ПРИЛОЖЕНИЕ №9.8.7.
к Правилам комплексного банковского обслуживания юридических лиц и индивидуальных предпринимателей, физических лиц, занимающихся в установленном законодательством Российской Федерации порядке частной практикой в ООО КБ «Агросоюз» от «20» сентября 2017г.

УСЛОВИЯ ОБСЛУЖИВАНИЯ СЧЕТА КЛИЕНТА, С ИСПОЛЬЗОВАНИЕМ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ СИСТЕМЫ ДИСТАНЦИОННОГО БАНКОВСКОГО ОБСЛУЖИВАНИЯ (СИСТЕМА ДБО)

1. УСЛОВИЯ ОБСЛУЖИВАНИЯ:

1.1. Настоящие Условия являются неотъемлемой частью Правил КБО, и устанавливают порядок предоставления Услуги «Обслуживание счета Клиента, с использованием программного обеспечения системы дистанционного банковского обслуживания (Система ДБО)» (далее - Условия) на основании Заявления на присоединение к Правилам КБО в целом, которые в совокупности являются Договором ДБО. Правила КБО и Заявление на присоединение к Правилам КБО опубликованы на web-сайте Банка.

Система ДБО работает через сеть Интернет и любой Web-браузер (разработчик ООО «БИФИТ»).

1.2. Обслуживание с использованием Системы ДБО подразумевает обязательное использование Клиентом в течение всего периода обслуживания в Системе ДБО аппаратного криптопровайдера в виде USB-токена, который предназначен для противодействия хищениям электронных ключей программными средствами.

Для обслуживания Клиента Банк предоставляет в возмездное пользование исправный комплект шифровальных средств и средств изготовления ключевых документов, далее именуемый «Ключевой носитель» (USB-токен), для совершения операций в Системе ДБО. Ключевой носитель передается Банком Клиенту при подаче Заявки на выдачу оборудования (по форме Приложения №3 к настоящим Условиям), при одновременном оформлении Акта передачи устройства генерации и хранения ключей ЭП (по форме Приложения №4 настоящих Условий). В случае наличия у Клиента Ключевого носителя, дополнительный Ключевой носитель может не предоставляться.

Банк и Клиент за собственный счет поддерживают в рабочем состоянии свои программно-технические средства, используемые при работе с Системой ДБО.

Для работы с системой Клиент должен иметь:

- Современный компьютер с операционной системой. Работа с сервисом возможна на следую-щих ОС:
  — Microsoft Windows: 7 (x86/x64), 8 (x86/x64), 8.1 (x86/x64), 10 (x86/x64) и выше;
  — Apple Mac OC X: 10.7 (Lion) и выше;
  — Linux: AltLinux 7 (x86/x64), Debian 7 (x86/x64), Mint 13 (x86/x64), SUSE Linux Enterprise Desktop 12 (x64), openSUSE 13 (x86/x64), Ubuntu 12.04 (x86/x64) и более современные версии указанных дистрибутивов.
- Монитор с разрешением не менее 1280x1024; - Web-браузер с поддержкой плагина "BIFIT Signer" для использования электронной подписи с применением аппаратных устройств. Поддержка плагина обеспечена в следующих браузерах:
  — Internet Explorer версия 11;
  — Firefox версия 44 и выше;
  — Opera версия 35 и выше;
  — Safari версия 9 и выше;
  — Chrome версия 49 и выше.
- выход в Интернет со скоростью обмена данных не менее 33,6 Кбит/сек и возможностью использования для обмена порт 443.

1.3 ***Изготовление сертификатов ключей проверки электронной подписи***

1.3.1.Уполномоченный работник Клиента (владелец сертификата ключа проверки электронной подписи) самостоятельно изготавливает ключ ЭП, ключ проверки ЭП для работы в Системе ДБО, распечатывает два экземпляра сертификата ключа проверки электронной подписи с использованием предоставленных Банком программных средств электронной подписи. Подготовленные и подписанные руководителем Клиента и владельцем сертификата ключа проверки электронной подписи экземпляры сертификата ключа проверки электронной подписи

предоставляются Клиентом в Банк для регистрации в Системе ДБО. Должностное лицо Банка на основании полученного экземпляра сертификата ключа проверки электронной подписи заполняет и передает Клиенту один экземпляр сертификата ключа проверки электронной подписи клиента, второй оставляет в Банке.

Ключи ЭП изготавливаются Клиентом только для лиц, указанных в Карточке с образцами подписей и оттиска печати при использовании Системы ДБО. Никакие иные лица не должны иметь доступ к Ключу ЭП. Ответственность за использование ключа ЭП иными лицами полностью возлагается на Клиента. Сформированный сертификат ключа оформляется сроком на 1 год. В случае, если срок полномочий лиц, имеющих право распоряжения денежными средствами на счета менее 1 года, сертификат действует до окончания срока полномочий указанных лиц.

Сформированный сертификат ключа проверки электронной подписи принадлежит Клиенту и достаточен для определения Банком корректности ЭП.

1.3.2. В случае окончания срока действия сертификата ключа электронной подписи, Уполномоченный работник Клиента (владелец сертификата ключа) самостоятельно изготавливает новый ключ ЭП, ключ проверки ЭП для работы в Системе ДБО.

Сертификата ключа электронной подписи при формировании нового ключа ЭП может быть оформлен как на бумажном носителе, так и в электронном виде в Системе ДБО. Для формирования нового сертификата ключа электронной подписи, сформированного в электронном виде, прежний сертификат ключа должен быть активным (срок действия не окончен).

В случае оформления на бумажном носителе подготовленные и подписанные руководителем Клиента и владельцем ключа электронной подписи, экземпляры сертификата ключа проверки электронной подписи предоставляются Клиентом в Банк, для регистрации их в Системе ДБО. Должностное лицо Банка на основании полученного экземпляра сертификата ключа проверки электронной подписи заполняет и передает Клиенту один экземпляр сертификата ключа проверки электронной подписи клиента, второй оставляет в Банке.

В случае оформления сертификата ключа ЭП в электронном виде, Клиент в Системе ДБО заполняет Заявление на выпуск сертификата ключа проверки ЭП, подписанное уже имеющейся электронной подписью. Заполненное Заявление на выпуск сертификата ключа проверки ЭП подается в Банк по каналам Системы ДБО. Должностное лицо Банка на основании полученного в электронном виде Заявления на выпуск сертификата ключа проверки ЭП проверяет актуальность представленных данных и в случае корректности его заполнения подает заявку на подключение к Системе ДБО нового сертификата ключа электронной подписи в ДИТ. Отметка о подключении нового сертификата ключа проверки ЭП делается в электронном виде в Системе ДБО.

1.4. Заверения и утверждения.

Клиент и Банк признают, что алгоритмы шифрования и создания ЭП в Системе ДБО при передаче электронных документов, достаточны для обеспечения защиты от несанкционированного доступа, подтверждения авторства и подлинности информации, содержащейся в электронных документах, а также сохранения банковской тайны.

Клиент и Банк в целях определения безопасной работы в Системе ДБО считают необходимым признать следующее:

- положительный результат подтверждения подлинности ЭП в Электронном документе Клиента в Системе ДБО на сервере Банка является подтверждением того, что полученный электронный документ подписывался соответствующим ключом ЭП Клиента и получен в том виде, в котором он исходил от Клиента;
- хранящиеся в Системе ДБО электронные документы, подписанные ЭП Клиента, проверка которой ключом проверки ЭП Клиента дала положительный результат, является доказательным материалом для решения спорных вопросов в соответствии с действующим законодательством;
- любое уведомление признается полученными Клиентом по истечении одного дня с даты отправки Уведомления Банком, если Клиент в течение указанного срока не сообщил в Банк о неполучении такого Уведомления (электронного письма).
- электронные документы: «паспорт сделки», "платежное поручение", "заявление об отказе от акцепта", "заявление на перевод", "поручение на продажу валюты", "распоряжение на списание иностранной валюты с транзитного счета", "поручение на покупку валюты", "справка о валютных операциях", "справка о подтверждающих документах", документы, являющиеся основанием для проведения валютной операции в соответствии с ч.4 ст.23 Федеральным законом от 10.12.2003 № 173-ФЗ "О валютном регулировании и валютном контроле" и Инструкцией Банка

России от 04.06.2012 № 138-И "О порядке представления резидентами и нерезидентами уполномоченным банкам документов и информации, связанных с проведением валютных операций, порядке оформления паспортов сделок, а также порядке учета уполномоченными банками валютных операций и контроля за их проведением", "письма Клиентов" ("письмо"), "заявление на закрытие счета" заверенные Электронной подписью Клиента, хранящиеся в виде записи в контрольных архивах Системы или извлеченные из нее в виде специального файла, юридически эквивалентны соответствующим документам на бумажном носителе, подписанным уполномоченным(и) представителем(ями) Клиента и имеющим оттиск печати Клиента, обладают юридической силой и подтверждают наличие правовых отношений между Сторонами. Электронные документы, исходящие от Клиента, без ЭП Клиента не имеют юридической силы, Банком не рассматриваются и не исполняются.

Стороны считают, что Электронные документы: "выписка по счету", "письмо", «уведомление», «ведомость банковского контроля» заверенные Электронной подписью Банка, юридически эквивалентны соответствующим документам на бумажном носителе, подписанным уполномоченными лицами Банка и имеющим оттиск печати Банка. Электронные документы, исходящие от Банка, без ЭП Банка не имеют юридической силы.

Вышеуказанный перечень Электронных документов может изменяться Банком с предварительным уведомлением Клиента сообщением по Системе ДБО.

Направление Клиентом Банку иных видов Электронных документов может осуществляться после предварительного согласования с Банком посредством обмена подтверждающими Электронными документами, направляемыми по Системе ДБО.

- электронные документы, заверенные ЭП Банка, юридически эквивалентны соответствующим документам на бумажном носителе, распечатанном Клиентом самостоятельно.
- хранящиеся в контрольных архивах Системы ДБО Электронные документы, подписанные Ключом ЭП Клиента, проверка которой Ключом проверки ЭП Клиента дала положительный результат, являются доказательным материалом для решения спорных вопросов в соответствии с действующим законодательством и "Положением о порядке разрешения спорных ситуаций".
- при изменении Электронного документа, заверенного к моменту внесения изменений Электронной подписью, ЭП становится некорректной, то есть проверка ЭП Ключом проверки ЭП дает отрицательный результат. Исправление или изменение Электронного документа, заверенного Электронной подписью, возможно только путем создания нового Электронного документа.
- в качестве единой шкалы времени при работе с системой Московское является поясное время. Контрольным является время системных часов Системы ДБО, а также признают информацию о дате и времени поступления, исполнения, неисполнения Электронных документов в Банк, содержащуюся в контрольных архивах Банка, необходимым и достаточным доказательством даты и времени передачи, исполнения, неисполнения Клиентом Банку Электронного документа.
- использование всемирной телекоммуникационной сети общего доступа Интернет может вызывать перерывы в приеме и обработке Электронных документов в Системе ДБО, связанные с отказами телекоммуникационного оборудования провайдеров телекоммуникационных услуг, а также вирусными и иными атаками на систему. Стороны обязаны принимать все доступные способы защиты от указанных угроз.
- контроль за сроком действия ЭП, а также контроль за наличием соответствующих полномочия у Владельца Сертификата Ключа проверки Электронной подписи осуществляется Клиентом, а не Банком.

1.5. В соответствии с требованиями Федерального закона «Об электронной подписи» от 06.04.2011 г. № 63-ФЗ при использовании усиленной электронной подписи участники электронного взаимодействия обязуются:

- обеспечивать конфиденциальность ключей ЭП, в частности не допускать использование принадлежащих им ключей ЭП без их согласия;
- уведомлять в письменном виде другую Сторону о нарушении конфиденциальности ключа ЭП в течение не более чем одного рабочего дня со дня получения информации о таком нарушении;
- не использовать ключ ЭП при наличии оснований полагать, что конфиденциальность данного ключа нарушена.

1.6. В случае возникновения конфликтных ситуаций между Банком и Клиентом при использовании Системы ДБО Стороны обязуются выполнять требования Договора ДБО и нести ответственность согласно выводам по рассмотрению конфликтной ситуации (раздел 4 настоящих Условий). В случае, если Клиент отказывается от принятия на себя обязательств по электронному документу (оспаривает факт или время передачи электронного документа, его содержание), бремя доказывания обстоятельств, на основании которых он отказывается от принятия на себя обязательств, ложится на него. Ответственность может быть возложена на Банк в случае, если создание электронного документа обусловлено его противоправными действиями.

Стороны обязуются при разрешении споров, которые могут возникнуть в связи с использованием электронной Системы ДБО, предоставлять в письменном виде свои оценки, доказательства и выводы по запросу противоположной Стороны.

1.7. ***Предоставление Услуг СМС-информирование и СМС-пароль.***

1.7.1. В целях повышения безопасности проведения платежей посредством Системы ДБО Банк предоставляет Клиенту Услуги СМС-пароль и СМС-информирование.

Клиент уведомлен и согласен с тем, что используемые Банком телекоммуникации являются открытыми и не гарантируют полную защиту передаваемой информации.

Клиент согласен с тем, что Банк не несет ответственности за возможное раскрытие информации, составляющей банковскую тайну, и принимает на себя риск такого разглашения.

Клиент также подтверждает, что все лица, допущенные к получению Услуг СМС-пароль и СМС-информирование, уполномочены на то Клиентом.

1.7.2. Услуга СМС-пароль направляется на мобильные телефоны Клиента, указанные в заявлении о подключении/отключении/изменении параметров подключения Услуги СМС-пароль и СМС-информирования (далее по тексту - Заявление о подключении) (по форме Приложении № 2 к Условиям обслуживания счета клиента, с использованием программного обеспечения Системы ДБО – далее по тексту Приложение №2). Заявление о подключении оформляется в одном экземпляре и передается в Банк.

В каждом случае изменения номеров телефонов Клиента, а также для отказа от Услуги СМС-пароль и СМС-информирования, Клиент предоставляет в Банк Приложение №.2.

Для предоставления Услуги СМС-информирования Клиент проставляет необходимую отметку в Заявлении о подключении и самостоятельно указывает номера мобильных телефонов, для направления Банком СМС-сообщений, в Системе ДБО.

Банк не несет ответственность за возможные неблагоприятные последствия несвоевременного извещение Клиентом Банка об изменении номеров телефонов.

1.7.3. Для самостоятельного формирования пароля Клиентом может использоваться иное специальное техническое устройство (OTP-токен), для чего Клиент получает устройство и проставляет необходимую отметку в Заявление о подключении. OTP-токен – это техническое устройство защиты информации. Устройство применяется для аутентификации Клиента в Системе ДБО.

1.7.3.1 Параметры подключения устройства:

- OTP-токен на вход в систему;
- OTP-токен на подтверждение расходных операций по Счету.

1.7.4. Банк отправляет Клиенту:

- СМС-пароль на совершение/подтверждение следующих действий по счету Клиента:
  - вход в Систему ДБО;
  - на подтверждение расходных операций по Счету;
- Банк направляет Клиенту текстовые СМС-сообщения о событиях предусмотренными системой ДБО с возможностью выбора необходимых событий:
  - факт подключения (входа) в Систему ДБО;
  - информация о поступлении в Банк документов от Клиента;
  - утверждение документа;
  - о входящих документах;
  - о движении денежных средств по счету;
  - о текущих остатках;
  - о выписке по счету.

События, по которым Банк отправляет СМС-пароль и необходимость подключения СМС-информирования указываются Клиентом в Приложении №.2

Банк оставляет за собой право вносить изменения в перечень событий и форматов СМС-

сообщений, предварительно уведомив об этом Клиента посредством передачи СМС-сообщения или другим доступным способом, не менее чем за 3 (Три) рабочих дня до предполагаемой даты изменения.

1.7.5. Предоставление Услуги СМС-пароль и СМС-информирования начинается не позднее 3 (Три) рабочих дней с момента предоставления подписанного Клиентом Приложения№2 в Банк и осуществляется в течение действия Договора ДБО.

1.7.6. Банк имеет право в одностороннем порядке временно приостановить оказание Услуг СМС-пароль и СМС-информирования Клиенту без предварительного уведомления Клиента, если, по мнению Банка, такая мера необходима для обеспечения безопасности системы.

1.7.7. В случае утраты/кражи Клиентом мобильного телефона или SIM-карты, Банк не несет ответственности за возможное раскрытие информации, составляющей банковскую тайну Клиента или персональные данные Клиента.

1.7.8. Банк не несет ответственности за:

- задержки и сбои, возникающие в сетях операторов сотовой связи и сервисах провайдеров, которые могут повлечь за собой задержку или недоставку сообщения с СМС-паролем Клиенту;

- убытки Клиента (как прямые (реальный ущерб), так и упущенную выгоду), которые могут возникнуть в силу неполучения или несвоевременного получения Клиентом СМС-пароля, а также в случаях утраты/кражи мобильного телефона или SIM-карты.

1.7.9. В случае утраты/кражи Клиентом мобильного телефона или SIM-карты, Клиент по телефону обязан незамедлительно уведомить об этом Банк для отключения телефона от услуги СМС-пароль и СМС-информирования, с обязательным последующим представлением в Банк Заявления о присоединении (по форме Приложения № 2).

При обращении по телефону Клиент должен назвать кодовое слово, указанное им в Заявлении о присоединении при подключении Услуг СМС-пароль и СМС-информирования.

1.7.10. Вознаграждение Банка за предоставление услуги СМС-пароль определяется в соответствии с действующими Тарифами Банка, которые могут быть изменены Банком в одностороннем порядке.

Уведомление Клиентов об изменении Тарифов осуществляется Банком путем опубликования новых Тарифов на официальном сайте Банка.

В случае несогласия с новыми Тарифами Клиент имеет право в 10 - дневный срок с момента опубликования Тарифов на сайте Банка отказаться от Услуги, оплатив ее до момента расторжения по старым Тарифам.

Вознаграждение Банка за предоставление услуги СМС-информирования не взимается.

1.7.11. Денежные средства в счет оплаты Услуги СМС-пароль списываются в безакцептном порядке с расчетного счета Клиента, открытого в валюте Российской Федерации, в соответствии с Тарифами Банка.

При этом подписанием Договора ДБО Клиент предоставляет заранее данный акцепт Банку произвести списание суммы излишне выплаченных процентов со Счета.

Денежные средства списываются не позднее последнего рабочего дня месяца, в котором была оказана Услуга СМС-пароль.

В случае отсутствия денежных средств на расчетном счете Клиента, открытого в валюте Российской Федерации, денежные средства списываются в безакцептном порядке со счета, открытого в иностранной валюте. Списание осуществляется по официальному курсу Банка России на день списания.

В случае отсутствия денежных средств на счетах Клиента, необходимых для оплаты Услуги СМС-пароль, и неоплаты Услуги СМС-пароль Клиентом самостоятельно, Банк имеет право приостановить оказание Услуги СМС-пароль, начиная с первого рабочего дня месяца, следующего за месяцем, за который возникла задолженность по оплате.

Повторное подключение Клиента к Услуге СМС-пароль осуществляется Банком на основании Заявления о присоединении и после оплаты Клиентом услуги за подключение согласно Тарифам Банка.

1.8 Права и обязанности Банка по работе в Системе ДБО.

1.8.1. Банк имеет право по своему усмотрению прекратить принятие от Клиента электронных документов по Системе ДБО и потребовать от Клиента смены ключей, направив уведомление в свободной форме.

1.8.1.1. Банк имеет право приостановить оказание услуг по Системе ДБО по основаниям, предусмотренным действующим законодательством, в том числе нормативными актами Банка России РФ.

1.8.1.2. Банк имеет право отказать в исполнении Электронного документа Клиента в случае несоответствия реквизитов такого документа обязательным реквизитам, установленным действующим законодательством РФ и банковскими правилами.

В случае выявления сомнительных операций Клиента, Банк имеет право отказать в приеме от него распоряжений на проведение операций по Счету, подписанных ЭП Клиента, предварительно предупредив об этом Клиента. После отказа в приеме распоряжений на проведение операции по счету, Банк принимает от Клиента только надлежащим образом оформленные расчетные документы на бумажном носителе.

1.8.1.3. Банк имеет право по согласованию с Клиентом установить предел максимальных сумм, подлежащих перечислению с применением Системы ДБО.

1.8.1.4. Банк имеет право расторгнуть Договор ДБО в одностороннем порядке в случае невнесения платы за пользование Системой в соответствии с Тарифами, без предварительного уведомления Клиента, по истечении **30-ти** дней с момента неоплаты.

1.8.1.5. Банк имеет право расторгнуть Договор ДБО в одностороннем порядке в случае неиспользования Системы ДБО Клиентом в течение **2-х** месяцев.

1.8.2. Банк обязан:

1.8.2.1. исполнять принятые от Клиента Электронные документы, подписанные корректной ЭП Клиента, в соответствии с условиями Договора ДБО и действующим законодательством.

1.8.2.2. после получения от Клиента (в том числе по факсу, а также по телефону при правильно названном проверочном слове) уведомления о прекращении (приостановлении) действия ключа электронной подписи и соответствующего ему сертификата ключа проверки электронной подписи временно блокировать соответствующий ключ Клиента в Системе ДБО. Наложенная блокировка снимается только на основании письменного требования Клиента не позднее дня, следующего за днем получения такого требования.

1.8.2.3. обеспечить строго контролируемый и ограниченный доступ к помещениям, в которых находятся программно-аппаратные средства, содержащие контрольные архивы Системы ДБО.

1.8.2.4. информировать Клиента об условиях и о порядке использования электронных подписей и средств электронной подписи, о рисках, связанных с использованием электронных подписей, и о мерах, необходимых для обеспечения безопасности электронных подписей и их проверки.

1.8.2.5. хранить в секрете и не передавать третьим лицам Ключи ЭП Банка и Ключ проверки ЭП Клиента, используемые при работе в Системе ДБО.

1.8.2.6. обеспечивать конфиденциальность созданных Банком ключей электронных подписей.

1.8.2.7. прекратить принятие от Клиента Электронных документов по Системе ДБО и потребовать от Клиента смены Пары ключей ЭП Клиента.

1.8.2.8. незамедлительно направлять в адрес Клиента Уведомление методом, установленным согласно заявлению Клиента, при наступлении события, связанного с обработкой ЭД.

1.9. Права и обязанности Клиента по работе в Системе ДБО.

1.9.1. Клиент имеет право:

1.9.1.1. 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,

1.9.1.2. досрочно прекращать действие ключей, направив (письменно, а также по телефону при правильно названном блокировочном слове) уведомление. Для продолжения дальнейшей работы в Системе ДБО уполномоченный представитель Клиента должен самостоятельно сформировать новые ключи ЭП, ключ проверки ЭП, оформить сертификаты ключа проверки электронной подписи и передать их в Банк для регистрации,

1.9.1.3. блокировать свой ключ проверки ЭП в Системе ДБО, т.е. приостановить свою работу в Системе ДБО, направив письменное уведомление. Блокировка снимается не позднее дня, следующего за днем получения Банком письменного требования Клиента о снятии блокировки,

1.9.1.4. подключить необходимое количество USB-токенов (при первичном подключении и в последующем) за плату согласно Тарифам Банка, генерировать новые Пары ключей ЭП Клиента и регистрировать в Банке новые Ключи проверки ЭП Клиента. При этом не позднее, чем на следующий день, Клиент обязан письменно уведомить Банк об этом и представить новый Сертификат Ключа проверки ЭП Клиента,

В случае генерации ключей ЭП Клиента и регистрации их в Банке для сотрудника организации не имеющего права распоряжения денежными средствами на счете, сведения об этом указываются в Сертификате Ключа проверки ЭП Клиента.

1.9.1.5. пользоваться дополнительными услугами Банка по получению информации по Счету, Уведомлений и информационных сообщений Банка в электронном виде и средствами по подтверждению Электронных документов.

1.9.2. Клиент обязан:

1.9.2.1. при создании электронных документов в Системе ДБО соблюдать условия Договора ДБО, нормы действующего законодательства и банковские правила в отношении обязательных реквизитов документов,

1.9.2.2. выполнять требования информационной безопасности, обеспечив хранение в секрете и отсутствие доступа неуполномоченных лиц к ключу электронной подписи, используемому при работе в Системе ДБО. Риск неблагоприятных последствий, связанных с невыполнением требований информационной безопасности и использованием ключа электронной подписи Клиента неуполномоченными лицами, несет Клиент,

1.9.2.3. сообщать Банку об обнаружении попытки несанкционированного доступа к Системе ДБО или к ключу электронной подписи Клиента в день ее обнаружения и блокировать свою работу в Системе ДБО, направив в Банк уведомление. Клиент несет риск всех последствий, связанных с несанкционированным доступом к Системе ДБО или ключу электронной подписи Клиента.

1.9.2.4. незамедлительно извещать Банк обо всех случаях возникновения технических неисправностей и о фактах утери USB-токена,

1.9.2.5. по требованию Банка приостановить работу в Системе ДБО и для ее возобновления сгенерировать новую Пару ключей ЭП Клиента и передать Банку Сертификат нового Ключа проверки ЭП Клиента,

1.9.2.6. уведомлять Банк о смене лиц, уполномоченных работать с Системой ДБО и распоряжаться Счетом, и для возможности работы с Системой ДБО новых лиц обеспечить им возможность сгенерировать Пару ключей ЭП Клиента. Риск неблагоприятных последствий, связанных с несвоевременным уведомлением Банка о том, что необходимо приостановить действие Ключей ЭП Клиента несет Клиент,

1.9.2.7. регулярно производить оплату за пользование Системой ДБО в соответствии с Тарифами, являющимися неотъемлемой частью Договора КБО,

1.9.2.8. не реже одного раза в пять дней осуществлять просмотр информации, переданной ему Банком по Системе ДБО. Информация считается доведенной до сведения Клиента по истечение **5-ти** календарных дней с даты ее передачи Клиенту по Системе ДБО, независимо от фактического восприятия такой информации Клиентом.

2. СОВМЕСТНЫЕ ОБЯЗАТЕЛЬСТВА И ОТВЕТСТВЕННОСТЬ СТОРОН

2.1. Ответственность Банка и Клиента в рамках работы в Системе ДБО определяется законодательством РФ, Договором ДБО.

2.2. Каждая Сторона обязана за собственный счет поддерживать в рабочем состоянии свои программно-технические средства, используемые при работе с Системой ДБО.

2.3. В случае возникновения конфликтных ситуаций между Сторонами при использовании Системы ДБО, Стороны обязуются участвовать в рассмотрении конфликтов в соответствии с Положением о порядке разрешения спорных ситуаций, выполнять требования указанного Положения и нести ответственность согласно выводам по рассмотрению конфликтной ситуации. В случае, если Клиент отказывается от принятия на себя обязательств по Электронному документу (оспаривает факт или время передачи Электронного документа, его содержание), бремя доказывания обстоятельств, на основании которых он отказывается от принятия на себя обязательств, ложится на него. Ответственность может быть возложена на Банк в случае, если создание Электронного документа обусловлено его противоправными действиями.

2.4. Стороны обязуются при разрешении споров, которые могут возникнуть в связи с

использованием электронной Системы ДБО, предоставлять в письменном виде свои оценки, доказательства и выводы по запросу противоположной Стороны.

2.5. Банк не несет ответственности:

- за ущерб, причиненный Клиенту в результате использования третьими лицами ключа электронной подписи Клиента;
- за техническое состояние компьютерного оборудования Клиента;
- в случае, если электронный документ подписан корректной ЭП Клиента, но исходил не от Клиента;
- за неисполнение, несвоевременное или неправильное исполнение электронных документов Клиента, если это было вызвано предоставлением Клиентом недостоверной информации и (или) платежных реквизитов в переданном в Банк электронном документе;
- за неисполнение или несвоевременное исполнение электронных документов Клиента, если выполнение этих распоряжений Банком невозможно без определенных действий третьей стороны, в том числе, территориальных учреждений Центрального банка Российской Федерации, и невыполнение или несвоевременное выполнение связано с тем, что третья сторона отказывается совершить необходимые действия, совершает их неправильно, с задержкой или недоступна для Банка;
- за полное или частичное неисполнение, неправильное или несвоевременное исполнение своих обязательств, если неисполнение является следствием форс-мажорных обстоятельств, включая пожар, отключение электроэнергии, телефонных линий и иных каналов связи, наводнение, землетрясение, военные операции, изменение действующего законодательства, действия или решения органов государственной власти РФ, Центрального банка РФ, забастовки и иные действия персонала телефонных компаний, провайдеров телекоммуникационных услуг, органов электроснабжения, Центрального Банка РФ, иные ограничения правового, технического, экономического или политического характера вне контроля Банка, объективно препятствующие исполнению Банком его обязательств;
- за передачу информации об операциях Клиента, если такая информации была предоставлена по законному требованию уполномоченных органов (суд, органы дознания и предварительного следствия, прокуратура, служба судебных приставов и т.д.);
- за неисполнение (ненадлежащее исполнение) обязательств по Договору ДБО только при наличии своей вины;
- за убытки, понесенные Клиентом в результате использования ошибочных электронных документов, если эти документы надлежащим образом оформлены и отправлены Клиентом, а Банком проверены и приняты.

2.6. Банк не производит замену поврежденного или испорченного (неработающего) USB-токена и не возмещает расходы Клиента, связанные с подключением, в случае утраты USB-токена, за исключением случаев, когда повреждение USB-токена произошло по вине Банка, доказанной Клиентом в установленном законодательством Российской Федерации порядке.

3. ПОРЯДОК ОБСЛУЖИВАНИЯ КЛИЕНТА В СИСТЕМЕ ДБО.

3.1. До начала работы в Системе ДБО Клиент осуществляет оплату за подключение к Системе ДБО в соответствии с Тарифами и предоставить Банку Сертификат(ы) Ключа проверки ЭП Клиента (согласно карточки с образцами подписей и оттиском печати) Банк не принимает Электронные документы Клиента без оплаты за услуги Банка по подключению в Системе ДБО.

3.2. При доступе в Систему ДБО Банк осуществляет идентификацию Клиента путем проверки достоверности ключа проверки электронной подписи Клиента. При получении Банком Электронных документов, либо соответствующих документов на бумажных носителях, подтверждающих прекращение полномочий какого-либо из представителей Клиента, Банк прекращает прием Электронных документов, подписанных ЭП данного лица.

При предоставлении Клиентом полномочий по работе с Системой ДБО и распоряжению Счетом новому лицу, Банк начинает прием от Клиента Электронных документов, подписанных ЭП данного лица, начиная со дня, следующего за днем получения Сертификата Ключа проверки ЭП Клиента, содержащего Ключ проверки ЭП данного лица.

Банк осуществляет прием Электронных документов, передаваемых по Системе ДБО, круглосуточно. Исполнение документов осуществляется в сроки, предусмотренные настоящими Правилами. Использование Системы ДБО не лишает Клиента права предоставлять Банку расчетные и иные документы на бумажном носителе.

3.3. При получении Электронного документа Банк производит проверку:

- достоверности ЭП Клиента и ее принадлежности Клиенту;
- правильности заполнения реквизитов Электронного документа;
- возможности возникновения дебетового сальдо на Счете Клиента, за исключением случаев, когда возникновение дебетового сальдо допустимо в соответствии с соглашением Сторон.

При выявлении отрицательного результата проверки любого из вышеуказанных обстоятельств полученный Электронный документ Банком не принимается, считается возвращенным Клиенту, поручение, содержащееся в нем, Банком не исполняется. Статус документа "отвергнут" в Системе ДБО информирует Клиента о неисполнении переданного им по Системе ДБО Электронного документа. Иного информирования Клиента о неисполнении Электронного документа Банк не осуществляет. Свидетельством того, что документ принят, является статус Электронного документа "исполнен" в Системе ДБО.

3.4. Дальнейшее оформление Электронных документов, переданных в Банк по Системе ДБО, осуществляется Банком без участия Клиента, в том числе оформление копий таких документов на бумажном носителе для передачи иным участникам расчетов. При этом дополнительное оформление документов по сравнению с установленными Банком России правилами безналичных расчетов осуществляется Банком только по требованию Клиента при явке его представителя в Банк.

3.5. Если по истечении **10-ти** рабочих дней с момента проведения Банком операции по Счету на основании полученного от Клиента Электронного документа, Клиентом не заявляется претензий по такой операции, признается, что Клиент подтвердил правильность проведения операции по его Счету.

3.6. Клиент имеет право с использованием Системы ДБО самостоятельно получать информацию о состоянии своего Счета на начало текущего операционного дня.

3.7. Работа с Системой ДБО осуществляется по следующему адресу в сети Интернет: "https://ibank2.ru." или по резервному адресу, опубликованному на сайте Банка. Об изменении адреса в сети Интернет Банк уведомляет Клиента по Системе ДБО.

3.8. Банк осуществляет обслуживание всех банковских счетов, указанных в Заявлении о присоединении к Условиям обслуживания счета Клиента, с использованием программного обеспечения системы дистанционного банковского обслуживания. В случае необходимости подключения дополнительных банковских счетов, открытых после подачи Заявления о присоединении к Условиям обслуживания счета клиента, с использованием программного обеспечения системы дистанционного банковского обслуживания, Клиент подает заявление о подключении дополнительных счетов. Заявление оформляется в произвольной форме с указанием номера банковского счета.

4. ПОРЯДОК РАЗРЕШЕНИЯ СПОРНЫХ СИТУАЦИЙ ПО РАБОТЕ В СИСТЕМЕ ДБО.

4.1. Настоящий раздел регламентирует процедуры, связанные с конфликтными ситуациями

- по факту передачи Клиентом Банку электронного документа;
- по дате передачи Клиентом Банку электронного документа;
- содержания переданного Клиентом Банку Электронного документа.

В случае несогласия Клиента с действиями Банка, Клиент подает в Банк письменное заявление с изложением спорной ситуации, указав детально суть конфликта, а также представляет документы и информацию, имеющие отношение к предмету спора.

На основании изучения материалов, предоставленных Клиентом, и имеющихся в распоряжении Банка, Банк в течение 5 рабочих дней со дня получения заявления выносит письменное заключение о правомерности и обоснованности претензии. Согласие или несогласие Клиента с выводами Банка оформляется письменно в форме заключения.

В случае несогласия Клиента с заключением Банка, Клиент и Банк («Стороны») в течение 5 банковских дней от даты выражения Клиентом несогласия формируют согласительную комиссию численностью не более 6 человек из числа представителей обеих Сторон. По договоренности Сторон в согласительную комиссию дополнительно могут быть включены независимые эксперты числом не более 3 человек.

Создание согласительной комиссии утверждается протоколом, подписываемым обеими Сторонами, в котором указываются Ф.И.О. членов комиссии от каждой Стороны и независимые эксперты, а также описывается регламент работы комиссии и график заседаний.

В случае уклонения Клиента или его представителей от создания согласительной комиссии или участия в ее работе Банк вправе сформировать комиссию самостоятельно, включив в состав комиссии в качестве представителей Клиента не более 3 независимых экспертов.

4.2. Согласительная комиссия осуществляет свою работу непосредственно в помещениях, в которых располагается Банк, с использованием сертификатов ключей проверки электронной подписи, участвующих в конфликте Сторон.

Согласительная комиссия запрашивает у Клиента и Банка необходимые материалы, относящиеся к спорной операции, в том числе материалы, находящиеся в юридическом деле Клиента; заявления Клиента о проведении спорной операции, электронные документы Системы ДБО в виде файлов и на бумажном носителе, пояснения работников Банка по сути спорной операции, документы бухгалтерского учет и подтверждающие факт проведения операции.

4.3. По результатам работы согласительной комиссии составляется соответствующий Акт, который является окончательным и не может быть оспорен Сторонами. Возражения членов согласительной комиссии, не согласных с выводами, изложенными в Акте, оформляются в письменном виде и прилагаются к Акту как его неотъемлемая часть.

4.4. Расходы по формированию и работе согласительной комиссии, исключая расходы Клиента, связанные с привлечением им в одностороннем порядке независимых экспертов, возлагаются на Банк. В случае признания согласительной комиссией требований Клиента необоснованными, Клиент обязан в течение пяти банковских дней с момента составления Акта согласительной комиссии возместить Банку все указанные расходы.

5. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ПРИ РАБОТЕ В СИСТЕМЕ ДБО.

Под информационной безопасностью понимается защищенность системы ДБО от случайного или преднамеренного вмешательства в нормальный процесс ее функционирования, а также от попыток хищения, модификации или разрушения ее компонентов. Безопасность достигается только путем выполнения комплекса организационных и технических мер защиты.

5.1. Организационные меры защиты.

В целях организации технологического процесса работы с Системой ДБО клиент:

- определяет и утверждает порядок учета, хранения и использования носителей ключевой информации, который должен полностью исключать возможность несанкционированного доступа к ним.
- утверждает список лиц, имеющих доступ к носителям ключевой информации, и выдаются данные ключи их владельцам под роспись. Доступ неуполномоченных лиц к носителям ключевой информации должен быть исключен.
- утверждает список лиц, имеющих доступ к АРМ Системы ДБО (для технического обслуживания и т.п.). Доступ неуполномоченных лиц к АРМ Системы ДБО должен быть исключен.
- в случае применения в качестве средств Уведомления и Подтверждения электронного документа средств сотовой связи, утверждает список лиц, имеющих доступ к средству сотовой связи (аппарат, sim-карта), предназначенного для работы с Системой ДБО. Доступ неуполномоченных лиц к данному устройству должен быть исключен.

5.2. Требования к помещению для размещения АРМ.

5.2.1. Планировка помещений должна исключать возможность визуального просмотра другими лицами (посетителями или неуполномоченными сотрудниками) обрабатываемой или передаваемой информации.

5.2.2. Помещение должно исключать возможность бесконтрольного проникновения в них посторонних лиц и обеспечивать целостность, сохранность аппаратуры, программных средств, носителей ключевой информации и документов.

5.2.3. При хранении носителей с ключевой информацией в помещении должны быть исключены возможности несанкционированного доступа к носителям ключевой информации.

5.2.4 Уборка и проведение ремонтных работ в помещении производятся при отключенной аппаратуре под контролем сотрудника, имеющего доступ в помещение.

5.2.5. При использовании в помещении дополнительных технических средств защиты, их эксплуатация осуществляется в соответствии с инструктивно-технологической документацией, к ним прилагаемой.

5.3. Требования к АРМ.

5.3.1. Эксплуатацию АРМ Системы ДБО могут осуществлять только лица, обладающие правом работы на данном рабочем месте.

5.3.2. Программное обеспечение, установленное на АРМ Системы ДБО должно выполнять только функции, определенные технологическим процессом Системы ДБО. Рекомендуется выделить для АРМ Системы ДБО отдельный компьютер или ноутбук. Не допускается размещать систему ДБО на АРМ, на которых осуществляется неконтролируемый доступ в сеть Интернет.

5.3.3. Пользователи АРМ, работающие с Системой ДБО не должны иметь прав администратора, с целью ограничения возможностей установки под этими учетными записями программного обеспечения на компьютере. Доступ к файловым ресурсам компьютера, особенно на запись, должен быть ограничен минимально необходимыми правами. Пользователи должны запускать только те приложения, которые им разрешены.

5.3.4. Локальными (или доменными) политиками на компьютере рекомендуется ограничить список пользователей, имеющих возможность входа в операционную систему.

5.3.5. На компьютере должна быть установлена только одна ОС.

5.3.6. Для ограничения доступа к компьютеру, проверки целостности используемого ПО, рекомендуется установить и настроить на компьютер программно-аппаратный комплекс защиты от НСД.

5.3.7. Не рекомендуется подключать к АРМ Системы ДБО внешние устройства, в том числе носители информации, не предусмотренные производственной необходимостью.

5.3.8. Средствами BIOS компьютера следует исключить возможность загрузки операционной системы, отличной от установленной на жестком диске, т.е. отключить загрузку с дискет, CD/DVD приводов, USB flash дисков, сетевую загрузку и т.п. Доступ к изменению настроек BIOS должен быть защищен паролем.

5.3.9. АРМ Системы ДБО должен быть оснащен антивирусными средствами защиты с актуальными обновляемыми базами, обеспечивающим антивирусный контроль программного обеспечения и обрабатываемой информации.

5.3.10. С помощью штатного функционала операционной системы (или с применением дополнительных средств защиты) АРМ Системы ДБО должны быть выполнены следующие настройки:

- установлен парольный вход. Пользователям операционной системы должны быть назначены пароли, длина паролей должна составлять не менее шести символов, срок действия паролей должен быть ограничен;
- установление уровня доступа пользователя к информации (в случае, если имеет место наличие нескольких пользователей с разными полномочиями), в том числе минимально возможного для лиц, уполномоченных применять систему ДБО;
- установление правил сетевого экрана на АРМ системы ДБО (или сетевом маршрутизаторе), допускающего доступ только к необходимым IP-адресам в локальную сеть и сеть Internet, ограничение сетевого доступа к АРМ системы ДБО с других АРМ клиента;
- автоматическую регистрацию действий пользователя в системном журнале.

5.3.11. Не допускается применять на АРМ Системы ДБО программное обеспечение для удаленного доступа в систему (TeamViewer, VNC, Radmin и т.п.).

5.4. Обеспечение безопасности при работе с ключевой информацией СКЗИ. Порядок учета и хранения ключевой информации СКЗИ.

5.4.1. Лица, допущенные к работам с ключевой информацией, должны нести персональную ответственность за ее использование и хранение.

5.4.2. Доступ неуполномоченных лиц к носителям с ключевой информацией должен быть исключен.

5.4.3. Условия хранения носителей с ключевой информацией по окончанию рабочего дня, а также вне времени работы с Системой ДБО должны исключить возможность несанкционированного доступа к ним.

Категорически запрещается:

- оставлять носители с ключевой информацией бесконтрольно на рабочем месте;
- передавать носители с ключевой информацией лицам, к ним не допущенным;

- устанавливать носитель с ключевой в устройство считывания в режимах, не предусмотренных штатным режимом, а также в устройства считывания других АРМ.

5.4.4. Для сохранения необходимого уровня защищенности информации в случае прекращения полномочий работника, имевшего доступ к ключевому носителю, необходима немедленная смена ключевых документов.

5.5. Контроль за обеспечением безопасности Системы ДБО.

Контроль за обеспечением безопасности Системы ДБО в рамках всего комплекса технологических, организационных, технических и программных мер и средств защиты и возлагается на подразделение безопасности Клиента или, в случае его отсутствия, на руководителя Клиента.

5.6 Действия Клиента в случае подозрения на атаку злоумышленников на Систему ДБО

5.6.1. В случае выявления подозрения на атаку в Системе ДБО немедленно прекратить любые действия с АРМ Системы ДБО, обесточить его (принудительно отключить электропитание в обход штатной процедуры завершения работы, извлечь аккумуляторную батарею из ноутбука и т.п.) и отключить от информационных сетей (если было подключение, например, по Ethernet, USB, Wi-Fi и др.) или перевести в режим гибернации.

5.6.2. Немедленно позвонить в Банк для уточнения состояния счета и совершенных платежей.

5.6.3. Действовать согласно рекомендациям работников Банка.

5.7. Действия Клиента в случае хищения денежных средств

5.7. 1. При наличии технической возможности отозвать перевод с использованием иного АРМ, после чего заблокировать Систему ДБО.

5.7.2. При отсутствии технической возможности отозвать перевод по Системе ДБО немедленно обратиться в Банк по телефону (или иным каналам связи) с заявлением о приостановке исполнения платежа и возврате средств.

5.7.3. Произвести фотосъёмку рабочего места и его расположения в помещении. Обеспечить сохранность (целостность) АРМ Системы ДБО 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 АРМ, следует поместить его в непрозрачный пакет (мешок) и опечатать горловину. При необходимости ведения хозяйственной деятельности – задействовать другой АРМ.

5.7.4. Обратиться в Банк с письменным заявлением об отзыве платежа, возврате средств и блокировании доступа к системе ДБО, а также о компрометации ключей.

5.7.5. 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.

5.7.6. В течение одного дня обратиться в банк получателя или к оператору соответствующей платежной системы с письменным заявлением о приостановлении платежа и возврате денежных средств.

5.7.7. Предпринять меры для обеспечения сохранности и неизменности записей с внутренних и внешних камер систем видео-наблюдения, 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.

5.7.8. Провести сбор записей с межсетевых экранов, клиентского приложения Системы ДБО, систем авторизации пользователей (AD, NDS и т.д.), АРМ, используемых для управления денежными средствами через Систему ДБО, устройств, которые могут использоваться для удалённого управления.

5.7.9. В течение одного дня обратиться с письменным заявлением к своему Интернет-провайдеру для получения в электронной форме журналов соединений с Интернет с электронного устройства клиента или из его ЛВС как минимум за три месяца, предшествовавшие факту хищения денежных средств.

5.7.10. Не предпринимать никаких действий для самостоятельного или с привлечением сторонних ИТ-специалистов поиска и удаления компьютерных вирусов, восстановления

работоспособности АРМ, не отправлять АРМ в сервисные службы ИТ для восстановления работоспособности.

5.7.11. Зафиксировать в протокольной форме значимые действия и события, в том числе действия с АРМ, подключенным к Системе ДБО, предшествовавшие факту хищения денежных средств, подготовить объяснения клиента (работников клиента) об использовании АРМ в целях, отличных от осуществления операций в системе ДБО, посещаемых сайтах, о странностях при работе электронных устройств, перебоях или отказах электронных устройств, обращениях в ИТ-службы, в Банк, о посторонних лицах, побывавших в месте расположения АРМ и т.д.

5.7.12. В течение одного дня обратиться с заявлением в правоохранительные органы о возбуждении уголовного дела по факту хищения денежных средств.

5.7.13. 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 КУСП, содержащую отметку правоохранительного органа о его приеме.

6. СРОК ДЕЙСТВИЯ ДОГОВОРА И ПОРЯДОК ЕГО ИЗМЕНЕНИЯ

6.1. Договор ДБО вступает в силу с даты подписания Банком заявления о присоединении к настоящим Условиям. Договор ДБО заключен на неопределенный срок.

6.2. Каждая из Сторон вправе расторгнуть Договор ДБО в одностороннем порядке не ранее, чем через п**ять** рабочих дней после письменного уведомления об этом противоположной Стороны. При этом обязательства по Договору ДБО, возникшие в период его действия, не прекращаются до полного исполнения их Сторонами.

6.3. Договор ДБО может быть расторгнут в порядке, установленном в разделе 9 Правил КБО.

6.4. Договор ДБО может быть расторгнут в одностороннем порядке в случае:

- невнесения платы за пользование Системой в соответствии с Тарифами, без предварительного уведомления Клиента, по истечении 30-ти дней с момента неоплаты;
- в случае неиспользования Системы ДБО Клиентом в течение 2-х месяцев.

6.5. Основанием для прекращения Договора ДБО является расторжение последнего ДБС в рамках Правил КБО с одновременным закрытием банковского счета.

6.6. Расторжение Договора ДБО не влечет недействительности Электронных документов, содержащих корректную ЭП Клиента, переданных Клиентом по Системе ДБО до дня расторжения Договора ДБО включительно.