке по Банковскому счету.

4.11. В случае неприятия (отказа в принятии) ЭД Клиента - Клиенту направляется SMS-сообщение об отказе в исполнении ЭД (позволяющее идентифицировать ЭД, дату и основание отказа).

4.12. Прием ЭД, передаваемых Клиентом посредством Системы ДБО «iBank2», производится Банком в автоматическом режиме ежедневно и круглосуточно. Обработка Платежных ЭД и их исполнение в операционное и послеоперационное время осуществляется согласно Тарифам Банка.

5. ПОРЯДОК ИНФОРМИРОВАНИЯ КЛИЕНТОВ О СОВЕРШЕННИИ ОПЕРАЦИЙ В СИСТЕМЕ ДБО «IBANK2»

5.1. Информирование Клиента о совершении Операций в Системе ДБО «iBank2», в соответствии с действующим законодательством Российской Федерации, осуществляется одним из следующих способов по выбору Клиента:

- путем направления SMS-сообщений на телефонный номер, указанный Клиентом в Заявлении;

- путем предоставления через WEB-интерфейс Системы в режиме онлайн информации об Операциях Клиента и их статусе, а также выписок по Банковским счетам Клиента.

5.1.1. Телефонный номер и электронный адрес, указанные в Заявлении, признаются актуальным для Банка для направления сообщений о совершении операций с использованием Системы ДБО «iBank2».

5.1.2. Для получения оперативной информации по совершенным Операциям и остаткам на Банковских счетах, а также для получения информации по Операциям на Банковском счете за конкретный период Клиент имеет возможность получать выписки в соответствующем разделе Системы ДБО «iBank2», указывая номера Банковских счетов и интересующий период.

5.1.3. В случае, если на указанные в Заявлении телефонный номер и электронный адрес, отправка сообщений по каким-либо причинам стала невозможна, Клиент обязан самостоятельно, на регулярной основе (не реже 1 (одного) раза в сутки) производить контроль за произошедшими операциями посредством Системы ДБО «iBank2».

5.1.4. Клиент вправе в любой момент внести изменения в сведения об актуальном номере телефона и электронном адресе, а также способе информирования о совершении Операций, представив в Банк корректирующее Заявление.

5.2. Клиент признает надлежащим способ информирования о совершении Операций, указанный им в Заявлении в соответствии с пунктом 5.1 настоящих Правил.

5.3. Обязанность Банка по информированию Клиента считается исполненной в момент направления Клиенту сообщений в соответствии с выбранным Клиентом способом информирования и при размещении Банком в Системе ДБО «iBank2» информации о совершенных Клиентом Операциях.

5.4. Клиент уведомлен и согласен с тем, что используемые для передачи сообщений телекоммуникационные линии связи являются открытыми и не гарантируют полную защиту информации, передаваемой в рамках настоящих Правил. Клиент согласен с тем, что Банк не несет ответственности за возможное раскрытие информации о состоянии Банковских счетов Клиента, которое может быть вызвано использованием открытых каналов связи.

5.5. Банк не несет ответственности за искажение, непредставление или задержку информации в виде SMS-сообщений, связанное с перебоями в работе операторов сотовой связи и провайдеров сети Интернет, участвующих в доставке информационных сообщений.

6. СИСТЕМА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ.

6.1. Средства обеспечения информационной безопасности Информация, содержащая персональные данные, и конфиденциальная информация в системе электронного документооборота должна быть защищена. Соблюдение требований информационной безопасности при организации электронного документооборота обеспечивает:

- конфиденциальность информации (получить доступ к информации могут только уполномоченные лица);
- целостность передаваемой информации (гарантирование, что данные передаются без искажений и исключается возможность подмены информации);
- аутентификацию (когда передаваемую информацию может получить только то лицо, кому она предназначена, а отправителем является именно тот, от чьего имени она отправлена).

Требования по информационной безопасности при организации электронного документооборота реализуются посредством применения программно-технических средств и организационных мер. К программно-техническим средствам относятся:

- программные средства, специально разработанные для осуществления электронного документооборота;
- система паролей и идентификаторов для ограничения доступа пользователей и операторов к техническим и программным средствам системы электронного документооборота;
- средства электронной подписи;
- средства криптографической защиты информации;

– программно-аппаратные средства защиты от несанкционированного доступа;
– средства защиты от программных вирусов;
– средства защиты от атак.

К организационным мерам относятся:
– размещение технических средств в помещениях с контролируемым доступом;
– административные ограничения доступа к этим средствам;
– задание режима использования пользователями и операторами паролей и идентификаторов;
– допуск к осуществлению документооборота только специально обученных и уполномоченных лиц;
– поддержание программно-технических средств в исправном состоянии;
– резервирование программно-технических средств;
– обучение технического персонала;
– защита технических средств от повреждающих внешних воздействий (пожар, воздействие воды и т.п.).

Порядок использования средств криптографической защиты информации, применяемых в Системе ДБО «iBank2», определяется настоящими Правилами.

6.2. Порядок действий при компрометации криптографических ключей В случае компрометации криптографических ключей владелец скомпрометированных ключей обязан в установленном порядке незамедлительно уведомить Банк о компрометации. Порядок действий при компрометации устанавливается в Приложении к настоящим Правилам (Организация управления ключевыми системами электронного банкинга «iBank2» ООО КБ «Столичный кредит»). В случае получения уведомления о компрометации криптографических ключей, датой и временем компрометации считаются дата и время, указанные в уведомлении о компрометации. Уведомление о компрометации должно быть подтверждено в течение одного рабочего дня официальным уведомлением о компрометации в письменном виде. Уведомление должно содержать:

- идентификационные параметры скомпрометированного закрытого ключа электронной подписи и/или шифрования;
- дату и время, начиная с которого закрытый ключ электронной подписи и/или шифрования считаются скомпрометированными. Дата и время компрометации криптографических ключей, указываемые в уведомлении о компрометации, не могут быть ранее даты и времени получения данного уведомления.

После получения уведомления о компрометации получатель данного уведомления не должен использовать скомпрометированные открытые ключи электронной подписи и/или шифрования при выполнении проверки подлинности электронных документов, полученных после уведомления о компрометации, а также для шифрования новых электронных документов. При получении электронного документа, подписанного скомпрометированным закрытым ключом электронной подписи, данный ЭД считается не полученным.

7. ЧРЕЗВЫЧАЙНЫЕ СИТУАЦИИ ПРИ ОСУЩЕСТВЛЕНИИ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА.

7.1. К числу обстоятельств, которые способны послужить причиной возникновения чрезвычайных ситуаций, в том числе технических сбоев, могут быть отнесены следующие: – любые события и/или обстоятельства, которые, по оценке Банка, временно или на неопределенный срок сделали, делают или могут сделать невозможным или значительно затруднить осуществление электронного документооборота; к таким событиям/обстоятельствам, в том числе, могут быть отнесены:

- пожары, наводнения, иные стихийные бедствия или техногенные катастрофы; разрушения или значительные повреждения занимаемых указанными организациями помещений; нестабильность или отключение электроэнергии, которое не может быть нейтрализовано имеющимися в распоряжении указанных организаций техническими средствами;

неработоспособность программного обеспечения, вычислительной техники, оргтехники, средств связи, включая средства телекоммуникаций; массовые беспорядки, вооруженные столкновения, демонстрации; террористические акты или диверсии.

- неспособность Банка выполнять свои функции, в том числе и в случае расторжения Договора;
- любые другие подобные события или обстоятельства, которые могут существенным образом затруднить или сделать невозможным осуществление электронного документооборота.

К числу обстоятельств, которые способны послужить причиной возникновения чрезвычайных ситуаций могут быть отнесены принятие или любые изменения законодательных или иных актов государственных органов Российской Федерации или распоряжения данных органов, инструкции, указания, заявления, письма, телеграммы или иные действия, (далее – акты), которые прямо или косвенно или при определенном их толковании или определенном стечении обстоятельств, начиная с момента утверждения данных актов или с иного срока, временно или на неопределенный срок сделали, делают или могут сделать невозможным или значительно затруднить дальнейшее осуществление электронного документооборота в том виде, форме и порядке, в которых он осуществлялся до принятия данных актов.

7.2. **Порядок уведомления о наступлении обстоятельств, могущих послужить причиной возникновения чрезвычайных ситуаций**. В случае наступления хотя бы одного из обстоятельств, соответствующих перечисленным в статье 7.1 настоящих Правил:

- Клиент обязан незамедлительно с учетом сложившейся ситуации и способом, доступным в сложившихся обстоятельствах, известить Банк о возникших обстоятельствах;
- Банк обязан незамедлительно с учетом сложившейся ситуации и способом, доступным в сложившихся обстоятельствах, известить всех Клиентов. Впоследствии Клиент или Банк обязаны письменным сообщением подтвердить уведомление о возникших обстоятельствах, способных послужить причиной возникновения чрезвычайных ситуаций.

Банк незамедлительно после возникновения у него обстоятельств, соответствующих перечисленным в статье 7.1. настоящих Правил или получения уведомления, указанного в абзаце первом настоящей статьи, обязан рассмотреть возникшую ситуацию и принять квалифицирующее решение. Для квалификации ситуации, связанной с наличием хотя бы одного из обстоятельств, соответствующих перечисленным в статье 7.1. настоящих Правил в качестве чрезвычайной ситуации, в том числе технического сбоя, достаточно решения единоличного исполнительного органа Банка. Решение единоличного исполнительного органа Банка о квалификации обстоятельств, из числа перечисленных в статье 7.1 настоящих Правил в качестве чрезвычайной ситуации (квалифицирующее решение Банка) оформляется документом, составленным в письменной форме.

7.3. **Последствия принятия квалифицирующего решения единоличного исполнительного органа Банка**. В случае признания единоличным исполнительным органом Банка ситуации, связанной с наличием хотя бы одного из обстоятельств, соответствующих перечисленным в статье 7.1. настоящих Правил в качестве чрезвычайной ситуации, Банк незамедлительно способом, наиболее удобным с учетом сложившейся ситуации, связывается с Клиентом / Клиентами и уведомляет о возникновении чрезвычайной ситуации. В случае признания единоличным исполнительным органом Банка ситуации, связанной с наличием хотя бы одного из обстоятельств, соответствующих перечисленным в статье 7.1. настоящих Правил в качестве чрезвычайной ситуации, электронный документооборот может быть прекращен по решению единоличного исполнительного органа Банка. Одновременно с признанием ситуации чрезвычайной Банк приступает к разработке мер по урегулированию сложившейся чрезвычайной ситуации в Системе ДБО «iBank2». Возобновление электронного документооборота осуществляется по решению единоличного Исполнительного органа Банка.

7.4. **Меры по урегулированию чрезвычайных ситуаций** В качестве мер по урегулированию сложившейся чрезвычайной ситуации Банк вправе:

- прекратить или ограничить обращение всех или части электронных документов в ДБО;

- совместно с Клиентом определить порядок действий по устранению технического сбоя (договоренность сторон о порядке совместных действий оформляется Протоколом, составленным в письменной форме и подписанным уполномоченными представителями сторон);
- потребовать от Клиента, являвшихся отправителями электронных документов в рамках Договора между Банком и Клиентом, безвозмездного и незамедлительного с учетом сложившихся обстоятельств предоставления Банку копий на бумажных носителях всех или части электронных документов, обращавшихся в ДБО за определенный период времени;
- потребовать от Клиентов за их счет незамедлительного с учетом сложившихся обстоятельств восстановления, в том числе, в виде копий на бумажных носителях обращения всех или части электронных документов в ДБО;
- потребовать от Клиентов безвозмездного и незамедлительного с учетом сложившихся обстоятельств предоставления копий, в том числе и, в случае необходимости, нотариально заверенных копий журналов электронных документов, обращавшихся в ДБО за определенный период;
- предусмотреть иные меры, направленные на преодоление чрезвычайной ситуации.

При принятии решений по урегулированию чрезвычайных ситуаций единоличный исполнительный орган Банка вправе:
- устанавливать сроки и форму уведомления Клиентов о своих решениях;
- устанавливать сроки и порядок исполнения своих решений;
- обуславливать порядок вступления в силу своих решений определенными обстоятельствами. Решения Банка по урегулированию чрезвычайной ситуации в ДБО являются обязательными для исполнения Клиентами. О решениях Банка о мерах по урегулированию чрезвычайной ситуации Клиенты уведомляются не позднее принятия данных мер в соответствии с данным решением.

8. ПОРЯДОК РАЗРЕШЕНИЯ КОНФЛИКТНЫХ СИТУАЦИЙ И СПОРОВ, ВОЗНИКШИХ В СВЯЗИ С ОСУЩЕСТВЛЕНИЕМ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА В СИСТЕМЕ ДБО «IBANK2»

8.1. **Возникновение конфликтных ситуаций в связи с осуществлением электронного документооборота в Системе ДБО «iBank2»**. В связи с осуществлением электронного документооборота, возможно возникновение конфликтных ситуаций, связанных с формированием, доставкой, получением, подтверждением получения электронных документов, а также использованием в данных документах электронной подписи. Данные конфликтные ситуации могут возникать, в частности, в следующих случаях:
- не подтверждение подлинности электронных документов средствами электронной подписи принимающей Стороны;
- оспаривание факта формирования электронного документа;
- оспаривание факта идентификации владельца открытого ключа электронной подписи, подписавшего документ;
- заявление Клиента об искажении электронного документа;
- оспаривание факта отправления и/или доставки электронного документа;
- оспаривание времени отправления и/или доставки электронного документа;
- оспаривание аутентичности экземпляров электронного документа и/или подлинника и копии электронного документа на бумажном носителе;
- иные случаи возникновения конфликтных ситуаций, связанных с функционированием Системы ДБО «iBank2».

Конфликтная ситуация возникает также в случае, если Клиент или Банк:
- высказывает недоверие к составу и формату электронных документов, хранящихся в локальном архиве рабочего места Клиента или Банка;
- высказывает недоверие к программному обеспечению, функционирующему на данном рабочем месте.

8.2. Уведомление о конфликтной ситуации В случае возникновения конфликтной ситуации Клиент или Банк, предполагающий возникновение конфликтной ситуации, должен незамедлительно, но не позднее чем в течение 3-х трех рабочих дней после возникновения конфликтной ситуации, направить уведомление о конфликтной ситуации Банку. Уведомление о предполагаемом наличии конфликтной ситуации должно содержать информацию о существе конфликтной ситуации и обстоятельствах, которые, по мнению уведомителя, свидетельствуют о наличии конфликтной ситуации. Независимо от формы, в которой составлено уведомление (письменная или электронный документ), оно должно содержать все реквизиты электронного документа, предусмотренные настоящими Правилами. Кроме того, в нем должны быть указаны фамилия, имя и отчество, должность, контактные телефоны, факс, адрес электронной почты лица или лиц, уполномоченных вести переговоры по урегулированию конфликтной ситуации. Сторона, которой направлено уведомление, обязана незамедлительно, однако не позднее чем в течение следующего рабочего дня, проверить наличие обстоятельств, свидетельствующих о возникновении конфликтной ситуации, и направить уведомителю информацию о результатах проверки и, в случае необходимости, о мерах, принятых для разрешения возникшей конфликтной ситуации.

8.3. Разрешение конфликтной ситуации в рабочем порядке Конфликтная ситуация признается разрешенной в рабочем порядке в случае, если уведомитель удовлетворен информацией, полученной от Клиента / Банка, которому было направлено уведомление.

8.4. В случае если уведомитель не удовлетворен информацией, полученной от Клиента / Банка, которому направлялось уведомление, для рассмотрения конфликтной ситуации формируется экспертная комиссия. Порядок создания и работы экспертной комиссии описан в Приложении №2 к Договору обмена электронными документами с использованием системы электронного банкинга "iBank2"

9. ИНЫЕ ПОЛОЖЕНИЯ

9.1. Все споры и разногласия, которые могут возникнуть в связи с применением, нарушением, толкованием настоящих Правил, признанием недействительными настоящих Правил или их части, стороны должны разрешить, используя механизмы согласительного урегулирования споров и разногласий.

9.2. Если по итогам проведения согласительной процедуры конфликтная ситуация остается полностью или частично неурегулированной, стороны вправе передать неурегулированный спор и разногласия в Арбитражный суд г. Москвы в соответствии с законодательством Российской Федерации.

9.3. К настоящим Правилам прилагаются и являются их неотъемлемой частью:

- Приложение № 1. Типовая форма Договора о присоединении к системе электронного документооборота.
- Приложение № 2. Организация управления ключевыми системами электронного банкинга «iBank2» ООО КБ «Столичный кредит».

9.4. Настоящие Правила прекращают свое действие на основании решения Банка. Прекращение действия настоящих Правил и Приложений к ним не влияет на юридическую силу и действительность электронных документов, которыми Банк и Клиент обменивались до прекращения действия настоящих Правил и Приложений к ним.