



АТБ

Азиатско-
Тихоокеанский
Банк

УТВЕРЖДЕНО
Приказом заместителя председателя правления
«Азиатско-Тихоокеанский Банк» (ПАО)
от «16» ноября 2016 г.
№ 2016111604-П

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

[РЕДАКЦИЯ 2.0]

г. Благовещенск
2016 г.

ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящие Правила дистанционного банковского обслуживания посредством информационно-торговой системы «QUIK» (далее – Правила) устанавливают порядок взаимодействия «Азиатско-Тихоокеанский Банк» (ПАО) (далее – Банк) и Клиента (далее – Клиент, при совместном упоминании – Стороны) при исполнении Договора об оказании брокерских услуг на финансовых рынках с использованием системы электронного документооборота и определяет права, обязанности и ответственность Сторон, возникающие в связи с этим.

1.2. В целях обеспечения оперативного взаимодействия с Клиентом при исполнении Договора об оказании брокерских услуг на финансовых рынках, Банк предоставляет Клиенту возможность использовать программное обеспечение информационно-торговой системы «QUIK» (далее - ИТС «QUIK») путем предоставления Клиенту указанного выше программного обеспечения, а также обмена открытыми ключами доступа.

1.3. Настоящие Правила являются документом, обязательным к исполнению при заключении Договора об оказании брокерских услуг на финансовых рынках, носят открытый характер, публикуются на официальном сайте Банка в сети Интернет www.atb.su. Во всем ином, что не предусмотрено настоящими Правилами, Стороны в своих взаимоотношениях руководствуются положениями Регламента оказания услуг на финансовых рынках «Азиатско-Тихоокеанский Банк» (ПАО) (далее – Регламент) и действующего законодательства Российской Федерации.

1.4. Использование системы ИТС «QUIK» Клиентом возможно только в случае, если Клиент выразил свое желание на использование данной системы для подачи поручений Банку в Заявлении на обслуживание на финансовых рынках (Приложение №4 к Регламенту), а также обеспечил технические и коммуникационные ресурсы, необходимые для подключения (Приложение №1 к Правилам).

1.5. Акцепт Клиента на использование для обмена сообщениями ИТС «QUIK», будет означать согласие Клиента со всеми положениями настоящих Правил.

1.6. 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 и настоящими Правилами с использованием ИТС «QUIK».

1.7. Правообладателем ПО ИТС «QUIK» является ЗАО «АРКА Текнолоджиз».

1.8. Клиент обязуется не переуступать третьим лицам все или часть полученных по настоящим Правилам прав на использование ПО ИТС «QUIK».

1.9. Клиент обязуется не допускать удаления, искажения или модификации в переданном Клиенту экземпляре программного обеспечения имени правообладателя ПО ИТС «QUIK».

1.10. Клиент обязуется не допускать декомпиляции и деасSEMBлирования, а также не санкционированного правообладателем и Банком копирования и распространения любых программных компонентов, используемых в ПО ИТС «QUIK».

1.11. 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».

1.12. Клиент самостоятельно обеспечивает защиту от несанкционированного доступа третьих лиц к средствам идентификации Клиента в ИТС «QUIK» (логин, пароль), а также ключу шифрования и мобильному телефону. Банк не несет ответственность за несанкционированный доступ в ИТС «QUIK», произошедший по вине Клиента.

1.13. 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.

1.14. Банк обязуется по первому требованию Клиента, заявленному устно, письменно или любым иным способом, незамедлительно приостановить доступ к ИТС «QUIK» с текущими ключами и информировать об этом Клиента наиболее быстрым доступным способом.

1.15. Все претензии, возникающие у Клиента при использовании ИТС «QUIK», принимаются Банком в соответствии с претензионным порядком рассмотрения спора, указанным в настоящем Регламенте.

2. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

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

Клиент - любое юридическое или физическое лицо, индивидуальный предприниматель, заключившее с Банком договор об оказании брокерских услуг на финансовых рынках.

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 Аналогом собственноручной подписи 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, то есть в виде пригодном для восприятия человека с использованием электронных вычислительных машин, а также для передачи по информационно-телекоммуникационным сетям или обработки в информационных системах, содержащая все обязательные реквизиты, предусмотренные для составления данной формы документа в соответствии с Регламентом. В рамках настоящего договора - Поручение (приказ) Клиента данное Банку посредством ИТС «QUIK». Электронный документ подписанный Аналогом собственноручной подписи обладает следующими свойствами, позволяющими обеспечить подтверждение авторства, целостности и неизменности Электронного документа:

- создание корректного Электронного документа с Аналогом собственноручной подписи невозможно без знания соответствующего Закрытого ключа АСП;
- при любом изменении Электронного документа Аналог собственноручной подписи, сформированный до внесения изменений, становится некорректным;
- знание информации, которая содержится в Электронных документах, Аналоге собственноручной подписи и открытых ключах, не приводит к компрометации закрытых ключей.

Аналог собственноручной подписи (АСП) – реквизит электронного документа (обозначение), полученный в результате криптографического преобразования информации с использованием закрытого ключа, пароля, не являющегося одноразовым паролем (Кодом подтверждения), позволяющий идентифицировать лицо (Владельца ключа АСП), подписавшего электронный документ. АСП является юридически эквивалентным подписи Клиента (для клиентов - физических лиц) или подписи и печати (для клиентов - юридических лиц) на документах, составленных на бумажном носителе, в смысле п.2 ст. 160 Гражданского кодекса РФ.

Владелец ключа АСП – физическое лицо - Клиент или его Представитель; идентифицированное Банком и уполномоченное Клиентом подавать поручения посредством ИТС «QUIK».

Пара ключей АСП - Закрытый ключ и соответствующий ему Открытый ключ АСП.

Закрытый ключ АСП – уникальная последовательность символов, известная владельцу ключа АСП и предназначенная для создания в Электронных документах АСП.

Открытый ключ АСП – уникальная последовательность символов, соответствующая Закрытому ключу АСП, предназначенная для подтверждения факта формирования АСП определенным лицом. Открытый ключ, автоматически формируется программными средствами СЭД при изготовлении Закрытого ключа АСП и однозначно зависит (производный) от него. Открытый ключ доступен широкому кругу лиц. Знание открытого ключа не приводит к Компрометации ключа. Открытый ключ считается принадлежащим Клиенту, если он был зарегистрирован в установленном настоящими Правилами порядке.

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) Закрытого ключа;
- несанкционированное копирование или подозрение на копирование информационного носителя с Закрытыми 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).

АСП Клиента – АСП Клиента или уполномоченного Клиентом лица.

Код подтверждения – одноразовый СМС пароль направляемый Банком Клиенту на номер мобильного телефона, указанный в Заявлении на присоединение и/или Заявлении на обслуживание и/или Заявлении на подключение ИТС «QUIK» при подключении Клиента к ИТС «QUIK» с целью проведения процедуры аутентификации Клиента.

3. СОГЛАШЕНИЯ СТОРОН

3.1. Клиент признает факт предоставления Банком информации о методах полноты обеспечения аутентификации сторон, конфиденциальности и целостности сообщений в ИТС «QUIK».

3.2. Акцепт Клиента на использование ИТС «QUIK», выраженный в Заявлении на обслуживание на финансовых рынках (Приложение №4 к Регламенту), означает признание Клиентом всех заявок на сделки, заверенных АСП 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.

3.3. Клиент признает, что используемые в ИТС «QUIK» методы обеспечения аутентификации сторон, конфиденциальности и целостности сообщений, а также алгоритмы создания и функционирования АСП 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.

3.4. Клиент отказывается от претензий к Банку, основанием для которых является недостаточная, по мнению Клиента, степень обеспечения аутентификации сторон, конфиденциальности и целостности сообщений в ИТС «QUIK».

3.5. Положительный результат проверки на сервере Банка АСП Клиента при получении от него ЭД по ИТС «QUIK» является подтверждением того, что полученный ЭД подписан АСП Клиента; и ЭД получен в том виде, в котором он исходил от Клиента.

3.6. Клиент несет полную ответственность за сохранность своего Закрытого ключа АСП и пароля для его защиты. Банк не несет ответственности за любые убытки, понесенные Клиентом, причиной которых является использование третьими лицами Закрытого ключа АСП и пароля Клиента. Клиент подтверждает, что все заявки, поданные с использованием системы QUIK до получения Банком письменного уведомления Клиента о компрометации ключа или пароля, считаются поданными от имени Клиента, а все сделки, совершенные на основании таких заявок, совершенными по поручению Клиента.

3.7. Стороны согласны с тем, что Открытый ключ АСП, указанный в Заявлении на регистрацию открытых ключей АСП (Приложение №2 к Правилам) заверенном подписью Клиента или его Представителя, принадлежит Клиенту и достаточен для определения Банком корректности АСП.

3.8. 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.

3.9. Стороны признают в качестве единой шкалы времени при работе с СЭД Московский часовой пояс. 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.

3.10. Стороны согласны с тем, что наличие у Банка надлежаще оформленного ЭД, подписанного АСП Клиента, проверка корректности которой Открытым ключом АСП Клиента дала положительный результат, является необходимым и достаточным основанием для проведения Банком соответствующей операции на основании указанного ЭД.

3.11. 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.

3.12. Стороны согласны с тем, что контроль за сроком действия АСП, а также контроль за наличием соответствующих полномочий у Владельца ключа АСП осуществляется Клиентом, а не Банком.

3.13. 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, то признается, что Клиент подтвердил правильность проведения операции.

4. ПОРЯДОК ПРЕДОСТАВЛЕНИЯ ДОСТУПА К СЭД

4.1. Клиент допускается к осуществлению электронного документооборота посредством ИТС «QUIK» после выполнения им всей совокупности следующих действий и условий:

- заключение Договора об оказании брокерских услуг на финансовых рынках;
- установка на рабочем компьютере программного обеспечения, необходимого для работы с ИТС «QUIK» (далее – ПО);
- генерация персонального ключа АСП;
- регистрации Открытого ключа АСП Банком.

4.2. Клиент самостоятельно обеспечивает технические и коммуникационные ресурсы, необходимые для подключения (Приложение №1 к Правилам), и устанавливает на рабочем компьютере программное обеспечение.

4.3. Клиент самостоятельно генерирует ключи АСП. При генерации ключей Клиент определяет логин и пароль и указывает их в специальных полях в СЭД.

4.4. Генерация ключей АСП Клиентом происходит в условиях исключающих компрометацию Закрытого ключа АСП.

4.5. Дистрибутив ПО и инструкции по установке и генерации ключей Клиент может получить на специальном разделе сайта Банка или от сотрудника Банка.

4.6. После формирования ключей Клиент направляет Банку Открытый ключ АСП в виде файла, а также Заявление на регистрацию Открытого ключа АСП (Приложение №2 к Правилам) посредством Личного кабинета или предоставляет в бумажном виде.

4.7. Заявление на регистрацию Открытого ключа АСП, направленное посредством Личного кабинета, должно быть заверено электронной подписью Клиента в соответствии с Соглашением об использовании электронной подписи (ЭП) «Азиатско-Тихоокеанский банк» (ПАО). Заявление на регистрацию Открытого ключа ЭП предоставленное в бумажном виде должно быть заверено собственноручной подписью Клиента (для Клиентов – физических лиц) или подписью и печатью (для Клиентов – юридических лиц).

4.8. Заявление на регистрацию Открытого ключа АСП Клиента – юридического лица, должно передаваться в Банк уполномоченным лицом Клиента (единоличным исполнительным органом либо через доверенное лицо при наличии доверенности).

4.9. Банк, получив от Клиента Открытый ключ АСП и Заявление на его регистрацию, регистрирует Открытый ключ АСП на серверной части ПО, присваивает терминалу ПО (рабочей станции) Клиента уникальный идентификатор (UID) и подключает Клиента к ИТС «QUIK».

4.10. Клиент узнает присвоенный его терминалу ПО UID в наименовании окна запущенного ПО.

4.11. Банк предоставляет Клиенту 1 терминал ПО. Клиент в праве запросить подключение дополнительных терминалов ПО. Для этого Клиент направляет в Банк Заявление на подключение ИТС «QUIK» (Приложение №46 к Регламенту). За дополнительные терминалы Банк взимает плату в соответствии с тарифами Банка.

5. УСЛОВИЯ ОТПРАВКИ И ПРИЕМА ЭЛЕКТРОННЫХ ДОКУМЕНТОВ

5.1. 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, Код подтверждения);
- формирует в СЭД текст ЭД;
- проверяет правильность составленного ЭД;
- направляет в Банк по СЭД подписанный АСП ЭД.

5.2. Процедура аутентификации состоит из двух этапов (двухфакторная аутентификация). На первом этапе Клиент вводит в специальные поля терминала ПО логин и пароль.

5.3. По факту успешной проверки соответствия логина и пароля Открытому ключу АСП Клиента Банк направляет Клиенту СМС с Кодом подтверждения на телефон указанный в Заявлении на присоединении и/или Заявлении на обслуживание на финансовых рынках и/или в Заявлении на подключение к ИТС «QUIK».

5.4. Клиент, получив СМС с Кодом подтверждения, вводит Код подтверждения в специальное поле в терминале ПО.

5.5. Процедура аутентификации считается успешно пройденной при одновременном выполнении следующих условий:

5.5.1. Клиент ввел в специальные поля терминала ПО логин и пароль, соответствующие Открытому ключу АСП;

5.5.2. Клиент ввел в специальное поле терминала ПО последовательность символов в точности совпадающей с отправленным Банком Клиенту посредством СМС Кодом подтверждения.

5.6. Банк принимает к исполнению полученные от Клиента ЭД при одновременном наличии следующих условий:

- Клиент успешно прошел процедуру аутентификации (проверку подлинности АСП и ввел корректный Код подтверждения);
- ЭД содержит АСП, прошедшую успешную проверку при помощи зарегистрированного действующего Открытого ключа АСП Клиента;
- на момент принятия ЭД у Банка нет полученного от Клиента уведомления о компрометации Закрытого ключа АСП Клиента;
- ЭД содержит все необходимые реквизиты в соответствии с предъявляемыми к нему требованиями;
- Клиентом соблюдены иные положения, закрепленные в Договоре об оказании брокерских услуг на финансовых рынках и Регламенте оказаний услуг на финансовых рынках, регулирующие условия принятия Банком к исполнению Поручений.

5.7. 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 АСП Клиента, является достаточным основанием для исполнения Банком содержащихся в таком ЭД инструкций.

5.8. 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.

5.9. В случае принятия Банком ЭД, подтверждением поступления данного документа, является присвоение следующего статуса данному документу:

- активен;
- снят;
- исполнен.

5.10. 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.

6. ОСОБЕННОСТИ ИСПОЛЬЗОВАНИЯ ПРИЛОЖЕНИЙ ДЛЯ МОБИЛЬНЫХ УСТРОЙСТВ

6.1. Клиент, обслуживаемый в ИТС «QUIK», может использовать приложения для мобильных устройств. Данная опция предоставляет Клиенту возможность подключения одного из

указанных рабочих мест: iQUIK или iQUIK-HD или QUIK-Android. Во время использования Клиентом ИТС «QUIK» Клиенту предоставляется право только 1 (одного) одновременного подключения к серверу Банка посредством мобильного коммуникационного устройства с использованием любого из приложений для мобильных устройств.

6.2. Клиент самостоятельно обеспечивает необходимые технические ресурсы для использования приложений для мобильных устройств согласно следующим условиям:

6.2.1. iQUIK функционирует на устройствах под управлением операционной системы iOS версии 4.2 или более поздней, совместимой с iPhone, iPod touch. iQUIK-HD работает на устройствах iPad и iPad2;

6.2.2. QUIK-Android функционирует на устройствах, под управлением операционной системы Android версии 2.3 или более поздней, удовлетворяющих следующим требованиям: процессор семейства ARMv7 и выше, минимальное разрешение устройства 800x480.

6.3. Клиент самостоятельно получает и устанавливает на своем мобильном устройстве программное обеспечение - Приложение для мобильных устройств. Указанное программное обеспечение загружается Клиентом через официальный интернет-ресурс компании Apple - AppStore и/или через официальный интернет-ресурс компании GOOGLE.

6.4. Обслуживание Клиента с использованием Приложений для мобильных устройств осуществляется только после подачи Клиентом Заявления на обслуживание на финансовых рынках (Приложение №4 к Регламенту), где он выразил свое желание на подключение к ИТС «QUIK» с использованием Приложений для мобильных устройств (графа 6 Заявления).

6.5. Использование ключей доступа, формирование и передача Сообщений посредством Приложений для мобильных устройств осуществляются в порядке, установленном разделами 4 и 5 настоящих Правил и Регламентом оказания услуг на финансовых рынках «Азиатско-Тихоокеанский Банк» (ПАО).

6.6. Для обмена Сообщениями с Банком посредством Приложений для мобильных устройств Клиент использует ключи доступа, сгенерированные и зарегистрированные в Банке в порядке, установленном разделом 4 настоящих Правил.

6.7. За услугу по предоставлению доступа к ИТС «QUIK» с использованием мобильных устройств Банк взимает плату в соответствии с тарифами Банка.

7. УЧЕТ И ХРАНЕНИЕ ЭЛЕКТРОННЫХ ДОКУМЕНТОВ

7.1. 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).

7.2. Все ЭД, учтенные в журнале учета, хранятся в электронных архивах Банка (далее – Контрольные архивы) не менее 5 (пяти) лет. ЭД хранятся в том же формате, в котором они были сформированы, отправлены или получены.

7.3. Банком осуществляется ежедневное резервное копирование и архивное хранение ЭД. Электронные архивы подлежат защите от несанкционированного доступа и непреднамеренного уничтожения и/или искажения.

8. КОМПРОМЕТАЦИЯ ЗАКРЫТОГО КЛЮЧА

8.1. Под компрометацией Закрытого ключа АСП Сторонами понимается утрата доверия к тому, что используемый Клиентом Закрытый ключ АСП недоступен посторонним лицам.

8.2. К событиям, связанным с компрометацией Закрытого ключа АСП, относятся:

- утрата ключевых дискет или иных носителей ключей АСП (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 ключам АСП Клиента третьих лиц.

- 8.3. В случае компрометации Закрытого ключа АСП Банк рекомендует Клиенту незамедлительно направить в Банк уведомление о компрометации ключа и прекратить направление ЭД в Банк (Приложение №3 к Правилам).

9. ПРАВА И ОБЯЗАННОСТИ СТОРОН

9.1. Клиент имеет право:

- Использовать СЭД лично или через своих Представителей, учитывая, что каждый Представитель Клиента является Владельцем ключа АСП, 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 АСП Клиента (вместе с соответствующим Закрытым ключом АСП Клиента), направив уведомление по форме Приложения №3 к настоящим Правилам, подписанное уполномоченным лицом (данное уведомление может быть направлено в Банк с использованием Личного кабинета Клиента, либо в письменном виде передано в Банк). Для продолжения дальнейшей работы в СЭД уполномоченное лицо Клиента должно сгенерировать новую Пару ключей АСП Клиента и совершить действия необходимые для регистрации Банком нового Открытого ключа АСП Клиента.
- Клиент имеет право блокировать Открытый ключ АСП Клиента, т.е. приостановить свою работу в СЭД, направив уведомление по форме Приложения №3 к настоящим Правилам, подписанное уполномоченным лицом (данное уведомление может быть направлено в Банк с использованием Личного кабинета Клиента, либо в письменном виде передано в Банк). Блокировка снимается не позднее дня, следующего за днем получения Банком письменного требования Клиента о снятии блокировки, подписанного уполномоченным лицом Клиента.

9.2. 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 АСП Клиента, направив уведомление по форме Приложения №4 к настоящим Правилам. 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 Российской Федерации.
- Банк вправе отказать в регистрации открытого ключа АСП Клиента, если подписи Владельца ключа АСП или руководителя Клиента проставлены не в присутствии уполномоченного представителя Банка или если подлинность вышеуказанных подписей не заверена нотариально.

9.3. Клиент обязуется:

- По требованию Банка представлять документы на бумажном носителе, оформленные в соответствии с требованиями действующего законодательства Российской Федерации, соответствующие полученным Банком от Клиента ЭД.
- Незамедлительно уведомлять Банк о компрометации Закрытого ключа АСП по телефону и в письменном виде.
- Своевременно уведомлять Банк об изменениях в руководстве Клиента (если Клиент является юридическим лицом), о смене лиц (Представителей клиента), уполномоченных работать с СЭД от имени Клиента, о прекращении действия доверенностей Представителей Клиента, и для возможности работы с СЭД новых лиц обеспечить им возможность сгенерировать Пару ключей АСП Клиента. Риск неблагоприятных последствий, связанных с несвоевременным уведомлением Банка о том, что необходимо приостановить действие АСП Клиента несет Клиент.
- Клиент обязан при создании ЭД в СЭД соблюдать условия настоящих Правил, нормы действующего законодательства Российской Федерации и банковские правила в отношении обязательных реквизитов данных документов.

- Клиент обязан обеспечить хранение в секрете и отсутствие доступа неуполномоченных лиц к Закрытому ключу АСП Клиента, используемого при работе в СЭД. Риск неблагоприятных последствий, связанных с использованием Закрытого ключа АСП Клиента неуполномоченными лицами, несет Клиент.

- Клиент обязан сообщать Банку об обнаружении попытки несанкционированного доступа к СЭД или к Закрытому ключу АСП Клиента в день ее обнаружения и блокировать свою работу в СЭД, направив в Банк уведомление по форме Приложения №3 к настоящим Правилам. Клиент несет риск всех последствий, связанных с несанкционированным доступом к СЭД или Закрытому ключу АСП Клиента.

- Клиент обязан по требованию Банка приостановить работу в СЭД и для ее возобновления сгенерировать новую АСП Клиента и совершить действия необходимые для регистрации Банком нового Открытого ключа АСП Клиента.

- Клиент обязан хранить свой Закрытый ключ в течение срока действия Договора об оказании брокерских услуг на финансовых рынках, а также не менее 8 (восьми) лет после его расторжения. В случае, если Клиент после расторжения Договора об оказании брокерских услуг на финансовых рынках оспаривает операции, проведенные Банком с использованием его АСП (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 АСП (в т.ч. Закрытого ключа).

9.4. 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 ключей АСП Клиента не позднее окончания рабочего дня, если уведомление было получено до 16:00 (время Московское) и не позднее окончания следующего рабочего дня после дня получения уведомления, если уведомление было получено после 16:00 (время Московское).

- Банк обязан исполнять принятые от Клиента ЭД посредством СЭД, подписанные корректной АСП Клиента, в соответствии с условиями Регламента оказания услуг на финансовых рынках и действующим законодательством Российской Федерации.

- Банк обязан при получении от Клиента уведомления по форме Приложения №3 к настоящим Правилам временно прекратить доступ к СЭД, блокировать или досрочно прекратить действие ключа АСП 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. Наложённая блокировка снимается только на основании требования письменного требования Клиента, подписанного его уполномоченным лицом, 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 Открытые ключи АСП Клиента, используемые при работе в СЭД.

- 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 Российской Федерации.

10. СОВМЕСТНЫЕ ОБЯЗАТЕЛЬСТВА И ОТВЕТСТВЕННОСТЬ СТОРОН

10.1. 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.

10.2. 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 действующей АСП, но исходил не от Клиента.

11. ПОРЯДОК РАЗРЕШЕНИЯ СПОРОВ

11.1. Стороны договорились считать наличие корректной АСП 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 АСП Клиента в оспариваемом ЭД устанавливается разрешительной комиссией в установленном ниже порядке. Иные споры разрешаются в соответствии с действующим законодательством Российской Федерации в Арбитражном суде г. Москвы.

11.2. В случае возникновения споров о наличии АСП под ЭД, бремя доказывания лежит на Стороне, не соглашающейся с наличием АСП.

11.3. В случае возникновения споров о факте внесения изменений в ЭД после его подписания АСП, бремя доказывания лежит на Стороне, утверждающей, что в данный документ были внесены изменения.

11.4. В случае возникновения споров о факте получения одной из Сторон какого-либо ЭД, подписанного АСП, бремя доказывания лежит на Стороне, не соглашающейся с фактом получения Стороной ЭД, подписанного АСП.

11.5. 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.

11.6. 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 привлечь 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 (тридцати) рабочих 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 (десять) рабочих дней.

11.7. 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 компетентный суд РФ по месту нахождения Банка.

11.8. 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; АСП Клиента в ЭД оказалась некорректной.

**Требования к программно-аппаратному обеспечению для установки и
функционирования
программного обеспечения ИТС «QUIK»**

Клиент самостоятельно и за свой счет обеспечивает технические и коммуникационные ресурсы, необходимые для подключения к системе QUIK, в том числе:

- **минимальные требования к оборудованию:**
 - процессор Pentium 4 2 Ghz или более мощный;
 - оперативная память не менее 512 Mb (рекомендуется 1 Gb);
 - не менее 2 Gb свободного пространства на диске после установки всех программ;
 - операционная система Windows 98/NT4/2000/2003/XP/Vista;
 - наличие дисководов или другого сменного носителя данных;
 - подключение к серверу QUIK по локальной сети или через сеть Интернет;
- **требования к каналу связи:**
 - протокол передачи данных TCP/IP;
 - пропускная способность канала связи не менее 14,4 Кбит/сек;
 - время прохождения сигнала (ping) до сервера QUIK не более 1 с.;
 - процент потерь пакетов данных не более 5%.

**Заявление
На регистрацию Открытых ключей АСП**

" ____ " _____ 200__ г.

_____ (далее – Клиент) просит «Азиатско-Тихоокеанский Банк» (ПАО) зарегистрировать следующие Открытые ключи АСП, предназначенные для проверки подлинности АСП Клиента под Электронными документами направляемыми посредством СЭД ИТС «QUIK»:

Идентификатор Пользователя	ID ключа

Договор на брокерское обслуживание № _____ от « __ » _____ 20__ г.

Настоящим Клиент подтверждает, что Закрытые ключи АСП, соответствующие указанным выше Открытым ключам, сформированы при помощи программного обеспечения «АРКА Текнолоджиз» полученного от «Азиатско-Тихоокеанский Банк» (ПАО), известны только Клиенту, не передавались третьим лицам и хранятся в условиях обеспечивающих невозможность доступа к ним третьих лиц.

Настоящим Клиент признает, что АСП Электронного документа корректность которого подтверждается при помощи указанных выше Открытых ключей АСП равнозначна собственноручной подписи Клиента (для Клиента – физического лица) или подписи и печати (для Клиента – юридического лица), а Электронные документы, подписанные таким АСП, порождают обязательства со стороны Клиента равные обязательствам аналогичным документам на бумажном носителе заверенным собственноручной подписью Клиента (для Клиента – физического лица) или подписью и печатью (для Клиента – юридического лица).

Должность, наименование
организации, ФИО

М.П. _____
/ _____ /

УВЕДОМЛЕНИЕ
о прекращении (приостановлении) действия
Закрытого и соответствующего ему Открытого ключей
АСП _____

(Наименование Владельца ключа АСП Клиента)

_____ уведомляет «Азиатско-Тихоокеанский Банк» (ПАО) о
том, что с
(Наименование Владельца ключа АСП Клиента)

«__» _____ 201__ г. следует считать недействительным / заблокировать на срок
(Ненужное вычеркнуть)

_____ Открытый ключ АСП _____
ID ключа: _____ и соответствующий ему Закрытый ключ АСП.

Должность, наименование
организации, ФИО

М.П. _____
/ _____ /