Утверждено
Протоколом Правления
№ 24 от 09.09.2016 г.
(вступают в действие
с 12.09.2016 г.)

Правила обслуживания клиентов в системе дистанционного банковского обслуживания «Интернет Клиент-Банк»

1. ТЕРМИНЫ И СОКРАЩЕНИЯ

В Правилах обслуживания клиентов в системе дистанционного банковского обслуживания «Интернет Клиент-Банк» (далее - Правила) используются следующие термины и сокращения:

1.1. **Архив электронных документов** – набор электронных записей, содержащий ЭД. Архивы электронных документов ведутся Банком.

1.2. **Аутентификация Уполномоченного лица Клиента** – удостоверение правомочности обращения Уполномоченных лиц Клиента в Систему. Аутентификация осуществляется по Паролю Системы.

1.3. **Банк** – Банк "Кузнецкий мост" Акционерное Общество.

1.4. **Банковская карточка Клиента** – карточка с образцами подписей и оттиска печати (бланк формы № 0401026 по Общероссийскому классификатору управленческой документации ОК 011-93), оформленная в соответствии с требованиями Банка России.

1.5. Договор о присоединении к Правилам обслуживания клиентов в системе дистанционного банковского обслуживания «Интернет Клиент-Банк» **(Договор)** – договор между Клиентом и Банком, заключенный путем присоединения Клиента к условиям настоящих Правил;

1.6. **Клиент** – юридическое лицо или индивидуальный предприниматель, физическое лицо, занимающееся частной практикой в установленном законодательством Российской Федерации порядке, заключившее с Банком Договор;

1.7. **Ключ электронной подписи (Ключ ЭП)** – уникальная последовательность символов, известная только Уполномоченному лицу Клиента / Банка и предназначенная для создания электронной подписи в ЭД, передаваемых по Системе, с использованием СКЗИ.

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

1.9. **Компрометация ключа ЭП** – нарушение конфиденциальности ключа ЭП, констатация Уполномоченным лицом Клиента обстоятельств, или наступление обстоятельств, при которых возможно несанкционированное использование ключа ЭП неуполномоченными лицами;

1.10. **Логин** – уникальный идентификатор Клиента в Системе.

1.11. **Операционное время –** период приема документов, установленный в соответствии с условиями Договора банковского счета, а также иных договоров, заключенных между Банком и Клиентом.

1.12. **Подтверждение подлинности электронной подписи в ЭД** – положительный результат проверки принадлежности электронной подписи в ЭД Уполномоченному лицу Клиента и отсутствия искажений в подписанном данной электронной подписью ЭД, проводимой с использованием Ключа проверки электронной подписи Уполномоченного лица Клиента.

Электронная подпись в ЭД признается Сторонами подлинной при выполнении по совокупности следующих условий:

- подтверждена принадлежность электронной подписи Уполномоченному лицу Клиента;
- Ключ проверки электронной подписи Уполномоченного лица Клиента, соответствующий Ключу электронной подписи, используемому для создания электронной подписи в ЭД, зарегистрирован в Системе и являлся действующим (не утратил силу) на момент формирования электронной подписи в ЭД;
- проверка электронной подписи Уполномоченного лица Клиента в ЭД при помощи СКЗИ с использованием Ключа проверки электронной подписи Уполномоченного лица Клиента дала положительный результат.

1.13. **Пароль** – уникальная последовательность символов, известная только Уполномоченному лицу Клиента, соответствующая присвоенному ему Логину и использующаяся для Аутентификации Уполномоченного лица Клиента. Пароль регистрируется Банком в момент выдачи Уполномоченному лицу Клиента СД и в момент изменения пароля по инициативе Уполномоченного лица Клиента.

1.14. **Система дистанционного банковского обслуживания «Интернет Клиент-Банк» (далее – Система)** – часть корпоративной информационной системы Банка, являющаяся электронным средством платежа, предназначенная для удаленного обслуживания Клиента с использованием сети Интернет,

обеспечивающая подготовку, передачу, прием, обработку ЭД, предоставление информации о движении средств по счету(ам), а также ввод в действие Ключа электронной подписи, хранящегося на средстве защищённого хранения данных eToken, и Ключа проверки электронной подписи Уполномоченного лица Клиента для формирования (на его основе) с использованием СКЗИ электронной подписи в ЭД, передаваемых в Банк / из Банка.

1.15. **СКЗИ** – программное, аппаратное и программно-аппаратное средство, являющееся неотъемлемой частью Системы, позволяющее в необходимом объеме обеспечить целостность и защиту ЭД от несанкционированного доступа с помощью выполнения преобразований исходных данных с использованием Ключей электронной подписи и Ключей проверки электронной подписи.

1.16. **Статус документа** – информация о текущем состоянии ЭД в Системе.

1.17. **Средства доступа (далее – СД)** – набор средств, позволяющих Банку Идентифицировать и Аутентифицировать Уполномоченных Лиц Клиента и проводить проверку подлинности и целостности ЭД Клиента в Системе:

- Логин и Пароль Системы для Идентификации и Аутентификации Уполномоченных лиц Клиента, доступа Уполномоченных лиц Клиента к Системе, а также обеспечения возможности подготовки, передачи, приема, и обработки ЭД в Системе;
- Ключи электронной подписи и Ключи проверки электронной подписи Уполномоченных лиц Клиента, созданные ими в порядке, установленном в п. 6 настоящих Правил (предназначены для формирования электронной подписи, Идентификации и Аутентификации Уполномоченных лиц Клиента в Системе и для подтверждения подлинности и целостности ЭД Клиента в Системе).

1.18. **Стороны –** Банк и Клиент при совместном упоминании;

1.19. **Счет** – банковский счет, открытый Клиенту в соответствии с договором банковского счета, заключенным между Клиентом и Банком.

1.20. **Тарифы** – тарифы Банка «Кузнецкий мост» АО для юридических лиц и индивидуальных предпринимателей.

1.21. **Уполномоченное лицо Клиента** – физическое лицо, представитель Клиента, включенный в Банковскую карточку Клиента, уполномоченный Клиентом подписывать ЭД и выполнять иные действия в Системе.

1.22. **Электронная подпись (далее ЭП)** – информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию. В Системе используется усиленная неквалифицированная электронная подпись.

1.23. **Электронный документ (далее ЭД)** – документ, в котором информация представлена в электронно-цифровой форме, подписанный электронной подписью, равнозначный документу, на бумажном носителе, подписанному собственноручной подписью и заверенному печатью. Перечень электронных документов, подлежащих обработке в Системе, приведен в Приложении № 1 к настоящему Договору.

1.24. **Электронный журнал** – взаимосвязанный набор электронных записей, отражающий действия Уполномоченных лиц Клиента в Системе. Хранится в Банке.

1.25. **Средство защищённого хранения данных eToken** – используемый в Системе персональный электронный носитель информации с USB интерфейсом, который является аппаратным средством защиты информации, и предназначен для хранения цифровых криптографических данных Клиента в защищенной памяти носителя информации. Используются в обязательном порядке Уполномоченными лицами Клиента. Средства защищённого хранения данных eToken передаются Клиенту на возмездной основе, в соответствии с тарифами Банка. Клиент вправе использовать средства защищённого хранения данных eToken, приобретенные им самостоятельно.

1.26. **PIN код** – пароль доступа к содержимому и функциям средства защищённого хранения данных eToken.

2. ОБЩИЕ ПОЛОЖЕНИЯ

2.1. Настоящие Правила являются неотъемлемой частью Договора и могут быть приняты Клиентом не иначе как путем присоединения к Правилам в целом, при заключении Договора.

2.2. Перечень ЭД, подлежащих обработке в Системе (далее – Перечень ЭД), и требования по оформлению ЭД установлены в Приложении №1 к настоящим Правилам.

2.3. Стороны признают используемые ими в рамках настоящих Правил системы телекоммуникаций, обработки и хранения информации достаточными для обеспечения надежной и эффективной работы при приеме, передаче, обработке и хранении информации, а систему защиты информации и порядок создания и проверки электронной подписи, обеспечивающие разграничение доступа, формирование и проверку

подлинности электронной подписи достаточной для защиты от несанкционированного доступа, подтверждения авторства и подлинности информации, содержащейся в получаемых ЭД, и разбора конфликтных ситуаций.

2.4. Стороны признают юридическую эквивалентность документов, подписанных ЭП и переданных при помощи Системы, документам на бумажном носителе, подписанным Клиентом.

2.5. Обслуживание Клиента в Системе производится через сеть Интернет. Требования к средствам, необходимым для работы с Системой, установлены в Приложении № 2 к настоящим Правилам.

2.6. Подключение и порядок работы Клиента в сети Интернет не является предметом настоящих Правил.

3. ПОРЯДОК И УСЛОВИЯ РАБОТЫ С СИСТЕМОЙ

3.1. Подключение Клиента к Системе производится после заключения Сторонами договора банковского счета, Договора о присоединении к Правилам обслуживания клиентов в системе дистанционного банковского обслуживания «Интернет Клиент-Банк» и передачи Банком Уполномоченным лицам Клиента Логина и Пароля на доступ к Системе..

3.2. Логин и Пароль на доступ к Системе передаются Уполномоченному лицу Клиента либо его представителю, действующему на основании доверенности, составленной по форме Приложения №3.

3.3. Ключи электронной подписи и Ключи проверки электронной подписи создаются Уполномоченным лицом Клиента. Ключи электронной подписи создаются и хранятся на защищенном носителе eToken.

3.4. Ключи проверки электронной подписи вводятся в эксплуатацию Банком после оформления Акта признания открытого ключа / сертификата для обмена сообщениями по форме Приложения 7.

3.5. Передача ЭД в Системе осуществляется посредством сети Интернет. Адрес сайта для работы в Системе: https://ib.kmbank.ru.

3.6. Защита информации от несанкционированного доступа при ее передаче по каналам связи осуществляется при помощи защищенного протокола SSL. При подключении к Системе Клиент обязан проверить сертификат сайта (https://ib.kmbank.ru) и убедиться в его корректности.

3.7. Клиент оформляет и передает в Банк ЭД с использованием Системы.

3.8. Полученный Банком ЭД Клиента, заверенный электронной подписью, принимается Банком к исполнению, если вышеуказанный ЭД оформлен в соответствии с требованиями, изложенными в Приложении № 1 к настоящим Правилам, и результат проверки Банком подлинности ЭП в ЭД положительный.

3.9. Моментом формирования Уполномоченным лицом Клиента электронной подписи в ЭД считается время, внесенное в Электронный журнал Системы.

3.10. Стороны признают в качестве единой шкалы московское время и обязуются поддерживать системное время своих аппаратных средств, используемых для работы с Системой, с точностью до 5 минут. Определяющим временем является текущее время по системным часам аппаратных средств Банка.

3.11. В случае отрицательного результата проверки Банком подлинности ЭП ЭД или несоответствия ЭД хотя бы одному из требований, указанных в п. 3 Приложения № 1 к настоящим Правилам, а также в случае непредставления Клиентом в Банк документов и информации об осуществляемой им операции в случаях и порядке, установленных договором банковского счета, заключенным между Сторонами, ЭД не принимается Банком к исполнению..

3.12. Стороны имеют право передавать или получать с использованием Системы только ЭД, перечисленные в Перечне ЭД Приложения № 1 к настоящему Договору.

3.13. Учет отправленных/принятых ЭД ведется Банком в Архиве электронных документов.

3.14. Учет действий по обработке отправленных/принятых ЭД ведется Банком в Электронном журнале Системы.

3.15. Электронные документы, применяемые в Системе, аутентичны бухгалтерским документам, используемым в соответствии с нормативными актами Банка России, и являются основанием для осуществления бухгалтерских записей.

4. ОБЯЗАННОСТИ СТОРОН

4.1. Банк обязуется:

4.1.1. Консультировать Клиента по вопросам функционирования Системы, использования программных средств, приема/передачи информации и технологии ее обработки.

4.1.2. Предоставить Уполномоченным лицам Клиента Логин и Пароль к Системе, средства защищённого хранения данных eToken (по желанию Клиента), а также возможность выполнения Уполномоченными лицами Клиента действий, предусмотренных в п. 6. настоящих Правил.

4.1.3. Зарегистрировать Клиента в качестве участника обмена ЭД в Системе, а также Ключ проверки электронной подписи Уполномоченного лица Клиента.

4.1.4. Осуществлять обработку полученных ЭД в строгом соответствии с установленными нормами, техническими требованиями, стандартами, инструкциями Банка России по подготовке данных, обработке, хранению и передаче информации.

4.1.5. Осуществлять переводы денежных средств и иные распоряжения Клиента по Счету в сроки, установленные Договором банковского счета.

4.1.6. Передавать Клиенту выписки по расчетным счетам и приложения к ним в электронном виде.

4.1.7. Информировать Клиента о состоянии каждого ЭД при помощи присваиваемых им статусов. Статусы ЭД отображаются во время сеансов связи, проводимых Клиентом.

4.1.8. Информировать Клиента о совершении каждой операции с использованием SMS-информирования по 10-тизначному номеру операторов сотовых сетей РФ, определенному Клиентом, при подключении к Системе (Приложение № 1 к Договору). Форма заявления на изменение 10-тизначного номера приведена в Приложении № 6 к настоящим Правилам. Временем информирования Клиента о совершении операции является время в электронном журнале Системы о моменте отправки SMS-сообщения Клиенту.

4.1.9. Предоставлять по запросу Клиента документы и информацию, которые связаны с использованием Системы при наличии такой возможности.

4.1.10. Контролировать полноту заполнения реквизитов в ЭД Клиента. Неправильно оформленные ЭД Клиента Банком к исполнению не принимаются.

4.1.11. Не изменять реквизиты ЭД Клиента.

4.1.12. Своевременно, не позднее окончания Операционного времени, после обнаружения неправильно оформленных ЭД информировать об этом Клиента, проставляя соответствующий Статус ЭД.

4.1.13. Направлять Клиенту ЭД, не содержащие компьютерных вирусов и/или иных вредоносных программ.

4.1.14. Вести и хранить Архивы электронных документов Системы в соответствии с порядком и сроками, установленными для расчетных документов, оформленных на бумажных носителях.

4.1.15. Вести Электронный Журнал Системы и хранить его не менее трех лет после прекращения действия Договора.

4.1.16. Своевременно информировать Клиента об изменениях порядка организации и проведения электронного документооборота между Банком и Клиентом и другой информации о Системе.

4.1.17. Информировать Клиента об условиях использования электронного средства платежа, в частности о любых ограничениях способов и мест использования, случаях повышенного риска использования электронного средства платежа до заключения с Клиентом Договора.

4.1.18. Фиксировать направленные Клиенту и полученные от Клиента уведомления, а также хранить соответствующую информацию не менее трех лет.

4.2. Клиент обязуется:

4.2.1. Назначить Уполномоченных лиц Клиента, ответственных за осуществление обмена ЭД с Банком, с представлением в Банк документов, подтверждающих назначение и полномочия указанных лиц.

4.2.2. Использовать для работы в Системе только лицензионные программные средства, указанные в Приложении № 2 к настоящим Правилам.

4.2.3. Регулярно знакомиться с объявлениями, размещенными Банком в разделе «Новости», а также с объявлениями, направленными Клиентам в виде произвольных документов. Неознакомление с объявлениями не дает Клиенту право ссылаться на их незнание при возникновении возможных споров.

4.2.4. Сменить Пароль при первом входе в Систему.

4.2.5. Сформировать Ключи электронной подписи и Ключи проверки электронной подписи, в соответствии с предоставленной банком инструкцией.

4.2.6. Своевременно осуществлять формирование и замену Ключей электронной подписи и Ключей проверки электронной подписи. Для электронных Ключей Клиента установлен срок их действия 1 год. Рекомендуется производить замену Ключей за месяц до истечения срока их действия.

4.2.7. Не передавать Ключ электронной подписи и Пароль третьим лицам. Рекомендуется регулярно менять Пароль для входа в систему и не использовать в Пароле простых комбинаций букв и цифр. Минимальная длина пароля - 6 символов, максимальная - 10 символов.

4.2.8. Хранить средство защищённого хранения eToken в недоступном для неуполномоченных лиц месте и отдельно от PIN кода.

4.2.9. Подключать eToken к компьютеру только на время работы с Системой. Не оставлять eToken в компьютере после завершения работы с Системой.

4.2.10. Своевременно обновлять программно-технические средства, указанные в Приложении № 2 к настоящим Правилам.

4.2.11. Использовать для работы в Системе только исправный и проверенный на отсутствие компьютерных вирусов персональный компьютер и направлять в Банк ЭД, не содержащие компьютерных вирусов и/или иных вредоносных программ.

4.2.12. Регулярно обновлять базы данных антивирусного ПО на рабочих местах Уполномоченных лиц клиента.

4.2.13. Выполнять требования по обеспечению безопасности при работе в Системе, приведенные в Приложении 11 к настоящим правилам.

4.2.14. Немедленно уведомлять Банк в порядке, указанном в п. 8 настоящих Правил обо всех случаях компрометации ключей электронной подписи, PIN кода и Пароля для входа в Систему Уполномоченного лица Клиента: утраты, хищения, несанкционированного использования (или подозрения о несанкционированном использовании) средства защищённого хранения eToken, PIN кода, Пароля или наступлении иного события, определенного Уполномоченным лицом Клиента как ознакомление неуполномоченным лицом (лицами) с перечисленными конфиденциальными данными. При этом доступ к Системе Уполномоченного лица Клиента с использованием скомпрометированных средств приостанавливается.

4.2.15. Немедленно информировать Банк о смене Уполномоченных лиц Клиента. При этом прекращается доступ к Системе лиц, право подписи ЭД которых прекращено Клиентом, а доступ к Системе новых Уполномоченных лиц Клиента предоставляется с момента регистрации Банком их ключей проверки электронной подписи.

4.2.16. Незамедлительно информировать Банк об изменении телефонного номера Клиента, предназначенного для SMS-информирования, предусмотренного п.4.1.8. настоящих Правил.

4.2.17. Не тиражировать и не передавать третьей стороне предоставленные Банком средства, необходимые для работы в Системе .

4.2.18. Оплачивать комиссии Банка в соответствии с Тарифами.

4.2.19. В случае утраты либо кражи мобильного телефона или SIM-карты с номером телефона, указанного в п.4.1.8. настоящих Правил, и иных обстоятельствах, в результате которых рассылка информации на указанный номер мобильного телефона прекращается, Клиент обязан незамедлительно уведомить об этом Банк для отключения номера телефона от SMS-информирования и предоставить новый номер мобильного телефона по форме Приложения 6. Клиент обязуется не предъявлять требований, а Банк не несет ответственности за возможное раскрытие информации, составляющей банковскую тайну Клиента или персональные данные Клиента, произошедшее до отключения Банком номера телефона от SMS-информирования.

4.2.20. Клиент самостоятельно оплачивает услуги других организаций, привлечение которых необходимо для нормального функционирования его системы получения SMS-сообщений, а также за собственный счет поддерживает в надлежащем состоянии свои технические и аппаратные средства.

4.3. Стороны взаимно обязуются:

4.3.1. Не предпринимать действий, способных нанести ущерб другой Стороне вследствие использования Системы.

4.3.2. Строго выполнять требования технической и эксплуатационной документации по средствам защиты информации, содержащиеся в инструкции по установке, настройке и работе с Системой.

4.3.3. Своевременно информировать другую Сторону обо всех случаях возникновения технических неисправностей или наступления других обстоятельств, препятствующих обмену ЭД.

4.3.4. В случае обнаружения возможных угроз безопасности Системы и обрабатываемым в ней ЭД Стороны обязуются незамедлительно извещать друг друга о них для принятия согласованных мер по защите.

4.3.5. Организовать внутренний режим функционирования рабочего места таким образом, чтобы исключить возможность использования Системы лицами, не имеющими доступа к ней, а также исключить возможность использования средств доступа неуполномоченными лицами.

4.3.6. Не разглашать третьим лицам, за исключением случаев, предусмотренных законодательством Российской Федерации или дополнительным соглашением Сторон, конкретные способы защиты информации, реализованные в Системе.

4.3.7. Своевременно рассматривать полученные по Системе ЭД и выполнять в установленные (согласованные) сроки действия в соответствии с настоящими Правилами.

4.3.8. Клиент признает информацию, хранимую на сервере Банка, в Архиве ЭД и в Электронном журнале в качестве эталонной, которая может быть предъявлена в Арбитражный суд для разрешения споров.

5. ПРАВА СТОРОН

5.1. Банк имеет право:

5.1.1. Не принимать к исполнению ЭД Клиента в случае несоответствия их законодательству Российской Федерации и Договору банковского счета с Клиентом.

5.1.2. Осуществлять обновление программного обеспечения Системы.

5.1.3. В одностороннем порядке устанавливать и изменять:

- Тарифы Банка;
- Настоящие Правила;

Информация об изменении настоящих Правил доводится до сведения Клиента за 10 (десять) рабочих дней до даты начала использования указанных изменений путем публичного оповещения: с использованием Системы и/или в сети Интернет на сайте Банка www.kmbank.ru или иными способами по выбору Банка.

5.1.4. Приостановить или прекратить по инициативе Клиента в порядке, предусмотренном в пункте 8.1. настоящих Правил, использование Системы Клиентом на основании полученного от него уведомления.

5.1.5. Приостановить или прекратить по собственной инициативе, использование Системы Клиентом, направив уведомление об этом Клиенту не позднее дня, следующего за днем совершения указанных действий, в случаях:

5.1.5.1. неисполнения или ненадлежащего исполнения Клиентом своих обязательств, указанных в Договоре и настоящих Правилах;

5.1.5.2. предъявления требований уполномоченных государственных органов в случаях и в порядке, предусмотренных законодательством Российской Федерации;

5.1.5.3. выявления подозрения на компрометацию у Уполномоченных лиц Клиента средств доступа к Системе, включая Пароль, PIN код доступа к средству защищенного хранения данных eToken, а также Ключа электронной подписи, в том числе вследствие нарушения Клиентом порядка использования Системы. Приостановка использования Системы Уполномоченными лицами Клиента действует до ввода в действие новых средств доступа к Системе взамен скомпрометированных;

5.1.5.4. наличия оснований, предусмотренных законодательством РФ и нормативно-правовыми актами и рекомендациями Банка России, регламентирующими порядок деятельности кредитных организаций. Возобновление использования Системы Клиентом выполняется Банком с учетом условий, предусмотренных законодательством РФ, нормативно-правовыми актами и рекомендациями Банка России;

5.1.6. отказать Клиенту в приеме ЭД, направив уведомление об этом Клиенту не позднее дня, следующего за днем получения ЭД:

5.1.6.1. в случаях и на основаниях, предусмотренных законодательством РФ и нормативно-правовыми актами и рекомендациями Банка России, регламентирующими порядок деятельности кредитных организаций;

5.1.6.2. в случаях, если право Клиента распоряжаться денежными средствами не удостоверено;

5.1.6.3. при выявлении подозрения о том, что ЭД фальсифицирован в целях совершения мошеннических действий третьими лицами. Для этих целей Банк использует систему выявления фальсифицированных ЭД, в том числе систему выявления имитации третьими лицами действий Клиентов при использовании Системы и иные средства выявления фальсифицированных ЭД.

Если Уполномоченное лицо Клиента подтвердит, в порядке установленном Приложением № 10 к настоящим Правилам, достоверность ЭД, Банк имеет право принять от Клиента ЭД к исполнению.

5.1.7. В случае отсутствия средств или их недостаточности, а также в случае приостановки операций по решению государственных органов на счетах Клиента, необходимых для оплаты сопровождения очередного месяца, приостановить обслуживание без письменного уведомления Клиента. Обслуживание возобновляется с момента оплаты текущего месяца сопровождения Системы в размере абонентской платы за полный месяц сопровождения.

5.1.8. В случае отсутствия средств или их недостаточности, а также в случае приостановки операций по решению государственных органов на счетах Клиента, необходимых для оплаты сопровождения до конца второго подряд месяца, отключить доступ Клиента к Системе и расторгнуть Договор в одностороннем порядке с первого числа следующего месяца.

5.1.9. Не принимать распоряжение Клиента на перевод денежных средств, в случае недостаточности денежных средств на Счете. При недостаточности денежных средств на Счете Клиент получает уведомление от Банка об отказе в приеме распоряжения.

В течение операционного дня Клиент имеет право многократно направить в Банк каждое распоряжение на перевод денежных средств. После определения достаточности денежных средств на Счете, распоряжение принимается к исполнению и ЭД присваивается статус «В обработке».

В случае, предусмотренном Соглашением об овердрафте, который является дополнительным соглашением к Договору банковского счета, достаточность денежных средств на Счете определяется указанным Соглашением.

5.1.10. Приостановление или прекращение использования Клиентом Системы не прекращает обязательств Клиента и Банка, возникших до момента приостановления или прекращения указанного использования.

5.1.11. Банк оставляет за собой право вносить изменения в перечень событий и форматов SMS-сообщений, предусмотренных в п.4.1.8. настоящих Правил, уведомив об этом Клиента через Систему или другим доступным образом не менее чем за 5 (Пять) рабочих дней до предполагаемого изменения.

5.1.12. Банк имеет право в одностороннем порядке временно приостановить передачу SMS-сообщений Клиенту, предусмотренных в п.4.1.8. настоящих Правил, без предварительного оповещения Клиента, если, по мнению Банка, такая мера необходима для обеспечения безопасности системы.

5.2. Клиент имеет право:

5.2.1. Требовать от Банка предоставления информации о причинах неисполнения ЭД.

5.2.2. Получать от Банка необходимую информацию и консультационные услуги по вопросам использования Системы.

5.2.3. Получать от Банка необходимые подтверждения выполненных операций.

5.2.4. Получать от Банка информацию по счету в любой момент времени.

5.2.5. В случае несогласия с изменением Банком Правил или Тарифов, отказаться от исполнения Договора, уведомив Банк за пять рабочих дней до предполагаемой даты его расторжения.

5.2.6. Подключать доступ к Системе пользователей, не являющихся Уполномоченными лицами Клиента. Эти пользователи не имеют права подписи под платежными ЭД и не включены в Банковскую карточку. Эти пользователи подключаются к системе аналогично Уполномоченным лицам в соответствии с п.п. 6.2 – 6.9. настоящих Правил. Электронная подпись пользователей, не являющихся Уполномоченными лицами используется исключительно для авторизации. Кроме того, Ключ электронной подписи такого пользователя используется для установки подписи под запросом на регистрацию ключа проверки электронной подписи при плановой смене ключей в соответствии с п. 7 настоящих Правил.

6. ПОРЯДОК ПОДКЛЮЧЕНИЯ К СИСТЕМЕ

6.1. Уполномоченными лицами Клиента являются руководитель и главный бухгалтер (при его наличии) и/или другие Уполномоченные лица Клиента, которым Клиентом предоставлено право создавать ЭД (соответственно, право первой или второй подписи) и которые в обязательном порядке должны быть указаны в Банковской карточке Клиента, представляемой в Банк в соответствии с Договором банковского счета.

6.2. Клиент направляет в Банк Заявку на выдачу средства защищенного хранения данных eToken (Приложение № 4 к настоящим Правилам), в которой указывает необходимое количество средств защищенного хранения eToken, а также данные Уполномоченных лиц Клиента, для которых в Системе будут заведены пары Логин и Пароль. Клиент также может использовать устройство eToken, приобретенное им самостоятельно.

6.3. Логин и Пароль к Системе, средства защищённого хранения данных eToken выдаются в Банке непосредственно Уполномоченному лицу Клиента или его представителю при представлении в Банк надлежащим образом оформленной доверенности, форма которой приведена в Приложении №3 к настоящим Правилам. Передача средства защищенного хранения данных eToken оформляется Актом приема-передачи (Приложение №5 к настоящим Правилам).

6.4. Логин и Пароль к Системе выдаются Уполномоченному лицу Клиента либо его представителю в защищенных от вскрытия конвертах.

6.5. Уполномоченное лицо Клиента либо его представитель при приеме от Банка Логина и Пароля Системы проверяет целостность конвертов и подписывает Расписку в получении Логина и Пароля к Системе по типовой форме, утвержденной в Банке.

6.6. Для защиты и подтверждения подлинности ЭД в Системе используется электронная подпись, формируемая для каждого ЭД с использованием СКЗИ, являющегося неотъемлемой частью Системы. Для подписания ЭД электронной подписью Уполномоченному лицу Клиента необходимо создать Ключи электронной подписи и Ключи проверки электронной подписи.

6.7. Создание Ключа электронной подписи и Ключа проверки электронной подписи в Системе производится на рабочем месте Клиента.

6.8. После создания Ключа электронной подписи и Ключа проверки электронной подписи Клиент должен предоставить в Банк в двух экземплярах с подписью и печатью Акт признания открытого ключа (сертификата) для обмена сообщениями (Приложение №7 к настоящим Правилам). Регистрация Ключа

проверки электронной подписи в Системе производится в Банке на основании Акта признания открытого ключа (сертификата) для обмена сообщениями.

6.9. До начала работы в Системе Уполномоченное лицо Клиента обязано сменить Пароль (PIN код), установленный по умолчанию для средства защищённого хранения данных eToken.

6.10. В Систему встроен механизм ограничения доступа клиентов с IP-адресов, не входящих в список разрешенных Клиентом. Данный механизм ограничения доступа по IP-адресам является индивидуальным для каждого Клиента и может быть включён Банком по письменному требованию Клиента (форма заявки приведена в Приложении №12 к настоящим Правилам).

7. ПЛАНОВАЯ СМЕНА РАБОЧИХ КЛЮЧЕЙ ЭЛЕКТРОННОЙ ПОДПИСИ.

7.1. Срок действия рабочих Ключей электронной подписи и проверки электронной подписи Клиента, используемых в Системе, составляет 12 (двенадцать) месяцев.

7.2. За 30 календарных дней до окончания срока действия рабочего ключа электронной подписи Банк уведомляет Клиента посредством Системы о необходимости смены Ключей.

7.3. Клиенту необходимо произвести генерацию Ключа электронной подписи и Ключа проверки электронной подписи и направить в Банк посредством Системы запрос на регистрацию Ключа проверки электронной подписи.

7.4. Клиенту необходимо распечатать в двух экземплярах Акт признания открытого ключа (сертификата) для обмена сообщениями (Приложение №7 к настоящим Правилам) и с подписью руководителя, заверенной печатью, предоставить в Банк не позднее, чем за сутки до истечения срока действия рабочего Ключа электронной подписи.

7.5. Если Клиент не произвел своевременную смену своих ключей, его обслуживание в Системе будет приостановлено с даты окончания действия рабочих ключей. Обслуживание будет возобновлено после обращения Клиента в Банк и генерации новых Ключей.

8. ПРИОСТАНОВКА И ПРЕКРАЩЕНИЕ ИСПОЛЬЗОВАНИЯ СИСТЕМЫ УПОЛНОМОЧЕННЫМИ ЛИЦАМИ КЛИЕНТА

8.1. В случае необходимости приостановки или прекращения использования Системы Уполномоченными лицами Клиента в результате компрометации Ключа электронной подписи Клиенту следует незамедлительно сообщить в Банк по телефону: (495) 510-63-91 в рабочий день с 09 до 18 часов московского времени (в пятницу с 09 до 17 часов московского времени), назвав действующее кодовое слово, указанное в Приложении № 1 к Договору или в соответствующем Заявлении об изменении кодового слова для идентификации, после чего предоставить в Банк не позднее следующего рабочего дня Уведомление по форме Приложения № 8 к настоящим Правилам.

8.2. Уведомление, указанное в п. 8.1. настоящих Правил, может быть направлено в Банк:

- в виде документа на бумажном носителе, заверенного печатью и подписью Клиента в двух экземплярах.
- в форме ЭД, направленного с использованием Системы, прикрепленного к ЭД “Произвольный документ в Банк”.

8.3. При получении от Клиента Уведомления, указанного в п. 8.1. настоящих Правил, на бумажном носителе работник Банка указывает на Уведомлении дату и время его получения и передает второй экземпляр Уведомления Клиенту с отметкой о регистрации. При отправке Клиентом Уведомления, указанного в п. 8.1. настоящих Правил, в виде документа Системы, дата и время получения такого Уведомления фиксируется средствами Системы автоматически.

8.4. Банк не позднее 4 (четырех) часов после получения Уведомления, указанного в п. 8.1. настоящих Правил, прекращает прием документов сформированных с использованием скомпрометированного Ключа электронной подписи.

8.5. Если Уведомление, указанное в п. 8.1. настоящих Правил, получено Банком менее чем за 4 (четыре) часа до истечения рабочего дня, то срок исполнения Уведомления может быть перенесен на следующий рабочий день.

9. СРОКИ ПРИЕМА И ОТЗЫВА ЭД

9.1. Прием ЭД производится Банком в рабочие дни (с понедельника по четверг) с 9 час. 00 мин. до 18 час. 00 мин., а в пятницу и предпраздничные дни с 9 час. 00 мин. до 17 час. 00 мин. по московскому времени за исключением периодов технического обслуживания Системы. В последнем случае Банк заранее предупреждает Клиента о возможных перерывах в обслуживании средствами Системы.

9.2. Отзыв ЭД осуществляется после получения Банком от Клиента сообщения по Системе, с указанием реквизитов отзываемого ЭД. Отзыв расчетного документа, переданного в Банк в виде ЭД, может быть произведен только в том случае, если у Банка имеется возможность отменить его исполнение. Отзыв ЭД производится Клиентом не позднее 1-го часа с момента передачи ЭД в Банк при условии, что сумма по ЭД не списана с корреспондентского счета Банка/не зачислена на счет получателя в Банке.

9.3. Безотзывность перевода денежных средств наступает с момента списания денежных средств с банковского счета Клиента. Перевод денежных средств становится безотзывным и окончательным после осуществления Банком действий, указанных в п. 9.2. настоящих Правил.

9.4. Стороны устанавливают, что все Статусы ЭД, передаваемые Банком в Системе, считаются доведенными до сведения Клиента не позднее рабочего дня, следующего за днем их направления Клиенту.

10. ОТВЕТСТВЕННОСТЬ СТОРОН

10.1. Стороны несут ответственность за содержание любого ЭД при условии подтверждения подлинности электронной подписи в данном ЭД.

10.2. Банк несет ответственность в случаях несвоевременного либо необоснованного списания денежных средств со Счета, а также невыполнения указаний Клиента о перечислении денежных средств в установленные сроки в соответствии с условиями Договора банковского счета.

10.3. В случае, если Банк исполняет обязанность по информированию Клиента о совершенной операции в соответствии с п. 4.1.8. настоящих Правил и Клиент не позднее дня, следующего за днем получения уведомления о совершении операции без согласия клиента, не направил Банку уведомление по форме, указанной в Приложении № 8 к настоящим Правилам, Банк не обязан возместить сумму операции, совершенной без согласия Клиента.

10.4. Клиент несет ответственность за любую операцию в Системе с момента ввода в действие Ключа проверки электронной подписи Уполномоченных лиц Клиента, использованных для совершения такой операции.

10.5. При выполнении распоряжений Клиента Банк не несет ответственности за достоверность и правильность информации, указанной в ЭД Клиента, при условии подтверждения подлинности электронной подписи Уполномоченных лиц Клиента в ЭД.

Стороны признают, что передача данных с использованием протокола SSL обеспечивает защиту от несанкционированного доступа.

Риски возникновения неблагоприятных последствий в связи с нарушением Клиентом конфиденциальности использования средств доступа Уполномоченного лица Клиента, лежат на Клиенте.

10.6. Банк не несет ответственность за последствия исполнения ЭД, подписанных неуполномоченными лицами, в тех случаях, когда с использованием предусмотренных банковскими правилами и настоящими Правилами процедур Банк не мог установить факта подписания ЭД неуполномоченными лицами.

10.7. Банк не несет ответственности за убытки, понесенные Клиентом, или упущенную прибыль Клиента в связи с задержкой или невозможностью передачи ЭД, если это явилось следствием неисправностей или некачественного функционирования каналов Интернет, либо неправильного функционирования программного обеспечения, используемого Клиентом, если это произошло не по вине Банка.

10.8. Банк не несет ответственности за последствия, возникшие в результате того, что Клиент не ознакомился или несвоевременно ознакомился со Статусами ЭД в Системе в порядке и сроки, установленные Правилами.

10.9. Банк не несет ответственность за корректность работы Системы, в случае если на рабочем месте Клиента установлено, либо используется программное обеспечение (включая средства защиты информации), предназначенное для систем дистанционного банковского обслуживания других Банков.

10.10. Клиент несет ответственность за своевременность предоставления Банку актуальной информации, предусмотренной п. 4.1.8. Правил.

10.11. Банк не несет ответственность за несвоевременность информирования Клиента о совершении каждой операции в соответствии с п. 4.1.8. Правил в случае несвоевременного предоставления Клиентом актуальной информации, указанной п. 4.1.8. Правил.

10.12. Банк не несет ответственности за сбои в Системе в случаях:

- модификации клиентской части Системы Клиентом;
- удаления элементов программного обеспечения Клиентом;
- повреждения операционной системы Клиента вирусами и вредоносными программами;
- нестабильной работы операционной системы или аппаратного обеспечения рабочего места Клиента;
- несвоевременной смены ключей Клиентом.

10.13. Банк не несет ответственность за убытки Клиента, возникшие в результате:

- нарушения или невыполнения Клиентом настоящих Правил;

- в результате умышленной или неосторожной утраты (порчи, передачи, утери, разглашения) Клиентом применяемых в Системе паролей, ключей, конфиденциальной информации и/или программного обеспечения;

- несвоевременного сообщения Клиентом в Банк о компрометации своих ключей;

- несанкционированного доступа третьих к Клиентскому рабочему месту;

- заражения рабочего места Клиента вирусами и вредоносными программами.

10.14. Клиент проинформирован и согласен с тем, что используемые Банком телекоммуникации, предусмотренные п. 4.1.8. настоящих Правил, являются открытыми и не гарантируют полную защиту передаваемой информации. Клиент также согласен с тем, что банк не несет ответственности за возможное раскрытие информации, составляющей банковскую тайну, и принимает на себя риск такого разглашения. Клиент также подтверждает, что все лица, имеющие доступ к рассылаемой информации, уполномочены на то Клиентом.

11. ПОРЯДОК РАЗРЕШЕНИЯ СПОРОВ

11.1. Ответственность Банка перед Клиентом ограничивается только документально подтвержденным реальным ущербом, возникшим у Клиента в результате виновных действий или бездействий Банка и не распространяется на ущерб, вызванный действиями третьих лиц путем несанкционированного доступа к информации и данным на стороне Клиента.

11.2. Любые споры между Банком и Клиентом, предметом которых является:

- неподтверждение подлинности ЭД средствами принимающей Стороны;

- оспаривание факта формирования ЭД;

- заявление Клиента об искажении ЭД;

- оспаривание факта отправления и/или доставки ЭД;

- оспаривание времени отправления и/или доставки ЭД;

- иные случаи возникновения спорных ситуаций, связанных с функционированием Системы, передаются для разрешения специально создаваемой согласительной комиссии, если спор не урегулирован Сторонами путем переговоров.

11.3. Согласительная комиссия созывается Банком на основании письменного заявления (претензии) Клиента, оспаривающего ЭД или иные фактические обстоятельства, связанные с использованием Системы. В указанном заявлении Клиент, помимо реквизитов оспариваемого документа, также должен указать лицо (лиц), уполномоченных представлять интересы Клиента в согласительной комиссии.

11.4. В случае получения от Клиента письменного запроса о предоставлении информации о результатах рассмотрения заявления (претензии) Банк информирует Клиента о результатах рассмотрения заявления (претензии) не позднее 30 (тридцати) рабочих дней со дня получения Банком заявления (претензии), а также не позднее 60 (шестидесяти) рабочих дней в случае оспаривания трансграничного перевода денежных средств.

11.5. Не позднее 10 (десяти) рабочих дней с даты получения претензии Банк по согласованию с Клиентом назначает дату, место и время начала работы согласительной комиссии. Банк письменно, не позднее, чем за 3 (три) рабочих дня до начала работы согласительной комиссии, уведомляет Клиента о назначенной дате, времени и месте начала работы согласительной комиссии и необходимости предоставить в Банк копию оспариваемого документа на бумажном носителе, заверенную подписями и печатью Клиента.

11.6. Состав согласительной комиссии формируется в равном количестве из представителей Банка и Клиента. При необходимости в состав согласительной комиссии могут быть включены представители разработчика используемого программного обеспечения и/или другие эксперты

11.7. В случае, если Клиент не направит своих представителей для участия в работе согласительной комиссии, он лишается права предъявления каких-либо претензий к результатам работы согласительной комиссии.

11.8. Для работы комиссии Банк предоставляет помещение и оборудование, необходимое для работы комиссии.

11.9. Проверка оспариваемого ЭД осуществляется в присутствии всех членов согласительной комиссии.

11.10. Результаты работы согласительной комиссии оформляются в виде письменного заключения – акта согласительной комиссии, подписываемого всеми членами комиссии (далее – Акт). Акт составляется немедленно после завершения оценки всех обстоятельств, подлежащих установлению согласительной комиссией в 3 (трех) экземплярах (1 (один) экземпляр – для Клиента и 2 (два) – для Банка).

11.11. В Акте фиксируются:

- результаты всех этапов работы согласительной комиссии;
- все существенные реквизиты оспариваемого ЭД.

Акт комиссии является окончательным и пересмотру не подлежит.

11.12. Подтверждение подлинности ЭД, зафиксированное в Акте, будет означать, что этот ЭД имеет юридическую силу и является законным основанием для осуществленных Банком сделок за счет Клиента или иных операций по счетам Клиента.

11.13. Неподтверждение подлинности ЭД, зафиксированное в Акте, будет означать, что этот ЭД не имеет юридической силы и не является законным основанием для осуществленных Банком сделок за счет Клиента или иных операций по счетам Клиента.

11.14. Составленный Акт может быть предъявлен в судебные и иные органы в случае необходимости такого разбирательства и будет являться доказательством подлинности ЭД/неподтверждения подлинности ЭД, в зависимости от того, что было зафиксировано в Акте в соответствии с п.п. 11.10, 11.11, 11.12 Правил.

11.15. Неурегулированные в предусмотренном настоящим разделом Правил порядке споры подлежат рассмотрению в Арбитражном суде г.Москвы.

Приложение № 1
к Правилам обслуживания клиентов в системе
дистанционного банковского обслуживания
«Интернет Клиент-Банк»

Перечень электронных документов, подлежащих обработке в Системе и требования по их оформлению

1. Перечень ЭД, подлежащих обработке в Системе:

1.1. Платежные поручения;

1.2. Поручения на перевод валюты;

1.3. Поручения на покупку валюты;

1.4. Поручения на продажу валюты;

1.5. Произвольные документы в Банк;

1.6. Запросы на отзыв документа;

1.7. Запросы на получение выписки;

2. Перечисленные в пункте 1 настоящего приложения ЭД при надлежащем оформлении и заверении электронной подписью имеют юридическую силу документов на бумажных носителях, оформленных в соответствии с требованиями законодательства, а также подписанных соответствующим количеством подписей Уполномоченных лиц и заверенных оттиском печати Стороны, оформившей ЭД, и порождают аналогичные им права и обязательства Сторон.

3. Требования по оформлению ЭД:

Все ЭД Клиента должны содержать необходимые реквизиты и информацию, установленные законодательством Российской Федерации, нормативными актами Банка России, банковскими правилами, договором банковского счета и настоящими Правилами обслуживания клиентов в системе дистанционного банковского обслуживания «Интернет Клиент-Банк» и должны быть подписаны двумя электронными подписями (первая и вторая подпись) или одной электронной подписью (при отсутствии в штате Клиента лица, которому может быть предоставлено право второй подписи) Уполномоченных лиц Клиента.

ЭД порождает обязательства Сторон, если он передающей Стороной должным образом оформлен, заверен электронной подписью и передан, а принимающей Стороной получен, проверен и принят.

Электронная подпись в ЭД равнозначна собственноручной подписи в документе на бумажном носителе.

Приложение № 2
к Правилам обслуживания клиентов в системе
дистанционного банковского обслуживания
«Интернет Клиент-Банк»

Перечень средств необходимых для организации работы в Системе

1. Канал доступа в Интернет по протоколу HTTPS.
2. USB-порт для подключения средства защищенного хранения данных eToken.
3. Программные средства:
   3.1. Базовая операционная система:
   • Microsoft Windows Vista/7/8/10;
   3.2. Интернет-браузер:
   • Microsoft Internet Explorer версий 9.0, 10.0, 11.0;
   .3.3. Офисные программы (рекомендованы для печати и выгрузки документов):
   • Microsoft Word, Microsoft Excel версий 2003, 2007, 2010;
   3.3. Специальное программное обеспечение (драйверы) для обеспечения работы со средством защищенного хранения данных eToken;.
   3.4. Антивирусное программное обеспечение.

4. Права локального администратора в операционной системе (на период установки или обновления программного обеспечения).
5. Средства доступа к Системе (логин, пароли для входа в систему и для авторизации на устройстве защищенного хранения данных eToken).
6. Средство защищенного хранения данных eToken (для формирования и хранения Ключа электронной подписи)

Приложение № 3
к Правилам обслуживания клиентов в системе
дистанционного банковского обслуживания
«Интернет Клиент-Банк»

На бланке организации

ДОВЕРЕННОСТЬ

г. Москва «_____» _____ 20___ г.

Общество с ограниченной ответственностью "НАИМЕНОВАНИЕ" в лице
(название организации)
Генерального директора ФАМИЛИЯ ИМЯ ОТЧЕСТВО,
(должность, Фамилия, Имя, Отчество руководителя)
действующего на основании Устава, доверяет

_____
(Ф.И.О., паспортные данные уполномоченного лица)
_____

осуществлять в Банке «Кузнецкий мост» АО все действия по оформлению документов, связанных с договором об участии в системе дистанционного банковского обслуживания «Интернет Клиент-Банк», в том числе совершать следующие действия:

1) получать из банка договоры о присоединении к Правилам обслуживания клиентов в системе дистанционного банковского обслуживания «Интернет Клиент-Банк» с приложениями;
2) получать материальные ценности: средство защищённого хранения данных eToken;
3) получать Акт приема-передачи средства защищённого хранения данных eToken;
4) получать Соглашение о расторжении договора об участии в системе дистанционного банковского обслуживания «Интернет Клиент-Банк».*

Настоящая Доверенность выдана без права передоверия третьим лицам и действительна в течение тридцати календарных дней со дня выдачи.

Подпись Фамилия Имя Отчество _____ удостоверяю.
(Фамилия, Имя, Отчество уполномоченного лица) (Образец подписи)

Генеральный директор _____ ФАМИЛИЯ И.О.
(Должность руководителя) (Подпись) (Фамилия И.О. руководителя)

М.П.

Примечания:
* Пункт 4 указывается в случае расторжения договора о присоединении к Правилам обслуживания клиентов в системе дистанционного банковского обслуживания «Интернет Клиент-Банк»

Приложение № 4
к Правилам обслуживания клиентов в системе
дистанционного банковского обслуживания
«Интернет Клиент-Банк»

ЗАЯВКА

на выдачу средства защищённого хранения данных eToken

г. Москва «____»_____ 20__ г.

_____
(наименование Клиента)
_____, именуемый в дальнейшем «Клиент», в лице _____
(Ф.И.О. представителя Клиента)
_____, действующ _____ на основании _____, расчетный / текущий счет № _____ прошу выдать средство защищённого хранения данных eToken, в количестве _____ штук.
(прописью)

Прошу Вас зарегистрировать ключи электронной подписи Системы «Интернет Клиент-Банк» для следующих уполномоченных лиц:

1._____ _____
(фамилия, имя, отчество) (должность)
2._____ _____
(фамилия, имя, отчество) (должность)
3._____ _____
(фамилия, имя, отчество) (должность)
4._____ _____
(фамилия, имя, отчество) (должность)

Примечание: на одно уполномоченное лицо может быть зарегистрировано несколько ключей.

_____ (_____)
(подпись) (расшифровка подписи)

"_____" _____ 20 ___ г.

М.П.

==========

Заполняется Банком.

Выдано средство защищённого хранения данных eToken в количестве _____ штук.

_____ _____ (_____)
(должность) (подпись) (расшифровка подписи)

Приложение № 5
к Правилам обслуживания клиентов в системе
дистанционного банковского обслуживания
«Интернет Клиент-Банк»

АКТ
приема-передачи средства защищённого хранения данных eToken

г. Москва «__» _____ 20 г.

Банк "Кузнецкий мост" АО, именуемый в дальнейшем «Банк», в лице Первого Заместителя Председателя Правления Мокрушева Андрея Борисовича, действующего на основании Доверенности, удостоверенной 11.01.2016 года Врублевской Татьяной Вячеславовной, нотариусом города Москвы, зарегистрированной в реестре за № 6-5541, с одной стороны, и Общество с ограниченной ответственностью «_____», именуемое в дальнейшем «Клиент», в лице _____, действующего по _____ от __.__.____г., с другой стороны, вместе в дальнейшем именуемые Стороны, подписали настоящий Акт о нижеследующем:

Для работы в системе дистанционного банковского обслуживания «Интернет Клиент-Банк» Банк передает Клиенту, а Клиент принимает средство защищённого хранения данных eToken (сертификат соответствия ФСТЭК от 11.08.2009 г. № 1883) в количестве ___ штук. Данное устройство является аппаратным средством хранения цифровых криптографических данных Клиента в защищенной памяти устройства.

Клиент несёт ответственность за выполнение следующего порядка хранения и обращения со средством защищенного хранения данных:

- хранить eToken в недоступном месте;
- подключать eToken к компьютеру только на время работы с системой «Интернет Клиент-Банк» .

При передаче средства защищённого хранения данных eToken представителями Сторон проверена комплектность. Претензии у Клиента к средству защищённого хранения данных eToken и факту его передачи отсутствуют. Настоящий Акт составлен в двух экземплярах по одному для каждой из сторон.

Серийные номера переданных eToken:

_____
_____
_____
_____
_____
_____

БАНК:

Первый Заместитель Председателя Правления

_____ А.Б. Мокрушев
(подпись) (Фамилия И.О.)

М.П.

КЛИЕНТ:

Доверенное лицо/Генеральный директор

_____ _____ _._.
(подпись) (Фамилия И.О.)

М.П.

Приложение № 6
к Правилам обслуживания клиентов в системе дистанционного банковского обслуживания «Интернет Клиент-Банк»

В Банк «Кузнецкий мост» АО

От _____
(должность)
_____
_____
_____
(полное наименование Клиента)
_____
_____
(Фамилия, имя, отчество)

Заявление об изменении телефонного номера для получения SMS-уведомлений от Банка

Во исполнение Договора о присоединении к Правилам обслуживания клиентов в системе дистанционного банковского обслуживания «Интернет Клиент-Банк» № _____ от _____

прошу изменить телефонный номер для получения SMS-уведомлений о совершенных платежах и паролей для подтверждения электронных документов на следующий:

+	7										

Подтверждаю, что указанный мною номер принадлежит российскому сотовому оператору, является действующим и доступен для входящих SMS-сообщений.

Я предупреждён, что в случае изменения номера необходимо предоставить в Банк «Кузнецкий мост» АО Заявление об изменении телефонного номера для получения SMS-уведомлений о совершенных платежах и паролей для подтверждения электронных документов.

Дата подписания заявления: _____

КЛИЕНТ:
Руководитель

_____ _____
м.п. Фамилия И.О.

ПРИНЯТО:

Дата и время принятия заявления: _____

БАНК:
Уполномоченный сотрудник Банка

_____ Ф.И.О.
м.п.

Приложение № 7
к Правилам обслуживания клиентов в системе
дистанционного банковского обслуживания
«Интернет Клиент-Банк»

АКТ
признания открытого ключа (сертификата)
для обмена сообщениями

"__ "_____ 20__ г. г. Москва

Настоящим Актом признается ключ проверки электронной подписи и открытый ключ шифрования, принадлежащий уполномоченному представителю Организации: _____

Параметры ключа:
Алгоритм:

Текст открытого ключа:

Ключ действителен с "____"_____20__г. по "___"_____20__г.

Ключ зарегистрирован и может использоваться для обмена сообщениями.

БАНК **КЛИЕНТ**

_____ _____

_____ _____

М.П. **М.П.**

Приложение № 8
к Правилам обслуживания клиентов в системе
дистанционного банковского обслуживания
«Интернет Клиент-Банк»

В Банк «Кузнецкий мост» АО

От _____
(должность)
_____
_____
_____
(полное наименование Клиента)
_____
_____
(Фамилия, имя, отчество)

Уведомление

Во исполнение Договора о присоединении к Правилам обслуживания клиентов в системе дистанционного банковского обслуживания «Интернет Клиент-Банк» № _____ от _____

1) заблокировать имеющиеся ключи электронной подписи системы «Интернет Клиент-Банк» уполномоченного лица

._____ _____
(фамилия, имя, отчество) (должность)

по причине *(отметить)*:

- ☐ Компрометация ключей электронной подписи
- ☐ Прекращение полномочий
- ☐ Утеря пароля к устройству eToken, блокировка устройства eToken
- ☐ Неисправность устройства eToken
- ☐ Пропуск срока плановой замены ключа электронной подписи
- ☐ Другая причина: _____

2) зарегистрировать новые ключи электронной подписи системы «Интернет Клиент-Банк» для уполномоченного лица

._____ _____
(фамилия, имя, отчество) (должность)

Я предупрежден о том, что:

Банк «Кузнецкий мост» АО будет продолжать осуществлять отправку SMS для информирования и подтверждения электронных платежей с использованием ранее указанного номера мобильного телефона.

В случае изменения номера мобильного телефона Клиент обязан предоставить в Банк «Кузнецкий мост» АО Заявление об изменении телефонного номера для получения SMS-уведомлений от Банка.

Должность _____ (_____)
(подпись) (расшифровка подписи)

"_____" _____ 20 ___ г.

М.П.

ПРИНЯТО:

Дата и время принятия заявления: _____

БАНК:

Уполномоченный сотрудник Банка

_____ Ф.И.О.

м.п.

Приложение № 9
к Правилам обслуживания клиентов в системе
дистанционного банковского обслуживания
«Интернет Клиент-Банк»

Заявление об изменении кодового слова для идентификации

Во исполнение Договора о присоединении к Правилам обслуживания клиентов в системе дистанционного банковского обслуживания «Интернет Клиент-Банк» № _____ от _____

прошу изменить кодовое слово для идентификации на следующее:

Дата подписания заявления: _____

КЛИЕНТ:
Руководитель

_____ _____
м.п. Фамилия И.О.

ПРИНЯТО:

Дата и время принятия заявления: _____

БАНК:
Уполномоченный сотрудник Банка

_____ Ф.И.О.
м.п.

Приложение № 10
к Правилам обслуживания клиентов в системе
дистанционного банковского обслуживания
«Интернет Клиент-Банк»

Порядок действий Клиента в случае необходимости подтверждения ЭД.

В случае появления подозрения в фальсификации отдельным ЭД может быть присвоен статус «требует подтверждения».

Клиент **обязан** произвести необходимые действия для подтверждения подлинности или компрометации ЭД.

Для подтверждения подлинности ЭД Клиенту необходимо выполнить следующие действия:

1) **Запросить** с помощью соответствующего функционала Системы SMS-сообщение, содержащее информацию, содержащую реквизиты подозрительного ЭД и пароль подтверждения, которое будет отправлено на 10-тизначный номер, указанный в Приложении 6 к настоящим Правилам.

2) Сверить реквизиты ЭД с указанными в полученном SMS-сообщении и **ввести** пароль подтверждения в Систему. В случае правильного ввода пароля, после определения достаточности денежных средств на Счете, распоряжение принимается к исполнению и ЭД присваивается статус «В обработке». В случае трехкратного ошибочного ввода пароля ЭД присваивается статус «не принят» и данный ЭД Банком не обрабатывается. В случае, если процедура подтверждения ЭД была проведена позднее, чем через 10 дней после отправки документа, Банк имеет право не принимать документ.

Для компрометации ЭД Клиенту необходимо выполнить следующие действия:

1) **Запросить** с помощью соответствующего функционала Системы SMS-сообщение, содержащее информацию о подозрительном ЭД и пароль подтверждения, которое будет отправлено на 10-тизначный номер сотовых операторов РФ, указанный в Приложении 6 к настоящим Правилам.

2) **Три раза ввести** пароль «**0**» в Систему. В этом случае ЭД присваивается статус «не принят» и данный ЭД Банком не обрабатывается.

Пароль подтверждения является конфиденциальной информацией и ни при каких обстоятельствах не может быть передан третьим лицам, в т.ч. сотрудникам Банка.

Приложение № 11
к Правилам обслуживания клиентов в системе
дистанционного банковского обслуживания
«Интернет Клиент-Банк»

Требования к Клиенту по обеспечению безопасности при работе в системе «Интернет Клиент-Банк»

Использование Системы сопряжено с наличием рисков несанкционированного использования средств Клиента злоумышленниками: внутренними, в том числе персоналом Клиента, и внешними, как правило, использующими для хищения средств заражение компьютеров вирусами. С помощью электронных писем, при просмотре интернет страниц или после подключения инфицированного USB-накопителя (флеш карта, смартфон, внешний жесткий диск) компьютер Клиента может быть заражен вирусом. Далее злоумышленник скрытно устанавливает программное обеспечение для перехвата пароля на вход в систему и PIN кода доступа к устройству eToken, затем удаленно подключается к компьютеру Клиента и либо ждет удобного момента (когда подключено средство защищенного хранения данных eToken и компьютер оставлен без присмотра), чтобы скрытно создать и подписать электронной подписью платежное поручение от его имени, либо устанавливает дополнительное программное обеспечение для подмены реквизитов в платежных поручениях в момент создания для них электронной подписи.

Чтобы минимизировать риски Клиенту следует исполнять требования по обеспечению безопасности. Данные требования разработаны как для технических специалистов Клиента, так и для Уполномоченных лиц, непосредственно работающих в системе.

1. Обязательно следует использовать и регулярно обновлять антивирусное программное обеспечение. Наличие антивируса даже с актуальными базами в настоящее время не может полностью гарантировать того, что компьютер не будет заражен вирусом, однако значительно снижает данный риск.

2. Следует использовать межсетевой экран (фаерволл) либо на границе сети предприятия, либо персональный фаерволл на компьютере предназначенном для работы в Системе. Рекомендуется изолировать используемые в системе компьютеры от остальной сети предприятия, оставив открытыми только необходимые для работы порты. Рекомендуется разрешить подключение компьютера к серверу системы (https://ib.kmabnk.ru) и серверам обновлений используемого программного обеспечения, любые иные подключения рекомендуется запретить.

3. Не реже чем раз в неделю следует выполнять антивирусные проверки компьютера.

4. Подключить услугу IP-фильтрации, ограничив доступ к Системе только с ip-адресов организации.

5. Необходимо ежедневно получать выписку по счетам и сверять данные о проведенных операциях

6. Необходимо следить за SMS-уведомлениями о совершенных платежах. Быстро обнаруженное несанкционированное Клиентом платежное поручение, позволяет отозвать или приостановить его исполнение до того момента когда похищенные средства будут обналичены злоумышленниками.

7. При обнаружении SMS сообщений для подтверждения платежных поручений, которые не были созданы Клиентом, необходимо незамедлительно связаться с Банком по телефону, даже если подтверждаемые платежные поручения отсутствуют в системе.

8. Злоумышленники могут создать мошеннический ресурс с похожим на сайт Системы адресом и визуально похожим интерфейсом. Чтобы избежать ввода конфиденциальной информации на таком ресурсе, в начале работы каждого сеанса в Системе необходимо убедиться в правильности адреса Банка (https://ib.kmbank.ru) и в корректности SSL-сертификата Банка (Наличие иконки “закрытый замок” в адресной строке браузера).

9. На рабочем месте для работы в Системе следует использовать только лицензионное ПО, регулярно (не реже 1 раза в месяц) устанавливать обновления операционной системы (желательно в автоматическом режиме).

10. Запретить удаленный доступ к ресурсам компьютера, используемого для работы в Системе. Не создавать на компьютере общие файловые ресурсы и не устанавливать программы для доступа к удаленному рабочему столу.

11. Не устанавливать и не сохранять подозрительные файлы, полученные из ненадежных источников, полученные по электронной почте, через службы мгновенного обмена сообщениями (ICQ, mail-агент), скачанные с неизвестных web-сайтов.

12. При завершении работы в Системе и при длительных перерывах извлекать средство защищенного хранения данных eToken из компьютера, не оставлять его подключенным к компьютеру даже на короткое время без необходимости. Следует хранить средство защищенного хранения данных eToken в месте, исключающем несанкционированный доступ (в сейфе, запираемом шкафу).

13. Ограничить доступ к компьютеру посторонних лиц.

14. В случае использования смартфона для получения SMS сообщений от Банка не рекомендуется производить на нем операцию jailbreak (для ОС IOS) или получать root права (для ОС Android).

15. В случае использования смартфона для получения SMS сообщений от Банка не рекомендуется устанавливать приложения полученные не из доверенных магазинов приложений (например App Store, Google Play Market).

16. Не следует работать в Системе с компьютеров, по отношению к которым отсутствует уверенность, что принимаются необходимые меры обеспечения безопасности.

17. При ежедневной работе на компьютере не использовать права администратора. Следует установить пароли для входа пользователя и администратора в операционной системе. Рекомендуется использовать встроенный в операционную систему механизм контроля учетных записей (UAC) для защиты от несанкционированных действий.

18. Не использовать компьютер, предназначенный для работы в Системе, для развлечений и просмотра произвольных интернет-страниц (интернет-серфинга).

19. Рекомендуется вариант подключения к Системе с двумя подписями, в этом случае работу каждого Уполномоченного лица следует выполнять с отдельного компьютера.

20. При обнаружении подозрительной активности на компьютере (например, самопроизвольное движение курсора) следует немедленно извлечь средство защищенного хранения данных eToken. Если есть возможность, необходимо авторизоваться в Системе с другого компьютера и убедиться в отсутствии несанкционированных операций.

21. При обнаружении несанкционированных операций в Системе следует незамедлительно связаться с Банком по телефону или любым другим способом. Оперативное обращение в Банк может предотвратить несанкционированное списание средств, либо приостановить его, снизив финансовые потери.

22. При утрате средства защищенного хранения данных eToken, компрометации ключа электронной подписи, увольнении уполномоченных лиц необходимо незамедлительно связаться с Банком по телефону или любым другим способом и направить в Банк уведомление о компрометации ключа электронной подписи.

Банк никогда не осуществляет рассылку электронных писем с просьбой предоставить конфиденциальную информацию, а также содержащих компьютерные программы.

Если Вы получили письмо от имени Банка, содержание которого вызывает подозрение, либо с Вами связались по телефону от имени Банка, с просьбой установить какое-либо программное обеспечение или сообщить какие-либо коды из SMS-сообщений, просьба связаться со службой поддержки Банка и уточнить ситуацию. Всегда используйте контактную информацию служб поддержки Банка, указанную в официальных источниках информации, и не используйте контактную информацию, указанную в письме или полученную в ходе телефонного разговора.

Напоминаем, что основными способами электронного взаимодействия Банка и Клиентов являются штатные возможности и информационные каналы, предоставляемые Системой. Любые электронные сообщения, отправленные с бесплатных почтовых служб Интернет (@mail.ru, @yandex.ru, @rambler.ru, @gmail.com, @yahoo.com и т.п.), не являются почтой, отправленной Банком.

Приложение № 12
к Правилам обслуживания клиентов в системе
дистанционного банковского обслуживания
«Интернет Клиент-Банк»

В Банк «Кузнецкий мост» АО

От _____
(должность)
_____
_____
_____
(полное наименование Клиента)
_____
_____
(Фамилия, имя, отчество)

Заявление

Во исполнение Договора о присоединении к Правилам обслуживания клиентов в системе дистанционного банковского обслуживания «Интернет Клиент-Банк» № _____ от _____
прошу:

☐ Подключить услугу IP-фильтрации в системе «Интернет Клиент-Банк»

☐ Изменить список адресов для IP-фильтрации в системе «Интернет Клиент-Банк»

☐ Отключить услугу IP-фильтрации в системе «Интернет Клиент-Банк»
(необходимо отметить требуемый пункт)

Актуальный список разрешенных IP-адресов (диапазонов IP-адресов), с которых разрешена работа в системе «Интернет Клиент-Банк»:
1. _____
2. _____
3. _____
4. _____

Я предупрежден о том, что подключение, внесение изменений в список IP-адресов (диапазонов IP-адресов) и отключение услуги IP-фильтрации производится только по письменному заявлению клиента.

_____ (_____)
(подпись) (расшифровка подписи)
"_____" _____ 20 ___ г.

М.П.

ПРИНЯТО:
Дата и время принятия заявления: _____

БАНК:
Уполномоченный сотрудник Банка

_____ Ф.И.О.
м.п.