**ДОПОЛНИТЕЛЬНОЕ СОГЛАШЕНИЕ № б/н**

**к Договору банковского счета №\_\_\_\_\_\_\_\_ от «\_\_\_» \_\_\_\_\_\_\_\_\_ 20\_\_г.**

г. Самара «07» сентября 2018 года

**Общество с ограниченной ответственностью «Русфинанс Банк»**, именуемое в дальнейшем **«Банк»**, в лице Заместителя Председателя Правления Ревякиной Ольги Петровны, действующего на основании Доверенности №1792/РУК/17-07 от 01.01.2017г. с одной стороны, и \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,

(полное наименование организации)

именуемый в дальнейшем **«Клиент»**, в лице \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 (должность)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, действующего на основании

(фамилия, имя, отчество)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, с другой стороны, совместно именуемые в дальнейшем

(учредительный документ/доверенность)

**«Стороны»**, а по отдельности – **«Сторона»**, заключили настоящее Дополнительное соглашение (далее **«Соглашение»**) к Договору банковского счета №\_\_\_\_\_\_\_ от «\_\_\_\_» \_\_\_\_\_\_\_\_\_\_ 20\_\_ года (далее - **«Договор банковского счета»**) о нижеследующем:

**1. Термины и определения**

**Банковский счет** – расчетный/ корреспондентский счет Клиента в рублях РФ или текущий валютный счет в иностранной валюте, открытый в Банке и предназначенный для осуществления расчетов, связанных с предпринимательской деятельностью Клиента.

**Безотзывность перевода денежных средств** – характеристика перевода денежных средств, обозначающая отсутствие или прекращение возможности отзыва распоряжения об осуществлении перевода денежных средств (электронного платежного документа) в определенный момент времени. Наступает в момент списания денежных средств с расчетного счета Клиента.

**Блокировочное слово** – уникальное слово, определяемое Клиентом при регистрации, для блокирования работы Клиента по телефонному звонку в Банк.

**Владелец сертификата ключа проверки ЭП** – лицо, которому в установленном Соглашением порядке выдан сертификат ключа проверки ЭП.

**Внеплановая смена ключевых документов** – смена ключевых документов при компрометации (подозрении на компрометацию) ключа ЭП Клиента/ Банка или изменении состава лиц, имеющих доступ к ключам ЭП Клиента/ Банка.

**Группа подписи ключа** – полномочия ключа ЭП при подписи электронного документа. По аналогии с собственноручной подписью, образец которой есть в карточке с образцами подписей и оттиска печати должностных лиц организации, различают подпись (группу подписи). Электронный документ может исполняться Банком только после того, как под ним собрано столько подписей, сколько указано в Приложении №1 к Соглашению (по одной подписи каждой группы). ЭП может оформляться только на лицо, включенное в карточку с образцами подписей и оттиска печати. При наличии в карточке с образцами подписей и оттиска печати нескольких лиц, наделенных правом подписи, ЭП может быть оформлена на каждое из таких лиц; при наличии в карточке с образцами подписей и оттиска печати лиц, наделенных правом 1-й и 2-й подписи, количество ЭП не может быть менее двух – на лицо, наделенное правом 1-й подписи и лицо, наделенное правом 2-й подписи.

**Действующий ключ проверки ЭП** – ключ проверки ЭП, зарегистрированный в Банке, срок действия которого не истек, действие не отменено.

**Дополнительная электронная подпись** (далее – **дополнительная ЭП**) – электронная подпись, предоставляющая ее владельцу право доступа к информации о движении денежных средств по счету в режиме просмотра (получение выписки движения средств по счету и др.).

Упоминание в тексте Соглашения электронной подписи означает, в т.ч. дополнительную ЭП. Владельцу дополнительной ЭП присваивается группа подписи «нет», которая предоставляет полномочия исключительно в части получения информации о состоянии счета. Наличие дополнительной ЭП на поступившем в Банк платежном документе не является основанием для исполнения такого документа.

**Компрометация ключа** – утрата, хищение, несанкционированное копирование, передача ключа электронной подписи в линию связи в открытом виде, любые другие виды разглашения содержания ключа, а также случаи, когда нельзя достоверно установить, что произошло с носителями, содержащими ключевую информацию (в том числе случаи, когда носитель вышел из строя и доказательно не опровергнута возможность того, что данный факт произошел в результате действий злоумышленника).

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

**Ключ электронной подписи (**далее **– ключ ЭП)** – уникальная последовательность символов, предназначенная для создания электронной подписи.

**Корректная (подлинная) электронная подпись** – электронная подпись электронного документа, проверка которой с использованием соответствующего ключа проверки ЭП дает положительный результат.

**Лицо, уполномоченное доверенностью (Уполномоченное лицо)** – сотрудник Клиента, уполномоченный лицом, осуществляющим функции единоличного исполнительного органа Клиента - юридического лица или Клиентом-физическим лицом, занимающимся в установленном законом порядке предпринимательской деятельностью без образования юридического лица, представлять интересы этого лица в Банке на основании Доверенности.

**Персональный аппаратный криптопровайдер** – специализированное аппаратное устройство, предназначенное для генерации ключей ЭП и формирования ЭП под документами при осуществлении электронного документооборота между Клиентом и Банком в системе ДБО.

**Платежные документы** – в рамках настоящего Дополнительного соглашения следует понимать электронный расчетный документ, содержащий информацию о платеже Клиента, составленный в соответствии с правилами оформления расчетных (платежных) документов, установленных действующими нормативно-правовыми актами.

**Окончательность перевода денежных средств** – характеристика перевода денежных средств, обозначающая предоставление денежных средств получателю средств в определенный момент времени. Наступает в момент зачисления денежных средств на счет получателя (корреспондентский счет банка получателя).

**Перевод денежных средств** – действия Банка по переводу денежных средств в рамках применяемых форм безналичных расчетов по предоставлению получателю средств денежных средств, перечисляемых с расчетного счета Клиента.

**Плановая смена ключевых документов** – смена ключевых документов по окончанию срока действия сертификата ключа проверки ЭП Клиента/ Банка.

**Сертификат ключа электронной подписи Клиента** – документ на бумажном носителе, выданный Банком либо доверенным лицом Банка и подтверждающий принадлежность ключа проверки ЭП владельцу сертификата ключа проверки ЭП, заверенный подписью руководителя Клиента и имеющий оттиск печати Клиента.

**Система «Интернет-Клиент-Банк»/Дистанционное банковское обслуживание (далее – ДБО) /Система ДБО)** – комплекс программно-технических средств и организационных мероприятий для создания и передачи электронных платежных документов по каналам связи.

**Средства электронной подписи (**далее – **средства криптографической защиты конфиденциальной информации**/**СКЗИ)** – сертифицированные ФСБ шифровальные (криптографические) средства, используемые для реализации хотя бы одной из следующих функций – создание ЭП, проверка ЭП, создание ключа ЭП и ключа проверки ЭП. К ним относятся:

* реализующие криптографические алгоритмы преобразования информации аппаратные, программные и аппаратно-программные средства, системы и комплексы, обеспечивающие безопасность информации при ее обработке, хранении и передаче по каналам связи;
* реализующие криптографические алгоритмы преобразования информации аппаратные, программные и аппаратно-программные средства, системы и комплексы защиты от навязывания ложной информации, включая средства имитозащиты и ЭП;
* аппаратные, программные и аппаратно-программные средства, системы и комплексы изготовления и распределения ключевых документов для СКЗИ независимо от вида носителя ключевой информации;
* прикладная библиотека защиты информации – программный или аппаратный модуль, взаимодействующий с Системой ДБО, обеспечивающий защиту информации в соответствии с утвержденными стандартами (ГОСТ 28147-89, ГОСТ Р34.10-94, ГОСТ Р34.10-2001, ГОСТ Р34.11-2001, ГОСТ Р34.11-94, ГОСТ Р34.10-2012, ГОСТ Р34.11-2012) и сертифицированный в соответствии с действующим законодательством;

**Шифрование** – криптографическое преобразование данных, позволяющее предотвратить доступ неуполномоченных лиц к содержимому зашифрованного электронного документа.

**Электронный документ** – документ, в котором информация представлена в электронно-цифровой форме.

**Электронная подпись (**далее **– ЭП)** – информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемому электронному документу) или иным образом связана с такой информацией и которая используется для определения лица (владельца сертификата ключа подписи), подписывающего информацию.

Под электронной подписью в настоящем Дополнительном соглашении понимается усиленная неквалифицированная электронная подпись, отвечающая требованиям Федерального закона от 06.04.2011 №63-ФЗ «Об электронной подписи».

**2. Предмет Соглашения**

2.1. Банк и Клиент устанавливают между собой Соглашение к порядку проведения расчетных операций по Договору банковского счета о выполнении расчетных операций в электронной форме с использованием системы «Интернет-Клиент-Банк».

2.2. Соглашение устанавливает порядок приема к исполнению Банком электронных платежных документов Клиента, а также документов, указанных в Приложении №1 к Соглашению, переданных по системе ДБО.

2.3. Использование электронных платежных документов не изменяет содержание установленных законодательством и Договором банковского счета прав и обязанностей участников расчетов, содержания платежных документов и правил заполнения их реквизитов.

2.4. Действие Соглашения распространяется в отношении всех электронных платежных документов Клиента, подписанных ЭП, за исключением расчетов с использованием иных установленных законодательством или Договором банковского счета форм расчетов, и не изменяет содержания установленных законодательством и Договором банковского счета прав и обязанностей участников расчетов, содержания платежных документов и правил заполнения их реквизитов.

2.5. При проведении расчетов между Клиентом и Банком могут использоваться как электронные документы, подписанные ЭП, так и расчетные документы на бумажных носителях, оформленные в установленном действующим законодательством и правилами Банка России порядке при использовании соответствующих форм расчетов.

2.6. Банк и Клиент признают, что при использовании персонального аппаратного криптопровайдера закрытый ключ не извлекаем.

**3. Соглашения сторон**

3.1. Стороны признают, что ЭП в электронном документе равнозначна собственноручной подписи в документе на бумажном носителе при одновременном соблюдении следующих условий:

3.1.1. ключ проверки ЭП, относящийся к этой ЭП, не утратил силу (действует) на момент проверки или на момент подписания электронного документа при наличии доказательств, определяющих момент подписания;

3.1.2. подтверждена подлинность ЭП в электронном документе. Электронные документы, заверенные ЭП Клиента (Приложение №1к Соглашению), хранящиеся в виде записи в контрольных архивах или в виде отдельных файлов, юридически равнозначны соответствующим документам на бумажном носителе, подписанным уполномоченным(-и) представителем(-ми) Клиента и имеющим оттиск печати Клиента, обладают юридической силой и подтверждают наличие правовых отношений между Сторонами. Электронные документы, исходящие от Клиента без необходимой ЭП Клиента, не имеют юридической силы, Банком не рассматриваются и не исполняются;

3.1.3. ЭП используется в соответствии со сведениями, указанными в сертификате ключа подписи.

3.2. Стороны признают, что используемое сертифицированное СКЗИ, которое обеспечивает простановку (проверку) ЭП, достаточно для подтверждения подлинности и авторства электронных документов, а также разбора конфликтных ситуаций.

3.3. Стороны признают, что обеспечиваемое системой ДБО шифрование передаваемых электронных документов достаточно для защиты информации от несанкционированного доступа.

3.4. Стороны признают, что при изменении электронного документа, заверенного ЭП, электронная подпись становится некорректной, то есть проверка ЭП дает отрицательный результат.

3.5. Стороны признают, что подделка ЭП Клиента, то есть создание корректной ЭП электронного документа от имени Клиента, невозможна без знания ключа ЭП Клиента.

3.6. Стороны признают, что электронные документы с ЭП Клиента, являются доказательным материалом для решения спорных вопросов в соответствии с Положением о порядке проведения технической экспертизы при возникновении спорных ситуаций (см. раздел 3 Приложения №12к Соглашению). Электронные документы, не имеющие необходимого количества ЭП, при наличии спорных вопросов, не являются доказательным материалом.

3.7. Стороны признают, что ключ проверки ЭП Клиента, указанный в заверенном подписью руководителя и оттиском печати Клиента сертификате ключа проверки ЭП Клиента, принадлежит Клиенту.

3.8. Стороны признают необходимость архивного хранения электронных документов, заверенных ЭП, не менее пяти лет.

3.9. Стороны признают в качестве единой шкалы времени - «московское время». Контрольным является время системных часов аппаратных средств Банка.

**4. Порядок обслуживания Клиента в системе ДБО**

4.1. Клиент передает Банку по каналу связи распоряжения на перевод денежных средств в электронной форме (далее - электронные платежные документы), которые оформляются в рамках применяемых форм безналичных расчетов, установленных действующим законодательством и нормативно-правовыми актами ЦБ Российской Федерации, а также запросы на отзыв электронных платежных документов, отправленных Клиентом в тот же день ранее, и не исполненных к моменту направления запроса на отзыв. Клиент вправе передавать Банку по каналу связи иные документы в электронной форме, включенные в перечень, приведенный в Приложении №1 к Соглашению.

4.2. При невозможности передачи документов в Банк с использованием системы ДБО документы могут поступить от Клиента на бумажном носителе.

4.3. Электронный документ должен быть оформлен надлежащим образом Клиентом и подписан ЭП Клиента. При получении электронного документа Банк производит проверку корректности ЭП Клиента, проверку правильности заполнения реквизитов документа.

4.4. Банк принимает к исполнению правильно составленный электронный платежный документ, прошедший проверку корректности электронной подписи Клиента, в результате чего статус сообщения Клиента в системе ДБО у Клиента изменяется с «Отправлен» на «В обработке».

4.5. В случае неправильного составления электронного платежного документа электронный платежный документ не принимается Банком к исполнению, сообщению Клиента в системе ДБО у Клиента изменяется статус с «Отправлен» на «Ошибочный» с указанием причины ошибки.

4.6. Банк принимает к исполнению электронные платежные документы Клиента, прошедшие подтверждение их достоверности, текущим операционным днем, если они были получены Банком: внутрирегиональные до 16 часов 00 минут, иногородние (межрегиональные) до 15 часов 30 минут по московскому времени. В противном случае, документы могут быть обработаны как текущим, так и следующим операционным днем по усмотрению Банка.

4.7. Безотзывность перевода денежных средств, осуществленного на основании правильно составленного электронного платежного документа, наступает с момента списания денежных средств с расчетного счета Клиента.

4.8. Окончательность перевода денежных средств, осуществленного на основании правильно оформленного электронного платежного документа, наступает:

4.8.1. в случае, если расчетный счет получателя средств открыт в Банке – в момент зачисления денежных средств на расчетный счет получателя;

4.8.2. в случае, если расчетный счет получателя средств открыт в другой кредитной организации – в момент зачисления денежных средств на корреспондентский счет кредитной организации, обслуживающей получателя средств.

4.9. Инициатива в установлении связи с Банком принадлежит Клиенту.

**5. Права и обязанности Банка**

**5.1. Банк обязан:**

5.1.1. Обладать организационно-техническим оборудованием, необходимым для эксплуатации системы ДБО в исправном состоянии и количестве, достаточном для надлежащего обслуживания Клиента, располагать квалифицированными кадрами, необходимыми для работы с Клиентом с использованием системы ДБО.

5.1.2. Содержать компьютеры Банка, на которых установлена серверная часть системы ДБО в служебном помещении, исключающем доступ посторонних лиц.

5.1.3. Не допускать появления в компьютере Банка, на котором установлена система ДБО вредоносных или деструктивных программ (вирусов).

5.1.4. Обеспечить функционирование системы ДБО и обслуживание Клиента в соответствии с режимом обслуживания.

5.1.5. Передать Клиенту следующий набор документации и программно-технических средств, необходимый для работы с расчетными документами в электронной форме:

* программное обеспечение системы ДБО;
* инструкция по эксплуатации системы ДБО;
* средство криптографической защиты информации - персональный аппаратный криптопровайдер. Персональный аппаратный Крипто-провайдер предоставляется Банком Клиенту во временное владение и пользование при заключении настоящего Дополнительного соглашения и Акта соответствия требованиям к организационно-техническому оборудованию и программно-аппаратным средствам Клиента (см. Приложение №2 к Соглашению). Дополнительный персональный аппаратный криптопровайдер предоставляется по заявлению Клиента (см. Приложение №8 к Соглашению).

Факт передачи программно-технических средств фиксируется двусторонним Актом приема-передачи (см. Приложение №3 к Соглашению).

5.1.6. Обеспечить Клиенту необходимое сопровождение и техническую поддержку (консультации по вопросам эксплуатации, предоставление дополнительной информации, необходимой для организации электронного документооборота). Техническая поддержка осуществляется Банком с 08 часов 00 минут до 17 часов 00 минут московского времени по рабочим дням по тел. **(846) 276-44-11.**

5.1.7. При отрицательном результате проверки корректности электронной подписи Клиента на электронных платежных документах, а также в случае некорректного заполнения цифровых реквизитов платежных документов не производить соответствующую расчетную операцию, вернуть Клиенту эти расчетные документы как не принятые без исполнения и сообщить об этом Клиенту путем изменения статуса сообщения Клиента с «Отправлен» на «Ошибочный» с указанием причины ошибки.

Сообщить сведения об исполненных документах Клиенту путем изменения статуса сообщения, которое Клиент принимает во время очередного сеанса связи с Банком, в системе ДБО у Клиента, с «В обработке» на «Проведен».

5.1.8. По письменному требованию Клиента объяснить причину прекращения принятия электронных документов от Клиента.

5.1.9 При изменении формы Платежных документов и при изменении перечня электронных платежных документов, реализуемых через систему ДБО, в плановом порядке заменить Клиенту версию программного обеспечения системы ДБО и предоставить новые формы Платежных документов.

5.1.10 Обеспечивать подготовку и передачу через систему ДБО электронным способом по мере проведения операций (формирования документов) следующих документов (информации) для Клиента:

* выписки по состоянию счетов Клиента в Банке, которые создаются на основе стандартных банковских выписок и являются документами отчетности Клиента;
* справки о подтверждающих документах (в порядке, предусмотренном действующим валютным законодательством РФ);
* ведомости банковского контроля (в порядке, предусмотренном действующим валютным законодательством РФ);
* подтверждение принятия к исполнению электронных платежных документов, а также электронных документов по валютному контролю Клиента, посредством изменения статуса документа у Клиента при повторном сеансе связи с Банком (повторный сеанс связи осуществляется со стороны Клиента);
* возврат ошибочных электронных платежных документов Клиента с указанием ошибки при повторном сеансе связи с Банком (повторный сеанс связи осуществляется со стороны Клиента);
* возврат отозванных электронных платежных документов Клиента посредством изменения статуса документа на «Документ отложен» при повторном сеансе связи с Банком (повторный сеанс связи осуществляется со стороны Клиента);
* персональные и циркулярные письма официального характера;
* справочник банков БИК;
* другие документы по согласованию с Клиентом.

5.1.11. Сохранять конфиденциальность принимаемой и передаваемой информации.

5.1.12. Зарегистрировать в системе ДБО ключи проверки ЭП Клиента при условии предоставления Клиентом в Банк Заявления на регистрацию ключей ЭП (Приложение №5 к Соглашению) и подписанных сертификатов ключей проверки ЭП Клиента (Приложение №6 к Соглашению), а в случае предоставления уполномоченным лицом Клиента – еще и Доверенности (Приложение №4 к Соглашению) в срок до 5 рабочих дней с момента предоставления этих документов.

**5.2. Банк имеет право:**

5.2.1. По своему усмотрению приостановить принятие от Клиента электронных документов и потребовать от Клиента смены пары ключей ЭП Клиента, направив уведомление через систему ДБО или по телефону.

5.2.2. При подозрении на возможность несанкционированного доступа к передаваемой от имени Клиента информации с целью осуществления переводов денежных средств лицами, не обладающими правом распоряжения этими денежными средствами приостановить работу Клиента в системе ДБО и не производить исполнения полученного электронного документа, сообщив Клиенту о возможных рисках при несанкционированном доступе не позднее дня, следующего за днем его получения и рекомендовать меры по их снижению соблюдая требования п.5.1.2, п.6.1.2,п.6.1.3, п.6.1.18, п.6.1.19, п.6.1.23, п.6.1.25 и затребовать от Клиента оформления документа на бумажном носителе с подписью уполномоченных лиц и оттиском печати Клиента.

5.2.3. После предварительного предупреждения отказать Клиенту в приеме платежных документов в электронной форме в случае непредставления Клиентом в течение 5 рабочих дней со дня доставки Клиенту электронного сообщения Банка о предоставлении документов (сведений) о совершаемых операциях. В этом случае Банк принимает от Клиента только надлежащим образом оформленные расчетные документы на бумажных носителях, до фактического предоставления запрошенных документов (сведений).

5.2.4. Отказать в исполнении электронного платежного документа Клиента в случае несоответствия реквизитов документа обязательным реквизитам, установленным действующим законодательством РФ и правилами Банка России.

5.2.5. Изготавливать копии с Платежных документов Клиента, подписанных ЭП, на бумажных носителях, при этом сохранение ЭП Клиента на копиях документов на бумажных носителях необязательно.

5.2.6. В случае невнесения Клиентом платы за рассчетно-кассовое обслуживание (далее – РКО) в соответствии с Тарифами и/или платы за ДБО, приостановить обслуживание Клиента в системе ДБО, с предварительно направив Клиенту уведомление по системе ДБО об этом. В случае невнесения Клиентом вышеуказанной платы по истечении 60 календарных дней с момента возникновения задолженности, Соглашение считается прекратившим свое действие.

5.2.7. Банк имеет право без согласования с Клиентом блокировать всю работу Клиента в системе (за исключением возможности обмена с Банком письмами произвольного формата), в случае нарушения Клиентом установленных сроков предоставления документов, затребованных Банком в соответствии с Договором банковского счета и Дополнительным соглашением к Договору банковского счета, до момента получения Банком требуемых документов. Банк, в день блокировки работы Клиента в системе отправляет последнему соответствующее уведомление. До момента разблокировки Клиента в системе, Банк принимает расчетные и прочие документы от Клиента на бумажном носителе.

5.2.8. В случае изменений в системе ДБО Банк обеспечивает своевременное обновление информации по эксплуатации системы ДБО на портале.

5.2.9. Банк имеет право отказать Клиенту в приеме Платежных документов подписанных Электронной подписью, по основаниям, предусмотренным законодательством о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма.

5.2.10. В одностороннем порядке вносить в настоящее Соглашение изменения. Информация об изменениях и новая редакция Соглашения доводится до сведения Клиента путем размещения соответствующей информации с полным текстом изменений в помещении Банка и/или на сайте Банка, а также другими способами по выбору Банка за 14 (четырнадцать) календарных дней до момента введения новой редакции Соглашения.

5.2.11. В одностороннем порядке инициировать замену персонального аппаратного криптопровайдера Клиента и потребовать от Клиента смены пары ключей ЭП Клиента.

**6. Права и обязанности Клиента**

**6.1. Клиент обязан:**

6.1.1. Обладать организационно-техническим оборудованием, необходимым для эксплуатации системы ДБО в исправном состоянии и количестве, достаточном для надлежащего использования системы ДБО. Организационно-техническое оборудование Клиента должно отвечать требованиям (Приложение №2 к Соглашению), предъявляемым к этому оборудованию для осуществления работы в системе ДБО.

6.1.2. Содержать компьютер, на котором установлена клиентская часть системы ДБО, в исправном состоянии, в помещении, доступ в которое разрешен только тем сотрудникам Клиента, которые непосредственно работают в системе ДБО.

6.1.3. Не вносить изменений в программно-технические средства системы без согласования с Банком, не передавать их третьим лицам. Внесение изменений в программно-технические средства системы ДБО оформляется соответствующим Актом (Приложение №2 к Соглашению).

6.1.4. Подписать Акт соответствия требованиям, предъявляемым к АРМ Клиента, на котором установлена система ДБО (Приложение №2 к Соглашению).

6.1.5. Перед началом эксплуатации системы ДБО установить программное обеспечение согласно Инструкции по эксплуатации системы ДБО (далее - Инструкция), полученной в Банке.

6.1.6. Устанавливать на компьютер, используемый для работы в системе ДБО, межсетевые экраны.

6.1.7. Использовать пароли, отвечающие требованиям, указанным в п.6.1.20 Соглашения, для всех учетных записей операционной системы на компьютере, используемом для работы в системе ДБО.

6.1.8. Следить, чтобы обновления операционных систем и антивирусных программ, установленных на компьютер, используемый для работы в системе ДБО, были актуальными.

6.1.9. С компьютера, предназначенного для работы в системе ДБО, избегать посещения сайтов сомнительного содержания, а также открытия без проверки файлов и перехода по ссылкам, полученным в почтовых сообщениях, сообщениях систем обмена мгновенными сообщениями и др.

6.1.10. Не отвечать на сообщения, полученные от лиц, запрашивающих личные сведения Клиента, информирующих о необходимости срочного ответа на полученное сообщение с дальнейшим подтверждением личных данных Клиента.

6.1.11. Перед началом генерации ключей ЭП получить в Банке средство криптографической защиты.

6.1.12. Самостоятельно производить генерацию ключа ЭП и ключа проверки ЭП только с помощью персонального аппаратного криптопровайдера в соответствии с Инструкцией.

6.1.13. Для завершения регистрации ключа проверки ЭП, заполнить и передать в Банк подписанный сертификат ключа проверки ЭП Клиента (Приложение №6 к Соглашению) в двух экземплярах, а также Заявление на регистрацию ключей ЭП (Приложение №5 к Соглашению) не позднее 25 календарных дней с момента создания ключей ЭП.

6.1.14. Использовать предоставленное средство криптографической защиты информации только в системе ДБО, без права продажи или передачи каким-либо другим способом иным физическим или юридическим лицам, обеспечивать возможность контроля со стороны федеральных органов за соблюдением требований и условий осуществления лицензионной деятельности.

6.1.15. Обеспечивать сохранность и целостность программного комплекса системы ДБО и средства криптографической защиты информации.

6.1.16. Строго соблюдать правила эксплуатации системы ДБО.

6.1.17. В случае повреждения персонального аппаратного криптопровайдера и иных обстоятельств в том числе, препятствующих дальнейшее его использование, передать его в Банк, оформив передачу Актом приема-передачи (Приложение №9 к Соглашению).

6.1.18. В случае расторжения Соглашения:

* + - * удалить установленное на компьютер программное обеспечение ДБО и СКЗИ, а также уничтожить полученный в Банке носитель с дистрибутивами системы ДБО и СКЗИ и все его копии;
			* вернуть Банку не позднее 1 рабочего дня, следующего за днем прекращения настоящего Соглашения, персональный аппаратный криптопровайдер по Акту приема-передачи (Приложение №9 к Соглашению), даже в случае его повреждения;
			* в случае утраты персонального аппаратного криптопровайдера оформить и предоставить в Банк Акт об утрате (Приложение №10 к Соглашению).

6.1.19. Хранить в тайне от посторонних лиц пароль для получения доступа к ключам ЭП Клиента.

6.1.20. Соблюдать правила выбора пароля:

* + - * пароль выбирается самостоятельно;
			* если пароль записан на бумаге, то хранится в месте, недоступном для посторонних лиц;
			* пароль содержит не менее 6 различных символов;
			* должен меняться не реже 1 раза в 60 календарных дней;
			* пароль обязательно меняется, если он стал известен постороннему лицу;
			* в качестве пароля не используются: последовательности, состоящие из одних цифр (в том числе даты, номера телефонов, номер автомобиля и т.п.), последовательности повторяющихся букв или цифр; подряд идущие в раскладке клавиатуры или в алфавите символы; имена и фамилии; ИНН или другие реквизиты Клиента.

6.1.21. При работе с ключевой информацией:

* + - * не оставлять включенной без присмотра свою рабочую станцию (компьютер);
			* подключать персональный аппаратный криптопровайдер только на период работы в системе ДБО;
			* перед подключением персонального аппаратного криптопровайдера проверить рабочую станцию (компьютер) на отсутствие программных закладок и вирусов.

6.1.22. Производить плановую смену ключей ЭП не реже 1 раза в год, не позднее, чем за 15 календарных дней до окончания срока действия сертификата ключа проверки ЭП Клиента (Приложение №6 к Соглашению). По истечении срока действия сертификата ключа проверки ЭП Клиента происходит автоматическая блокировка ключей. Каждый новый сертификат ключа ЭП, подписанный Сторонами, автоматически отменяет действие Сертификата ключа данного пользователя.

Ключи ЭП Клиента считаются действующими с даты и времени регистрации Банком связанных с этими ключами ключей поверки ЭП, и до момента наступления одного из следующих событий:

* истечения срока действия сертификата ключа проверки ЭП;
* аннулирования действия сертификата ключа проверки ЭП;
* плановой или внеплановой смены ключей ЭП Клиента;
* прекращения действия Договора ДБО.

6.1.23. Извещать Банк обо всех случаях компрометации ключей ЭП.

6.1.24. Извещать Банк об увольнении работника(ов), имеющего(их) доступ к системе ДБО любым доступным способом (информационным сообщением через ДБО, по электронной почте и т.п.).

6.1.25. Производить внеплановую смену ключей в случае компрометации ключей Клиента и каждый раз при изменении состава лиц, работающих в системе ДБО.

6.1.26. Немедленно сообщить Банку обо всех случаях, свидетельствующих о попытках посторонних лиц получить доступ к системе ДБО с целью совершения несанкционированной передачи средств, а также при обнаружении на компьютере, с которого производится работа в системе ДБО, вируса, вызывающего подозрения в компрометации ключей. При подтверждении этих фактов Клиент обязан немедленно заблокировать действующие открытые ключи ЭП, сгенерировать и зарегистрировать в Банке новые ключи.

6.1.27. Клиент берет на себя полную ответственность и обязуется самостоятельно обеспечить целостность, неразглашение, нераспространение ключей ЭП, а также обязуется хранить ключи ЭП в месте, исключающем доступ посторонних лиц к ключам ЭП. Персональный аппаратный криптопровайдер должен храниться исключительно у уполномоченных лиц. В случае потери персонального аппаратного криптопровайдера, кражи, Клиент обязан незамедлительно заявить о компрометации утерянных ключей ЭП в Банк в порядке, предусмотренном п. 6.2.6. Соглашения.

6.1.28 По требованию Банка сгенерировать новую пару ключей ЭП Клиента и зарегистрировать новый ключ проверки ЭП Клиента в Банке.

6.1.29. Регулярно производить оплату в соответствии с действующими Тарифами Банка за РКО, включая плату за ДБО.

6.1.30. Устанавливать связь с Банком в порядке, установленным разделом 4 Соглашения, для получения от Банка подтверждений о результатах обработки переданных Клиентом документов (не ранее, чем через 1 (один) час после отправки документа, но не позднее следующего рабочего дня). Осуществлять прочтение подготовленных для Клиента служебных электронных сообщений не позднее дня, следующего за днем их получения. Любая просрочка в выполнении Банком своей обязанности, которая произошла из-за отсутствия инициативы Клиента в связи с Банком, не влечет за собой ответственности Банка.

6.1.31. Заполнять электронные документы в соответствии с действующим законодательством и нормативно-правовыми актами.

6.1.32. Представлять в Банк до совершения валютной операции все необходимые документы для валютного контроля.

6.1.33. В течение 10 (десяти) календарных дней после выдачи ему выписок письменно сообщить Банку о суммах, ошибочно записанных в кредит или дебет счета. При не поступлении от Клиента в указанные сроки возражений совершенные операции и остаток средств на счете считаются подтвержденными.

6.1.34. Во всех случаях получения отрицательного результата при проверке электронной подписи принимаемого документа (подпись воспринимается как фальсифицированная), фиксировать все относящиеся к этому случаю фактические данные и файлы.

6.1.35. По требованию Банка передавать ему письменное изложение обстоятельств по случаям, связанным с приемом и отправкой документов, ЭП под которыми не была подтверждена как подлинная, а также всех случаев несанкционированных электронных переводов и все относящиеся к таким случаям файлы.

6.1.36. В целях исполнения положений законодательства о национальной платежной системе Клиент обязан по факту обнаружения незамедлительно информировать Банк:

* в случае обнаружения вредоносного кода или факта воздействия вредоносного кода;
* в случае нарушения требований к обеспечению защиты информации при осуществлении переводов.

6.1.37. Выполнять рекомендации по обеспечению информационной безопасности (Приложение №12 к Соглашению).

**6.2. Клиент имеет право:**

6.2.1. На основании имеющейся у Банка лицензии ФСБ осуществлять эксплуатацию, предоставленного Банком сертифицированного ФСБ средства криптографической защиты информации без получения собственной лицензии ФСБ.

6.2.2. Получить набор документации и программно-технических средств в Банке, уполномоченное лицо Клиента – только при наличии Доверенности (Приложение №4 к Соглашению).

6.2.3. Получать консультации и инструкции по процедурам работы программного обеспечения и средства криптографической защиты информации, а также формированию и регистрации ключей от сотрудников Банка. Одновременно с использованием системы ДБО работать с Банком в обычном порядке, с использованием документов на бумажных носителях.

6.2.4. Предоставлять Банку свои предложения по совершенствованию работы в системе ДБО.

6.2.5. По своему усмотрению генерировать новые пары ключей ЭП Клиента и регистрировать в Банке новые ключи проверки ЭП Клиента при условии предоставления в Банк Заявления на регистрацию ключей ЭП (Приложение №5 к Соглашению) и подписанного в двух экземплярах сертификата ключа проверки ЭП Клиента (Приложение №6 к Соглашению) не позднее 25 календарных дней с момента создания ключей ЭП.

6.2.6. Позвонив по телефону, указанному в реквизитах Соглашения, в Банк и произнеся блокировочное слово, указанное в реквизитах Соглашения, до письменного уведомления, потребовать от Банка приостановить операции со счетом с использованием скомпрометированного ключа ЭП через систему ДБО, и после последующего подтверждения блокировки в письменной форме (Приложение №7 к Соглашению) временно блокировать свою работу в системе ДБО. До момента постановки отметки об исполнении на письменном уведомлении Банк не несет ответственности за возможные убытки, возникшие у Клиента в результате незаконного использования ключей ЭП.

6.2.7. Требовать от Банка предоставления на бумажном носителе копий полученных Банком электронных документов с проставлением на них соответствующих отметок Банка (об исполнении и др.). Указанные документы предоставляются уполномоченному лицу Клиента при его явке в Банк.

6.2.8. В день передачи Банку электронного платежного документа направить Банку отзыв указанного документа до момента наступления безотзывности перевода. Отзыв направляется с помощью встроенных функций системы ДБО, либо в произвольной форме в письменном виде с подписью руководителя и печатью Клиента. Отзыв должен содержать однозначное указание на неисполнение конкретного ранее переданного документа и не содержать терминов, допускающих произвольное толкование.

6.2.9. Предоставить в Банк заявление на определение ограничений параметров операций, которые могут осуществляться Клиентом с использованием системы ДБО, по форме Приложения №11к Соглашению**.**

**7. Совместные обязательства и ответственность Сторон**

7.1. Банк не несёт ответственности за ущерб, причинённый Клиенту в результате использования третьими лицами ключа ЭП Клиента.

7.2. Банк не несет ответственности за возможные помехи в линиях связи, прекращение работы в системе ДБО из-за отключения электроэнергии и повреждения линий связи, а также программно-аппаратные сбои системы ДБО, если указанные обстоятельства возникли не по вине сотрудников Банка.

7.3. Банк не несет ответственности перед Клиентом, в случае, если в аппаратную или программную конфигурацию технических средств. Клиента были внесены изменения без согласования с Банком.

7.4. Банк не несет ответственности за нарушения в работе системы ДБО, вызванные программным обеспечением Клиента, установленным на том же компьютере, что и система ДБО и не входящим в состав программно-технических средств системы ДБО.

7.5. Банк не несет ответственности за нарушения в работе программного обеспечения Клиента, установленного на том же компьютере, что и система ДБО, возникшие в результате работы последней.

7.6. При расторжении Соглашения Стороны несут ответственность по всем электронным документам с электронными подписями Клиента, в соответствии с действующим законодательством РФ, поступившим до момента расторжения Соглашения.

7.7. В случае возникновении конфликтных ситуаций между Клиентом и Банком, Стороны обязуются участвовать в рассмотрении конфликтов в соответствии с Положением о порядке проведения технической экспертизы при возникновении спорных ситуаций (см. раздел 3 Приложения №12 к Соглашению), выполнять требования указанного Положения и нести ответственность согласно выводам по рассмотрению конфликтной ситуации.

7.8. Стороны обязуются вести архивы подписанных ЭП электронных документов, соответствующие им ключи проверки ЭП, и осуществлять их хранение в течение срока, установленного для хранения эквивалентных документов на бумажных носителях.

7.9. Стороны обязуются самостоятельно следить за окончанием срока действия сертификатов ключей проверки своих ЭП.

7.10. Стороны не несут ответственности за неисполнение электронных документов в случае отрицательного результата проверки ЭП.

7.11. Стороны освобождаются от ответственности за неисполнение или ненадлежащее исполнение взятых по настоящему Соглашению обязательств в случае возникновения обстоятельств непреодолимой силы, к которым относятся: стихийные бедствия, пожары, аварии, отключения электроэнергии, повреждение линий и устройств связи, массовые беспорядки, забастовки, военные действия, противоправные действия третьих лиц, вступление в силу законодательных актов, актов органов федеральных или местных органов власти и обязательных для исполнения одной из сторон, прямо или косвенно запрещающих указанные в Соглашении виды деятельности или препятствующие выполнению Сторонами своих обязательств по Соглашению, если Сторона, пострадавшая от их влияния, доведет до сведения другой Стороны известие о случившемся в срок до 5 (пяти) рабочих дней после возникновения этих обстоятельств. Приведенный перечень обстоятельств непреодолимой силы не является исчерпывающим, в качестве таких обстоятельств могут рассматриваться иные действия и события, независящие от воли Сторон, препятствующие исполнению ими обязательств по настоящему Соглашению.

**8. Ответственность сторон**

8.1. Если в результате работы разрешительной комиссии выяснится, что у Стороны, отправившей документ, произошел сбой в работе программно-аппаратных средств или было подозрение на попытку хищения средств, отказ другой Стороны от исполнения документа является правомерным.

8.2. Клиент несет полную ответственность за все убытки, которые могут возникнуть у него в результате несанкционированного перевода средств из-за нарушения им условий Соглашения.

8.3. Банк несет ответственность за несоблюдение сроков проведения расчетных операций по счету Клиента, при условии надлежащим образом оформленного Клиентом платежного (расчетного) документа.

8.4. В случае выявления Клиентом хищения денежных средств в системе ДБО, либо подозрительного перевода денежных средств, необходимо воспользоваться Методическими рекомендациями (см.Приложение №12 к Соглашению).

**9. Срок действия Соглашения и порядок его досрочного расторжения**

9.1. Соглашение вступает в силу с момента подписания его Сторонами и действует неограниченное время.

9.2. Соглашение может быть расторгнуто по Соглашению Сторон, а также в любое время по Заявлению Клиента.

9.3. Соглашение может быть расторгнуто в случае утверждения Банком Соглашения на осуществление безналичных платежей с использованием системы дистанционного обслуживания в новой редакции с предварительным уведомлением о расторжении, направленным Клиенту не позднее 1 месяца до даты расторжения.

9.4. Соглашение считается расторгнутым в случае, если по истечении 6 месяцев с даты прекращения действия сертификата проверки ключей ЭП Клиентом не были предоставлены сведения о вновь созданных ключах ЭП при условии направления Банком уведомления Клиенту по системе ДБО или в письменном виде по истечении 2 месяцев со дня направления такого уведомления.

**10. Заключительные положения**

10.1. Споры по Соглашению решаются путем переговоров с учетом взаимных интересов в соответствии с «Положением о порядке проведения технической экспертизы при возникновении спорных ситуаций» (Приложение №12 к Соглашению), а при не достижении соглашения – в судебном порядке.

10.2. Соглашение составлено и подписано в двух экземплярах, по одному для каждой Стороны, оба экземпляра имеют одинаковую силу.

**11. Адреса и реквизиты сторон**

|  |  |
| --- | --- |
| **ООО «Русфинанс Банк»** | **Краткое наименование юридического лица** |
| ИНН 5012003647 КПП 631501001 | ИНН/ КПП |
| 443013, г. Самара, ул. Чернореченская, д.42А | Адрес места нахождения |
| Корр.счет 30101810622023601975 |  |
| в ОТДЕЛЕНИИ САМАРА Волго-Вятского ГУ Банка России |  |
| БИК 043601975 | Тел./Факс |
| Тел./Факс (846) 247-89-11/ (846) 276-44-11 | Блокировочное слово -  |
| **От Банка:** | **От Клиента:** |
| Заместитель Председателя Правления | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_должность |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/О.П.Ревякина/ | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ /\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/подпись расшифровка подписи |
| **М.П.** | **М.П.** |

Приложение №1 к Дополнительному соглашению

№\_\_\_\_\_от «\_\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_ года

**Перечень электронных документов, передаваемых по системе ДБО и необходимое количество ЭП**

Настоящим прошу осуществить подключение к системе дистанционного банковского обслуживания

*(полное или краткое наименование организации)*

в соответствии с условиями Дополнительного соглашения для получения следующих услуг:

|  |  |  |
| --- | --- | --- |
|  | **Наименование электронного документа** | **Количество ЭП** |
|  | **Рублевые документы** |  |
| 1 | Платежное поручение |  |
| 2 | Заявление на аккредитив |   |
| 3 | Заявление об акцепте / отказе от акцепта |   |
|   | **Валютные документы** |   |
| 1 | Заявление на перевод иностранной валюты |   |
| 2 | Поручение на покупку иностранной валюты |   |
| 3 | Поручение на продажу иностранной валюты  |   |
| 4 | Паспорт сделок по контракту  |   |
| 5 | Ведомость банковского контроля |   |
| 6 | Справка о подтверждающих документах  |   |
|   | **Информационные документы1** |   |
| 1 | Письма и заявки  |  |
| 2 | Выписки  |  |
| 3 | Уведомление о поступлении иностранной валюты |   |
| 4 | Обосновывающие документы, связанные с проведением валютных операций |  |
| 5 | Подтверждающие документы, связанные с проведением валютных операций |  |
| 6 | Сообщение с файлом  |  |
| 7 | Сообщение свободного формата |  |
|  |  |  |

|  |  |
| --- | --- |
| От Банка: | От Клиента: |
| Заместитель Председателя Правления | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/О.П.Ревякина/ | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ /\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/ |
| М.П. | М.П. |
|  |  |

**1** Каждый владелец ключа ЭП, надлежащим образом наделенный правом подписи платежных документов Клиента, имеет право единолично подписывать информационные (неплатежные) документы Клиента.

Приложение №2 к Дополнительному соглашению

№\_\_\_\_от «\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_ года

**Акт соответствия требованиям к организационно-техническому оборудованию**

**и программно-аппаратным средствам Клиента**

 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

*(полное или краткое наименование организации)*

в лице\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, действующего(ей) на основании \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ подтверждает, что автоматизированное рабочее место, используемое в дальнейшем для работы в системе ДБО, соответствует требованиям, предъявляемым к организационно-техническому оборудованию и программно-аппаратным средствамКлиента.

1. Минимальные и рекомендуемые параметры:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **п/п** | **Параметры** | **Минимальные** | **Рекомендуемые** | **На автоматизированном рабочем месте Клиента установлено** |
| 1 | Процессор | Intel Celeron1 GHz | от 1.6 GHz |  |
| 2 | Оперативная память | 512 Mb | 1Gb |  |
| 3 | Объем дискового пространства для инсталляции | 100mb | 100mb |  |
| 4 | Объем дискового пространства для эксплуатации | 100mb | 100mb |  |
| 5 | Операционная система | Windows 7 и выше |  |
| 6 | Доступ в Интернет (скорость соединения) | 256 Кбит/сек | 512 Кбит/сек |  |
| 7 | Привод CD-ROM | с возможностью чтения CD-RW дисков |  |
| 8 | Свободный USB 2.0 порт для работы с персональным аппаратным криптопровайдером (USB-токеном) |  |
| 9 | Персональный аппаратный криптопровайдер (USB-токен), необходимый для работы с ключами ЭП Клиента |  |
| 10 | Web-браузер | Microsoft Internet Explorer 11 и выше |  |
| 11 | Антивирусное ПО  | ОБЯЗАТЕЛЬНОЕ НАЛИЧИЕ (режим обновления установить раз в 6 часов) |  |
| 12 | ПО виртуальная JAVA-машина. При отсутствии последней версии JAVA-машина может быть бесплатно загружена с сайта разработчика http://www.java.com/ru/. |  |
| 13 | Наличие принтера (для печати Сертификата ключа проверки ЭП Клиента) |  |
| 14 | Наличие межсетевого экрана (внешний) |  |
| 15 | Наличие Крипто-ПРО CSP 4.0 и выше. Крипто-ПРО CSP может быть бесплатно загружено с сайта разработчика https://www.cryptopro.ru/downloads. |  |

2. Для корректной установки и настройки системы ДБО необходим локальный уровень доступа в операционной системе на уровне «Опытного пользователя» или «Администратора». В случае последующего изменения состава программно-аппаратных средств АРМ, используемого для работы в системе ДБО, обязуюсь предоставить в Банк настоящий Акт с учетом вносимых изменений.

Настоящий Акт составлен в 2-х экземплярах по одному для каждой из Сторон и является неотъемлемой частью Дополнительного соглашения.

|  |  |
| --- | --- |
| От Банка: | От Клиента: |
| Заместитель Председателя Правления | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/О.П.Ревякина/ | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ /\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/ |
| М.П. | М.П. |

Приложение №3 к Дополнительному соглашению

№\_\_\_\_\_от «\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_ года

**Акт приема-передачи персонального аппаратного криптопровайдера.**

**«\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_ года**

Общество с ограниченной ответственностью «Русфинанс Банк», именуемое в дальнейшем «Банк», в лице Заместителя Председателя Правления Ревякиной Ольги Петровны, действующего на основании Доверенности №1792/РУК/17-07 ОТ 01.01.2017г. с одной стороны, и \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, именуемое в дальнейшем «Клиент», в лице\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, действующего(ей) на основании \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, с другой стороны, составили настоящий акт о том, что Банком надлежаще передан(ы), а Клиентом получен(ы) персональный(ые) аппаратный(ые) криптопровайдер(ы) в количестве \_\_\_\_\_\_ (\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_) экз. со встроенным в него СКЗИ.

|  |  |
| --- | --- |
| № п/п | Номер персонального аппаратного криптопровайдера |
|  |  |
|  |  |

С момента подписания Сторонами настоящего акта Банк считается исполнившим свои обязательства по передаче необходимых для работы программных средств в полном объеме и надлежащем состоянии,
обеспечивающим возможность их эксплуатации для осуществления Клиентом доступа в систему ДБО и
получения оговоренных Дополнительным соглашением на дистанционное банковское обслуживание Соглашением услуг.

Настоящий Акт является неотъемлемой частью действующего Дополнительного соглашения на дистанционное банковское обслуживание к Договору банковского счета, составлен в двух экземплярах, имеющих равную юридическую силу, по одному экземпляру для каждой из Сторон.

ПОДПИСИ СТОРОН

|  |  |
| --- | --- |
| От Банка: | От Клиента: |
| Заместитель Председателя Правления | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/О.П.Ревякина/ | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ /\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/ |

|  |  |
| --- | --- |
| М.П. | М.П. |

Приложение №4 к Дополнительному соглашению

№\_\_\_\_\_\_от «\_\_\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_ года

**Доверенность №\_\_\_\_\_\_\_на получение программно-технических средств, средств криптографической защиты информации, персонального аппаратного криптопровайдера, сопроводительной документации и на регистрацию ключей ЭП**

г. Самара «\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_\_ г.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

*(полное наименование организации)*

Счет № \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ в ООО «Русфинанс Банк» в лице \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, *(должность, фамилия* имя, отчество)

действующего на основании \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_настоящей доверенностью уполномочивает

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

*(должность, фамилия, имя, отчество, серия и номер паспорта, кем и когда выдан)*

**на совершение следующих видов действий:**

* представлять интересы \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_юридического лица при получении от

 *(краткое наименование организации)*

ООО «Русфинанс Банк» согласно условиям Дополнительного соглашения № \_\_\_ от «\_\_» \_\_\_\_ 20\_\_ года к Договору банковского счета №\_\_\_ от «\_\_» \_\_\_\_ 20\_\_ года программно-технических средств, персонального аппаратного криптопровайдера и сопроводительной документации к ним;

* предоставить в ООО «Русфинанс Банк» необходимые документы для регистрации ключей ЭП в системе ДБО;
* получить сертификат(ы) ключа(ей) проверки ЭП с отметкой ООО «Русфинанс Банк» о регистрации.

Представитель наделяется правом расписываться в соответствующих документах для исполнения поручений, определенных настоящей доверенностью.

Настоящая доверенность выдана без права передоверия и действительна до «\_\_\_\_» \_\_\_\_\_\_\_\_\_ 20\_\_\_ г.

Руководитель организации\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ /\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/

*(подпись) (фамилия, имя, отчество)*

М.П.

Приложение №5 к Дополнительному соглашению

№\_\_\_\_\_\_\_\_от «\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_ года

Экз. №\_\_\_\_

**Заявление на регистрацию ключей ЭП в системе дистанционного банковского обслуживания**

Настоящим \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

*наименование организации*

просит на основании Дополнительного соглашения №\_\_\_\_\_ от «\_\_\_»\_\_\_\_\_\_\_\_\_\_20\_года зарегистрировать в системе ДБО сертификаты ключей проверки ЭП следующих уполномоченных лиц Клиента, наделенных полномочиями по распоряжению денежными средствами Клиента:

|  |  |  |
| --- | --- | --- |
| **Фамилия, имя, отчество****уполномоченного лица Клиента** | **Группа подписи** | **Идентификатор ключа** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

Вместе с заявлением представлены сертификаты ключей проверки ЭП уполномоченных лиц.

Руководитель организации

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ /

*подпись (Ф.И.О.)*

«\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_20 \_\_\_ г.

М.П.

Заполняется Банком

Заявление зарегистрировано в Банке «\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_\_\_ г.

Работник Банка \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/

*подпись (Ф.И.О.)*

Приложение №6 к Дополнительному соглашению

№\_\_\_\_\_\_\_\_от «\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_ года

**СЕРТИФИКАТ КЛЮЧА ПРОВЕРКИ ЭЛЕКТРОННОЙ ПОДПИСИ СОТРУДНИКА КЛИЕНТА В СИСТЕМЕ ДИСТАНЦИОННОГО БАНКОВСКОГО ОБСЛУЖИВАНИЯ**

ОБРАЗЕЦ

ОБРАЗЕЦ

Приложение №7 к Дополнительному соглашению

№\_\_\_\_\_\_\_\_\_\_от «\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_ года

Экз. №\_\_\_\_

**Заявление об отмене действия ключа ЭП и соответствующего ему ключа проверки ЭП**

*наименование организации*

р/с \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

уведомляет Банк о том, что с «\_\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_20\_\_\_г. \_\_\_:\_\_\_\_ считать недействительным ключ проверки ЭП Клиента, со следующим идентификатором ключа проверки ЭП Клиента \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ в связи с \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Соответствующий ему ключ ЭП Клиента утрачивает силу для дальнейшего применения с вышеуказанной даты.

Руководитель организации \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/

*подпись фамилия, имя, отчество*

 М.П.

Принял \_\_\_:\_\_\_:\_\_\_\_\_ «\_\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_20\_\_\_г.

 чч мм сс

Работник Банка \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/

*подпись фамилия, имя, отчество*

Отметки администратора СКЗИ:

Блокировка произведена \_\_\_:\_\_\_:\_\_\_\_\_ «\_\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_20\_\_\_г.

 чч мм сс

Администратор СКЗИ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/

*подпись фамилия, имя, отчество*

\* До момента постановки отметки об исполнении на письменном уведомлении Банк не несет ответственности за возможные убытки, возникшие у Клиента в результате незаконного использования ключей ЭП

Приложение №8 к Дополнительному соглашению

№\_\_\_\_\_\_\_\_от «\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_ года

Экз. №\_

**Заявление на регистрацию дополнительного персонального аппаратного криптопровайдера**

*наименование организации*

р/счет \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

просит осуществить дополнительную регистрацию персонального(ых) аппаратного(ых) криптопровайдера(ов) в количестве \_\_\_\_\_\_ экз. для осуществления операций по расчетному счету (расчетным счетам) с использованием системы дистанционного банковского обслуживания в порядке и на условиях, установленных Дополнительным соглашением №\_\_\_\_\_\_\_\_ от «\_\_\_» \_\_\_\_\_\_\_\_\_ 20\_\_\_ г.

Руководитель организации

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ /\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/

*подпись ( Ф.И,О.)*

МП

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

Приложение № 9 к Дополнительному соглашению

№\_\_\_\_\_\_\_\_от «\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_ года

Экз. №\_\_\_\_

**Акт приема-передачи персонального аппаратного криптопровайдера Банку**

«\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_ года

Общество с ограниченной ответственностью «Русфинанс Банк», именуемое в дальнейшем «Банк», в лице Заместителя Председателя Правления Ревякиной Ольги Петровны, действующего на основании Доверенности №1792/РУК/17-07 ОТ 01.01.2017 г. с одной стороны, и \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, именуемое в дальнейшем «Клиент», в лице\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, действующего(ей) на основании \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ другой стороны, составили настоящий акт о том, что Клиентом передан(ы), а банком получен(ы) персональный(ые) аппаратный(ые) криптопровайдер(ы):

|  |  |  |  |
| --- | --- | --- | --- |
| **№п/п** | **Причина возврата Банку персонального аппаратного криптопровайдера** | **Номер персонального аппаратного криптопровайдера** | **Количество переданных в Банк персональных аппаратных криптопровайдеров со встроенным в них СКЗИ** |
| 1 | В связи с прекращением Дополнительного соглашения №\_\_\_\_от «\_\_\_»\_\_\_\_\_\_\_\_\_\_\_ 20\_\_\_ г. |  |  |
| 2 | В связи с прекращением Дополнительного соглашения №\_\_\_\_от «\_\_\_»\_\_\_\_\_\_\_\_\_\_\_ 20\_\_\_ г., в случае повреждения персонального аппаратного криптопровайдера |  |  |
| 3 | В случае повреждения персонального аппаратного криптопровайдера |  |  |
| 4 | Иные обстоятельства, препятствующие дальнейшее использование персонального аппаратного криптопровайдера (пример, превышение ёмкости персонального аппаратного криптопровайдера и т.п.) |  |  |
| 5 | Иные случаи |  |  |

Настоящий Акт является неотъемлемой частью действующего Дополнительного соглашения на дистанционное банковское обслуживание к Договору банковского счета, составлен в 2 (двух) экземплярах, имеющих равную юридическую силу, по одному экземпляру для каждой из Сторон.

ПОДПИСИ СТОРОН

|  |  |
| --- | --- |
| От Банка: | От Клиента: |
| Заместитель Председателя Правления | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ /О.П. Ревякина/ | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ /\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/ |
| М.П. | М.П. |

Приложение № 10 к Дополнительному соглашению

№\_\_\_\_\_\_\_\_\_от «\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_ года

Экз. №\_\_\_\_

**Акт об утрате персонального аппаратного криптопровайдера**

«\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_ года

Общество с ограниченной ответственностью «Русфинанс Банк», именуемое в дальнейшем «Банк», в лице Заместителя Председателя Правления Ревякиной Ольги Петровны, действующего на основании Доверенности \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_с одной стороны, и \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, именуемое в дальнейшем «Клиент», в лице \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, действующего(ей) на основании \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, с другой стороны, в связи с прекращением Дополнительного соглашения № \_\_\_\_\_\_\_\_\_ от «\_\_\_»\_\_\_\_\_\_\_\_\_\_\_ 20\_\_\_ г. составили настоящий акт о том, что персональный(е) аппаратный(е) криптопровайдер(ы) в количестве \_\_\_ (\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_) экз. со встроенным в него СКЗИ.

|  |  |
| --- | --- |
| № п/п | Номер персонального аппаратного криптопровайдера |
| 1. |  |
| 2. |  |

На момент прекращения названого выше Дополнительного соглашения не могут быть возвращены Клиентом Банку в связи с его (их) утратой.

Настоящий Акт является неотъемлемой частью действующего Дополнительного соглашения на дистанционное банковское обслуживание к Договору банковского счета, составлен в 2 (двух) экземплярах, имеющих равную юридическую силу, по одному экземпляру для каждой из Сторон.

ПОДПИСИ СТОРОН

|  |  |
| --- | --- |
| От Банка: | От Клиента: |
| Заместитель Председателя Правления | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/О.П. Ревякина/ | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ /\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/ |
| М.П. | М.П. |

Приложение №11 к Дополнительному соглашению

№\_\_\_\_\_\_от «\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_ года

Экз. №\_\_\_\_

**Заявление на определение ограничений параметров операций, которые могут осуществляться Клиентом с использованием системы ДБО**

*наименование организации*

р/счет \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* прошу ограничить максимальную сумму перевода денежных средств суммой \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(сумма цифрами)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (сумма прописью)

* предоставляем перечень возможных получателей денежных средств в адрес которых будут совершаться переводы \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

при осуществлении операций по расчетному счету (расчетным счетам) с использованием системы дистанционного банковского обслуживания в порядке и на условиях, установленных Дополнительным соглашением №\_\_\_\_\_\_\_\_ от «\_\_\_» \_\_\_\_\_\_\_\_\_ 20\_\_\_ г.

Руководитель организации

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ /\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/

*подпись фамилия, имя, отчество*

**М.П.**

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

Приложение № 12 к Дополнительному соглашению

№\_\_\_\_\_\_от «\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 201\_ года

**РЕКОМЕНДАЦИИ ПО БЕЗОПАСНОМУ ИСПОЛЬЗОВАНИЮ ДБО**

**I. Рекомендации по обеспечению информационной безопасности при работе в ДБО.**

**1. Размещение АРМ**

1.1. Размещение, специальное оборудование, охрана и организация режима помещений, в которых хранятся ключевые носители и расположен, АРМ, должны исключать возможность неконтролируемого проникновения или пребывания в них посторонних лиц, а также просмотра посторонними лицами ведущихся там работ.

1.2. Помещения, предназначенные для размещения АП и хранения ключевых носителей, должны быть оборудованы прочными дверями, замками и сигнализацией. Окна помещений, расположенных на первых или последних этажах зданий, а также находящиеся около пожарных лестниц и других мест, откуда возможно проникновение посторонних, должны быть оборудованы решетками или сигнализацией.

**2. Защита АРМ**

2.1. Клиент, эксплуатирующий АРМ, должен принять необходимые меры, позволяющие исключить внесение несанкционированных изменений в технические и программные средства АП, изменение их состава, появление на АРМ и в системе ДБО компьютерных вирусов, а также программ, направленных на разрушение или модификацию программного обеспечения системы ДБО, ЭД, либо на перехват паролей, закрытых ключей и другой конфиденциальной информации.

2.2. Перед началом работы в ДБО обязательно провести сканирование АРМ на вирусы.

2.3. Выполнять полную проверку АРМ альтернативными антивирусными средствами раз в 1 месяц.

2.4. При работе в ДБО не допускается работа под учетной записью с правами администратора.

2.5. Обязательное использование межсетевого экрана (кроме штатного Windows).

2.6. Не запускать ДБО до установки последних обновлений безопасности для ОС и ПО.

2.7. Вставлять персональный аппаратный криптопровайдер в АРМ только на период работы и подписания документов.

2.8. Раз в день проверять остаток денежных средств на счете Клиента.

**3. Правила хранения ключевых носителей**

3.1. Для хранения ключевых носителей, а также эксплуатационной и технической документации, носителей информации с дистрибутивами средств криптографической защиты информации необходимо использовать надежные металлические хранилища, оборудованные внутренними замками.

3.2. Хранение ключевых носителей допускается в хранилище, используемом совместно с другими работниками, но при этом в отдельной упаковке (контейнере), опечатанной личной печатью владельца ключевых носителей и исключающей возможность негласного доступа к ним посторонних лиц.

3.3. Запрещается:

* копировать закрытые ключи на носители информации, которые не зарегистрированы в качестве ключевых носителей;
* передавать ключевые носители другим лицам;
* выводить закрытые ключи на дисплей или принтер;
* оставлять ключевые носители без присмотра;
* записывать на ключевой носитель постороннюю информацию.

**4. Требования к персоналу абонентского пункта**

4.1. Работники, допущенные к работе на АРМ, назначаются приказом и должны иметь утвержденные должностные инструкции.

4.2. Непосредственная работа работников на АРМ возможна только после прохождения обучения и проверки знания ими правил эксплуатации АРМ.

4.3. Каждый работник, имеющий доступ к ключам шифрования, паролям и другой конфиденциальной информации, должен быть проинформирован об ответственности за разглашение конфиденциальной информации и подписать соответствующие обязательства.

**II. Методические рекомендации о порядке действий Клиента в случае выявления хищения денежных средств в системе ДБО, использующих электронные устройства Клиента.**

1. В случае выявления хищения денежных средств в системе Дистанционного банковского обслуживания (**Далее по тексту «ДБО»**) немедленно прекратить любые действия с ЭУ, подключенным к системе ДБО, обесточить его (принудительно отключить электропитание в обход штатной процедуры завершения работы, извлечь все аккумуляторные батареи из ноутбука и т.п.) и отключить от информационных сетей (если было подключение, например, по Ethernet, USB, Wi-Fi, Dial-Up и др.) или перевести в режим гибернации ("спящий" режим).

При отсутствии возможности обесточивания ЭУ, осуществить отключение по штатной процедуре и запротоколировать указанный факт.

2. При наличии технической возможности отозвать подозрительный перевод денежных средств с использованием иного ЭУ, после чего принять меры к блокировке системы ДБО.

3. При отсутствии технической возможности отозвать перевод денежных средств по системе ДБО, незамедлительно обратившись в Банк по телефону **(846) 276-44-11,** связавшись с сотрудником ООЮЛ/ОКОиПП с заявлением о блокировке системы ДБО, приостановке исполнения подозрительного платежа и возврате денежных средств по данному платежу, используя кодовое слово, указанное в Соглашении с Банком.

4. Произвести фотосъемку ЭУ (с подключенными кабелями и иными периферийными устройствами), рабочего места и его расположения в помещении. Обеспечить сохранность (целостность) ЭУ как возможного средства совершения преступления, поместив его в место с ограниченным доступом, обеспечив при этом защиту от вскрытия (стикеры, наклейки, пластилин, мастичная печать, пломбы и т.п.) и по возможности зафиксировать средства контроля целостности фотографированием со всех ракурсов. Если позволяют размеры ЭУ, следует поместить его в непрозрачный пакет (мешок) и заклеить горловину. При необходимости ведения хозяйственной деятельности - задействовать другое ЭУ.

5. Дополнительно обратиться в Банк с письменным заявлением об отзыве подозрительного платежа, возврате денежных средств и блокировании доступа к системе ДБО ([Приложение №1](#Par129) к Рекомендациям), а также о компрометации ключей и необходимости смены пароля (закрытого ключа). Копия заявления должна быть направлена в Банк незамедлительно по факсу или по электронной почте (скан-копия): **Отдел обслуживания юридических лиц -****/Otdel\_Yuridich\_Litc@rusfinance.ru/****, либо, Отдел корротношений /Korrotnosheniya@rusfinance.ru/.** Оригинал заявления должен быть доставлен в Банк не позднее дня, следующего за днем направления копии Заявления.

6. Проинформировать все Банки, с которыми Клиент имеет договорные отношения, предусматривающие использование ДБО, о факте хищения денежных средств и обратиться с просьбой о внеплановой замене ключевой информации.

7. Предпринять меры для обеспечения сохранности и неизменности записей с внутренних и внешних камер систем видеонаблюдения, журналов систем контроля доступа, средств обеспечения и разграничения доступа в сеть Интернет (при наличии таковых) за максимальный период времени, как до, так и после даты совершения хищения денежных средств.

8. Провести сбор записей с межсетевых экранов и других средств защиты информации, серверов баз данных и иных компонент клиентского приложения системы ДБО, систем авторизации пользователей (AD, NDS и т.д.), коммуникационного оборудования (включая АТС), ЭУ, используемых для управления денежными средствами через систему ДБО Банка, которые могут использоваться для удаленного управления указанными ЭУ.

9 При возможности оперативно обратиться с письменным заявлением к своему Интернет-провайдеру или оператору связи для получения в электронной форме журналов соединений с Интернет с электронного устройства клиента или из его локальной вычислительной сети (далее - ЛВС) как минимум за три месяца, предшествовавшие факту хищения денежных средств.

10. Не предпринимать никаких действий для самостоятельного или с привлечением сторонних ИТ-специалистов поиска и удаления компьютерных вирусов, восстановления работоспособности ЭУ, не отправлять ЭУ в сервисные службы ИТ для восстановления работоспособности.

11. Зафиксировать в протокольной форме значимые действия и события, в том числе имена лиц, имеющих доступ к ЭУ, действия с ЭУ, подключенным к системе ДБО, предшествовавшие факту хищения денежных средств, подготовить объяснения клиента (работников клиента) об использовании ЭУ в целях, отличных от осуществления операций в системе ДБО, посещаемых сайтах, о странностях при работе ЭУ, перебоях или отказах ЭУ, обращениях в ИТ-службы, в банк плательщика, о сторонних лицах, побывавших в месте расположения ЭУ и т.д.

12. Все действия производить коллегиально, протоколировать и документировать, в т.ч. с использованием фотосъемки.При невозможности осуществления коллегиальных действий (для индивидуальных предпринимателей) отдельно зафиксировать данный факт.

13 Оперативно обратиться с заявлением в правоохранительные органы о возбуждении уголовного дела по факту хищения денежных средств.

14. Оперативно обратиться в суд с исковым заявлением в отношении получателя денежных средств (указав все известные реквизиты получателя) о взыскании неосновательно полученного обогащения и процентов за пользование денежными средствами (глава 60 ГК РФ), а также с ходатайством о принятии судом мер по обеспечению иска в виде ареста денежных средств на счете получателя в сумме неосновательно полученного обогащения. К исковому заявлению необходимо приложить копию заявления о возбуждении уголовного дела либо копию талона, содержащего порядковый номер из книги учета сообщений о преступлениях (далее - КУСП) содержащую отметку правоохранительного органа о его приеме.

15. Копии вышеуказанных документов, направить в Банк с приложением Справки по факту инцидента информационной безопасности в системе ДБО ([Приложение №2](#Par417) к Методическим рекомендациям о порядке действий Клиента в случае выявления хищения денежных средств в системе ДБО, использующих электронные устройства Клиента.), а также подтверждающих документов ([Приложение №3](#Par545) к Методическим рекомендациям о порядке действий Клиента в случае выявления хищения денежных средств в системе ДБО, использующих электронные устройства Клиента.).

Приложение №1 к Методическим рекомендациям о порядке действий Клиента в случае выявления хищения денежных средств в системе ДБО, использующих электронные устройства Клиента.

**ЗАЯВЛЕНИЕ КЛИЕНТА В БАНК ОБ ОТЗЫВЕ ПЛАТЕЖА, ВОЗВРАТЕ ДЕНЕЖНЫХ СРЕДСТВ И БЛОКИРОВАНИИ ДОСТУПА К СИСТЕМЕ ДБО**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

должность руководителя

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

наименование банка

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Фамилия И.О.

Уважаемый(ая) \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

имя, отчество руководителя Банка

"\_\_" \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 201\_ года с нашего счета №…., открытого в Вашем банке, по системе дистанционного банковского обслуживания были похищены денежные средства, которые, по имеющейся информации, были переведены по следующим реквизитам:

Дата платежа: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Номер документа: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Наименование банка плательщика: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_

Наименование плательщика: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

ИНН плательщика: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Номер счета плательщика: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Наименование банка получателя: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

БИК Банка получателя: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Корреспондентский счет Банка получателя\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Наименование получателя: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

ИНН получателя: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Номер счета получателя: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Сумма платежа: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Назначение платежа: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Прошу Вас заблокировать нашу учетную запись в системе ДБО, провести процедуру компрометации всех ключей ЭП и оказать содействие в отзыве платежа и в возврате денежных средств.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

должность подпись расшифровка подписи

М.П.

"\_\_" \_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_

Исп. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

тел. \_\_\_\_\_\_\_\_\_\_\_\_\_\_ Фамилия И.О.

Приложение №2

к Методическим рекомендациям

 о порядке действий Клиента

в случае выявления хищения денежных средств в системе ДБО,

использующих электронные устройства Клиента

**СПРАВКА КЛИЕНТА**

 **В БАНК ПО ФАКТУ ИНЦИДЕНТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СИСТЕМЕ ДБО**

"\_\_\_\_" \_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_г. неустановленным лицом через систему ДБО была совершена несанкционированная операция по переводу денежных средств по следующим реквизитам:

Дата платежа: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Номер распоряжения: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Наименование банка плательщика: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Наименование плательщика: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

ИНН плательщика: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Номер счета плательщика: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Наименование Банка получателя: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

БИК Банка получателя: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Корреспондентский счет Банка получателя:)\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Наименование получателя: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

ИНН получателя: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Номер счета получателя: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Сумма платежа: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Назначение платежа: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Дополнительно сообщаю:

Количество ЭУ, настроенных для доступа в систему ДБО: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

Для доступа в системы ДБО хотя бы раз использовались:

* корпоративные ЭУ
* личные ЭУ
* ЭУ, находящиеся в общественном пользовании

Периодичность смены пароля системы ДБО: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Применяемые элементы безопасности ЭУ включают:

* соблюден порядок подготовки ЭУ к установке системы ДБО
* используется только программное обеспечение для работы системы ДБО
* используется только лицензионное программное обеспечение
* операционная система и приложения обновляются в автоматическом режиме
* используется антивирусное программное обеспечение: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
* антивирусное программное обеспечение обновляется ежедневно
* из числа съемных носителей информации на ЭУ используются только ключевые носители
* передача файлов и обмен сообщениями электронной почты на ЭУ ограничены
* целостность исполняемых файлов и файлов конфигураций контролируется с периодичностью\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
* используются средства сетевой защиты: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
* на ЭУ запрещены входящие соединения из сети Интернет
* с ЭУ разрешены исходящие соединения с Банком и ограниченным числом сайтов сети

 Интернет для проведения обновлений программного обеспечения, число разрешенных

 сайтов составляет \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* обеспечивается возможность доступа к ЭУ только уполномоченных лиц
* обеспечивается возможность доступа к ключевым носителям только уполномоченных лиц

Иная информация, имеющая отношение к инциденту: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* Я намерен обратиться в правоохранительные органы по факту хищения денежных средств.

Заявление в правоохранительные органы принято в ОВД \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(район, округ, город, субъект федерации и иные идентифицирующие ОВД данные)

и зарегистрировано за №\_\_\_\_\_\_ в КУСП

* Я не намерен обращаться в правоохранительные органы по факту хищения денежных средств.

О необходимости предоставления доступа сотрудников правоохранительных органов к электронному устройству, об ответственности за использование нелицензированного и контрафактного программного обеспечения в соответствии со статьей 146 УК Российской Федерации предупрежден.

ФИО/Должность: \_\_\_\_\_\_\_\_\_\_\_\_\_\_/\_\_\_\_\_\_\_\_\_\_\_\_/ Дата: \_\_\_\_\_\_\_\_\_\_/ Телефон:\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Печать организации

М.П.

Приложение №3

к Методическим рекомендациям

о порядке действий Клиента

 в случае выявления хищения денежных средств в системе ДБО,

использующих электронные устройства Клиента

**ПЕРЕЧЕНЬ**

**ДОКУМЕНТОВ, ПРЕДОСТАВЛЯЕМЫХ КЛИЕНТОМ В БАНК,**

**В СЛУЧАЕ ВЫЯВЛЕНИЯ ХИЩЕНИЯ ДЕНЕЖНЫХ СРЕДСТВ**

1. Копия лицензии на операционную систему ПК.

2. Копия чека на приобретение операционной системы ПК.

3. Описание используемого ПО (перечень использованного лицензионного ПО на рабочем месте, информация о версии операционной системы и наличии критических обновлений, рекомендуемых разработчиком операционной системы).

4. Копия договора на оказание телематических услуг информационно-телекоммуникационной сети Интернет.

5. Описание организации доступа в сеть Интернет на рабочем месте.

6. Копия чека на оказание доступа в сеть Интернет на повременной основе.

7. Копия заявления в правоохранительные органы.

8. Копия лицензии на антивирусное ПО.

9. Копия чека на антивирусное ПО.

10. Описание по антивирусной защите рабочего места (наличие установленного на жестком диске автоматизированного рабочего места клиента антивирусного программного обеспечения и актуальность его баз, частота обновления, сканирования, наличие сведений о проявлении на автоматизированном рабочем месте клиента вредоносных программ).

11. Описание системы защиты информации (наличие или отсутствие персонального межсетевого экрана у клиента, сведения об использовании рабочего места в иных целях, кроме осуществления платежно-расчетных операций, в частности - интернет-серфинга, сведения о порядке хранения и использования ключевых носителей).

**III. Положение о порядке проведения технической экспертизы при возникновении спорных ситуаций**

В настоящем Положении под спорной ситуацией понимается существование претензий у Клиента к Банку, справедливость которых может быть однозначно установлена по результату проверки электронных подписей Клиента под электронным документом.

Клиент представляет Банку заявление, содержащее существо претензии с указанием на электронный документ, на основании которого Банк выполнил операции по счёту Клиента.

Банк обязан в течение пяти рабочих дней от даты подачи заявления Клиента сформировать Разрешительную комиссию (далее – Комиссия) для рассмотрения заявления.

В состав Комиссии включаются:

* представители Клиента;
* представители Банка;
* при необходимости представители компании-разработчика системы ДБО или независимые эксперты.

Выбор членов Комиссии осуществляется по согласованию со всеми участниками.

Стороны обязуются при разрешении экономических и иных споров, которые могут возникнуть в связи с использованием системы ДБО, предоставлять в письменном виде свои оценки, доказательства и выводы по запросу заинтересованной Стороны, участвующей в настоящем Дополнительном соглашении.

Стороны обязуются способствовать работе комиссии и не допускать отказа от предоставления необходимых документов.

Стороны обязуются предоставить комиссии возможность ознакомления с условиями и порядком работы своих программных и аппаратных средств, используемых в системе.

В ходе работы комиссии каждая Сторона обязана доказать, что она исполнила обязательства по Дополнительному соглашению надлежащим образом.

Результатом рассмотрения спорной ситуации Комиссией является определение стороны, несущей ответственность согласно выводу о подлинности электронных подписей Клиента под приложенным документом.

Комиссия в течение не более пяти рабочих дней проводит рассмотрение заявления. Рассмотрение заявления включает следующие этапы:

Разрешительная комиссия проводит техническую экспертизу:

* ключа (ключей) ЭП Клиента с использованием штатного программного обеспечения (ПО) системы ДБО выполняется распечатка сертификата ключа проверки ЭП Клиента;

Результат сверяется с сертификатом ключа проверки ЭП, заверенным подписью уполномоченного лица Клиента и являющимся приложением к Дополнительному соглашению. Сверяются ID ключа и его шестнадцатеричный дамп. При обнаружении расхождений ситуация далее не рассматривается как не соответствующая заявленной.

* + электронного документа на наличие необходимого количества (согласно Приложению №1 к Дополнительному соглашению) электронных подписей Клиента, на основании которого Банком выполнены оспариваемые Клиентом действия с его счетом;
* корректности электронных подписей Клиента в электронном документе, с использованием штатного ПО системы ДБО выбирается документ и выполняется операция «Проверить ЭП».

При невозможности получить доступ к документу с помощью штатного ПО системы ДБО, может использоваться специализированные утилиты от разработчика для выгрузки документа из базы данных системы и автономной проверки.

На основании данных технической экспертизы Комиссия составляет Акт произвольной формы, содержащий следующие данные:

* + фактические обстоятельства, послужившие основанием возникновения разногласий;
	+ порядок работы членов Комиссии;
	+ вывод о подлинности (ложности, приеме, передаче, отзыве и т.п.) оспариваемого электронного документа и его обоснование.

Акт составляется в 2-х экземплярах, подписываемых представителями Банка и Клиента, принимающих участие в работе Комиссии, или в 3-х экземплярах, если в состав Комиссии включаются представители компании разработчика ДБО или независимые эксперты, подписываемых представителями Банка, Клиента и представителем компании разработчика ДБО или независимого эксперты принимающих участие в работе Комиссии. Один из экземпляров акта вручается уполномоченному представителю Клиента или направляется в адрес Клиента почтой в срок не позднее 30 календарных дней с даты поступления в Банк претензии Клиента; указанный срок может быть продлен до 60 календарных дней в случае, если предметом рассмотрения Комиссии является претензия о ненадлежащем осуществлении трансграничного перевода, т.е. перевода денежных средств, при осуществлении которого плательщик либо получатель средств находится за пределами Российской Федерации, и (или) перевод денежных средств, при осуществлении которого плательщика или получателя средств обслуживает иностранный центральный (национальный) банк или иностранный банк.

Банк несет ответственность перед Клиентом в случае, когда имело место хотя бы одна из следующих ситуаций:

* + Банк не предъявляет электронного документа, переданного Клиентом, на основании которого Банк выполнил операции по счёту Клиента;
	+ хотя бы одна ЭП Клиента в исполненном электронном документе оказалась некорректной;
	+ Клиент предоставляет уведомление об отмене действия ключа ЭП и соответствующего ему ключа проверки ЭП Клиента (см. Приложение №8 к Дополнительному соглашению), подписанное должностными лицами Банка и имеющим оттиск печати Банка. При этом Администратором СКЗИ проставлены в уведомлении Клиента дата и время блокировки в системе ДБО пары ключей ЭП Клиента раньше даты и времени, указанных в рассматриваемом электронном документе.

В случае, когда Банк предъявляет электронный документ, в котором корректность электронных подписей Клиента признана Комиссией и принадлежность Клиенту ключей проверки ЭП Клиента подтверждена, Банк перед Клиентом по выполненным операциям со счётом Клиента ответственности не несёт. Отказ Клиента от подписания акта при наличии перечисленных в настоящем пункте Положения обстоятельств не является основанием для признания обоснованности претензии Клиента и не влечет ответственности Банка.

Если Клиент настаивает на том, что данный документ он не создавал или не подписывал одной или несколькими подписями, Комиссия может вынести определение о компрометации ключа (ключей) ЭП Клиента, что не снимает ответственности Клиента за данный документ.

|  |  |
| --- | --- |
| От Банка: | От Клиента: |
| Заместитель Председателя Правления | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/О.П. Ревякина/ | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ /\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/ |
| М.П. | М.П. |