

ПРАВИЛА
обслуживания банковских счетов, открытых в ПАО «МОСКОВСКИЙ КРЕДИТНЫЙ БАНК»,
с использованием электронной системы «Ваш Банк Онлайн» (версия 2)
(действуют с 15.03.2019)

1. ПРИМЕНЯЕМЫЕ В ПРАВИЛАХ ОСНОВНЫЕ ПОНЯТИЯ И УСЛОВНЫЕ
ОБОЗНАЧЕНИЯ

В Правилах используются следующие основные понятия и условные обозначения:

Администратор безопасности – ответственный сотрудник Банка, в функциональные обязанности и полномочия которого входит создание сертификата Клиента и Банка, а также управление (выдача, аннулирование, прекращение, приостановление и возобновление действия) сертификатами Клиента;

Банк – «МОСКОВСКИЙ КРЕДИТНЫЙ БАНК» (публичное акционерное общество) (генеральная лицензия № 1978 от 06 мая 2016 г.; место нахождения: 107045, г. Москва, Луков переулок, д. 2, стр. 1; почтовый адрес: 107045, г. Москва, Луков переулок, д. 2, стр. 1; ИНН 7734202860; КПП 770801001; ОГРН 1027739555282; БИК 044525659, к/с 30101810745250000659 в Главном управлении Центрального банка Российской Федерации по Центральному федеральному округу г. Москва; SWIFT: MCRB RU MM; тел.: (495) 777-48-88, факс: (495) 797-42-10);

банковский программный модуль – модуль Системы, который установлен и работает в Банке. Банковский программный модуль обеспечивает прием, расшифрование электронных сообщений, содержащих расчетные (платежные) и иные документы, проверку подлинности ЭП в электронном документе и обработку указанных документов, отправленных в Банк от имени Клиента с использованием Системы, а также обеспечивает подготовку и отправку Клиенту электронных сообщений, зашифрованных и подписанных ЭП Банка, в том числе выписок о движении денежных средств по счетам (по запросу Клиента), и информации об исполнении или неисполнении документов, полученных от Клиента, и причинах их неисполнения, а также ведет контрольные архивы принятых и не принятых к исполнению документов, используемые в том числе при разрешении претензий Клиента;

браузер – свободно распространяемое программное обеспечение для просмотра сайтов в сети Интернет;

владелец сертификата – Клиент, которому в соответствии с законодательством Российской Федерации выдан сертификат. Выдача сертификатов Банком, выполняющим функции удостоверяющего центра по созданию и выдаче сертификатов, осуществляется в порядке, установленном разделом 5 Правил;

Договор – договор на обслуживание счетов с использованием Системы на условиях и в порядке, определенных Правилами, заключаемый между Банком и Клиентом в соответствии с законодательством Российской Федерации;

Документы валютного контроля – заявление на постановку на учет / снятие с учета контракта (кредитного договора), информация о коде вида операции, заявление о внесении изменений в ведомость банковского контроля и справка о подтверждающих документах (последняя является формой учета и отчетности по валютным операциям резидентов), иные документы и информация, требование о представлении которых содержится в нормативном акте Банка России, устанавливающим порядок представления резидентами и нерезидентами уполномоченным банкам подтверждающих документов и информации при осуществлении валютных операций, единые формы учета и отчетности по валютным операциям, порядок и сроки их предоставления (далее – Порядок Банка России);

Запрос на сертификат – запрос на изготовление сертификата в формате электронного документа, который формируется (форма 2 Сборника) и направляется Уполномоченным лицом в Банк посредством использования функционала Личного кабинета на основании Заявки на Уполномоченное лицо. Запрос на сертификат содержит сведения о владельце сертификата согласно Заявке на Уполномоченное лицо и уникальный ключ проверки ЭП;

Заявка на дополнительные услуги – заявка Клиента на предоставление дополнительных услуг по установке, обслуживанию и эксплуатации Системы, составленная на бумажном носителе по форме 9 Сборника;

Заявка на Уполномоченное лицо – заявка-доверенность на предоставление Уполномоченному лицу сертификата и доступа к Системе, а также на предоставление полномочий по работе с Системой, составленная Клиентом на бумажном носителе или сформированная в Системе (при наличии такой опции в Системе) по форме 1 Сборника;

Инициализационный пароль – пароль, направляемый Банком на номер телефона согласно Заявке на Уполномоченное лицо в случаях, предусмотренных Правилами, подлежащий обязательной процедуре его смены Уполномоченным лицом для получения доступа к Личному кабинету / Системе (далее – пароль Уполномоченного лица). Смена инициализационного пароля на пароль Уполномоченного лица завершается успешно при положительном результате проверки Банком имени пользователя и инициализационного пароля, с использованием которых осуществляется запрос подключения ПЭВМ к Личному кабинету / Системе;

Клиент – юридическое лицо, иностранная структура без образования юридического лица, индивидуальный предприниматель или физическое лицо, занимающееся в установленном законодательством Российской Федерации порядке частной практикой, имеющее открытый (е) счет (а) в Банке;

ключ проверки ЭП – уникальная последовательность символов, однозначно связанная с ключом ЭП и предназначенная для проверки подлинности ЭП Банка / Клиента;

ключ ЭП – уникальная последовательность символов, предназначенная для создания ЭП Банком / Уполномоченным лицом Клиента;

ключевой носитель – материальный носитель ключевой информации, предназначенной для шифрования, расшифрования, создания ЭП (ключ ЭП), проверки подлинности ЭП (ключ проверки ЭП), а также другой информации, необходимой для работы СКЗИ. Вся информация, хранящаяся на ключевом носителе, является конфиденциальной;

Кодовое слово – слово или комбинация слов, состоящее (их) из комбинации букв и/или цифр, которое (ая) устанавливается Клиентом и фиксируется в Заявке на Уполномоченное лицо. Кодовое слово предназначается для идентификации данного Уполномоченного лица при его обращении в Контакт-центр;

компрометация – факт несанкционированного доступа к защищаемой информации или возникновение подозрения на осуществление такого доступа. К событиям, связанным с компрометацией ключа ЭП / логина, пароля для доступа к Личному кабинету / Системе, в результате которых указанная информация может стать известной или доступной постороннему лицу, относятся следующие:

- утрата ключевого носителя и/или ключа ЭП, в том числе с последующим их обнаружением;
- утрата логина и пароля / пароля для доступа к Личному кабинету / Системе;
- утрата пин-кода на USB-токен;
- доступ неуполномоченных лиц к ключевому носителю и/или ключу ЭП;
- доступ неуполномоченных лиц к логину и паролю / паролю для доступа к Личному кабинету / Системе;
- доступ неуполномоченных лиц к пин-коду на USB-токен;
- прекращение полномочий (в том числе в случае увольнения) Уполномоченного лица Клиента, имевшего доступ к ключу ЭП и логину, паролю для доступа к Личному кабинету / Системе;
- обнаружение вредоносных программ на ПЭВМ, используемой для работы в Личном кабинете / Системе;
- иные обстоятельства, в результате которых имеется возможность несанкционированного доступа к ключевому носителю и/или ключу ЭП / логину и паролю / паролю для доступа к Личному кабинету / Системе / пин-коду на USB-токен либо указанная информация может стать известной постороннему лицу;

Контакт-центр – служба Банка, осуществляющая техническую поддержку систем дистанционного банковского обслуживания Клиентов, номер телефона которой: (495) 797-42-34, адрес электронной почты: 03@mkb.ru. Режим работы Контакт-центра указан на сайте Банка;

лицензия на право использования прикладного программного обеспечения «КриптоПро CSP» – документ, удостоверяющий право Клиента на использование прикладного программного

обеспечения СКЗИ «КриптоПро CSP». Условия более поздней лицензии на прикладное программное обеспечение являются преимущественными по отношению к условиям более ранних лицензий и спецификаций на прикладное программное обеспечение;

Личный кабинет – web-страница Уполномоченного лица на сайте Банка, защищенная технологией парольной защиты и предназначенная для формирования ключей ЭП и ключей проверки ЭП Клиента, направления в Банк от имени Клиента Запроса на сертификат и Подтверждения о получении сертификата, получения от Банка сертификата, а также получения от Банка информации, указанной в п. 2.10 Правил, необходимой для использования Личного кабинета и работы Уполномоченного лица в Системе. Порядок использования Личного кабинета установлен разделом 5 Правил;

мобильное приложение «МКБ Бизнес» – программное приложение Системы, предназначенное для установки на мобильные устройства, посредством которого осуществляется дистанционное банковское обслуживание Клиента. Условия предоставления Клиенту доступа к мобильному приложению «МКБ Бизнес» и объем дистанционного банковского обслуживания счетов с его использованием определены Условиями;

мобильное устройство – мобильное устройство (мобильный телефон, смартфон, электронный планшет и т. п.), работающее под управлением операционной системы iOS / Android;

НКО «Инкахран» (АО) – небанковская кредитная организация «ИНКАХРАН» (акционерное общество) (ИНН 7750003904), являющаяся участником банковской группы, которой Банк оказывает информационные услуги на основании соответствующего договора;

операционный день – операционное время, в течение которого Банком совершаются банковские операции и осуществляется обслуживание Клиента в Системе в соответствии с Тарифами;

Операция – расходная операция по счету Клиента, осуществляемая Банком на основании расчетных (платежных) документов, поступивших посредством Системы;

Ответственное лицо – ответственный сотрудник Банка, имеющий право совершать от имени Банка как агента валютного контроля действия по валютному контролю, предусмотренные Порядком Банка России, в том числе подписывать Документы валютного контроля и заверять их на бумажном носителе оттиском печати Банка, используемой для целей валютного контроля;

Подтверждение о получении сертификата – подтверждение о получении сертификата в формате электронного документа, которое формируется (форма 3 Сборника) и направляется Уполномоченным лицом в Банк посредством использования функционала Личного кабинета на основании Заявки на Уполномоченное лицо. Подтверждение о получении сертификата содержит сведения о параметрах полученного сертификата, в том числе о его уникальном номере и владельце, а также уникальный ключ проверки ЭП;

Правила – настоящие Правила обслуживания банковских счетов, открытых в ПАО «МОСКОВСКИЙ КРЕДИТНЫЙ БАНК», с использованием электронной системы «Ваш Банк Онлайн» (версия 2);

Правила безопасного использования систем ДБО – Правила безопасного использования систем дистанционного банковского обслуживания и сервисов электронного документооборота, предоставляемых ПАО «МОСКОВСКИЙ КРЕДИТНЫЙ БАНК» клиентам – юридическим лицам, индивидуальным предпринимателям и физическим лицам, занимающимся в установленном законодательством Российской Федерации порядке частной практикой, в рамках соответствующих договоров (соглашений);

простая ЭП – ЭП, которая посредством использования кодов, паролей или иных средств подтверждает факт формирования ЭП определенным лицом;

ПЭВМ – персональная электронная вычислительная машина;

рабочее место Администратора безопасности – аппаратно-программный комплекс, установленный в Банке и предназначенный для выполнения Администратором безопасности своих обязанностей в рамках предоставленных ему полномочий по созданию сертификатов Клиента и Банка, а также по управлению (выдача, аннулирование, прекращение, приостановление и возобновление действия) сертификатами Клиента;

репозиторий – информационный ресурс, предназначенный в том числе для размещения, хранения и распространения с использованием сети Интернет программного обеспечения для мобильных устройств (AppStore / Google Play Market);

сайт Банка – официальный сайт Банка в сети Интернет по адресу: www.mkb.ru;

Сборник – сборник форм документов, предусмотренных Правилами обслуживания банковских счетов, открытых в ПАО «МОСКОВСКИЙ КРЕДИТНЫЙ БАНК», с использованием электронной системы «Ваш Банк Онлайн», являющийся неотъемлемой частью Правил (приложение 2 к Правилам);

сертификат (сертификат ключа проверки ЭП) – электронный документ или документ на бумажном носителе, выданный удостоверяющим центром либо доверенным лицом удостоверяющего центра и подтверждающий принадлежность ключа проверки ЭП владельцу сертификата;

Система – электронная система «Ваш Банк Онлайн», оператором которой является Банк, состоящая из банковского программного модуля, web-приложений, а также мобильного приложения «МКБ Бизнес», с использованием которой реализуются функции электронного документооборота и дистанционного банковского обслуживания Клиента. В состав указанного модуля и web-приложений входит блок криптографической защиты, с помощью которого реализуются процедуры создания ЭП, проверки подлинности ЭП;

СКЗИ – средство криптографической защиты информации, при использовании которого в результате криптографического преобразования информации реализуются следующие функции: создание ЭП, проверка ЭП, создание ключа ЭП и ключа проверки ЭП;

Стороны – Банк и Клиент;

счет – открытый Клиенту в Банке банковский счет, не имеющий особого правового режима, Операции по которому могут совершаться без согласия лица, уполномоченного давать согласие на списание денежных средств со счетов Клиента в случаях, предусмотренных законом и нормативными актами Российской Федерации (в том числе специализированного депозитария, арбитражного управляющего) / договором банковского счета (особый правовой режим);

Тарифы – *тарифы для клиентов, не являющихся кредитными организациями*: Тарифы ПАО «МОСКОВСКИЙ КРЕДИТНЫЙ БАНК» на обслуживание счетов в российских рублях и иностранной валюте клиентов – юридических лиц и индивидуальных предпринимателей – резидентов и нерезидентов Российской Федерации, а также счетов платежных агентов и банковских платежных агентов; *тарифы для клиентов, являющихся кредитными организациями*: Тарифы и условия обслуживания корреспондентских счетов кредитных организаций в валюте Российской Федерации в ПАО «МОСКОВСКИЙ КРЕДИТНЫЙ БАНК», Тарифы и условия обслуживания корреспондентских счетов банков в иностранной валюте в ПАО «МОСКОВСКИЙ КРЕДИТНЫЙ БАНК»;

Условия – Условия использования мобильного приложения «МКБ Бизнес» электронной системы «Ваш Банк Онлайн», содержащиеся в приложении 1 к Правилам, являющиеся неотъемлемой частью Правил;

Уполномоченное лицо – лицо, указанное в п. 2.5 Правил, уполномоченное осуществлять электронный документооборот и совершать иные действия от имени Клиента в Личном кабинете / Системе, в том числе формировать ключ ЭП и ключ проверки ЭП Клиента, направлять Банку Запрос на сертификат и Подтверждение о получении сертификата, получать сертификат, распоряжаться денежными средствами, имеющимися на счетах Клиента, и совершать сделки с Банком (в том числе заключать договоры банковского счета / депозита), используя аналог собственноручной подписи (подписывать ЭП расчетные (платежные) и иные документы от имени Клиента);

ЭП (электронная подпись) – информация в электронной форме, которая присоединена к расчетному (платежному) и иному документу, передаваемому с использованием Системы, и которая используется для определения лица, подписывающего информацию. В Системе, кроме мобильного приложения «МКБ Бизнес», используется усиленная неквалифицированная электронная подпись, если иное не установлено Правилами. Электронная подпись является аналогом собственноручной подписи;

ЭП Ответственного лица – простая ЭП, которая представляет собой уникальный идентификатор Ответственного лица;

IP-адрес – идентификационная информация, используемая для адресации в сети Интернет устройства, с использованием которого осуществляется доступ к Личному кабинету / Системе посредством web-приложений;

SMS-код – одноразовый код, представляющий собой уникальную последовательность цифровых символов, направляемую Банком Клиенту посредством передачи SMS-сообщения на согласованные между Банком и Клиентом номера телефонов в случаях, предусмотренных

Правилами, в том числе Условиями, который:

- действителен на протяжении ограниченного периода времени, установленного Банком;
- однозначно соответствует сеансу использования Личного кабинета / Системы и расчетному (платежному), иному документу, направляемому в Банк;

USB-токен – компактное USB-устройство, предназначенное для безопасного хранения в защищенной пин-кодом памяти ключей ЭП Клиента, соответствующее требованиям Банка согласно п. 2.23 Правил. USB-токен, содержащий ключи ЭП, является ключевым носителем, и к его хранению и использованию предъявляются требования, установленные для ключевого носителя Правилами и Правилами безопасного использования систем ДБО;

web-приложение – программное приложение, использующее для работы браузер. *Web-приложение, предоставляемое Клиенту*, – программный модуль Системы, позволяющий подготавливать и отправлять в Банк электронные сообщения, содержащие расчетные (платежные) и иные документы, подписанные ЭП Клиента; принимать электронные сообщения Банка, проверять подлинность ЭП и обрабатывать электронные сообщения / документы, отправленные Клиенту от имени Банка, а также управлять доступом Уполномоченных лиц к Системе (далее – основной функционал Системы).

2. ОБЩИЕ ПОЛОЖЕНИЯ

2.1. Правила определяют условия и порядок осуществления электронного документооборота, а также проведения банковских операций по счетам с использованием Системы в рамках Договора.

2.2. После вступления в силу Правил в случае оказания Банком Клиенту в рамках Договора (при наличии такового) дополнительных услуг данные услуги продолжают оказываться Банком в порядке и на условиях, определенных Правилами. Предоставление Клиентом заявок, а также иных документов, представленных в Банк ранее в рамках Договора для получения дополнительных услуг, не требуется.

2.3. Банк для ознакомления Клиентов с Правилами, в том числе с новыми редакциями Правил, публично размещает указанную выше информацию на сайте Банка.

В дополнение к указанному выше способу публичного размещения информации Банк вправе доводить эту информацию до сведения Клиентов, а также потенциальных Клиентов иными способами по усмотрению Банка.

2.4. В случае если любой из пунктов Правил содержит ссылку на юридическое лицо, то положения такого пункта применяются равным образом как к отношениям Сторон, возникающим в случае предоставления доступа к Системе Клиенту, являющемуся юридическим лицом, так и к отношениям, возникающим в случае предоставления доступа к Системе Клиенту, являющемуся иностранной структурой без образования юридического лица.

2.5. Уполномоченными лицами являются:

если Клиент является юридическим лицом – единоличный исполнительный орган Клиента, а также иные лица, уполномоченные совершать от имени Клиента действия посредством Системы, используя аналог собственноручной подписи;

если Клиент является индивидуальным предпринимателем, физическим лицом, занимающимся в установленном законодательством Российской Федерации порядке частной практикой, – Клиент, а также иные лица, уполномоченные совершать от имени Клиента действия посредством Системы, используя аналог собственноручной подписи.

Клиент наделяет указанных лиц полномочиями совершать действия в Личном кабинете / Системе от имени Клиента (формировать ключ ЭП и ключ проверки ЭП Клиента, направлять Банку Запрос на сертификат и Подтверждение о получении сертификата, получать сертификат, распоряжаться денежными средствами, имеющимися на счетах Клиента, совершать сделки с Банком (в том числе заключать договоры банковского счета / депозита), использовать Систему без права подписи документов в web-приложениях Системы, разграничивать права доступа Уполномоченных лиц Клиента к Системе и иное) в Заявке на уполномоченное лицо / распорядительном акте / доверенности / ином документе, предоставляемом в Банк в соответствии с Правилами.

2.6. Клиент с целью подключения Уполномоченного лица к Системе (основному функционалу Системы) предоставляет в Банк:

- Заявку на Уполномоченное лицо;

– сведения для идентификации Уполномоченного лица, наделенного правом совершать сделки с Банком и/или распоряжаться денежными средствами, находящимися на счетах Клиента (в случае предоставления такого права), согласно требованиям законодательства о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма, по установленным Банком формам вопросников.

В случае наделения Клиентом, являющимся индивидуальным предпринимателем или физическим лицом, занимающимся в установленном законодательством Российской Федерации порядке частной практикой, иного лица полномочиями совершать от имени Клиента действия посредством Системы с правом подписи документов Заявка на Уполномоченное лицо (содержащая положения доверенности) должна быть нотариально удостоверена.

Предоставляя Банку Заявку на Уполномоченное лицо, содержащую в том числе контактные данные Уполномоченного лица, используемые Банком для направления Уполномоченному лицу его учетных данных (логин, пароль) для доступа к Личному кабинету / Системе и иной информации в рамках использования Личного кабинета, Клиент подтверждает и гарантирует, что:

- указанные в данной заявке номер телефона и адрес электронной почты принадлежат данному Уполномоченному лицу;
- Уполномоченное лицо ознакомлено с порядком использования Личного кабинета, содержащимся в разделе 5 Правил;
- Уполномоченное лицо ознакомлено с Правилами безопасного использования систем ДБО, в том числе безопасного хранения ключей ЭП и учетных данных, используемых для доступа к Личному кабинету / Системе.

Клиент также подтверждает наличие оснований, предусмотренных Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», для передачи Банку персональных данных своих Уполномоченных лиц, а также подтверждает и гарантирует, что от Уполномоченных лиц получено необходимое согласие на обработку их персональных данных для осуществления прав и законных интересов Клиента в рамках Договора.

Клиент поручает Банку в целях исполнения Договора осуществлять обработку персональных данных своих Уполномоченных лиц с соблюдением принципов и правил их обработки, предусмотренных указанным в настоящем пункте законом.

Цель обработки Банком персональных данных Уполномоченных лиц – исполнение своих обязательств по Договору, и Банк не обязан получать согласие Уполномоченных лиц на обработку их персональных данных.

Согласие на обработку персональных данных Уполномоченных лиц действует в течение срока действия Договора. Указанное согласие может быть отозвано путем предоставления в Банк письменного заявления Клиента / Уполномоченного лица.

2.7. Для подписания расчетных (платежных) и иных документов от имени Клиента в Системе достаточно одной ЭП Уполномоченного лица Клиента, если Договором не установлено иное.

В случае если Клиент использует несколько ЭП для подписания расчетных (платежных) документов и иных документов в Системе (Клиент предоставил Банку несколько Заявок на Уполномоченное лицо, наделенное правом подписи), Стороны признают, что для подписания таких документов от имени Клиента в Системе используется одна любая ЭП Уполномоченного лица при условии соблюдения его полномочий по работе в Системе согласно п. 2.5 Правил.

2.8. Стороны признают, что передаваемые Клиентом в Банк с использованием web-приложений Системы расчетные (платежные) и иные документы, заверенные надлежащим образом ЭП Клиента, идентичны расчетным (платежным) и иным документам на бумажном носителе, подписанным уполномоченными от имени Клиента представителями и скрепленным оттиском печати (при наличии) Клиента.

Стороны признают, что передаваемые Клиентом в Банк с использованием мобильного приложения «МКБ Бизнес» расчетные (платежные) документы, заверенные надлежащим образом ЭП Клиента, идентичны расчетным (платежным) документам на бумажном носителе, подписанным Уполномоченным лицом Клиента, указанным в п. 9.1 Условий.

2.9. Для создания ЭП, проверки ЭП, создания ключа ЭП, ключа проверки ЭП и сертификата, используемых в web-приложениях Системы, Стороны используют прикладное программное обеспечение СКЗИ «КриптоПро CSP», сертифицированное ФСБ России.

2.10. Банк передает Клиенту установочный комплект, содержащий программное обеспечение

для Системы, в том числе дистрибутив прикладного программного обеспечения СКЗИ «КриптоПро CSP» (далее – программная часть Системы), серийный номер данного СКЗИ и лицензию на право его использования путем передачи серийного номера указанной лицензии, руководство по использованию указанного СКЗИ.

Указанная в настоящем пункте информация передается Клиенту в электронном виде путем ее передачи Уполномоченному лицу (по запросу) посредством Личного кабинета. Факт передачи Банком данной информации Клиенту фиксируется банковским программным модулем и отображается в Личном кабинете.

2.11. Банк передает Клиенту за счет Клиента согласно Тарифам USB-токен на основании Заявки на Уполномоченное лицо по акту приема-передачи, составленному Сторонами по форме 5 Сборника.

2.12. Формирование ключа ЭП и ключа проверки ЭП Клиента, используемых в web-приложениях Системы, осуществляется Уполномоченным лицом в Личном кабинете на автоматизированном рабочем месте Клиента.

Создание сертификата Клиента осуществляется в Банке на автоматизированном рабочем месте Администратора безопасности.

Порядок использования Личного кабинета и процедура получения Уполномоченным лицом сертификата установлены разделом 5 Правил.

2.13. Банк не позднее рабочего дня, следующего за днем принятия документов, указанных в п. 2.6 Правил, предоставляет Уполномоченному лицу доступ к Личному кабинету и направляет учетные данные (логин, инициализационный пароль) для доступа к Личному кабинету на его контактные данные, указанные в Заявке на Уполномоченное лицо.

В случае если в дату предоставления Банком Уполномоченному лицу доступа к Личному кабинету в рамках Договора данное лицо уже использует Личный кабинет в соответствии с Правилами, инициализационный пароль повторно Банком не направляется. В этом случае Банк направляет Уполномоченному лицу на адрес электронный почты, указанный в Заявке на Уполномоченное лицо, соответствующее уведомление.

Факт передачи Уполномоченному лицу учетных данных для доступа к Личному кабинету / указанного выше уведомления подтверждает принятие Банком Заявки на Уполномоченное лицо, а также возможность формирования ключа ЭП и получения сертификата в порядке, установленном разделом 5 Правил.

Банк не позднее рабочего дня, следующего за днем принятия Банком от данного Уполномоченного лица Подтверждения о получении сертификата, регистрирует Уполномоченное лицо в Системе и направляет учетные данные (логин, инициализационный пароль) для доступа к Системе на его контактные данные, указанные в Заявке на Уполномоченное лицо.

Факт принятия Банком Подтверждения о получении сертификата в порядке, установленном разделом 5 Правил, подтверждает возможность доступа данного Уполномоченного лица к Системе в соответствии с Заявкой на Уполномоченное лицо и использования в Системе ЭП, удостоверенной данным сертификатом.

SMS-сообщение, содержащее инициализационный пароль для доступа к Личному кабинету / Системе, передается Банком Уполномоченному лицу один раз. Вне зависимости от возможности передачи сообщений на номер телефона Уполномоченного лица (аппарат абонента выключен или находится вне зоны действия сети, оказание услуг связи абоненту приостановлено / отключено или имеются иные, не зависящие от Банка, причины) SMS-сообщение считается отправленным Уполномоченному лицу, что может быть подтверждено оператором связи.

Сообщение электронной почты, содержащее логин для доступа к Личному кабинету / Системе, передается Банком Уполномоченному лицу один раз. Вне зависимости от возможности передачи сообщений на адрес электронной почты, используемый Уполномоченным лицом (указанный в Заявке на Уполномоченное лицо адрес электронной почты не существует или имеются иные, не зависящие от Банка, причины), сообщение электронной почты считается отправленным Уполномоченному лицу, что может быть подтверждено почтовым сервером Банка.

2.14. Датой начала использования Системы является дата получения Банком от Клиента первого Подтверждения о получении сертификата согласно разделу 5 Правил, которая фиксируется в данном подтверждении, если иное не установлено Договором, в том числе Правилами, либо соглашением, являющимся неотъемлемой частью Договора.

В случае если в дату получения Банком указанного подтверждения Банку не уплачено комиссионное вознаграждение в рамках Договора согласно Тарифам (за подключение к Системе / подключение дополнительных услуг / предоставление USB-токена для хранения ключей ЭП / иное), доступ к Системе Клиенту не предоставляется до погашения задолженности перед Банком. В этом случае датой начала использования Системы является дата списания со счета комиссий в рамках Договора в полном объеме, которая отражается в выписке о движении средств по счету.

2.15. Уполномоченное лицо осуществляет запрос подключения ПЭВМ к Системе путем ввода имени пользователя и инициализационного пароля, направленных Банком на его контактные данные, указанные в Заявке на Уполномоченное лицо, либо путем ввода имени пользователя, полученного указанным способом, и пароля Уполномоченного лица, установленного в настройках Системы.

Банк предоставляет доступ к Системе только в случае положительного результата следующих процедур проверки:

- имени пользователя и пароля Уполномоченного лица;
- соответствия данных сертификата, предъявленного Банку в запросе на подключение ПЭВМ к Системе, данным действующего сертификата, зарегистрированного в Системе, в котором указано данное Уполномоченное лицо;
- подлинности ЭП Уполномоченного лица, удостоверенной сертификатом, которой подписан запрос на подключение ПЭВМ к Системе;
- наличия IP-адреса, с которого осуществляется доступ к web-приложениям Системы, в Перечне IP-адресов, предусмотренном пп. 2.19, 6.4.10 Правил.

Стороны признают сертификат действующим в рамках Системы при наличии в Банке подписанного Уполномоченным лицом в соответствии с Правилами Подтверждения о получении сертификата и при одновременном соблюдении следующих условий:

- указанный в сертификате срок его действия не истек;
- сертификат не аннулирован / не приостановил свое действие в связи с блокировкой доступа к Системе в соответствии с Правилами, по любому основанию;
- указанные в сертификате сведения о его владельце соответствуют сведениям, указанным в Заявке на Уполномоченное лицо.

В случае утраты Уполномоченным лицом пароля доступа к Системе Клиент вправе обратиться в Банк с целью его восстановления согласно п. 6.4.6 Правил.

Новый инициализационный пароль доступа Уполномоченного лица к Системе Банк направляет на номер телефона, указанный в Заявке на Уполномоченное лицо.

2.16. В случаях, предусмотренных Правилами, Банк в течение сеанса использования Клиентом Системы осуществляет дополнительную проверку сведений о Клиенте (далее – дополнительная аутентификация) в целях подтверждения Клиентом правомочности направления расчетных (платежных) документов, содержащих распоряжения о переводе денежных средств в валюте Российской Федерации, иных документов / внесения изменений в содержание ранее представленных Банку заявок, заявлений, иных документов.

Банк осуществляет дополнительную аутентификацию Клиента с использованием SMS-кода (одноразового кода аутентификации) при условии подключения Клиента к данному сервису в порядке, предусмотренном п. 2.17 Правил, в следующих случаях:

- при наличии у Банка сомнений в подлинности расчетного (платежного) документа, направляемого в Банк посредством Системы, когда Перечень получателей, предусмотренный пп. 2.18, 6.4.9 Правил, Клиентом не установлен;
- при совершении операций по переводу денежных средств в пользу получателей, не указанных Клиентом в Перечне получателей, установленном согласно пп. 2.18, 6.4.9 Правил;
- предусмотренных пп. 2.18, 6.4.8, 6.4.9 Правил, независимо от наличия / отсутствия установленного Клиентом Перечня получателей, предусмотренного пп. 2.18, 6.4.9 Правил.

2.16.1. Банк при совершении Клиентом в Системе действия «Отправить документ в Банк» и необходимости осуществления дополнительной аутентификации Клиента формирует в Системе соответствующий запрос.

2.16.2. Клиент при получении запроса, указанного в п. 2.16.1 Правил, формирует в Системе запрос на отправку Банком одноразового кода аутентификации.

При формировании Клиентом данного запроса Банк генерирует одноразовый код аутентификации и направляет посредством SMS-сообщения на номера телефонов, указанные

Клиентом в заявлении, предусмотренном пп. 2.17, 6.4.8 Правил.

2.16.3. SMS-сообщение, направляемое Банком Клиенту, содержит следующую информацию (написанную буквами латинского алфавита):

- наименование и ИНН Клиента;
- действие от имени Клиента с использованием Системы, правомочность которого необходимо подтвердить;
- номер и сумма расчетного (платежного) документа, наименование и маскированный номер счета получателя, в пользу которого будут переведены денежные средства по распоряжению Клиента о переводе денежных средств, содержащемуся в данном документе (указывается при иницировании платежа);
- одноразовый код аутентификации.

2.16.4. После получения SMS-сообщения, содержащего информацию, указанную в п. 2.16.3 Правил, Клиент обязан проверить правильность указанных в ней данных. В случае успешной проверки информации, а также согласия с осуществлением указанного в ней действия от имени Клиента с использованием Системы Клиент вводит одноразовый код аутентификации в соответствующем поле окна Системы, предназначенном для осуществления дополнительной аутентификации Клиента.

2.16.5. Стороны признают, что процедура дополнительной аутентификации Клиента осуществлена успешно и правомочность направления расчетных (платежных), иных документов / внесения изменений в содержание ранее представленных Банку заявок, заявлений, иных документов подтверждена Клиентом в случае соответствия одноразового кода аутентификации, введенного Клиентом в Системе согласно п. 2.16.4 Правил, одноразовому коду аутентификации, сгенерированному Банком на основании запроса Клиента согласно п. 2.16.2 Правил.

2.16.6. Банк направляет Клиенту SMS-сообщения, содержащие одноразовые коды аутентификации, одновременно по всем номерам телефонов, указанным Клиентом в заявлении, предусмотренном пп. 2.17, 6.4.8 Правил.

Клиент подтверждает и гарантирует, что номера телефонов, указанные в заявлении, предусмотренном пп. 2.17, 6.4.8 Правил, принадлежат лицам, уполномоченным Клиентом на получение информации, предусмотренной п. 2.16.3 Правил.

SMS-сообщение, содержащее одноразовый код аутентификации, передается Банком Клиенту один раз. Вне зависимости от возможности передачи сообщений на номер телефона Клиента (аппарат абонента выключен или находится вне зоны действия сети, оказание услуг связи абоненту приостановлено / отключено или имеются иные, не зависящие от Банка, причины) SMS-сообщение считается отправленным Клиенту, что может быть подтверждено оператором связи.

2.17. Клиент, не являющийся кредитной организацией, в случае необходимости осуществления Банком дополнительной аутентификации Клиента по SMS-коду в порядке, предусмотренном п. 2.16 Правил, предоставляет в Банк заявление (далее – Заявление о дополнительной аутентификации).

Заявление о дополнительной аутентификации может быть составлено на бумажном носителе либо с использованием Системы (при наличии такой опции в Системе) по форме 5 Сборника.

При этом Клиент должен по запросу Банка подтвердить Заявление о дополнительной аутентификации, направляемое с использованием Системы, путем ввода в Системе в соответствующее поле запроса требуемых Банком реквизитов:

если Клиент является юридическим лицом – реквизитов документа, удостоверяющего личность единоличного исполнительного органа Клиента;

если Клиент является индивидуальным предпринимателем, физическим лицом, занимающимся в установленном законодательством Российской Федерации порядке частной практикой, – реквизитов документа, удостоверяющего личность Клиента.

Банк исполняет Заявление о дополнительной аутентификации в течение 3 (Трех) рабочих дней, следующих за днем его получения, и направляет Клиенту посредством Системы соответствующее уведомление об исполнении с указанием даты, часов и минут по московскому времени, которые фиксируются Системой.

Под исполнением Заявления о дополнительной аутентификации понимается завершение Банком технических процедур, необходимых для изменения порядка работы с Системой согласно установленным Клиентом данным.

Стороны признают, что с даты, часов и минут по московскому времени, указанных в

направленном Клиенту посредством Системы уведомлении об исполнении Заявления о дополнительной аутентификации, Банк осуществляет передачу SMS-сообщений, содержащих одноразовые коды аутентификации, на указанные в данном заявлении номера телефонов.

2.18. Клиент, подключенный к сервису дополнительной аутентификации по SMS-коду согласно п. 2.17 Правил, вправе установить перечень возможных получателей денежных средств, в пользу которых переводы денежных средств осуществляются с использованием Системы на основании расчетных (платежных) документов, содержащих распоряжения о переводе денежных средств в валюте Российской Федерации, без проведения Банком дополнительной аутентификации Клиента (далее – Перечень получателей), несмотря на наличие данного сервиса.

Перечень получателей формируется и передается Клиентом в Банк с использованием Системы посредством подачи заявления по форме ба Сборника (далее – Заявление на установление Перечня получателей).

При направлении в Банк Заявления на установление Перечня получателей Банк осуществляет дополнительную аутентификацию Клиента в порядке, предусмотренном п. 2.16 Правил, и при положительном результате указанной процедуры исполняет данное заявление.

Банк направляет Клиенту посредством Системы соответствующее уведомление об исполнении Заявления на установление Перечня получателей с указанием даты, часов и минут по московскому времени, которые фиксируются Системой.

Под исполнением Заявления на установление Перечня получателей понимается завершение Банком технических процедур, необходимых для изменения порядка работы с Системой согласно установленным Клиентом данным.

Стороны признают, что с даты, часов и минут по московскому времени, указанных в направленном Клиенту посредством Системы уведомлении об исполнении Заявления на установление Перечня получателей, при направлении в Банк с использованием Системы расчетных (платежных) документов, содержащих распоряжения о переводе денежных средств в валюте Российской Федерации, от имени Клиента Банк:

- не осуществляет дополнительную аутентификацию Клиента в том случае, если ИНН и номер счета получателя средств, указанные в таких расчетных (платежных) документах, идентичны ИНН и номеру счета получателя, указанного в установленном Перечне получателей;

- осуществляет дополнительную аутентификацию Клиента в порядке, предусмотренном п. 2.16 Правил, при отсутствии получателя денежных средств в установленном Перечне получателей.

2.19. Клиент, подключенный к сервису дополнительной аутентификации по SMS-коду согласно п. 2.17 Правил, вправе установить перечень IP-адресов, с которых может осуществляться доступ к Системе посредством web-приложений и обмен расчетными (платежными), иными документами с Банком с использованием web-приложений Системы (далее – Перечень разрешенных IP-адресов).

Перечень разрешенных IP-адресов формируется и передается Клиентом в Банк с использованием Системы посредством подачи заявки по форме 7 Сборника (далее – Заявка на установление Перечня разрешенных IP-адресов).

При направлении в Банк Заявки на установление Перечня разрешенных IP-адресов Банк осуществляет дополнительную аутентификацию Клиента в порядке, предусмотренном п. 2.16 Правил, и при положительном результате указанной процедуры исполняет данную заявку.

После исполнения Заявки на установление Перечня разрешенных IP-адресов Банк направляет Клиенту посредством Системы соответствующее уведомление об исполнении с указанием даты, часов и минут по московскому времени, которые фиксируются Системой.

Под исполнением Заявки на установление Перечня разрешенных IP-адресов понимается завершение Банком технических процедур, необходимых для изменения порядка работы с Системой согласно установленным Клиентом данным.

Стороны признают, что с даты, часов и минут по московскому времени, указанных в направленном Клиенту посредством Системы уведомлении об установлении Перечня разрешенных IP-адресов на основании заявки, предусмотренной настоящим пунктом и п. 6.4.10 Правил, доступ к Системе посредством web-приложений и обмен расчетными (платежными), иными документами с Банком с использованием web-приложений Системы могут осуществляться только с IP-адресов, содержащихся в установленном Перечне разрешенных IP-адресов.

2.20. Банк информирует Клиента о совершении каждой Операции с использованием Системы в порядке, предусмотренном п. 6.1.6 Правил.

Клиент, не являющийся кредитной организацией, использующий Систему в рамках Договора на обслуживание счетов без особого правового режима, в случае необходимости информирования Клиента посредством SMS-сообщений о результатах обработки Банком платежных поручений, содержащих распоряжения о переводе денежных средств в валюте Российской Федерации по расчетным счетам Клиента, полученных Банком с использованием Системы (услуга «SMS-информирование по расчетному счету»), предоставляет в Банк заявку, составленную на бумажном носителе либо сформированную и направленную с использованием Системы, по форме 8 Сборника (далее – Заявка на SMS-информирование) с указанием параметра информирования «Списание при расчетах платежными поручениями». В этом случае Банк информирует Клиента об отражении списания денежных средств со счета в плановой выписке по счету после присвоения в Системе платежному поручению статуса «Принят Банком к рассмотрению», а также информирует в случае присвоения платежным поручениям в Системе статусов «Отложен для исполнения», «Отказан», «Картотека», «Недостаточно средств на счете».

В Заявке на SMS-информирование Клиент вправе указать дополнительные параметры информирования об операциях по указанным выше счетам Клиента и/или остатках денежных средств, находящихся на них на начало операционного дня.

После исполнения Заявки на SMS-информирование Банк направляет Клиенту посредством Системы соответствующее уведомление об исполнении с указанием даты, часов и минут по московскому времени, которые фиксируются Системой, а также направляет на указанные в данной заявке номера телефонов SMS-сообщение, содержащее уведомление о подключении SMS-информирования в отношении данных номеров телефонов.

Под исполнением Заявки на SMS-информирование понимается завершение Банком технических процедур, необходимых для осуществления информирования Клиента согласно установленным Клиентом данным.

Стороны признают, что с даты, часов и минут по московскому времени, указанных в направленном Банком посредством Системы уведомлении об исполнении Заявки на SMS-информирование, Банк осуществляет передачу Клиенту SMS-сообщений, содержащих информацию о расчетных счетах Клиента согласно указанным Клиентом в данной заявке параметрам информирования.

Клиент подтверждает и гарантирует, что номера телефонов, указанные им в Заявке на SMS-информирование, предусмотренной настоящим пунктом и п. 6.4.11 Правил, принадлежат лицам, уполномоченным Клиентом на получение информации о расчетных счетах Клиента.

Клиент информирован о том, что предоставление Банком услуги «SMS-информирование по расчетному счету» может повлечь разглашение банковской тайны, и принимает на себя риск такого разглашения.

SMS-сообщения, содержащие уведомление о подключении услуги «SMS-информирование по расчетному счету» и информацию о расчетных счетах Клиента, передаются Банком Клиенту один раз. Вне зависимости от возможности передачи сообщений на номер телефона Клиента (аппарат абонента выключен или находится вне зоны действия сети, оказание услуг связи абоненту приостановлено / отключено или имеются иные, не зависящие от Банка, причины) SMS-сообщение считается отправленным Клиенту, что может быть подтверждено оператором связи.

2.21. Банк гарантирует работоспособность программного обеспечения Системы при неукоснительном исполнении Клиентом требований, описанных в документации по использованию Системы. Указанные гарантийные обязательства распространяются на весь срок действия Договора. В состав гарантийных обязательств включаются обязательства по обновлению программного обеспечения Системы, а также устранению недостатков, выявленных в процессе использования Системы.

2.22. Банк до заключения Договора предоставляет Клиенту информацию об условиях безопасного использования Системы, в частности, о любых ограничениях способов и мест использования, случаях повышенного риска использования Системы путем ознакомления Клиента с Правилами безопасного использования систем ДБО, размещенными на сайте Банка и являющимися неотъемлемой частью Правил.

2.23. Требования к оборудованию и программному обеспечению, необходимым для работы ПЭВМ Клиента с Системой, размещены на сайте Банка и являются неотъемлемой частью Правил (далее – Требования).

2.24. Перечень услуг, которые могут быть предоставлены Клиенту с использованием

Системы, доступен Клиенту при установлении связи с Системой.

2.25. Предусмотренные Правилами заявки и заявления Клиента, составленные на бумажном носителе, подписанные уполномоченным представителем и заверенные печатью (при наличии) Клиента, предоставляются в дополнительный офис Банка, в котором обслуживается счет. Указанные документы предоставляются уполномоченным представителем Клиента, чьи полномочия подтверждены Банку путем предоставления соответствующих документов. В случае если документом, подтверждающим полномочия, является доверенность, Стороны признают, что указанная доверенность должна быть заверена печатью Клиента (при наличии печати).

2.26. В случае если Правилами предусмотрено предоставление Клиентом заявок / заявлений посредством Системы, указанные документы формируются в Системе в электронной форме и подписываются ЭП Клиента.

2.27. В случае блокировки Системы в соответствии с пп. 6.2.10–6.2.13, 6.4.3 Правил проведение операций по счету возможно на основании надлежащим образом оформленных распоряжений / расчетных документов на бумажном носителе, и обслуживание Клиента осуществляется согласно Тарифам за ведение счета без использования Системы.

2.28. В качестве единого учетно-отчетного времени при работе с Личным кабинетом / Системой Стороны признают московское время. Контрольным временем является время системных часов аппаратных средств Банка. Записи в электронных журналах Системы относительно действий, совершаемых от имени Клиента, имеют доказательственную силу при рассмотрении спорных ситуаций.

3. ПРОЦЕДУРА ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА

3.1. Подлинность документов, переданных с использованием Системы, и правомочность осуществления Банком Операций обеспечиваются применением ЭП и шифрования передаваемой информации.

3.2. Стороны признают, что алгоритм усиленной неквалифицированной ЭП, применяемый в Системе, позволяет обнаружить любые изменения, внесенные в текст расчетного (платежного) или иного документа, подписанного ЭП, и обеспечивает невозможность подделки ЭП без наличия ключа ЭП и / или доступа к нему.

3.3. В течение операционного дня Банк совершает Операции без ограничения по сумме перевода денежных средств в пользу любых получателей денежных средств на основании расчетных (платежных) документов Клиента, направленных посредством Системы с любых устройств, соответствующих Требованиям Банка, если иное не установлено Договором, в том числе Правилами.

3.4. Расчетный (платежный) документ, направляемый в Банк с использованием Системы, кроме мобильного приложения «МКБ Бизнес», принимается Банком только при соблюдении следующих условий:

- документ оформлен в соответствии с установленной формой;
- документ подписан ЭП Клиента;
- все указанные в документе реквизиты являются верными;
- соблюдены условия, предусмотренные п. 2.16.5 Правил;
- соблюдены иные условия, предусмотренные Договором.

Расчетный (платежный) документ, направляемый в Банк с использованием мобильного приложения «МКБ Бизнес», принимается Банком только при соблюдении условий, предусмотренных п. 9.8 Условий.

В случае, предусмотренном п. 6.1.10 Правил, Банк приостанавливает исполнение расчетного (платежного) документа Клиента в порядке, предусмотренном указанным пунктом Правил.

В случае отрицательного результата проверки Банком поступившего расчетного (платежного) или иного документа Банк отказывает в его приеме, о чем уведомляет Клиента путем направления соответствующего сообщения с использованием Системы с указанием причин отказа в принятии (исполнении) такого документа и/или путем присвоения такому документу соответствующего статуса в Системе, который свидетельствует о том, что данный документ Банком не принимается, а также путем направления соответствующего SMS-сообщения в случае, предусмотренном п. 2.20 Правил.

3.5. При наличии ограничений прав Клиента на распоряжение денежными средствами, находящимися на счетах, исполнение расчетных (платежных) документов осуществляется в порядке,

в том числе в очередности, предусмотренном (й) действующим законодательством Российской Федерации.

3.6. В случае если условиями договора между Клиентом и НКО «Инкахран» (при наличии такового) предусмотрен обмен документами с использованием Системы, Банк предоставляет Клиенту возможность направить в НКО «Инкахран» через Банк с использованием Системы указанные документы по согласованным между Банком и НКО «Инкахран» формам (далее – транзитный документ).

Стороны признают, что лицом, уполномоченным направлять в Банк с использованием Системы транзитные документы от имени Клиента для их передачи Банком в НКО «Инкахран», является указанное в п. 2.5 Правил Уполномоченное лицо, наделенное правом совершать сделки с Банком (в случае предоставления такого права).

Транзитный документ, направляемый в Банк с использованием Системы, принимается Банком только при соблюдении следующих условий:

- документ сформирован с использованием Системы;
- документ подписан ЭП Уполномоченного лица, наделенного правом совершать сделки с Банком;

- соблюдены условия, предусмотренные п. 2.16.5 Правил;

- соблюдены иные условия, предусмотренные Договором.

В случае положительного результата проверки поступившего документа Банк направляет в НКО «Инкахран» сообщение, содержащее данный документ, подписанный ЭП Банка, с использованием защищенного телекоммуникационного канала связи в рамках интеграции банковского программного модуля и программного модуля, установленного и работающего в НКО «Инкахран», в предусмотренном соответствующим договором между Банком и НКО «Инкахран» порядке.

В случае положительного результата доставки в НКО «Инкахран» сообщения, содержащего транзитный документ, Банк информирует Клиента об этом путем присвоения данному документу в Системе статуса «Принят Банком к рассмотрению».

Банк информирует Клиента о положительном / отрицательном результате обработки принятого НКО «Инкахран» транзитного документа посредством присвоения в Системе данному документу соответствующего статуса: «в Архиве» / «Исполнен» / «Отказан», датой присвоения которого является дата, указанная в последнем событии по данному документу, отражаемом в Системе.

Банк обязуется обеспечить неизменность и целостность транзитного документа с момента его подписания ЭП Клиента до момента доставки в НКО «Инкахран» в соответствии с настоящим пунктом.

Банк не контролирует и не несет ответственности за содержание транзитных документов, а также не осуществляет контроль полномочий лица, подписавшего ЭП транзитный документ, чьи полномочия подтверждены Клиентом НКО «Инкахран» путем предоставления соответствующих документов (распорядительного акта / доверенности / иного). Ответственность Банка за использование ключей ЭП Клиента неуполномоченными лицами исключается и все возникающие в связи с этим риски Клиент несет самостоятельно.

3.7. Оригиналы расчетных (платежных) или иных документов на бумажных носителях, заверенные подписями уполномоченных представителей и оттиском печати Стороны (при наличии печати), предоставляются только по запросу одной из Сторон в течение 5 (Пяти) рабочих дней с момента поступления такого запроса.

3.8. Банковский программный модуль функционирует круглосуточно, за исключением остановок на техническое обслуживание.

3.9. В банковском программном модуле ведутся контрольные архивы принятых и не принятых к исполнению документов, которые в соответствии с разделом 7 Правил используются при разрешении споров и конфликтных ситуаций, связанных с передачей данных и исполнением распоряжений Клиента, направленных с использованием Системы.

4. ОБМЕН ДОКУМЕНТАМИ И ИНФОРМАЦИЕЙ, СВЯЗАННЫМИ С ПРОВЕДЕНИЕМ ВАЛЮТНЫХ ОПЕРАЦИЙ

4.1. Клиент предоставляет в Банк с использованием Системы Документы валютного контроля

– как сформированные в электронном виде (при наличии такой опции в Системе), так и полученные с использованием сканирующих устройств изображения Документов валютного контроля, оформленных первоначально на бумажном носителе.

4.2. Документы валютного контроля, представляемые Клиентом для обоснования проводимой валютной операции, должны соответствовать следующим требованиям:

- документы должны быть действительными на день их представления в Банк;
- документы, исполненные полностью или в какой-либо их части на иностранном языке, представляются Клиентом в Банк с надлежащим образом заверенным переводом на русский язык;
- документы, исходящие от государственных органов иностранных государств, подтверждающие статус юридических лиц – нерезидентов, должны быть легализованы в установленном законодательством Российской Федерации порядке. Иностранные официальные документы могут быть представлены без их легализации в случаях, предусмотренных международным договором Российской Федерации.

4.3. При предоставлении Документов валютного контроля в виде полученных с использованием сканирующих устройств изображений документов, оформленных первоначально на бумажном носителе, Клиент обеспечивает их отправку в сопровождении текстового сообщения, сформированного в Системе в свободном формате и содержащего сведения о наименовании и реквизитах вложенных документов, а также наименования, номера и даты документа, к которому прилагаются указанные документы.

4.4. Документы валютного контроля, направляемые Клиентом в Банк посредством Системы в электронном виде, подписываются ЭП Клиента.

4.5. Документы валютного контроля, направляемые Клиентом с использованием Системы, подписанные ЭП Клиента, признаются Сторонами равнозначными Документам валютного контроля, составленным на бумажном носителе, подписанным уполномоченным представителем и заверенным печатью Клиента (при наличии у Клиента печати).

4.6. Датой представления Клиентом Документов валютного контроля с использованием Системы является дата их получения Банком, зафиксированная Системой. В случае получения Банком Документов валютного контроля после окончания операционного дня, продолжительность которого устанавливается Банком, датой представления Клиентом в Банк указанных документов считается операционный день, следующий за днем направления Клиентом указанных документов.

4.7. При положительном результате проверки Документов валютного контроля (заявления на постановку на учет / снятие с учета контракта (кредитного договора) и/или заявления о внесении изменений в ведомость банковского контроля, и/или информации о коде вида операции, и/или справки о подтверждающих документах), полученных Банком посредством Системы, Ответственное лицо присваивает указанному электронному документу статус «Валютный контроль пройден». Дата присвоения Ответственным лицом Документу валютного контроля указанного статуса является датой принятия данного документа Банком.

После присвоения Ответственным лицом Документу валютного контроля (заявлению на постановку на учет / снятие с учета контракта (кредитного договора) и/или заявлению о внесении изменений в ведомость банковского контроля, и/или информации о коде вида операции, и/или справке о подтверждающих документах) статуса «Валютный контроль пройден» указанный документ возвращается Клиенту посредством Системы с добавлением информации о принятии Документа валютного контроля, дате получения Документа валютного контроля и дате его принятия Банком. При этом в заявлении на постановку на учет контракта (кредитного договора) проставляется уникальный номер контракта (кредитного договора).

4.8. При отрицательном результате проверки Документов валютного контроля (заявления на постановку на учет / снятие с учета контракта (кредитного договора) и/или заявления о внесении изменений в ведомость банковского контроля, и/или информации о коде вида операции, и/или справки о подтверждающих документах), полученных Банком посредством Системы, Ответственное лицо присваивает указанному электронному документу статус «Отказ валютного контроля». Дата присвоения Ответственным лицом Документу валютного контроля указанного статуса является датой отказа Банка в принятии данного документа.

После присвоения Ответственным лицом Документу валютного контроля (заявлению на постановку на учет / снятие с учета контракта (кредитного договора) и/или заявлению о внесении изменений в ведомость банковского контроля, и/или информации о коде вида операции, и/или справке

о подтверждающих документах) статуса «Отказ валютного контроля» указанный документ возвращается Клиенту посредством Системы с добавлением информации о непринятии Документа валютного контроля, дате получения Документа валютного контроля, дате и причине отказа в его принятии Банком.

4.9. Документы валютного контроля, направляемые Банком Клиенту в электронном виде посредством Системы, подписываются ЭП Ответственного лица.

Стороны признают, что передаваемые с использованием Системы Документы валютного контроля, заверенные надлежащим образом ЭП Ответственного лица и ЭП Банка, идентичны Документам валютного контроля на бумажном носителе, подписанным Ответственным лицом и заверенным оттиском печати Банка, используемой для целей валютного контроля.

4.10. В случае отказа Банка в принятии Документов валютного контроля в соответствии с п. 4.8 Правил Банк не принимает к исполнению расчетный (платежный) документ по валютной операции, для осуществления которой Клиентом были представлены указанные Документы валютного контроля.

В случае когда Банк не принимает к исполнению расчетный (платежный) документ по валютной операции, Банк отказывает Клиенту в принятии Документов валютного контроля, предназначенных для осуществления валютной операции в соответствии с указанным расчетным документом.

4.11. Предоставление Банком Клиенту Документов валютного контроля на бумажном носителе, представленных Клиентом в электронном виде посредством Системы, осуществляется по письменному запросу Клиента и оплачивается Клиентом согласно Тарифам.

5. ИСПОЛЬЗОВАНИЕ ЛИЧНОГО КАБИНЕТА И ПРОЦЕДУРА ПОЛУЧЕНИЯ УПОЛНОМОЧЕННЫМ ЛИЦОМ СЕРТИФИКАТА

5.1. Банк для ознакомления Клиентов / Уполномоченных лиц с руководством по использованию Личного кабинета (далее – Руководство по ЛК) публично размещает указанную выше информацию на сайте Банка, а также в Личном кабинете.

5.2. Уполномоченное лицо осуществляет запрос подключения ПЭВМ к Личному кабинету путем ввода имени пользователя и инициализационного пароля, направленных Банком на его контактные данные согласно Заявке на Уполномоченное лицо, либо путем ввода имени пользователя, полученного указанным способом, и пароля, установленного в настройках Личного кабинета.

Банк предоставляет доступ к Личному кабинету только в случае положительного результата проверки имени пользователя и пароля Уполномоченного лица.

В случае утраты Уполномоченным лицом пароля доступа к Личному кабинету данное лицо вправе обратиться в Контакт-центр с целью его восстановления.

Новый инициализационный пароль доступа к Личному кабинету Банк направляет на номер телефона, указанный в Заявке на Уполномоченное лицо.

5.3. Уполномоченное лицо посредством Личного кабинета получает от Банка программную часть Системы (по запросу), осуществляет формирование ключа ЭП, ключа проверки ЭП и направляет Банку Запрос на сертификат в порядке, установленном пп. 5.7–5.10 Правил.

При этом Клиент обязан обеспечить:

- смену стандартного пароля администратора и пользователя USB-токена на пароль, известный только Уполномоченному лицу;
- сохранение ключа ЭП исключительно на USB-токене.

Стороны признают, что Банком получено подтверждение того, что Уполномоченное лицо, обратившееся за получением сертификата от имени Клиента, владеет ключом ЭП, который соответствует ключу проверки ЭП, указанному таким лицом в Запросе на сертификат, при положительном результате процедур проверки, указанных в п. 5.12 Правил, осуществляемых Банком.

5.4. Банк создает в электронном виде сертификат согласно данному запросу и Заявке на Уполномоченное лицо, информирует Уполномоченное лицо о его готовности путем отображения соответствующей информации в Личном кабинете, а также обеспечивает возможность его получения Уполномоченным лицом в Личном кабинете не позднее рабочего дня, следующего за днем принятия Банком указанного запроса согласно п. 5.12 Правил, при условии установления личности и полномочий получателя сертификата согласно Заявке на Уполномоченное лицо.

5.5. После получения сертификата Уполномоченное лицо обязано проверить правильность

указанных в нем данных.

В случае успешной проверки информации факт получения Уполномоченным лицом сертификата отражается в Подтверждении о получении сертификата, направляемом Банку в порядке, установленном пп. 5.7–5.10 Правил.

5.6. Банк не позднее рабочего дня, следующего за днем принятия данного Подтверждения о получении сертификата согласно п. 5.12 Правил, обеспечивает возможность использования Уполномоченным лицом в Системе ЭП, удостоверенной сертификатом, параметры которого указаны в данном подтверждении.

5.7. Для подписания и отправки в Банк Запроса на сертификат / Подтверждения о получении сертификата Уполномоченное лицо совершает в Личном кабинете действие «Подписать и отправить» и формирует запрос на отправку Банком SMS-кода.

При формировании Уполномоченным лицом запроса на отправку Банком SMS-кода Банк генерирует одноразовый код и направляет посредством SMS-сообщения на номер телефона, используемый данным лицом согласно Заявке на Уполномоченное лицо.

5.8. SMS-сообщение, содержащее одноразовый код, направляется Банком один раз. Вне зависимости от возможности передачи SMS-сообщений на номер телефона, используемый Уполномоченным лицом (аппарат абонента выключен или находится вне зоны действия сети, оказание услуг связи абоненту приостановлено / отключено или имеются иные, не зависящие от Банка, причины), SMS-сообщение считается отправленным Уполномоченному лицу, что может быть подтверждено оператором связи.

5.9. SMS-сообщение, направляемое Банком Уполномоченному лицу, содержит следующую информацию (написанную буквами латинского алфавита):

- наименование документа (Запрос на сертификат / Подтверждение о получении сертификата);
- наименование и ИНН / КИО Клиента;
- одноразовый код.

5.10. После получения SMS-сообщения, содержащего информацию, указанную в п. 5.9 Правил, Уполномоченное лицо обязано проверить правильность указанных в ней данных.

В случае успешной проверки информации Уполномоченное лицо вводит SMS-код в соответствующее поле Личного кабинета, подтверждая факт формирования ЭП данным Уполномоченным лицом.

5.11. Уполномоченное лицо, подписавшее Запрос на сертификат / Подтверждение о получении сертификата простой ЭП, считается определенным при одновременном соблюдении следующих условий:

- установлен факт доступа к Личному кабинету при положительном результате процедуры проверки имени пользователя и пароля, используемых данным Уполномоченным лицом, согласно п. 5.2 Правил;
- установлен факт регистрации IP-адреса, с которого предоставлен доступ к Личному кабинету согласно п. 5.2 Правил;
- установлен факт направления запроса на отправку Банком SMS-кода с IP-адреса, зарегистрированного при предоставлении доступа к Личному кабинету согласно п. 5.2 Правил;
- установлен факт направления Банком SMS-кода на номер телефона, принадлежащий данному Уполномоченному лицу согласно Заявке на Уполномоченное лицо;
- установлен факт ввода SMS-кода с использованием IP-адреса, зарегистрированного при предоставлении доступа к Личному кабинету согласно п. 5.2 Правил;
- установлен факт, что SMS-код, введенный с использованием IP-адреса, зарегистрированного при предоставлении доступа к Личному кабинету согласно п. 5.2 Правил, идентичен одноразовому коду, сгенерированному Банком согласно п. 5.7 Правил.

5.12. Запрос на сертификат / Подтверждение о получении сертификата принимается Банком только при соблюдении следующих условий:

- документ оформлен по форме Банка;
- сведения о владельце сертификата, содержащиеся в Запросе на сертификат, идентичны сведениям о владельце сертификата, содержащимся в Заявке на уполномоченное лицо;
- сведения о владельце сертификата и ключ проверки ЭП, содержащиеся в Подтверждении о получении сертификата, идентичны сведениям, содержащимся в данном сертификате;

- полномочия Уполномоченного лица, направившего в Банк документ, подтверждены Банку согласно п. 2.5 Правил, и Банк не располагает сведениями об их прекращении;
- соблюдены условия, предусмотренные п. 5.11 Правил.

Стороны признают, что такой документ, переданный Уполномоченным лицом в Банк с использованием Личного кабинета, равнозначен документу на бумажном носителе, подписанному Уполномоченным лицом.

В случае отрицательного результата проверки Банком поступившего документа Банк отказывает в его приеме, о чем уведомляет Уполномоченное лицо путем отображения в Личном кабинете соответствующей информации, которая свидетельствует о том, что данный документ Банком не принимается.

5.13. Стороны признают, что используемый для передачи Запроса на сертификат и Подтверждения о получении сертификата, подписанных простой ЭП, протокол https является достаточным для надежной защиты передаваемых сообщений от модификации.

Стороны признают, что пароль Уполномоченного лица для доступа в Личный кабинет является ключом простой ЭП, используемой для подписания Запроса на сертификат и Подтверждения о получении сертификата, известным только Уполномоченному лицу.

Стороны признают, что простая ЭП признается корректной при одновременном соблюдении следующих условий:

- Уполномоченное лицо успешно аутентифицировалось в Личном кабинете с использованием инициализационного пароля, направляемого посредством SMS-сообщения, и пароля Уполномоченного лица;

- дальнейшая передача подписанных простой ЭП Запроса на сертификат и Подтверждения о получении сертификата осуществлялась в рамках установленной сессии аутентифицировавшегося в Личном кабинете Уполномоченного лица;

- соблюдены условия, предусмотренные п. 5.11 Правил.

5.14. Банк не менее чем за 30 (Тридцать) календарных дней до окончания срока действия сертификата, указанного в сертификате, обеспечивает возможность Уполномоченному лицу осуществить формирование ключа ЭП, ключа проверки ЭП и получить новый сертификат в порядке, установленном настоящим разделом Правил (далее – плановая смена ключей).

Уполномоченное лицо до окончания срока действия сертификата осуществляет формирование ключа ЭП, ключа проверки ЭП и направляет Банку Запрос на сертификат, получает от Банка новый сертификат и направляет Банку Подтверждение о получении сертификата в порядке, установленном настоящим разделом Правил.

Банк не позднее рабочего дня, следующего за днем принятия Подтверждения о получении сертификата, согласно п. 5.12 Правил обеспечивает возможность использования Уполномоченным лицом в Системе ЭП, удостоверенной новым сертификатом. Одновременно прекращается использование Уполномоченным лицом в Системе ЭП, удостоверенной ранее выданным ему сертификатом.

5.15. В случае истечения срока действия сертификата, при невыполнении Уполномоченным лицом действий, предусмотренных п. 5.14 Правил / прекращении действия сертификата в случаях, предусмотренных Правилами, доступ к Системе данного лица будет заблокирован.

В этом случае Клиент для получения возможности формирования нового ключа ЭП и ключа проверки ЭП, получения сертификата и продолжения работы данного Уполномоченного лица с Системой предоставляет в Банк Заявку на дополнительные услуги (далее – внеплановая смена ключей).

В этом случае Банк обеспечивает возможность:

- формирования Уполномоченным лицом нового ключа ЭП и ключа проверки ЭП, а также получения нового сертификата в порядке, установленном настоящим разделом Правил, не позднее рабочего дня, следующего за днем получения указанной в настоящем пункте заявки;

- доступа к Системе и использования Уполномоченным лицом ЭП, удостоверенной новым сертификатом, не позднее рабочего дня, следующего за днем принятия Подтверждения о получении сертификата согласно п. 5.12 Правил.

6. ПРАВА И ОБЯЗАННОСТИ СТОРОН

6.1. Банк обязан:

6.1.1. Предоставить Клиенту в пользование программные средства и СКЗИ, необходимые для работы Системы на ПЭВМ Клиента. Предоставить документацию по использованию Личного кабинета / Системы.

6.1.2. Обеспечивать возможность формирования и использования в Системе Уполномоченным лицом Клиента ключей ЭП согласно Заявке на Уполномоченное лицо.

6.1.3. Обеспечивать соблюдение в Банке порядка обращения с ключевой информацией, необходимой для работы Системы, исключающего несанкционированный доступ к ней посторонних лиц.

6.1.4. Обеспечивать за счет Клиента возможность смены ключей ЭП, используемых Уполномоченными лицами Клиента, в период, отличный от указанного в п. 5.14 Правил, на основании Заявки на дополнительные услуги (внеплановая смена ключей).

6.1.5. Принимать Запрос на сертификат, направленный в Банк посредством Личного кабинета, в том случае, если сведения о владельце сертификата, указанные в таком запросе, идентичны сведениям, содержащимся в действующей Заявке на Уполномоченное лицо, а также при соблюдении иных условий, установленных разделом 5 Правил.

6.1.6. Информировать Клиента о совершении или отказе в совершении каждой Операции с использованием Системы посредством присвоения в Системе расчетному (платежному) документу, содержащему распоряжение Клиента на совершение данной Операции, соответствующего статуса: «в Архиве» / «Исполнен» / «Отказан», датой присвоения которого является дата, указанная в последнем событии по данному расчетному (платежному) документу, отражаемом в Системе.

Датой получения Клиентом уведомления о совершении или отказе в совершении Операции считается дата присвоения расчетному (платежному) документу соответствующего статуса.

6.1.7. Направлять по запросу Клиента выписки о движении средств по счету с 10:00 часов утра по московскому времени рабочего дня, следующего за днем исполнения Банком Операций по этому счету.

6.1.8. Оказывать Клиенту техническое и консультационное содействие по вопросам выполнения обязанностей, возложенных на него Правилами.

6.1.9. Обеспечивать защиту информации, получаемой от Клиента, в порядке, предусмотренном федеральными законами от 02.12.90 № 395-1 «О банках и банковской деятельности», от 27.07.2006 № 152-ФЗ «О персональных данных» и иными нормативными правовыми актами Российской Федерации.

Необходимые правовые, организационные и технические меры по защите информации, в том числе защите персональных данных Уполномоченных лиц от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения и иных неправомерных действий в отношении персональных данных, определяются Банком самостоятельно с учетом требований законодательства и нормативных документов Российской Федерации.

6.1.10. Приостановить в соответствии с требованиями Федерального закона от 27.06.2011 № 161-ФЗ «О национальной платежной системе» на срок не более 2 (Двух) рабочих дней исполнение расчетного (платежного) документа Клиента, поступившего в Банк с использованием Системы, а также заблокировать использование Клиентом Системы (в том числе прекратить прием расчетных (платежных) и иных документов от Клиента с использованием Системы) в том случае, если Банком будет выявлено, что Операция, подлежащая совершению на основании данного расчетного (платежного) документа, соответствует следующим признакам осуществления перевода денежных средств без согласия Клиента:

а) совпадение информации о получателе средств с информацией о получателе средств по переводам денежных средств без согласия клиента, имеющейся в соответствующей базе данных, формируемой Банком России в соответствии с Федеральным законом от 27.06.2011 № 161-ФЗ «О национальной платежной системе» (далее – База данных);

б) совпадение информации о параметрах устройства, с использованием которого осуществлен доступ к Системе с целью осуществления Операции, с информацией о параметрах устройств, с использованием которых был осуществлен доступ к автоматизированной системе, программному обеспечению с целью осуществления перевода денежных средств без согласия клиента, имеющейся в Базе данных;

в) несоответствие характера и/или параметров и/или объема проводимой Операции (в том

числе время / день осуществления Операции, место осуществления Операции, устройство, с использованием которого осуществляется Операция, и параметры его использования, сумма осуществления Операции, получатель средств / иное) операциям, обычно совершаемым Клиентом (осуществляемой Клиентом деятельности). Необходимые правовые, организационные и технические меры по выявлению операций, не соответствующих осуществляемой Клиентом деятельности, определяются Банком самостоятельно в соответствии с принятыми в Банке мерами по защите переводов денежных средств Клиентов.

Банк приостанавливает Операцию независимо от положительного результата процедур дополнительной аутентификации Клиента по SMS-коду и/или проверки наличия получателя средств в установленном Клиентом Перечне получателей и/или IP-адреса, с которого осуществлен доступ к Системе, в установленном Клиентом Перечне разрешенных IP-адресов (при предоставлении Клиенту указанных сервисов), выполняемых Банком в соответствии с Правилами, в случае выявления признаков осуществления перевода денежных средств без согласия Клиента, указанных в подпунктах а) и б) настоящего пункта.

Банк незамедлительно информирует Клиента письменно / устно по имеющимся каналам связи с Клиентом / Уполномоченным лицом Клиента (номер телефона, адрес электронной почты, посредством Системы, иное) о приостановлении Операции и блокировании использования Системы, о рекомендациях по снижению рисков осуществления перевода денежных средств без согласия Клиента, а также запрашивает у Клиента подтверждение возобновления исполнения расчетного (платежного) документа.

Если расчетный (платежный) документ подлинный и подписан ЭП Клиента, Клиент обязуется подтвердить данный факт способом и в срок (при наличии), которые указаны в соответствующем запросе Банка, но не позднее рабочего дня, следующего за днем отправки данного расчетного (платежного) документа в Банк.

При неполучении от Клиента подтверждения, указанного в настоящем пункте, Банк возобновляет исполнение расчетного (платежного) документа с использованием Системы.

6.1.11. Оказывать Клиенту за счет Клиента услуги по установке, обслуживанию и эксплуатации Системы, не предусмотренные Условиями, на основании Заявки на дополнительные услуги или иных заявок / заявлений, предоставляемых в Банк по формам и в порядке согласно Правилам, при соблюдении условий, предусмотренных п. 6.2.9 Правил.

6.1.12. Предоставлять Клиенту доступ к информации об электронных документах, направленных Клиентом в Банк с использованием Системы, а также полученных Клиентом от Банка, не менее 1 (Одного) года с даты их отправления / получения Клиентом.

6.2. Банк имеет право:

6.2.1. Требовать от Клиента оформления расчетных (платежных) или иных документов без использования Системы в случае невозможности передачи указанных документов с использованием Системы (расчетный (платежный) или иной документ не может быть расшифрован, не проходит проверку подлинности ЭП или имеются другие технические причины), а также при нарушении условий, предусмотренных пп. 6.3.5, 6.3.8, 6.3.10 Правил, до устранения причин невозможности передачи документов и/или опасных последствий вследствие допущенных нарушений.

6.2.2. Приостанавливать осуществление Операций с использованием Системы в случае неправомерного отказа или задержки в предоставлении Клиентом надлежащим образом оформленных платежных документов в соответствии с п. 6.2.1 Правил.

6.2.3. Хранить в Системе отправленные Клиенту и не полученные им электронные сообщения не более 2 (Двух) месяцев с момента формирования электронного сообщения.

6.2.4. Расторгнуть Договор в одностороннем порядке в соответствии с п. 10.2 Правил в следующих случаях:

- переход Банка на использование другого программного обеспечения и программных комплексов и отказ Клиента от их установки либо невозможность установления связи с Клиентом в целях переоформления правоотношений по новому программному комплексу;
- невыполнение Клиентом обязанности, предусмотренной п. 6.3.16 Правил;
- в случае неиспользования Клиентом Системы по истечении 1 (Одного) года с даты блокировки Системы в связи с неуплатой Банку соответствующих комиссий за ее использование или по иным причинам;

– в иных случаях, предусмотренных действующим законодательством Российской Федерации.

6.2.5. Без согласования с Клиентом осуществлять выпуск новых версий программного обеспечения для Системы в целях улучшения ее функциональных качеств, в том числе связанных с выполнением требований к защите информации при осуществлении переводов денежных средств, с предотвращением несанкционированного доступа к защищаемой информации, передаваемой посредством Системы, и/или в связи с внесением изменений в действующее законодательство Российской Федерации.

При этом:

– актуальная версия web-приложений доступна Клиенту при установлении связи с Системой в браузере;

– информация, необходимая для обновления мобильного приложения «МКБ Бизнес», размещается Банком в репозитории. Клиент осуществляет обновление мобильного приложения «МКБ Бизнес» стандартными средствами операционной системы мобильного устройства. Банк оставляет за собой право прекратить доступ к счетам с мобильного устройства, на котором установлена устаревшая версия мобильного приложения «МКБ Бизнес».

6.2.6. Клиент предоставляет Банку право на списание с любого счета Клиента (за исключением банковского счета, с которого не допускается осуществлять списание комиссий Банка согласно законодательству Российской Федерации либо условиям договора банковского счета) суммы комиссионного вознаграждения за подключение и использование Системы, а также за дополнительные услуги, оказываемые Клиенту в соответствии с пп. 6.1.11, 6.2.15 Правил, в размере и сроки, предусмотренные Тарифами, действующими на дату списания комиссионного вознаграждения, если иное не установлено Договором.

6.2.7. Не принимать на исполнение расчетные (платежные) документы в случае несоблюдения условий п. 3.4 Правил / п. 9.8 Условий.

6.2.8. Осуществлять дополнительную аутентификацию Клиента в порядке, предусмотренном п. 2.16 Правил, при наличии у Банка сомнений в подлинности расчетного (платежного) документа в том случае, если Клиентом не установлен Перечень получателей согласно пп. 2.18, 6.4.9 Правил.

6.2.9. Отказать Клиенту в исполнении Заявления о дополнительной аутентификации, Заявки на установление Перечня разрешенных IP-адресов в случае, если на дату их предоставления Клиентом между Банком и Клиентом заключен и действует договор о предоставлении услуги «Технологическое взаимодействие с «1С:Предприятие» при проведении платежей», в рамках которого Клиент имеет возможность направлять в Банк распоряжения на перевод денежных средств по счетам, обслуживание которых осуществляется на основании Договора.

6.2.10. Заблокировать использование Системы / web-приложений Системы (в том числе прекратить прием расчетных (платежных) и иных документов от Клиента с использованием Системы) в случае неуплаты Клиентом Банку соответствующих комиссий в рамках Договора согласно действующим Тарифам.

Банк возобновляет обслуживание с использованием Системы в полном объеме после погашения задолженности Клиента перед Банком.

6.2.11. Заблокировать использование Уполномоченным лицом Системы (в том числе прекратить прием расчетных (платежных) и иных документов, направляемых от имени Клиента с использованием Системы) в случае истечения срока полномочий данного Уполномоченного лица, в том числе установленного Заявкой на Уполномоченное лицо, и/или при получении Банком информации о недействительности основного документа, удостоверяющего личность данного Уполномоченного лица.

Банк возобновляет доступ к Системе данного Уполномоченного лица в полном объеме после предоставления Банку новой Заявки на Уполномоченное лицо и иных документов, подтверждающих полномочия данного Уполномоченного лица.

6.2.12. Заблокировать использование одним, несколькими или всеми Уполномоченными лицами Клиента Системы (в том числе прекратить прием расчетных (платежных) и иных документов от Клиента с использованием Системы) на основании полученного от Клиента уведомления в случаях и порядке, предусмотренных п. 6.3.11 Правил, а также по инициативе Банка в случае нарушения Клиентом обязанностей, возложенных на него Правилами.

6.2.13. Заблокировать использование Уполномоченным лицом Системы (в том числе

прекратить прием расчетных (платежных) и иных документов от Клиента с использованием Системы) в случае истечения срока действия сертификата, в котором данное лицо указано в качестве его владельца.

Банк возобновляет доступ данного лица к Системе в порядке, указанном в п. 5.15 Правил.

6.2.14. Приостановить после предварительного предупреждения прием с использованием Системы расчетных (платежных) документов, иных распоряжений Клиента на проведение расходных операций по счету, заявлений об акцепте распоряжения получателя денежных средств, документов на проведение валютных операций, подписанных ЭП.

При этом проведение операций по счету (ам) / валютных операций возможно только на основании указанных в настоящем пункте документов, надлежащим образом оформленных Клиентом на бумажном носителе.

В этом случае Клиент продолжает использовать Систему с ограниченным функционалом, и обслуживание Клиента осуществляется согласно Тарифам за ведение счета с использованием Системы.

Банк возобновляет обслуживание с использованием Системы в полном объеме при отсутствии в Едином государственном реестре юридических лиц записей о недостоверности сведений о Клиенте, а также выполнении Клиентом условий, установленных Банком:

- личного обращения в Банк физического лица, исполняющего функции единоличного исполнительного органа Клиента;
- обновления сведений о Клиенте, представителе Клиента, выгодоприобретателе, бенефициарном владельце;
- представления в Банк документов, связанных с деятельностью Клиента, в том числе с целью определения источников происхождения денежных средств или иного имущества Клиента;
- представления Клиентом объяснений о причинах начала активного использования банковского счета, подтверждаемых соответствующими договорами (контрактами) и / или иными документами.

6.2.15. Оказывать Клиенту, не являющемуся кредитной организацией, при наличии технической возможности услуги, предусмотренные Условиями.

Банк имеет право отказать Клиенту в предоставлении услуг, предусмотренных Условиями, в случае отсутствия у Банка технической возможности / нарушения Клиентом Условий / наличия заключенного и действующего договора между Банком и Клиентом о предоставлении услуги «Технологическое взаимодействие с «1С:Предприятие» при проведении платежей», в рамках которого Клиент имеет возможность направлять в Банк распоряжения на перевод денежных средств по счетам, обслуживание которых осуществляется на основании Договора.

6.2.16. Отказать Клиенту в создании и выдаче сертификата при несоблюдении условий, предусмотренных п. 5.4, 6.3.1 Правил.

6.2.17. При необходимости в одностороннем порядке вносить изменения в Правила.

6.3. Клиент обязан:

6.3.1. При заключении Договора представить Банку Заявку (и) на Уполномоченное лицо, указанное в п. 2.5 Правил, сведения для идентификации данного лица (в случае, предусмотренном п. 2.6 Правил) и иные документы согласно п. 2.6 Правил.

Клиент обязуется в случае изменения контактных данных Уполномоченного лица, указанных в Заявке на Уполномоченное лицо, незамедлительно предоставить Банку обновленные сведения в порядке, установленном п. 6.4.7 Правил, используемые Банком для исполнения обязанностей по информированию Клиента о приостановлении исполнения расчетного (платежного) документа, предусмотренных п. 6.1.10 Правил.

Клиент обязуется уведомлять Банк с предоставлением соответствующих документов об изменении наименования и о внесении иных изменений в учредительные документы, изменении статуса, места нахождения (жительства), о введении в отношении Клиента любой процедуры несостоятельности (банкротства), а также об изменении иной информации, предоставляемой при открытии счета, в течение 2 (Двух) рабочих дней с момента таких изменений / получения документов от регистрирующего органа.

В случае изменения сведений о документе, удостоверяющем личность Уполномоченного лица, Клиент обязан предоставить в Банк новую Заявку на Уполномоченное лицо, отменяющую

действие предыдущей, а также в случае наделения данного лица правом совершать сделки с Банком и/или распоряжаться денежными средствами, находящимися на счетах Клиента, – обновленные сведения о данном лице в соответствующей форме вопросника, установленной Банком. При наличии у Банка информации об изменении указанных сведений и непредоставлении Банку новой Заявки на Уполномоченное лицо Банк блокирует доступ данного лица к Системе согласно п. 6.2.11 Правил.

В случае изменения сведений о месте нахождения владельца сертификата, указанных в действующей Заявке на Уполномоченное лицо, Клиент обязан предоставить в Банк новую Заявку на Уполномоченное лицо в период плановой смены ключей согласно п. 5.14 Правил. При наличии у Банка информации об изменении указанных сведений и непредоставлении Банку новой Заявки на Уполномоченное лицо Банк не предоставляет Клиенту возможность формирования ключей и получения нового сертификата в указанный период.

В случае изменения иных сведений о владельце сертификата, указанных в действующей Заявке на Уполномоченное лицо, Клиент обязан предоставить в Банк новую Заявку на Уполномоченное лицо. В этом случае Банк признает недействительными ключи ЭП и сертификат, используемые данным Уполномоченным лицом, блокирует его доступ к Системе, а также обеспечивает за счет Клиента возможность формирования данным Уполномоченным лицом нового ключа ЭП и получения нового сертификата не позднее даты получения такой заявки Клиента.

6.3.2. Оборудовать рабочее место Уполномоченного лица (ПЭВМ) в соответствии с Требованиями Банка. Использовать Систему только на исправном оборудовании и на корректно работающем базовом программном обеспечении.

6.3.3. Обеспечить сохранение на USB-токене ключей ЭП Клиента, формируемых Уполномоченными лицами согласно разделу 5 Правил / полученных в Банке на ключевом носителе в порядке, установленном Договором (при наличии), и обеспечить использование данных ключей ЭП Уполномоченными лицами при работе в Системе.

Обеспечить хранение на таком USB-токене только ключей ЭП, используемых Уполномоченными лицами в Системе.

6.3.4. Сохранить на ПЭВМ, используемой для установления связи с Системой, сертификат, полученный Уполномоченным лицом в Личном кабинете в порядке, установленном разделом 5 Правил / в Банке на ключевом носителе / иным способом в порядке, установленном Договором (при наличии).

6.3.5. Соблюдать (ознакомить и обеспечить соблюдение Уполномоченным лицом) Правила безопасного использования систем ДБО, размещенные на сайте Банка и являющиеся неотъемлемой частью Правил.

6.3.6. Использовать лицензионное специализированное программное обеспечение для защиты ПЭВМ Клиента, а также мобильных устройств уполномоченных лиц Клиента, используемых для проведения сеанса связи с Системой, от вредоносных кодов.

Под вредоносным кодом понимаются программный код, самостоятельное программное обеспечение или его часть, приводящие к нарушению штатного функционирования средств вычислительной техники.

Банк не несет ответственности в случаях финансовых потерь, понесенных Клиентом в связи с нарушением условия, предусмотренного настоящим пунктом Правил.

6.3.7. Не передавать третьим лицам программно-аппаратные средства Системы и сведения о применяемой системе защиты информации.

6.3.8. Обеспечивать соблюдение порядка учета, хранения и использования ключевых носителей, в том числе USB-токена с ключами ЭП, пин-кода на USB-токен, а также логина, инициализационного пароля и пароля Уполномоченного лица для доступа к Личному кабинету / Системе, SMS-кодов, направляемых Банком Клиенту в соответствии с Правилами, в том числе Условиями, исключающего несанкционированный доступ к ним посторонних лиц.

6.3.9. Сообщать Банку обо всех случаях получения от Банка сообщений / документов, которые не удалось расшифровать или которые не прошли проверку подлинности ЭП, не позднее 1 (Одного) рабочего дня, следующего за днем получения такого документа.

6.3.10. В случае прекращения полномочий Уполномоченного лица:

– незамедлительно прекратить доступ данного лица к Системе в порядке, указанном в п. 6.3.11 Правил;

– в случае использования таким лицом мобильных устройств, подключенных к мобильному

приложению «МКБ Бизнес», отменить их регистрацию в Системе в порядке, предусмотренном Условиями.

6.3.11. Клиент обязуется при возникновении угрозы несанкционированного доступа к Системе в случаях компрометации ключа (ей) ЭП / логина и пароля / пароля для доступа к Системе, использовании Системы без согласия Клиента незамедлительно сообщить об этом в Банк посредством обращения по телефону Контакт-центра с последующим предоставлением Заявки на дополнительные услуги.

При получении указанного выше уведомления от Клиента Банк признает ключ ЭП / все ключи ЭП Клиента недействительным (и) и блокирует доступ к Системе одного или нескольких Уполномоченных лиц / Систему. При этом Банк признает Заявку на Уполномоченное лицо недействительной при получении уведомления о прекращении полномочий данного лица и прекращает возможность формирования ключа ЭП и получения сертификата в рамках такой заявки.

Банк предоставляет возможность за счет Клиента:

– Уполномоченному лицу, ключ ЭП которого признан недействительным и полномочия которого не прекращены, сформировать новый ключ ЭП и получить сертификат в порядке, установленном разделом 5 Правил, не позднее рабочего дня, следующего за днем получения Банком Заявки на дополнительные услуги (внеплановая смена ключей);

– новому Уполномоченному лицу Клиента сформировать ключ ЭП и получить сертификат в порядке, установленном разделом 5 Правил, не позднее рабочего дня, следующего за днем получения Банком Заявки на Уполномоченное лицо и иных документов согласно п. 2.6 Правил.

Банк обеспечивает возможность использования Уполномоченным (и) лицом (ами) Клиента ЭП, удостоверенной новым сертификатом, снимает блокировку доступа к Системе и возобновляет обслуживание счетов с использованием Системы не позднее рабочего дня, следующего за днем принятия от него Подтверждения о получении сертификата согласно разделу 5 Правил.

6.3.12. Клиент обязуется в случае компрометации номера телефона, который используется для направления Банком Клиенту SMS-сообщений согласно пп. 2.16, 2.20 Правил, в том числе в случае утраты мобильного устройства / прекращения полномочий лица, уполномоченного на получение посредством таких SMS-сообщений информации, предусмотренной Правилами, незамедлительно прекратить использование данного номера телефона в указанных целях путем представления в Банк соответствующего (ей) заявления / заявки, предусмотренных пп. 6.4.8, 6.4.11 Правил.

6.3.13. Клиент обязуется обеспечивать наличие на счетах денежных средств, необходимых для уплаты комиссионного вознаграждения Банку за предоставление услуг в рамках Договора согласно Тарифам.

6.3.14. Клиент обязуется регулярно, не реже одного раза в день, осуществлять вход в Систему с целью ознакомления с информацией, направляемой Банком в порядке, предусмотренном п. 6.1.6 Правил.

6.3.15. Клиент обязуется по требованию Банка осуществлять оформление расчетных (платежных) и иных документов без использования Системы в случае невозможности передачи указанных документов с использованием Системы (расчетный (платежный) или иной документ не может быть расшифрован, не проходит проверку подлинности ЭП или имеются другие технические причины), а также при нарушении условий, предусмотренных пп. 6.3.5, 6.3.8, 6.3.10 Правил, до устранения причин невозможности передачи документов и/или последствий допущенных нарушений.

6.3.16. Клиент обязуется не использовать предоставляемое СКЗИ «КриптоПро CSP» в сервисах, отличных от предоставляемых Банком.

6.4. Клиент имеет право:

6.4.1. Передавать с использованием Системы расчетные (платежные) документы на осуществление переводов денежных средств со счета согласно действующему законодательству Российской Федерации в пределах остатка денежных средств на счете, за исключением ограничений, налагаемых законодательством Российской Федерации, Банком России, налоговыми и правоохранительными органами, а также Банком на основании существующих договоров и соглашений, осуществлять электронный документооборот.

6.4.2. Расторгнуть Договор, в том числе в случае несогласия Клиента с изменениями Правил, в любое время в соответствии с п. 10.2 Правил.

6.4.3. Заблокировать использование Системы (в том числе приостановить прием Банком расчетных (платежных) и иных документов от Клиента с использованием Системы) на определенный период времени путем предоставления в Банк Заявки на дополнительные услуги.

6.4.4. Заблокировать использование Системы конкретным Уполномоченным лицом на определенный период времени путем предоставления в Банк Заявки на дополнительные услуги.

6.4.5. Получать с использованием Системы выписки о движении денежных средств по счету (ам) Клиента с 10:00 часов утра по московскому времени рабочего дня, следующего за днем совершения Операций.

6.4.6. Оформить за счет Клиента заказ на предоставление дополнительных услуг по установке, обслуживанию и эксплуатации Системы путем предоставления Заявки на дополнительные услуги или иных заявок / заявлений по формам и в порядке согласно Правилам.

6.4.7. Вносить изменения в содержание предоставленной Банку ранее Заявки на Уполномоченное лицо без прекращения действия сертификата и доступа данного Уполномоченного лица к Системе путем предоставления Банку новой Заявки на Уполномоченное лицо, а именно изменить в отношении Уполномоченного лица:

- номер телефона или адрес электронной почты;
- Кодовое слово;
- сведения об основном документе, удостоверяющем личность;
- срок действия полномочий по работе с Системой;
- объем полномочий по работе с Системой.

После исполнения Банком новой Заявки на Уполномоченное лицо Клиенту направляется посредством Системы уведомление об исполнении с указанием даты, часов и минут по московскому времени, которые фиксируются Системой.

Под исполнением Заявки на Уполномоченное лицо понимается завершение Банком технических процедур, необходимых для изменения порядка работы Уполномоченного лица с Системой согласно измененным Клиентом данным.

С даты и времени, содержащихся в указанном выше уведомлении, ранее предоставленная в Банк Заявка на Уполномоченное лицо считается измененной на условиях новой Заявки на Уполномоченное лицо.

6.4.8. Изменить номера телефонов, используемые для дополнительной аутентификации Клиента по SMS-коду / отменить дополнительную аутентификацию Клиента по SMS-коду путем предоставления Банку заявления, составленного на бумажном носителе либо сформированного и направленного с использованием Системы, по форме 5 Сборника (далее – Заявление об изменении параметров / отмене дополнительной аутентификации).

В случае направления в Банк Заявления об изменении параметров / отмене дополнительной аутентификации с использованием Системы Банк осуществляет дополнительную аутентификацию Клиента в порядке, предусмотренном п. 2.16 Правил, и при положительном результате указанной процедуры исполняет данное заявление.

После исполнения Заявления об изменении параметров / отмене дополнительной аутентификации Банк направляет Клиенту посредством Системы соответствующее уведомление об исполнении с указанием даты, часов и минут по московскому времени, которые фиксируются Системой.

Под исполнением Заявления об изменении параметров / отмене дополнительной аутентификации понимается завершение Банком технических процедур, необходимых для изменения порядка работы с Системой согласно установленным Клиентом данным.

С даты и времени, указанных в уведомлении об исполнении Банком Заявления об изменении параметров / отмене дополнительной аутентификации, ранее предоставленное в Банк Заявление о дополнительной аутентификации считается измененным / отмененным на условиях Заявления об изменении параметров / отмене дополнительной аутентификации.

6.4.9. Вносить изменения в содержание предоставленного Банку ранее Перечня получателей / отменить установленный Перечень получателей путем предоставления Банку заявления, сформированного и переданного с использованием Системы по форме 6а Сборника либо составленного на бумажном носителе по форме 6б Сборника (только в случае отмены Перечня получателей) (далее – Заявление на установление / отмену Перечня получателей).

В случае направления в Банк Заявления на установление / отмену Перечня получателей с

использованием Системы Банк осуществляет дополнительную аутентификацию Клиента в порядке, предусмотренном п. 2.16 Правил, и при положительном результате указанной процедуры исполняет данное заявление.

После исполнения Заявления на установление / отмену Перечня получателей Банк направляет Клиенту посредством Системы соответствующее уведомление об исполнении с указанием даты, часов и минут по московскому времени, которые фиксируются Системой.

Под исполнением Заявления на установление / отмену Перечня получателей понимается завершение Банком технических процедур, необходимых для изменения порядка работы с Системой согласно измененным Клиентом данным.

С даты и времени, указанных в уведомлении об исполнении Банком Заявления на установление / отмену Перечня получателей, ранее предоставленное в Банк Заявление на установление Перечня получателей считается измененным / отмененным на условиях Заявления на установление / отмену Перечня получателей.

6.4.10. Вносить изменение в содержание предоставленного Банку ранее Перечня разрешенных IP-адресов / отменить установленный Перечень разрешенных IP-адресов путем предоставления Банку заявки, сформированной и направленной с использованием Системы по форме 7 Сборника (далее – Заявка на установление / отмену Перечня разрешенных IP-адресов).

В случае направления в Банк Заявки на установление / отмену Перечня разрешенных IP-адресов с использованием Системы Банк осуществляет дополнительную аутентификацию Клиента в порядке, предусмотренном п. 2.16 Правил, и при положительном результате указанной процедуры исполняет данную заявку.

После исполнения Заявки на установление / отмену Перечня разрешенных IP-адресов Банк направляет Клиенту посредством Системы соответствующее уведомление об исполнении с указанием даты, часов и минут по московскому времени, которые фиксируются Системой.

Под исполнением Заявки на установление / отмену Перечня разрешенных IP-адресов понимается завершение Банком технических процедур, необходимых для изменения порядка работы с Системой согласно установленным Клиентом данным.

С даты и времени, указанных в уведомлении об исполнении Банком Заявки на установление / отмену Перечня разрешенных IP-адресов, ранее представленная в Банк Заявка на установление Перечня разрешенных IP-адресов считается измененной / отмененной на условиях Заявки на установление / отмену Перечня разрешенных IP-адресов.

6.4.11. Вносить изменение в содержание предоставленной Банку ранее Заявки на SMS-информирование / отменить услугу «SMS-информирование по расчетному счету» путем предоставления Банку на бумажном носителе либо с использованием Системы новой Заявки на SMS-информирование (форма 19 Сборника).

После исполнения Заявки на SMS-информирование Банк направляет Клиенту посредством Системы соответствующее уведомление об исполнении с указанием даты, часов и минут по московскому времени, которые фиксируются Системой, а также направляет на используемые в рамках услуги «SMS-информирование по расчетному счету» номера телефонов SMS-сообщение, содержащее уведомление об изменении параметров SMS-информирования / отключении SMS-информирования в отношении данных номеров телефона.

Под исполнением Заявки на SMS-информирование понимается завершение Банком технических процедур, необходимых для осуществления информирования Клиента согласно установленным Клиентом данным.

С даты и времени, указанных в уведомлении об исполнении Банком Заявки на SMS-информирование, ранее представленная в Банк Заявка на SMS-информирование считается измененной / отмененной на условиях новой Заявки на SMS-информирование.

7. ПОРЯДОК РАССМОТРЕНИЯ ПРЕТЕНЗИЙ КЛИЕНТА

При разрешении спорных ситуаций Стороны обязуются руководствоваться следующими принципами:

7.1. Принимающая Сторона обязуется признавать подлинными переданные ей с использованием Системы электронные сообщения, содержащие документы, подписанные ЭП и успешно прошедшие проверку подлинности ЭП.

7.2. В случае получения принимающей Стороной с использованием Системы электронного сообщения, содержащего документ, подписанный ЭП и успешно прошедший проверку подлинности ЭП, ответственность принимает на себя передающая Сторона как не обеспечившая сохранность своего ключа (ей) ЭП.

7.3. При возникновении у Клиента претензий к Банку в связи с совершением Операций, осуществление которых он Банку не поручал:

- Клиент должен направить в Банк претензию в письменном виде с указанием реквизитов Операции, исполнение которой считает неправомерным;

- для разрешения спорной ситуации Клиент должен направить в Банк полномочного представителя, а также передать все имеющиеся у Клиента документы с информацией об указанной Операции;

- для разрешения спорной ситуации из контрольного архива банковского программного модуля извлекается расчетный (платежный) документ, на основании которого Банком была исполнена указанная Операция;

- устанавливается подлинность ЭП, учитывая содержание сертификата;

- определяется, являлся ли сертификат действующим в дату исполнения спорной Операции.

Если результат проверки подлинности ЭП отрицательный и/или не соблюдены условия, предусмотренные п. 2.16.5 Правил, то претензии Клиента принимаются.

Если результат проверки подлинности ЭП положительный и соблюдены условия, предусмотренные пп. 2.16.5, 2.19 Правил, то претензии Клиента отклоняются.

7.4. При возникновении у Клиента претензий к Банку в связи с неисполнением операции, совершение которой Клиент поручал Банку:

- Клиент должен направить в Банк претензию в письменном виде с указанием реквизитов не исполненной Банком операции и распечатку копии расчетного (платежного) документа;

- для разрешения спорной ситуации Клиент должен направить в Банк полномочного представителя, а также передать все имеющиеся у Клиента документы с информацией об указанной операции;

- для разрешения спорной ситуации Банк извлекает из контрольного архива банковского программного модуля сведения о протоколах соединения при проведении сеансов связи с Системой.

Если указанный расчетный (платежный) документ найден в контрольном архиве банковского программного модуля:

- устанавливается подлинность ЭП, учитывая содержание сертификата;

- определяется, являлся ли сертификат действующим в дату исполнения спорной операции.

Если указанный расчетный (платежный) документ найден в контрольном архиве банковского программного модуля, результат проверки подлинности ЭП положительный и соблюдены условия, предусмотренные пп. 2.16.5, 2.19 Правил, то претензии Клиента принимаются.

Если указанный документ не найден в контрольном архиве банковского программного модуля, то претензии Клиента отклоняются.

Банк не рассматривает претензии Клиента в случае несвоевременного прочтения Клиентом электронных сообщений, полученных от Банка с использованием Системы, содержащих причины отказа в обработке документа.

7.5. В случае направления претензий в отношении действий, совершенных с использованием Личного кабинета, Стороны признают основными доказательствами содержимое журналов Личного кабинета, выгружаемых Банком и предоставляемых Клиенту в рамках рассмотрения претензии.

7.6. По результатам проверки при обнаружении несоответствия либо ошибок в документах уполномоченными представителями Банка и Клиента составляется акт с целью определения виновной Стороны и принятия необходимых мер по урегулированию конфликтной ситуации.

7.7. Претензия Клиента рассматривается Банком в течение 10 (Десяти) рабочих дней с даты поступления в Банк. Если в ходе рассмотрения претензии по объективным причинам возникают сложности в расследовании обстоятельств претензии, то срок ее рассмотрения может быть увеличен Банком, но в любом случае не может превышать: 30 (Тридцати) календарных дней со дня ее поступления в Банк – по переводу денежных средств в пределах территории Российской Федерации, 60 (Шестидесяти) календарных дней со дня ее поступления в Банк – по трансграничному переводу денежных средств.

8. ОТВЕТСТВЕННОСТЬ СТОРОН

8.1. Стороны несут ответственность за неисполнение или ненадлежащее исполнение своих обязанностей, предусмотренных Правилами, в соответствии с действующим законодательством Российской Федерации.

8.2. Стороны несут ответственность за нарушение сроков проведения расчетных операций по электронным документам, полученным с использованием Системы, в соответствии с договорами банковского счета, заключенными между Банком и Клиентом.

8.3. Стороны несут ответственность за обеспечение сохранности прикладного программного обеспечения и архивов документов, предусмотренных Правилами.

8.4. Каждая из Сторон несет ответственность за конфиденциальность своих ключей ЭП, а также за все действия, совершенные в Личном кабинете и Системе с использованием ключа ЭП и/или логина и пароля.

8.5. Сторона не несет ответственности за ущерб, возникший вследствие передачи другой Стороной третьим лицам программного обеспечения «КриптоПро CSP», используемого для шифрования данных, и/или ключей ЭП и/или логина, инициализационного пароля, пароля Уполномоченного лица, используемых для доступа в Личный кабинет / Систему, вне зависимости от причин.

8.6. Стороны не несут ответственности за сбои и помехи в работе линий связи, приводящие к невозможности передачи расчетных (платежных) или иных документов с использованием Системы, в том числе web-приложения Системы.

8.7. Банк не несет ответственности за сбои в работе Системы, в том числе задержки и искажения в обмене документами / информацией, обусловленные неисправностью программно-аппаратных средств Клиента, нарушением работоспособности программного обеспечения и/или СКЗИ, производителем которых Банк не является, или иными внешними факторами, в том числе повреждением программного обеспечения Системы.

Банк также не несет ответственности за искажение и/или непредоставление / несвоевременное предоставление информации в виде SMS-сообщений, связанное с перебоями в работе операторов сотовой связи, участвующих в доставке информационных сообщений (в том числе при нахождении в роуминге, а также в случае блокирования телефонного номера Клиента или по иным, не зависящим от Банка, причинам).

8.8. Банк не несет ответственности по Операциям, а также ответственности за любые финансовые потери Клиента, иные убытки Клиента при невыполнении либо ненадлежащем выполнении Клиентом обязательств, предусмотренных Правилами, в том числе, но не исключительно п. 6.3 Правил и / или соответствующими пунктами Условий.

8.9. Банк не несет ответственности за последствия исполнения полученных с использованием Системы расчетных (платежных) и иных документов, содержащих ЭП, конфиденциальность которых была нарушена по вине Клиента, в случае отсутствия информации у Банка о нарушении конфиденциальности ключа (ей) ЭП Клиента.

Клиент несет ответственность за использование ключей ЭП исключительно лицами, указанными в п. 2.5 Правил, информация о которых предоставлена Банку в порядке, предусмотренном п. 6.3.1 Правил.

8.10. В случае неисполнения обязанностей, предусмотренных пп. 6.3.10, 6.3.11 Правил, ответственность Банка за использование ключей ЭП Клиента неуполномоченными лицами исключается и все возникающие в связи с этим риски Клиент несет самостоятельно.

9. ПОРЯДОК ВНЕСЕНИЯ ИЗМЕНЕНИЙ В ПРАВИЛА

9.1. Внесение изменений и дополнений в Правила, а также утверждение Банком новой редакции Правил производится в одностороннем порядке по инициативе Банка.

9.2. Если отдельные положения Правил становятся недействительными или вступают в противоречие с действующим законодательством Российской Федерации, остальные положения Правил сохраняют силу. В этом случае Банк должен устранить недействительные положения Правил и внести в них соответствующие изменения.

9.3. Банк информирует Клиента об изменениях и дополнениях, вносимых Банком в Правила, в том числе об утверждении Банком новой редакции Правил, не менее чем за 5 (Пять) календарных

дней до вступления их в силу. Информирование производится путем размещения новой редакции Правил на сайте Банка и/или направления соответствующего уведомления с использованием Системы.

9.4. Стороны признают, что любые изменения и дополнения, вносимые Банком в Правила, в том числе утвержденная Банком новая редакция Правил, распространяются на Стороны с даты вступления их в силу. В случае несогласия Клиента с изменениями или дополнениями, внесенными Банком в Правила, Клиент имеет право расторгнуть Договор в порядке, предусмотренном п. 10.2 Правил.

10. СРОК ДЕЙСТВИЯ ДОГОВОРА

10.1. Договор вступает в силу с даты его подписания Сторонами / с даты подписания Сторонами дополнительного соглашения к ранее заключенному договору, регулиющему порядок проведения банковских операций по счетам с использованием Системы, о его изложении в новой редакции, предусматривающей обслуживание счетов с использованием Системы на условиях и в порядке, определенных Правилами, если иное не установлено Договором либо указанным соглашением.

После вступления Договора в силу автоматически утрачивают силу все ранее заключенные и действующие договоры и соглашения (при их наличии), регулирующие порядок проведения банковских операций с использованием Системы по счетам, обслуживание которых осуществляется на основании Договора. Действие Договора автоматически распространяется на период действия договоров банковского счета, заключенных между Банком и Клиентом, и прекращается без дополнительного уведомления при условии закрытия всех счетов, указанных в настоящем пункте Правил, а также в иных случаях, предусмотренных Правилами.

10.2. Договор может быть расторгнут по взаимной договоренности Сторон или в одностороннем порядке в случаях, предусмотренных действующим законодательством Российской Федерации и пп. 6.2.4, 6.4.2 Правил.

В случае неиспользования Клиентом Системы по истечении 1 (Одного) года с даты блокировки Системы в связи с неуплатой Банку соответствующих комиссий за ее использование Договор может быть расторгнут Банком без дополнительного уведомления Клиента.

В иных случаях Договор может быть расторгнут в одностороннем порядке путем письменного уведомления другой Стороны не позднее чем за 10 (Десять) календарных дней до предполагаемой даты расторжения, указанной в данном уведомлении. Банк уведомляет Клиента о расторжении Договора путем направления уведомления на бумажном носителе или с использованием Системы. Клиент уведомляет Банк о расторжении Договора путем направления уведомления на бумажном носителе.

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

11. РАЗРЕШЕНИЕ СПОРОВ

Все споры, возникающие при исполнении Сторонами обязательств, предусмотренных Правилами, решаются путем переговоров. В случае если Стороны не придут к взаимному согласию, неурегулированные споры подлежат рассмотрению в Арбитражном суде г. Москвы в соответствии с действующим законодательством Российской Федерации.

12. ПРОЧИЕ ПОЛОЖЕНИЯ

12.1. Договор является неотъемлемой частью договоров банковского счета, заключенных между Банком и Клиентом. Во всем, что не предусмотрено Правилами, Стороны руководствуются положениями заключенных договоров банковского счета и действующим законодательством Российской Федерации.

12.2. Договор в период его действия может быть дополнен или изменен Сторонами, если иное не предусмотрено Договором и настоящими Правилами. При этом все дополнения или изменения имеют силу, если они совершены в письменном виде и подписаны Сторонами.

Стороны признают, что документы, связанные с дополнениями или изменениями к Договору,

обмен которыми осуществляется между Банком и Клиентом с использованием Системы, подписанные ЭП Банка и ЭП Клиента, являются равнозначными аналогичным документам на бумажном носителе, подписанным собственноручной подписью уполномоченных лиц Сторон и заверенным печатями Сторон (при наличии у Сторон печатей).

12.3. Размеры комиссий, взимаемых Банком с Клиента за предоставление Клиенту услуг в рамках исполнения Договора, определяются Тарифами.

Банк имеет право в одностороннем порядке без согласования с Клиентом вносить изменения в действующие Тарифы. При этом Банк извещает Клиента об изменении Тарифов в срок, установленный Тарифами, путем направления соответствующей информации с использованием Системы, размещения указанной информации на стендах в помещениях дополнительных офисов Банка или на сайте Банка.

12.4. Стороны признают, что начиная с календарного дня, следующего за датой начала использования Системы согласно п. 2.14 Правил, все положения заключенных договоров банковского счета, касающиеся обязанности Банка предоставлять выписки о движении денежных средств по счетам Клиента на бумажных носителях, приостанавливают свое действие на срок действия Договора и вступают в силу автоматически с момента прекращения Договора согласно разделу 10 Правил.

12.5. После принятия Банком от Клиента первого Подтверждения о получении сертификата согласно п. 5.12 Правил все ранее признанные ключи ЭП Клиента, переданные Клиенту на ключевом носителе / иным способом в порядке, установленном Договором, при их наличии, автоматически считаются недействительными.

Банк предоставляет возможность Клиенту осуществить за счет Банка в порядке, предусмотренном пп. 2.12, 2.13 Правил, внеплановую смену ключей, используемых Уполномоченным лицом, информация о котором предоставлена Банку ранее и полномочия которого не были прекращены, чей ключ ЭП признан недействительным.

12.6. Правила и все приложения к ним, в том числе Условия, Требования, Руководство по ЛК и Правила безопасного использования систем ДБО, являются неотъемлемой частью Договора.

Приложение 1
к Правилам обслуживания банковских счетов,
открытых в ПАО «МОСКОВСКИЙ
КРЕДИТНЫЙ БАНК», с использованием
электронной системы «Ваш Банк Онлайн»
(версия 2)

Условия использования мобильного приложения «МКБ Бизнес» электронной системы «Ваш Банк Онлайн»

1. В дополнение к основным понятиям, содержащимся в разделе 1 Правил, в настоящих Условиях используются следующие понятия:

идентификатор мобильного устройства – уникальная информация о мобильном устройстве, на котором установлено мобильное приложение «МКБ Бизнес», предоставляемая операционной системой, под управлением которой работает данное мобильное устройство, используемая Банком для его идентификации в Системе. В зависимости от операционной системы для мобильного устройства и технической возможности используются идентификаторы: identifierForVendor (для устройств, работающих под управлением операционной системы iOS), AndroidId (для устройств, работающих под управлением операционной системы Android) и/или иная идентификационная информация;

номер абонентского ящика – цифровой идентификатор Клиента в Системе, присваиваемый Банком при заключении Договора, а также (при необходимости) в случае предоставления Клиенту дополнительных услуг в рамках Договора. Информация о номере абонентского ящика отображается в Системе;

Сервис «Мобильный платеж» – сервис, позволяющий Клиенту составлять, удостоверить и передавать в Банк расчетные (платежные) документы с использованием мобильного устройства, подключенного к мобильному приложению «МКБ Бизнес».

2. Настоящие Условия определяют порядок предоставления Клиенту, не являющемуся кредитной организацией, доступа к мобильному приложению «МКБ Бизнес» и осуществления с его использованием дистанционного банковского обслуживания счетов, в рамках которого Уполномоченное лицо Клиента осуществляет следующие действия с использованием мобильного устройства:

2.1. Получает информацию об операциях, оборотах и остатках по счетам.

2.2. Составляет, подписывает простой ЭП посредством использования SMS-кода и передает в Банк расчетные (платежные) документы, содержащие распоряжения о переводе денежных средств в валюте Российской Федерации в пользу получателей средств, указанных в Перечне получателей, установленном согласно пп. 2.18, 6.4.9 Правил, не являющихся получателями бюджетных средств, при условии подключения Сервиса «Мобильный платеж» в порядке, предусмотренном настоящими Условиями.

В случае если Клиенту предоставлен доступ к мобильному приложению «МКБ Бизнес» в объеме, предусмотренном п. 2.1 настоящих Условий, под Уполномоченным лицом Клиента понимается лицо, являющееся пользователем мобильных устройств, успешно зарегистрированных в Системе в порядке, предусмотренном настоящими Условиями.

В случае если Клиенту предоставлен доступ к мобильному приложению «МКБ Бизнес» в объеме, предусмотренном пп. 2.1, 2.2 настоящих Условий, под Уполномоченным лицом Клиента понимается исключительно:

если Клиент является юридическим лицом – единоличный исполнительный орган Клиента;

если Клиент является индивидуальным предпринимателем, физическим лицом, занимающимся в установленном законодательством Российской Федерации порядке частной практикой, – Клиент.

3. Банк предоставляет Клиенту доступ к мобильному приложению «МКБ Бизнес» не позднее рабочего дня, следующего за днем получения Заявки на дополнительные услуги либо заявки, сформированной (форма 10 Сборника) и направленной Клиентом посредством Системы.

4. Банк информирует Клиента о предоставлении доступа к мобильному приложению «МКБ Бизнес» путем направления соответствующего уведомления посредством Системы, отображаемого в

web-приложении.

Датой начала использования Клиентом мобильного приложения «МКБ Бизнес» является дата получения Клиентом указанного уведомления, которая фиксируется в Системе.

5. Для получения Уполномоченными лицами Клиента доступа к счетам посредством мобильного приложения «МКБ Бизнес» Клиент самостоятельно осуществляет регистрацию мобильного устройства в Системе (далее – регистрация мобильного устройства), на котором мобильное приложение «МКБ Бизнес» установлено путем скачивания соответствующего файла, размещенного Банком в репозитории.

6. Для регистрации мобильного устройства Уполномоченное лицо Клиента формирует в мобильном приложении «МКБ Бизнес» запрос путем ввода номера абонентского ящика, имени пользователя и пароля, используемых Клиентом для доступа к Системе в рамках Договора.

Клиент подтверждает в web-приложении Системы указанный выше запрос путем присвоения регистрируемому мобильному устройству соответствующего статуса, разрешающего доступ к счетам посредством мобильного приложения «МКБ Бизнес» (далее – статус разрешенного доступа), отображаемого в web-приложении Системы в разделе «Мобильный Банк».

В случае положительного результата процедуры проверки Банком наличия у Клиента действующего сертификата в Системе регистрируется идентификатор мобильного устройства, отображаемый в разделе «Мобильный Банк» web-приложения Системы, и формируется код регистрации мобильного устройства, который представляет собой уникальную последовательность цифровых символов. Код регистрации мобильного устройства отображается в web-приложении Системы в разделе «Мобильный Банк», а также может быть направлен Банком посредством передачи SMS-сообщения на номер телефона, указанный Клиентом при регистрации мобильного устройства.

Уполномоченное лицо Клиента с целью завершения процедуры регистрации мобильного устройства вводит код регистрации мобильного устройства в соответствующее поле мобильного приложения «МКБ Бизнес».

В случае положительного результата процедуры проверки Банком идентификатора мобильного устройства, имени пользователя и пароля Клиента, кода регистрации мобильного устройства и наличия у него статуса разрешенного доступа Банк подтверждает регистрацию мобильного устройства в Системе путем предоставления доступа к счетам с зарегистрированного мобильного устройства в объеме, предусмотренном п. 2.1 настоящих Условий.

Клиент подтверждает и гарантирует, что мобильные устройства, зарегистрированные им в Системе, подключенные к мобильному приложению «МКБ Бизнес», используются исключительно лицами, уполномоченными Клиентом на получение информации, указанной в п. 2.1 настоящих Условий.

7. Уполномоченное лицо Клиента осуществляет с мобильного устройства запрос на получение доступа к счетам посредством мобильного приложения «МКБ Бизнес» путем ввода:

– номера абонентского ящика, имени пользователя и пароля, используемых Уполномоченным лицом для доступа к Системе в рамках Договора;

либо

– короткого кода доступа, установленного Уполномоченным лицом Клиента самостоятельно (при необходимости) в настройках мобильного приложения «МКБ Бизнес», используемого на подключенном мобильном устройстве (далее – короткий код доступа).

8. Банк предоставляет доступ к счетам с мобильных устройств посредством мобильного приложения «МКБ Бизнес» только в случае положительного результата процедуры проверки имени пользователя и пароля Уполномоченного лица / короткого кода доступа, идентификатора мобильного устройства, а также наличия у данного мобильного устройства статуса разрешенного доступа.

9. Клиент в случае необходимости использования мобильного приложения «МКБ Бизнес» в объеме, предусмотренном пп. 2.1, 2.2 настоящих Условий, может обратиться в Банк для подключения Сервиса «Мобильный платеж» в том случае, если зарегистрированное в Системе мобильное устройство, к которому подключается Сервис «Мобильный платеж», имеет статус разрешенного доступа, отображаемый в web-приложении Системы в разделе «Мобильный Банк».

Сервис «Мобильный платеж» может использоваться только на одном мобильном устройстве, зарегистрированном в Системе и отображаемом в web-приложении Системы в списке зарегистрированных мобильных устройств.

Клиент с целью подключения Сервиса «Мобильный платеж» формирует и направляет в Банк

с использованием Системы заявку по форме 10 Сборника (далее – Заявка на подключение Сервиса «Мобильный платеж»).

После исполнения Заявки на подключение Сервиса «Мобильный платеж» Банк присваивает мобильному устройству, к которому подключен указанный сервис, соответствующий статус, отображаемый в web-приложении Системы в разделе «Мобильный Банк». Также Банк направляет Клиенту посредством Системы соответствующее уведомление об исполнении с указанием даты, часов и минут по московскому времени, которые фиксируются Системой.

Под исполнением Заявки на подключение Сервиса «Мобильный платеж» понимается завершение Банком технических процедур, необходимых для изменения порядка работы с мобильным приложением «МКБ Бизнес» согласно установленным Клиентом данным.

9.1. Клиент подтверждает и гарантирует, что мобильное устройство, идентификатор которого указан в заявке, предусмотренной пп. 9, 9.9 настоящих Условий, а также номер телефона, используемый Банком для направления Уполномоченному лицу Клиента SMS-кодов согласно п. 9.3 настоящих Условий, указанный в данной заявке, используются исключительно:

если Клиент является юридическим лицом – единоличным исполнительным органом Клиента;
если Клиент является индивидуальным предпринимателем, физическим лицом, занимающимся в установленном законодательством Российской Федерации порядке частной практикой, – Клиентом.

9.2. Создание расчетного (платежного) документа в мобильном приложении «МКБ Бизнес» осуществляется путем копирования расчетного (платежного) документа:

– созданного и подписанного ЭП Клиента в web-приложении Системы,
либо

– созданного в мобильном приложении «МКБ Бизнес» указанным выше способом,
и (при необходимости) изменения после копирования номера, суммы и назначения платежа.

Создание расчетного (платежного) документа по валютной операции не допускается.

9.3. Для подписания и отправки в Банк расчетного (платежного) документа Уполномоченное лицо Клиента совершает в мобильном приложении «МКБ Бизнес» действие «Подписать и отправить» и формирует запрос на отправку Банком SMS-кода.

При формировании Уполномоченным лицом Клиента данного запроса Банк генерирует одноразовый код и направляет посредством SMS-сообщения на номер телефона, указанный Клиентом в заявке, предусмотренной пп. 9, 9.9 настоящих Условий.

9.4. SMS-сообщение, содержащее одноразовый код, направляется Банком один раз. Вне зависимости от возможности передачи SMS-сообщений на номер телефона, используемый Уполномоченным лицом Клиента (аппарат абонента выключен или находится вне зоны действия сети, оказание услуг связи абоненту приостановлено / отключено или имеются иные, не зависящие от Банка, причины), SMS-сообщение считается отправленным Уполномоченному лицу Клиента, что может быть подтверждено оператором связи.

9.5. SMS-сообщение, направляемое Банком Уполномоченному лицу Клиента, содержит следующую информацию (написанную буквами латинского алфавита):

– номер и сумма расчетного (платежного) документа;
– наименование Клиента;
– маскированный номер счета, с которого будут перечисляться денежные средства по распоряжению Клиента о переводе денежных средств;
– наименование и ИНН получателя средств;
– маскированный номер счета получателя средств;
– одноразовый код.

9.6. После получения SMS-сообщения, содержащего информацию, указанную в п. 9.5 настоящих Условий, Уполномоченное лицо Клиента обязано проверить правильность указанных в ней данных.

В случае успешной проверки информации Уполномоченное лицо Клиента вводит SMS-код в соответствующее поле мобильного приложения «МКБ Бизнес», подтверждая факт формирования ЭП данным Уполномоченным лицом Клиента.

9.7. Банк предоставляет Клиенту возможность успешно завершить процедуры создания, подписания простой ЭП посредством использования SMS-кода и передачи в Банк расчетных (платежных) документов с мобильного устройства посредством мобильного приложения «МКБ

Бизнес» только в случае положительного результата процедуры проверки идентификатора мобильного устройства, а также наличия у данного мобильного устройства соответствующего статуса разрешенного доступа.

Уполномоченное лицо Клиента, подписавшее расчетный (платежный) документ простой ЭП, считается определенным при одновременном соблюдении следующих условий:

- установлен факт доступа к мобильному приложению «МКБ Бизнес» при положительном результате процедуры проверки имени пользователя и пароля Уполномоченного лица / короткого кода доступа, используемых Уполномоченным лицом Клиента согласно п. 7 настоящих Условий;

- установлен факт направления запроса на отправку Банком SMS-кода с мобильного устройства, идентификатор которого указан в заявке, предусмотренной пп. 9, 9.9 настоящих Условий, используемого Уполномоченным лицом Клиента согласно п. 9.1 настоящих Условий;

- установлен факт направления Банком SMS-кода на номер телефона, указанный в заявке, предусмотренной пп. 9, 9.9 настоящих Условий, используемый Уполномоченным лицом Клиента согласно п. 9.1 настоящих Условий;

- установлен факт ввода SMS-кода на мобильном устройстве, идентификатор которого указан в заявке, предусмотренной пп. 9, 9.9 настоящих Условий, используемом Уполномоченным лицом Клиента согласно п. 9.1 настоящих Условий;

- установлен факт, что SMS-код, введенный на мобильном устройстве, идентификатор которого указан в заявке, предусмотренной пп. 9, 9.9 настоящих Условий, используемом Уполномоченным лицом Клиента согласно п. 9.1 настоящих Условий, идентичен одноразовому коду, сгенерированному Банком согласно п. 9.3 настоящих Условий.

9.8. Расчетный (платежный) документ принимается Банком только при соблюдении следующих условий:

- документ оформлен в соответствии с требованиями, установленными нормативным документом Банка России;

- все указанные в документе реквизиты являются верными;

- ИНН и номер счета получателя средств, указанные в документе, идентичны ИНН и номеру счета получателя, указанного в Перечне получателей, установленном согласно пп. 2.18, 6.4.9 Правил;

- получатель средств не является получателем бюджетных средств;

- соблюдены условия, предусмотренные п. 9.7 настоящих Условий.

Стороны признают, что такие расчетные (платежные) документы, переданные Уполномоченным лицом Клиента в Банк с использованием мобильного устройства, равнозначны расчетным (платежным) документам на бумажном носителе, подписанным Уполномоченным лицом Клиента.

В случае отрицательного результата проверки Банком поступившего расчетного (платежного) документа Банк отказывает в его приеме, о чем уведомляет Клиента путем присвоения такому документу соответствующего статуса в Системе, который свидетельствует о том, что данный документ Банком не принимается.

9.9. Клиент имеет право вносить изменение в содержание представленной Банку ранее Заявки на подключение Сервиса «Мобильный платеж» / отменить Заявку на подключение Сервиса «Мобильный платеж» путем предоставления Банку заявки, сформированной и направленной с использованием Системы по форме 10 Сборника (далее – Заявка на изменение параметров / отключение Сервиса).

В том случае если согласно указанной выше заявке Сервис «Мобильный платеж» подключается к другому мобильному устройству, зарегистрированному в Системе, для ранее зарегистрированного мобильного устройства указанный сервис автоматически отключается. Мобильному устройству, к которому подключен указанный сервис, присваивается соответствующий статус, отображаемый в web-приложении Системы в разделе «Мобильный Банк».

После исполнения Заявки на изменение параметров / отключение Сервиса Банк направляет Клиенту посредством Системы соответствующее уведомление об исполнении с указанием даты, часов и минут по московскому времени, которые фиксируются Системой.

Под исполнением Заявки на изменение параметров / отключение Сервиса понимается завершение Банком технических процедур, необходимых для изменения порядка работы с мобильным приложением «МКБ Бизнес» согласно установленным Клиентом данным.

С даты и времени, указанных в уведомлении об исполнении Банком Заявки на изменение

параметров / отключение Сервиса, ранее представленная в Банк Заявка на подключение Сервиса «Мобильный платеж» считается измененной / отмененной на условиях Заявки на изменение параметров / отключение Сервиса.

В случае отключения Сервиса «Мобильный платеж» в порядке, предусмотренном настоящим пунктом Условий, Клиент продолжает использовать мобильное устройство, зарегистрированное в Системе, для которого указанный сервис отключен, в целях получения информации, предусмотренной п. 2.1 настоящих Условий.

9.10. Информирование Клиента о совершении каждой Операции с использованием Сервиса «Мобильный платеж» осуществляется в соответствии с п. 6.1.6 Правил.

10. Клиент обязан:

10.1. Обеспечить сохранность мобильных устройств от несанкционированного доступа и их использование исключительно Уполномоченными лицами Клиента, а также соблюдение порядка учета, хранения и использования имени пользователя и пароля / короткого кода доступа к мобильному приложению «МКБ Бизнес» / SMS-кода, исключающих несанкционированный доступ посторонних лиц к мобильному приложению «МКБ Бизнес» и совершение Операций с использованием Сервиса «Мобильный платеж».

10.2. В случае угрозы несанкционированного доступа к счетам посредством мобильного устройства, к которому подключен Сервис «Мобильный платеж» согласно пп. 9, 9.9 настоящих Условий, использования Сервиса «Мобильный платеж» без согласия Клиента, в том числе в случае утраты мобильного устройства / прекращения полномочий лица, мобильное устройство которого используется для доступа к счетам с функционалом Сервиса «Мобильный платеж», незамедлительно сообщить об этом в Банк посредством обращения по телефону Контакт-центра.

При получении указанного выше уведомления от Клиента Банк удаляет скомпрометированное мобильное устройство, к которому подключен Сервис «Мобильный платеж», из списка мобильных устройств, зарегистрированных в Системе (отменяет регистрацию мобильного устройства), и прекращает предоставлять доступ к счетам Клиента с мобильного устройства, регистрация которого отменена.

10.3. В случае угрозы несанкционированного доступа к счетам посредством мобильного устройства, на котором мобильное приложение «МКБ Бизнес» используется без подключения Сервиса «Мобильный платеж», в том числе в случае утраты мобильного устройства / прекращения полномочий лица, мобильное устройство которого используется для доступа к счетам, незамедлительно блокировать (прекратить) доступ к счетам одним из следующих способов:

10.3.1. Самостоятельно удалить скомпрометированное мобильное устройство из списка мобильных устройств, зарегистрированных в Системе (отменить регистрацию мобильного устройства), в порядке, указанном в п. 11 настоящих Условий.

В этом случае Банк прекращает предоставлять доступ к счетам с мобильного устройства, регистрация которого отменена.

10.3.2. Обратиться в Банк по телефону Контакт-центра.

При этом в случае предоставления Банку информации об идентификаторе мобильного устройства (зарегистрированном в Системе и отображаемом в web-приложении Системы в разделе «Мобильный Банк»), которое было скомпрометировано, Банк удаляет скомпрометированное мобильное устройство из списка мобильных устройств, зарегистрированных в Системе (отменяет регистрацию мобильного устройства), и прекращает предоставлять доступ к счетам Клиента с мобильного устройства, регистрация которого отменена.

В случае непредоставления Банку информации об идентификаторе мобильного устройства (зарегистрированном в Системе и отображаемом в web-приложении Системы в разделе «Мобильный Банк»), которое было скомпрометировано, Банк прекращает предоставлять доступ к счетам Клиента со всех мобильных устройств, зарегистрированных в Системе на момент указанного обращения Клиента. При этом Банк присваивает указанным мобильным устройствам соответствующий статус, запрещающий доступ к счетам посредством мобильного приложения «МКБ Бизнес» (далее – статус запрещенного доступа), отображаемый в web-приложении Системы в разделе «Мобильный Банк».

Клиент обязан самостоятельно удалить скомпрометированное мобильное устройство из списка мобильных устройств, зарегистрированных в Системе (отменить регистрацию мобильного устройства), а также снять блокировку доступа к счетам Клиента с тех мобильных устройств, с которых доступ к счетам разрешен, в порядке, указанном в п. 11 настоящих Условий.

10.4. В случае компрометации номера телефона, используемого для направления Банком Клиенту SMS-кодов согласно п. 9.3 настоящих Условий, незамедлительно прекратить использование данного номера телефона в указанных целях путем представления в Банк соответствующей заявки, предусмотренной п. 9.9 настоящих Условий.

11. Клиент имеет право:

- прекратить доступ к счетам с мобильного устройства, отменив его регистрацию (удалить мобильное устройство из списка зарегистрированных в Системе мобильных устройств);
- временно блокировать доступ к счетам с мобильного устройства (присвоить данному мобильному устройству статус запрещенного доступа);
- снять блокировку доступа к счетам с мобильного устройства (присвоить данному мобильному устройству статус разрешенного доступа);
- возобновить использование Сервиса «Мобильный платеж» в случае его блокировки, предусмотренной п. 12.2 настоящих Условий (присвоить мобильному устройству, к которому подключен данный сервис, соответствующий статус разрешенного доступа).

Для установления параметров доступа к счетам с мобильных устройств, указанных в настоящем пункте, Клиент совершает соответствующие действия в web-приложении Системы в разделе «Мобильный Банк».

Новые параметры доступа к счетам с мобильных устройств будут установлены только в случае положительного результата процедуры проверки Банком наличия у Клиента действующего сертификата.

12. Банк имеет право:

12.1. Отказать в исполнении заявки, предусмотренной пп. 9, 9.9 настоящих Условий, в случае необходимости обновления идентификационных сведений об Уполномоченном лице Клиента, указанном в п. 9.1 настоящих Условий, а также в случаях, предусмотренных п. 6.2.15 Правил.

12.2. Приостановить направление SMS-сообщений на номер телефона, указанный в заявке, предусмотренной пп. 9, 9.9 настоящих Условий, при наличии у Банка подозрений в несанкционированном использовании данного номера телефона, в том числе при получении информации о замене SIM-карты с данным номером телефона.

При этом Банк приостанавливает использование Клиентом Сервиса «Мобильный платеж» (блокирует) путем присвоения мобильному устройству соответствующего статуса, отображаемого в web-приложении Системы в разделе «Мобильный Банк».

Для возобновления использования Сервиса «Мобильный платеж» Клиент обязан самостоятельно снять указанную в настоящем пункте блокировку данного сервиса в порядке, предусмотренном п. 11 настоящих Условий.

12.3. Приостановить использование Клиентом Сервиса «Мобильный платеж» в случае использования Клиентом Системы с ограниченным функционалом в соответствии с п. 6.2.14 Правил. В этом случае Клиент продолжает использовать мобильное приложение «МКБ Бизнес» для получения информации, предусмотренной п. 2.1 настоящих Условий.

Банк возобновляет доступ Клиента к мобильному приложению «МКБ Бизнес» не позднее даты возобновления обслуживания с использованием Системы в полном объеме в порядке, предусмотренном п. 6.2.14 Правил.

12.4. Отменить регистрацию в Системе мобильного устройства, к которому подключен Сервис «Мобильный платеж» (удалить мобильное устройство из списка зарегистрированных в Системе мобильных устройств), при наличии в Банке информации о прекращении полномочий лица, указанного в п. 9.1 настоящих Условий.

12.5. Заблокировать (прекратить) доступ Клиента к мобильному приложению «МКБ Бизнес» в случаях блокирования использования Системы по инициативе Банка / Клиента в соответствии с пп. 6.1.10, 6.2.10–6.2.13, 6.4.3 Правил.

Банк возобновляет доступ Клиента к мобильному приложению «МКБ Бизнес» не позднее даты снятия блокировки Системы в порядке, указанном в Правилах.

12.6. Заблокировать (прекратить) доступ Клиента к мобильному приложению «МКБ Бизнес», а также к разделу «Мобильный Банк» в web-приложении Системы в случае нарушения Клиентом настоящих Условий / Правил.

Банк возобновляет доступ Клиента к мобильному приложению «МКБ Бизнес» в полном объеме после устранения Клиентом указанных в настоящем пункте нарушений.

13. Клиент несет ответственность за использование мобильных устройств, зарегистрированных им в Системе, исключительно Уполномоченными лицами Клиента.

Банк не несет ответственности за последствия доступа к счетам посредством мобильного приложения «МКБ Бизнес», совершение Операций с использованием Сервиса «Мобильный платеж» неуполномоченными лицами в случае нарушения Клиентом обязанностей, установленных пп. 10.1, 10.2 настоящих Условий.

14. Банк не несет ответственности за ущерб, возникший вследствие передачи Клиентом / Уполномоченным лицом Клиента третьим лицам мобильного устройства, логина, пароля / короткого кода доступа к мобильному приложению «МКБ Бизнес» / SMS-кода, вне зависимости от причин.

15. Банк не несет ответственности за сбои и помехи в работе линий и средств связи, приводящие к невозможности доступа и использования мобильного приложения «МКБ Бизнес».

16. Банк не несет ответственности за сбои в работе мобильного приложения «МКБ Бизнес», обусловленные неисправностью мобильного устройства, нарушением работоспособности установленного на мобильном устройстве программного обеспечения, производителем которого Банк не является, или иными внешними факторами, в том числе повреждением мобильного приложения «МКБ Бизнес», установленного на мобильном устройстве.

17. Стороны могут прекратить действие настоящих Условий в одностороннем порядке с обязательным письменным уведомлением другой Стороны.

17.1. Банк уведомляет Клиента о прекращении услуги доступа к мобильному приложению «МКБ Бизнес» путем направления Клиенту уведомления на бумажном носителе или посредством Системы не позднее чем за 10 (Десять) календарных дней до даты предполагаемого отключения. В этом случае Банк отключает доступ к мобильному приложению «МКБ Бизнес» с даты, указанной в уведомлении.

17.2. Клиент уведомляет Банк о прекращении услуги доступа к мобильному приложению «МКБ Бизнес» путем предоставления Заявки на дополнительные услуги либо заявки, сформированной (форма 10 Сборника) и направленной посредством Системы. В этом случае Банк отключает доступ к мобильному приложению «МКБ Бизнес» не позднее рабочего дня, следующего за днем получения указанной заявки.

18. Настоящие Условия автоматически прекращают действие в случае прекращения Договора.

19. Настоящие Условия и все приложения к ним являются неотъемлемой частью Правил.

20. Термины и определения, используемые в настоящих Условиях, значения которых не указаны, имеют те же значения, что и соответствующие термины и определения, содержащиеся в Правилах.

Приложение 2
к Правилам обслуживания банковских счетов,
открытых в ПАО «МОСКОВСКИЙ
КРЕДИТНЫЙ БАНК», с использованием
электронной системы «Ваш Банк Онлайн»
(версия 2)

**Сборник форм документов, предусмотренных Правилами обслуживания банковских
счетов, открытых в ПАО «МОСКОВСКИЙ КРЕДИТНЫЙ БАНК», с использованием
электронной системы «Ваш Банк Онлайн» (версия 2)**

Форма 1
Сборника типовых форм документов,
предусмотренных Правилами обслуживания
банковских счетов, открытых в
ПАО «МОСКОВСКИЙ КРЕДИТНЫЙ БАНК», с
использованием электронной системы «Ваш Банк
Онлайн» (версия 2)

В ПАО «МОСКОВСКИЙ КРЕДИТНЫЙ БАНК»

**ЗАЯВКА-ДОВЕРЕННОСТЬ
на предоставление сертификата и доступа к Системе
(основной функционал)**

« ____ » _____ 20 ____ г.

Место составления ЗАЯВКИ-ДОВЕРЕННОСТИ
(указывается в случае ее оформления в части доверенности):

_____ *город (село, поселок, район), край, область, республика, автономная область, автономный округ полностью*

Настоящим _____ (далее – Клиент),
в соответствии с договором на обслуживание счетов с использованием электронной системы «Ваш Банк
Онлайн» № _____ от « ____ » _____ 20 ____ г. (далее – Договор), условия которого определены в
Правилах обслуживания банковских счетов, открытых в ПАО «МОСКОВСКИЙ КРЕДИТНЫЙ БАНК», с
использованием электронной системы «Ваш Банк Онлайн» (далее – Правила), являющихся неотъемлемой
частью Договора, просит Банк:

1. Зарегистрировать в Системе Уполномоченное лицо Клиента / Клиента (далее при совместном
упоминании – Уполномоченное лицо) и предоставить сертификат на основании предоставленного в Банк
запроса на его изготовление согласно следующей информации о владельце сертификата:

Наименование (сокращенное) Клиента* / Фамилия, имя, отчество (при наличии) Клиента**:

ИНН / КИО***: _____

Место нахождения****: _____

Уполномоченное лицо Клиента*****: _____

* Клиент – юридическое лицо.

** Клиент – индивидуальный предприниматель / физическое лицо, занимающееся в установленном законодательством
Российской Федерации порядке частной практикой (далее – физическое лицо).

*** КИО – код иностранной организации.

**** Юридический адрес Клиента.

***** Для Клиента – юридического лица поле обязательно к заполнению.

Сведения об основном документе, удостоверяющем личность Уполномоченного лица:

наименование _____, серия и номер _____, наименование органа,
выдавшего документ _____

дата выдачи « ____ » _____ г., код подразделения (при наличии) _____.
Дата рождения Уполномоченного лица (указывается в случае оформления ЗАЯВКИ-ДОВЕРЕННОСТИ в части доверенности): _____.

2. Направить Уполномоченному лицу учетные данные для доступа в Личный кабинет и Систему.
Мобильный телефон: +7 (____) _____.
E-mail (адрес электронной почты): _____.

Передавать на указанный номер телефона SMS-коды, используемые для подписания от имени Клиента документов в Личном кабинете, а также иную информацию в рамках использования Личного кабинета. Клиент подтверждает и гарантирует, что указанные в настоящей ЗАЯВКЕ-ДОВЕРЕННОСТИ номер телефона и адрес электронной почты принадлежат Уполномоченному лицу.

3. Установить в Системе Кодовое слово Уполномоченного лица: _____.

4. Предоставить USB-токен (Рутокен) (заполняется на бумажном носителе):

ДА

НЕТ, при этом Клиент подтверждает и гарантирует, что располагает USB-токеном (Рутокеном), предназначенным для хранения ключей ЭП согласно требованиям Банка.

Нижеследующее положение доверенности применяется в отношении:

– Уполномоченного лица, не являющегося единоличным исполнительным органом Клиента – юридического лица;

– Уполномоченного лица, наделенного Клиентом – физическим лицом полномочиями работать в Системе. В случае наделения Уполномоченного лица правом подписи документов настоящая ЗАЯВКА-ДОВЕРЕННОСТЬ должна быть нотариально удостоверена.

Настоящим Клиент предоставляет Уполномоченному лицу без права передоверия на срок до « ____ » _____ 20 ____ г. (включительно) полномочия формировать ключ ЭП и ключ проверки ЭП Клиента, осуществлять от имени Клиента электронный документооборот с Банком, используя аналог собственноручной подписи (ЭП), в том числе направлять запрос на изготовление сертификата, в котором указано данное Уполномоченное лицо, получать сертификат и направлять подтверждение о его получении, а также следующие полномочия по работе с Системой:

Объем полномочий	Подпись руководителя Клиента (проставляется на бумажном носителе)* / Нужно отметить знаком «V» (проставляется в Системе)**
Разграничение прав доступа к Системе (администрирование)	
Право подписи	
а также право совершать сделки с Банком, в том числе заключать договоры банковского счета / дистанционного банковского обслуживания / депозита, подписывать дополнения и изменения к Договору и иным договорам, заявки, заявления, акты и иные документы, предусмотренные указанными договорами, кроме ЗАЯВОК-ДОВЕРЕННОСТЕЙ	
а также право распоряжаться денежными средствами, находящимися на счетах Клиента	
Доступ без права подписи	

* Зачеркнутое считается ненаписанным.

** Каждое поле, в котором проставлен знак «V», считается подписанным электронной подписью Клиента.

Клиент подтверждает, что ознакомлен и согласен с действующими Тарифами, Правилами, в том числе с порядком предоставления Уполномоченному лицу сертификата и доступа к Системе.

Клиент согласен, что термины и определения, используемые в настоящей ЗАЯВКЕ-ДОВЕРЕННОСТИ, имеют те же значения, что и соответствующие термины и определения, указанные в Правилах.

Клиент согласен с тем, что ранее представленная в Банк ЗАЯВКА-ДОВЕРЕННОСТЬ на предоставление сертификата и доступа к Системе (при ее наличии) на Уполномоченное лицо, указанное в настоящей ЗАЯВКЕ-ДОВЕРЕННОСТИ, утрачивает силу с даты исполнения Банком настоящей ЗАЯВКИ-ДОВЕРЕННОСТИ в порядке, установленном Правилами.

От имени Клиента (заполняется на бумажном носителе):

_____ (должность руководителя, фамилия, имя, отчество)
действующ _____ на основании _____
(наименование документа, подтверждающего полномочия)

_____ (подпись) _____ (расшифровка подписи)
МП

Отметки Банка (заполняется на бумажном носителе):

Получено: « ____ » _____ 20 ____ г.

_____ (наименование должности) _____ (подпись) _____ (расшифровка подписи)

Принято к исполнению: « ____ » _____ 20 ____ г.

_____ (наименование должности) _____ (подпись) _____ (расшифровка подписи)

Форма 2
Сборника типовых форм документов,
предусмотренных Правилами обслуживания
банковских счетов, открытых в
ПАО «МОСКОВСКИЙ КРЕДИТНЫЙ БАНК», с
использованием электронной системы «Ваш Банк
Онлайн» (версия 2)

Формируется в Личном кабинете

В ПАО «МОСКОВСКИЙ КРЕДИТНЫЙ БАНК»

Запрос на изготовление сертификата

« ____ » _____ 20 ____ г.

Прошу изготовить сертификат ключа проверки электронной подписи (далее – сертификат) на основании ЗАЯВКИ-ДОВЕРЕННОСТИ на предоставление сертификата и доступа к Системе от « ____ » _____ 20 ____ г., являющейся неотъемлемой частью договора на обслуживание счетов с использованием электронной системы «Ваш Банк Онлайн» от « ____ » _____ 20 ____ г. № _____ (далее – Договор), в соответствии с указанными сведениями:

Сведения о владельце сертификата:

Наименование юридического лица* / Фамилия, имя и отчество (при наличии)**:

ИНН / КИО _____

Место нахождения: _____

Уполномоченное лицо: _____

* Для владельца сертификата – юридического лица.

** Для владельца сертификата – физического лица.

Ключ проверки электронной подписи (открытый ключ):

Подтверждаю, что ознакомлен и согласен с действующими Правилами обслуживания банковских счетов, открытых в ПАО «МОСКОВСКИЙ КРЕДИТНЫЙ БАНК», с использованием электронной системы «Ваш Банк Онлайн», являющимися неотъемлемой частью Договора, в том числе с порядком использования Личного кабинета и получения сертификата.

Запрос на изготовление сертификата направил: _____

Форма 3
Сборника типовых форм документов,
предусмотренных Правилами обслуживания
банковских счетов, открытых в
ПАО «МОСКОВСКИЙ КРЕДИТНЫЙ БАНК», с
использованием электронной системы «Ваш Банк
Онлайн» (версия 2)

Формируется в Личном кабинете

В ПАО «МОСКОВСКИЙ КРЕДИТНЫЙ БАНК»

Подтверждение о получении сертификата

« ____ » _____ 20 ____ г.

Настоящим подтверждаю получение сертификата ключа проверки электронной подписи (далее – сертификат) на основании ЗАЯВКИ-ДОВЕРЕННОСТИ на предоставление сертификата и доступа к Системе от « ____ » _____ 20 ____ г., являющейся неотъемлемой частью договора на обслуживание счетов с использованием электронной системы «Ваш Банк Онлайн» № _____ от « ____ » _____ 20 ____ г. (далее – Договор), при этом:

1. Подтверждаю, что принял от Банка сертификат в форме электронного документа со следующими параметрами:

Уникальный номер сертификата: _____

Дата начала срока действия сертификата: _____

Дата окончания срока действия сертификата: _____

Сведения о владельце сертификата:

Наименование юридического лица* / Фамилия, имя и отчество (при наличии)**: _____

ИНН / КИО _____

Место нахождения: _____

Уполномоченное лицо: _____

* Для владельца сертификата – юридического лица.

** Для владельца сертификата – физического лица.

Ключ проверки электронной подписи (открытый ключ):

2. Подтверждаю, что содержащийся в сертификате ключ проверки электронной подписи используется для проверки подлинности электронной подписи на документе, полученном Банком посредством электронной системы «Ваш Банк Онлайн», а также иных сервисов электронного документооборота при наличии соответствующих договоров / соглашений, заключенных между Банком и Клиентом (далее – системы ДБО).

Согласен, что Банк обеспечивает возможность использования в системах ДБО электронной подписи, удостоверенной сертификатом, не позднее рабочего дня, следующего за днем принятия Банком настоящего Подтверждения о получении сертификата в соответствии с условиями Договора.

3. Подтверждаю, что ознакомлен и согласен с Правилами безопасного использования систем ДБО, размещенными на сайте Банка и являющимися неотъемлемой частью Договора.

Подтверждение о получении сертификата направил: _____

Форма 4
Сборника типовых форм документов,
предусмотренных Правилами обслуживания
банковских счетов, открытых в
ПАО «МОСКОВСКИЙ КРЕДИТНЫЙ БАНК», с
использованием электронной системы «Ваш Банк
Онлайн» (версия 2)

АКТ приема-передачи

г. Москва

« _____ » _____ 20 ____ г.

ПАО «МОСКОВСКИЙ КРЕДИТНЫЙ БАНК», именуемое в дальнейшем «Банк», в лице _____, действующ _____ на основании _____, с одной стороны, и _____, именуем _____ в дальнейшем «Клиент», в лице _____, действующ _____ на основании _____, с другой стороны, далее вместе именуемые «Стороны», составили настоящий Акт о нижеследующем:

1. Банк передал, а Клиент принял USB-токен (Рутокен) в количестве _____ штук (и).
Серийный (е) номер (а) _____.

2. Настоящий Акт является неотъемлемой частью договора на обслуживание счетов с использованием электронной системы «Ваш Банк Онлайн» № _____ от « _____ » _____ 20 ____ г. (далее – Договор), в том числе Правил обслуживания банковских счетов, открытых в ПАО «МОСКОВСКИЙ КРЕДИТНЫЙ БАНК», с использованием электронной системы «Ваш Банк Онлайн», являющихся неотъемлемой частью Договора.

3. Настоящий Акт составлен в 2 (Двух) экземплярах, имеющих равную юридическую силу, по одному экземпляру для каждой из Сторон.

4. Подписи Сторон

От имени Банка:

От имени Клиента:

(подпись)

(расшифровка подписи)

МП

(подпись)

(расшифровка подписи)

МП

Форма 5
Сборника типовых форм документов,
предусмотренных Правилами обслуживания
банковских счетов, открытых в
ПАО «МОСКОВСКИЙ КРЕДИТНЫЙ БАНК», с
использованием электронной системы «Ваш Банк
Онлайн» (версия 2)

В ПАО «МОСКОВСКИЙ КРЕДИТНЫЙ БАНК»

ЗАЯВЛЕНИЕ*
о предоставлении сервиса дополнительной аутентификации клиента по SMS-коду

** Термины и определения, используемые в настоящем Заявлении, имеют те же значения, что и соответствующие термины и определения, указанные в Правилах обслуживания банковских счетов, открытых в ПАО «МОСКОВСКИЙ КРЕДИТНЫЙ БАНК», с использованием электронной системы «Ваш Банк Онлайн» (далее – Правила).*

« ____ » _____ 20 ____ г.

Настоящим _____, ИНН _____ (далее – Клиент)
просит Банк в соответствии с договором на обслуживание счетов с использованием электронной системы «Ваш Банк Онлайн» № _____ от « ____ » _____ 20 ____ г. (далее – Договор), условия которого определены в Правилах, являющихся неотъемлемой частью Договора, предоставить следующий сервис:
(нужное отметить в соответствующей ячейке)

<p>Предоставить сервис дополнительной аутентификации Клиента по SMS-коду. Прошу осуществлять передачу SMS-сообщений, содержащих одноразовые коды аутентификации, на следующие номера телефонов*:</p> <p>1) _____; 2) _____; 3) _____.</p> <p>Согласен, что с даты, часов и минут по московскому времени, указанных в направленном Банком посредством Системы уведомлении об исполнении настоящего Заявления, Банк осуществляет передачу SMS-сообщений, содержащих одноразовые коды аутентификации для осуществления дополнительной аутентификации Клиента, на указанные номера телефонов.</p> <p>Подтверждаю и гарантирую, что номера телефонов, указанные в настоящем Заявлении, принадлежат лицам, уполномоченным на получение информации, предусмотренной п. 2.16.3 Правил</p>	
<p>Изменить телефонные номера, используемые Банком для передачи Клиенту SMS-сообщений, содержащих одноразовые коды аутентификации. Прошу осуществлять передачу SMS-сообщений, содержащих одноразовые коды аутентификации, на следующие номера телефонов*:</p> <p>1) _____; 2) _____; 3) _____.</p> <p>Согласен, что с даты, часов и минут по московскому времени, указанных в направленном Банком посредством Системы уведомлении об исполнении настоящего Заявления, Банк осуществляет передачу SMS-сообщений, содержащих одноразовые коды аутентификации для осуществления дополнительной аутентификации Клиента, на указанные номера телефонов.</p> <p>Подтверждаю и гарантирую, что номера телефонов, указанные в настоящем Заявлении, принадлежат лицам, уполномоченным на получение информации, предусмотренной п. 2.16.3 Правил</p>	
<p>Прекратить предоставление сервиса дополнительной аутентификации Клиента по SMS-коду.</p>	

Отменить установленный перечень возможных получателей денежных средств, в пользу которых от имени Клиента могут быть совершены переводы денежных средств с использованием Системы без дополнительной аутентификации Клиента по SMS-коду, при его наличии на дату исполнения Банком настоящего Заявления.

Согласен, что с даты, часов и минут по московскому времени, указанных в направленном Банком посредством Системы уведомлении об исполнении настоящего Заявления, Банк не осуществляет дополнительную аутентификацию Клиента

** Клиент может указать не более 3 (Трех) номеров телефонов, которые будут использоваться Банком для передачи Клиенту SMS-сообщений, содержащих одноразовые коды аутентификации.*

Клиент подтверждает, что на дату подачи настоящего Заявления ознакомлен и согласен с Правилами, в том числе с порядком осуществления Банком дополнительной аутентификации по SMS-коду, определенным Правилами.

От имени Клиента (заполняется на бумажном носителе):

_____ (должность руководителя, фамилия, имя, отчество)
действующ _____ на основании _____
(наименование документа, подтверждающего полномочия)

_____ (подпись) _____ (расшифровка подписи)
МП

Отметки Банка:

Получено: « ____ » _____ 20 ____ г.

_____ (наименование должности) _____ (подпись) _____ (расшифровка подписи)

Принято к исполнению: « ____ » _____ 20 ____ г.

_____ (наименование должности) _____ (подпись) _____ (расшифровка подписи)

Форма ба
Сборника типовых форм документов,
предусмотренных Правилами обслуживания
банковских счетов, открытых в
ПАО «МОСКОВСКИЙ КРЕДИТНЫЙ БАНК», с
использованием электронной системы «Ваш Банк
Онлайн» (версия 2)

Формируется в электронной системе «Ваш Банк Онлайн»

В ПАО «МОСКОВСКИЙ КРЕДИТНЫЙ БАНК»

ЗАЯВЛЕНИЕ*
об установлении / отмене перечня возможных получателей денежных средств

* Термины и определения, используемые в настоящем Заявлении, имеют те же значения, что и соответствующие термины и определения, указанные в Правилах обслуживания банковских счетов, открытых в ПАО «МОСКОВСКИЙ КРЕДИТНЫЙ БАНК», с использованием электронной системы «Ваш Банк Онлайн» (далее – Правила).

« ____ » _____ 20 ____ г.

Настоящим _____, ИНН _____ (далее – Клиент), просит Банк в соответствии с договором на обслуживание счетов с использованием электронной системы «Ваш Банк Онлайн» № _____ от « ____ » _____ 20 ____ г. (далее – Договор), условия которого определены в Правилах, являющихся неотъемлемой частью Договора, установить следующее:

1. Перечень возможных получателей денежных средств, в пользу которых переводы денежных средств по счету Клиента осуществляются с использованием Системы на основании расчетных (платежных) документов, содержащих распоряжения о переводе денежных средств в валюте Российской Федерации, без проведения Банком дополнительной аутентификации Клиента по SMS-коду, несмотря на наличие данного сервиса:

№ п/п	Наименование получателя	ИНН получателя	№ счета получателя	Банк получателя	БИК банка получателя
1	2	3	4	5	6
1					
2					
3					
4					

а также получатели бюджетных средств.

2. Отменить установленный перечень возможных получателей денежных средств, в пользу которых переводы денежных средств по счету Клиента осуществляются с использованием Системы без проведения Банком дополнительной аутентификации Клиента по SMS-коду.

Клиент подтверждает, что на дату подачи настоящего Заявления ознакомлен и согласен с Правилами, в том числе с порядком осуществления Банком дополнительной аутентификации по SMS-коду, определенным Правилами.

Согласен с тем, что с даты, часов и минут по московскому времени, указанных в направленном Банком посредством Системы уведомлении об исполнении настоящего Заявления в части раздела 1, при направлении в Банк с использованием Системы расчетных (платежных) документов от имени

Клиента, содержащих распоряжения о переводе денежных средств в валюте Российской Федерации, Банк:

– не осуществляет дополнительную аутентификацию Клиента по SMS-коду в том случае, если ИНН и номер счета получателя средств, указанные в таких расчетных (платежных) документах, идентичны ИНН и номеру счета получателя, указанного в установленном перечне согласно разделу 1;

– осуществляет дополнительную аутентификацию Клиента по SMS-коду при отсутствии получателя денежных средств в установленном перечне согласно разделу 1.

Согласен с тем, что с даты, часов и минут по московскому времени, указанных в направленном Банком посредством Системы уведомлении об исполнении настоящего Заявления в части раздела 2, Банк осуществляет дополнительную аутентификацию Клиента по SMS-коду только при наличии сомнений в подлинности расчетного (платежного) документа, направляемого в Банк от имени Клиента с использованием Системы.

Форма бб
Сборника типовых форм документов,
предусмотренных Правилами обслуживания
банковских счетов, открытых в
ПАО «МОСКОВСКИЙ КРЕДИТНЫЙ БАНК», с
использованием электронной системы «Ваш Банк
Онлайн» (версия 2)

В ПАО «МОСКОВСКИЙ КРЕДИТНЫЙ БАНК»

ЗАЯВЛЕНИЕ*
об отмене перечня возможных получателей денежных средств

** Термины и определения, используемые в настоящем Заявлении, имеют те же значения, что и соответствующие термины и определения, указанные в Правилах обслуживания банковских счетов, открытых в ПАО «МОСКОВСКИЙ КРЕДИТНЫЙ БАНК», с использованием электронной системы «Ваш Банк Онлайн» (далее – Правила).*

« ____ » _____ 20 ____ г.

Настоящим _____, ИНН _____ (далее – Клиент), просит Банк в соответствии с договором на обслуживание счетов с использованием электронной системы «Ваш Банк Онлайн» № _____ от « ____ » _____ 20 ____ г. (далее – Договор), условия которого определены в Правилах, являющихся неотъемлемой частью Договора, отменить установленный перечень возможных получателей денежных средств, в пользу которых переводы денежных средств по счету Клиента осуществляются с использованием Системы без проведения Банком дополнительной аутентификации Клиента по SMS-коду.

Клиент подтверждает, что на дату подачи настоящего Заявления ознакомлен и согласен с Правилами, в том числе с порядком осуществления Банком дополнительной аутентификации по SMS-коду, определенным Правилами.

Согласен с тем, что с даты, часов и минут по московскому времени, указанных в направленном Банком посредством Системы уведомлении об исполнении настоящего Заявления, Банк осуществляет дополнительную аутентификацию Клиента по SMS-коду только при наличии сомнений в подлинности расчетного (платежного) документа, направляемого в Банк от имени Клиента с использованием Системы.

От имени Клиента:

(должность руководителя, фамилия, имя, отчество)
действующ _____ на основании _____
(наименование документа, подтверждающего полномочия)

(подпись) _____
(расшифровка подписи)

МП

Отметки Банка:

Получено: « ____ » _____ 20 ____ г.

(наименование должности) _____
(подпись) _____
(расшифровка подписи)

Принято к исполнению: « ____ » _____ 20 ____ г.

(наименование должности)

(подпись)

(расшифровка подписи)

Форма 7
Сборника типовых форм документов, предусмотренных Правилами обслуживания банковских счетов, открытых в ПАО «МОСКОВСКИЙ КРЕДИТНЫЙ БАНК», с использованием электронной системы «Ваш Банк Онлайн» (версия 2)

Формируется в электронной системе «Ваш Банк Онлайн»

В ПАО «МОСКОВСКИЙ КРЕДИТНЫЙ БАНК»

ЗАЯВКА*
на установление / отмену перечня разрешенных IP-адресов

** Термины и определения, используемые в настоящей Заявке, имеют те же значения, что и соответствующие термины и определения, указанные в Правилах обслуживания банковских счетов, открытых в ПАО «МОСКОВСКИЙ КРЕДИТНЫЙ БАНК», с использованием электронной системы «Ваш Банк Онлайн» (далее – Правила).*

« ____ » _____ 20 ____ г.

Настоящим _____, ИНН _____ (далее – Клиент), просит Банк в соответствии с договором на обслуживание счетов с использованием электронной системы «Ваш Банк Онлайн» № _____ от « ____ » _____ 20 ____ г. (далее – Договор), условия которого определены в Правилах, являющихся неотъемлемой частью Договора, оказать следующие услуги:

(нужное отметить в соответствующей ячейке)

<p>Установление перечня IP-адресов, с которых могут осуществляться доступ к Системе посредством web-приложений и обмен расчетными (платежными), иными документами с Банком с использованием web-приложений Системы</p> <p>Прошу установить следующий перечень разрешенных IP-адресов*:</p> <p>1) _____;</p> <p>2) _____;</p> <p>3) _____.</p> <p>Согласен, что с даты, часов и минут по московскому времени, указанных в направленном Банком посредством Системы уведомлении об исполнении настоящей Заявки, доступ к Системе посредством web-приложений и обмен расчетными (платежными), иными документами с Банком с использованием web-приложений Системы могут осуществляться только с IP-адресов, содержащихся в перечне, установленном по настоящей Заявке</p>	
<p>Отмена установленного перечня разрешенных IP-адресов</p> <p>Согласен, что с даты, часов и минут по московскому времени, указанных в направленном Банком посредством Системы уведомлении об исполнении настоящей Заявки, доступ к Системе и обмен расчетными (платежными), иными документами с Банком с использованием Системы могут осуществляться с любых IP-адресов</p>	

** В перечне указываются статические IP-адреса. При этом для устройств, находящихся в локальной сети, указывается IP-адрес, используемый локальной сетью для доступа в сеть Интернет (внешний IP-адрес).*

Клиент подтверждает, что на дату подачи настоящей Заявки ознакомлен и согласен с условиями ограничения доступа и использования Системы путем установления перечня разрешенных IP-адресов в порядке, определенном Правилами.

Форма 8
Сборника типовых форм документов, предусмотренных Правилами обслуживания банковских счетов, открытых в ПАО «МОСКОВСКИЙ КРЕДИТНЫЙ БАНК», с использованием электронной системы «Ваш Банк Онлайн» (версия 2)

В ПАО «МОСКОВСКИЙ КРЕДИТНЫЙ БАНК»

ЗАЯВКА*
на предоставление услуги «SMS-информирование по расчетному счету»

** Термины и определения, используемые в настоящей Заявке, имеют те же значения, что и соответствующие термины и определения, указанные в Правилах обслуживания банковских счетов, открытых в ПАО «МОСКОВСКИЙ КРЕДИТНЫЙ БАНК», с использованием электронной системы «Ваш Банк Онлайн» (далее – Правила).*

« ____ » _____ 20 ____ г.

Настоящим _____, ИНН _____ (далее – Клиент), в соответствии с договором на обслуживание счетов с использованием электронной системы «Ваш Банк Онлайн» № _____ от « ____ » _____ 20 ____ г. (далее – Договор), условия которого определены в Правилах, являющихся неотъемлемой частью Договора, просит Банк:

1. Осуществлять SMS-информирование Клиента об остатках и/или операциях по расчетным счетам в валюте Российской Федерации, открытым в Банке (далее – Счета), согласно нижеприведенным параметрам*:

Номер (а) телефона (ов) для передачи SMS-сообщений**: 1) _____; 2) _____		Допустимый период времени передачи SMS-сообщений: <input type="checkbox"/> круглосуточно <input type="checkbox"/> с __ ч. __ мин. по __ ч. __ мин.	
Номер (а) Счета (ов)***: 1) _____; 2) _____			
Списание:		Зачисление:	
при расчетах платежными поручениями****		при расчетах платежными поручениями	
при выдаче наличных денежных средств в кассе Банка		при приеме наличных денежных средств в кассе Банка	
Остаток:		при инкассации денежной наличности силами Банка	
входящий остаток денежных средств на начало операционного дня*****		при внесении наличных денежных средств через ПТС	

* Настоящая Заявка может быть дополнена необходимым количеством таблиц при необходимости установления различных параметров информирования.

** Количество номеров телефонов, которые используются Банком для передачи Клиенту SMS-сообщений, не ограничено.

*** Количество расчетных счетов, по которым Банк направляет Клиенту информацию, не ограничено.

**** Платежные поручения, направляемые в Банк от имени Клиента с использованием Системы.

***** Банк направляет SMS-сообщение с 10:00 часов утра по московскому времени текущего операционного дня.

2. Прекратить SMS-информирование Клиента об остатках и операциях по Счетам.

Подтверждаю и гарантирую, что номера телефонов, указанные в разделе 1 настоящей Заявки, принадлежат лицам, уполномоченным на получение информации об остатках и операциях по Счетам согласно параметрам, указанным в настоящей Заявке.

Согласен, что с даты, часов и минут по московскому времени, указанных в направленном Банком посредством Системы уведомления об исполнении настоящей Заявки в части раздела 1, Банк осуществляет передачу Клиенту SMS-сообщений, содержащих информацию об остатках и/или операциях по Счетам согласно параметрам, указанным в настоящей Заявке.

Согласен, что с даты, часов и минут по московскому времени, указанных в направленном Банком посредством Системы уведомления об исполнении настоящей Заявки в части раздела 2, Банк не осуществляет SMS-информирование Клиента об остатках и операциях по Счетам.

Клиент согласен с тем, что ранее предоставленная в Банк Заявка на предоставление услуги «SMS-информирование по расчетному счету» (при ее наличии) утрачивает силу с даты исполнения Банком настоящей Заявки в порядке, установленном Правилами.

Клиент подтверждает, что на дату подачи настоящей Заявки ознакомлен и согласен с Правилами, в том числе с порядком предоставления Банком услуги «SMS-информирование по расчетному счету», определенным Правилами.

С действующими Тарифами ознакомлен и согласен.

От имени Клиента (заполняется на бумажном носителе):

(должность руководителя, фамилия, имя, отчество)
действующ _____ на основании _____
(наименование документа, подтверждающего полномочия)

(подпись) _____
(расшифровка подписи)

МП

Отметки Банка (заполняется на бумажном носителе):

Получено: «___» _____ 20___ г.

(наименование должности) _____ (подпись) _____ (расшифровка подписи)

Принято к исполнению: «___» _____ 20___ г.

(наименование должности) _____ (подпись) _____ (расшифровка подписи)

Форма 9
Сборника типовых форм документов, предусмотренных Правилами обслуживания банковских счетов, открытых в ПАО «МОСКОВСКИЙ КРЕДИТНЫЙ БАНК», с использованием электронной системы «Ваш Банк Онлайн» (версия 2)

В ПАО «МОСКОВСКИЙ КРЕДИТНЫЙ БАНК»

ЗАЯВКА*
на предоставление услуг по установке / эксплуатации
электронной системы «Ваш Банк Онлайн»

* Термины и определения, используемые в настоящей Заявке, имеют те же значения, что и соответствующие термины и определения, указанные в Правилах обслуживания банковских счетов, открытых в ПАО «МОСКОВСКИЙ КРЕДИТНЫЙ БАНК», с использованием электронной системы «Ваш Банк Онлайн» (далее – Правила).

«__» _____ 20__ г.

Настоящим _____, ИНН _____ (далее – Клиент), просит Банк в соответствии с договором на обслуживание счетов с использованием электронной системы «Ваш Банк Онлайн» № _____ от «__» _____ 20__ г. (далее – Договор), условия которого определены в Правилах, являющихся неотъемлемой частью Договора, оказать следующие услуги:

(нужное отметить в соответствующей ячейке)

1. Блок формируется и заполняется при необходимости	
Услуги с выездом специалиста к Клиенту для установки программной части Системы на оборудование Клиента (в том числе вызов специалиста в процессе эксплуатации Системы)*	
<input type="checkbox"/>	в Москве в пределах МКАД
<input type="checkbox"/>	в Москве за пределами МКАД и в Московской области в пределах автодороги А-107
* В случае если в ходе установки / обслуживания программной части Системы специалистом Банка возникнет конфликт функционирования Системы и программного обеспечения Клиента, могут потребоваться дополнительные мероприятия по настройке программного обеспечения Системы на ПЭВМ Клиента. В случае если указанный конфликт программного обеспечения устранить невозможно, программная часть Системы не может быть установлена на ПЭВМ Клиента. По результатам выполненных работ составляется акт выполненных работ, являющийся основанием для взимания Банком комиссионного вознаграждения.	
Желаемая дата выполнения услуг «__» _____ 20__ г.	
Контактные данные: _____ (контактный телефон) _____ (ФИО контактного лица)	

2. Блок формируется и заполняется при необходимости	
Блокировка / снятие блокировки Системы	
<input type="checkbox"/>	Блокировка* в случае несанкционированного доступа к Системе ** Подтверждаю блокировку «__» _____ 20__ г. при обращении по телефону Банка
<input type="checkbox"/>	Временная блокировка* на срок с «__» _____ 20__ г. до «__» _____ 20__ г. включительно
<input type="checkbox"/>	Снятие временной блокировки (досрочно) «__» _____ 20__ г.***

* Абонентская плата за использование Системы взимается согласно Тарифам.
 ** В случае блокировки Системы по указанным причинам Банк признает все ключи ЭП Клиента недействительными согласно условиям Правил.
 *** В данном поле указывается дата не ранее рабочего дня, следующего за днем предоставления в Банк настоящей Заявки

3. Блок формируется и заполняется при необходимости

Услуги в рамках доступа Уполномоченного лица Клиента к web-приложению Системы (основной функционал)*

Прекращение действия сертификата, выданного Уполномоченному лицу _____ (указать ФИО) согласно Заявке на Уполномоченное лицо от «___» _____ 20___ г.

Подтверждаю уведомление о компрометации ключа ЭП, используемого данным Уполномоченным лицом, при обращении по телефону Банка «___» _____ 20___ г.

Временное приостановление действия сертификата, выданного Уполномоченному лицу _____ (указать ФИО) согласно Заявке на Уполномоченное лицо от «___» _____ 20___ г., на период с «___» _____ 20___ г. до «___» _____ 20___ г. включительно

Замена сертификата при внеплановой смене ключей в процессе эксплуатации Системы
 Прошу предоставить возможность формирования новых ключей и получения сертификата, используемых Уполномоченным лицом _____ (указать ФИО) согласно Заявке на Уполномоченное лицо от «___» _____ 20___ г.

Восстановление пароля доступа к web-приложению Системы
 Прошу направить на номер телефона, указанный в Заявке на Уполномоченное лицо _____ (указать ФИО) от «___» _____ 20___ г., новый пароль доступа к web-приложению Системы

Прекращение действия (отмена) Заявки на Уполномоченное лицо _____ (указать ФИО) от «___» _____ 20___ г. и прекращение возможности формирования ключа ЭП и выдачи сертификата в рамках данной Заявки на Уполномоченное лицо

* В случае необходимости получения услуг в рамках доступа к web-приложению Системы нескольких Уполномоченных лиц Клиента таблица может быть дополнена необходимым количеством полей

4. Блок формируется и заполняется при необходимости

Услуги в рамках мобильного приложения «МКБ Бизнес»

Предоставление доступа к мобильному приложению «МКБ Бизнес» *

Отключение доступа к мобильному приложению «МКБ Бизнес»

* Услуга может быть оказана при наличии у Банка технической возможности.

Клиент, проставляя отметку в любой позиции настоящего блока, подтверждает, что ознакомлен и согласен с *Условиями использования мобильного приложения «МКБ Бизнес» электронной системы «Ваш Банк Онлайн»*, являющимися неотъемлемой частью Правил (приложение 1 к Правилам)

5. Блок формируется и заполняется при необходимости

Прочие услуги:

Предоставление USB-токена для хранения ключей ЭП* (указать количество в цифрах)

* USB-токен (ы) передается (ются) Клиенту по акту приема-передачи, составленному по форме 4 Сборника

Клиент подтверждает, что с действующими на дату подачи настоящей Заявки Правилами, а также Тарифами ознакомлен и согласен.

От имени Клиента:

_____ (должность руководителя, фамилия, имя, отчество)
действующ _____ на основании _____
_____ (наименование документа, подтверждающего полномочия)

_____ (подпись) _____ (расшифровка подписи)

МП

Отметки Банка:

Получено: « ____ » _____ 20 ____ г.

_____ (наименование должности) _____ (подпись) _____ (расшифровка подписи)

Принято к исполнению: « ____ » _____ 20 ____ г.

_____ (наименование должности) _____ (подпись) _____ (расшифровка подписи)

Форма 10
Сборника типовых форм документов, предусмотренных Правилами обслуживания банковских счетов, открытых в ПАО «МОСКОВСКИЙ КРЕДИТНЫЙ БАНК», с использованием электронной системы «Ваш Банк Онлайн» (версия 2)

Формируется в электронной системе «Ваш Банк Онлайн»

ПАО «МОСКОВСКИЙ КРЕДИТНЫЙ БАНК»

ЗАЯВКА*
на предоставление услуг в рамках мобильного приложения «МКБ Бизнес»

** Термины и определения, используемые в настоящей Заявке, имеют те же значения, что и соответствующие термины и определения, указанные в Правилах обслуживания банковских счетов, открытых в ПАО «МОСКОВСКИЙ КРЕДИТНЫЙ БАНК», с использованием электронной системы «Ваш Банк Онлайн» (далее – Правила).*

«__» _____ 20__ г.

Настоящим _____, ИНН _____ (далее – Клиент), просит Банк в соответствии с договором на обслуживание счетов с использованием электронной системы «Ваш Банк Онлайн» № _____ от «__» _____ 20__ г. (далее – Договор), условия которого определены в Правилах, являющихся неотъемлемой частью Договора, оказать следующие услуги:
(нужное отметить в соответствующей ячейке)

Предоставление доступа к мобильному приложению «МКБ Бизнес»*	
<p>Подключение Сервиса «Мобильный платеж» Прошу подключить Сервис «Мобильный платеж» к мобильному устройству, имеющему следующий идентификатор, зарегистрированный в Системе: _____**.</p> <p>Прошу осуществлять передачу SMS-кодов на номер телефона: _____.</p> <p>Согласен, что с даты, часов и минут по московскому времени, указанных в направленном Банком посредством Системы уведомлении об исполнении настоящей Заявки, Банк осуществляет передачу SMS-кодов на указанный номер телефона, а также идентифицирует мобильное устройство, с которого в Банк направляются расчетные (платежные) документы и иная информация, на основе указанного идентификатора мобильного устройства.</p> <p>Подтверждаю и гарантирую, что мобильное устройство и номер телефона, указанные в настоящей Заявке, используются исключительно Уполномоченным лицом Клиента, указанным в п. 9.1 Условий***</p>	
<p>Изменение номера телефона, используемого Банком для передачи SMS-кодов Клиенту Прошу осуществлять передачу SMS-кодов на номер телефона: _____.</p> <p>Согласен, что с даты, часов и минут по московскому времени, указанных в направленном Банком посредством Системы уведомлении об исполнении настоящей Заявки, Банк осуществляет передачу SMS-кодов на указанный номер телефона.</p> <p>Подтверждаю и гарантирую, что номер телефона, указанный в настоящей Заявке, используется исключительно Уполномоченным лицом Клиента, указанным в п. 9.1 Условий***</p>	
Отключение Сервиса «Мобильный платеж»	

Согласен, что с даты, часов и минут по московскому времени, указанных в направленном Банком посредством Системы уведомлении об исполнении настоящей Заявки, Клиент использует мобильное устройство, зарегистрированное в Системе, для которого Сервис «Мобильный платеж» отключен, в целях получения информации, предусмотренной п. 2.1 Условий***	
Отключение доступа к мобильному приложению «МКБ Бизнес»	

* Клиент согласен, что услуга может быть оказана при наличии у Банка технической возможности.

** Проставляется идентификатор мобильного устройства, зарегистрированный в Системе и отображаемый в разделе «Мобильный банк» web-приложения Системы.

*** Условия использования мобильного приложения «МКБ Бизнес» электронной системы «Ваш Банк Онлайн» (приложение 1 к Правилам).

Клиент подтверждает, что с действующими на дату подачи настоящей Заявки Правилами, в том числе Условиями использования мобильного приложения «МКБ Бизнес» электронной системы «Ваш Банк Онлайн», являющимися неотъемлемой частью Правил, а также Тарифами ознакомлен и согласен.