

## **Правила обслуживания клиентов ПАО «МОСКОВСКИЙ КРЕДИТНЫЙ БАНК» с использованием ИТС QUIK**

### **1. Введение**

1.1. В настоящих Правилах используются следующие основные понятия и условные обозначения:

Актуальный список аннулированных (отозванных) сертификатов – список аннулированных (отозванных) сертификатов, являющийся последним изданным Удостоверяющим центром на данный момент времени и действующим;

Аутентификация – проверка соответствия источника информации или самой информации предъявленным идентификаторам и определение их подлинности;

Банк – ПАО «МОСКОВСКИЙ КРЕДИТНЫЙ БАНК»;

Владелец открытого ключа QUIK – физическое лицо, на имя которого выдан сертификат ключа и которое владеет закрытым и открытым ключами QUIK, однозначно соответствующими друг другу и позволяющими проводить аутентификацию Клиента;

Владелец сертификата ключа проверки ЭП (Владелец ключа ЭП) – физическое лицо, на имя которого Удостоверяющим центром выдан сертификат ключа проверки ЭП, наделенное правом подписи электронных документов электронной подписью для последующей передачи с использованием ИТС QUIK и владеющее соответствующим Закрытым ключом ЭП, позволяющим создавать ЭП в электронных документах (подписывать электронные документы);

Второй фактор аутентификации – процедура проверки Клиента посредством ввода Пароля доступа, полученного в виде сообщения по электронной почте или через сервис Google Authenticator. Является вторым этапом идентификации Клиента (после ввода Логина и Пароля) при входе в ИТС QUIK;

Дистрибутивный пакет – программное обеспечение, включающее в себя:

базовое Рабочее место Клиента в ИТС QUIK

или

Криптографическую библиотеку «КриптоПро CSP»;

Договор – договор об обмене электронными документами в ИТС QUIK, заключенный между Банком и Клиентом путем присоединения Клиента к настоящим Правилам;

Документация ИТС / Руководство пользователя – описание набора функциональных возможностей, предоставляемых ИТС QUIK, размещенное на сайте разработчика ИТС QUIK. Клиент обязан самостоятельно ознакомиться с Документацией ИТС QUIK до начала использования ИТС QUIK, а также периодически отслеживать изменения, внесенные в Документацию ИТС QUIK, в течение срока действия Договора;

Закрытый ключ QUIK (secring) – уникальная последовательность символов, известная только Клиенту и предназначенная для дешифрования потока передаваемых в ИТС QUIK данных Клиентом. Закрытому ключу QUIK однозначно соответствует парный ему открытый ключ QUIK; дешифрование кода без знания Закрытого ключа QUIK (secring) неосуществимо; выступает в качестве ключа простой электронной подписи;

Закрытый ключ ЭП – уникальная последовательность символов, известная только владельцу Сертификата Ключа проверки ЭП и предназначенная для создания ЭП в электронном документе с использованием средств ЭП (используется применительно к Квалифицированной ЭП);

Заявление – для целей настоящих Правил любое Заявление, предусмотренное Порядком и передаваемое Клиентом в Банк посредством ИТС QUIK;

Идентификатор Клиента – натуральное число (комбинация цифр), однозначно выделяющее (идентифицирующее) Клиента среди других клиентов Банка;

идентификация – процесс распознавания определенных субъектов или объектов ИТС QUIK с помощью уникальных, воспроизводимых указанной системой параметров (имен, паролей или ключей);

Идентификация Клиента – определение Банком личности Клиента по предъявленному им Идентификатору;

Интернет-сайт разработчика ПО (Сайт разработчика) – [www.arqatech.com](http://www.arqatech.com);

информационно-торговая система QUIK (ИТС QUIK) – совокупность программных средств, позволяющих Клиенту в режиме реального времени через сеть Интернет наблюдать за ходом биржевых торгов в торговой системе, подавать Банку Поручения Клиента, Сообщения (в том числе заявления и т. д.), получать от Банка Сообщения информационного и уведомительного характера в порядке, предусмотренном настоящими Правилами;

Квалифицированная электронная подпись (Квалифицированная ЭП) – электронная подпись, которая соответствует всем признакам усиленной квалифицированной ЭП, предусмотренным Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи», а именно:

1) получена в результате криптографического преобразования информации с использованием Закрытого ключа ЭП;

2) позволяет определить лицо, подписавшее электронный документ;

3) позволяет обнаружить факт внесения изменений в электронный документ после момента его подписания;

4) создается с использованием средств электронной подписи;

5) ключ проверки электронной подписи указан в Сертификате ключа проверки ЭП;

6) для создания и проверки электронной подписи используются сертифицированные средства электронной подписи, произведенные ООО «КРИПТО-ПРО» и сертифицированные ФСБ России;

7) иные признаки в соответствии с требованиями действующего законодательства;

Ключ проверки электронной подписи – уникальная последовательность символов, однозначно связанная с ключом электронной подписи и предназначенная для проверки подлинности электронной подписи (далее – проверка электронной подписи);

ключевая информация – совокупность Закрытого ключа ЭП и Закрытого ключа QUIK, принадлежащих Клиенту и находящихся на Ключевых носителях;

Ключевой носитель – физический носитель, предназначенный для размещения на нем ключевой информации. Должен использоваться токен с неизвлекаемой памятью (например, eToken, ruToken) либо иной носитель ключей. При этом в случае использования иного носителя ключей Клиент принимает и самостоятельно обрабатывает все риски, связанные с компрометацией хранимой ключевой информации;

Ключ простой электронной подписи – Закрытый ключ QUIK (secring), известный только Клиенту, использование которого при направлении Поручений позволяет однозначно идентифицировать отправителя и автора электронного документа;

Компрометация (Компрометация ключевой информации или Пароля) – утрата доверия к тому, что используемая ключевая информация или Пароль известны только Уполномоченным представителям Клиента;

Лицензии на право эксплуатации СКЗИ – разрешительные документы, дающие право на выполнение действий, предусмотренных законодательством Российской Федерации в области использования сертифицированных криптографических средств защиты информации;

Логин – имя Клиента или последовательность символов, установленная Клиентом, которая служит средством аутентификации Клиента при подключении к ИТС QUIK и является подстроками открытой части ключа в файле `pubring.txk` и закрытой части ключа в файле `secring.txk`;

Мобильная версия QUIK X – пользовательское приложение, работающее на мобильных устройствах под управлением операционной системы IOS или Android;

Несанкционированный доступ – доступ к информации или функциям ИТС QUIK лицами, не имеющими на это полномочий, например, в случае наступления события Компрометации;

Открытый ключ QUIK (pubring) – уникальная последовательность символов, соответствующая Закрытому ключу QUIK (secring), доступная обеим Сторонам и предназначенная для шифрования передаваемых данных и аутентификации Клиента. Открытый ключ QUIK может быть доступен широкому кругу лиц, при этом конфиденциальность Закрытого ключа QUIK не нарушается;

Пароль – последовательность символов, установленная Клиентом, которая служит средством защиты Закрытого ключа QUIK (secring) и используется для аутентификации Клиента при подключении к ИТС QUIK в дополнение к Логину;

Пароль доступа – цифровой код, действующий только для одного сеанса аутентификации.

Действие такого пароля ограничено определенным промежутком времени, заданным Банком;

Пин-код – последовательность символов, установленная Клиентом, которая служит ключом Простой электронной подписи при использовании Мобильной версии QUIK X и ПО WebQUIK и используется для аутентификации Клиента при подключении к ИТС QUIK;

Подлинность электронной подписи в электронном документе – положительный результат проверки соответствующим сертифицированным средством электронной подписи с использованием Сертификата ключа проверки электронной подписи или Открытого ключа QUIK принадлежности электронной подписи в электронном документе владельцу Сертификата ключа проверки электронной подписи Открытого ключа QUIK и отсутствия искажений в подписанном данной электронной подписью электронном документе;

Поручение – распоряжение Клиента, переданное в Банк с использованием ИТС QUIK, на совершение сделок (операций) в соответствии с Соглашением о предоставлении услуг на финансовых рынках путем присоединения к Порядку;

Порядок – Порядок обслуживания клиентов ПАО «МОСКОВСКИЙ КРЕДИТНЫЙ БАНК» на финансовых рынках, утвержденный в установленном в Банке порядке;

Правообладатель – Общество с ограниченной ответственностью «АРКА Текнолоджиз» (ОГРН 1155476002714);

Простая электронная подпись (Простая ЭП, ПЭП) – совокупность информации, позволяющая однозначно идентифицировать отправителя и автора электронного документа (Клиента), состоящая из идентификатора Рабочего места Клиента в ИТС QUIK (UID), Логина и Пароля и Открытого ключа QUIK (pubring) ключей или связки Логина и Пароля (WebQUIK, Мобильные версии QUIK X), используемых при аутентификации пользователя и последующей отправке данных;

ПО QUIK – программный комплекс для организации доступа к биржевым торгам, к функциям которого относится получение участником торгов биржевой информации, а также информации о собственных заявках и сделках в режиме реального времени;

ПО ИТС QUIK – рабочее место пользователя, является основным универсальным пользовательским приложением программного комплекса для торговли на биржевых рынках и доступа к рыночной информации;

ПО WebQUIK – программное обеспечение (торговый терминал, рабочее место), предоставляющее доступ к торгам и рыночной информации и работающее в окне любого популярного браузера под управлением разных операционных систем;

Рабочее место Клиента – совокупность программно-технических средств, позволяющая Клиенту установить и использовать ИТС QUIK в соответствии с функциональными возможностями. Объем информации, предоставляемый Банком на Рабочее место Клиента, определяется Банком по своему усмотрению с учетом обеспечения возможности подачи Банку Поручений Клиента и технических возможностей используемого Банком оборудования и каналов связи. Тип Рабочего места Клиента устанавливается на основании заключенного договора об использовании ИТС QUIK;

Руководство пользователя ПО – документ, разработанный Правообладателем и опубликованный на Сайте разработчика;

Сертификат ключа проверки ЭП (СКП) – электронный документ или документ на бумажном носителе, созданный аккредитованным Минкомсвязи России Удостоверяющим центром и подтверждающий принадлежность ключа проверки электронной подписи Владелец сертификата ключа проверки ЭП;

Серверная часть ПО (Сервер ПО) – совокупность программно-технических средств, включающих ПО, необходимая для исполнения Банком своих обязанностей перед Клиентом в рамках настоящих Правил;

Сообщения – для целей настоящих Правил любые документы и все типы сообщений, направляемые Банком или Клиентом друг другу в процессе проведения операций в рамках Порядка посредством ИТС QUIK, в том числе любое Поручение, Заявление, направленное посредством ИТС QUIK;

Список аннулированных (отозванных) сертификатов (САС) – электронный документ с электронной подписью уполномоченного лица Удостоверяющего центра, включающий в себя список серийных номеров сертификатов ключей ЭП, которые на момент времени формирования списка аннулированных сертификатов были отозваны;

Средства криптографической защиты информации (СКЗИ) – совокупность программно-

технических средств, обеспечивающих применение ЭП и шифрования при организации электронного документооборота;

торговая система (ТС) – площадки, в том числе внебиржевые, для заключения и исполнения сделок с Ценными бумагами / Инструментами ТС СЭЛТ или Срочных сделок в соответствии с определенными установленными процедурами, зафиксированными в Правилах ТС или иных нормативных документах, обязательных или рекомендуемых для исполнения всеми участниками ТС;

Транзакция – операция, совершаемая Клиентом в ИТС QUIK в процессе подключения к серверу, хранящаяся в электронном виде на сервере Банка;

Удостоверяющий центр – юридическое лицо, индивидуальный предприниматель либо государственный орган или орган местного самоуправления, аккредитованные Минкомсвязи России, осуществляющие функции по созданию и выдаче квалифицированных сертификатов ключей проверки ЭП, а также иные функции, предусмотренные Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи». Порядок работы Удостоверяющего центра устанавливается документами Удостоверяющего центра;

Уникальный идентификатор терминала, или Unique ID (UID) – уникальный номер терминала ИТС QUIK, зарегистрированный Банком на определенного пользователя (Клиента) в момент предоставления технического доступа к ПО;

Уполномоченное лицо Банка – работник Банка, уполномоченный выполнять действия, предусмотренные настоящими Правилами, от имени Банка;

Уполномоченный представитель Клиента – физическое лицо, имеющее в соответствии с законом либо на основании надлежащим образом оформленных доверенностей полномочия на совершение от имени Клиента действий, предусмотренных настоящими Правилами. Во всех случаях, даже когда это не обозначено прямо в тексте настоящих Правил, любые действия от имени Клиента могут осуществлять только Уполномоченные представители;

электронный документ (ЭД) – документ, информация в котором представлена в электронно-цифровой форме, а ее целостность, неизменность и авторство удостоверены путем Идентификации и Аутентификации Клиента, а также проставления Квалифицированной или Простой электронной подписи;

электронная подпись (ЭП) – информация в электронной форме, которая присоединена к электронному документу (подписываемому документу) и используется для определения лица, подписывающего информацию. Виды электронных подписей, применимых в рамках настоящих Правил:

- Квалифицированная электронная подпись (Квалифицированная ЭП/КЭП);
- Простая электронная подпись (Простая ЭП/ПЭП);

Google Authenticator – приложение для двухэтапной аутентификации, устанавливается на смартфонах Apple, мобильных устройствах под управлением ОС Android.

Прочие термины, используемые в настоящих Правилах, понимаются в соответствии с законодательством Российской Федерации, Порядком и обычаями делового оборота.

## 1.2. Область применения настоящих Правил

1.2.1. Настоящие Правила являются соглашением между ПАО «МОСКОВСКИЙ КРЕДИТНЫЙ БАНК» (далее – Банк) и Клиентом (далее – Стороны), налагающим обязательства на взаимодействующие Стороны, а также средством официального уведомления и информирования Сторон о взаимоотношениях, возникающих в процессе взаимодействия. Настоящие Правила являются неотъемлемой частью Порядка.

1.2.2. Настоящие Правила регламентируют процедуры обмена Сообщениями и обеспечения технического доступа к информационно-торговой системе QUIK, а также регулируют взаимоотношения Клиента и Банка при оказании Банком услуг:

– по предоставлению Клиенту технического доступа к информационно-торговой системе QUIK с использованием подключенного через канал связи (посредством сети Интернет) Рабочего места Клиента, позволяющего Клиенту в режиме реального времени наблюдать за ходом торгов в ТС, а также передавать Банку Поручения и/или осуществлять обмен с Банком иными электронными документами и Сообщениями, действуя в рамках Соглашения к Порядку обслуживания клиентов ПАО «МОСКОВСКИЙ КРЕДИТНЫЙ БАНК» на финансовых рынках (далее – Соглашение), заключенного между Банком и Клиентом;

– по предоставлению дополнительной информации посредством информационно-торговой

системы QUIK. Под дополнительной информацией для целей настоящих Правил понимается предоставление Клиенту доступа к дополнительному массиву финансово-экономической информации справочного, аналитического и/или новостного характера. Предоставление дополнительной информации является вспомогательной услугой и отдельно от предоставления Клиентам технического доступа к информационно-торговой системе QUIK не оказывается.

Указанные выше услуги являются дополнительными, связанными с оказанием Клиенту услуг по Соглашению, и отдельно от Соглашения не предоставляются.

Указанные в настоящих Правилах услуги не являются обязательными, и Клиент самостоятельно принимает решение о необходимости получения перечисленных услуг в рамках Соглашения путем направления в Банк соответствующего Заявления о присоединении.

Банк предоставляет дополнительные услуги при наличии технической возможности.

В рамках настоящих Правил Банк предлагает для использования Клиентом следующее программное обеспечение (ПО):

- информационно-торговая система QUIK (ИТС QUIK);
- WebQUIK;
- Мобильная версия QUIK X.

Доступ к ПО WebQUIK и Мобильной версии QUIK X может быть предоставлен Клиенту только после получения уведомления от Банка о готовности предоставить соответствующую услугу.

## **2. Общие положения**

2.1. Настоящие Правила являются стандартной формой договора присоединения, утвержденной Банком. Приложения к настоящим Правилам являются их неотъемлемой частью. Количество и содержание приложений к настоящим Правилам не является окончательным и может быть изменено и/или дополнено Банком в одностороннем порядке с соблюдением условий, установленных настоящими Правилами.

2.2. Заключение договора об использовании ИТС QUIK (далее – Договор) на условиях настоящих Правил осуществляется путем присоединения к условиям (акцепта) настоящих Правил в соответствии со ст. 428 Гражданского кодекса Российской Федерации (ГК РФ).

Для заключения Договора заинтересованные лица должны представить в Банк Заявление о присоединении к Порядку обслуживания клиентов ПАО «МОСКОВСКИЙ КРЕДИТНЫЙ БАНК» на финансовых рынках по форме приложений 1 (б), 1 (г) к Порядку, выражающих согласие Клиента на заключение Договора.

2.3. Настоящие Правила размещены в сети Интернет на сайте Банка [www.mkb.ru](http://www.mkb.ru), при этом такое размещение не является в смысле ст. 426 ГК РФ публичным предложением (офертой) Банка заключить Договор.

Заключение Договора возможно только при условии заключения между Клиентом и Банком Соглашения о предоставлении услуг на финансовых рынках путем присоединения к Порядку обслуживания клиентов ПАО «МОСКОВСКИЙ КРЕДИТНЫЙ БАНК» на финансовых рынках (далее – Соглашение). Заключение Договора между Клиентом, выбравшим Тарифный план «МКБ Онлайн», и Банком не производится.

2.4. Договор считается заключенным с момента регистрации Банком Заявления о присоединении, указанного в п. 2.2 настоящих Правил.

2.5. Клиенты, заключившие Договор, пользуются правами и принимают на себя обязательства, предусмотренные настоящими Правилами, равно как и Банк пользуется правами и принимает на себя обязательства, предусмотренные настоящими Правилами, в полном объеме.

2.6. Настоящие Правила устанавливают особенности взаимодействия Сторон посредством ИТС QUIK в дополнение к обычным способам взаимодействия Сторон по Соглашению и не отменяют и не заменяют последние.

2.7. В случае невозможности осуществления взаимодействия Сторон посредством ИТС QUIK по каким-либо, в том числе техническим, причинам или по причине ограничения Банком доступа Клиента к ИТС QUIK взаимодействие Сторон должно осуществляться способами, предусмотренными Порядком, без ущерба для взаимоотношений Сторон.

2.8. Во всех случаях, когда в настоящих Правилах прямо не установлено иное, положения Порядка распространяются на случаи взаимодействия Сторон посредством ИТС QUIK без ограничений и с учетом положений настоящих Правил.

2.9. Все взаиморасчеты Сторон, связанные с оказанием Банком Клиенту дополнительных услуг в объеме, определенном в настоящих Правилах, регулируются положениями Порядка.

2.10. Операции, осуществляемые в рамках настоящих Правил, отражаются в учете на общих основаниях и включаются в общую отчетность, предоставляемую Клиенту в соответствии с положениями Порядка.

2.11. Для обеспечения безопасности электронного документооборота в ИТС QUIK Поручения, поданные Клиентом с помощью ИТС QUIK, подписываются:

2.11.1. Аналогом собственноручной подписи отправителя – Квалифицированной ЭП владельца СКП.

или

2.11.2. Аналогом собственноручной подписи отправителя – Простой ЭП, содержащей средства для защиты передаваемой информации по телекоммуникационным каналам и метод аутентификации Клиента в ИТС QUIK с использованием Открытого ключа QUIK (pubring) и Закрытого ключа QUIK (secring), Логина и Пароля, а также дополнительного Пароля доступа в качестве средства подтверждения авторства и подлинности передаваемых Банку электронных документов.

Стороны признают, что получение электронного документа, подписанного ПЭП в порядке, установленном настоящими Правилами, эквивалентно получению подписанного собственноручной подписью соответствующей Стороны документа на бумажном носителе, оформленного в соответствии с Порядком.

Стороны признают, что применение Ключей ПЭП, Логина и Пароля Клиента при отправке электронных документов Банку обеспечивает достаточную защиту электронных документов, передаваемых с использованием ИТС QUIK, от несанкционированного доступа и рассматривается Сторонами как использование аналога собственноручной подписи Клиента в соответствии с Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи». Ни одна из Сторон не вправе оспаривать факт совершения, действительность или условия сделки только на том основании, что она была заключена с использованием или на основании электронных документов в соответствии с условиями настоящих Правил.

Поручения Клиента, созданные и/или переданные в соответствии с условиями настоящих Правил, безусловно признаются Клиентом и Банком в качестве документов, удостоверяющих факт подачи Поручений в соответствии с Порядком, и могут быть использованы в качестве достаточного доказательства при решении споров в суде.

2.12. Клиент безусловно подтверждает полномочия лиц, осуществляющих действия от имени Клиента в рамках настоящих Правил и/или направляющих Банку любой документ и/или Сообщение (включая Поручения Клиента) посредством ИТС QUIK.

2.13. Клиент обязуется:

– обеспечить доступ к системе ИТС QUIK (включая Рабочее место Клиента, Закрытый ключ QUIK и Закрытый ключ ЭП, если применимо) исключительно лицам, которые уполномочены выполнять от имени Клиента действия, предусмотренные настоящими Правилами, а также направлять в Банк любой документ и/или Сообщение (включая Поручения) посредством ИТС QUIK;

– обеспечить невозможность доступа неуполномоченных лиц к ИТС QUIK (включая Рабочее место Клиента, Закрытый ключ QUIK и Закрытый ключ ЭП, если применимо);

– возместить Банку все убытки, связанные с невыполнением вышеуказанных обязательств.

2.14. Каждая Сторона настоящим соглашается с тем, что факт:

– доступа какого-либо лица к ИТС QUIK посредством аутентификации в ИТС QUIK с использованием ключей аутентификации, Логина и Пароля, Пароля доступа (в зависимости от вида ЭП)

или

– направления таким лицом документа и/или Сообщения с использованием ИТС QUIK является неоспоримым свидетельством полномочий такого лица на осуществление действий от имени Клиента, предусмотренных в Порядке и настоящих Правилах, независимо от того, получила ли другая Сторона доверенность или иной документ, подтверждающий полномочия такого лица.

2.15. Информация по установке и запуску программного обеспечения QUIK в части, не зафиксированной настоящими Правилами, публикуется на сайте Банка в сети Интернет [www.mkb.ru](http://www.mkb.ru).

2.16. Стороны признают, что инициатором сеансов связи является Клиент. Банк не несет

ответственности за неисполнение или просрочку исполнения Поручений Клиента, если таковые произошли из-за отсутствия инициативы Клиента в установлении сеанса связи с Банком.

2.17. Консультации по вопросам технической поддержки ПО QUIK Банк осуществляет по телефону (495) 601-99-34 (доб.2) по рабочим дням с 09:30 до 19:00.

### **3. Общее описание взаимодействия Сторон**

#### **3.1. Общие положения**

3.1.1. При оказании услуг в рамках настоящих Правил Банк не является разработчиком ИТС QUIK, используемой для этих целей, не предоставляет Клиентам услуги по доступу в сеть Интернет, не выполняет функций организатора сети.

3.1.2. Исключительные права на ИТС QUIK и на все программные составляющие указанной системы принадлежат Правообладателю.

3.1.3. Услуги, предоставляемые в рамках настоящих Правил, оказываются Банком на основании договоров, заключенных Банком с разработчиком (ами) ИТС QUIK, провайдером (ами) услуг доступа к сети Интернет.

3.1.4. Банк не гарантирует и не несет ответственности перед Клиентом за правильность работы вышеуказанного программного обеспечения и не несет ответственности за возникновение у Клиента убытков (в виде реального ущерба, упущенной выгоды), косвенных убытков, иных материальных потерь, наступление которых было вызвано неправильностью работы ПО, неполадками в работе ПО.

Банк не несет ответственности за неполадки в работе ПО и за их устранение. Банк обязуется, тем не менее, предпринять по просьбе Клиента и за его счет разумные усилия для содействия организации технической поддержки ПО силами Правообладателя.

3.1.5. Использование Клиентом ИТС QUIK не требует получения Клиентом каких-либо лицензий.

В соответствии с настоящими Правилами Клиент НЕ приобретает исключительных прав на использование ИТС QUIK, а также каких-либо прав на его передачу, воспроизведение или распространение.

3.1.6. Для обеспечения возможности получения услуг в рамках настоящих Правил Клиент самостоятельно обеспечивает доступ в сеть Интернет, приобретает необходимое оборудование и/или программное обеспечение для эксплуатации ИТС QUIK.

3.1.7. Информация по использованию систем ИТС QUIK в части, не зафиксированной настоящими Правилами, регламентируется руководством пользователя ИТС QUIK, публикуемым на сайте Банка в сети Интернет ([www.mkb.ru](http://www.mkb.ru)).

3.1.8. Информация о лимитах денежных средств и/или ценных бумаг, предоставляемая Клиенту в течение торгового дня средствами ИТС QUIK, не является официальной и предоставляется Клиенту только для удобства осуществления операций.

3.1.9. Для подтверждения фактов осуществления Сторонами тех или иных действий, а также содержания таких действий, включая, но не ограничиваясь, факты подачи / получения любых Сообщений, переданных с использованием ИТС QUIK, в том числе подачи Банку Поручений Клиента, изменения либо отмены поданных Банку Поручений Клиента посредством ИТС QUIK, осуществляется сохранение данных (логирование) действий Клиентов по совершаемым транзакциям. Срок хранения Банком данных (логов) по транзакциям составляет не менее 5 (Пяти) лет.

3.1.10. Банк может отказать Клиенту в предоставлении услуг, предусмотренных настоящими Правилами.

#### **3.2. Особенности приема Банком Поручений посредством ИТС QUIK**

3.2.1. Все Поручения Клиента, созданные и/или переданные с использованием ИТС QUIK, принимаются Банком к исполнению наравне с Поручениями, поданными иными предусмотренными Порядком способами. Поручения Клиента, содержащие одинаковые обязательные элементы, но по каким-либо причинам поданные Клиентом в различных формах и/или различными способами, рассматриваются Банком как разные Поручения Клиента, каждое из которых подлежит исполнению в соответствии с Соглашением, если иное не согласовано Сторонами отдельно в соответствующем Поручении Клиента при подаче каждого такого Поручения.

Обязательными элементами Поручений Клиента, создаваемых и/или передаваемых с

использованием ИТС QUIK, являются элементы, ввод (заполнение) которых является необходимым для надлежащей работы ИТС QUIK.

3.2.2. Учитывая возможности, предоставляемые торговой системой и Разработчиком ИТС QUIK, ИТС QUIK может допускать ввод Поручений Клиента, тип которых отличается от описанных в Порядке или содержащих отличные элементы и/или дополнительные спецификаторы. Если иное не установлено Банком в одностороннем порядке, все типы Поручений Клиента, а также любые их элементы и/или дополнительные спецификаторы, реализованные и допустимые к использованию в ИТС QUIK, признаются Сторонами допустимыми при осуществлении ими взаимодействия в рамках настоящих Правил и Порядка.

3.2.3. При этом использование предоставленных торговой системой и разработчиком ИТС QUIK возможностей ИТС QUIK может приводить к определенным ограничениям в использовании предусмотренных Порядком типов Поручений Клиента и/или их элементов или дополнительных спецификаторов. Указанные ограничения при осуществлении Сторонами взаимодействия в рамках настоящих Правил признаются Сторонами не нарушающими взаимных прав и обязанностей Сторон.

3.2.4. Настоящим Стороны договорились, что все Поручения Клиента, создаваемые и/или передаваемые Клиентом посредством ИТС QUIK, имеют срок действия в соответствии с функциональными возможностями ИТС QUIK и торговых систем и указываются Клиентом в электронной форме Поручения Клиента в ИТС QUIK.

3.2.5. Учитывая возможности ИТС QUIK, Стороны договорились использовать (только при взаимодействии по настоящим Правилам) элементы и/или спецификаторы инструментов финансового рынка, установленные и определенные ИТС QUIK.

3.2.6. Регистрация Поручений Клиента, создаваемых и/или передаваемых Клиентом с использованием ИТС QUIK, и присвоение им входящего номера, ссылка на который обязательна при дальнейшем взаимодействии Сторон, связанном с конкретным Поручением Клиента (процедура идентификации Поручений Клиента), осуществляется средствами ИТС QUIK.

3.2.7. Отмена Поручения Клиента, созданного и/или переданного Клиентом ранее с использованием ИТС QUIK и/или способами связи, предусмотренными Порядком, осуществляется средствами ИТС QUIK путем выполнения соответствующих команд / осуществления действий, предусмотренных для этих целей функциональными возможностями ИТС QUIK.

3.2.8. Исполнение полученных Банком Поручений Клиента, созданных и/или переданных Клиентом с использованием ИТС QUIK, осуществляется в общем порядке, предусмотренном Порядком.

3.2.9. Приостановка доступа Клиента к ИТС QUIK по каким-либо причинам, в том числе техническим или по причине ограничения Банком доступа Клиента к ИТС QUIK, не влияет на исполнение Поручений Клиента, поданных до момента приостановки.

3.2.10. Все действия, совершенные с Рабочего места Клиента с использованием Ключа ЭП, при работе через ИТС QUIK признаются совершенными Клиентом. Клиент принимает на себя риск:

- совершения действий на Рабочем месте Клиента с использованием Ключа ЭП Клиента лицом, не имеющим на то полномочий;
- ошибок в Поручениях Клиента;
- получения Несанкционированного доступа к Рабочему месту Клиента третьими лицами;
- несвоевременного получения Банком информации о Компрометации ключей ЭП.

3.2.11. Банк настоящим уведомляет Клиента, а Клиент, подавая Поручение на совершение в интересах Клиента Сделок с использованием ИТС QUIK, принимает и соглашается с тем, что:

- Поручения Клиента, созданные и/или переданные с использованием ИТС QUIK, автоматически (моментально) формируют заявку Банка на сделку;
- Банк не анализирует условия сделок, которые подлежат заключению по Поручению Клиента, а принимает Поручения к исполнению в рамках установленного Банком в отношении Клиента лимита.

Клиент самостоятельно принимает решение в отношении возможности подачи Банку Поручений на совершение в интересах Клиента сделок, определяет приемлемый для Клиента вид такой сделки и ее условия.

Клиент, подавая Поручение на совершение сделок с использованием ИТС QUIK, принимает на себя всю ответственность и риски, возникающие в связи с заключением Банком в интересах Клиента сделок по Поручениям Клиента, переданным Клиентом с использованием ИТС QUIK.



Банк не несет ответственности за исполнение ошибочных Поручений Клиента, поданных Клиентом самостоятельно через ИТС QUIK.

### **3.3. Информационное обслуживание**

3.3.1. Предоставляемая в рамках информационного обслуживания через ИТС QUIK информация не принадлежит Банку и является собственностью соответствующих информационных агентств, указание на которые всегда сопровождает такую информацию.

3.3.2. Предоставляя Клиенту в соответствии с настоящими Правилами доступ к информации, принадлежащей и распространяемой информационными агентствами, Банк не несет в отношении данной информации никакой ответственности за полноту, точность, своевременность, достоверность и другие существенные характеристики такой информации.

### **3.4. Действия Сторон при возникновении сбоев**

3.4.1. Независимо от причин и источников возникновения технических проблем (сбоев), препятствующих нормальному взаимодействию Сторон по настоящим Правилам, Сторона, нормальной работе которой препятствуют возникшие сбои, обязана незамедлительно уведомить о случившемся другую Сторону.

3.4.2. При возникновении любых технических проблем или сбоев Клиент обязан максимально быстро связаться с Банком по телефону +7 (495) 601-99-34 (доб.2) или электронной почте [quik@mkb.ru](mailto:quik@mkb.ru) для выяснения причин технических проблем или сбоев, а также по телефону +7 (495) 601-99-34 (доб.2) для принятия Клиентом решения в отношении переданных Банку, но не исполненных Поручений Клиента, если таковые имеются.

3.4.3. В случае любых технических проблем или сбоев Клиент имеет право предоставить в Банк любым способом, предусмотренным Порядком, поручение на отмену ранее поданного и неисполненного Поручения Клиента. Неотмененные Поручения Клиентов считаются действительными, надлежаще оформленными и исполняются в обычном режиме.

3.4.4. Банк не несет ответственность за технические сбои, возникшие не по вине Банка.

### **3.5. Компрометация Закрытого ключа ЭП и/или Закрытого ключа QUIK. Внеплановая замена ключевой информации и СКП**

3.5.1. Компрометация Закрытого ключа ЭП или Закрытого ключа QUIK

3.5.1.1. К событиям, на основании которых Клиент может принять решение о Компрометации, относятся, включая, но не ограничиваясь, следующие события:

- а) потеря ключевых носителей;
- б) потеря ключевых носителей с их последующим обнаружением;
- в) увольнение работников Клиента, имевших доступ к ключевой информации;
- г) нарушение установленных правил хранения и уничтожения (после окончания срока действия) Закрытого ключа ЭП или Закрытого ключа QUIK;
- д) возникновение подозрений на утечку информации или ее искажение в системе электронного документооборота;
- е) нарушение печати на сейфе с ключевыми носителями;
- ж) случаи, когда нельзя достоверно установить, что произошло с ключевыми носителями (в том числе случаи, когда ключевой носитель вышел из строя и доказательно не опровергнута возможность того, что данный факт произошел в результате несанкционированных действий злоумышленника).

В случае принятия решения о Компрометации Закрытого ключа ЭП или Закрытого ключа QUIK Клиент обязан в самые короткие сроки известить Банк о принятом решении по телефону (495) 601-99-34 (доб.2), по адресу электронной почты [quik@mkb.ru](mailto:quik@mkb.ru) (соответствующее сообщение должно быть отправлено с электронного адреса, указанного Клиентом в Заявлении о присоединении, составленном по форме приложений 1 (б), 1 (г) к Порядку) или через Личный кабинет (при наличии технической возможности).

3.5.1.2. В случае извещения Клиентом Банка по телефону или электронной почте о Компрометации Закрытого ключа ЭП и/или Закрытого ключа QUIK, Банк не позднее 1 часа приостанавливает прием, регистрацию и исполнение Поручений Клиента через ИТС QUIK, а также передачу Клиенту электронных документов и сообщений посредством ИТС QUIK.

В случае отзыва Открытого ключа QUIK через Личный кабинет, в Личном кабинете статус ключа меняется на «Отозван дд.мм.гггг».

3.5.1.3. Не позднее окончания рабочего дня, в который Клиент сообщил Банку по телефону

или электронной почте о факте Компрометации, Клиент направляет письменное:

– Заявление на блокировку Сертификата ключа проверки электронной подписи (приложение 5 к настоящим Правилам)

или

– Заявление на аннулирование ключей аутентификации (приложение 2 к настоящим Правилам).

После успешной процедуры идентификации Клиента и его полномочий, регламентированной условиями Соглашения, Банк осуществляет блокировку Сертификата ключа проверки ЭП и/или Открытого ключа QUIK (pubring) в самые короткие сроки, но не позднее одного рабочего дня с даты извещения о факте Компрометации.

3.5.1.4. При появлении квалифицированного СКП Клиента в списках аннулированных сертификатов, публикуемых аккредитованным Удостоверяющим центром, выдавшим СКП, Сертификат ключа проверки ЭП Клиента считается аннулированным. В этом случае Банк приостанавливает прием, регистрацию и исполнение Поручений Клиента через ИТС QUIK, а также передачу Клиенту электронных документов и сообщений посредством ИТС QUIK, уведомляя об этом Клиента способами связи, предусмотренными Соглашением. При принятии Банком решения о факте Компрометации Закрытого ключа ЭП Клиента Банк уведомляет об этом Клиента способами связи, предусмотренными Соглашением. С момента принятия Банком решения о факте Компрометации Закрытого ключа ЭП Клиента Сертификат ключа проверки ЭП считается аннулированным.

3.5.1.5. Вне зависимости от того, аннулирован Закрытый ключ ЭП и/или Закрытый ключ QUIK вследствие Компрометации или отзыва Удостоверяющим центром, возобновление использования ИТС QUIK происходит после осуществления Клиентом действий по замене Закрытого ключа ЭП и Закрытого ключа QUIK средствами СКЗИ и самостоятельной смене Логина и Пароля Клиента в соответствии с процедурой, изложенной в главе 5 настоящих Правил.

#### **4. Порядок получения и использования информационно-торговой системы QUIK с применением Квалифицированной электронной подписи<sup>1</sup>**

##### **4.1. Средства ЭП**

4.1.1. Стороны принимают, что в качестве средств Квалифицированной ЭП Клиентом используется ПО СКЗИ КРИПТО-ПРО CSP, имеющее действительные на момент использования сертификаты ФСБ России, подтверждающие соответствие программного обеспечения требованиям к средствам электронной подписи, ООО «Крипто-Про».

4.1.2. Стороны признают, что Квалифицированная ЭП, сформированная в соответствии с п. 4.1.1 настоящих Правил, соответствует всем признакам и требованиям, предъявляемым к усиленной Квалифицированной ЭП и предусмотренным Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи».

4.1.3. Стороны признают, что средства Квалифицированной ЭП, используемые в рамках настоящих Правил:

– позволяют установить факт изменения подписанного электронного документа после момента его подписания;

– обеспечивают практическую невозможность вычисления ключа ЭП из ЭП или из ключа ее проверки;

– не нарушают конфиденциальности информации, циркулирующей в системе.

4.1.4. Стороны обязуются использовать средства Квалифицированной ЭП, полученные легальным путем.

4.1.5. Стороны обязуются использовать средства Квалифицированной ЭП в соответствии с лицензионными ограничениями и требованиями по эксплуатации, предъявляемыми производителем СКЗИ и размещаемыми производителем на своем сайте <https://www.cryptopro.ru/support/docs>.

Клиент обязуется исполнять требования информационной безопасности при доступе к ИТС QUIK, размещенные в приложении 7 к настоящим Правилам.

4.1.6. Средства электронной подписи выдаются Банком Клиенту во временное пользование на срок действия Соглашения / использования ИТС QUIK, оформленного в установленном

---

<sup>1</sup> При наличии технической возможности.

настоящими Правилами порядке, либо приобретаются Клиентом самостоятельно. При этом Клиент обеспечивает приобретение и использование средств ЭП, соответствующих установленным п. 4.1 настоящих Правил требованиям.

При расторжении Соглашения или отказе от использования ИТС QUIK в установленном настоящими Правилами порядке Клиент обязуется удалить средства ЭП, переданные Банком, со средств вычислительной техники, использовавшихся для формирования и проверки ЭП.

4.1.7. Стороны принимают, что при необходимости эталонные образцы средства Квалифицированной ЭП и СКЗИ могут быть запрошены у соответствующего производителя СКЗИ.

## **4.2. Сертификаты ключей проверки ЭП**

4.2.1. Клиенты обязуются использовать, принимать и признавать Сертификаты ключей проверки ЭП, изданные Удостоверяющим центром (УЦ), в составе и формате, определяемом документами УЦ.

4.2.2. Стороны признают, что Закрытые ключи ЭП, подлежащие сертификации УЦ, формируются каждым Клиентом самостоятельно либо сертифицированным УЦ.

4.2.3. Банк обязуется реализовать поддержку УЦ (кроме УЦ, не поддерживающих технологии работы со средством электронной подписи КриптоПро CSP), выдавшего Сертификат проверки ключа ЭП Клиенту, в ИТС QUIK в срок не более 3 (Трех) дней с момента подачи заявления Клиентом.

4.2.4. СКП признается изданным УЦ, если подтверждена подлинность ЭП владельца СКП с использованием средства ЭП и СКП уполномоченного лица УЦ.

4.2.5. Стороны принимают, что идентификационные данные, занесенные в соответствующее поле СКП, однозначно идентифицируют владельца СКП и соответствующего Закрытого ключа ЭП и соответствуют идентификационным данным, зарегистрированным в УЦ.

4.2.6. Стороны признают, что в силу части 2 статьи 14 Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи» персональные данные, внесенные в Сертификат ключа проверки ЭП, подлежат опубликованию и являются общедоступной информацией, предоставление которой участникам электронного взаимодействия является обязанностью УЦ.

4.2.7. Стороны принимают, что для определения действительности СКП используется список аннулированных сертификатов, издаваемый и публикуемый УЦ в порядке и с периодичностью, которые определяются документами УЦ.

4.2.8. Электронный документ, подписанный ЭП, принадлежащей Клиенту (или его уполномоченному лицу), и полученный Банком, не влечет правовых последствий, если до момента получения данного электронного документа Банком последний был уведомлен отправителем об отсутствии полномочий у лица, на имя которого зарегистрирован СКП, и/или об иных обстоятельствах, свидетельствующих об отсутствии у Клиента (уполномоченного им лица), на имя которого зарегистрирован СКП, возможности подписать такой электронный документ в определенный момент времени, и/или о том, что СКП аннулирован в соответствии с п. 3.5.1.4 настоящих Правил. Уведомление может осуществляться способом, предусмотренным Порядком.

4.2.9. Использование Клиентом для подписания (подготовки, формирования) электронных документов в соответствии с настоящими Правилами возможно только после подписания двумя Сторонами акта признания ключа проверки ЭП по форме приложения 3 к настоящим Правилам (для юридических лиц или индивидуальных предпринимателей) или по форме приложения 4 к настоящим Правилам (для физических лиц).

## **4.3. Плановая замена ключевой информации и Сертификатов ключей проверки ЭП**

4.3.1. Проведение плановой замены криптографических ключей и СКП Клиента является обязательным условием эксплуатации системы криптографической защиты информации и осуществляется в порядке, установленном УЦ.

4.3.2. Формирование Клиентом электронных документов с применением новых криптографических ключей возможно только после подписания двумя Сторонами акта признания ключа проверки ЭП по форме приложения 3 (для юридических лиц или индивидуальных предпринимателей) или по форме приложения 4 (для физических лиц) к настоящим Правилам.

## **4.4. Процедура начала работы**

4.4.1. При получении Банком от Клиента Заявления о присоединении с указанием (выбором) в Заявлении о присоединении использования ИТС QUIK с Квалифицированной ЭП – с внешним подключаемым программным обеспечением СКЗИ КРИПТО-ПРО CSP, имеющим действительные

на момент использования сертификаты ФСБ России, подтверждающие соответствие программного обеспечения требованиям к средствам электронной подписи, ООО «Крипто-Про» (далее – ИТС с Квалифицированной ЭП), Банк передает Клиенту Дистрибутивный пакет на цифровом носителе Клиента или Клиент самостоятельно получает Дистрибутивный пакет на сайте Банка.

4.4.2. При использовании Квалифицированной ЭП создание и регистрация Ключей ЭП осуществляется в следующем порядке:

4.4.3. Клиент самостоятельно осуществляет следующие последовательные действия:

4.4.3.1. В отношении Квалифицированной ЭП:

– в соответствии с правилами аккредитованного Минкомсвязи России УЦ получает или генерирует Закрытый ключ ЭП и Сертификат ключа проверки ЭП;

– передает в Банк Сертификат ключа проверки ЭП в виде электронного документа на адрес электронной почты quik@mkb.ru и устанавливает его на Рабочее место Клиента;

– подписывает два экземпляра акта признания ключа проверки ЭП. При этом Клиент контролирует правильность заполнения полей акта признания ключа проверки ЭП;

– выполняет настройки ИТС QUIK для работы с Квалифицированной ЭП.

4.4.3.2. С Дистрибутивным пакетом:

– осуществляет установку Рабочего места Клиента;

– генерирует (создает) Закрытый и Открытый ключи QUIK к ИТС QUIK;

– в процессе генерации Клиент самостоятельно присваивает Логин и Пароль, которые будут использоваться при аутентификации пользователя ИТС QUIK;

– файл ключа (pubring.txk) направляет на адрес электронной почты quik@mkb.ru или на адрес электронной почты Уполномоченного лица (сотрудника) Банка либо посредством Личного кабинета;

– файл ключа (secring.txk) хранится на индивидуальном носителе / компьютере пользователя ИТС QUIK.

4.4.4. Банк осуществляет следующие последовательные действия:

4.4.4.1. В отношении Квалифицированной ЭП:

– проверяет Сертификат ключа проверки ЭП Клиента на соответствие требованиям, предъявляемым к квалифицированным сертификатам ключа проверки ЭП, установленным Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи»;

– в случае отрицательного результата проверки Сертификата ключа проверки ЭП Клиента Банк извещает Клиента способами связи, предусмотренными Соглашением, о необходимости повторного выполнения процедуры получения Сертификата ключа проверки ЭП в соответствии с п. 4.4.4.1 настоящих Правил;

– в случае положительного результата проверки Сертификата ключа проверки ЭП Клиента Банк:

1) передает Клиенту для подписи два экземпляра акта признания ключа проверки ЭП;

2) регистрирует Сертификат ключа проверки ЭП Клиента в ИТС QUIK после получения подписанного Клиентом экземпляра акта признания ключа проверки ЭП.

4.4.4.2. В отношении Открытого ключа QUIK:

– после получения Открытого ключа QUIK (pubring.txk) Банк готовит и передает Клиенту (на бумажном носителе или с использованием Личного кабинета) для подписания акт приема-передачи ключей аутентификации (приложение 1 к настоящим Правилам), содержащий следующие сведения:

1) Логин пользователя системы ИТС QUIK;

2) содержание ключа pubring.txk;

3) UID;

– регистрирует Открытый ключ QUIK после получения подписанного Клиентом экземпляра акта приема-передачи ключей аутентификации на бумажном носителе или с использованием Личного кабинета.

Не позднее двух рабочих дней с момента подписания Клиентом акта признания ключа проверки ЭП и акта приема-передачи ключей аутентификации Клиент получает возможность совершать операции с использованием ИТС QUIK.

**4.5. Процедура замены ключевой информации, Пароля, присвоенных Клиенту**

4.5.1. Замена ключевой информации или Пароля осуществляется Клиентом по собственному усмотрению и самостоятельно:

4.5.1.1. По инициативе Клиента или по окончании срока действия Сертификата ключа проверки ЭП или Открытого ключа QUIK, если в акте приема-передачи ключей аутентификации указан срок действия ключей аутентификации (использование ключевой информации, срок действия Сертификата ключа проверки ЭП или Открытого ключа QUIK которой истек, прекращается автоматически).

Клиент не позднее чем за 5 (Пять) рабочих дней до планируемой даты прекращения использования ключевой информации выполняет процедуры в соответствии с п. 4.4.3.2 настоящих Правил.

4.5.1.2. При Компрометации ключевой информации или Пароля Клиент осуществляет действия в соответствии с п. 3.5 настоящих Правил.

#### **4.6. Порядок проверки ЭП**

4.6.1. Проверка электронной подписи в электронных документах осуществляется в соответствии с технологической документацией производителя средств ЭП.

4.6.2. Исходными данными для процедуры проверки ЭП являются:

- электронный документ, переданный Клиентом и подписанный его ЭП;
- сертификат ключа проверки ЭП Клиента, подписавшего электронный документ;
- сертификат УЦ, выпустившего сертификат ключа проверки ЭП Клиента.

4.6.3. Электронная подпись в электронных документах, передаваемых Клиентом, признается действительной до тех пор, пока решением суда не установлено иное, при одновременном соблюдении следующих условий:

– Сертификат ключа проверки ЭП создан и выдан аккредитованным Минкомсвязи России УЦ, аккредитация которого действительна на день выдачи указанного сертификата;

– Сертификат ключа проверки ЭП действителен на момент подписания электронного документа (при наличии достоверной информации о моменте подписания электронного документа) или на день проверки действительности указанного сертификата, если момент подписания электронного документа не определен;

– имеется положительный результат проверки принадлежности владельцу Сертификата ключа проверки ЭП электронной подписи, с помощью которой подписан электронный документ;

– подтверждено отсутствие изменений, внесенных в электронный документ после его подписания;

– Квалифицированная ЭП используется с учетом ограничений, содержащихся в Сертификате ключа проверки ЭП лица, подписывающего электронный документ (если такие ограничения установлены).

4.6.4. Проверка ЭП должна осуществляться средствами ЭП, предусмотренными п. 4.1 настоящих Правил, и с использованием Сертификата ключа проверки ЭП лица, подписавшего электронный документ.

4.6.5. Сертификат ключа проверки ЭП, используемый при проверке электронной подписи, должен соответствовать положениям п. 4.2 настоящих Правил.

### **5. Порядок получения и замены Простой электронной подписи для использования информационно-торговой системы QUIK**

#### **5.1. Процедура начала работы**

5.1.1. В соответствии с п. 2.2 настоящих Правил Клиент предоставляет в Банк Заявление о присоединении к Порядку обслуживания клиентов ПАО «МОСКОВСКИЙ КРЕДИТНЫЙ БАНК» на финансовых рынках по форме приложений 1 (б), 1 (г) к Порядку.

После регистрации Банком полученного от Клиента Заявления о присоединении Банк передает Клиенту Дистрибутивный пакет на цифровом носителе или направляет Дистрибутивный пакет на электронную почту, указанную в Заявлении о присоединении, или Клиент самостоятельно получает Дистрибутивный пакет на сайте Банка.

5.1.2. Клиент самостоятельно в соответствии с инструкцией, встроенной в Дистрибутивный пакет, последовательно осуществляет следующие действия:

- осуществляет установку Рабочего места Клиента;
- присваивает Логин и Пароль, которые впоследствии будут использоваться при Аутентификации Клиента.

Для версий ПО, в которых доступ осуществляется с использованием Ключей ПЭП, для завершения получения технического доступа к ПО Клиент в соответствии с Руководством

пользователя ПО создает Открытый и Закрытый ключ QUIK.

В результате у Клиента должны сформироваться два файла:

- файл с содержанием Открытого ключа QUIK (pubring.txk),
- файл с содержанием Закрытого ключа QUIK (secring.txk), который хранится на индивидуальном носителе или компьютере Клиента.

Файл с содержанием Открытого ключа QUIK (pubring.txk) направляется Клиентом на электронную почту quik@mkb.ru или посредством Личного кабинета для размещения на сервере Банка.

После получения от Клиента файла с содержанием Открытого ключа QUIK (pubring.txk) по электронной почте Банк готовит и передает Клиенту для подписания акт приема-передачи ключей аутентификации (далее – Акт) (приложение 1 к настоящим Правилам), содержащий следующие сведения:

- Логин, присвоенный Клиентом;
- содержимое Открытого ключа QUIK (pubring);
- UID.

Открытый ключ QUIK (pubring.txk) считается зарегистрированным Банком: а) с момента подписания Клиентом и передачи в Банк Акта на бумажном носителе; б) для Клиентов, предоставивших Открытый ключ (pubring.txk) посредством Личного кабинета – с момента появления новости о регистрации Открытого ключа QUIK в Личном кабинете (при наличии технической возможности).

Не позднее 2 (Двух) рабочих дней с момента получения Банком подписанного Акта / появления новости о регистрации Открытого ключа QUIK в Личном кабинете Клиент получает возможность подавать Поручения с использованием ИТС QUIK.

Клиент после регистрации Банком Открытого ключа QUIK (pubring.txk) осуществляет подключение к ИТС QUIK с использованием присвоенного Логина и Пароля, а также Пароля доступа, полученного при использовании двухфакторной аутентификации.

## **5.2. Использование Пароля доступа**

5.2.1. Механизм двухфакторной аутентификации позволяет снизить вероятность возникновения попыток Несанкционированного доступа, происходящих по причине утраты либо кражи Ключей доступа к системе ИТС QUIK Клиента злоумышленниками.

5.2.2. Клиент при каждом подключении к ПО QUIK наряду с обычными параметрами (Логин и Пароль для защиты Закрытого ключа QUIK (secring.txk)) вводит дополнительную информацию (Пароль доступа).

5.2.3. Инструкцию по получению и использованию Пароля доступа Банк направляет Клиенту на электронную почту, указанную в Заявлении о присоединении, в течение 2 (Двух) рабочих дней после регистрации Банком Заявления о присоединении.

5.2.4. При возникновении любых технических проблем (в том числе если при подключении к ИТС QUIK не поступило сообщение с Паролем доступа) или сбоев Клиент обязан максимально быстро связаться с Банком по телефону (495) 601-99-34 или электронной почте **quik@mkb.ru** для выяснения причин возникновения технических проблем или сбоев, а также для принятия Клиентом решения в отношении переданных Банку, но неисполненных Поручений Клиента, если таковые имеются, а также подачи новых Поручений.

5.3. При первом входе в ПО Клиент до совершения любых действий (в том числе подачи электронных документов / совершения операций) обязан сверить присвоенный его терминалу ПО UID в наименовании окна запущенного ПО (в случае отсутствия технической возможности просмотра UID необходимо воспользоваться альтернативной версией ПО) с полученным от Банка сообщением о регистрации Открытых ключей QUIK.

В случае совпадения ключей Клиент признает, что Закрытый ключ QUIK, соответствующий зарегистрированному Открытому ключу QUIK, известен только Клиенту и ПЭП электронного документа, корректность которой подтверждается при проверке с помощью Открытого ключа QUIK, равнозначна собственноручной подписи Клиента, а электронные документы, подписанные такой ПЭП, порождают со стороны Клиента обязательства, равные обязательствам по документам аналогичного содержания на бумажном носителе, заверенным собственноручной подписью Клиента. В случае несоответствия UID в окне ПО с уведомлением о регистрации Открытого ключа QUIK Клиент обязан немедленно прекратить работу с ПО и сообщить об этом Банку любым доступным способом.

5.4. Клиент вправе в любой момент осуществить повторную генерацию ключей ПЭП. В случае повторной генерации Клиентом ключей ПЭП последний в целях регистрации в Банке своего Открытого ключа QUIK передает Банку регистрируемый Открытый ключ QUIK в виде электронного документа и прикладывает вновь полученный у Банка уникальный код регистрации ключа.

5.5. Правила идентификации Клиента, подписывающего Поручение Простой ЭП

Клиент, использующий Простую ЭП, однозначно идентифицируется Банком при одновременном выполнении следующих условий:

– соответствие данных Клиента, указанных при оформлении Акта / при регистрации через Личный кабинет, данным Клиента, имеющимся в Банке в рамках Соглашения;

– соответствие данных Открытого ключа QUIK (pubring.txk) и UID Клиента, указанных в оформленном Клиентом Акте / указанных при регистрации через Личный кабинет, файлу с содержанием Открытого ключа QUIK (pubring.txk), переданному Клиентом для привязки к Рабочему месту Клиента на сервере Банка (проверка при регистрации в ИТС QUIK нового ключа Клиента);

– корректный ввод Логина и Пароля и последующей аутентификации в ИТС QUIK;

– соответствие Закрытого ключа QUIK (secring.txk), используемого для доступа на сервер Банка с Рабочего места Клиента, Открытому ключу QUIK (pubring.txk), размещенному на сервере Банка и соответствующему Рабочему месту Клиента (проверка при аутентификации Клиента для установления связи с Банком);

– соответствие Пароля доступа, полученного Клиентом способом, указанным Клиентом в Заявлении о присоединении, Паролю доступа, введенному при входе в ИТС QUIK.

Соединение с сервером ИТС QUIK с Рабочего места Клиента происходит только после ввода Клиентом:

– Логина и Пароля (при этом Пароль известен только Клиенту)

и

– Второго фактора аутентификации – дополнительного ввода Пароля доступа, полученного способом, указанным в Заявлении о присоединении.

Для Банка данное соединение однозначно считается установленным Клиентом.

Все Поручения в ТС или Сообщения после подключения к ИТС QUIK Клиента, использующего Простую ЭП, в случае присутствия данного Поручения в ТС или Сообщения в отчете по транзакциям, сформированном по UID, на который зарегистрирован его Открытый ключ QUIK (pubring.txk), Стороны признают поданными / направленными Клиентом.

5.6. Процедура замены Закрытого ключа QUIK

5.6.1. Замена Закрытого ключа QUIK и Пароля осуществляется Клиентом самостоятельно средствами Дистрибутивного пакета в следующих случаях:

– по инициативе Клиента;

– при Компрометации Закрытого ключа QUIK.

5.6.2. При замене Закрытого ключа QUIK по инициативе Клиента или по окончании срока действия Открытого ключа QUIK Клиент, не позднее чем за 5 (Пять) рабочих дней до планируемой даты прекращения использования Закрытого ключа QUIK, выполняет процедуры в соответствии с п. 4.5 настоящего Порядка.

5.6.3. При замене Закрытого ключа QUIK в случае Компрометации Клиент осуществляет действия в соответствии с разделом 3.5 настоящих Правил.

## **6. Особенности предоставления технического доступа к ПО WebQUIK<sup>2</sup> и Мобильной версии QUIK X**

6.1. Предоставление технического доступа к ПО WebQUIK и Мобильной версии QUIK X может быть осуществлено только после получения уведомления от Банка о готовности предоставить соответствующую услугу.

6.2. Предоставление технического доступа к ПО WebQUIK и Мобильной версии QUIK X осуществляется путем первичного создания Банком Пин-кода и передачи его Клиенту на адрес электронной почты, указанный Клиентом в Заявлении о присоединении.

6.3. Клиент получает техническую возможность использовать ПО WebQUIK и Мобильную версию QUIK X не позднее 2 (Двух) рабочих дней с момента предоставления Банком Пин-кода

<sup>2</sup> При наличии технической возможности.

(password). При этом в качестве имени пользователя (login) Клиент использует цифры из номера Соглашения.

6.4. Клиент уведомлен, что при первом входе в ПО WebQUIK и Мобильную версию QUIK X он обязан заменить Пин-код, предоставленный ему при регистрации Банком, на новый Пин-код. Настоящим Клиент признает, что все заявки, поданные с использованием Пин-кода, считаются поданными от имени Клиента, а все сделки, совершенные на основании таких заявок, совершенными по поручению Клиента.

6.5. Ответственность за своевременное осуществление смены Пин-кода, полученного у Банка, а также за обеспечение конфиденциальности нового Пин-кода возлагается на Клиента. Банк не несет ответственности за возможные негативные последствия несвоевременной смены, утраты или разглашения Пин-кода Клиентом.

6.6. Защита данных, передаваемых по сети Интернет с использованием ПО WebQUIK и Мобильной версии QUIK X, от несанкционированного доступа обеспечивается штатными средствами операционной системы и программного обеспечения для доступа в Интернет, установленных на компьютере / мобильном устройстве, используемом Клиентом для обмена Сообщениями через ПО WebQUIK и Мобильную версию QUIK X. Стороны признают, что использование этих средств обеспечивает достаточную защиту электронных документов, передаваемых по сети Интернет в ПО WebQUIK и Мобильной версии QUIK X, от несанкционированного доступа.

6.7. Стороны признают способ идентификации и аутентификации Клиента в ПО WebQUIK и Мобильной версии QUIK X на основе специального имени пользователя (login) и Пин-кода достаточным для подтверждения авторства и подлинности электронных документов, передаваемых Клиентом Банку. Стороны признают корректность Простой электронной подписи, проставленной для электронного документа, если успешно пройдена проверка соответствия установленной в процессе аутентификации сессии ПО WebQUIK и Мобильной версии QUIK X и переданного в рамках сессии электронного документа.

6.8. Стороны признают в качестве достаточного доказательства (пригодного для предъявления при разрешении споров в суде) формируемые серверной частью ПО WebQUIK записи в электронных файлах протокола сообщений между сервером Банка, на котором установлено программное обеспечение системы WebQUIK, и компьютером / мобильным устройством, использованным Клиентом для подачи Сообщений Банку через ПО WebQUIK и/или Мобильную версию QUIK X.

6.9. В случае компрометации Пин-кода Клиент обязан незамедлительно сообщить Банку о компрометации Пин-кода.

6.10. Клиент несет полную ответственность за сохранность своего Пин-кода. Банк не несет ответственности за любые убытки, понесенные Клиентом, причиной которых является использование третьими лицами Пин-кода Клиента. Клиент подтверждает, что все заявки, поданные с использованием ПО WebQUIK и/или Мобильной версии QUIK X до получения Банком письменного уведомления Клиента о компрометации Пин-кода, считаются поданными от имени Клиента, а все сделки, совершенные на основании таких заявок, – совершенными по поручению Клиента.

6.11. В случае компрометации (наличия обстоятельств, свидетельствующих о наличии возможности доступа третьих лиц к Пин-коду) / утраты Клиентом Пин-кода Банк осуществляет аннулирование Пин-кода Клиента для ПО WebQUIK и Мобильной версии QUIK X и прекращает прием Поручений Клиента на основании соответствующего заявления Клиента, составленного в письменной форме на бумажном носителе, подписанного Клиентом или его уполномоченным представителем, либо на основании заявления Клиента, сделанного по телефону (495) 601-99-34, с идентификацией Клиента согласно правилам Банка.

6.12. Особенности предоставления технического доступа к ПО Мобильной версии QUIK X

6.12.1. Порядок работы с ПО Мобильной версии QUIK X определяется наряду с настоящими Правилами также Руководством пользователя, разработанным обладателем исключительных прав на ПО, ознакомиться с которым Клиент может на сайте Разработчика, на сайте Банка.

6.12.2. Работа с ПО Мобильной версии QUIK X, в том числе порядок изготовления специальных ключей, необходимых для проведения идентификации Клиента в ПО Мобильной версии QUIK X, осуществляется в порядке и на условиях, установленных п. 4.1 настоящих Правил для ПО QUIK.



## **7. Права и обязанности Сторон**

### **7.1. Банк обязан:**

7.1.1. Приложить все разумные усилия с целью обеспечения работоспособности ИТС QUIK, своевременного и в полном объеме исполнения Поручений Клиента на совершение сделок и операций, созданных и/или переданных с использованием ИТС QUIK.

7.1.2. Каждый торговый день до начала торгов в Торговой системе вводить в ИТС QUIK информацию о плановых лимитах / свободных остатках денежных средств и/или ценных бумаг, соответствующих позиции Клиента.

7.1.3. Осуществлять действия, предусмотренные настоящими Правилами, при замене ключевой информации в срок не более 5 (Пяти) рабочих дней с момента такой замены.

7.1.4. По письменному запросу Клиента подготовить, подписать и скрепить своей печатью / штампом документы из архива электронных протоколов, осуществляемых средствами ИТС QUIK в отношении действий, предпринятых / осуществленных Клиентом за определенный период, с учетом срока хранения таких протоколов, определяемого Банком самостоятельно.

### **7.2. Банк имеет право:**

7.2.1. Не принимать к исполнению Поручения Клиента, созданные и/или переданные с использованием ИТС QUIK, если существуют причины, которые Банк считает препятствующими электронному взаимодействию Сторон, а также в случае неисполнения требований Клиентом настоящих Правил и/или Порядка.

7.2.2. Не принимать, не регистрировать и не исполнять Поручения Клиента, созданные и/или переданные с использованием ИТС QUIK, если нарушены какие-либо из требований настоящих Правил и/или Порядка либо если у Банка имеются какие-либо причины, вызывающие сомнения в авторстве и/или подлинности полученных по ИТС QUIK Поручений Клиента, а также в случае получения информации или возникновения подозрений о Компрометации ключевой информации или Пароля.

7.2.3. Временно приостановить доступ Клиента к ИТС QUIK в случае:

– обнаружения (или получения соответствующего сообщения от Клиента) ошибок / неточностей, связанных с исполнением Поручений Клиента, созданных и/или переданных с использованием ИТС QUIK, либо с предоставляемой Клиенту отчетностью по итогам таких операций, на период проверки и устранения указанных ошибок / неточностей;

– нарушения Клиентом обязательств по оплате комиссионного вознаграждения и возмещения расходов Банка, предусмотренных Порядком;

– возникновения у любой из Сторон подозрений в Компрометации ключевой информации или Пароля;

– непредоставления в Банк оригиналов Поручений Клиента, подписанных реестров Поручений в соответствии с Порядком;

– нарушения Клиентом иных обязательств, вытекающих или связанных с настоящими Правилами и/или Порядком;

– наличия каких-либо причин технического характера, препятствующих нормальной работе ИТС QUIK, включая, но не ограничиваясь:

- технические проблемы (сбои), независимо от причин их возникновения;

- профилактические / испытательные работы в отношении используемого оборудования и/или каналов связи;

- работы, связанные с внесением изменений / устранением неполадок / заменой ИТС QUIK;

- в иных случаях в соответствии с настоящими Правилами.

### **7.3. Клиент обязан:**

7.3.1. Ознакомиться с техническим описанием порядка эксплуатации ИТС QUIK в Руководстве пользователя до начала ее эксплуатации и соблюдать условия технического доступа к ИТС QUIK.

7.3.2. Использовать ИТС QUIK только по прямому назначению.

7.3.3. Незамедлительно поставить Банк в известность в случае отзыва Сертификата ключа проверки ЭП, о событиях Компрометации ключевой информации, Закрытого ключа ЭП или Закрытого ключа QUIK, а также о любых иных действиях и/или фактах, которые могут свидетельствовать о таких событиях.

7.3.4. Организовать по согласованию с Банком подключение технических средств к

телекоммуникационным каналам, обеспечивающим выбранный способ соединения с сервером Банка.

7.3.5. Своевременно и в полном объеме оплачивать услуги, оказываемые в соответствии с настоящими Правилами, в порядке, предусмотренном Порядком.

7.3.6. Обеспечить доступ к ключевой информации, Паролю, Пин-коду и Паролю доступа Клиента исключительно уполномоченным лицам Клиента.

7.3.7. Соблюдать конфиденциальность ключевой информации, Пароля, Пин-кода и Пароля доступа и обеспечить соблюдение конфиденциальности указанных сведений Уполномоченными представителями Клиента.

7.3.8. Не допускать копирования, декомпиляции и/или дизассемблирования любого программного обеспечения, используемого Сторонами при осуществлении взаимодействия по настоящим Правилам.

7.3.9. Немедленно прекратить использование ключевой информации в случае ее Компрометации.

7.3.10. Не использовать ключевую информацию при наличии оснований полагать, что конфиденциальность ключей нарушена.

7.3.11. Для оперативной блокировки Сертификатов ключей проверки ЭП незамедлительно ставить в известность Банк о Компрометации ключевой информации, Пароля доступа, Пин-кода и Пароля.

7.3.12. Соблюдать требования эксплуатационной документации на средства ЭП.

7.3.13. Содержать в исправном состоянии программно-технические средства, которые подключены к ИТС QUIK, принимать организационные меры для предотвращения несанкционированного доступа к данным компьютерам и установленному на них ПО и СКЗИ, а также в помещения, в которых они установлены.

7.3.14. Не допускать появления в компьютерной среде, где функционирует система электронного документооборота, компьютерных вирусов и вредоносных программ.

7.3.15. Немедленно сообщать Банку обо всех случаях, свидетельствующих о попытках несанкционированного доступа к компьютерам с установленными СКЗИ.

7.3.16. Каждый торговый день до начала торгов в торговой системе осуществлять сверку информации о свободных остатках / лимитах денежных средств и/или ценных бумаг, введенных Банком в ИТС QUIK, с данными собственного учета и незамедлительно ставить в известность Банк обо всех выявленных расхождениях.

В случае обнаружения Клиентом в ИТС QUIK некорректной информации о собственных текущих свободных остатках / лимитах денежных средств и/или ценных бумаг Клиент обязан незамедлительно уведомить Банк способами, предусмотренными Порядком.

7.3.17. Соблюдать разрешенные способы использования биржевой информации и нести ответственность за нарушения при использовании биржевой информации (приложение 22 к Порядку).

7.3.18. Соблюдать положения Требования к реализации мер по защите информации клиентом при работе с ИТС QUIK (приложение 7 к настоящим Правилам).

#### **7.4. Клиент имеет право:**

По собственному усмотрению приостановить / возобновить получение услуг по настоящим Правилам.

#### **7.5. Клиент не имеет права:**

7.5.1. Транслировать сведения и информацию из ИТС QUIK третьим лицам.

7.5.2. Подключаться к ИТС QUIK с использованием не принадлежащих ему ключевой информации, Пароля, Пароля доступа или Пин-кода либо методом подбора таких данных.

7.5.3. Использовать предоставленную ИТС QUIK либо любые иные средства, оборудование и/или каналы связи для проникновения в локальные сети Банка.

7.5.4. Предпринимать какие-либо действия, не предусмотренные Соглашением и/или настоящими Правилами, в том числе такие, которые могут вызвать сбои / технические проблемы в работе каких-либо компонентов ИТС QUIK и/или локальных сетей Банка.

7.5.5. Передавать третьим лицам программное обеспечение, Дистрибутивный пакет, Документацию ИТС, ключевую информацию, Пароль, Пароль доступа и Пин-код, сведения по форматам электронных документов и технологии их обработки, а также прочие сведения, относящиеся к настоящим Правилам. Исключение составляют профессиональные участники рынка ценных бумаг (профучастники), передающие данное программное обеспечение своим клиентам.

## **8. Стоимость услуг и порядок оплаты**

8.1. Плата за подключение ИТС QUIK, абонентские платежи за использование Клиентом ИТС QUIK взимаются Банком в соответствии с действующими на момент оплаты Тарифами Банка, являющимися приложением к Порядку.

8.2. Датой подключения ИТС QUIK считается дата, с которой Клиент получает возможность совершать операции с использованием ИТС QUIK.

8.3. Датой отказа от использования ИТС QUIK является дата регистрации Банком Заявления о прекращении доступа к ИТС QUIK (приложение 6 к настоящим Правилам) с указанием прекратить технический доступ к ИТС QUIK.

8.4. Возмещение Клиентом расходов, понесенных Банком при предоставлении Клиенту дополнительных сервисов и функций, запрашиваемых Банком у разработчиков ИТС QUIK в индивидуальном порядке по письменному запросу Клиента, осуществляется на основании счетов, получаемых от разработчиков ИТС QUIK или иных третьих лиц.

8.5. Плата за подключение ИТС QUIK, абонентская плата за использование ИТС QUIK, возмещение расходов Банка, понесенных в соответствии с п. 8.4 настоящих Правил, удерживается Банком с Лицевого (брокерского) счета Клиента. На основании отдельного соглашения, заключенного Клиентом с Банком, Клиент оплачивает указанные в настоящем пункте услуги самостоятельно на основании выставяемого Банком счета.

## **9. Ответственность Сторон**

9.1. Ответственность Сторон при осуществлении ими взаимодействия в рамках настоящих Правил определяется положениями заключенного ими Соглашения с учетом особенностей, установленных данным разделом настоящих Правил.

9.2. Банк не несет ответственности за ошибки и искажения в электронных документах, отправленных Клиентом, возникшие не по вине Банка.

9.3. Банк не несет ответственности за ошибки и искажения в электронных документах, отправленных Банком, возникшие не по вине Банка.

9.4. Банк не несет ответственности за убытки, понесенные Клиентом из-за несанкционированного доступа к ИТС QUIK неуполномоченных или третьих лиц, если такой доступ имел место не по вине Банка.

9.5. Банк не несет ответственности за убытки, понесенные Клиентом, в том числе в форме упущенной выгоды Клиента, в связи с задержкой или временной невозможностью передачи электронных документов посредством ИТС QUIK.

9.6. Банк не несет ответственности за несоблюдение банковской тайны в отношении содержания электронных документов, переданных посредством ИТС QUIK, кроме случаев, когда это несоблюдение стало возможным в результате виновных действий Банка.

9.7. Получение Банком от Клиента Сообщений по ИТС QUIK с использованием Ключа ЭП или ключей аутентификации, Логина и Пароля, Пароля доступа является исчерпывающим признаком, идентифицирующим Клиента и/или его уполномоченного представителя при направлении / получении Сообщений по ИТС QUIK, при этом Клиент несет полную ответственность за сохранность и неразглашение этой информации.

9.8. Клиент несет полную ответственность за все действия, совершенные с использованием его Логина, Пароля, ключевой информации, Пин-кода и/или Пароля доступа, а также принимает на себя риск возникновения негативных последствий, связанных с исполнением Банком Поручений Клиента и инструкций, полученных им от лиц, использующих Логин, Пароль, ключевую информацию, Пин-код и/или Пароль доступа Клиента.

9.9. Правообладателями имущественных авторских прав на ИТС QUIK, предоставляемую Клиенту в рамках настоящих Правил, являются ее разработчики, перечисленные в п. 14.1 настоящих Правил. ИТС QUIK является собственностью разработчиков и содержит информацию без права ее копирования.

9.10. Предоставляемая в рамках информационного обслуживания через электронные каналы связи информация является собственностью соответствующих информационных агентств. Клиент несет полную ответственность за нарушение законодательно установленного режима использования такой информации.

9.11. Стороны несут ответственность за разглашение (в том числе раскрытие, воспроизведение, распространение) любой информации, полученной ими при оказании Банком Клиенту дополнительных услуг по настоящим Правилам.

#### **9.12. Ограничения ответственности**

9.12.1. Банк не несет ответственности за неисполнение или ненадлежащее исполнение своих обязательств по Соглашению и/или настоящим Правилам, а также за какие-либо убытки, включая, но не ограничиваясь, случаи неполучения Клиентом прибыли (упущенная выгода), возникшие, в частности, в результате прерывания деятельности, потери информации, использования или невозможности использования Клиентом дополнительных услуг по настоящим Правилам, вызванных нарушением нормального функционирования ИТС QUIK по следующим причинам:

- неисправности какого-либо используемого технологического оборудования;
- сбоев, неисправностей и/или отказов в работе ИТС QUIK, каналов связи, энергоснабжения;
- ошибок, неисполнения или ненадлежащего исполнения своих обязательств со стороны провайдеров услуг связи и доступа в Интернет либо со стороны торговой системы в части предоставления доступа / обеспечения надлежащего функционирования программно-технического комплекса торговой системы;
- другим причинам технического характера, влияющим на работоспособность ИТС QUIK.

9.12.2. В отношении информации, предоставляемой в рамках информационного обслуживания через электронные каналы связи, Банк является таким же пользователем, как и Клиент, и, соответственно, не несет перед Клиентом никакой ответственности за полноту, точность, своевременность, достоверность и другие существенные характеристики такой информации, а также за возможные убытки Клиента, вызванные использованием такой информации.

9.12.3. Банк не несет ответственности за нарушение Клиентом авторских и имущественных прав разработчиков ИТС QUIK и СКЗИ. В случае неавторизованного или незаконного использования Клиентом переданной ему ИТС QUIK Клиент возмещает разработчикам и Банку все убытки, в том числе упущенную выгоду, явившиеся частично или полностью результатом действия или бездействия Клиента.

### **10. Обстоятельства форс-мажора**

10.1. В случае возникновения обстоятельств непреодолимой силы, к которым относятся: стихийные бедствия, аварии, пожары, массовые беспорядки, забастовки, революции, военные действия, вступающие в силу законодательные акты, правительственные постановления и распоряжения государственных органов, судебные решения, и иных обстоятельств, не зависящих от волеизъявления Сторон, Стороны освобождаются от ответственности за неисполнение или ненадлежащее исполнение взятых на себя обязательств по Договору, если в течение 48 часов с момента наступления таких обстоятельств Сторона, пострадавшая от их влияния, доведет до сведения другой Стороны известие о случившемся.

10.2. Действие Договора приостанавливается на время действия обстоятельств форс-мажора и возобновляется сразу после прекращения их действия.

## 11. Порядок рассмотрения претензий и разрешения споров

11.1. Споры и разногласия, возникающие в связи с настоящими Правилами, решаются Сторонами путем переговоров, результаты которых оформляются протоколом согласования разногласий или протоколом разногласий. Урегулирование споров и разногласий в этом случае осуществляется в порядке, установленном Порядком.

11.2. В случае возникновения у любой из Сторон сомнений в полноте и/или целостности (отсутствие, искажение, присутствие ошибочной) информации, зафиксированной ИТС QUIK, Стороны могут привлечь в качестве независимого эксперта разработчика (ов) ИТС QUIK. При этом оплата услуг независимого эксперта, если необходимо, осуществляется за счет Стороны, выступившей инициатором приглашения эксперта, либо иным образом – при наличии согласия Сторон.

11.3. Стороны обязуются признавать подлинным полученный / отправленный (соответственно) электронный документ, имеющий ЭП, созданную с использованием Закрытого ключа передающей Стороны, при условии, что подлинность ЭП подтверждена в результате ее проверки, проведенной получающей Стороной с использованием соответствующего Открытого ключа передающей Стороны.

11.4. В случае получения принимающей Стороной электронного документа с успешно подделанной ЭП ответственность за последствия выполнения такого документа возлагается на передающую Сторону как не обеспечившую сохранность своей ключевой информации.

11.5. При возникновении у Клиента претензий к Банку в связи с выполнением последним операций с Ценными бумагами / Инструментами ТС СЭЛТ Клиента или Срочных сделок, которые не были поручены, Клиент должен направить в Банк письменную претензию с указанием реквизитов операции, исполнение которой он считает неправомерным.

Для разрешения спора Клиент должен направить в Банк полномочных представителей и представить действовавшие в этот период ключевую информацию, Сертификат проверки ключа ЭП (в случае наличия) и Открытый ключ QUIK, а также все имеющиеся у Клиента документы с информацией о данной операции, включая данные из архива ИТС QUIK.

Если документ, на основании которого выполнена рассматриваемая спорная операция, в архиве ИТС QUIK не найден, то претензии к рассмотрению не принимаются.

Если документ, на основании которого выполнена рассматриваемая спорная операция, в архиве ИТС QUIK найден:

- претензии Клиента принимаются к рассмотрению при условии, что подлинность ЭП Клиента не подтверждена в результате ее проверки, проведенной Банком в установленном порядке;
- претензии Клиента отклоняются в случае подтверждения подлинности ЭП Клиента в результате ее проверки, проведенной Банком в установленном порядке.

11.6. При возникновении у Клиента претензий к Банку в связи с неисполнением последним порученной операции Клиент должен направить в Банк письменную претензию (с указанием неисполненной операции), заверенную копию неисполненного электронного документа на бумажном носителе, дискету с файлом из архива ИТС QUIK, содержащим этот электронный документ.

Если данный электронный документ в архиве ИТС QUIK не найден, то претензии к рассмотрению не принимаются.

Если данный электронный документ в архиве ИТС QUIK найден, в установленном порядке проверяются наличие и подлинность ЭП Банка в подтверждении о получении электронного документа. В случае если в результате проверки установлено отсутствие ЭП Банка или не подтверждена подлинность ЭП Банка, претензии Клиента отклоняются.

11.7. Если при проведении проверок подлинности ЭП Клиента и ЭП Банка в случаях, предусмотренных пп. 11.5 и 11.6 настоящих Правил, обнаружено несоответствие электронного документа установленной форме либо выявлены ошибки в электронном документе, уполномоченными представителями Банка и Клиентом / Уполномоченными представителями Клиента составляется акт произвольной формы с целью определения виновной Стороны и принятия необходимых мер по урегулированию конфликтной ситуации.

11.8. Претензия рассматривается в течение 10 рабочих дней с даты получения ее другой Стороной.

11.9. В случае если Стороны не придут к взаимному согласию, предмет спора должен быть передан на рассмотрение в Арбитражный суд г. Москвы, если Клиент является юридическим лицом,

а в случае если Клиент является физическим лицом – в судебные инстанции по месту нахождения Банка для разрешения в соответствии с законодательством Российской Федерации.

## **12. Внесение изменений в настоящие Правила**

12.1. Банк имеет право вносить изменения и дополнения в настоящие Правила и приложения к ним в одностороннем порядке, в том числе путем введения в действие новой редакции настоящих Правил. Раскрытие информации о внесении изменений и дополнений осуществляется Банком не позднее чем за 10 (Десять) рабочих дней до вступления в силу указанных изменений и дополнений.

12.2. Изменения и дополнения, вносимые в настоящие Правила и приложения к ним в связи с изменением законодательства Российской Федерации, в том числе нормативных актов Банка России, а также Правил ТС, вступают в силу одновременно с вступлением в силу соответствующих нормативно-правовых актов, правил и других документов указанных органов и организаций.

12.3. Раскрытие информации о внесении изменений и дополнений в настоящие Правила осуществляется путем размещения соответствующей информации на сайте Банка в сети Интернет ([www.mkb.ru](http://www.mkb.ru)).

12.4. Клиент обязан не реже одного раза в 7 (Семь) календарных дней знакомиться с информацией, публикуемой Банком в порядке, установленном настоящими Правилами.

12.5. Банк не несет ответственности в случае неполучения Клиентом информации о внесении изменений в настоящие Правила, если указанная информация была опубликована в порядке и в сроки, установленные настоящими Правилами.

12.6. Любые изменения настоящих Правил с момента их вступления в силу равно распространяются на всех лиц, присоединившихся к настоящим Правилам, в том числе присоединившихся к настоящим Правилам до даты вступления изменений в силу.

12.7. В случае несогласия Клиента с вносимыми Банком в одностороннем порядке изменениями Клиент имеет право отказаться от получения дополнительных услуг по настоящим Правилам путем направления Банку Заявления о прекращении доступа к ИТС QUIK (приложение 6 к настоящим Правилам) не позднее чем за 1 (Один) рабочий день до даты отказа от настоящих Правил.

## **13. Порядок расторжения Договора**

13.1. Договор может быть расторгнут в любое время по инициативе любой из Сторон путем направления второй Стороне уведомления об отказе от исполнения условий Договора. Указанное уведомление направляется Клиентом в письменном виде на бумажном носителе по форме приложения 6 к настоящим Правилам. Уведомление Банка направляется Клиенту в письменном виде заказным письмом по почтовому адресу, указанному в анкете Клиента, а в случае отсутствия такового – по адресу регистрации (места нахождения) либо может быть вручено Клиенту лично под роспись при его визите в Банк либо при доставке уведомления курьером (курьерской службой).

13.2. При направлении Клиентом уведомления согласно п. 13.1 настоящих Правил действие Договора прекращается с момента получения Банком уведомления при отсутствии у Клиента невыполненных обязательств по Договору.

При вручении (направлении) уведомления Банком действие Договора прекращается со дня вручения Клиенту уведомления либо по истечении 10 (Десяти) рабочих дней со дня отправки уведомления в порядке, определенном в п. 13.1 настоящих Правил, при отсутствии у Клиента невыполненных обязательств по Договору. При наличии у Клиента невыполненных обязательств действие Договора считается прекращенным с момента их полного исполнения.

13.3. Прекращение действия Договора не влечет прекращения действия других договоров и соглашений между Банком и Клиентом.

13.4. При прекращении действия Договора Клиент обязан в течение 3 (Трех) рабочих дней с даты прекращения действия Договора удалить все компоненты ИТС QUIK, полученные им от Банка, и вернуть последнему соответствующий Дистрибутивный пакет (если таковой передавался Клиенту Банком на цифровом носителе).

## **14. Технические характеристики**

14.1. Разработчики ИТС QUIK:

14.1.1. Разработчиком ИТС QUIK, используемого Сторонами при осуществлении взаимодействия в рамках Порядка и Соглашения, является ООО «АРКА Текнолоджиз».

14.1.2. В соответствии с условиями заключенного Банком с разработчиком соглашения разработчик обязуется в течение всего срока действия такого соглашения осуществлять абонентское обслуживание ИТС QUIK, включающее консультации по эксплуатации и администрированию, содействие при восстановлении работоспособности после сбоев, устранение обнаруженных в процессе эксплуатации дефектов, передачу обновлений эксплуатируемой версии ИТС QUIK.

14.2. По всем вопросам технической поддержки ПО QUIK Клиент имеет право обратиться в Банк по телефону +7 (495) 601-99-34 по рабочим дням с 09:30 до 19:00.

14.3. Банк обязуется оказывать Клиенту необходимое содействие в процессе взаимодействия Клиента с разработчиком, а при наличии возможности и/или технических ресурсов – самостоятельно принимать меры и прилагать усилия для устранения причин или разрешения вопросов, послуживших причиной обращения Клиента к разработчику.

14.4. Руководство пользователя ИТС QUIK Клиент получает в составе дистрибутива ИТС QUIK.

14.5. Технические требования к оборудованию и каналам связи

Для инсталляции программного обеспечения ИТС QUIK на компьютерном оборудовании Клиента должны быть выполнены технические требования ИТС QUIK, опубликованные на Сайте разработчика <https://arqatech.com/ru/>.

Приложение 1  
к Правилам обслуживания клиентов  
ПАО «МОСКОВСКИЙ КРЕДИТНЫЙ  
БАНК» с использованием ИТС QUIK

**АКТ № \_\_\_\_\_ приема-передачи ключей аутентификации**

г. Москва

« \_\_\_\_ » \_\_\_\_\_ 20\_\_ г.

ПАО «МОСКОВСКИЙ КРЕДИТНЫЙ БАНК», именуемое в дальнейшем «Банк», в лице \_\_\_\_\_, действующее на основании \_\_\_\_\_, с одной стороны, и \_\_\_\_\_, именуемое в дальнейшем «Клиент», в лице \_\_\_\_\_, действующее на основании \_\_\_\_\_, с другой стороны, далее вместе именуемые «Стороны», заключили настоящий Акт о том, что в соответствии с Правилами обслуживания клиентов ПАО «МОСКОВСКИЙ КРЕДИТНЫЙ БАНК» с использованием ИТС QUIK, а также в рамках заключенного между Банком и Клиентом Соглашения о предоставлении услуг на финансовых рынках № \_\_\_\_\_ от \_\_. \_\_. \_\_\_\_ (далее – Соглашение) Клиент передал, а Банк принял Открытый ключ QUIK (pubring.txk), предназначенный для аутентификации пользователя системы ИТС QUIK (Уникальный номер Клиента в ИТС QUIK – UID...).

Содержание Открытого ключа QUIK (pubring.txk):

«Пользователь: \_\_\_\_\_ (указывается Логин, присвоенный Клиентом)

USERID=  
KEYID=  
TIME=  
SECRET=  
BITS=  
KEY= »

Настоящий Акт составлен в двух экземплярах и является неотъемлемой частью Соглашения.

**От имени Банка:**

**От имени Клиента:**

\_\_\_\_\_  
(подпись)      (расшифровка подписи)

\_\_\_\_\_  
(подпись)      (расшифровка подписи)

МП

МП



**Заявление на аннулирование ключей аутентификации**

г. Москва

« \_\_\_\_ » \_\_\_\_\_ 20\_\_ г.

Уникальный идентификационный номер \_\_\_\_\_

Клиент: \_\_\_\_\_

(наименование /ФИО)

Соглашение № \_\_\_\_\_ от « \_\_\_\_ » \_\_\_\_\_ 20\_\_ г.

**Лицевой счет**

|   |   |   |   |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|---|---|---|---|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|
| 3 | 0 | 6 | 0 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|---|---|---|---|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|

В соответствии с разделом 3.5 Правил обслуживания клиентов ПАО «МОСКОВСКИЙ КРЕДИТНЫЙ БАНК» с использованием ИТС QUIK сообщает о \_\_\_\_\_ (указать причину отзыва ключей авторизации: компрометация Открытого ключа QUIK (pubring.tsk) и т. д.). В связи с чем **прошу ПАО «МОСКОВСКИЙ КРЕДИТНЫЙ БАНК» аннулировать (отозвать)** Открытый ключ QUIK и Сертификат проверки ключа ЭП, оформленные в соответствии с Актом приема-передачи ключей аутентификации.

Дата « \_\_\_\_ » \_\_\_\_\_ 20\_\_ г.

**Клиент:**

**Уполномоченный сотрудник Банка:**

\_\_\_\_\_  
(подпись) (расшифровка подписи)

\_\_\_\_\_  
(подпись) (расшифровка подписи)

« \_\_\_\_ » \_\_\_\_\_ 20\_\_ г.

« \_\_\_\_ » \_\_\_\_\_ 20\_\_ г.

МП

МП

**АКТ № \_\_\_\_\_ признания ключа проверки электронной подписи юридического лица  
или индивидуального предпринимателя**

г. Москва

« \_\_\_\_\_ » \_\_\_\_\_ 20\_\_ г.

ПАО «МОСКОВСКИЙ КРЕДИТНЫЙ БАНК», именуемое в дальнейшем «Банк», в лице \_\_\_\_\_, действующее на основании \_\_\_\_\_, с одной стороны, и \_\_\_\_\_, именуемое в дальнейшем «Клиент», в лице \_\_\_\_\_, действующее на основании \_\_\_\_\_, с другой стороны, далее вместе именуемые «Стороны», составили настоящий Акт о следующем:

**1. Клиент передал Банку следующий квалифицированный Сертификат ключа проверки электронной подписи (ЭП):**

Серийный номер сертификата: XX:XX:XX:XX:XX:XX:XX:XX:XX  
Издатель сертификата: Квалифицированный Удостоверяющий центр  
Сертификат действителен с: Mar 30 07:44:21 2018GMT  
Сертификат действителен до: May 23 07:43:19 2019 GMT  
Ключ проверки ЭП: 04:f3:df:26:e8:22:69:05:cd:95:f0:99:87:3f:cc:  
20:be:f6:26:88:fa:67:4b:65:34:8f:af:b7:c4:83:  
55:aa:b2:82:c5:54:55:54:2c:aa:b3:cc:4d:97:16:  
57:44:3e:a7:cb:40:a5:cb:60:b8:39:d5:3f:bc:ef:  
f0:32:60:c5:a8

Владелец ключа ЭП: \_\_\_\_\_

(Фамилия, Имя, Отчество)

Документ,  
удостоверяющий  
личность (паспорт): \_\_\_\_\_

(номер документа, кем, когда выдан)

Подпись владельца ключа ЭП:

для регистрации и использования в соответствии с Правилами обслуживания клиентов ПАО «МОСКОВСКИЙ КРЕДИТНЫЙ БАНК» с использованием ИТС QUIK.

2. Владелец сертификата ключа проверки ЭП подтверждает принадлежность ему ЭП, которые будут формироваться с использованием ключа ЭП, соответствующего приведенному выше ключу проверки ЭП.

3. Владелец сертификата ключа проверки ЭП соглашается с обработкой своих персональных данных Банком и признает, что персональные данные, заносимые в сертификаты ключей подписей, владельцем которых он является, относятся к общедоступным персональным данным.

4. Стороны признают ЭП в качестве аналога собственноручной подписи Владельца соответствующего ключа ЭП с момента подписания Акта уполномоченными представителями Сторон и регистрации переданного сертификата ключа проверки ЭП.

**От имени Банка:**

**От имени Клиента:**

\_\_\_\_\_  
\_\_\_\_\_  
(подпись)

(расшифровка подписи)

\_\_\_\_\_  
\_\_\_\_\_  
(подпись) (расшифровка подписи)

МП

МП

**АКТ**  
**признания ключа проверки электронной подписи физического лица**

г. Москва

«\_\_\_» \_\_\_\_\_ 20\_\_ г.

ПАО «МОСКОВСКИЙ КРЕДИТНЫЙ БАНК», именуемое в дальнейшем «Банк», в лице \_\_\_\_\_, действующее на основании \_\_\_\_\_, с одной стороны, и \_\_\_\_\_, именуемое в дальнейшем «Клиент», с другой стороны, далее вместе именуемые «Стороны», составили настоящий Акт о следующем:

1. Клиент передал Банку следующий квалифицированный сертификат ключа проверки электронной подписи (ЭП):

|                             |  |
|-----------------------------|--|
| Серийный номер сертификата: | XX:XX:XX:XX:XX:XX:XX:XX:XX   |
| Издатель сертификата:       | Квалифицированный Удостоверяющий центр   |
| Сертификат действителен с:  | Mar 30 07:44:21 2018GMT  |
| Сертификат действителен до: | May 23 07:43:19 2019 GMT   |
| Ключ проверки ЭП:           | 04:f3:df:26:e8:22:69:05:cd:95:f0:99:87:3f:cc:<br>20:be:f6:26:88:fa:67:4b:65:34:8f:af:b7:c4:83:<br>55:aa:b2:82:c5:54:55:54:2c:aa:b3:cc:4d:97:16:<br>57:44:3e:a7:cb:40:a5:cb:60:b8:39:d5:3f:bc:ef:<br>f0:32:60:c5:a8 |

Владелец ключа ЭП:

.....  
(Фамилия, Имя, Отчество)

Документ,  
удостоверяющий  
личность (паспорт):

.....  
(номер документа, кем, когда выдан)

для регистрации и использования в соответствии с Правилами обслуживания клиентов ПАО «МОСКОВСКИЙ КРЕДИТНЫЙ БАНК» с использованием ИТС QUIK.

2. Владелец сертификата ключа проверки ЭП подтверждает принадлежность ему ЭП, которые будут формироваться с использованием ключа ЭП, соответствующего приведенному выше ключу проверки ЭП.

3. Владелец сертификата ключа проверки ЭП соглашается с обработкой своих персональных данных Банком и признает, что персональные данные, заносимые в сертификаты ключей подписей, владельцем которых он является, относятся к общедоступным персональным данным.

4. Стороны признают ЭП в качестве аналога собственноручной подписи Владельца соответствующего ключа ЭП с момента подписания Акта уполномоченными представителями Сторон и регистрации переданного сертификата ключа проверки ЭП.

**От имени Банка:**

**Владелец Сертификата ключа проверки ЭП:**

\_\_\_\_\_  
(подпись) (расшифровка подписи)

\_\_\_\_\_  
(подпись) (расшифровка подписи)

МП

МП

**Заявление  
на блокировку Сертификата ключа проверки электронной подписи**

г. Москва

«\_\_\_» \_\_\_\_\_ 20\_\_ г.

Уникальный идентификационный номер \_\_\_\_\_

Клиент: \_\_\_\_\_

(наименование / ФИО)

Соглашение № \_\_\_\_\_ от «\_\_\_» \_\_\_\_\_ 20\_\_ г.

**Лицевой счет**

|   |   |   |   |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|---|---|---|---|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|
| 3 | 0 | 6 | 0 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|---|---|---|---|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|

В соответствии с разделом 3.5 Правил обслуживания клиентов ПАО «МОСКОВСКИЙ КРЕДИТНЫЙ БАНК» с использованием ИТС QUIK извещает ПАО «МОСКОВСКИЙ КРЕДИТНЫЙ БАНК» о \_\_\_\_\_ (указать причину блокировки сертификата: компрометация Закрытого ключа ЭП, отзыв доверенности уполномоченного представителя и т. д.). В связи с чем **прошу** ПАО «МОСКОВСКИЙ КРЕДИТНЫЙ БАНК» **заблокировать Сертификат ключа проверки электронной подписи**, оформленный на

\_\_\_\_\_  
(ФИО физического лица – владельца ключа ЭП)

серийный номер блокируемого сертификата: \_\_\_\_\_;  
издатель блокируемого сертификата: \_\_\_\_\_.

Дата «\_\_\_» \_\_\_\_\_ 20\_\_ г.

**Владелец Сертификата ключа проверки ЭП: Уполномоченный сотрудник Банка:**

\_\_\_\_\_  
(подпись)

\_\_\_\_\_  
(расшифровка подписи)

\_\_\_\_\_  
(подпись)

\_\_\_\_\_  
(расшифровка подписи)

«\_\_\_» \_\_\_\_\_ 20\_\_ г.

«\_\_\_» \_\_\_\_\_ 20\_\_ г.

МП

МП

**ЗАЯВЛЕНИЕ**  
**о прекращении доступа к информационно-торговой системе QUIK**

Уникальный идентификационный номер \_\_\_\_\_

Клиент: \_\_\_\_\_  
(наименование / ФИО)

Соглашение № \_\_\_\_\_ от « \_\_\_\_\_ » \_\_\_\_\_ 20\_\_ г.

**Лицевой счет**

|   |   |   |   |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|---|---|---|---|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|
| 3 | 0 | 6 | 0 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|---|---|---|---|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|

Прошу **прекратить** доступ к информационно-торговой системе QUIK с « \_\_\_\_\_ » \_\_\_\_\_ 20\_\_ г.

Клиент: \_\_\_\_\_ / \_\_\_\_\_ /  
(подпись клиента / уполномоченного лица клиента) (расшифровка подписи)  
МП

**Для служебных отметок:**

**Принято к исполнению**

вход. № \_\_\_\_\_ от « \_\_\_\_\_ » \_\_\_\_\_ 20\_\_ г. Время \_\_\_\_\_ час. \_\_\_\_\_ мин.

Дата прекращения доступа « \_\_\_\_\_ » \_\_\_\_\_ 20\_\_ г.

ФИО уполномоченного сотрудника, подпись \_\_\_\_\_ / \_\_\_\_\_ /

### **Требования к реализации мер по защите информации Клиентом при работе с ИТС QUIK**

1. Требования технической защиты устройства доступа Клиента к ИТС QUIK, реализуемые Клиентом

Перед подключением к ИТС QUIK Клиент должен обеспечить работу устройства в следующем режиме:

– на устройстве, с которого планируется осуществлять подключение к ИТС QUIK, должны быть установлены лицензионные, регулярно обновляемые (устанавливаются обновления безопасности) операционная система, антивирусное программное обеспечение и web-браузер;

– на устройстве, с которого планируется осуществлять подключение к ИТС QUIK, должен быть настроен и использоваться локальный межсетевой экран, настроенный на работу только с необходимыми сетевыми ресурсами по поддерживаемым ими протоколам;

– устройство должно использовать процедуру аутентификации доступа к устройству, прежде чем предоставить ресурсы пользователю (требуется ввод Логина и Пароля).

2. Организационные меры по защите информации, реализуемые Клиентом:

– Клиент никогда и никому не сообщает Пароль и Ключи для электронной подписи (при их использовании);

– при использовании одноразовых Паролей Клиент использует установленное не на устройстве для доступа к ИТС QUIK приложение Google Authenticator либо получает доступ к почте с отличного от используемого для доступа к ИТС QUIK устройства;

– Клиент, используя устройство, с которого получает доступ в ИТС QUIK, осуществляет избирательную навигацию в сети Интернет и старается не посещать неизвестные ему сайты;

– Клиент при возникновении подозрений на компрометацию используемых им ключей, Паролей, Пароля для доступа к электронной почте или устройства с установленным Google Authenticator немедленно обращается в Банк для инициации процедуры, предусмотренной при компрометации ключей.

### **Требования к реализации мер по защите информации Клиентом при работе с Мобильной версией QUIK X**

1. Требования технической защиты мобильного устройства, реализуемые Клиентом

Перед подключением к Мобильной версии QUIK X Клиент должен обеспечить работу мобильного устройства в следующем режиме:

– на мобильном устройстве, с которого планируется осуществлять подключение к ИТС QUIK, должны быть установлены лицензионные, регулярно обновляемые (устанавливаются обновления безопасности) операционная система, антивирусное программное обеспечение (если операционная система подвержена вирусным атакам);

– мобильное устройство не должно быть подвергнуто операциям повышения привилегий / взлома операционной системы устройства (jail-break rooting);

– Клиент должен использовать процедуру аутентификации доступа мобильному устройству (ввод Пароля для разблокировки мобильного устройства), прежде чем приступить к работе с Мобильной версией QUIK X.

2. Организационные меры по защите информации, реализуемые Клиентом:

– установленный Пароль для входа в Мобильную версию QUIK X должен быть сложен для угадывания (отличаться от последовательности одинаковых символов, даты или года рождения Клиента и т. д.);

– Клиент никогда и никому не сообщает Пароль для входа в Мобильную версию QUIK X или получения доступа к мобильному устройству;

– Клиент, используя мобильное устройство, с которого получает доступ к Мобильной версии QUIK X, осуществляет избирательную навигацию в сети Интернет и старается не посещать неизвестные ему сайты, не устанавливать сомнительные приложения;

– Клиент обязуется не подключать мобильное устройство к компьютерам, безопасность которых (обеспечение доверенных сред, лишенных удаленного управления и установленных / запущенных вредоносных программ) он не может гарантировать;

– Клиент обязуется не модифицировать или изменять Мобильную версию QUIK X, устанавливать приложение только из официальных хранилищ AppStore и Google Play;

– Клиент понимает и подтверждает, что в Банк могут отправляться сведения о его геолокации.

Клиент обеспечивает режим доступа к его электронной почте, используемой для активации доступа к Мобильной версии QUIK X, исключающий доступ к письмам третьих лиц.