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

Настоящее Соглашение (далее – Соглашение) является договором присоединения в соответствии со ст.428 Гражданского кодекса Российской Федерации. Заключение Соглашения производится в порядке, установленном Соглашением.

В целях повышения эффективности обслуживания Клиента Банка при совершении банковских операций (в том числе расчетных), депозитарных операций, иных сделок, в целях осуществления Банком функций агента валютного контроля, а также в соответствии с п.2 ст.160, п.3 ст. 847 Гражданского кодекса Российской Федерации, Стороны согласны установить и взаимно использовать электронную систему документооборота при проведении банковских, депозитарных операций, иных сделок, которая является корпоративной информационной системой, организованной Банком, в которой Банк осуществляет, в частности, создание и выдачу сертификатов ключей проверки электронной подписи, здесь и далее именуемую "**Система"** и договорились в отношении эксплуатации Системы о нижеследующем:

Термины и определения

Банк – АО АКБ «ЕВРОФИНАНС МОСНАРБАНК». Полное наименование: АКЦИОНЕРНЫЙ КОММЕРЧЕСКИЙ БАНК «ЕВРОФИНАНС МОСНАРБАНК» (акционерное общество).

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

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.

Закрытый ключ ЭП – уникальная последовательность символов, известная только Уполномоченному представителю Клиента, и предназначенная для создания в Электронных документах ЭП.

Клиент – юридическое лицо (российское/иностранное), заключившее с Банком Соглашение путем присоединения к нему.

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.

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

Компрометация ключей – возникновение сомнений в том, что используемые Закрытые ключи ЭП и Секретные ключи шифрования недоступны посторонним лицам.

К событиям, влекущим за собой компрометацию ключей, относятся, включая, но не ограничиваясь, следующие события:

- утрата электронных носителей ключа;
- утрата электронных носителей ключа с последующим обнаружением;
- доступ посторонних лиц (не Уполномоченного представителя Клиента) к Ключам, ключевой информации, использование Ключей без согласия Клиента;
- другие события, которые, по мнению Сторон, могут повлечь компрометацию Ключей.

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 к информации – доступ к информации лиц, не имеющих 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.

Пакет Электронных документов – произвольное количество Электронных документов, переданных в один сеанс связи.

Плановая смена рабочих ключей – создание Уполномоченным представителем Клиента новых Рабочих ключей, осуществляемое 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, в противном случае Электронный документ считается ошибочным, а ЭП под ним - недействительной. Процедура выработки и проверки ЭП соответствуют алгоритмам ГОСТ Р34.10-2001 и ГОСТ Р34.11-94.

Рабочие ключи – Секретный и открытый ключи шифрования, Закрытый и Открытый ключи ЭП, предназначенные для обеспечения авторства, целостности и конфиденциальности Электронных документов, передаваемых в Системе. Рабочие ключи формируются Уполномоченным представителем Клиента самостоятельно посредством Системы. Срок действия Рабочих ключей составляет 15 месяцев с даты формирования запроса на создание Сертификата Рабочего ключа.

Секретный и открытый ключи шифрования – Ключи, используемые при создании общего секретного ключа связи для шифрования при отправлении и расшифрования

при получении Электронных документов. При шифровании, с целью дальнейшей передачи информации используется секретный ключ Стороны-отправителя и открытый ключ Стороны-получателя. При расшифровании информации по получении используется секретный ключ Стороны-получателя и открытый ключ Стороны-отправителя.

Сертификат Рабочего ключа - электронный документ с ЭП Банка, содержащий Открытые ключи 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.

Средства защиты информации – сертифицированные криптографические средства, обеспечивающие реализацию следующих функций - создание ЭП в Электронном документе с использованием Закрытого ключа ЭП, проверки 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 или/и Клиент.

Счета Клиента - все счета, открытые Банком Клиенту на момент заключения настоящего Соглашения или 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 подписания настоящего Соглашения Тарифы доводятся до сведения Клиента при подписании 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 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 15 месяцев с момента создания Банком Технологических ключей.

Уполномоченный представитель Клиента – физическое лицо, указанное в Данных о Владельце сертификата ключа проверки ЭП, наделенное Клиентом правом в течение срока действия Ключей подписывать Электронные документы 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 – определенный ГОСТ Р34.11-94 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. При шифровании используется алгоритм криптографического преобразования ГОСТ 28147-89.

Расшифрование – операция обратная шифрованию.

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) и заверенному печатью, если в соответствии с законодательством РФ или обычаем делового оборота документ должен быть заверен печатью.

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, а также удостовериться в целостности информации Электронного документа. Для выработки и проверки ЭП используются сертифицированные программные Средства защиты информации. В рамках настоящего Соглашения под Электронной подписью понимается усиленная неквалифицированная электронная подпись.

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 РФ о легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма.

Статья 2. Общие положения.

2.1.Система будет использоваться для обмена Электронными документами. 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 Средства обработки и хранения информации, а также способ доставки, указанный в Приложении №2 к Соглашению, 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.
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.

Статья 3. Порядок подключения Клиента к Системе.

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 направляет в Банк 2 (два) экземпляра Данных о Владельце сертификата ключа проверки ЭП по форме Приложения №5 к Соглашению с приложением заверенной надлежащим образом копии документа, удостоверяющего личность Уполномоченного

представителя Клиента и документа, подтверждающего право лица на пребывание (проживание) в РФ 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;
г) обеспечивает наличие и приведение оборудования, предназначенного для установки Системы, в соответствие с требованиями к аппаратно-программным средствам, приведенными в Приложении №1 к Соглашению;
д) по каждому из Уполномоченных представителей Клиента заверяет собственноручной подписью уполномоченного лица Клиента полученный от Банка Акт признания Открытого ключа ЭП и передает один экземпляр указанного акта в Банк.
3.1.2.Банк выполняет следующие действия:
а) изготавливает Технологические ключи в течении 4-х рабочих дней со дня принятия Банком Данных о Владельце сертификата ключа проверки ЭП;
б) передает Клиенту Технологические ключи на электронном носителе; 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 уполномоченными Клиентом лицами в согласованные Сторонами сроки.
3.2.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.
3.3.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;

  - предоставляет в Банк на бумажном носителе сведения, используемые при работе в Системе (по форме Приложения №7 к Соглашению) и Акт признания Открытого ключа ЭП.

- Банк:

  - проставляет отметки о получении на каждом экземпляре принятых от Клиента сведений, используемых при работе в Системе (Приложение №7 к Соглашению);

  - в течении двух рабочих дней при условии принятия сведений, используемых при работе в Системе (Приложение №7 к Соглашению), полученных от Клиента, изготавливает Сертификат Рабочего ключа на основании электронного запроса Клиента на создание Сертификата Рабочего ключа;

  - направляет Клиенту Сертификат Рабочего ключа.

3.4. Клиент после получения из Банка Сертификата Рабочего ключа 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.
3.5.Банк, обладая соответствующими правами, предоставленными ему в соответствии с контрактом, заключенным между Банком и ООО «Банк Софт Системс», предоставляет Клиенту право на пользование Системой в течение действия настоящего Соглашения. Право на пользование предоставляется с учетом ограничений, предусмотренных законодательством РФ 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 РФ, нормативными актами Банка России, ДБС, настоящим Соглашением и приложениями к нему, иными соглашениями между Банком и Клиентом.
4.1.2. Стороны обязуются не разглашать третьей стороне (за исключением случаев, предусмотренных законодательством РФ и настоящим Соглашением) информацию о Средствах защиты информации, реализованных в используемой по Соглашению Системе.
4.1.3. Каждая из Сторон обязуется немедленно (в течение не более чем одного рабочего дня со дня получения соответствующей информации) информировать другую Сторону обо всех случаях Компрометации ключей, несанкционированного использования Системы, а также повреждениях программно-аппаратных средств обработки, хранения, передачи Электронных документов, а также Ключей на электронном носителе и не использовать Ключи при наличии оснований полагать, что они скомпрометированы.
4.1.4. Средства защиты информации, предоставленные Системой, признаются Сторонами достаточным для защиты информации от несанкционированного доступа, подтверждения авторства и подлинности Электронных документов.
4.1.5. Вывоз полученных Клиентом от Банка шифровальных (криптографических) средств с территории РФ возможен только на основании отдельного решения соответствующего уполномоченного государственного органа РФ, при отсутствии указанного решения установка Системы осуществляется по адресу помещения Клиента, находящегося на территории РФ.
4.1.6. Какие-либо ограничения полномочий Уполномоченного представителя Клиента, Банком не признаются, если иное не установлено отдельным соглашением между Клиентом и Банком. В связи с чем, Банк не осуществляет контроль за суммами платежей, суммами сделок, осуществляемых Уполномоченными представителями Клиента в соответствии с ДБС, Соглашением, иными соглашениями между Сторонами, а также за иными ограничениями Уполномоченного представителя Клиента.

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, вызвать 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 (в случае необходимости ее наличия).
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 Компрометации ключей Клиент обязан незамедлительно (в течение не более чем одного рабочего дня со дня получения соответствующей информации) направить в Банк письмо об аннулировании соответствующего комплекта Ключей по факсу, указанному в Договоре об использовании электронной системы дистанционного банковского обслуживания (Приложение №6 к Соглашению) (далее – Договор об использовании ДБО), с последующим немедленным предоставлением в Банк оригинала.
Направление указанных документов по факсу означает требование Клиента прекратить прием и исполнение любых Электронных документов, подписанных ЭП, сформированной на скомпрометированном 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 сведения, используемые при работе в Системе (Приложение №7 к Соглашению) с приложением заверенной надлежащим образом копии документа, удостоверяющего личность Уполномоченного представителя Клиента, и документа, подтверждающего право лица на пребывание (проживание) в РФ и/или миграционной карты – для иностранных граждан и лиц без гражданства.
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, а также в случае непринятия Банком от Клиента на бумажном носителе сведений, используемых при работе в Системе

(Приложение №7 к Соглашению), Банк прекращает действие Технологического ключа/ Рабочего ключа.

В случае прекращения действия Технологического ключа/Рабочего ключа порядок изготовления нового Технологического ключа/Рабочего ключа аналогичен порядку изготовления Технологического ключа/Рабочих ключей, предусмотренных соответствующими положениями п.3.1.1 настоящего Соглашения.

4.2.10.Клиент обязан в случае изменения своего адреса, контактной информации и реквизитов, указанных в Договоре об использовании ДБО, а также изменения иной информации, касающейся исполнения Сторонами Соглашения, по мере внесения изменений, незамедлительно представлять в Банк необходимые документы, подтверждающие изменение данных сведений. Все риски неблагоприятных последствий, связанные с несвоевременным уведомлением Банка о произошедших изменениях, в том числе, указанных в п.4.2.6, п.4.2.7, п.4.2.8 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 согласия Банка.

4.2.13.Клиент обязуется по требованию Банка представлять документы, подтверждающие данные об Уполномоченном представителе Клиента.

4.2.14.Клиент обязуется соблюдать требования к информационной безопасности при работе с Системой, указанные в Приложении № 4 к Соглашению, а также периодически 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 РФ, Соглашения.

4.3.2.Банк имеет право отказать Клиенту в приеме к исполнению Электронных документов, если Клиент не предоставит документы, указанные в п. 4.2.6 Соглашения. В случае непредставления подтверждающих документов, 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.

4.3.3.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, 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.

4.3.4.Банк имеет право отказать Клиенту в приеме 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 и/или операция, осуществляемая с помощью Электронного документа, имеет признаки мошенничества и/или в случае иного нарушения Клиентом Соглашения, 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 РФ. О своем отказе в приеме Электронного документа Банк обязуется уведомить Клиента не позднее дня, следующего за днем поступления Электронного документа в Банк, путем направления сообщения Клиенту по Системе или по факсу, номер которого указан в Договоре об использовании ДБО.

4.3.5.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.

4.3.6.Банк имеет право запрашивать у Клиента подтверждение данных об Уполномоченном представителе Клиента в рамках работы, связанной с обновлением данных об Уполномоченных представителях Клиента.

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

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

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

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

4.3.11.Банк обязуется в течение 7 (семи) рабочих дней 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.

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

4.3.13.Банк информирует Клиента о совершении каждой операции по Счету, счету депо с использованием Системы или без ее использования путем предоставления Клиенту выписки по Счетам, счету депо, не позднее рабочего дня следующего за днем совершения операции по Счетам, счету депо, путем направления их посредством Системы. Днем выдачи (получения) указанных выписок считается день ее направления Банком по Системе.

4.3.14.Банк обязуется консультировать Клиента по вопросам работы с Системой, предоставлять Клиенту новые версии Системы, а также информировать Клиента обо всех изменениях порядка функционирования Системы в течение всего срока действия настоящего Соглашения.

4.3.15.Банк обязуется в случае невозможности устранить неполадки, возникшие в Системе, по месту нахождения Банка, направить специалиста к Клиенту в течение 7 (семи) рабочих дней с момента получения письменной заявки от Клиента. Необходимость выезда к Клиенту определяется специалистами Банка с учетом возникших неполадок в Системе.

4.3.16. Банк имеет право отказать Клиенту в приеме Электронных документов для проведения расчетных операций по Счету Клиента, подписанных ЭП, в случаях, предусмотренных действующим законодательством РФ в области противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма.

Статья 5. Конфиденциальность.

5.1. 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 РФ, предоставления такой информации независимым аудиторским организациям по их требованию в ходе проведения аудита бухгалтерского учета и финансовой (бухгалтерской) отчетности; когда она оказалась известной третьим лицами до того, как Стороны ее разгласили.

Статья 6. Финансовые взаимоотношения.

6.1. 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 РФ, 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.
6.2. 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 3 (три) рабочих дня. 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.
6.3. В случае расторжения Клиентом Соглашения в одностороннем порядке, Клиент обязан не позднее 7 (семи) рабочих дней от даты направления уведомления о расторжении оплатить стоимость оказанных услуг.
6.4. В части прав Банка на списание денежных средств (без дополнительных распоряжений Клиента) со счетов Клиента Соглашение вносит соответствующие изменения и дополнения и является составной и неотъемлемой частью ДБС.
6.5. 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.6.1 Соглашения, в течение срока действия Соглашения.

Статья 7. 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.

7.1. За неисполнение и/или ненадлежащее исполнение обязательств по Соглашению Стороны несут ответственность в соответствии с законодательством РФ.
7.2. 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/сведениях, используемых при работе в Системе (Приложение №7 к Соглашению).
7.3. Банк несет ответственность перед Клиентом в соответствии с законодательством РФ, при наличии вины за реальный ущерб, но не за упущенную выгоду, а также с учетом ограничений, предусмотренных п.7.4 настоящего 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.
7.4. 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, 4.3.3, 4.3.4 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 РФ, применимого к деятельности Клиента.

Статья 8. Порядок разрешения споров.

8.1. Стороны примут все меры к разрешению всех споров и разногласий, связанных с толкованием Сторонами Соглашения и его выполнением путем переговоров.
8.2. 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 календарных дней от даты получения уведомления, по истечении которых в письменном виде на бумажном носителе уведомляет другую Сторону о результатах расследования.
8.3. 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 5 (пяти) рабочих дней с момента истечения срока, указанного в п. 8.2 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 календарных дней.
8.4. Работа комиссии проходит на территории Банка.
8.5. 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.
8.6. Результат работы комиссии оформляется актом, в котором определяются последующие действия Сторон.
8.7. В случае если техническая комиссия не будет создана в сроки, предусмотренные Соглашением, либо, если в течение 14 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 РФ.
8.8. Стороны признают, что Электронные документы, направленные Сторонами друг другу по Системе или хранящиеся в Банке в соответствии с Соглашением, 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 9. Срок действия Соглашения.

9.1. Соглашение вступает в силу с момента его подписания уполномоченными представителями Сторон.
9.2. Соглашение действует до момента прекращения обязательств по всем ДБС.
9.3. Банк вправе отказаться от исполнения настоящего Соглашения в одностороннем порядке, письменно уведомив об этом Клиента, в случае, если по истечении 6 (Шести) месяцев с даты подписания Соглашения Банком от Клиента посредством Системы в течение указанного времени не будет получен Электронный документ в соответствии с п.3.4 Соглашения или в течение указанного времени Клиент не устанавливал защищенное соединение с Банком для приема и отправки любых Электронных документов.

9.4. Соглашение может быть расторгнуто по письменному заявлению одной из Сторон (односторонний отказ от исполнения Соглашения полностью), направленному другой Стороне не позднее, чем за 14 (четырнадцать) календарных дней до даты расторжения.
9.5. 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 РФ и Соглашением.

Статья 10. Обстоятельства непреодолимой силы.

10.1. 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.

10.2. 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.

10.3. 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.

10.4. 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 11. Заключительные положения.

11.1. Для заключения Соглашения Клиент предоставляет в Банк Договор об использовании ДБО, который заполняется, подписываются и предоставляется в Банк двух экземплярах.
11.2. Если отдельное положение Соглашения теряет силу или становится неисполнимым, это не приводит к недействительности других его положений.
11.3. С даты заключения Соглашения вся переписка и договоренности между Сторонами, касающиеся предмета Соглашения и предшествующие его заключению, теряют силу.
11.4. Вся переписка в рамках исполнения Соглашения осуществляется Сторонами на русском языке и может быть осуществлена посредством Системы.
11.5. Банк вправе в одностороннем порядке вносить изменения в Соглашение, уведомив об этом всех лиц, присоединившихся к Соглашению, не позднее чем за 20 (двадцать) 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 РФ.
11.6. Банк уведомляет всех лиц, присоединившихся к Соглашению, о внесении в них изменений путем публикации информационного письма, а также полного текста

изменений на информационных стендах Банка по обслуживанию клиентов-юридических лиц, а также на сайте Банка в сети Интернет www.evrofinance.ru. Дополнительно к указанному способу уведомления Банк по своему усмотрению может использовать иные способы информирования Клиента.

11.7. Действие изменений, внесенных в Соглашение, вступивших в силу, распространяется на всех лиц, присоединившихся к Соглашению, независимо от даты присоединения к Соглашению (даты заключения Соглашения). В случае несогласия с изменениями, вносимыми в Соглашение, Клиент вправе расторгнуть Соглашение до вступления таких изменений в силу в порядке, установленном в п.9.4 Соглашения.

11.8. Список Приложений, являющихся неотъемлемой частью Соглашения:

- Приложение №1 “Требования к аппаратно-программным средствам”.
- Приложение №2 “Способ доставки информации”.
- Приложение №3 “Порядок разбора конфликтных ситуаций”.
- Приложение №4 “Требования к информационной безопасности”.
- Приложение №5 “Данные о Владельце сертификата ключа проверки ЭП”.
- Приложение №6 “Договор об использовании электронной системы дистанционного банковского обслуживания”.
- Приложение №7 “Сведения абонента (наименование криптопрофиля абонента), используемые при работе в Системе. (Запрос на создание сертификата рабочего ключа)”.

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 криптозащиты информации (СКЗИ).
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

СПОСОБ ДОСТАВКИ ИНФОРМАЦИИ

Работа осуществляется через выделенное подключение к своему провайдеру услуг сети Интернет.

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://dbo.efbank.ru

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 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) 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, реализованного в соответствии с требованиями стандартов РФ ГОСТ Р 34.10-2001 и ГОСТ Р 34.11-94, гарантируют невозможность подделки значения ЭП любым лицом, не обладающим закрытым ключом подписи.

1.4. Стороны признают, что Квитанция, пришедшая в пакете сообщений Стороне-отправителю Документа от Стороны-получателя данного Документа, подписана ЭП, поставленной под пакетом сообщений.

1.5. Стороны должны представить комиссии следующие материалы:

- файлы, содержащие спорный Документ и полученную на него Квитанцию, выгруженные из Системы путем использования функционала Системы «Выгрузка данных для проверки подписи», а также распечатанный из Системы спорный Документ. Описание процедуры выгрузки данных для проверки подписи приведено в Документации;
- подписанные собственноручными подписями уполномоченных лиц Клиента и Банка оригиналы сведений, используемых при работе в Системе (Приложение №7 к Соглашению).

1.6. Проверка подлинности Электронного документа осуществляется посредством программных средств Системы, установленных в Банке.

2. Процедура проверки подлинности электронных сообщений и документов.

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

- проверяет подлинность ЭП под спорным Документом с использованием Открытого ключа ЭП Стороны-отправителя данного Документа;
- проверяет подлинность ЭП под Квитанцией на получение Документа с использованием Открытого ключа ЭП Стороны-получателя данного Документа;
- сверяет соответствие сведений, используемых при работе в Системе (Приложение №7 к Соглашению).

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 К ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Для минимизации рисков несанкционированного доступа к Счетам 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, не открывать ссылки в таких почтовых сообщениях, 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_____№_____выдан _____
серия номер

_____ _____
кем выдан паспорт

_____ _____
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 на подписание ЭП всех Электронных документов, предусмотренных Соглашением, направляемых Клиентом в Банк посредством Системы.
Полномочия «без права подписи» на вход в Систему, создание любых Электронных документов, предусмотренных Соглашением, установление защищенного соединения с Банком.

_____
(подпись Уполномоченного представителя Клиента)

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

Отметки АО АКБ «ЕВРОФИНАНС МОСНАРБАНК» (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

Договор № _____
об использовании электронной системы
дистанционного банковского обслуживания

г. Москва «___» _____20____г.

АО АКБ «ЕВРОФИНАНС МОСНАРБАНК», находящееся по адресу: г. Москва, ул. Новый Арбат, д. 29, в лице _____ _____, действующего на основании _____, именуемое далее «Банк», с одной стороны, и _____, находящееся по адресу: _____, в лице _____, действующего на основании _____, именуемое далее «Клиент», с другой стороны, заключили настоящий Договор о нижеследующем:

1. Настоящим Клиент заявляет о своем присоединении к действующей редакции Соглашения об использовании электронной системы дистанционного банковского обслуживания (далее – Соглашение) в порядке, предусмотренном ст.428 Гражданского кодекса Российской Федерации.
2. Все положения Соглашения, включая взаимные права и обязанности сторон, ответственность сторон, тарифы АО АКБ «ЕВРОФИНАНС МОСНАРБАНК», случаи и порядок уведомлений об операциях, совершаемых по моим банковским счетам с использованием электронного средства платежа, а также порядок внесения изменений в Соглашение, Клиенту разъяснены в полном объеме и поняты.

3. Адреса и реквизиты Сторон:

“БАНК”	**“КЛИЕНТ”**
121099, г. Москва, Новый Арбат, д. 29	
_____	_____
факс: _____	факс:_____
от имени БАНКА	**от имени КЛИЕНТА**
_____	_____
_____	_____
_____/_____/	_____/_____

Приложение № 7
к Соглашению об использовании электронной системы
дистанционного банковского обслуживания

ФОРМА

Сведения абонента (наименование криптопрофиля абонента), используемые при работе в Системе.
(Запрос на создание сертификата рабочего ключа).

Сведения об абоненте:

1. Наименование, _____
2. Место нахождения: _____
3. Почтовый адрес: _____
4. Тел._____ 5. Факс. _____

Сведения об Уполномоченном представителе абонента:

1. Фамилия, имя, отчество: _____
2. Удостоверение личности: паспорт серии _____ № _____,
выдан «___»_____ _____г _____
_____
ИНН (при его наличии, при его отсутствии – указать «отсутствует») _____
данные миграционной карты _____.

Личная подпись Уполномоченного представителя абонента _____

Личная подпись Руководителя _____ /Ф.И.О./

Параметры ключа:
Алгоритм: (указывается алгоритм)
Начало срока действия:
Окончание срока действия:
Текст открытого ключа:

Дополнительные поля открытого ключа (сертификата):

Серийный номер ключа: Название абонента: Дополнительная информация о владельце ключа: Код страны: Страна: Город: Организация: Подразделение в организации: E-mail: (идентификатор клиента в системе) Параметры издателя (центра сертификации): Имя: EVROFINANCE MOSNARBANK DBO CA Данные об издателе: EVROFINANCE MOSNARBANK

Администратор (заместитель администратора СКЗИ Банка)
_____/ФИО/