**С О Г Л А Ш Е Н И Е**
**об использовании электронной системы**
**дистанционного банковского обслуживания**

Настоящее Соглашение об использовании электронной системы дистанционного банковского обслуживания (далее – Соглашение) является договором присоединения в соответствии со ст.428 Гражданского кодекса Российской Федерации, и заключается в порядке, установленном настоящим Соглашением.

**Термины и определения**

В настоящем Соглашении следующие определения имеют следующее значение.

**Акт признания Открытого ключа ЭП** - документ на бумажном носителе, выдаваемый Банком Клиенту, в котором Стороны удостоверяют факт передачи Технологических ключей, Сертификата Технологического ключа.

**Банк** – АКЦИОНЕРНЫЙ КОММЕРЧЕСКИЙ БАНК «ЕВРОФИНАНС МОСНАРБАНК» (акционерное общество) (полное наименование), АО АКБ «ЕВРОФИНАНС МОСНАРБАНК» (сокращенное наименование), место нахождения постоянно действующего исполнительного органа – 121099, г. Москва, ул. Новый Арбат, д.29, официальный сайт: www.evrofinance.ru, генеральная лицензия на проведение банковских операций №2402, выданная Банком России 23.07.2015.

**Владелец сертификата ключа проверки ЭП** – Клиент, на имя которого Банком выдан Сертификат Технологического ключа и Сертификат Рабочего ключа.

**Документация** - все руководства, инструкции, рекомендации о мерах безопасности при совершении электронного документооборота в Системе, технические описания и другая документация, касающаяся Системы, которые передаются Банком Клиенту в электронном виде по акту об оказании услуг по установке Системы.

**Договор об использовании ДБО** - договор об использовании электронной системы дистанционного банковского обслуживания (по форме Банка), заключенный между Клиентом и Банком, с помощью которого Клиент присоединяется к Соглашению в целом в соответствии со статьей ст.428 Гражданского кодекса Российской Федерации. Заключение Договора об использовании ДБО осуществляется в порядке, установленном Соглашением.

**Закрытый ключ ЭП** – уникальная последовательность символов, известная только Владельцу сертификата ключа проверки ЭП и Уполномоченному представителю Клиента, предназначенная для создания в Электронных документах ЭП и идентификации Уполномоченного представителя Клиента в Системе, и однозначно связанная с Открытым ключом ЭП.

**Квитанция** – электронное сообщение о приеме Электронного документа Стороны-отправителя Стороной-получателем или смене статуса документа Стороной-получателем в процессе обработки. Получение квитанции в Системе влечет за собой смену статуса документа в Системе Стороны-отправителя.

**Клиент** – юридическое лицо, заключившее с Банком Соглашение путем присоединения к нему.

**Ключ (и)** – совместно или, если указано особо, раздельно, Открытый ключ ЭП, Закрытый ключ ЭП, Секретный и открытый ключи шифрования.

**Кодовое слово** – последовательность символов, известная только Клиенту и Банку, используемая для идентификации Клиента при телефонном разговоре с Клиентом в целях подтверждения/неподтверждения возобновления исполнения операции, соответствующей признакам осуществления перевода денежных средств без согласия Клиента. Кодовое слово может использоваться многократно.

**Компрометация ключей** – возникновение подозрений в том, что используемые Ключи доступны лицам, не имеющим на то полномочий. К событиям, влекущим за собой компрометацию Ключей, относятся, включая, но, не ограничиваясь, следующие события:
- утрата носителей с Ключами;
- утрата носителей с Ключами с последующим обнаружением;
- доступ посторонних лиц (не Уполномоченных представителей Клиента) к Ключам, использование Ключей без согласия Клиента;
- другие события, которые, по мнению Сторон, свидетельствуют о наличии возможности Несанкционированного доступа третьих лиц к Ключам.

**Конфиденциальная информация** – любая информация (сведения), которой Стороны обмениваются в соответствии с настоящим Соглашением и которая носит частный, непубличный и конфиденциальный характер и имеет действительную или потенциальную ценность в силу ее неизвестности третьим лицам.

**Несанкционированный доступ** – доступ к Системе (в том числе, к Электронным документам), ее использование лицами, не имеющими на то полномочий.

**Открытый ключ ЭП** – уникальная последовательность символов, соответствующая Закрытому ключу ЭП, доступная любому пользователю Системы и предназначенная для проверки подлинности ЭП в Электронном документе и его целостности.

**Плановая смена рабочих ключей** – создание Уполномоченным представителем Клиента новых Рабочих ключей, которое осуществляется до истечения срока действия действующего Рабочего ключа.

**Подсистема** – одна из двух подсистем Системы:
- подсистема «Клиент-Банк», в соответствии с которой на персональный компьютер Клиента устанавливается программа «Клиент», которая хранит все свои данные на этом персональном компьютере или на сетевых ресурсах Клиента;
- подсистема «Интернет клиент-банк», в соответствии с которой Клиент, используя стандартный браузер операционной системы своего персонального компьютера, получает доступ к указанной подсистеме и ее данным, размещенным на сервере Банка.

**Проверка ЭП Электронного документа** - проверка соотношения, связывающего хэш-функцию Электронного документа, ЭП такого документа и Открытого ключа ЭП подписавшего абонента. Если такая проверка, произведенная на Средствах защиты информации, даст положительный результат, то ЭП признается правильной, а сам Электронный документ – подлинным, без искажений, в противном случае Электронный документ считается ошибочным, а ЭП под ним - недействительной.

**Рабочий день** – рабочий день, признаваемый таковым применимым к деятельности Сторон законодательством каждой из Сторон.

**Рабочие ключи** – Ключи, предназначенные для подтверждения авторства, целостности и конфиденциальности Электронных документов, передаваемых в Системе. Рабочие ключи формируются Уполномоченным представителем Клиента самостоятельно посредством Системы. Срок действия Рабочих ключей составляет 36 месяцев с даты формирования запроса на создание Сертификата Рабочего ключа.

**Секретный и открытый ключи шифрования** – Ключи, используемые для процедуры шифрования и дешифрования Электронных документов. При шифровании используется открытый ключ Стороны-получателя, при расшифровании секретный ключ Стороны-получателя.

**Сертификат Рабочего ключа** - электронный документ с ЭП Банка, содержащий Открытый ключ ЭП и шифрования, а также сведения, идентифицирующие Уполномоченного представителя Клиента. Сертификат предназначен для подтверждения подлинности ЭП и идентификации Уполномоченного представителя Клиента в Системе.

**Сертификат Технологического ключа** - электронный документ с ЭП Банка, содержащий Открытые ключи ЭП и шифрования, а также сведения, идентифицирующие Уполномоченного представителя Клиента. Сертификат предназначен для создания Рабочих ключей Уполномоченного представителя Клиента в Системе. Выдается Банком Клиенту в электронном виде и на бумажном носителе по Акту признания Открытого ключа ЭП.

**Система** – корпоративная информационная система дистанционного банковского обслуживания, организованная Банком, представляющая собой комплекс программно-технических средств и организационных мероприятий для создания, защиты, передачи и обработки Электронных документов по открытым каналам связи, в том числе с использованием сети Интернет. Система используется как электронное средство платежа и обеспечивает создание ЭП в Электронном документе с использованием Закрытого ключа ЭП, подтверждение подлинности ЭП в Электронном документе с использованием Открытого ключа ЭП, создание Ключей.

**Средства защиты информации** – сертифицированные криптографические средства, обеспечивающие реализацию следующих функций: создание ЭП в Электронном документе с использованием Закрытого ключа ЭП, проверка ЭП Электронного документа с использованием Открытого ключа ЭП, создание Закрытых и Открытых ключей ЭП, а также создание и использование Секретных и открытых ключей шифрования, шифрование и расшифрование.

**Средства обработки и хранения информации** – программно-аппаратные средства, требования к которым приведены в Приложении №1 к Соглашению.

**Сторона (Стороны)** – Банк и/или Клиент.

**Счет Клиента** - счет, открытый Банком Клиенту на момент заключения настоящего Соглашения или счета, которые будут открыты Банком Клиенту в будущем, на основании соответствующих договоров банковского счета (далее – **“ДБС”**), заключенных между Сторонами.

**Тарифы** - размеры вознаграждения Банка за оказываемые по настоящему Соглашению работы и услуги. Тарифы устанавливаются Банком. Действующие на момент заключения настоящего Соглашения Тарифы доводятся до сведения Клиента при заключении настоящего Соглашения, а также по первому требованию Клиента. Тарифы могут быть изменены Банком в одностороннем порядке, о чем Банк уведомляет Клиента не позднее, чем за 5 (пять) Рабочих дней Банка до даты ввода в действие изменений путем размещения информации в операционном зале Банка, на официальном сайте Банка, а также путем передачи указанной информации посредством Системы.

**Технологические ключи** – Ключи Клиента, изготавливаемые Банком и предназначенные для технологической процедуры формирования (подписи) запроса на создание

Сертификата Рабочего ключа и для самостоятельного формирования Рабочих ключей Уполномоченным представителем Клиента, действующие до даты формирования Клиентом Рабочего ключа, либо до истечения 36 месяцев с момента изготовления Банком Технологических ключей.

**Уполномоченный представитель Клиента** – физическое лицо, указанное в Данных о Владельце сертификата ключа проверки ЭП, наделенное Клиентом правом подписания Электронных документов ЭП для последующей передачи посредством Системы и/или входа в Систему, создания любых Электронных документов, установления защищенного соединения с Банком для приема и отправки любых Электронных документов, подписанных ЭП Клиента, и владеющее Закрытым ключом ЭП, позволяющим создавать ЭП в Электронных документах (подписывать Электронные документы) и идентифицировать Уполномоченного представителя Клиента в Системе.

**Хэш-функция** – алгоритм вычисления контрольной последовательности для произвольных электронных сообщений с целью доказательной проверки их целостности.

**Шифрование** – преобразование данных исходных (открытых) сообщений таким образом, что их смысл становится недоступным для любого лица, не владеющего секретом обратного преобразования.

**Расшифрование** – операция обратная шифрованию.

**Электронная подпись (ЭП)** – реквизит Электронного документа, предназначенный для защиты данного Электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием Закрытого ключа ЭП и позволяющий идентифицировать Владельца сертификата ключа проверки ЭП и Уполномоченного представителя Клиента с правом подписи Электронных документов, а также удостовериться в целостности информации Электронного документа. Для выработки и проверки ЭП используются программные Средства защиты информации «OpenSSL». В рамках настоящего Соглашения под Электронной подписью понимается усиленная неквалифицированная электронная подпись.

**Электронный документ** – электронное сообщение, подписанное ЭП и переданное одной из Сторон другой Стороне посредством Системы, в котором информация представлена в электронной форме, равнозначное документу на бумажном носителе, подписанному собственноручной подписью (собственноручными подписями) уполномоченных лиц Сторон и скрепленному печатью (при ее наличии) в случае необходимости.

## Статья 1. Предмет Соглашения.

1.1. Стороны устанавливают между собой порядок и условия обмена Электронными документами по Системе в целях проведения на основании Электронных документов банковских операций (в том числе расчетных) по Счетам Клиента, а также осуществления депозитарных операций, заключения договоров банковского вклада (депозита), заключения иных сделок и осуществления других действий в соответствии с условиями заключенных между Сторонами ДБС и иных соглашений, осуществления Банком функций агента валютного контроля, предоставления в Банк документов, необходимых для осуществления Банком функций, установленных законодательством Российской Федерации о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма.

1.2. Информационный обмен в рамках Системы осуществляется по открытым каналам связи, в том числе с использованием сети Интернет.

1.3. Для обеспечения конфиденциальности Электронного документа при передаче по открытым каналам связи, а также для обеспечения авторства и целостности Электронного документа, в Системе используется Средство защиты информации «OpenSSL».
1.4. Клиент согласен с тем, что использование Средства защиты информации «OpenSSL» в качестве средства обеспечения конфиденциальности при передаче по открытым каналам связи, а также для обеспечения авторства и целостности Электронного документа, является достаточным, т.е. обеспечивающим защиту интересов Клиента.
1.5. Клиент отказывается от предъявления претензий к Банку, основанием которых является использование «OpenSSL» в качестве средства защиты Электронного документа от несанкционированного доступа при передаче по открытым каналам связи, а также для обеспечения авторства и целостности Электронного документа.

**Статья 2. Общие положения.**

2.1.Система будет использоваться для обмена Электронными документами в любом формате, за исключением архивных файлов, таких как: zip, 7z, arj, rar и аналогичных им. Формирование Электронных документов и обмен ими будет осуществляться в соответствии с требованиями Документации. Любая информация, передаваемая Сторонами по Системе, обрабатывается Средствами защиты информации.
2.2. Стороны признают, что используемые во взаимоотношениях между ними Электронные документы, подписанные ЭП, имеют равную юридическую силу с документами на бумажном носителе, подписанными собственноручными подписями уполномоченных лиц Сторон и скрепленными печатями в случае необходимости, и являются достаточным основанием для выполнения Банком операций, действий, а также для совершения Сторонами сделок, предусмотренных ДБС, Соглашением, иными соглашениями между Сторонами.
2.3. Стороны признают, что используемые ими по настоящему Соглашению способы доставки, указанные в Приложении №2 к Соглашению, Средства обработки и хранения информации достаточны для обеспечения надежной и эффективной работы по приему, передаче и хранению информации.
2.4. Электронный документ порождает обязательства Сторон по настоящему Соглашению, ДБС, а также иным соглашениям между Банком и Клиентом, является офертой или акцептом, если он оформлен передающей Стороной в соответствии с настоящим Соглашением, ДБС, иными соглашениями между Банком и Клиентом и Документацией, подписан ЭП и передан посредством Системы, а принимающей Стороной получен, и Проверка ЭП Электронного документа дала положительный результат.

Электронные документы не могут быть оспорены или отрицаться Сторонами и третьими лицами или быть признаны недействительными только на том основании, что они переданы в Банк с использованием Системы и способов доставки.

2.5. Банк и Клиент используют Систему для передачи Электронных документов друг другу в приоритетном порядке, при этом использование Системы не ограничивает права Клиента по предоставлению в Банк платежных, иных документов на бумажном носителе, составленных в соответствии с ДБС, Соглашением, иными соглашениями между Банком и Клиентом. Настоящим Стороны соглашаются с тем, что в случае поступления в Банк Электронного документа по Системе и соответствующего платежного, иного документа на бумажном носителе, содержащих идентичные условия проведения операции, осуществления соответствующих действий, в том числе, по Счету, счету депо, счету по вкладу (депозиту) либо поступления в Банк идентичных Электронных документов, Банк будет рассматривать каждый из указанных документов как самостоятельный платежный, иной документ, и осуществит все действия, необходимые для проведения операции, осуществления соответствующих сделок, действий, в том числе, по Счету, счету депо, счету по вкладу (депозиту), в соответствии с каждым из представленных/переданных Клиентом документов.
2.6. Внутренние процедуры использования Клиентом Системы и его внутренний документооборот устанавливаются Клиентом самостоятельно.

2.7. Клиент уведомлен о том, что информация, передаваемая Банком посредством Системы, не является информацией «в реальном времени».

**Статья 3. Порядок подключения Клиента к Системе и Плановой смены Рабочих ключей.**

3.1. Для участия в обмене Электронными документами:
3.1.1.Клиент выполняет следующие действия:

а) заполняет заявку на установку Системы, где указывает необходимую Подсистему и передает ее в Банк на бумажном носителе;

б) назначает и наделяет соответствующими полномочиями физических лиц, ответственных за осуществление обмена Электронными документами, в том числе:
- Уполномоченного представителя Клиента,
- администратора Системы – лицо, ответственное за техническую поддержку Системы;

в) для каждого Уполномоченного представителя Клиента заполняет и представляет в Банк 2 (два) экземпляра Данных о Владельце сертификата ключа проверки ЭП (по форме Приложения №5 к Соглашению) с приложением заверенной Банком/нотариально (в случае необходимости с проставлением апостиля/при условии ее легализации) копии документа, удостоверяющего личность Уполномоченного представителя Клиента и/или документа, подтверждающего право лица на пребывание (проживание) в Российской Федерации и/или миграционной карты, – для иностранных граждан и лиц без гражданства. При этом Банк проставляет отметки о получении на каждом экземпляре Данных о Владельце сертификата ключа проверки ЭП.

Для Уполномоченных представителей Клиента с полномочиями «без права подписи» документ, удостоверяющий личность Уполномоченного представителя Клиента и/или документ, подтверждающий право лица на пребывание (проживание) в Российской Федерации и/или миграционная карта, – для иностранных граждан и лиц без гражданства - могут быть представлены в Банк в копиях, заверенных в порядке, установленном Банком.

Документы, представляемые Клиентом и составленные на иностранном языке, должны сопровождаться переводом на русский язык, за исключением случаев установленных законодательством Российской Федерации. Перевод на русский язык должен быть заверен в порядке, установленном законодательством Российской Федерации;

г) обеспечивает наличие и приведение оборудования, предназначенного для установки Системы, в соответствие с требованиями к аппаратно-программным средствам, приведенными в Приложении №1 к Соглашению.

3.1.2. Банк выполняет следующие действия:

а) изготавливает Технологические ключи на каждого Уполномоченного представителя Клиента в течение 5-и (пяти) Рабочих дней Банка со дня принятия Банком данных по форме Приложения №5 к Соглашению;

б) передает Клиенту Технологические ключи; Акт признания Открытого ключа ЭП в двух экземплярах и один экземпляр Данных о Владельце сертификата ключа проверки ЭП с отметкой Банка, поставленной в соответствии с подпунктом в) п.3.1.1 Соглашения; пароль для входа в подсистему «Интернет клиент-банк» и информацию об адресе для входа в подсистему «Интернет клиент-банк» (при выборе Клиентом подсистемы «Интернет клиент-банк»), а также Документацию в электронном виде;

в) консультирует Клиента по вопросам установки Системы после проведения Клиентом подготовительных мероприятий, перечисленных в п.3.1.1 Соглашения. После завершения всех работ по подключению Клиента к Системе Стороны подписывают соответствующий акт на бумажном носителе;

г) по желанию Клиента, проводит в своем помещении занятия по обучению эксплуатации Системы с лицами, уполномоченными Клиентом, в согласованные Сторонами сроки.

3.2. Документы, указанные в п.3.1, п.3.4, п.3.6 Соглашения, а также документы, которые в соответствии с Соглашением Стороны обязаны предоставлять друг другу на бумажном носителе, Стороны вправе передавать друг другу через уполномоченного представителя или с помощью почты DHL, иной аналогичной почтовой службы.

3.3. После получения Клиентом Технологических ключей Стороны проводят мероприятия, в ходе которых проверяется (тестируется) следующее:

- наличие постоянной и устойчивой связи при работе Системы;
- работа всех основных функций программного обеспечения Системы;
- бессбойная работа Средств защиты информации;
- получение и передача Электронных документов, а также формирование архивов полученных и отправленных Электронных документов.

3.4. После успешного тестирования Системы:

- Клиент:

  - создает Рабочие ключи и электронный запрос на создание Сертификата Рабочего ключа;

  - направляет в Банк электронный запрос на создание Сертификата Рабочего ключа;

  - по каждому из Уполномоченных представителей Клиента заверяет собственноручной подписью уполномоченного лица Клиента и печатью Клиента (при ее наличии) полученный от Банка Акт признания Открытого ключа ЭП и передает один экземпляр указанного акта в Банк вместе с Актом признания открытого ключа (сертификата) для обмена сообщениями (по форме Приложения №6 к Соглашению), распечатанным из Системы, в двух экземплярах.

- Банк:

  - проставляет отметку о получении на каждом экземпляре принятого от Клиента Акта признания открытого ключа (сертификата) для обмена сообщениями (Приложение №6 к Соглашению);

  - в течении двух Рабочих дней Банка при условии принятия Акта признания открытого ключа (сертификата) для обмена сообщениями (Приложение №6 к Соглашению), полученного от Клиента в двух экземплярах, изготавливает Сертификат Рабочего ключа на основании электронного запроса Клиента на создание Сертификата Рабочего ключа;

  - направляет Клиенту Сертификат Рабочего ключа.

3.5. Клиент принимает от Банка в Системе Сертификат Рабочего ключа и отправляет в Банк извещение о начале передачи Электронных документов в рабочем режиме в виде Электронного документа, подписанного Рабочим ключом.

Банк начинает обслуживание Клиента с использованием Системы в рабочем режиме с момента получения от Клиента посредством Системы первого Электронного документа, подписанного Рабочим ключом.

3.6. При плановой смене Рабочих ключей:

- Клиент:

  - создает и направляет в Банк электронный запрос на создание нового Сертификата Рабочего ключа;

  - предоставляет в Банк на бумажном носителе Акт признания открытого ключа (сертификата) для обмена сообщениями (по форме Приложения №6 к Соглашению) в двух экземплярах:

  - принимает от Банка в Системе новый Сертификат Рабочего ключа.

- Банк:

  - проставляет отметку о получении на каждом экземпляре принятого от Клиента Акта признания открытого ключа (сертификата) для обмена сообщениями (Приложение №6 к Соглашению);

  - в течение двух Рабочих дней Банка при условии принятия Акта признания открытого ключа (сертификата) для обмена сообщениями (Приложение №6 к Соглашению), полученного от Клиента в двух экземплярах, изготавливает новый

Сертификат Рабочего ключа на основании электронного запроса Клиента на создание нового Сертификата Рабочего ключа;
- направляет Клиенту новый Сертификат Рабочего ключа.

3.7. Банк, обладая соответствующими правами, предоставленными ему в соответствии с договором, заключенным между Банком и ООО «БСС», предоставляет Клиенту право на пользование Системой в течение действия настоящего Соглашения. Право на пользование предоставляется с учетом ограничений, предусмотренных законодательством Российской Федерации о правовой охране программ для ЭВМ.

## Статья 4. Права и обязанности Сторон.

### 4.1. Взаимные права и обязанности Сторон.

4.1.1. Стороны при обмене Электронными документами с использованием Системы обязуются руководствоваться правилами и требованиями, установленными законодательством Российской Федерации, ДБС, настоящим Соглашением, иными соглашениями между Банком и Клиентом.
4.1.2. Стороны обязуются не разглашать третьей стороне (за исключением случаев, предусмотренных законодательством Российской Федерации и настоящим Соглашением) информацию о Средствах защиты информации, используемых в Системе.
4.1.3. Каждая из Сторон обязуется немедленно информировать другую Сторону обо всех случаях Компрометации ключей, несанкционированного использования Системы, а также повреждениях/утраты программно-аппаратных средств обработки, хранения, передачи Электронных документов, Средств защиты информации, а также Ключей и не использовать Ключи при наличии оснований полагать, что они скомпрометированы.
4.1.4. Средства защиты информации Электронных документов, предоставленные Системой, признаются Сторонами достаточными для защиты информации от несанкционированного доступа, подтверждения авторства и подлинности Электронных документов.
4.1.5. Любые Электронные документы, передаваемые по Системе, подлежат шифрованию.
4.1.6. Любые Электронные документы, передаваемые по Системе должны быть заверены ЭП Стороны - отправителя.
4.1.7. Какие-либо ограничения полномочий Уполномоченного представителя Клиента, в т.ч. указанные в соответствующих Данных о Владельце сертификата ключа проверки ЭП, Банком не признаются и не контролируются, если иное не установлено соглашением между Клиентом и Банком. Банк не осуществляет контроль за суммами платежей, суммами сделок, осуществляемых Уполномоченными представителями Клиента в соответствии с ДБС, Соглашением, иными соглашениями между Сторонами.

### 4.2. Права и обязанности Клиента.

4.2.1. Клиент не имеет права тиражировать и передавать третьей стороне программное обеспечение, предоставляемое Банком по Соглашению и все конфиденциальные данные, относящиеся к Соглашению.
4.2.2. Клиент имеет право, при необходимости, воспользоваться помощью специалиста Банка для устранения неполадок, возникших в Системе, направив в Банк письменную заявку. По результатам работы специалиста Банка Стороны подписывают акт об оказании услуг на бумажном носителе.
4.2.3. Клиент обязуется в сроки, предусмотренные Соглашением, обеспечить на своем расчетном и/или иных счетах, открытых в Банке, остаток денежных средств в размере, необходимом для оплаты услуг Банка в соответствии с Соглашением и Тарифами.
4.2.4. Клиент обязуется обеспечивать сохранность и целостность установленной Системы, включая Средства защиты информации, а также выполнять требования к эксплуатации Системы, изложенные в Документации.
4.2.5. Клиент по требованию Банка обязан предоставить оригиналы документов на бумажном носителе, преобразованных в Электронные документы и переданных по Системе, в течение 14 (четырнадцати) календарных дней с момента направления ему

требования. Документы на бумажном носителе должны быть подписаны уполномоченными лицами Клиента и заверены печатью Клиента (при ее наличии).
4.2.6. В случае смены руководителя (единоличного исполнительного органа) Клиент обязан подтвердить права действующего Уполномоченного представителя Клиента.
4.2.7. В случае прекращения полномочий действующего Уполномоченного представителя Клиента, а также в случае несанкционированного доступа к Системе, Компрометации ключей, Клиент обязан незамедлительно направить в Банк письмо об аннулировании соответствующего комплекта Ключей (вложенным файлом) по адресу электронной почты (e-mail), указанному в Договоре об использовании ДБО, с последующим немедленным предоставлением в Банк оригинала вышеуказанного письма об аннулировании соответствующего комплекта Ключей на бумажном носителе.

Направление указанных документов по адресу электронной почты (e-mail) означает требование Клиента прекратить прием и исполнение любых Электронных документов, подписанных ЭП, сформированной на скомпрометированном/аннулируемом Ключе.

Для изготовления нового комплекта Технологических ключей Клиент предоставляет в Банк Данные о Владельце сертификата ключа проверки ЭП в двух экземплярах (Приложение №5 к Соглашению) с приложением необходимых документов.
4.2.8. В случае изменения фамилии, имени, отчества (при наличии) Уполномоченного представителя Клиента, вида права подписи Электронных документов, а также наименования Клиента, Клиент предоставляет в Банк все документы, предусмотренные настоящим Соглашением для изготовления нового комплекта Технологических ключей, а также письмо об аннулировании соответствующего комплекта Ключей.

В случае изменения иных данных Уполномоченного представителя Клиента, Клиент предоставляет в Банк Акт признания открытого ключа (сертификата) для обмена сообщениями (Приложение №6 к Соглашению), с приложением заверенной Банком/нотариально (в случае необходимости с проставлением апостиля/при условии ее легализации) копии документа, удостоверяющего личность Уполномоченного представителя Клиента и/или документа, подтверждающего право лица на пребывание (проживание) в Российской Федерации и/или миграционной карты – для иностранных граждан и лиц без гражданства.

Для Уполномоченных представителей Клиента с полномочиями «без права подписи» документ, удостоверяющий личность Уполномоченного представителя Клиента и/или документ, подтверждающий право лица на пребывание (проживание) в Российской Федерации и/или миграционная карта, – для иностранных граждан и лиц без гражданства могут быть представлены в Банк в копиях, заверенных в порядке, установленном Банком.

Документы, представляемые Клиентом и составленные на иностранном языке, должны сопровождаться переводом на русский язык, за исключением случаев установленных законодательством Российской Федерации. Перевод на русский язык должен быть заверен в порядке, установленном законодательством Российской Федерации.
4.2.9. Клиент обязан самостоятельно контролировать сроки действия Технологических ключей/Рабочих ключей и своевременно инициировать процедуру создания Рабочих ключей/Плановой смены рабочих ключей до истечения срока действия действующих Рабочих ключей. Соответствующие уведомления о Плановой смене рабочих ключей могут направляться Банком по Системе в течение месяца до истечения срока действия действующих Рабочих ключей. В случае, если в установленные Соглашением сроки Клиентом не направлен в Банк запрос на создание Сертификата Рабочего ключа и/или не предоставлены в Банк на бумажном носителе Акт признания открытого ключа (сертификата) для обмена сообщениями (Приложение №6 к Соглашению) и Акт признания Открытого ключа ЭП (в случае необходимости), а также в случае непринятия Банком от Клиента на бумажном носителе перечисленных документов и/или непринятия Клиентом от Банка в Системе Сертификата Рабочего ключа, действие Технологического ключа/Рабочего ключа прекращается.

Порядок изготовления нового Технологического ключа/Рабочего ключа аналогичен порядку, установленному п.п.3.1, 3.2, 3.4, 3.6 Соглашения.

4.2.10. Клиент обязан информировать Банк об изменении информации, касающейся исполнения Сторонами Соглашения. По мере внесения соответствующих изменений, незамедлительно представлять в Банк документы, подтверждающие изменения данных сведений.

Все риски неблагоприятных последствий, связанных с несвоевременным уведомлением Банка о произошедших изменениях, в том числе, указанных в п.п.4.2.6-4.2.8, п.5.5 Соглашения, несет Клиент.

4.2.11. При расторжении Соглашения Клиент обязуется уничтожить все предоставленное ему в пользование программное обеспечение (исполняемые и вспомогательные файлы) Системы.

4.2.12. Клиент обязуется не передавать третьим лицам свои права и обязанности по Соглашению без письменного (на бумажном носителе) согласия Банка.

4.2.13. Клиент обязан проверять наличие новых Электронных документов от Банка, направленных в адрес Клиента, ежедневно, за исключением официально установленных выходных и праздничных нерабочих дней Банка, а также ежедневно проверять SMS-сообщения, направленные Банком в связи с выявлением им операций, соответствующих признакам осуществления перевода денежных средств без согласия Клиента.

Клиент обязан не реже одного раза в 5 (пять) календарных дней знакомиться с информацией, публикуемой Банком в соответствии с п.12.6 Соглашения.

За убытки, возникшие в результате неисполнения Клиентом вышеуказанных обязанностей, Банк ответственности не несет.

4.2.14. Клиент обязуется по требованию и форме Банка предоставлять документы (как на бумажном носителе, так и с помощью Системы), подтверждающие данные об Уполномоченном представителе Клиента.

4.2.15. Клиент обязуется соблюдать требования по информационной безопасности при работе с Системой, указанные в Приложении № 4 к Соглашению, а также направляемые Банком по Системе и размещаемые на официальном сайте Банка в сети Интернет.

### 4.3. Права и обязанности Банка.

4.3.1. Банк не принимает к исполнению Электронные документы, оформленные с нарушением требований законодательства Российской Федерации, Соглашения, ДБС, иных соглашений между Сторонами.

4.3.2. Банк имеет право отказать Клиенту в приеме к исполнению Электронного документа, если Клиент заполнил поля Электронного документа с ошибками. В этом случае Клиенту направляется Квитанция с указанием причины отказа.

4.3.3. Банк не имеет права самостоятельно корректировать реквизиты Электронных документов Клиента.

4.3.4. В случае непредоставления Клиентом документов, указанных в п.4.2.7 Соглашения, Банк не будет нести ответственность за последствия совершения операций, иных действий, сделок на основании надлежащим образом оформленного Клиентом Электронного документа, подписанного Уполномоченным представителем Клиента, данные о котором были предоставлены Клиентом в Банк ранее.

4.3.5. Банк прекращает прием и исполнение любых Электронных документов, подписанных ЭП, сформированной на скомпрометированном/аннулируемом Ключе в сроки, предусмотренные в письме об аннулировании соответствующего комплекта Ключей, а в случае отсутствия указания на такие сроки – немедленно. Все Электронные документы, поступившие в Банк до получения Банком указанного письма, исполняются в порядке, установленном Соглашением или иными соглашениями между Сторонами.

В случае непредставления оригинала письма об аннулировании соответствующего комплекта Ключей Клиентом на бумажном носителе Банк не будет нести ответственность за убытки, причиненные Клиенту в результате прекращения приема и исполнения Электронных документов, подписанных ЭП, сформированной на соответствующем скомпрометированном/аннулируемом Ключе.

4.3.6. Банк имеет право отказать Клиенту в приеме/приостановить исполнение любого Электронного документа по своему усмотрению, в том числе, но не ограничиваясь, в случае возникновения у него подозрений, что Электронный документ подписан не Уполномоченным представителем Клиента, Компрометации ключей, Несанкционированного доступа к Системе и/или в случае какого-либо нарушения Клиентом Соглашения, при выявлении Банком операции, соответствующей признакам осуществления перевода денежных средств без согласия Клиента, при этом Клиент вправе передать в Банк соответствующий платежный, иной документ на бумажном носителе, составленный в соответствии с условиями ДБС, Соглашения, иных соглашений между Банком и Клиентом, законодательством Российской Федерации.

О своем отказе в приеме Электронного документа Банк обязуется уведомить Клиента не позднее Рабочего дня Банка, следующего за днем поступления Электронного документа в Банк, путем направления сообщения Клиенту по Системе.

4.3.7. Банк имеет право отказать Клиенту в приеме Электронных документов/приостановить их исполнение для проведения расчетных операций по Счету Клиента, счету по вкладу (депозиту), подписанных ЭП, в случаях, предусмотренных законодательством Российской Федерации, в том числе, в области противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма.

4.3.8. Банк имеет право запрашивать у Клиента подтверждение данных об Уполномоченном представителе Клиента.

4.3.9. Банк имеет право вносить в одностороннем порядке изменения в порядок функционирования Системы и сообщать об этом Клиенту в письменном уведомлении на бумажном носителе или посредством Системы.

4.3.10. Банк имеет право приостановить обслуживание Клиента с использованием Системы на время спорных ситуаций с уведомлением об этом Клиента.

4.3.11. Банк имеет право приостановить обслуживание Клиента с использованием Системы для выполнения неотложных, аварийных и регламентных работ, связанных с обслуживанием Системы.

4.3.12. Банк обязуется в течение 7 (семи) Рабочих дней Банка от даты получения заявки на установку Системы и при условии выполнения Клиентом обязательств, в соответствии с п. 3.1.1 Соглашения, произвести работы и оказать услуги, предусмотренные п. 3.1.2 Соглашения.

4.3.13. Банк обязуется принимать от Клиента Электронные документы, подписанные Уполномоченным(и) представителем(лями) Клиента в соответствии с условиями настоящего Соглашения, требованиями законодательства Российской Федерации и осуществлять операции, сделки, иные действия на основании таких Электронных документов в сроки, предусмотренные ДБС, Соглашением, иными соглашениями между Сторонами.

В случае направления Электронного документа в нерабочие дни Банка, днем поступления Электронного документа является первый Рабочий день Банка, следующий за нерабочим днем. Стороны признают в качестве единой шкалы времени при работе с Системой местное время г. Москвы.

4.3.14. Банк информирует Клиента о совершении каждой операции по Счету, счету депо с использованием Системы или без ее использования путем предоставления Клиенту выписки по Счету, счету депо не позднее Рабочего дня Банка, следующего за днем совершения операции по Счету, счету депо, путем направления их посредством Системы. Днем выдачи (получения) указанных выписок считается день их направления Банком по Системе. Направление Банком указанных выписок по Системе является надлежащим уведомлением Клиента о совершении операции с использованием электронного средства платежа в соответствии с законодательством Российской Федерации, и не требует дополнительного направления Банком Клиенту каких-либо иных уведомлений.

4.3.15. Банк обязуется консультировать Клиента по вопросам работы с Системой (в Рабочие дни Банка с 10.00 до 16.00 московского времени), предоставлять Клиенту новые

версии Системы, а также информировать Клиента обо всех изменениях порядка функционирования Системы в течение всего срока действия настоящего Соглашения.
4.3.16. Банк обязуется в случае невозможности устранить неполадки, возникшие в Системе, по месту нахождения Банка, направить специалиста к Клиенту в течение 15 (пятнадцати) календарных дней с момента получения письменной заявки от Клиента. Необходимость выезда к Клиенту определяется Банком с учетом возникших неполадок в Системе.

**Статья 5. Права и обязанности Сторон при выявлении Банком операций, соответствующих признакам осуществления перевода денежных средств без согласия Клиента.**

5.1. Банк при выявлении им операции, соответствующей признакам осуществления перевода денежных средств без согласия Клиента, обязан до осуществления списания денежных средств со Счета Клиента на срок не более двух Рабочих дней Банка приостановить исполнение распоряжения о совершении операции, соответствующей признакам осуществления перевода денежных средств без согласия Клиента.
5.2. О приостановлении исполнения распоряжения Клиента о совершении операции, соответствующей признакам осуществления перевода денежных средств без согласия Клиента Банк обязуется уведомить Клиента незамедлительно путем направления сообщения Клиенту по своему усмотрению по Системе или по номеру мобильного телефона, указанному Клиентом в Договоре об использовании ДБО.

Днем получения Клиентом сообщения об операции, соответствующей признакам осуществления перевода денежных средств без согласия Клиента, является день направления Банком указанного сообщения по Системе или день направления Банком SMS- сообщения на номер мобильного телефона Клиента, указанный им в Договоре об использовании ДБО.
5.3. В случае, если Банк запрашивает у Клиента подтверждение возобновления исполнения распоряжения приостановленного из-за признаков осуществления перевода денежных средств без согласия Клиента, Клиент по номеру телефона Банка, направленного Банком Клиенту с помощью Системы/на мобильный номер телефона Клиента и с произнесением Кодового слова Клиента, которое указано в Договоре об использовании ДБО, подтверждает/не подтверждает исполнение Банком соответствующего распоряжения.

При поступлении в Банк подтверждения исполнения Банком соответствующего платежа в течение операционного дня, указанного в ДБС, денежные средства списываются со Счета в текущий Рабочий день Банка. При поступлении вышеуказанного подтверждения после операционного дня, денежные средства списываются со Счета не позднее следующего Рабочего дня Банка.

В случае, если Клиент соглашается с сообщением Банка о том, что операция по Счету соответствует признакам осуществления перевода денежных средств без согласия Клиента, Клиент вправе незамедлительно направить в Банк отзыв соответствующего распоряжения.

При неполучении от Клиента соответствующего подтверждения, Банк возобновляет исполнение распоряжения по истечении двух Рабочих дней Банка после дня приостановлении исполнения данного распоряжения о совершении операции, соответствующей признакам осуществления перевода денежных средств без согласия Клиента.

Клиент уведомлен о том, что все телефонные разговоры записываются и хранятся в Банке в течение срока, установленного законодательством Российской Федерации.
5.4. Банк вправе в одностороннем порядке изменить Кодовое слово Клиента, направив Клиенту уведомление на бумажном носителе с собственноручной подписью руководителя Банка (уполномоченного им лица) об изменении Кодового слова. 5.5. В случае утраты Клиентом контроля над номером мобильного телефона, а также утраты Клиентом уверенности в том, что Конфиденциальная информация (Кодовое слово и/или номер мобильного телефона) не может быть использована неуполномоченными лицами, а также

в случае замены Клиентом номера мобильного телефона и/или Кодового слова, Клиент обязан незамедлительно уведомить об этом Банк в письменном виде на бумажном носителе с собственноручной подписью уполномоченного лица Клиента с указанием нового Кодового слова и/или номера мобильного телефона.

До момента принятия Банком вышеуказанного уведомления Банк использует в соответствии с Соглашением ранее сообщенный Банку Клиентом номер мобильного телефона, ранее сообщенное Клиентом Банку/Банком Клиенту (в соответствии с п.5.4 Соглашения) Кодовое слово.

5.6. Банк не несет ответственности за ущерб, причиненный Клиенту вследствие несанкционированного использования третьими лицами (компрометации) Кодового слова/номера мобильного телефона/мобильного телефона, на номер которого Банком направляется SMS-сообщение о совершении операции, соответствующей признакам осуществления перевода денежных средств без согласия Клиента.

5.7. Банк не несет ответственности за негативные последствия, в том числе убытки Клиента, которые могут возникнуть у Клиента вследствие неполучения уведомления от Банка об операции, соответствующей признакам осуществления перевода денежных средств без согласия Клиента, в том числе, в связи с недостоверностью/неактуальностью информации, указанной Клиентом, а также в связи с недоступностью для Клиента указанных способов связи, а также по вине Клиента или мобильного оператора, в случае утраты Клиентом Кодового слова/номера мобильного телефона/мобильного телефона, на номер которого Банком направляется SMS-сообщение о совершении операции, соответствующей признакам осуществления перевода денежных средств без согласия Клиента, их компрометации.

5.8. Банк не несет ответственности за убытки Клиента, возникшие в результате утраты (порчи, передачи, утери, разглашении) Клиентом Кодового слова/номера мобильного телефона/мобильного телефона, на номер которого Банком направляется SMS-сообщение о совершении операции, соответствующей признакам осуществления перевода денежных средств без согласия Клиента.

5.9. Банк не несет ответственности за убытки Клиента, возникшие вследствие несвоевременного сообщения Банку об утрате Клиентом контроля над номером мобильного телефона, а также утрате Клиентом уверенности в том, что конфиденциальная информация (Кодовое слово, номер мобильного телефона) не может быть использована неуполномоченными лицами.

5.10. Клиент обязуется предоставить Банку действительный номер мобильного телефона и обеспечить постоянную доступность номера мобильного телефона для приема сообщений в формате SMS-сообщений на русском языке.

5.11. Клиент несет ответственность за достоверность номера мобильного телефона, обязан не допускать создание дубликатов (клонов) sim-карты, а также не допускать получение, использование и замену sim-карты и/или номера мобильного телефона, Кодового слова неуполномоченными лицами.

5.12. Клиент обязуется обеспечить хранение информации о Кодовом слове способом, делающим кодовое слово недоступным третьим лицам.

Банк обязуется принять все необходимые меры организационного и технического характера для обеспечения невозможности доступа неуполномоченных лиц к информации о Кодовом слове, номере мобильного телефона Клиента, находящейся в распоряжении Банка.

5.13. Клиент подтверждает, что ему известно о том, что в процессе передачи информации путем направления SMS-сообщения возможен риск несанкционированного доступа третьих лиц к такой информации и настоящим выражает свое согласие с тем, что Банк не несет ответственности за разглашение информации о Клиенте, операциях по его Счетам в случае такого несанкционированного доступа.

5.14. Клиент соглашается с тем, что Банк не несет ответственности за какие-либо аварии, сбои и перебои в обслуживании, связанные с оборудованием, системами передачи электроэнергии и/или линий связи, сети Интернет, которые обеспечиваются, подаются, эксплуатируются и/или обслуживаются третьими лицами в связи с направлением Банком

Клиенту SMS-сообщения, в том числе убытки, понесенные в связи с неправомерными действиями или бездействием третьих лиц. Банк не несет ответственность за доступность и работоспособность средств связи, с помощью которых Банк осуществляет уведомление Клиента.

**Статья 6. Конфиденциальность.**

6.1. Условия и информация, содержащаяся в Соглашении, а также вся переписка, связанная с его исполнением, считаются обеими Сторонами конфиденциальной информацией, составляющей, в том числе, банковскую и коммерческую тайну, которую Стороны не вправе разглашать третьим лицам без предварительного письменного согласия другой Стороны, за исключением случаев, предусмотренных Соглашением и законодательством Российской Федерации, предоставления такой информации независимым аудиторским организациям по их требованию в ходе проведения аудита бухгалтерского учета и финансовой (бухгалтерской) отчетности; когда она оказалась известной третьим лицам до того, как Стороны ее разгласили.

**Статья 7. Финансовые взаимоотношения.**

7.1. Порядок оплаты, стоимость работ и услуг, оказываемых Банком Клиенту по настоящему Соглашению, устанавливаются Тарифами[1] и настоящим Соглашением. Расчеты производятся в рублях путем списания Банком (без дополнительных распоряжений Клиента) денежных средств с расчетного и/или иных счетов Клиента, открытых в Банке, с которых такое списание допускается законодательством Российской Федерации, предварительно полностью до оказания услуг. Если денежные средства списываются со счета Клиента в иностранной валюте, а сумма, причитающаяся Банку в соответствии с Тарифами, выражена в рублях, Банк самостоятельно производит конверсию указанных средств по курсу Банка России на день совершения операции и направляет полученную сумму для оплаты услуг Банка.
7.2. В случае, если остаток денежных средств на расчетном и/или иных счетах Клиента не позволяет Банку в срок и в размере, определенных Соглашением и действующими Тарифами, произвести списание платы за услуги Банка, Банк имеет право не оказывать запрашиваемые Клиентом услуги и/или приостановить обслуживание Клиента по Системе до момента полной оплаты задолженности Клиентом, соответственно уведомив об этом Клиента не менее чем за 5 (пять) Рабочих дней Банка. Клиент отказывается от любых претензий к Банку за возникновение в этом случае возможных убытков, включая реальный ущерб и упущенную выгоду, связанных с задержками в проведении Клиентом операций по Счету, счету депо, счету по вкладу (депозиту), осуществления иных действий, сделок.
7.3. В случае расторжения Клиентом Соглашения в одностороннем порядке, Клиент обязан не позднее 3 (трех) Рабочих дней Банка от даты направления уведомления о расторжении оплатить стоимость оказанных услуг.
7.4. Клиент настоящим дает согласие (заранее данный акцепт) на исполнение (в том числе частичное) Банком, в полной сумме платежных требований/инкассовых поручений Банка или иных документов, установленных Банком России, для осуществления прав, предусмотренных п.7.1 Соглашения, в течение срока действия Соглашения.

**Статья 8. Ответственность Сторон.**

[1] Тарифы не включают расходы на выезд за пределы г. Москвы к месту проведения работ по установке и обслуживанию Системы, которые оплачиваются Клиентом дополнительно на основании представленных Банком документов, подтверждающих эти расходы и списываются Банком со счета Клиента без дополнительных распоряжений Клиента.

8.1. За неисполнение и/или ненадлежащее исполнение обязательств по Соглашению Стороны несут ответственность в соответствии с законодательством Российской Федерации.
8.2. Клиент несет ответственность за сохранность и целостность установленного программного обеспечения, включая Средства защиты информации, за выполнение требований к эксплуатации Системы, изложенных в Соглашении и Документации, за надлежащее выполнение условий Соглашения, а также за использование Ключей только Уполномоченным представителем Клиента, указанным в соответствующих Данных о Владельце сертификата ключа проверки ЭП (Приложение №5 к Соглашению).
8.3. Банк несет ответственность перед Клиентом в соответствии с законодательством Российской Федерации, при наличии вины за реальный ущерб, но не за упущенную выгоду, с учетом ограничений, предусмотренных п.8.4 Соглашения, за точное, своевременное и полное исполнение поручений и инструкций Клиента по проведению банковских, депозитарных операций, по совершению иных действий, сделок, на основании надлежащим образом оформленных и своевременно переданных по Системе Электронных документов Клиента.
8.4. Банк не несет ответственности:

- за последствия совершения операций, иных действий, сделок на основании надлежащим образом оформленного Клиентом Электронного документа, признанного верным и принятого Банком к исполнению (любой Электронный документ, подписанный Уполномоченным представителем Клиента в соответствии с Соглашением и полученный Банком по Системе, в любом случае признается Электронным документом, исходящим от Клиента, что не допускает отказ Клиента от того, что такой документ направлен с его стороны, ни при каких обстоятельствах);
- за последствия совершения операций, иных действий, сделок на основании надлежащим образом оформленного Клиентом Электронного документа, подписанного прежним Уполномоченным представителем Клиента, до получения от Клиента письма об аннулировании соответствующего комплекта Ключей;
- за последствия отказа Банка в соответствии с п.п. 4.3.2, 4.3.5 - 4.3.7 Соглашения от приема к исполнению Электронного документа, переданного Клиентом по Системе;
- за последствия использования Системы, установленной у Клиента, посторонними, а также неуполномоченными на это лицами;
- за последствия разглашения Клиентом информации о порядке работы Системы, включая порядок использования Средств защиты информации;
- за нарушение работы Системы и возникновение трудностей в осуществлении операций, иных действий посредством Системы в результате ошибок и неточностей, допущенных Клиентом;
- за нарушение работы Системы в результате неисправности Средств обработки и хранения информации Клиента, используемых для доступа к Системе;
- за нарушение работы Системы в результате действий третьих лиц;
- за последствия нарушения Клиентом требований и правил, приведенных в Соглашении и Документации;
- за последствия нарушения работоспособности телекоммуникационных линий связи, Интернета;
- за убытки Клиента, возникшие вследствие несвоевременного сообщения Банку о Компрометации ключей;
- за убытки, возникшие в результате утраты (порчи, передачи, утери, разглашении) Клиентом применяемых в Системе паролей, Ключей, Конфиденциальной информации и/или программного обеспечения;
- за убытки, возникшие в результате использования Системы в нарушение каких-либо требований законодательства Российской Федерации, применимого к деятельности Клиента.

**Статья 9. Порядок разрешения споров.**

9.1. Стороны примут все меры к разрешению всех споров и разногласий, связанных с толкованием Сторонами Соглашения и его выполнением путем переговоров.
9.2. В случае, если Стороны не придут к взаимоприемлемому решению путем переговоров, Сторона, предъявившая претензию, официально вручает другой Стороне уведомление о претензии в письменном виде на бумажном носителе. Сторона, получившая уведомление, проводит расследование по факту претензии в течение 7 (семи) календарных дней от даты получения уведомления, по истечении которых на бумажном носителе уведомляет другую Сторону о результатах расследования.
9.3. В случае, если результаты расследования не удовлетворяют Сторону, предъявившую претензию, либо если такое уведомление не получено Стороной, предъявившей претензию, Стороны формируют техническую комиссию для разбора конфликтной ситуации в течение 15 (пятнадцати) календарных дней с момента истечения срока, указанного в п. 9.2 Соглашения. Целью работы комиссии является установление правомерности и обоснованности претензии. Порядок разбора конфликтной ситуации приведен в Приложении №3 к Соглашению. В состав комиссии включаются в равном количестве представители Банка и представители Клиента, а также представители организации–разработчика Системы и, в случае необходимости, независимые эксперты. Состав комиссии согласовывается Сторонами в акте. Их полномочия подтверждаются доверенностями. Срок действия комиссии составляет не более 14 (четырнадцати) календарных дней.
9.4. Работа комиссии проходит на территории Банка.
9.5. В случае отсутствия у одной из Сторон каких-либо материалов, требуемых для установления правомерности и обоснованности претензии (перечень материалов приведен в Приложении №3 к Соглашению), спор решается в пользу другой Стороны.
9.6. Результат работы комиссии оформляется актом, в котором определяются последующие действия Сторон.
9.7. В случае, если техническая комиссия не будет создана в сроки, предусмотренные Соглашением, либо, если в течение 14 (четырнадцати) календарных дней с момента создания технической комиссии, ее работа не даст результата, либо, если Стороны не придут к взаимоприемлемому решению, спор передается на рассмотрение в Арбитражный суд г. Москвы в соответствии с законодательством Российской Федерации.
9.8. Стороны признают, что Электронные документы, направленные Сторонами друг другу по Системе или хранящиеся в Банке в соответствии с Соглашением, а также соответствующие протоколы почтовых серверов и(или) сведения из баз данных, протоколирующих отправку каждого уведомления с его содержанием, сформированные на бумажных носителях, подписанные уполномоченным лицом и скрепленные печатью, записи телефонных разговоров между Сторонами являются достаточным доказательством соответствующего факта и могут быть представлены в качестве надлежащего доказательства в суд в случае рассмотрения спора, возникшего в результате применения Системы, а также при рассмотрении споров в досудебном порядке в соответствии с Соглашением.

## Статья 10. Срок действия Соглашения.

10.1. Соглашение вступает в силу с момента подписания Договора об использовании ДБО уполномоченными представителями Сторон.
10.2. Соглашение действует до момента прекращения обязательств по всем ДБС.
10.3. Банк вправе отказаться от исполнения настоящего Соглашения полностью в одностороннем порядке, письменно уведомив об этом Клиента, в случае, если по истечении 6 (шести) месяцев с даты заключения Соглашения Банком от Клиента посредством Системы в течение указанного времени не будет получен Электронный документ в соответствии с п.3.5 Соглашения или в течение указанного времени Клиент не устанавливал защищенное соединение с Банком для приема и отправки любых Электронных документов.

10.4. Соглашение может быть расторгнуто по письменному заявлению одной из Сторон (односторонний отказ от исполнения Соглашения полностью).

В случае расторжения Соглашения по инициативе Банка, Банк уведомляет об этом Клиента не позднее, чем за 14 (четырнадцать) календарных дней до даты расторжения.

В случае расторжения Соглашения по инициативе Клиента, Клиент в письменной форме на бумажном носителе уведомляет об этом Банк не позднее, чем за 3 (три) Рабочих дня Банка до даты расторжения.

Расторжение Соглашения до истечения срока его действия не освобождает Стороны от выполнения обязательств, предусмотренных Соглашением и не исполненных до даты его расторжения, и не лишает Сторону, чьи права по Соглашению нарушены в результате невыполнения обязательств другой Стороной, требовать защиты своих прав в соответствии с законодательством Российской Федерации и Соглашением.

## Статья 11. Обстоятельства непреодолимой силы.

11.1. Стороны освобождаются от ответственности за неисполнение и/или ненадлежащее исполнение обязательств по Соглашению, если такое неисполнение явилось результатом действий или обстоятельств непреодолимой силы (далее - Форс-мажор), то есть чрезвычайных и непредотвратимых при данных условиях обстоятельств.
11.2. Под термином Форс-мажор понимаются наводнение, пожар, землетрясение, ураган, взрыв, оседание почвы, эпидемии и иные подобные явления, а также война или военные действия в месте нахождения Банка или Клиента, забастовки в отрасли или регионе, принятие органом законодательной, исполнительной или судебной власти акта, повлекшие за собой невозможность надлежащего исполнения Соглашения Сторонами.
11.3. Сторона, для которой возникли обстоятельства непреодолимой силы, обязана в течение 7 (семи) Рабочих дней от даты возникновения Форс-мажора уведомить другую Сторону о наступлении таких обстоятельств, с приложением соответствующих доказательств. Доказательством Форс-мажора может служить официальный документ компетентной организации, подтверждающий факт наступления обстоятельств непреодолимой силы.
11.4. В случае наступления обстоятельств непреодолимой силы срок выполнения Сторонами обязательств по Соглашению переносится соразмерно времени, в течение которого действуют такие обстоятельства и их последствия. После прекращения действия Форс-мажора обязательства Сторон возобновляются.

## Статья 12. Заключительные положения.

12.1. Настоящее Соглашение является типовым. Для заключения Соглашения Клиент предоставляет в Банк Договор об использовании ДБО (по форме Банка), который заполняется, подписывается и предоставляется в Банк в двух экземплярах.
12.2. Если отдельное положение Соглашения теряет силу или становится неисполнимым, это не приводит к недействительности других его положений.
12.3. С даты заключения Соглашения вся переписка и договоренности между Сторонами, касающиеся условий Соглашения и предшествующие его заключению, теряют силу.
12.4. Вся переписка в рамках исполнения Соглашения осуществляется Сторонами на русском языке и может быть осуществлена посредством Системы.
12.5. Банк вправе в одностороннем порядке вносить изменения в Соглашение, уведомив об этом всех лиц, присоединившихся к Соглашению, не позднее чем за 10 (десять) календарных дней до вступления в силу указанных изменений. Указанный в настоящем пункте срок уведомления может быть уменьшен Банком в случае внесения изменений в Соглашение в связи с изменением законодательства Российской Федерации.

В случае изменения законодательства Российской Федерации Соглашение, до момента его изменения Банком применяется в части, не противоречащей требованиям законодательства Российской Федерации.

12.6. Банк с целью ознакомления Клиентов с Соглашением публикует его на официальном сайте Банка в сети Интернет по адресу: www.evrofinance.ru.

Банк уведомляет всех лиц, присоединившихся к Соглашению, о внесении в него изменений путем публикации информационного письма, а также полного текста изменений на официальном сайте Банка в сети Интернет по адресу: www.evrofinance.ru. Дополнительно к указанному способу уведомления Банк по своему усмотрению может использовать иные способы информирования Клиента.

Моментом публикации Соглашения, Тарифов и информации для ознакомления Клиентов, а также моментом ознакомления Клиента с опубликованными Соглашением, Тарифами и информацией для ознакомления Клиентов считается момент их первого размещения на официальном сайте Банка в сети Интернет по адресу: www.evrofinance.ru.

12.7. Действие изменений, внесенных в Соглашение, и вступивших в силу, распространяется на всех лиц, присоединившихся к Соглашению, независимо от даты присоединения к Соглашению (даты заключения Договора об использовании ДБО). В случае несогласия с изменениями, вносимыми в Соглашение, Клиент вправе расторгнуть Соглашение в одностороннем порядке до вступления таких изменений в силу в порядке, установленном в п.10.4 Соглашения.

12.8. В случае, если до вступления в силу опубликованных Банком изменений и/или дополнений, внесенных в Соглашение, Соглашение не расторгнуто, Стороны признают, что указанные изменения и/или дополнения в Соглашение приняты Клиентом.

12.9. Банк не несет ответственности, если информация об изменении и/или дополнении Соглашения, опубликованная в порядке и в сроки, установленные Соглашением, не была получена и/или изучена и/или правильно истолкована Клиентом.

12.10. Список Приложений, являющихся неотъемлемой частью Соглашения:

- Приложение №1 «Требования к аппаратно-программным средствам».
- Приложение №2 «Способы доставки информации».
- Приложение №3 «Порядок разбора конфликтных ситуаций».
- Приложение №4 «Требования по информационной безопасности».
- Приложение №5 «Данные о Владельце сертификата ключа проверки ЭП».
- Приложение №6 «Акт признания открытого ключа (сертификата) для обмена сообщениями».

**Приложение № 1**
**к Соглашению об использовании электронной системы**
**дистанционного банковского обслуживания**

## ТРЕБОВАНИЯ К АППАРАТНО-ПРОГРАММНЫМ СРЕДСТВАМ

1. Операционная система Windows 7 и выше.
2. Браузер Internet Explorer версии 6.0 или выше (только для установки рабочего места Клиента подсистемы «Интернет Клиент-банк»).
3. Наличие подключенного сетевого или локального принтера.
4. Наличие подключения к сети Internet.
5. Microsoft Word версии не ниже 97 или OpenOffice версии не ниже 2.3.0.
6. Перед установкой системы необходимо установить программное обеспечение Средства защиты информации.
7. При обмене информацией с бухгалтерскими системами (далее - БС) «1С», «Парус», БЭСТ-4 и с другими БС, в которых есть возможность экспорта документов в текстовый формат, необходимо, чтобы формат дат и чисел импортируемых документов соответствовал форматам дат и чисел, задаваемых в региональных настройках операционной системы компьютера.
8. В региональных настройках операционной системы компьютера формат дат должен использоваться ДД.ММ.ГГГГ.
9. В региональных настройках операционной системы компьютера в качестве десятичного разделителя чисел и сумм должна использоваться точка («.»).
10. ODBC-драйвер MS Access (только для установки рабочего места Клиента подсистемы «Клиент-банк»).

**Приложение № 2**
**к Соглашению об использовании электронной системы**
**дистанционного банковского обслуживания**

## СПОСОБЫ ДОСТАВКИ ИНФОРМАЦИИ

**1. Работа осуществляется через выделенное подключение к своему провайдеру услуг сети Интернет – способ доставки информации на русском языке.**

Параметры подключения в случае использования
- подсистемы «Клиент-Банк»: открытые TCP порты 1024, 1400 на IP адрес 91.227.169.45
- подсистемы «Интернет Клиент-Банк»: открытые TCP порты 80, 443 на сайт https://online.efbank.ru или IP адрес 91.227.169.146

Параметры подключения могут быть изменены и сообщены Клиенту в письменном уведомлении или направлены Клиенту посредством Системы.

**Настройка Клиентом данной транспортной схемы осуществляется на рабочем месте самостоятельно согласно требованиям провайдера.**

**2. Работа осуществляется через выделенное подключение к своему провайдеру услуг сети Интернет – способ доставки информации на английском языке.**

Параметры подключения: открытые TCP порты 80, 443, 8443 на сайт https://dbo.efbank.ru или IP адрес 91.227.169.132

Параметры подключения могут быть изменены и сообщены Клиенту в письменном уведомлении или направлены Клиенту посредством Системы.

**Настройка Клиентом данной транспортной схемы осуществляется на рабочем месте самостоятельно согласно требованиям провайдера.**

**Приложение № 3**
**к Соглашению об использовании электронной системы**
**дистанционного банковского обслуживания**

# ПОРЯДОК РАЗБОРА КОНФЛИКТНЫХ СИТУАЦИЙ

## 1. Общие положения

1.1. Ниже приведен перечень конфликтных ситуаций по поводу исполнения Электронных документов (далее - «Документов»), рассматриваемых технической комиссией, действующей в соответствии с порядком, предусмотренным Соглашением:

- Документ исполнен, а Клиент утверждает, что Документ не посылал и не подписывал;
- Клиент утверждает, что он направил Документ, а Документ не исполнен, причем, по утверждению Клиента, от Банка получена Квитанция об исполнении;
- Клиент утверждает, что он направил один Документ, а исполнен другой Документ;
- другие конфликтные ситуации.

1.2. При разрешении спорных ситуаций Стороны обязуются руководствоваться следующими принципами:

- Сторона-получатель обязуется признать подлинным и действительным Документ, переданный ей посредством Системы и имеющий ЭП, сформированную на закрытых ключах Стороны-отправителя, при условии положительного результата проверки ЭП на соответствующих открытых ключах;
- Сторона-отправитель обязуется признать подлинным (переданным ею посредством Системы) и действительным Документ, имеющий ЭП, сформированную на ее закрытых ключах, при условии положительного результата проверки ЭП на соответствующих открытых ключах;
- ответственность возлагается на Сторону-отправителя, при получении Стороной-получателем ложного Документа с успешно подделанной ЭП, так как в этом случае Сторона-отправитель не обеспечила сохранность Закрытых ключей ЭП.

1.3. Стороны признают, что математические свойства алгоритма ЭП гарантируют невозможность подделки значения ЭП любым лицом, не обладающим закрытым ключом подписи.

1.4. Стороны должны представить комиссии следующие материалы:

- носители информации с файлами, содержащими выгруженные из Системы путем использования функционала «Выгрузка данных для проверки подписи» спорный Документ, а также распечатанный из Системы спорный Документ или Квитанцию на него. Описание процедуры выгрузки данных для проверки подписи приведено в Документации;
- подписанные собственноручными подписями уполномоченных лиц Клиента и Банка оригиналы Актов признания открытого ключа (сертификата) для обмена сообщениями (Приложение№6 к Соглашению);
- носитель с Ключами Средств защиты информации.

1.5. Проверка подлинности Электронного документа осуществляется посредством программы OpenSSL.exe. Описание программы приведено в документации на официальном сайте разработчика в сети Интернет: http://openssl.org/docs/.

## 2. Процедура проверки подлинности Электронных документов

2.1. Для разбора конфликтных ситуаций техническая комиссия выполняет следующие действия:

- проверяет подлинность ЭП под выгруженным спорным Документом с использованием Открытого ключа ЭП Стороны-отправителя данного Документа;
- проверяет соответствие экземпляров Актов признания открытого ключа (сертификата) для обмена сообщениями (Приложение №6 к Соглашению) предоставленных Сторонами в соответствии с п.1.4. Порядка разбора конфликтных ситуаций;

- сверяет соответствие ключевых полей открытого ключа из Актов признания открытого ключа (сертификата) для обмена сообщениями с распечаткой протокола проверки ЭП, полученной при помощи программы OpenSSL.exe.

2.2. Результаты работы технической комиссии отражаются в акте, подписанном всеми членами технической комиссии. Члены технической комиссии, не согласные с выводами большинства, подписывают акт с возражениями, который прилагается к основному акту.

**Приложение № 4**
**к Соглашению об использовании электронной системы**
**дистанционного банковского обслуживания**

## ТРЕБОВАНИЯ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Для минимизации рисков несанкционированного доступа к Счетам, счету по вкладу (депозиту) Клиента со стороны злоумышленников и компрометации ключевой информации, Банк настоятельно просит Клиентов соблюдать следующие меры информационной безопасности:

- Выделить компьютер, который не будет использоваться в иных целях, кроме как для работы в Системе; не осуществлять, а при наличии технической возможности, запретить выход в Интернет с этого компьютера на иные адреса, за исключением адресов серверов Банка.

- Ограничить или полностью запретить удаленный доступ к выделенному компьютеру с других компьютеров локальной сети. Не использовать средства удаленного администрирования на выделенном компьютере. При наличии технических средств, поместить выделенный компьютер в отдельную сеть, контролируемую межсетевым экраном и системами обнаружения атак.

- Заменить все стандартные пароли, заданные при установке Системы, на уникальные собственные, производить периодическую смену паролей (не реже одного раза в три месяца).

- Использовать на постоянной основе антивирусное программное обеспечение с последней актуальной версией баз.

- Регулярно (не реже одного раза в неделю) выполнять антивирусную проверку для своевременного обнаружения вредоносных программ.

- Использовать на компьютере исключительно лицензионное программное обеспечение.

- Регулярно (не реже одного раза в месяц или по факту публикации) устанавливать обновления операционной системы.

- Проверить группу «Администраторы» на выделенном компьютере, исключить всех рядовых пользователей из этой группы, не работающих с Системой.

- При наличии технической возможности, для пользователей, работающих с Системой, создать отдельную групповую политику, разрешающую запуск только определенных приложений.

- Для доступа к серверам Банка использовать только заведомо известные Вам адреса интернет серверов Банка.

- В случае отсутствия возможности подключения к серверу Банка незамедлительно сообщать об этом Банку.

- Хранить в безопасном месте (в сейфе) и никому не передавать носители с ключевой информацией, обеспечив к ним доступ только уполномоченных лиц.

- Никогда не осуществлять копирование закрытых (секретных) ключей электронной подписи на локальный жесткий диск компьютера, даже с последующим его удалением.

- Регулярно (не реже одного раза в месяц) проверять целостность ключевых носителей, проводя проверку наличия на них файлов электронной подписи.

- Своевременно (в соответствии с условиями Соглашения) проводить Плановую смену рабочих ключей.

- Не оставлять носители с ключевой информацией без присмотра, подключать их к компьютеру только на время использования и незамедлительно их отключать после проведения банковских операций. При оставлении рабочего места Системы без присмотра всегда блокировать экран с последующим вводом пароля для его разблокировки.

- Производить незамедлительную замену ключей электронной подписи в случае их компрометации или подозрении на компрометацию.

- Своевременно устанавливать все обновления Системы.

- Не устанавливать обновления, а также не открывать ссылки в почтовых сообщениях, полученных от имени Банка по электронной почте; получив такое сообщение, незамедлительно сообщать об этом Банку.

- Ежедневно, в течение операционного дня Банка и по окончании Рабочего дня, осуществлять дополнительный вход в Систему для контроля перечня исходящих документов за текущий день. При обнаружении подозрительных документов, незамедлительно обращаться в Банк.

- В случае подозрений на замедление работы компьютера отключить компьютер физически от локальной сети и интернет и обратиться к системному администратору с просьбой о необходимости проведения полной антивирусной проверки сканированием всех файлов и памяти компьютера.

- В случае, если инцидент информационной безопасности все же произошел, ни в коем случае не выключать компьютер, а отключить его физически только от локальной сети и интернет, незамедлительно обратиться к системному администратору и сообщить об инциденте в Банк для проведения оперативного расследования и принятия необходимых мер для сбора доказательств.

- В случае выявления Клиентом подозрительных операций в Системе незамедлительно сообщать об этом в Банк.

**Приложение № 5**
**к Соглашению об использовании электронной системы**
**дистанционного банковского обслуживания**

**ФОРМА**

## ДАННЫЕ О ВЛАДЕЛЬЦЕ СЕРТИФИКАТА КЛЮЧА ПРОВЕРКИ ЭП

_____
Наименование Клиента, ОГРН, место нахождения

_____
(Уполномоченный представитель Клиента - Фамилия Имя Отчество)

Паспорт/удостоверение личности:_____№_____ выдан _____
серия номер

_____
кем выдан паспорт/удостоверение личности

_____ _____
дата выдачи место и дата рождения

_____
адрес места жительства (регистрации)

_____ _____
Гражданство идентификационный номер налогоплательщика (ИНН)
(при его наличии, при его отсутствии - указать «отсутствует»)

данные миграционной карты _____

Логин (6-10 символов):_____(заполняется только для подсистемы «Интернет клиент-банк»)

Право подписи документов: «единственная», «первая», «вторая», «без права подписи».
(ненужное зачеркнуть)

**Полномочия при наличии права подписи: подписание ЭП всех Электронных документов, предусмотренных Соглашением, направляемых Клиентом в Банк посредством Системы.**

**Полномочия «без права подписи»: вход в Систему, создание любых Электронных документов, предусмотренных Соглашением, установление защищенного соединения с Банком для приема и отправки любых Электронных документов, подписанных Уполномоченными представителями Клиента.**

_____
(подпись Уполномоченного представителя Клиента)

Руководитель _____/_____/
(подпись) (Ф.И.О.)

М.П.

---

**Отметки Банка**

Администратор (заместитель администратора) СКЗИ Банка
_____/_____/
(подпись) (Ф.И.О.)

_____
(дата получения Данных)

**Приложение № 6**
**к Соглашению об использовании электронной системы**
**дистанционного банковского обслуживания**

**ФОРМА**

**АКТ**
**признания открытого ключа (сертификата)**
**для обмена сообщениями**

«____»_____20___г. г._____

Настоящим Актом признаётся ключ проверки электронной подписи и открытый ключ шифрования, принадлежащий уполномоченному представителю Клиента:

**Сведения о Клиенте:**

1. Наименование: _____
2. Место нахождения:_____
3. Тел._____ 4. Факс. _____

**Сведения об Уполномоченном представителе Клиента:**

1. Фамилия, имя, отчество: _____
2. Удостоверение личности/паспорт: серии _____ № _____,
выдан «___»_____ _____г _____
_____
3. Место и дата рождения;_____
4. Адрес места жительства (регистрации):_____
_____
5. Гражданство:_____

ИНН (при его наличии, при его отсутствии – указать «отсутствует») _____
данные миграционной карты _____.

Личная подпись Уполномоченного представителя Клиента _____

**Параметры ключа:**
Алгоритм: (указывается алгоритм)
Начало срока действия: «____»_____ 20___г.
Окончание срока действия: «____»_____ 20___г.

**Текст открытого ключа:**

| |
|---|
| |

**Дополнительные поля открытого ключа (сертификата):**

| |
|---|
| Имя владельца ключа:<br>Код страны:<br>Страна:<br>Город:<br>Наименование клиента:<br>Идентификатор клиента в системе:<br>Данные об издателе: EVROFINANCE MOSNARBANK DBO CA, RU, MOSCOW |

**Ключ зарегистрирован и может использоваться для обмена сообщениями.**

Администратор/Заместитель
администратора СКЗИ **БАНКА** Руководитель **КЛИЕНТА**

_____ _____

_____ _____

М.П. М.П.