УТВЕРЖДЕНО:
Решением Правления
Протокол № 31 от 10.10.2016г.

Председатель Правления
АО «КОШЕЛЕВ-БАНК»

_____ /Багаев О.В.

Условия
обеспечения технического доступа
к информационно-торговой системе QUIK

САМАРА
2016 год

Оглавление

1. Общие положения

1.1. Предметом настоящих Условий являются порядок и правила предоставления Банком Клиенту технического доступа к ИТС QUIK на срок действия Договора присоединения (Приложение №3 к Условиям), а также порядок работы при использовании Клиентом УРМ и определение прав, обязанностей и ответственности Сторон, возникающих в этой связи.

1.2. Разработчиком и правообладателем исключительных авторских прав на использование ИТС является ООО «АРКА Текнолоджиз».

2. Перечень терминов и определений

2.1. Исключительно для целей и в пределах настоящих Условий Сторонами используются следующие термины и определения:

Банк – АО «КОШЕЛЕВ-БАНК», профессиональный участник рынка ценных бумаг, осуществляющий брокерскую деятельность.

Брокерская деятельность – деятельность по исполнению поручения клиента (в том числе эмитента ценных бумаг при их размещении) на совершение гражданско-правовых сделок с ценными бумагами и (или) на заключение договоров, являющихся производными финансовыми инструментами, осуществляемая на основании возмездных договоров с клиентом.

Журнал транзакций – совокупность электронных записей в базе данных сервера ИТС, содержащих информацию об операциях Клиента, осуществляемых с использованием УРМ.

Идентификационные сведения – конфиденциальные данные (коды, пароли и т.п.), известные Клиенту и используемые для защиты от несанкционированного доступа неуполномоченных лиц к ИТС от имени Клиента

Информационно-торговая система QUIK (далее – ИТС) – совокупность программно-технических средств, с помощью которых Клиент имеет возможность в режиме реального времени наблюдать за ходом торгов и совершать операции на бирже, просматривать новости, совершать иные действия, предусмотренные техническими возможностями ИТС.

Ключ доступа – уникальная последовательность данных, представленная в электронном виде на цифровом или магнитном носителе информации и предназначенная для обеспечения доступа Клиента к ИТС с использованием УРМ путем надежной взаимной идентификации, а также для защиты информации, передаваемой по каналам связи. Ключ делится на две части – открытую (публичную) и закрытую (секретную), которые также могут называться публичным и секретным ключами соответственно.

Секретный (закрытый) ключ – уникальная последовательность символов, известная только владельцу ключа доступа, предназначенная для проверки подлинности.

Публичный (открытый) ключ – уникальная последовательность символов, соответствующая секретному ключу, предназначенная для передачи другой стороне для проверки подлинности секретной части ключа.

Криптографические ключи – секретный ключ и соответствующий ему публичный ключ.

Ключевой носитель информации (далее – Ключевой НИ) – материальный (цифровой или магнитный) носитель ключа доступа.

Компрометация ключа – констатация Клиентом, владеющим криптографическими ключами, обстоятельств, при которых возможно несанкционированное использование ключа доступа неуполномоченными лицами. Под компрометацией ключа доступа понимается утрата, хищение, несанкционированное копирование, передача закрытого ключа в линию связи в открытом виде, любые другие виды разглашения содержания ключа, а также случаи, когда нельзя достоверно установить, что произошло с ключевыми носителями (в том числе случаи, когда носитель вышел из строя и доказательно не опровергнута возможность того, что данный факт произошел в результате действий злоумышленника).

Технический сбой ИТС – нарушение нормального функционирования программно-технических средств, обеспечивающих работу ИТС или ее компонентов, вследствие не контролируемых Банком причин, которое лишает Клиента возможности подать/отменить поручение или изменить его параметры при разрешенном техническом доступе Клиента в ИТС.

Удаленное Рабочее место Клиента (далее – УРМ) – программно-аппаратный комплекс с установленной ИТС.

Условия – настоящие Условия обеспечения технического доступа к информационно-торговой системе QUIK.

Термины, специально настоящим Договором не определенные, используются в значениях, установленных иными договорами между Клиентом и Банком, нормативными правовыми актами РФ, регламентами и правилами профессиональных участников рынка ценных бумаг

2.2. Все приложения к Условиям являются его неотъемлемой частью.

3. Порядок присоединения к Условиям об обеспечении технического доступа к информационно-торговой системе QUIK

3.1. Заключение Договора присоединения (Приложение №3 к Условиям) производится на условиях, предусмотренных статьей 428 Гражданского кодекса Российской Федерации для договора присоединения, путем акцепта положений Условий без каких-либо изъятий, оговорок и условий в порядке, установленном Условиями.

3.2. Для заключения Договора присоединения Клиент должен предоставить в Банк: Заявление о предоставлении доступа к информационно-торговой системе QUIK (Приложение № 1 к Условиям - для физических лиц, Приложение № 2 к Условиям - для юридических лиц).

4. Условия подключения к ИТС и эксплуатации удаленного рабочего места Клиентом

4.1. Клиент самостоятельно и за свой счет обеспечивает технические и коммуникационные средства, необходимые для установки и работы ИТС.

4.2. Программно-техническое оборудование и организационные мероприятия Клиента должны отвечать требованиям (Приложение №7 к Условиям), рекомендуемым Клиенту для осуществления качественной и безопасной работы в ИТС с помощью УРМ Клиента.

4.3. Порядок работы с ИТС определяется Руководством пользователя, разработанным обладателем исключительных прав на ПО, ознакомиться с которым Клиент может на официальном сайте Банка (http://www.koshelev-bank.ru) и на сайте разработчика программного обеспечения (http://arqatech.com).

4.4. Для работы в ИТС Клиент (его уполномоченный представитель) должен подписать Договор присоединения (Приложение №3 к Условиям), получить клиентскую часть ИТС, сформировать ключ доступа (секретный и публичный) согласно Руководству пользователя, размещенного на официальном сайте Банка (http://www.koshelev-bank.ru), и предоставить в Банк Акт приема-передачи публичного ключа в соответствии с п.п. 5.2.5 Условий.

4.5. Первоначальное подключение Клиента к ИТС осуществляется не позднее рабочего дня, следующего за днем подписания Сторонами Договора присоединения (Приложение №3 к Условиям), при условии выполнения Клиентом его обязанностей, предусмотренных Условиями и иных сопутствующих договорных отношений с Банком.

4.6. Банк вправе предоставить Клиенту возможность получать доступ к ИТС с нескольких УРМ. Количество УРМ указывается в Заявлении о предоставлении доступа (Приложение №1 или №2 к Условиям). Оплата Клиентом услуг по подключению и эксплуатации каждого УРМ осуществляется в соответствии с Тарифами, установленными Банком.

4.7. Клиент передает Банку в электронном виде публичный (открытый) ключ для идентификации его в ИТС согласно Руководству пользователя, а также предоставляет в 2 (Двух) экземплярах Акт (Приложение № 4 к Условиям). Для каждого из УРМ, зарегистрированных на одного и того же Клиента должен быть создан и передан Банку отдельный публичный ключ.

4.8. Информация обо всех операция Клиента, осуществляемых с использованием УРМ, регистрируется в журнале транзакций и может быть предоставлена Клиенту по его требованию в письменной форме на бумажном носителе за любой период времени.

4.9. Стороны признают, что выписка из журнала транзакций, представленная на бумажном носителе и заверенная Банком, является безусловным доказательством осуществления Клиентом указанных в выписке операций или отсутствия таковых..

5. Права и обязанности Сторон

5.1. Клиент имеет право:

5.1.1 Получить набор документации и программно-технических средств в Банке.

5.1.2 Получать консультации и инструкции по процедурам установки и настройке ПО, формированию и регистрации ключей от сотрудников Банка, а также информацию, связанную с использованием ИТС.

5.1.3 По своему усмотрению создавать новые криптографические ключи и регистрировать их в Банке при условии предоставления в Банк подписанного в 2 (Двух) экземплярах Акта приема-передачи публичного ключа (Приложение №4 к Условиям).

5.1.4 Приостановить (временно блокировать) свою работу в ИТС в соответствии с разделом 5 настоящих Условий .

5.1.5 Использовать ИТС в соответствии с целевым назначением.

5.1.6 Запрашивать на основании заявления в письменной форме предоставить ему информацию обо всех операция, осуществляемых с использованием УРМ, регистрируемых в журнале транзакций, на бумажном носителе за любой период времени.

5.2. Клиент обязан:

5.2.1 Обладать программно-техническим оборудованием, необходимым для работы с УРМ в исправном состоянии и количестве, достаточном для надлежащего использования ИТС. Программно-техническое оборудование и организационные мероприятия Клиента должны отвечать требованиям (Приложение №7 к Условиям), рекомендуемым Клиенту для осуществления качественной и безопасной работы в ИТС с помощью УРМ Клиента.

5.2.2 Обеспечить УРМ требования, предъявляемым для работы в ИТС

5.2.3 Соблюдать требования и положения Руководства пользователя ИТС при установке и эксплуатации программного обеспечения.

5.2.4 Самостоятельно производить генерацию ключа доступа в соответствии с Руководством пользователя.

5.2.5 Для завершения регистрации ключа(ей) доступа, заполнить и передать в Банк подписанный(ые) в 2 (Двух) экземплярах Акты приема-передачи публичного ключа Клиента (Приложение №4 к Условиям) в количестве, соответствующем количеству УРМ, указанному в Заявлении о предоставлении доступа (Приложение №1 или №2 к Условиям).

5.2.6 Обеспечивать сохранность и целостность программного комплекса УРМ Клиента.

5.2.7 Для работы в ИТС использовать клиентскую часть ИТС только на исправном и предварительно проверенном на отсутствие компьютерных вирусов УРМ Клиента.

5.2.8 Предотвращать раскрытие, воспроизведение или распространение любой информации, получаемой посредством ИТС.

5.2.9 Не допускать копирования (за исключением случаев резервирования в личных целях), декомпиляции и дизассемблирования любых программных продуктов, используемых в ИТС.

5.2.10 Обеспечить допуск к ИТС только уполномоченных лиц Клиента.

5.2.11 Хранить в тайне от посторонних лиц пароль для получения доступа к секретным ключам Клиента.

5.2.12 Строго соблюдать правила выбора пароля доступа к секретным ключам и выполнять меры снижения рисков при работе с УРМ Клиента (Приложение №7 к Условиям).

5.2.13 Извещать Банк обо всех случаях компрометации ключей доступа, в том числе об утрате уполномоченными лицами Клиента права доступа к ИТС, увольнении уполномоченных лиц, имеющих доступ к ИТС, а также в случае непреднамеренного уничтожения ключей доступа на ключевом НИ и(или) его выхода из строя/утери (кражи) незамедлительно, но не позднее рабочего дня с даты возникновения указанных обстоятельств в соответствии с разделом 6 настоящих Условий.

5.2.14 Самостоятельно обеспечить целостность, неразглашение, нераспространение ключей доступа и идентификационных сведений, а также хранить криптографические ключи и идентификационные сведения в месте, исключающем доступ посторонних лиц к ним. Ключ доступа должен храниться исключительно у Клиента (уполномоченного лица).
Клиент обязуется не предъявлять Банку требования о компенсации любого ущерба, который может быть ему причинен вследствие использования криптографических ключей и идентификационных сведений Клиента неуполномоченными лицами.

5.2.15 Ответственность за события, произошедшие вследствие нарушения положений п.п. 5.2.13 Условий, полностью возлагается на Клиента.

5.2.16 В случае расторжения Договора присоединения (Приложение №3 к Условиям) удалить установленное программное обеспечение ИТС, а также уничтожить все его резервные копии.

5.3. Клиент не вправе совершать действия, направленные на:

5.3.1 Получение сведений с помощью ИТС, не принадлежащих и не относящихся непосредственно к Клиенту или уполномочившим его на это лицам.

5.3.2 Подключение к ИТС с использованием чужого идентификатора, либо методом подбора чужого идентификатора и пароля.

5.3.3 Использование программно-технических средств с целью проникновения в локальные сети Банка.

5.3.4 Любые другие действия, содержащие предпосылки для возникновения сбоев в работе отдельных подсистем ИТС или ИТС в целом.

5.4. Банк имеет право:

5.4.1. Осуществлять контроль за порядком использования Клиентом ИТС, переданного ему в рамках настоящих Условий.

5.4.2. Приостановить технический доступ Клиента к ИТС в случае:

- несоблюдения Клиентом условий договорных отношений, связанных с осуществлением операций на биржах, а также положений Условий;

- возникновения мотивированных претензий Клиента к переданной Банком (в т.ч. посредством ИТС) информации об остатках на лицевом счете/счете депо Клиента и/или к отчету Банка по сделкам Клиента, совершенным через УРМ;
- возникновения у Банка подозрений в нарушении безопасности ИТС, технических сбоев ИТС или программно-технических средств Банка;
- невнесения Клиентом платы в соответствии с Тарифами.

5.4.3. Приостановить технический доступ Клиента к ИТС на основании распоряжения Председателя Правления Банка или заместителя Председателя Правления Банка без объяснения причин

5.4.4. В случае компрометации, либо обоснованного подозрения на компрометацию ключа доступа Клиента, заблокировать его, сообщив об этом Клиенту на адрес электронной почты, указанный Клиентом в Заявлении о предоставлении доступа (Приложение №1 и №2 к Условиям).

5.5. Банк обязан:

5.5.1. Обладать организационно-техническим оборудованием, необходимым для эксплуатации ИТС в исправном состоянии и количестве, достаточном для надлежащего обслуживания Клиентов, располагать квалифицированными кадрами, необходимыми для работы с Клиентами с использованием УРМ.

5.5.2. Содержать компьютеры Банка, на которых установлена серверная часть ИТС в служебном помещении, исключающем доступ посторонних.

5.5.3. Не допускать появления в компьютере Банка, на котором установлено ИТС вредоносных или деструктивных программ (вирусов).

5.5.4. Предоставить Клиенту следующий набор документации и программно-технических средств, необходимый для работы с УРМ:

- программное обеспечение ИТС (клиентская часть);
- Руководство пользователя по установке, настройке и эксплуатации ИТС QUIK;
- Руководство пользователя по созданию криптографических ключей;
- программа генерации криптографических ключей;
- файл с публичным ключом (ключами) серверной части ИТС QUIK.
- Программное обеспечение и инструкции размещаются на официальном сайте Банка (http://www.koshelev-bank.ru).

5.5.5. Предоставлять Клиенту необходимые рекомендации о мерах снижения рисков при работе с УРМ (Приложение №7 к Условиям) и консультации по вопросам эксплуатации ИТС, а также эксплуатационную документацию при изменении ИТС.

5.5.6. Не разглашать третьим лицам за исключением обладателей исключительных прав на ИТС и иных случаев, предусмотренных нормативными актами РФ, информации Клиента, ставшей известной Банку в ходе исполнения своих обязательств в соответствии с Условиями.

5.5.7. В порядке и на условиях, определенных положениями Условий, предоставить Клиенту технический доступ к ИТС.

5.5.8. Зарегистрировать ключи доступа Клиента при условии предоставления Клиентом в Банк Заявления о предоставлении доступа (Приложение №1 или Приложение №2 к Условиям), подписанных в 2 (Двух) экземплярах акта приема-передачи публичного ключа (Приложение №4 к Условиям), не позднее рабочего дня, следующего за днем предоставления этих документов, при условии выполнения Клиентом его обязанностей, предусмотренных Условиями и иных сопутствующих договорных отношений с Банком.

5.5.9. Уведомлять Клиента о регистрации его ключа(ей) доступа в ИТС на адрес электронной почты, указанный в Заявлении о предоставлении доступа (Приложение №1 и Приложение №2 к Условиям).

5.5.10. По требованию Клиента блокировать его ключи доступа и зарегистрировать новые ключи в соответствии с настоящими Условиями.

5.5.11. На основании заявления Клиента в течение 10 (Десяти) рабочих дней предоставлять представителю Клиента информацию обо всех операциях, осуществляемых с использованием УРМ, регистрируемых в журнале транзакций, на бумажном носителе за любой период времени.

5.5.12. Фиксировать и хранить не менее 3 (Трех) лет полученные от Клиента уведомления об утрате/компрометации/подозрении на компрометацию ключа доступа.

6. Порядок действий при компрометации ключа доступа Клиента

6.1. К событиям, на основании которых Клиент принимает решение о компрометации ключа, относятся следующие:

- утрата/хищение ключевого НИ;
- утрата ключевого НИ с последующим обнаружением;
- временный доступ неуполномоченных лиц к информации, содержащейся на ключевом НИ;

- иные обстоятельства, прямо или косвенно свидетельствующие о наличии возможности несанкционированного доступа к криптографическому ключу третьих лиц.

6.2. В случае принятия решения о компрометации ключа Клиент обязан позвонить и уведомить об этом Банк.
После идентификации Клиента по параметрам, предусмотренными договорными отношениями по брокерскому обслуживанию между Банком и Клиентом, Банк устно подтверждает факт принятия уведомления и принимает меры по прекращению доступа к ИТС с использованием скомпрометированного ключа доступа Клиента.

6.3. Не позднее банковского дня, следующего за днем уведомления о компрометации ключа посредством телефонной связи, Клиент направляет Банку уведомление о факте компрометации в письменной форме (Приложение №6 к Условиям) с указанием идентификационного номера криптографического ключа, а также даты и времени вывода его из действия. До момента постановки отметки об исполнении на письменном уведомлении Банк не несет ответственности за возможные убытки, возникшие у Клиента в результате незаконного использования ключа доступа.

6.4. Формирование нового криптографического ключа и подключение Клиента осуществляется в соответствии с процедурой, предусмотренной разделом 4 настоящих Условий.

7. Стоимость услуг и порядок расчетов

7.1. Тарифы за услуги, предоставляемые Банком по настоящим Условиям, установлены в Тарифах АО «КОШЕЛЕВ-БАНК» по брокерскому обслуживанию, публикуемых на официальном сайте Банка (http://www.koshelev-bank.ru). Банк вправе в одностороннем порядке вносить изменения в тарифы, о чем уведомляет Клиента путем размещения информации на официальном сайте Банка, в порядке, установленном Условиями предоставления брокерских услуг АО «КОШЕЛЕВ-БАНК».

7.2. Клиент обязуется оплатить услуги Банка в рамках положений Условий в срок не позднее 5 (Пятого) рабочего дня месяца, следующего за месяцем оказания услуг.

7.3. Оплата услуг производится путем списания денежных средств с любого (по усмотрению Банка) из Брокерских счетов Клиента, открытых в рамках действующих Условий предоставления брокерских услуг АО «КОШЕЛЕВ-БАНК».

8. Ответственность Сторон

8.1. Клиент несет ответственность за все действия, совершенные с использованием УРМ вне зависимости от того, кто совершал действия через УРМ Клиента.

8.2. Банк несет ответственность за надлежащее исполнение своих обязанностей в рамках настоящих Условий.

8.3. Клиент несет ответственность за раскрытие, и/или воспроизведение, и/или распространение любой иной информации, связанной с использованием УРМ в случае, если Клиент не уполномочен на ее раскрытие и/или воспроизведение, и/или распространение Банком.

8.4. Банк не несет ответственности за неисполнение или ненадлежащее исполнение обязательств в соответствии с Условиями, а также за какой-либо ущерб (включая все, без исключения, случаи потери Клиентом прибылей, прерывания деловой активности, потери информации, иные потери) связанный с использованием или невозможностью использования ИТС, нарушения нормального функционирования программно-технических средств, входящих в состав ИТС по причинам:

- сбоев, неисправностей и отказов оборудования;
- сбоев и ошибок программного обеспечения;
- сбоев, неисправностей, и отказов систем связи, энергоснабжения, иных систем жизнеобеспечения ИТС.

8.5. Банк не несет ответственности за убытки, понесенные Клиентом из-за несанкционированного использования ИТС неуполномоченными лицами, в том числе за убытки, возникшие в результате таких действий.

8.6. Банк не несет ответственности за потери или потенциальные потери Клиента, связанные с ограничением Клиенту доступа к ИТС или ограничения режимов использования ИТС.

8.7. Клиент в полном объеме компенсирует ущерб, причиненный Банку и/или третьим лицам в случае совершения любого из ниже перечисленных действий:
а) нарушения авторских прав на ИТС, принадлежащих ООО «АРКА Текнолоджиз»;
б) раскрытия, воспроизведения или распространения любой информации, получаемой посредством ИТС, если Клиент прямо не уполномочен Банком на указанное раскрытие, воспроизведение или распространение;
в) невыполнения требований на запрет:
- копирования (за исключением случаев резервирования в личных целях), декомпиляции и дизассемблирования любых программных продуктов, используемых в ИТС;
- получения сведений из ИТС, не принадлежащих и не относящихся непосредственно к Клиенту или уполномочившим его на это лицам;
- использования программно-технических средств с целью проникновения в локальные сети Банка;

- подключения к ИТС с использованием чужих идентификационных сведений либо методом их подбора;
- совершения иных действий, влекущих возникновение технического сбоя ИТС.

г) умышленной передачи ключевого НИ и/или идентификационных сведений третьим лицам.

8.8. Банк не дает никаких гарантий:

- соответствия ИТС ожиданиям Клиента относительно его функционала и качества, а также соответствия ИТС бизнес задачам Клиента, внутренним регламентам качества и требованиям, предъявляемым Клиентом к ИТС;
- отсутствия рисков возникновения убытков в связи с использованием ИТС в предпринимательской деятельности, включая риски возникновения убытков в результате обнаружения скрытых недостатков ИТС, технических сбоев, виновных действий третьих лиц, обстоятельств непреодолимой силы и так далее;
- полноты технического описания ИТС, предоставляемого Банком, ООО «АРКА Текнолоджиз» в момент заключения Договора присоединения (Приложение №3 к Условиям);
- отсутствия скрытых дефектов или недостатков ИТС, которые могут быть выявлены в процессе использования.

8.9. Присоединяясь к настоящим Условиям Стороны выражают свое согласие на обработку персональных данных, в том числе, с использованием средств автоматизации, своих персональных данных в соответствии с требованиями Федерального Закона от 27.07.2006 г. № 152-ФЗ «О персональных данных», включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование.

9. Обстоятельства непреодолимой силы

9.1. Стороны освобождаются от ответственности за неисполнение (частичное или полное), несвоевременное или ненадлежащее исполнение обязательств по настоящим Условиям в случаях, если указанное неисполнение, несвоевременное или ненадлежащее исполнение явились следствием действия обстоятельств непреодолимой силы (форс-мажорных обстоятельств), возникших после заключения Договора присоединения (Приложение №3 к Условиям) в результате событий чрезвычайного характера, которые Стороны не могли ни предвидеть, ни предотвратить разумными мерами при данных условиях.

9.2. К форс-мажорным обстоятельствам Стороны, в частности, относят стихийные бедствия природного и техногенного характера, военные действия, массовые беспорядки и забастовки, решения и действия органов государственной власти, делающие невозможным либо несвоевременным исполнение обязательств по настоящим Условиям.

9.3. Сторона, которая оказалась затронутой обстоятельствами непреодолимой силы, должна не позднее 3 (Трех) рабочих дней после наступления указанных обстоятельств уведомить об этом другую Сторону в письменной форме, указав при этом дату их наступления и характер возникновения, а также принять все возможные меры для максимального ограничения их последствий. При этом надлежащим доказательством наличия и продолжительности действия таких обстоятельств могут служить свидетельства, выданные компетентными органами власти и уполномоченными специализированными службами.

Несоблюдение условий уведомления другой Стороны о возникновении обстоятельств непреодолимой силы лишает первую Сторону права ссылаться на действие таких обстоятельств, как освобождающих от ответственности, если оно само не явилось результатом форс-мажорных обстоятельств.

9.4. Сторона, не исполнившая или ненадлежащим образом исполнившая свои обязательства по настоящим Условиям вследствие действия обстоятельств непреодолимой силы, не освобождается от ответственности за исполнение иных обязательств по настоящим Условиям, которые не могут быть признаны неисполнимыми.

9.5. Не затронутая форс-мажорными обстоятельствами Сторона вправе расторгнуть Договор присоединения (Приложение №3 к Условиям) в одностороннем порядке, если срок действия названных обстоятельств превышает 30 (Тридцать) календарных дней.

9.6. Возникновение обстоятельств непреодолимой силы в момент просрочки одной из Сторон своих обязательств по Договору присоединения (Приложение №3 к Условиям) лишает соответствующую Сторону права ссылаться на эти обстоятельства как на основание, освобождающее от ответственности.

10. Срок действия, порядок изменения и расторжения договора

10.1. Договор присоединения заключается на неопределенный срок, и вступает в силу с момента его подписания уполномоченными на то представителями Сторон.

10.2. Договор присоединения может быть расторгнут в следующих случаях:

- по инициативе любой из Сторон с предварительным уведомлением другой стороны, не менее чем за 30 (Тридцать) календарных дней до даты расторжения;
- по инициативе Банка, в случае нарушения Клиентом требований как минимум одного из п.п.4.3 или пунктов раздела 7 настоящих Условий, или в случае начатой процедуры расторжения Договора на брокерское обслуживание или договора счета депо между Банком и Клиентом со дня, следующего за днем получения Клиентом уведомления о расторжении такого Договора;
- по обоюдному согласию Сторон.

10.3. Банк вправе в одностороннем порядке вносить изменения в Условия и приложения к нему. Данные изменения вступают в силу по истечению 10 (Десяти) календарных дней с даты уведомления Клиентов о внесении таких изменений, если Банком не установлен иной срок. Датой уведомления Клиентов считается дата размещения информации о внесении таких изменений на официальном сайте Банка http://www.koshelev-bank.ru.

10.4. С целью обеспечения гарантированного ознакомления всех лиц, заключивших Договор присоединения до вступления в силу изменений или дополнений, Клиент обязан не реже 1 (Одного) раза в 10 (Десять) календарных дней знакомиться с информацией, публикуемой Банком на официальном сайте Банка. При необходимости получения дополнительных разъяснений по изменениям в Условиях Клиент вправе обратиться за ними Банк.

10.5. В случае несогласия Клиента с измененной редакцией Условий, Клиент вправе расторгнуть заключенный с Банком Договор присоединения в сроки и порядке, определенном Условиями. Если в течение 10 (Десяти) календарных дней с момента раскрытия Банком информации об изменении Условий Клиент не обратился в Банк для расторжения Договора присоединения, Стороны соглашаются, что новые положения Условий приняты Клиентом полностью.

10.6. Банк не несет ответственности, если информация об изменении положений Условий, размещенная в установленном порядке и сроки, не была своевременно получена и/или изучена и/или правильно понята Клиентом.

10.7. Любые изменения Условий с момента их вступления в силу равно распространяются на всех Клиентов, в том числе заключивших Договор присоединения ранее даты вступления изменений в силу.

Приложение № 1
к Условиям
обеспечения технического доступа
к информационно-торговой системе QUIK

ЗАЯВЛЕНИЕ
о предоставлении доступа к ИТС QUIK
(для физического лица)

Клиент_____
(фамилия, имя, отчество полностью):
проживающий (ая) по адресу_____
Адрес места жительства (регистрации):
_____
Сведения о документе, удостоверяющем личность:
вид:_____
серия: _____ номер: _____ дата выдачи: _____
кем выдан: _____
код подразделения (при наличии): _____-_____
В лице_____,
(фамилия, имя, отчество уполномоченного лица Клиента полностью)

действующего на основании _____№ _____от __/__/____ г.
(наименование документа)

настоящим прошу предоставить

☐ доступ к ИТС QUIK в качестве пользователя УРМ:

☐ первоначальное подключение

☐ повторное подключение (Код Клиента № _____) с «____» _____ 20__ г. после приостановки технического доступа к ИТС на основании п.п.5.4 Условий обеспечения технического доступа к информационно-торговой системе QUIK;

☐ возможность осуществления доступа с УРМ в количестве____(*указать прописью*) шт..

E–mail:
_____
(указать адрес электронной почты, с которого будет отправлен в Банк публичный ключ)

Клиент _____ / _____

Дата: ***«___»_____20___ г.***

СЛУЖЕБНЫЕ ОТМЕТКИ БАНКА				
Дата получения Заявления:				
Документ подписан в моем присутствии. Идентификация проведена.				
Уполномоченный сотрудник АО «КОШЕЛЕВ-БАНК»				
		(подпись)	*М.П.*	*(фамилия, инициалы)*

Приложение № 2
к Условиям
обеспечения технического доступа
к информационно-торговой системе QUIK

ЗАЯВЛЕНИЕ
о предоставлении доступа к ИТС QUIK
(для юридического лица)

Клиент_____
(полное наименование организации):
В лице_____
Действующего (ей) на основании_____
Место нахождения_____
ИНН _____
КПП _____
ОГРН _____

настоящим прошу предоставить

☐ доступ к ИТС QUIK в качестве пользователя УРМ:

☐ первоначальное подключение

☐ повторное подключение (Код Клиента № _____) с «____» _____ 20__ г. после приостановки технического доступа к ИТС на основании п.п.5.4 Условий обеспечения технического доступа к информационно-торговой системе QUIK;

☐ возможность осуществления доступа с УРМ в количестве____(*указать прописью*) шт..

E–mail:
_____
(указать адрес электронной почты, с которого будет отправлен в Банк публичный ключ)

Клиент _____ / _____

Дата: ***«___»_____20___ г.***

СЛУЖЕБНЫЕ ОТМЕТКИ БАНКА				
Дата получения Заявления:				
Документ подписан в моем присутствии. Идентификация проведена.				
Уполномоченный сотрудник АО «КОШЕЛЕВ-БАНК»				
		(подпись)	*М.П.*	*(фамилия, инициалы)*

Приложение № 3
к Условиям
обеспечения технического доступа
к информационно-торговой системе QUIK

ДОГОВОР присоединения №_____/QUIK
к Условиям об обеспечении технического доступа
к информационно-торговой системе QUIK

г. _____ «___»_____ 20__г.

_____
в лице _____
действующего (-ей) на основании _____
далее по тексту именуем___ «Клиент», с одной стороны, и Акционерное общество «КОШЕЛЕВ-БАНК», далее по тексту именуемое «Банк», в лице _____, действующего (-ей) на основании _____, с другой стороны, далее по тексту именуемые как «Сторона» в отдельности и «Стороны» совместно, в соответствии со ст. 428 ГК РФ заключили настоящий Договор о нижеследующем:

1. Условия договора

1.1. Заключая настоящий Договор, Клиент присоединяется к Условиям обеспечения технического доступа к информационно-торговой системе QUIK (далее Условия) и принимает на себя обязательства следовать всем положениям Условий (включая условия, изложенные в приложениях к Условиям, и условия и обязательства, вытекающие из Условий).

1.2. Клиент заявляет и гарантирует, что он в полном объеме ознакомлен и согласен с порядком и положениями Условий обеспечения технического доступа к информационно-торговой системе QUIK.

1.3. Права, обязанности и ответственность Сторон по настоящему Договору определены и регулируются Условиями и дополнительными соглашениями к настоящему Договору.

1.4. Вознаграждение (комиссия) Банка за предоставление доступа к ИТС QUIK взимается в соответствии с тарифами Банка.

1.5. Настоящий Договор вступает в силу после его подписания уполномоченными представителями Сторон и после предоставления Клиентом полного комплекта документов, предусмотренных Условиями.

2. Срок действия, порядок изменения и расторжения договора

2.1. Настоящий Договор заключается на неопределенный срок.

2.2. Каждая из Сторон имеет право в одностороннем порядке расторгнуть настоящий Договор с предварительным письменным уведомлением об этом другой Стороны не менее чем за 30 (Тридцать) календарных дней до планируемой даты расторжения.

2.3. Прекращение действия настоящего Договора не освобождает Стороны от обязанности завершить все расчеты между собой, установленные Условиями.

2.4. Соглашения Сторон, изменяющие или дополняющие условия настоящего Договора после его подписания, могут быть признаны действительными только в случае их совершения в письменной форме и должны рассматриваться как неотъемлемая часть настоящего Договора.

2.5. Местом заключения Договора присоединения считается место нахождения Банка (адрес его головного офиса, филиала, представительства или структурного подразделения), указанное в разделе «Реквизиты и подписи Сторон».

2.6. Клиент дает согласие на осуществление обработки своих персональных данных и их передачу третьим лицам в рамках брокерского обслуживания согласно условиям данного договора и Условий в соответствии с требованиями ФЗ № 152-ФЗ от 27.07.2006г. «О персональных данных».

2.7. Все споры и разногласия между Сторонами разрешаются путем переговоров, а при невозможности урегулировать их подобным образом передаются на рассмотрение суда по месту нахождения Банка.

2.8. Настоящий Договор составлен на русском языке в 2 (Двух) экземплярах, имеющих одинаковую юридическую силу, по одному для каждой из Сторон.

3. Реквизиты и подписи Сторон

Банк:	**Клиент:**
_____	_____
_____	_____
_____/_____/	_____/_____/
М.П.	М.П.

Приложение №4
к Условиям
обеспечения технического доступа
к информационно-торговой системе QUIK

АКТ
приема-передачи публичного (открытого) ключа

«____»_____ 20__г.

_____
далее по тексту именуем___ «Клиент», в лице _____
действующего (-ей) на основании _____,
с одной стороны, и Акционерное общество «КОШЕЛЕВ-БАНК», далее по тексту именуемое «Банк», в лице _____, действующего (-ей) на основании _____, с другой стороны, в соответствии с Договором присоединения № _____/QUIK от «___» _____ 20__г. заключили настоящий Акт приема-передачи о том, что Клиент передает, а Банк принимает публичный(ые) (открытый(ые)) ключ(и) Клиента для его регистрации и дальнейшей идентификации в ИТС со следующим содержанием:

Содержимое файла открытого ключа

Клиент понимает повышенный риск несанкционированного использования ИТС, включая компрометацию ключей доступа и идентификационных сведений и несанкционированное удаленное управление ИТС при ненадлежащем соблюдении Клиентом мер безопасности (Приложения №7 к Условиям).

Банк:	**Клиент:**
_____	_____
_____	_____
_____/_____/	_____/_____/
М.П.	М.П.

Приложение №5
к Условиям
обеспечения технического доступа
к информационно-торговой системе QUIK

АКТ
о приостановке технического доступа к ИТС

г. Самара

Настоящий акт составлен по факту приостановки технического доступа к ИТС QUIK с «___» _____ 20__г. следующему Клиенту:

Полное наименование/ ФИО:	
Код Клиента	

СЛУЖЕБНЫЕ ОТМЕТКИ БАНКА				
Дата приостановления доступа:				
Основание:				
Уполномоченный сотрудник АО «КОШЕЛЕВ-БАНК»				
		(подпись)	*М.П.*	*(фамилия, инициалы)*

Приложение №6
к Условиям
обеспечения технического доступа
к информационно-торговой системе QUIK

УВЕДОМЛЕНИЕ
о компрометации ключа доступа

Настоящим Клиент _____
(полное наименование организации/Ф.И.О. Клиента)
_____

уведомляет о компрометации ключа доступа (идентификационный номер: _____), переданного по Акту приема-передачи от «___»_____ 20__г. и использовавшегося для доступа к ИТС QUIK в соответствии с Договором присоединения № _____/QUIK от «___» _____ 20__г.

Данный ключ прошу считать скомпрометированным и выведенным из действия с _____ час. _____ мин. московского времени «___»_____ 20__г.

Клиент:
_____
_____

_____/_____/

М.П.

СЛУЖЕБНЫЕ ОТМЕТКИ БАНКА				
Дата получения Уведомления:		Блокировка произведена: ___час. ___ мин.		
Документ подписан в моем присутствии. Идентификация проведена.				
Уполномоченный сотрудник АО «КОШЕЛЕВ-БАНК»				
		(подпись)	*М.П.*	*(фамилия, инициалы)*

Приложение №7
к Условиям
обеспечения технического доступа
к информационно-торговой системе QUIK

РЕКОМЕНДАЦИИ КЛИЕНТУ
о требованиях к программно-техническому оборудованию и
о мерах снижения рисков при работе с УРМ в ИТС

1. **Минимальные требования к оборудованию и программному обеспечению Клиента**

С требованиями, рекомендуемыми Клиенту для осуществления нормального функционирования программного обеспечения ИТС, Клиент может ознакомиться на официальном сайте разработчика ИТС (http://arqatech.com/ru/products/quik/requirements/).

2. **Меры снижения риска при работе с УРМ**

2.1. Случаи повышенного риска, связанные с использованием УРМ

2.1.1. Клиент соглашается на получение услуги с использованием УРМ, осознавая, что сеть Интернет не всегда является безопасным каналом связи для передачи информации, и осознает риски, связанные с возможным нарушением конфиденциальности, и иные риски, возникающие вследствие использования такого канала доступа, в частности риск осуществления операций по брокерским счетам Клиента лицами, не обладающими правом распоряжения этими брокерскими счетами.

2.1.2. Клиент понимает повышенный риск несанкционированного использования ПО ИТС, включая компрометацию ключей доступа и идентификационных сведений и несанкционированное удаленное управление ИТС, при ненадлежащем соблюдении Клиентом мер безопасности, определенными настоящими Рекомендациями.

2.1.3. К случаям повышенного риска, связанным с использованием УРМ, относится:

- Невыполнение условий обеспечения безопасности УРМ в ИТС (п.п. 2.2.2 настоящих Рекомендаций);
- Перемещение ключей доступа со сменного носителя на жесткий диск компьютера: хранение секретных ключей вместе с программой увеличивает риск несанкционированного доступа к ИТС, следовательно, к конфиденциальной информации и управлению средствами пользователя.
- Использование пароля на вход в ИТС и пароля доступа к секретным ключам, не соответствующего минимальным требованиям к его безопасности (п.п. 2.2.3 настоящих Рекомендаций).
- Получение доступа к ИТС с УРМ, содержащего вредоносный или модифицированный код, а также на котором произведена модификация системы с целью получения доступа к файловой системе или иных прав, не предусмотренных разработчиками операционной системы.

2.2. Меры обеспечения безопасности при пользовании УРМ

2.2.1. Обеспечьте безопасность работы в ИТС:

- Установите пароль доступа к секретным ключам.
- Храните ключи доступа на сменном носителе.
- Обязательно отключайте ключевой НИ от устройства доступа в ИТС даже при кратковременном прекращении работы в системе. Используйте его исключительно для входа в систему и при отправке поручений в Банк.
- В перерывах между использованием ключевого НИ храните его в месте, доступном только Клиенту (уполномоченному представителю). Не передавайте носитель ключей третьим лицам.
- Контролируйте состояние Ваших счетов.
- При смене/увольнении уполномоченного лица, осуществляющего работу с УРМ, проинформируйте Банк о произошедших изменениях и произведите замену криптографических ключей.
- При изменении контактной информации (электронный почтовый адрес, телефон) своевременно сообщайте обновленные данные специалистам Банка.

2.2.2. Обеспечьте безопасность УРМ, с использованием которого осуществляется работа в ИТС:

- Допускать к работе на УРМ только уполномоченных лиц, обеспечить физическую безопасность устройства, на котором осуществляется работа в УРМ.
- Перед входом в ИТС необходимо удостовериться в том, что на УРМ установлено, активировано и работает современное лицензионное антивирусное программное обеспечение, регулярно обновляются его антивирусные базы. Если существуют подозрения или основания считать, что УРМ может быть заражено вирусами – не осуществляйте с него работу в системе.
- Использовать на УРМ только лицензионное программное обеспечение.

- Своевременно обновлять операционную систему УРМ, браузеры и прикладное программное обеспечение. Обновления следует устанавливать только из доверенных источников (с официального сайта производителя)
- Использовать УРМ, на котором установлена только одна операционная система.
- Осуществлять работу с ИТС с использованием отдельной учетной записи в операционной системе УРМ, защищенной сложным паролем, известным только Вам (см п.п.2.2.3 настоящих Рекомендаций) с ограниченными правами доступа.
- Установить на УРМ специальные программные и аппаратные средства защиты (антивирусное программное обеспечение, средства обнаружения вредоносных программ, средства защиты информации от воздействия вредоносного кода, персональный межсетевой экран), которые должны регулярно обновляться.
- Регулярно проводить полную антивирусную проверку УРМ.
- Не оставлять без присмотра Ваше УРМ с активной сессией работы в ИТС, блокировать доступ к УРМ при помощи пароля на время Вашего отсутствия.
- Запускать на УРМ программы, полученные только из доверенных источников (особую опасность могут представлять программы, полученные по электронной почте или из сети Интернет); не рекомендуется открывать и использовать без проведения соответствующих проверок файлы, полученные из общедоступных сетей передачи данных, для исключения программных закладок и вирусов.
- Помните, что Банк не рассылает своим Клиентам диск с программным обеспечением ИТС по почте; ссылки или указания на установку ПО через SMS/MMS/Email – сообщения. Получить программно-технические средства можно, только скачав их на официальном сайте Банка http://www.koshelev-bank.ru
- Исключить посещение с УРМ потенциально опасных Интернет-ресурсов (социальные сети, форумы, чаты, телефонные сервисы, файлообменные сервисы и т.д.), а также работу с почтовыми сообщениями, полученными из недостоверных источников.

2.2.3. При выборе пароля доступа и его хранении придерживайтесь следующих правил:

- Установить парольную защиту на вход в УРМ. Регулярно проводить смену паролей.
- Для работы с ИТС необходимо использовать только сложные пароли, удовлетворяющие следующим требованиям:
  - пароль должен иметь длину от 8 символов, в нем должно быть не менее двух цифр и двух букв, допускается использование букв латинского алфавита, цифр, знаков !#$%&()*+-./:;<=>?[\, используйте буквы верхнего и нижнего регистра.
  - обратите внимание, что регистр и язык букв пароля имеет значение.
  - пароль не должен содержать последовательности одинаковых символов и групп символов, легко угадываемые комбинации символов (dddddd, 333444555, qwerty, 12345, abc123 и т.п.)
  - пароль не должен содержать связанных с Вами данных (имена и даты рождения членов семьи, адреса, телефоны, часть номера банковской карты и т.п.)
  - пароль не должен содержать словарных слов (password, football, русские слова, набранные в английской кодировке, например, gfhjkm – пароль).
  - пароль не должен совпадать с шестью предыдущими паролями и не должен совпадать с именем входа (логином).
  - пароль не должен быть копией или комбинаций паролей, используемых Вами в других системах или Интернет-ресурсах (вход в УРМ, на электронную почту, социальные сети, развлекательный ресурсы в сети Интернет и т.п.).
- Никогда не сообщайте свой пароль третьим лицам, в том числе родственникам и сотрудникам Банка. Помните, что сотрудник Банка не имеет права запрашивать у Вас пароль, даже если Вы самостоятельно обратились в Банк. Вводите пароль только в Системе ДБО, Банк никогда не отправляет сообщений с просьбой уточнить или предоставить пароль.
- Не записывайте и не храните пароль в местах доступа третьих лиц. Запрещается хранить пароль на УРМ, а также на иных электронных носителях, доступ к которым могут получить третьи лица, в том числе в случае заражения УРМ вирусом.
- При возникновении подозрений, что Ваш пароль доступа к секретному ключу (в ИТС), стали известны третьим лицам (в том числе представившимся сотрудниками Банка), незамедлительно заблокировать доступ в ИТС, обратившись в Банк по телефону 8 (846) 933 00 00 в соответствии с разделом.6 настоящих Условий.

2.2.4. Остерегайтесь мошенничества

- Банк никогда не связывается по телефону и не осуществляет рассылок сообщений по SMS или e-mail с просьбой предоставить, подтвердить или уточнить Вашу конфиденциальную информацию (пароли, логины, паспортные данные, номер мобильного телефона, на который приходят одноразовые пароли, параметры банковских карт и другие конфиденциальные данные). Не отвечайте на такие сообщения.
- Не открывайте подозрительные файлы, присланные Вам по электронной почте. При получении подозрительного сообщения от имени Банка не отвечайте на него, не переходите по ссылкам указанным в подозрительном сообщении.
- Банк никогда не запрашивает пароль на вход в ИТС (к ключам доступа) для отмены операций. При вводе пароля Вы даете Банку право на проведение операции, отменить ее с помощью пароля нельзя.
- Если Вы самостоятельно связались с Банком, сотрудники могут уточнить у Вас персональную информацию, но не имеют права запрашивать у Вас пароль на вход в ИТС.

- Сотрудники Банка никогда не связываются по телефону, чтобы сообщить о недоступности системы вследствие проведения каких-либо регламентных работ. Если Вы получили подозрительное сообщение от имени Банка, либо с Вами связались по телефону с одной из просьб, перечисленных в данном разделе, то рекомендуется сообщить о данном факте в Банк по телефону 8 (846) 933 00 00 (никогда не связывайтесь с Банком по телефону, указанному в подозрительном сообщении).