*Приложение № 10*

*к Регламенту оказания услуг на финансовых рынках*

*«АЛОР БАНК» (ОАО)*

**ПРАВИЛА ДИСТАНЦИОННОГО БАНКОВСКОГО ОБСЛУЖИВАНИЯ ПОСРЕДСТВОМ ИНФОРМАЦИОННО-ТОРГОВОЙ СИСТЕМЫ «QUIK»**

1. ОБЩИЕ ПОЛОЖЕНИЯ
   1. Настоящие Правила дистанционного банковского обслуживания посредством информационно-торговой системы «QUIK» (далее – Правила) устанавливают порядок взаимодействия Банка и Клиента (далее – Стороны) при исполнении Договора об оказании услуг с использованием системы электронного документооборота и определяет права, обязанности и ответственность Сторон, возникающие в связи с этим.
   2. Настоящие Правила являются приложением к Регламенту. Во всем ином, что не предусмотрено настоящими Правилами, Стороны в своих взаимоотношениях руководствуются положениями Регламента и действующего законодательства Российской Федерации.
   3. В целях обеспечения оперативного взаимодействия с Клиентом при оказании услун на финансовых рынках , Банк предоставляет Клиенту возможность использовать программное обеспечение информационно-торговой системы «QUIK» (ИТС «QUIK») путем предоставления Клиенту указанного выше программного обеспечения, а также обмена открытыми ключами доступа.
   4. Использование системы ИТС «QUIK» Клиентом возможно только в случае, если Клиент выразил свое желание на использование системы удаленного доступа в Заявлении.
   5. Акцепт Клиента на использование для обмена сообщениями ИТС «QUIK», будет означать согласие Клиента со всеми положениями настоящих Правил.
   6. Банк ведет журнал активных операций (транзакций) Клиента. Под журналом активных операций Клиента, ведущимся в электронной форме, подразумевается совокупность записей в базе данных брокерской системы, содержащая информацию об операциях Клиента, проводимых им в соответствии с Регламентом с использованием ИТС «QUIK».
   7. Правообладателем ПО ИТС «QUIK» является ЗАО «АРКА Текнолоджиз».
   8. Клиент обязуется не переуступать третьим лицам все или часть полученных по настоящему Регламенту прав на использование ПО ИТС «QUIK».
   9. Клиент обязуется не допускать удаления, искажения или модификации в переданном Клиенту экземпляре программного обеспечения имени правообладателя ПО ИТС «QUIK». Клиент обязуется не допускать декомпиляции и деассемблирования, а также не санкционированного правообладателем и Банком копирования и распространения любых программных компонентов, используемых в ПО ИТС «QUIK».
   10. Банк не несет ответственность за какой-либо ущерб (включая все случаи понесенных, либо предполагаемых расходов, потери прибылей, прерывания деловой активности, потери деловой информации, либо других материальных, денежных потерь), связанный с использованием или невозможностью использования ПО ИТС «QUIK».
   11. Клиент самостоятельно обеспечивает защиту от несанкционированного доступа третьих лиц к средствам идентификации Клиента в ИТС «QUIK» (логин, пароль), а также ключу шифрования. Банк не несет ответственность за несанкционированный доступ в ИТС «QUIK», произошедший по вине Клиента.
   12. В случае наличия у Клиента сведений, позволяющих предполагать нарушение правил пользования средствами идентификации и ключом шифрования или утечку сведений о них, он должен информировать об этом Банк наиболее быстрым доступным способом.
   13. Банк обязуется по первому требованию Клиента, заявленному устно, письменно или любым иным способом, незамедлительно приостановить удаленный доступ с текущими ключами и информировать об этом Клиента наиболее быстрым доступным способом.
   14. Все претензии, возникающие у Клиента при использовании ИТС «QUIK», принимаются Банком в соответствии с претензионным порядком рассмотрения спора, указанном в настоящем Регламенте.
2. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Термины, применяемые в тексте настоящих Правил, используются в следующем значении.

**Администратор безопасности (Администратор)** – сотрудник Банка, ответственный за генерацию и плановую замену ключей электронно-цифровой подписи и соответствующих сертификатов.

**Владелец сертификата ключа подписи** – юридическое лицо, на имя которого выдан сертификат ключа подписи и которое владеет соответствующим закрытым ключом электронной цифровой подписи, позволяющим создавать свою электронно-цифровую подпись в электронных документах (подписывать электронные документы);

**Система электронного документооборота (СЭД)** - совокупность программного обеспечения, обслуживаемого Банком, а также вычислительных средств и баз данных, принадлежащих или подконтрольных Банку, предназначенная для передачи зашифрованных и подписанных электронно-цифровой подписью электронных документов. Для обмена Электронными документами и взаимодействия Клиентов с Банком используется ИТС «QUIK»;

**Электронный документ (ЭД)** – документ, в котором информация представлена в электронно-цифровой форме. В рамках настоящего договора - Поручение (приказ) Клиента данное Банку посредством ИТС «QUIK». Электронный документ с электронно-цифровой подписью обладает следующими свойствами, позволяющими обеспечить подтверждение авторства, целостности и неизменности Электронного документа:

* создание корректного Электронного документа с электронно-цифровой подписью невозможно без знания соответствующего закрытого ключа;
* при любом изменении Электронного документа его электронно-цифровая подпись, сформированная до внесения изменений, становится некорректной;
* знание информации, которая содержится в Электронных документах, электронно-цифровой подписи и открытых ключах, не приводит к компрометации закрытых ключей.

**Электронная подпись (ЭП)** – реквизит ЭД, вид аналога собственноручной подписи, предназначенный для защиты данного документа от подделки, полученный в результате криптографического преобразования информации с использованием Закрытого ключа ЭП и позволяющий идентифицировать владельца Сертификата ключа ЭП, а также установить отсутствие искажения информации в электронном документе. ЭП однозначно увязывает в одно целое содержание документа и закрытый ключ подписывающего и делает невозможным изменение документа без нарушения подлинности данной подписи. Банк вправе в одностороннем порядке менять перечень средств криптографической защиты, используемых в СЭД, без дополнительного согласования и уведомления Клиента.

**Информационный носитель** – хранилище данных, в качестве которого может быть использован флэш – накопитель, USB – токен и аналогичное устройство хранения информации.

**Пара ключей ЭП** - Закрытый ключ и соответствующий ему Открытый ключ ЭП.

**Закрытый ключ ЭП** – уникальная последовательность символов, известная владельцу Сертификата ключа ЭП и предназначенная для создания в Электронных документах ЭП. Закрытый ключ изготавливается (генерируется) Клиентом при помощи криптобиблиотек и предназначен для формирования ЭП ЭД. Секретный ключ хранится в цифровом виде на устройстве хранения информации.

**Открытый ключ ЭП** – уникальная последовательность символов, соответствующая Закрытому ключу ЭП, предназначенная для подтверждения подлинности ЭП в Электронном документе. Открытый ключ, автоматически формируемый программными средствами СЭД при изготовлении секретного ключа подписи и однозначно зависящий (производный) от него. Открытый ключ предназначен для проверки ЭП ЭД, сформированной данным участником СЭД при подписании ЭД.

**Компрометация ключа** – утрата доверия к тому, что используемые ключи обеспечивают безопасность информации. К событиям, связанным с компрометацией ключей относятся (включая, но, не ограничиваясь):

* утрата ключевых элементов;
* утрата ключевых элементов с последующим обнаружением;
* увольнение сотрудников, имевших доступ к ключевой информации;
* нарушение правил хранения и уничтожения (после окончания срока действия) секретного ключа;
* несанкционированное копирование или подозрение на копирование Информационного носителя с секретными ключами;
* возникновение подозрений на утечку информации или ее искажение в системе конфиденциальной связи;
* случаи, когда нельзя достоверно установить, что произошло с Информационным носителем электронных ключей, содержащим ключевую информацию (в том числе случаи, когда Информационный носитель вышел из строя и достоверно не опровергнута возможность того, что данный факт произошел в результате несанкционированных действий злоумышленника).

Открытый ключ считается принадлежащим Клиенту, если он был зарегистрирован в установленном порядке (в Банк представлен Сертификат ключа ЭП).

**Сертификат ключа ЭП** - подписанный Владельцем ЭП и заверенный подписью руководителя и оттиском печати Клиента документ на бумажном носителе с указанным в шестнадцатеричном виде Открытым ключом ЭП Клиента. Банк имеет право в одностороннем порядке изменить форму Сертификата ключа ЭП.

**ЭП Банка** – электронно-цифровая подпись уполномоченного Банком лица.

**ЭП Клиента** – электронно-цифровая подпись уполномоченного Клиентом лица.

1. СОГЛАШЕНИЯ СТОРОН
   1. Клиент признает факт предоставления Банком информации о методах полноты обеспечения аутентификации сторон, конфиденциальности и целостности сообщений в ИТС «QUIK»;
   2. Акцепт Клиента на использование ИТС «QUIK», выраженный в Заявлении, означает признание Клиентом всех заявок на сделки, заверенных ЭП Клиента и переданных Клиентом с использованием ИТС «QUIK», абсолютным юридическим эквивалентом соответствующему Поручению на бумажном носителе, предусмотренным условиями настоящего Регламента, подписанным собственноручной подписью Клиента или его Представителя (для Клиентов – физических лиц), или подписанным уполномоченным лицом Клиента и заверенного печатью Клиента (для Клиентов – юридических лиц). Последующее письменное подтверждение Клиентом поручения не требуется;
   3. Клиент признает, что используемые в ИТС «QUIK» методы обеспечения аутентификации сторон, конфиденциальности и целостности сообщений, а также алгоритмы создания и функционирования ЭП при передаче ЭД достаточны для обеспечения защиты от несанкционированного доступа, подтверждения авторства, целостности, неизменности и подлинности информации, содержащейся в получаемых ЭД, сохранения банковской тайны, и обеспечивают защиту интересов Клиента;
   4. Клиент отказывается от претензий к Банку, основанием которых является недостаточная, по мнению Клиента, степень обеспечения аутентификации сторон, конфиденциальности и целостности сообщений в ИТС «QUIK»;
   5. Положительный результат проверки на сервере Банка ЭП Клиента при получении от него ЭД по ИТС «QUIK» является подтверждением того, что полученный ЭД подписан ЭП Клиента; и ЭД получен в том виде, в котором он исходил от Клиента.
   6. Стороны согласны с тем, что Открытый ключ ЭП, указанный в заверенном подписью руководителя и оттиском печати Клиента Сертификате открытого ключа ЭП, принадлежит Клиенту и достаточен для определения Банком корректности ЭП;
   7. Стороны признают, что выписка из журнала активных операций Клиента, представленная на бумажном носителе и заверенная собственноручной подписью ответственного лица Банка, является безусловным подтверждением факта проведения Клиентом указанных в выписке операций.
   8. Стороны признают в качестве единой шкалы времени при работе с СЭД Московское поясное время. Контрольным является время системных часов СЭД. Стороны признают информацию о дате и времени поступления, исполнения, неисполнения ЭД в Банк, содержащуюся в контрольных архивах Банка, необходимым и достаточным доказательством даты и времени передачи, исполнения, неисполнения Клиентом Банку ЭД;
   9. Стороны согласны с тем, что наличие у Банка надлежаще оформленного ЭД, подписанного ЭП Клиента, проверка корректности которой Открытым ключом ЭП Клиента дала положительный результат, является необходимым и достаточным основанием для проведения Банком соответствующей операции на основании указанного ЭД;
   10. Стороны согласны с тем, что использование всемирной телекоммуникационной сети общего доступа Интернет может вызывать перерывы в приеме и обработке ЭД в СЭД, связанные с отказами телекоммуникационного оборудования провайдеров телекоммуникационных услуг, а также вирусными и иными атаками на СЭД. Стороны обязаны принимать все доступные способы защиты от указанных угроз;
   11. Стороны согласны с тем, что контроль за сроком действия ЭП, а также контроль за наличием соответствующих полномочий у Владельца Сертификата ключа ЭП осуществляется Клиентом, а не Банком;
   12. Если по истечении 10 (десяти) рабочих дней с момента проведения Банком операции на основании полученного от Клиента ЭД, Клиентом не заявляется претензия по такой операции, признается, что Клиент подтвердил правильность проведения операции.
2. ПОРЯДОК ПРЕДОСТАВЛЕНИЯ ДОСТУПА К СЭД
   1. Клиент допускается к осуществлению электронного документооборота посредством ИТС «QUIK» после выполнения им всей совокупности следующих действий и условий:

* заключение Договора об оказании услуг;
* установка на рабочем компьютере программного обеспечения, необходимого для работы с ИТС «QUIK»;
* генерация персонального ключа ЭП;

1. УСЛОВИЯ ОТПРАВКИ И ПРИЕМА ЭЛЕКТРОННЫХ ДОКУМЕНТОВ
   1. Для направления ЭД Клиент:

* устанавливает соединение с удаленным сервером доступа СЭД, установленного в офисе Банка или в ином месте по усмотрению Банка;
* проходит процедуру аутентификации (вводится логин, пароль);
* формирует в СЭД текст ЭД;
* проверяет правильность составленного ЭД;
* направляет в Банк по СЭД подписанный ЭП ЭД.
  1. Банк принимает к исполнению полученные от Клиента ЭД при одновременном наличии следующих условий:
* Клиент успешно прошел процедуру аутентификации (проверку подлинности ЭП);
* На момент принятия ЭД у Банка нет полученного от Клиента уведомления о компрометации криптографического ключа;
* ЭД содержит все необходимые реквизиты в соответствии с предъявляемыми к нему требованиями;
* Клиентом соблюдены иные положения настоящего Договора об оказании услуг,, регулирующие условия принятия Банком к исполнению Поручений.
  1. Клиент соглашается, что ЭД, полученный Банком через СЭД, процедура аутентификации для доступа к которой была проведена успешно, считается направленным Клиентом и Клиент признает факт направления такого ЭД от его имени. Факт направления Клиентом и получения Банком ЭД посредством СЭД, подписанного корректной ЭП Клиента, является достаточным основанием для исполнения Банком содержащихся в таком ЭД инструкций.
  2. Временем и датой приема ЭД Банком считается время получения подтверждения о поступлении данного документа Клиентом. Время и дата приема ЭД фиксируется сервером доступа СЭД Банка.
  3. В случае принятия Банком ЭД, подтверждением поступления данного документа, является присвоение следующего статуса данному документу:
* активен;
* снят;
* исполнен.
  1. В случае отказа Банка от приема ЭД, Банк направляет Клиенту по СЭД сообщение об отказе от приема (мотивированный отказ в приеме) ЭД в течение рабочего дня с момента получения такого ЭД Банком.

1. УЧЕТ И ХРАНЕНИЕ ЭЛЕКТРОННЫХ ДОКУМЕНТОВ
   1. Банком осуществляется учет ЭД путем ведения журнала учета в электронном виде с возможностью распечатки на бумажном носителе.

При учете ЭД Банк обеспечивает учет следующих данных:

* уникальный входящий номер документа;
* дата и время поступления документа;
* дата и время отправки документа;
* адресат документа, иные данные (по усмотрению Банка).
  1. Все ЭД, учтенные в журнале учета, хранятся в электронных архивах Банка не менее 5 (пяти) лет. ЭД хранятся в том же формате, в котором они были сформированы, отправлены или получены.
  2. Банком осуществляется ежедневное резервное копирование и архивное хранение ЭД. Электронные архивы подлежат защите от несанкционированного доступа и непреднамеренного уничтожения и/или искажения.

1. КОМПРОМЕТАЦИЯ КРИПТОГРАФИЧЕСКОГО КЛЮЧА
   1. Под компрометацией криптографического ключа Сторонами понимается утрата доверия к тому, что используемый Клиентом криптографический ключ недоступен посторонним лицам.
   2. К событиям, связанным с компрометацией криптографического ключа, относятся:

* утрата ключевых дискет или иных носителей криптографических ключей (закрытых ключей);
* утрата ключевых дискет с последующим обнаружением;
* утрата полномочий лицами, имевших доступ к ключевой информации;
* временный доступ посторонних лиц к ключевой информации;
* иные обстоятельства, прямо или косвенно свидетельствующие о наличии возможности доступа к криптографическим ключам третьих лиц.
  1. В случае компрометации криптографического ключа Банк рекомендует Клиенту незамедлительно направить в Банк уведомление о компрометации ключа и прекратить направление ЭД в Банк.

1. ПРАВА И ОБЯЗАННОСТИ СТОРОН
   1. Клиент имеет право:

* Использовать СЭД лично или через своих Представителей, учитывая, что каждый Представитель Клиента является Владельцем сертификата ключа подписи, позволяющих однозначно установить инициатора действий в СЭД от имени Клиента.
* Направить в Банк уведомление о приостановке приема и исполнения любых документов, подаваемых в Банк через СЭД от имени Клиента или его Представителя.
* Клиент имеет право досрочно прекратить действие Открытых ключей ЭП Клиента (вместе с соответствующим Закрытым ключом ЭП Клиента), направив уведомление в свободной форме, подписанное уполномоченным лицом (данное уведомление может быть направлено в Банк с использованием СЭД, либо в письменном виде передано в Банк). Для продолжения дальнейшей работы в СЭД уполномоченный представитель Клиента должен сгенерировать новую Пару ключей ЭП Клиента и передать Банку Сертификат нового Открытого ключа ЭП Клиента.
* Клиент имеет право блокировать Открытый ключ ЭП Клиента, т.е. приостановить свою работу в СЭД, направив уведомление по форме Приложения No10г , подписанное уполномоченным лицом (данное уведомление может быть направлено в Банк с использованием СЭД, либо в письменном виде передано в Банк). Блокировка снимается не позднее дня, следующего за днем получения Банком письменного требования Клиента о снятии блокировки.
  1. Банк имеет право:
* В случае выявления признаков нарушения безопасности при осуществлении обмена ЭД через СЭД, Банк имеет право по своему усмотрению временно прекратить прием от Клиента ЭД, передаваемых в Банк от имени Клиента и потребовать от Клиента смены Пары ключей ЭП Клиента. По письменному требованию Клиента Банк обязан объяснить причину прекращения принятия ЭД от Клиента.
* Банк имеет право приостановить работу Клиента в СЭД и (или) не производить исполнение полученного ЭД, сообщив об этом Клиенту не позднее дня, следующего за днем его получения, путем направления сообщения по СЭД и, соответственно, затребовать от Клиента оформления документа на бумажном носителе с подписью уполномоченных лиц и оттиском печати Клиента, оформленных в соответствии с требованиями действующего законодательства.
* Банк вправе не принимать Сертификат открытого ключа ЭП Клиента, если подписи Владельца ключа ЭП или руководителя Клиента проставлена не в присутствии уполномоченного представителя Банка или если подлинность вышеуказанных подписей не заверена нотариально.
  1. Клиент обязуется:
* Клиент обязан по требованию Банка представлять документы на бумажном носителе, оформленные в соответствии с требованиями действующего законодательства, соответствующие полученным Банком от Клиента ЭД.
* Незамедлительно уведомлять Банк о компрометации криптографического ключа по телефону и в письменном виде.
* Своевременно уведомлять Банк об изменениях в руководстве Клиента (если Клиент является юридическим лицом), о смене лиц, уполномоченных работать с СЭД, о прекращении действия доверенностей уполномоченных пользователей Клиента, и для возможности работы с СЭД новых лиц обеспечить им возможность сгенерировать Пару ключей ЭП Клиента. Риск неблагоприятных последствий, связанных с несвоевременным уведомлением Банка о том, что необходимо приостановить действие ЭП Клиента несет Клиент.
* Клиент обязан при создании ЭД в СЭД соблюдать условия настоящих Правил, нормы действующего законодательства и банковские правила в отношении обязательных реквизитов данных документов.
* Клиент обязан обеспечить хранение в секрете и отсутствие доступа неуполномоченных лиц к Закрытому ключу ЭП Клиента и Открытому ключу ЭП Банка, используемым при работе в электронной СЭД. Риск неблагоприятных последствий, связанных с использованием закрытого Ключа ЭП Клиента неуполномоченными лицами, несет Клиент.
* Клиент обязан сообщать Банку об обнаружении попытки несанкционированного доступа к СЭД или к Закрытому ключу ЭП Клиента в день ее обнаружения и блокировать свою работу в СЭД, направив в Банк уведомление по форме Приложения No10г . Клиент несет риск всех последствий, связанных с несанкционированным доступом к СЭД или Закрытому ключу ЭП Клиента.
* Клиент обязан по требованию Банка приостановить работу в СЭД и для ее возобновления сгенерировать новую ЭП Клиента и передать Банку Сертификат нового открытого ключа ЭП Клиента. Сертификат открытого ключа ЭП Клиента должен передаваться в Банк уполномоченным лицом Клиента (единоличным исполнительным органом либо через доверенное лицо при наличии доверенности (например, по форме по форме, установленной в Банке) либо иным способом, позволяющим установить, что документ исходит от Клиента).
* Клиент обязан хранить свой Закрытый ключ в течение срока действия Генерального Соглашения, а также не менее 8 (восьми) лет после его расторжения. В случае, если Клиент после расторжения Генерального Соглашения оспаривает операции, проведенные Банком с использованием его ЭП (в т.ч. Закрытого ключа) и не может предъявить используемый Закрытый ключ для проведения проверки, то считается что Клиент подтверждает правильность проведения операций Банком с использованием данной ЭП (в т.ч. Закрытого ключа).
  1. Банк обязуется:
* Предоставить Клиенту во временное пользование программное обеспечение, необходимое для использования СЭД.
* Прекратить доступ к системам СЭД после получения от Клиента уведомления о компрометации криптографических ключей.
* Банк обязан исполнять принятые от Клиента ЭД посредством СЭД, подписанные корректной ЭП Клиента, в соответствии с условиями Генерального Соглашения и действующим законодательством РФ.
* Банк обязан при получении от Клиента уведомления по форме Приложения No10г временно Прекратить доступ к системам СЭД, (блокировать или досрочно прекратить действие) ключа ЭП Клиента в СЭД. Банк не обязан проверять подлинность подписи Клиента на полученном уведомлении, а обязан только установить путем обычного визуального контроля соответствие данной подписи имеющемуся у Банка образцу. Наложенная блокировка снимается только на основании требования Клиента не позднее дня, следующего за днем получения такого требования.
* Банк обязан обеспечить строго контролируемый и ограниченный доступ к помещениям, в которых находятся программно-аппаратные средства, содержащие контрольные архивы СЭД.
* Банк обязан хранить в секрете и не передавать третьим лицам Закрытые ключи ЭП Банка и Открытые ключи ЭП Клиента, используемые при работе в СЭД. Риск неблагоприятных последствий, связанных с использованием Закрытого Ключа ЭП Банка третьими лицами в случае несоблюдения условий сохранности, несет Банк.
* По письменному требованию Клиента Банк обязан объяснить причину приостановления работы Клиента и неисполнения принятого ЭД, которая может быть иной, чем несоответствие ЭД положениям настоящего Договора или действующего законодательства.

1. СОВМЕСТНЫЕ ОБЯЗАТЕЛЬСТВА И ОТВЕТСТВЕННОСТЬ СТОРОН
   1. В случае невыполнения или ненадлежащего исполнения обязательств по Соглашению одной из Сторон, другая Сторона имеет право потребовать от виновной Стороны исполнения принятых на себя обязательств, а также возмещения причиненного ей ущерба.
   2. Стороны обязуются:

* Организовать работу с СЭД таким образом, чтобы исключить возможность использования СЭД неуполномоченными лицами.
* При выявлении одной из Сторон признаков нарушения безопасности использования СЭД обеспечить незамедлительную приостановку всех действий по его осуществлению и известить о случившемся другую Сторону.
* Каждая Сторона обязана за собственный счет поддерживать в рабочем состоянии свои программно-технические средства, используемые при работе с СЭД.
* В случае возникновения конфликтных ситуаций между Сторонами при использовании СЭД Стороны обязуются участвовать в рассмотрении конфликтов в соответствии с Порядком разрешения споров настоящих Правил, выполнять требования указанного Положения и нести ответственность согласно выводам по рассмотрению конфликтной ситуации. В случае, если Клиент отказывается от принятия на себя обязательств по ЭД (оспаривает факт или время передачи ЭД, его содержание), бремя доказывания обстоятельств, на основании которых он отказывается от принятия на себя обязательств, ложится на него. Ответственность может быть возложена на Банк в случае, если создание ЭД обусловлено противоправными действиями Банка.
* Стороны обязуются при разрешении споров, которые могут возникнуть в связи с использованием СЭД, предоставлять в письменном виде свои оценки, доказательства и выводы по запросу противоположной Стороны.
* Банк не несет ответственности за ущерб, причиненный Клиенту в результате использования третьими лицами Закрытого ключа Клиента (компрометация ключа).
* Банк не несет ответственности за техническое состояние компьютерного оборудования Клиента, возможные помехи в телефонных линиях связи, прекращение работы СЭД из-за отключения электроэнергии и повреждения линий связи, программно-аппаратные сбои СЭД, если возникновение указанных обстоятельств не связано с виновными действиями Банка.
* Банк не несет ответственности перед Клиентом, в случае, если ЭД подписан корректной ЭП, но исходил не от Клиента.

1. ПОРЯДОК РАЗРЕШЕНИЯ СПОРОВ
   1. Стороны договорились считать наличие корректной ЭП Клиента в оспариваемом ЭД необходимым и достаточным доказательством, подтверждающим принадлежность данного ЭД Клиенту и, соответственно, фактом, удостоверяющим передачу ЭД или содержание переданного ЭД. Стороны признают информацию о дате и времени поступления ЭД в Банк, содержащуюся в контрольных архивах Банка, необходимым и достаточным доказательством даты и времени передачи Клиентом Банку ЭД, если разрешительной комиссией не будет установлен факт внесения Банком изменений в указанную информацию в части, касающейся предмета спора. Корректность ЭП Клиента в оспариваемом ЭД устанавливается разрешительной комиссией в установленном ниже порядке.
   2. В случае возникновения споров о наличии ЭП под ЭД, бремя доказывания лежит на Стороне, не соглашающейся с наличием ЭП.
   3. В случае возникновения споров о факте внесения изменений в ЭД после его подписания ЭП, бремя доказывания лежит на Стороне, утверждающей, что в данный документ были внесены изменения.
   4. В случае возникновения споров о факте получения одной из Сторон какого-либо ЭД, подписанного ЭП, бремя доказывания лежит на Стороне, не соглашающейся с фактом получения Стороной ЭД, подписанного ЭП.
   5. В случае несогласия Клиента с действиями Банка, связанными с исполнением Банком направленных по СЭД ЭД Клиента, Клиент направляет в Банк письменное заявление с изложением сути претензии. В таком заявлении должно быть указано: требования заявителя; обстоятельства, на которых основываются требования, и подтверждающие их доказательства; иные сведения, необходимые для урегулирования споров.
   6. Банк в течение 7 (семи) рабочих дней рассматривает заявление Клиента и либо удовлетворяет претензию, либо передает Клиенту письменное заключение о необоснованности его претензии, либо в течение согласованного с Клиентом срока создает экспертную комиссию. Стороны вправе привлекать независимых экспертов из числа представителей разработчика СЭД. Оплата участия в работе экспертной комиссии представителей разработчика производится за счет стороны, инициирующей проведение экспертизы. По результатам экспертизы комиссия составляет заключение в письменной форме, в котором указываются выводы о факте направления или получения ЭД, его содержании, наличии или отсутствии изменений в содержании ЭД с момента его направления до момента его исполнения Банком. Срок проведения соответствующего расследования экспертной комиссией не должен составлять более 30 дней с даты формирования экспертной комиссии. В случае невозможности в указанный срок осуществить соответствующие процедуры, срок может быть продлен, но не более чем на 10 дней.
   7. В случае несогласия одной из Сторон с решением экспертной комиссии либо препятствования участию одной из Сторон в работе экспертной комиссии, вторая Сторона вправе передать спор на рассмотрение в третейский суд НАУФОР.
   8. Банк несет ответственность перед Клиентом в случае, когда имела место хотя бы одна из следующих ситуаций:

* Банк не предъявляет ЭД, на основании которого Банк выполнил оспариваемую операцию;
* электронная цифровая подпись Клиента в ЭД оказалась некорректной.