

Правила дистанционного банковского обслуживания АО МС Банк Рус

Акционерное общество МС Банк Рус, именуемое в дальнейшем «Банк», устанавливает следующие Правила дистанционного обслуживания АО МС Банк Рус, именуемые в дальнейшем «Правила».

1. ОПРЕДЕЛЕНИЯ

Автоматизированное рабочее место (АРМ) – составная часть Системы ДБО, устанавливаемая в помещениях Клиента, используемая Клиентом для электронного документооборота с Банком.

Администратор – уполномоченное должностное лицо Банка, имеющее право обслуживать Систему ДБО, отвечающее за функционирование и работоспособность Системы ДБО и за эксплуатацию средств криптографической защиты информации в Системе ДБО.

Банковские правила – Правила открытия банковских счетов и расчетно-кассового обслуживания АО МС Банк Рус, являющиеся договором присоединения (в соответствии со статьей 428 Гражданского кодекса Российской Федерации), присоединение Клиента к которому и выражение согласия Клиента с условиями которого осуществляется путем подписания заявления по установленной ими форме.

Владелец ключа электронной подписи – Уполномоченный представитель Клиента (физическое лицо) или Банка (физическое лицо), на имя которого выдан Акт признания ключа проверки электронной подписи (КПЭП), зарегистрированный в соответствии с условиями Договора в реестре КПЭП Системы ДБО. Со стороны Клиента, только перечисленные в предоставленной Клиентом в Банк карточке с образцами подписей и оттиска печати (при наличии) лица могут обладать КПЭП с правом подписи электронных документов.

Договор о предоставлении Услуг – договор о предоставлении Услуг, заключенный между Банком и Клиентом путем подписания Клиентом Заявления о присоединении Клиента к условиям настоящих Правил. При этом Заявление и настоящие Правила совместно являются Договором о предоставлении Услуг.

Договор банковского счета – любой из договоров банковского счета (договоров расчетного счета), заключенный между Сторонами в соответствии с Банковскими правилами.

Документация Пользователя означает руководство по эксплуатации Системы ДБО, техническую документацию и другие письменные или зафиксированные в другой форме материалы, относящиеся к Системе ДБО.

ИС «Одно окно» – информационная система «Одно окно» в сфере внешнеторговой деятельности.

Заявление – заявление на присоединение к настоящим Правилам, подписываемое Клиентом в целях заключения Договора о предоставлении услуг по форме Приложения №9 к настоящим Правилам.

Клиент – юридическое лицо (за исключением кредитной организации), индивидуальный предприниматель или физическое лицо, занимающееся в установленном законодательством Российской Федерации порядке частной практикой, заключившее с Банком Договор о предоставлении Услуг.

Ключ проверки электронной подписи (КПЭП), Открытый ключ – уникальная последовательность символов, однозначно связанная с ключом электронной подписи и предназначенная для проверки подлинности электронной подписи;

Ключ электронной подписи (КЭП) – уникальная последовательность символов, известная Владелцу ключа электронной подписи и предназначенная для создания электронной подписи;

Компрометация КЭП – событие, при котором возникает недоверие к используемому КЭП как средству обеспечения подлинности, целостности и авторства электронных документов. В том числе, к компрометации КЭП, относят следующие события:

1. утрата или хищение Носителя ключевой информации;
2. утрата или хищение Носителя ключевой информации с последующим его обнаружением;
3. хищение КЭП;
4. увольнение сотрудника, имевшего доступ к КЭП;
5. передача КЭП по каналам связи в открытом виде;
6. нарушение правил хранения Носителей ключевой информации;
7. совершение операции по счету Клиента в Банке без добровольного согласия Владельца КЭП;
8. возникновение подозрения о несанкционированном распространении информации или ее искажении в Системе ДБО;
9. отрицательный результат при проверке ЭП документа;

10. нарушение целостности упаковки ключевых носителей и (или) печати на сейфе, где хранились Носители ключевой информации;

11. несанкционированное копирование Носителей ключевой информации или КЭП;

12. случаи, когда нельзя достоверно установить, что произошло с Носителями ключевой информации (в том числе случаи, когда носитель вышел из строя).

Корректная ЭП - ЭП, дающая положительный результат ее проверки с использованием действующего на момент проверки КПЭП, соответствующего КЭП, с использованием которого сформирована проверяемая ЭП.

Несанкционированный доступ в Систему ДБО или Несанкционированное использование Системы ДБО означает любое использование Системы ДБО лицом, не являющимся Пользователем Системы ДБО.

Носитель ключевой информации – носитель безопасного хранения данных (Рутокен), содержащий КЭП.

Единое Окно ДБО – автоматизированное рабочее место пользователя системы ДБО, без права подписи электронных документов, обеспечивающее возможность одновременного доступа в едином окне с единым КЭП и под единым логином и паролем к системе ДБО Клиента и его обособленных подразделений при условии, что от Клиента получено подписанное заявление по Форме Приложения № 20 к настоящим правилам.

Операционное время - часть Операционного дня Банка, определенная Банком в Тарифах, в течение которого Банком производится обслуживание Клиентов. Банк вправе устанавливать различную продолжительность Операционного времени для поступающих в Банк распоряжений. Банк с целью ознакомления Клиента с Операционным временем размещает соответствующую информацию в местах и способами, обеспечивающими возможность ознакомления с этой информацией Клиентов, в том числе путем:

- размещения на Сайте Банка в документе Тарифы;

- размещения объявлений на стендах в помещениях Банка;

- иными способами, позволяющими Клиенту получить информацию и установить, что она исходит от Банка.

Операционное время может быть изменено Банком в одностороннем порядке, о чем Банк извещает Клиента не позднее, чем за пятнадцати календарных дней до его изменения, любым из способов, предусмотренных выше.

Операционный день – календарный день, являющийся рабочим в соответствии с положениями действующего законодательства, за исключением выходных дней и нерабочих праздничных дней, установленных в соответствии с действующим законодательством Российской Федерации, и дней, в течение которых Банк не совершает операции на основании действующего законодательства Российской Федерации и (или) требования уполномоченного органа государственной власти Российской Федерации и (или) Банка России. Если срок уплаты Клиентом Банку любой суммы или срок исполнения Банком обязательств перед Клиентом приходится на день, который не является Операционным днем, то обязательства исполняются в следующий Операционный день.

Операция СБП – перевод денежных средств с использованием СБП, осуществляемый посредством формирования и передачи по Системе ДБО в режиме 24/7.

Отправитель - участник электронного документооборота Системы ДБО, отправляющий электронный документ, подписанный ЭП.

Получатель - участник электронного документооборота Системы ДБО, в адрес которого направляется электронный документ, подписанный ЭП, и который выполняет Процедуру подтверждения подлинности ЭП в электронном документе.

Пользователь – Уполномоченный представитель Клиента, наделенный правами по использованию Системы ДБО со стороны Клиента. Клиент доводит до Банка список Пользователей в порядке, установленном Правилами Системы ДБО.

Поручение означает распоряжение, которое Клиент дает Банку через Систему ДБО для осуществления операций по счету/счетам.

Процедура подтверждения подлинности ЭП в электронном документе - проверка соответствующим сертифицированным средством ЭП с использованием КПЭП принадлежности ЭП в электронном документе Владельцу КЭП, действительности КПЭП на момент создания ЭП и отсутствия искажений в подписанном данной ЭП электронном документе.

Сайт Банка - информационный ресурс Банка в сети Интернет по адресу: <http://www.mcbankrus.ru/>

Сайт Системы ДБО - информационный ресурс Банка, необходимый для входа и использования Системы ДБО, находящийся по адресу <https://bc.mcbankrus.ru>.

Акт признания ключа проверки электронной подписи (Акт признания КПЭП) - электронный документ или документ на бумажном носителе, подтверждающие принадлежность Ключа проверки электронной подписи (КПЭП) Владельцу ключа электронной подписи.

СБП – сервис быстрых платежей платёжной системы Банка России.

Сертификат ключа проверки электронной подписи - электронный документ, выданный удостоверяющим центром Банка, подтверждающий принадлежность КПЭП Владельцу ключа электронной подписи и регистрацию КПЭП для использования в Системе ДБО.

Система дистанционного банковского обслуживания (Система ДБО) - автоматизированная информационная система Банка, обеспеченная сертифицированной системой криптографической защиты информации, включающая в себя совокупность программно- аппаратных средств, устанавливаемых у Клиента и Банка и совместно эксплуатируемых Клиентом и Банком в соответствующих частях, предназначенная для обеспечения электронного

документооборота (подготовки, защиты, отправки, приема, проверки и обработки электронных документов) при обслуживании Клиентов в Банке в режиме удаленного доступа, в том числе, но, не ограничиваясь, в целях осуществления банковских операций, обмена расчетными (платежными) документами и иными документами, удаленного управления Клиентами их Счетами в Банке, заключения и исполнения Сторонами гражданско-правовых договоров, (включая, но, не ограничиваясь, договоров залога, дополнительных соглашений к ним, соглашений о внесудебном порядке обращения взыскания на предмет залога, и иных гражданско-правовых договоров). Обслуживание Клиента с использованием Системы ДБО производится на основании Правил Системы ДБО.

Сопроводительная документация – комплект документации, необходимый для установки и эксплуатации Клиентом Системы ДБО, передаваемый Банком Клиенту при подключении Клиента к Системе ДБО.

Средства криптографической защиты информации (СКЗИ) в Системе ДБО – специализированное программное обеспечение, используемое в Системе ДБО для создания ЭП, проверки подлинности ЭП, шифрования и расшифрования передаваемых по системе электронных документов.

Сторона / Стороны – Клиент или Банк/ Клиент и Банк.

Тарифы - документ Банка, устанавливающий перечень, стоимость и порядок оплаты банковских услуг, оказываемых в рамках Договора. В случае оказания услуг, не включенных в Тарифы, Банк отставляет за собой право взимать плату за такую оказанную услугу по отдельному соглашению Сторон.

Банк с целью ознакомления Клиента с Тарифами размещает Тарифы в местах и способами, обеспечивающими возможность ознакомления с этой информацией Клиентов, в том числе путем размещения на Сайте Банка; размещения объявлений на стендах в помещениях Банка; иными способами, позволяющими Клиенту получить информацию и установить, что она исходит от Банка.

Банк вправе в одностороннем порядке вносить в Тарифы изменения и (или) дополнения, в том числе вводить новые услуги, за получение которых Клиент обязан оплачивать комиссии в соответствии с Тарифами.

Тарифы вводятся в действие Банком не ранее 15 (пятнадцати) календарных дней со дня их размещения на сайте Банка.

Уполномоченный представитель - применительно к какому-либо лицу, лицо, надлежащим образом уполномоченное действовать от имени указанного лица: (а) на основании занимаемой им должности в соответствии с учредительными документами указанного лица; или (б) на основании доверенности или получения полномочий в иной надлежащей форме в порядке передоверия от другого уполномоченного представителя указанного лица; или (с) на основании распорядительного документа, приказа указанного лица.

Услуги – услуги по дистанционному банковскому обслуживанию, предоставляемые Банком Клиенту с использованием Системы ДБО в целях обеспечения электронного документооборота при обслуживании Клиентов в Банке в режиме удаленного доступа в соответствии с настоящими Правилами и Тарифами.

Установочный комплект означает электронные носители информации с Документацией Пользователя, а также бумажные носители, с указанием имени пользователя в системе ДБО и паролем для первоначального доступа в систему ДБО. Электронные и бумажные носители находятся в запечатанном конверте с указанием фамилии и имени Пользователя и наименования организации.

Шифрование - способ преобразования открытой информации в закрытую и обратно. Применяется для передачи важной информации по незащищенным каналам связи. Шифрование подразделяется на процесс зашифровывания и расшифровывания.

Электронный документ (ЭД) – документ, в котором информация представлена в электронной форме. ЭД порождает обязательства Сторон, если он передающей Стороной должным образом оформлен, подписан ЭП и передан, а принимающей Стороной получен, проверен и принят.

Электронная подпись (ЭП) - информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию. Применяемая в Системе ДБО ЭП является усиленной неквалифицированной электронной подписью.

Электронное средство платежа - средство или способ, позволяющие Клиенту составлять, удостоверять и передавать распоряжения в целях осуществления перевода денежных средств в рамках применяемых форм безналичных расчетов с использованием информационно-коммуникационных технологий, электронных носителей информации, а также иных технических устройств. Для целей настоящих Правил электронным средством платежа является Система ДБО.

Иные термины и определения, использованные в настоящих Правилах с заглавной буквы, имеют то же значение, что и в Договоре банковского счета, за исключением случаев, когда иное прямо установлено настоящими Правилами.

2. ОБЩИЕ ПОЛОЖЕНИЯ

2.1. Настоящие Правила устанавливают порядок дистанционного банковского обслуживания Клиентов с использованием Системы ДБО в целях предоставления Услуг на платной основе и определяют возникающие в этой связи права, обязанности и ответственность Сторон. Настоящие Правила могут быть приняты Клиентом не иначе как путем присоединения к настоящим Правилам в целом в порядке, установленном настоящими Правилами.

2.2. Банк с целью ознакомления Клиента с условиями Правил размещает Правила на Сайте Банка. Моментом публикации настоящих Правил и ознакомления Клиента с опубликованными настоящими Правилами считается момент их первого размещения на Сайте Банка. Банк не несет ответственности, если информация об изменении и/или

дополнении настоящих Правил и/или Тарифов Банка, опубликованная в порядке и в сроки, установленные настоящими Правилами, не была получена и/или изучена и/или правильно истолкована Клиентом.

2.3. Клиент может пользоваться Услугами после заключения с Банком Договора о предоставлении Услуг путем присоединения к настоящим Правилам на основании надлежащим образом оформленного и подписанного в 2 (двух) экземплярах Заявления с даты подписания Акта о подключении Клиента к Системе ДБО (Приложение №4 к настоящим Правилам). Подписывая Заявление, Клиент подтверждает, что он ознакомлен и полностью согласен со всеми положениями настоящих Правил, действующих Тарифов Банка. Один экземпляр Заявления возвращается Банком Клиенту с отметкой Банка о принятии Заявления Банком.

2.4. Стороны пришли к соглашению, что момент получения Банком надлежащим образом оформленного и подписанного Клиентом Заявления будет считаться моментом заключения между Банком и Клиентом Договора о предоставлении Услуг. После заключения Договора о предоставлении Услуг настоящие Правила распространяются на совершение Сторонами определенных сделок и/или выполнение Сторонами определенных действий. Клиент, заключивший Договор о предоставлении Услуг на условиях настоящих Правил, принимает на себя все обязательства, предусмотренные Правилами в отношении Клиентов, и обязуется их выполнять. Осуществление Клиентом действий, указанных в Пункте 2.3. настоящих Правил, признаются Сторонами выражением согласия о полном и безоговорочном принятии Клиентом условий настоящих Правил (акцептом) в соответствии с пунктом 1 статьи 438 части 1 Гражданского кодекса Российской Федерации.

2.5. Клиент соглашается с тем, что при использовании Сторонами Системы ДБО в соответствии с настоящими Правилами в качестве средства удостоверения права Клиента распоряжаться денежными суммами, находящимися на счетах Клиента, открытых в Банке, в случае открытия Клиенту в Банке новых счетов после вступления в силу Договора о предоставлении Услуг, настоящие Правила будут распространяться на такие счета автоматически, если только Клиент не уведомит Банк в письменной форме об обратном.

2.6. При заключении Договора о предоставлении Услуг Стороны исходят из следующего:

2.6.1. настоящие Правила содержат условия Договора о предоставлении Услуг, присоединение к которым влечет за собой заключение договора присоединения в соответствии со статьей 428 Гражданского кодекса Российской Федерации, все условия настоящих Правил обязательны для Сторон;

2.6.2. Система ДБО и заложенные в ее основу программно-технические средства достаточны для обеспечения надежной защиты информации от несанкционированного доступа, подтверждения авторства и подлинности информации, содержащейся в получаемых Сторонами Электронных документах, а также для сохранения банковской тайны;

2.6.3. положительный результат проверки ЭП в Системе ДБО является подтверждением подлинности ЭП, с использованием которой подписан Электронный документ, а также подтверждением отсутствия в Электронном документе любых искажений;

2.6.4. Электронные документы и файлы (а также их распечатанные копии), хранящиеся в архивах Банка, подписанные с использованием Корректной ЭП, являются надлежащим доказательством в суде для решения любых спорных вопросов, в том числе, вопросов, связанных с подлинностью Электронного документа;

2.6.5. Электронные документы, подписанные Корректной ЭП Клиента, хранящиеся в архивах Банка или извлеченные из них в виде отдельного файла, признаются равнозначными соответствующим документам на бумажном носителе, подписанным Уполномоченным(и) Представителем(ями) Клиента и имеющим оттиск печати Клиента (если применимо), обладают юридической силой. Электронные документы, исходящие от Клиента без ЭП Клиента не имеют юридической силы, Банком не рассматриваются и не исполняются;

2.6.6. наличие у Банка Электронного документа, подписанного ЭП Клиента, проверка подлинности которой ключом проверки ЭП Клиента дала положительный результат, является необходимым и достаточным основанием для проведения Банком соответствующей операции на основании указанного Электронного документа, если иное не предусмотрено Договором банковского счета.

2.7. В целях обеспечения электронного документооборота Банк осуществляет следующие действия (включая, но не ограничиваясь):

2.7.1. прием от Клиента Электронных документов, защищенных от подделки ЭП, на выполнение операций по счетам Клиента в Банке;

2.7.2. предоставление Клиенту в виде Электронных документов, защищенных от подделки ЭП, информации об операциях, совершенных по счетам Клиента в Банке;

2.7.3. прием от Клиента и предоставление Клиенту информации в виде Электронных документов свободного формата, защищенных от подделки ЭП;

Перечень Электронных документов, передаваемых между Банком и Клиентом, приведен в Приложении №1 к Правилам.

2.8. Электронные документы передаются и принимаются с использованием Системы ДБО без их последующего представления на бумажном носителе, кроме случаев, предусмотренных настоящими Правилами.

2.9. Прием Электронных документов от Клиента осуществляется Банком в пределах Операционного времени. В случае получения Банком Электронного документа по окончании Операционного времени такой Электронный документ считается принятым Банком на следующий Операционный день, если иное не предусмотрено Договором банковского счета. При этом Банк не гарантирует возможность приема документов и доступа Клиента к Системе ДБО за пределами Операционного времени.

2.10. Стороны признают, что применяемые ими системы защиты информации от несанкционированного доступа и используемые телекоммуникации являются достаточными для обеспечения надежной и эффективной работы при обработке, хранении, приеме и передаче информации, а также обеспечивающими контроль целостности и авторства ЭП, достаточный для защиты от несанкционированного доступа и подтверждения авторства и подлинности электронных документов.

3. ПРАВА И ОБЯЗАННОСТИ БАНКА

Банк обязуется:

3.1. Предоставлять Клиенту по требованию актуальные Акты признания КППЭП своих Уполномоченных Представителей.

3.2. Принимать к исполнению поступившие в пределах Операционного времени от Клиента ЭД, оформленные и переданные в Банк в соответствии с требованиями действующего законодательства Российской Федерации, нормативными документами Банка России, условиями настоящих Правил, и заверенные Корректной ЭП Клиента, если иное не предусмотрено Договором банковского счета. Отказ Банка в приеме данных ЭД не означает ограничения прав Клиента на распоряжение денежными средствами, находящимися на счете и не лишает Клиента права представлять в Банк в целях распоряжения денежными средствами, находящимися на счете, расчетный (платежный) документ на бумажном носителе.

3.3. Предоставлять Клиенту информацию о статусе направленного Банку ЭД, подтверждающего получение и обработку Банком ЭД Клиента.

3.4. Формировать и в течение установленных законодательством сроков поддерживать архивы: всех входящих ЭД в принятом виде с ЭП; всех исходящих ЭД - в исходном виде с ЭП; сообщений свободного формата, подписанных ЭП электронных протоколов сеансов обмена информацией.

3.5. Информировать Клиента об исполнении распоряжений Клиента в интерфейсе Системы ДБО, а также путем направления выписки посредством Системы ДБО не позднее рабочего дня, следующего за днем исполнения распоряжения.

3.6. Рассматривать заявления Клиента при возникновении споров, связанных с использованием Клиентом Системы ДБО.

3.7. Уведомлять Клиента:

1) о результате проверки ЭП, регистрации (отказе в регистрации), приеме к исполнению, исполнении, отзыве, возврате (аннулировании) Электронного документа посредством присвоения Электронному документу соответствующего статуса; дата и время присвоения статуса фиксируется в Системе ДБО. В случае отказа в регистрации или исполнении Электронного документа, к статусу добавляется причина отказа.

Присвоение Банком Электронному документу соответствующего статуса в Системе ДБО является надлежащим уведомлением Клиента, в том числе о результатах приема к исполнению, отзыва, возврата (аннулирования) Электронного документа в соответствии с нормативными актами Банка России и не требует дополнительного направления Банком Клиенту какого-либо уведомления.

2) о получении через ИС «Одно окно» видов сведений «Предоставление информации, необходимой для перевода денежных средств или информации о начислении», «Предоставление информации, необходимой для перевода денежных средств с акцептом плательщиков» - не позднее дня получения такой информации, если она была получена в течении Операционного времени, не позднее следующего Операционного дня – если такая информация была получена после завершения Операционного времени.

Порядок взаимодействия Банка и Клиента с ИС «Одно окно» определен в Приложении №21 к настоящим Правилам.

3.8. На основании заявления, составленного в соответствии с приложением №19 и подписанного Клиентом, в срок не позднее 3 (трех) рабочих дней, следующих за датой получения заявления, установить/отменить ограничения по параметрам операций на перевод денежных средств Клиента по указанному Клиентом счету. Информирование Банком Клиента осуществляется путем направления информационного сообщения посредством Системы ДБО.

Заявление на установление ограничений может быть подано в Банк в форме электронного документа по системе ДБО, заявление на отмену ограничения подается на бумажном носителе.

Любые заявления Клиента принимаются Банком к исполнению только при условии, что они разборчиво, корректно заполнены и оформлены. В случае неразборчивого, некорректного заполнения и оформления заявления, представленного в Банк на бумажном носителе, заявления возвращаются Клиенту. В случае неразборчивого, некорректно заполнения и оформления заявления, представленного в Банк по Системе ДБО, Банк уведомляет Клиента об отказе в исполнении заявления и причинах такого отказа путем направления сообщения по Системе ДБО не позднее рабочего дня, следующего за днем получения такого заявления Банком от Клиента.

3.9. При получении распоряжения Клиента на перевод денежных средств Банк осуществляет его проверку на наличие признаков осуществления перевода денежных средств без добровольного согласия Клиента или с согласия Клиента, полученного под влиянием обмана или при злоупотребления доверием (далее - перевод денежных средств без добровольного согласия Клиента). При выявлении таких признаков Банк:

- 3.9.1. Приостанавливает прием к исполнению распоряжения Клиента на период до истечения следующего дня (за исключением Операций СБП); для Операции СБП Банк отказывает в совершении соответствующей операции (перевода).
- 3.9.2. При выявлении указанных признаков Банк незамедлительно в течение Операционного времени предоставляет Клиенту информацию посредством электронной почты и/или телефона¹, указанных Клиентом в качестве своих контактных данных:
- а) о приостановлении в исполнении распоряжения /отказе в совершении операции Клиента;
 - б) о рекомендациях по снижению рисков повторного осуществления перевода денежных средств без добровольного согласия Клиента;
 - в) о возможности Клиента не позднее дня, следующего за днем приостановления приема к исполнению указанного распоряжения или отказа в совершении Операции СБП:
 - подтвердить распоряжение по электронной почте и/или телефону (за исключением операций СБП);
 - совершить повторную операцию, содержащую те же реквизиты получателя (плательщика) и ту же сумму перевода (далее – повторная операция) (для операций СБП).
- 3.9.3. При получении от Клиента в Операционное время подтверждения распоряжения или осуществлении действий по совершению Клиентом повторной операции, Банк незамедлительно принимает к исполнению подтвержденное распоряжение Клиента или совершает повторную операцию, при отсутствии иных установленных законодательством Российской Федерации оснований не принимать распоряжение Клиента к исполнению (не совершать повторную операцию).

При получении от Клиента после завершения Операционного времени распоряжения, его подтверждение или осуществлении действий по совершению Клиентом операции (повторной операции) СБП Клиент несет риск отклонения Банком такой операции.

При неполучении от Клиента подтверждения распоряжения, указанное распоряжение считается не принятым к исполнению. При осуществлении действий по совершению Клиентом повторной операции способом, не предусмотренным Правилами повторная операция считается несовершенной.

Признаки осуществления перевода денежных средств без добровольного согласия клиента устанавливаются Банком России и размещаются на его официальном сайте в информационно-телекоммуникационной сети "Интернет".

3.10. В случае, если от Банка России получена информация, содержащаяся в базе данных о случаях и попытках осуществления переводов денежных средств без добровольного согласия Клиента, которая содержит сведения, относящиеся к получателю, Банк:

- при подтверждении распоряжения Клиентом, повторно приостанавливает прием к исполнению подтвержденного распоряжения Клиента;
- при проведении повторной операции СБП, отказывает в проведении повторной операции СБП.

3.10.1. Банк незамедлительно в течение Операционного времени уведомляет посредством электронной почты и/или телефона Клиента о повторном приостановлении приема к исполнению подтвержденного распоряжения Клиента/отказе в совершении повторной Операции СБП с указанием причины и срока такого приостановления/отказа: до истечения дня, следующего за днем направления Клиентом подтверждения распоряжения или проведения повторной операции СБП (далее «Период охлаждения»).

3.10.2. В течение указанного срока Клиент вправе отозвать свое распоряжение, направив запрос на отзыв распоряжения посредством системы ДБО.

3.10.3. По истечении Периода охлаждения Банк незамедлительно принимает к исполнению приостановленное распоряжение Клиента/совершает направленную Клиентом последующую повторную Операцию СБП, содержащую те же реквизиты получателя (плательщика) и ту же сумму перевода, при отсутствии иных установленных законодательством РФ оснований не принимать подтвержденное распоряжение/последующую повторную операцию Клиента к исполнению. Последующая повторная операция может быть направлена Клиентом в течение суток после окончания Периода охлаждения.

3.11. Действие пунктов 3.9-3.10 настоящих Правил не распространяется на случаи осуществления переводов денежных средств, являющихся заработной платой и (или) иными доходами, в отношении которых статьей 99 Федерального закона от 2 октября 2007 года N 229-ФЗ "Об исполнительном производстве" установлены ограничения размеров удержания, а также переводов денежных средств, являющихся доходами, на которые в соответствии со статьей 101 Федерального закона от 2 октября 2007 года N 229-ФЗ "Об исполнительном производстве" не может быть обращено взыскание.

3.12. Банк приостанавливает использование Клиентом системы ДБО, если от Банка России получена информация, содержащаяся в базе данных о случаях и попытках осуществления переводов денежных средств без добровольного согласия клиента, которая содержит сведения, относящиеся к Клиенту или его Системе ДБО, при наличии сведений федерального органа исполнительной власти в сфере внутренних дел о совершенных противоправных действиях, на период

¹ При направлении указанной информации по электронной почте и/или телефону считается, что Банк надлежащим образом выполнил свои обязательства по информированию вне зависимости результатов получения информации клиентом (сообщение не доставлено/не прочтено, соединения с абонентом по телефону)

нахождения таких сведений в указанной базе данных. Банк незамедлительно в течении Операционного времени уведомляет Клиента о факте такого приостановления посредством электронной почты и/или телефона.

Банк имеет право:

3.13. Отказать Клиенту в заключении Договора о предоставлении Услуг, в том числе в случае возникновения у Банка подозрений, что целью заключения является совершение операций в целях легализации (отмывания) доходов, полученных преступным путем, или финансирования терроризма.

3.14. Требовать от Клиента представления с использованием Системы ДБО или на бумажном носителе любых документов и информации о соблюдении Правил безопасной работы в Системе дистанционного банковского обслуживания АО МС Банк Рус (Приложение 10 к Правилам), а также документов, необходимых для обеспечения соблюдения Банком и Клиентом действующего законодательства Российской Федерации.

3.15. Использовать бумажную форму ЭД при необходимости подтверждения подписания Сторонами ЭД в отношениях с третьими лицами, включая, но, не ограничиваясь, государственные органы, органы судебной системы, нотариусы, иные организации, обращение в которые может потребоваться в связи с исполнением заключенных между Сторонами договоров в целях обеспечения прав и законных интересов Банка. Стороны признают заверение такой копии Уполномоченным Представителем Банка надлежащим и достаточным для целей, указанных выше. Клиент подтверждает свое согласие с тем, что в том случае, если какому-либо третьему лицу, включая, но, не ограничиваясь, государственному органу, органу судебной системы, нотариусу, иной организации, потребуется ознакомиться с Электронным документом, Банк может представить такой Электронный документ на любом электронном носителе информации. Такой способ предоставления ЭД Банк и Клиент признают надлежащим.

3.16. Отказывать Клиенту в приеме от него ЭД в случаях, предусмотренных законодательством Российской Федерации и нормативными актами Банка России. При принятии решения об отказе в приеме от Клиента ЭД Банк направляет Клиенту по Системе ДБО уведомление о прекращении приема ЭД в день принятия соответствующего решения и прекращает принимать ЭД от Клиента с момента направления Клиенту данного уведомления.

3.17. Отказать Клиенту в приеме ЭД по системе ДБО, если проводимая операция противоречит действующему законодательству, Договору банковского счета или если по операции не представлены документы, необходимые для фиксации информации в соответствии с законодательством.

3.18. Отказать Клиенту в исполнении принятого от него ЭД, кроме случаев, указанных в Правилах, в случае признания Банком операций Клиента сомнительными и/или совершаемыми в целях легализации (отмывания) доходов, полученных преступным путем, или финансирования терроризма, а также в иных случаях, предусмотренных законодательством Российской Федерации и внутренними нормативными документами Банка о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма.

3.19. Приостановить оказание Клиенту Услуг или расторгнуть Договор о предоставлении Услуг в следующих случаях (при этом Клиент вправе представить в Банк надлежащим образом оформленный расчетный документ на бумажном носителе), в случаях:

- 3.19.1. непредставления/несвоевременного представления или представления Клиентом неполных сведений (документов) в части идентификации, в том числе при обновлении сведений о Клиенте, его представителе, выгодоприобретателе, бенефициарном (-ых) владельце (-ах);
- 3.19.2. непредставления Банку в установленный срок затребованных документов относительно проводимых/проведенных операций либо деятельности Клиента в целом;
- 3.19.3. возникновения подозрений, что операция осуществляется в целях легализации (отмывания) доходов, полученных преступным путем, и финансирования терроризма;
- 3.19.4. при наличии фактов, свидетельствующих о нарушении Клиентом законодательства РФ, нормативных актов Банка России, требований, установленных настоящими Правилами, а также в случае выявления сомнительных операций Клиента и иных случаях, предусмотренных законодательством Российской Федерации;
- 3.19.5. ненадлежащего исполнения Клиентом своих обязательств по Договору банковского счета или по Договору о предоставлении Услуг;
- 3.19.6. по требованию уполномоченных государственных органов в случаях и в порядке, предусмотренных законодательством Российской Федерации;
- 3.19.7. нарушения Клиентом порядка использования электронного средства платежа, содержащегося в Правилах;
- 3.19.8. на период нахождения сведений, относящихся к Клиенту или его электронному средству платежа, в базе данных Банка России о случаях и попытках осуществления переводов денежных средств без добровольного согласия клиента.
- 3.19.9. в иных случаях по усмотрению Банка с уведомлением не позднее дня принятия решения.

3.20. В случае приостановления оказания Клиенту Услуг или расторжения Договора о предоставлении Услуг в случаях, предусмотренных настоящими Правилами, Банк уведомляет об этом Клиента посредством электронной почты и/или телефона.

4. ПРАВА И ОБЯЗАННОСТИ КЛИЕНТА

Клиент обязуется:

- 4.1. Строго следовать всем требованиям и инструкциям, описанным в настоящих Правилах и Приложениях к ним. Соблюдать Правила безопасной работы в Системе дистанционного банковского обслуживания АО МС Банк Рус (Приложение 10 к Правилам), в том числе с целью противодействия осуществлению перевод денежных средств без добровольного согласия Клиента.
- 4.2. Клиент обязан выполнять требования Банка по устранению возможных уязвимостей в защите Системы ДБО, выявленных в процессе эксплуатации Системы ДБО.
- 4.3. Оплачивать услуги Банка в соответствии со Статьей 5 настоящих Правил.
- 4.4. Обеспечивать получение и использование КЭП Владельцами КЭП в порядке, предусмотренном Правилами.
- 4.5. Производить смену КЭП своих Уполномоченных Представителей в случаях, предусмотренных настоящими Правилами и Приложениями к ним.
- 4.6. Передать Банку по его требованию в срок не позднее трех рабочих дней с даты его обращения распечатанную на бумажном носителе и заверенную подписями Уполномоченных Представителей Клиента и оттиском печати (при наличии) Клиента копию ЭД, принятого Банком от Клиента по Системе ДБО.
- 4.7. Сверять данные, содержащиеся в ЭД, с собственными данными и незамедлительно информировать Банк о любых обнаруженных расхождениях или ошибках.
- 4.8. Заполнять ЭД в Системе ДБО в соответствии с действующим законодательством РФ, нормативными документами Банка России и требованиями Банка.
- 4.9. Соблюдать Регламент действий клиентов АО МС Банк Рус в случае осуществления или попытки осуществления несанкционированного доступа в Систему ДБО (Приложение 11 к Правилам) и незамедлительно, но не позднее дня, следующего за днем получения от Банка уведомления о совершенной операции, сообщать об этом Банку. При выявлении нарушения безопасности Системы ДБО, выявлении фактов или признаков таких нарушений (в т.ч. выявления вредоносного программного обеспечения или доступа к оборудованию с установленной Системой ДБО неуполномоченных лиц), немедленно приостановить использование Системы ДБО и оповестить Банк любым доступным способом, в т.ч. по телефону, по электронной почте с последующим предоставлением заявления (Приложение 14 к Правилам). При наступлении событий, связанных с Компрометацией пароля доступа в Систему ДБО или КЭП, независимо от наличия или отсутствия сведений о несанкционированном использовании КЭП и/или Системы ДБО, в том числе КЭП Единого окна ДБО, Клиент должен незамедлительно проинформировать об этом Банк.
- Информирование Банка может осуществляться любым доступным способом, в т.ч. по телефону, по электронной почте dbosupport@mcbankrus.ru с последующим предоставлением в произвольной форме заявления, оформленного надлежащим образом на бумажном носителе или по системе электронного документооборота (согласно Банковским правилам). При наступлении событий, связанных с Компрометацией КЭП, соответствующие КЭП не подлежат дальнейшему использованию Клиентом. При наступлении событий, связанных с Компрометацией КЭП, Банк прекращает предоставление Клиенту Услуг с использованием КЭП, в отношении которых поступили уведомления о таких событиях в установленном настоящим пунктом порядке.
- 4.10. Клиент обязан незамедлительно уведомлять Банк в письменной форме об изменении своего наименования, местонахождения, организационно-правовой формы, смене Уполномоченных Представителей, а также смене их имен и фамилий. В случае изменения состава пользователей Системы ДБО, Клиент обязан предоставить в Банк обновленное Заявление с предоставлением документов, подтверждающие такие изменения.
- Правом подписания ЭД обладают только те лица, которых Клиент указал в карточке с образцами подписей и оттиска печати Клиента, имеющейся в Банке. В случае, если Клиенту необходимо предоставить доступ к системе ДБО Пользователю, не имеющему право подписи (не указанному в карточке с образцами подписей и оттиска печати), данный Пользователь должен быть указан в Заявлении с отметкой «Без права подписи» с предоставлением в Банк копии документа, удостоверяющей его личность, заверенной Клиентом.
- 4.11. В случае возникновения конфликтных ситуаций между Клиентом и Банком при использовании Системы ДБО Клиент обязуется участвовать в разрешении конфликтов в соответствии с процедурой, установленной Приложением №5 к настоящим Правилам, выполнять требования данной процедуры и выполнять принятые в соответствии с ней решения и нести за них ответственность.
- 4.12. В момент заключения Договора о предоставлении Услуг уведомить Банк о том, кто из представителей Клиента уполномочен действовать от имени Клиента в качестве Пользователя Системы ДБО.
- 4.13. Проверять официальный сайт Банка (www.mcbankrus.ru) на предмет изменений в Правилах.
- 4.14. Проверять в Системе ДБО уведомления Банка о статусе, присвоенном ЭД Клиента по мере направления Клиентом ЭД в Банк, и изменения Банком Статусов, присвоенных ЭД в Системе ДБО, а также проверять выписки, направленные Банком.

Клиент имеет право:

- 4.15. Аннулировать, приостанавливать, возобновлять действие КЭП в порядке, предусмотренном Правилами.
- 4.16. В случае возникновения у Клиента претензий, связанных с принятием или непринятием, исполнением или неисполнением Банком ЭД, требовать от Банка проведения согласительной комиссии в соответствии с Приложением № 5 к настоящим Правилам.

4.17. Отозвать ранее переданный ЭД, имеющий Корректные ЭП Клиента, путем направления в Банк по Системе ДБО соответствующего заявления об отзыве в электронном виде в виде ЭД, защищенного ЭП, при условии, что к моменту получения соответствующего заявления Клиента по отзываемому ЭД не наступила безотзывность соответствующего распоряжения в соответствии с действующим законодательством Российской Федерации и нормативными актами Банка России.

4.18. Подать заявление в Банк России об исключении сведений из базы данных Банка России о случаях и попытках осуществления переводов денежных средств без добровольного согласия клиента, относящихся к Клиенту и (или) его Системе ДБО, самостоятельно в порядке, установленном Указанием Банка России от 13.06.2024 N 6748-У², или через Банк путем предоставления заявления. Заявление может быть подано Клиентом в Банк лично, направлено в Банк через Систему ДБО, либо почтой России. Заявление должно содержать наименование Клиента, ИНН, номер счета и описание ситуации.

4.19. Клиент не вправе, ни при каких обстоятельствах, передавать третьим лицам свои права или обязанности, возникающие у него в соответствии с настоящими Правилами.

4.20. Клиент, присоединяясь к настоящим Правилам, подтверждает, что при передаче персональных данных Владельцев КЭП, Клиент обладает согласием вышеуказанных лиц на передачу Банку, дальнейшую обработку и хранение персональных данных Владельцев КЭП Банком. Персональные данные вышеуказанных лиц состоят из имени, фамилии, отчества, паспортных данных (или данных иного документа, удостоверяющего личность), даты и места рождения, адреса регистрации/места жительства, и иной информации, предоставленной Клиентом. Клиент подтверждает, что Владельцы КЭП уведомлены и предоставили свое согласие на обработку и хранение Банком их персональных данных в целях предоставления Клиенту банковских и иных услуг в рамках своей деятельности.

4.21. Дополнительные права и обязанности Клиента устанавливаются в Приложениях к настоящим Правилам.

4.22. Направить Заявление на конфигурирование Системы ДБО в соответствии с приложением №19 с целью установить/отменить ограничения по параметрам операций на перевод денежных средств по указанному Клиентом счету.

4.23. Направить Заявление на создание Единого окна ДБО для Клиента и его обособленных подразделений в соответствии с приложением № 20. На основании поданного заявления предоставляется доступ ко всем подключенным к системе ДБО счетам Клиента и его обособленных подразделений.

5. ПЛАТА ЗА УСЛУГИ БАНКА И ПОРЯДОК РАСЧЕТОВ

5.1. Стоимость Услуг устанавливается согласно Тарифам Банка.

5.2. Клиент дает Банку заранее данный акцепт на списание в полном объеме со счетов Клиента, открытых в Банке, причитающихся Банку сумм стоимости Услуг и перечисления указанных сумм в пользу Банка, Клиент обязан предоставить Банку заявление о заранее данном акцепте по установленной Банком форме.

5.3. В случае расторжения Договора о предоставлении Услуг Клиент обязан оплатить Услуги за весь календарный месяц, в котором было завершено обслуживание по Системе ДБО.

5.4. Клиент обязан также возмещать Банку любые дополнительные расходы и затраты, которые могут возникнуть у Банка в результате пользования Клиентом Услугами.

6. ОТВЕТСТВЕННОСТЬ СТОРОН

6.1. За невыполнение или ненадлежащее выполнение обязательств по настоящим Правилам виновная Сторона несет ответственность в соответствии с действующим законодательством Российской Федерации.

6.2. Стороны несут ответственность за содержание Электронных документов, подписанных КЭП их Уполномоченных Представителей, и не отвечают за правильность заполнения и оформления Электронных документов другой Стороной.

6.3. Банк не несет ответственность:

6.3.1. за ущерб, возникший вследствие разглашения Владельцем КЭП, Уполномоченным Представителем Клиента КЭП, его утраты или его передачи, вне зависимости от причин, неуполномоченным лицам.

6.3.2. за убытки Клиента, вызванные прямо или косвенно, несанкционированным использованием КЭП в случае, если Клиент не исполнил свои обязанности по обеспечению безопасности Системы ДБО, информированию Банка о наступлении событий, связанных с несанкционированным списанием денежных средств, несанкционированными попытками доступа в Систему ДБО, выявления признаков нарушения безопасности Системы ДБО Компрометации пароля доступа в Систему ДБО или КЭП.

² Указание Банка России от 13.06.2024 № 6748-У «О порядке подачи клиентом оператора по переводу денежных средств в Банк России заявления об исключении сведений, относящихся к клиенту и (или) его электронному средству платежа, из базы данных о случаях и попытках осуществления переводов денежных средств без добровольного согласия клиента, порядке принятия Банком России мотивированного решения об удовлетворении или об отказе в удовлетворении заявления клиента оператора по переводу денежных средств или мотивированного заявления оператора по переводу денежных средств об исключении сведений, относящихся к клиенту и (или) его электронному средству платежа, из базы данных о случаях и попытках осуществления переводов денежных средств без добровольного согласия клиента»

6.3.3. за последствия исполнения расчетного Электронного документа, защищенного Корректной ЭП Клиента, в т.ч. в случае использования Ключей ЭП и/или Ключей проверки ЭП, программно-аппаратных средств клиентской части Системы ДБО неуполномоченным лицом.

6.3.4. за ущерб, возникший вследствие неправильного оформления Клиентом Электронных документов; за убытки Клиента, возникшие в случае отклонения операции, если она соответствует признакам осуществления перевода денежных средств без добровольного согласия Клиента, в случае направления распоряжения о совершении операции или подтверждения такого распоряжения после завершения Операционного времени.

6.3.5 за срывы и помехи в работе используемого Клиентом канала связи, приводящих к невозможности передачи в Банк Электронных документов.

6.3.6. за ненадлежащее функционирование, либо неисправности в функционировании технических и программных средств, каналов связи, принадлежащих Клиенту или третьим лицам и используемых в процессе работы с Системой ДБО.

6.3.7. за неработоспособность оборудования или программных средств Клиента или третьих лиц, повлекших за собой невозможность доступа Клиента к Системе ДБО и возникшие в результате этого задержки в осуществлении платежей Клиента, а также за возможное уничтожение (в полном или частичном объеме) информации, содержащейся на вычислительных средствах Клиента для обеспечения предоставления Услуг согласно настоящим Правилам.

6.3.8. за неисправности в функционировании аппаратно-программного обеспечения Клиента, а также за неисправности в функционировании Системы ДБО, вызванные неисправностями аппаратно-программного обеспечения Клиента.

6.3.9. ни при каких обстоятельствах за убытки, которые Клиент может понести в связи с тем, что Электронные документы, направленные посредством Системы ДБО, могут оказаться неправильно отражающими состояние счетов Клиента в Банке на момент их получения Клиентом, за исключением случаев, когда такие убытки являются результатом умышленных действий/бездействия Банка или его грубой неосторожности. Клиент соглашается с тем, что на нем всецело будут лежать риски, сопряженные с принятием коммерческих решений, основанных на Электронных документах, направленных Банком Клиенту.

6.3.10. ни при каких обстоятельствах за убытки, которые Клиент может понести в связи с тем, что Клиентом не были соблюдены требования, указанные в разделе 4 настоящих Правил.

6.3.11. ни при каких обстоятельствах за убытки, которые Клиент может понести в связи с тем, что Клиент произвел установку и подключение к Системе ДБО не с Установочных комплектов, распространяемых Банком.

6.4. Банк несет ответственность за целостность и достоверность архивов, указанных в п. 3.4. настоящих Правил.

6.5. Стороны несут ответственность по всем ЭД с ЭП Клиента, сформированным в Системе ДБО, в соответствии с действующим законодательством РФ.

6.6. В случае возникновения обстоятельств непреодолимой силы Стороны по настоящим Правилам освобождаются от ответственности за неисполнение или ненадлежащее исполнение взятых на себя обязательств.

6.7. Обстоятельствами непреодолимой силы считаются события, наступившие после заключения Договора о предоставлении Услуг независимо от воли Сторон, и которые невозможно было предусмотреть в момент заключения Договора о предоставлении Услуг. Указанные события своим влиянием откладывают или препятствуют выполнению всех или части обязательств по настоящим Правилам. Обстоятельствами непреодолимой силы считаются, в частности, но, не ограничиваясь, следующие обстоятельства: война, эпидемия, пожар, природные катаклизмы, изменения законодательства, запрещающие или препятствующие исполнению Сторонами своих обязательств по настоящим Правилам. Данный выше перечень не является исчерпывающим.

6.8. Если выполнение обязательств должно быть отложено из-за действия обстоятельств непреодолимой силы, Сторона, подвергшаяся действию указанных обстоятельств, письменно в течение 5 (пяти) календарных дней с момента наступления обстоятельства непреодолимой силы извещает другую Сторону о дне начала действия обстоятельств непреодолимой силы. Извещение должно содержать данные о характере обстоятельств, а также оценку их влияния на возможность исполнения Стороной обязательств по настоящим Правилам. Обстоятельства непреодолимой силы Стороны подтверждают путем представления копий актов компетентных органов. С прекращением действия обстоятельств непреодолимой силы и восстановлением нормальных условий Сторона, подвергшаяся действию непреодолимой силы, извещает об этом таким же образом другую Сторону.

6.9. Если Сторона не известит другую Сторону о наступлении и прекращении обстоятельств непреодолимой силы с приложением подтверждающих документов, она теряет право ссылаться на их действие.

6.10. В случае неоплаты Банку предоставленных Услуг (в том числе по причине отсутствия достаточной суммы средств на счетах Клиента в Банке или невозможности списания средств в связи с приостановлением расходных операций по счету или наложением ареста на денежные средства, находящиеся на счетах Клиента в Банке), Банк имеет право приостановить на срок до одного месяца предоставление Услуг по настоящим Правилам, а в случае неоплаты по истечении указанного срока – расторгнуть Договор о предоставлении Услуг в одностороннем порядке без соблюдения срока, установленного Пунктом 7.2. настоящих Правил. При этом Клиенту направляется письменное уведомление о расторжении Договора о предоставлении Услуг.

6.11. Стороны обязуются сохранять конфиденциальность и без предварительного письменного согласия другой Стороны не разглашать третьим лицам для каких-либо целей любые факты и информацию или иных данные, предостав-

ленные Сторонами в связи с настоящими Правилами, за исключением случаев, когда это требуется согласно законодательству РФ, а также за исключением случаев раскрытия этих сведений юристам, налоговым и финансовым консультантам Сторон и лицам, которым были уступлены права и обязанности по Договору о предоставлении Услуг. Обязательства по соблюдению конфиденциальности не распространяются на общедоступную информацию.

7. ПРОЧИЕ УСЛОВИЯ

7.1. Договор о предоставлении Услуг действует в течение неопределенного срока.

7.2. Стороны имеют право расторгнуть Договор о предоставлении Услуг в одностороннем порядке. Сторона, инициирующая расторжение Договора о предоставлении Услуг, обязуется известить вторую Сторону в письменной форме не менее чем за 30 (Тридцать) дней до предполагаемой даты расторжения.

7.3. Досрочное расторжение Договора о предоставлении Услуг возможно при условии выполнения Сторонами обязательств, предусмотренных настоящими Правилами, а также Приложениями к настоящим Правилам. При этом Стороны обязаны завершить расчеты и подписать соответствующее соглашение о расторжении Договора о предоставлении Услуг. Договор о предоставлении Услуг в этом случае считается расторгнутым с даты, определенной в соглашении о расторжении.

7.4. При возникновении разногласий и споров в связи с обменом ЭД с помощью Системы ДБО с целью установления фактических обстоятельств, послуживших основанием для их возникновения, а также для проверки целостности и подтверждения Авторства ЭД, назначается согласительная комиссия, процедура и сроки проведения которой установлены Приложением №5 к настоящим Правилам. Споры, по которым не достигнуто соглашение Сторон после проведения согласительной комиссии, а также иные споры, возникающие между Сторонами в рамках настоящих Правил, разрешаются в Арбитражном суде г. Москвы в соответствии с действующим законодательством Российской Федерации.

7.5. Банк имеет право в одностороннем порядке вносить в настоящие Правила изменения, которые вступают в силу через 15 (Пятнадцать) календарных дней с момента уведомления Клиента путем размещения новой редакции Правил на Сайте Банка. Датой уведомления будет считаться дата размещения новой редакции Правил на Сайте Банка. В случае несогласия Клиента с вносимыми изменениями, он имеет право отказаться от использования Услуг и расторгнуть Договор о предоставлении Услуг в порядке, предусмотренном Пунктом 7.2. настоящих Правил.

7.6. Клиент обязан регулярно знакомиться с информацией, публикуемой Банком в порядке, установленном настоящими Правилами. Банк не несет ответственности, если информация об изменении настоящих Правил, опубликованная в порядке и в сроки, установленные настоящими Правилами, не была получена Клиентом. Любые изменения настоящих Правил с момента их вступления в силу равно распространяются на всех Клиентов, присоединившихся к настоящим Правилам, в том числе присоединившихся к настоящим Правилам ранее даты вступления изменений в силу.

7.7. В случаях, непредусмотренных настоящими Правилами, Стороны руководствуются действующим законодательством РФ, Договором банковского счета, а также иными договорами, заключенными между Сторонами.

7.8 Все положения Правил распространяют свое действие так же на формат работы в Едином окне ДБО.

7.9. Приложения, являющиеся неотъемлемыми частями настоящих Правил:

Приложение №1. Перечень электронных документов, направляемых Сторонами.

Приложение №2. Порядок регистрации Уполномоченных представителей в Системе ДБО.

Приложение №3. Порядок обслуживания по банковскому счету/ счетам с применением Электронных документов.

Приложение № 4. Акт о подключении Клиента к Системе ДБО.

Приложение № 5. Порядок создания и работы согласительной комиссии.

Приложение № 6. Форма Доверенности.

Приложение № 7. Акт признания ключа проверки электронной подписи.

Приложение № 8. Акт приема/ передачи.

Приложение № 9. Заявление о присоединении к Правилам дистанционного банковского обслуживания АО МС Банк Рус.

Приложение № 10. Правила безопасного использования Системы дистанционного банковского обслуживания АО МС Банк Рус.

Приложение № 11. Регламент действий клиентов АО МС Банк Рус в случае несанкционированного списания или попытки списания денежных средств со счета.

Приложение № 12. Акт об изъятии носителей информации.

Приложение № 13. Форма письма интернет-провайдеру о предоставлении журналов соединений (логов).

Приложение № 14. Заявление о блокировании доступа к Системе дистанционного банковского обслуживания (Системе ДБО).

Приложение № 15. Заявление об отзыве платежа, возврате денежных средств и блокировании доступа к Системе дистанционного банковского обслуживания АО МС Банк Рус.

Приложение № 16. Примерный перечень вопросов, на которые необходимо дать ответ при описании инцидента.

Приложение № 17. Справка по факту инцидента информационной безопасности, обнаруженном при использовании Системы дистанционного банковского обслуживания АО МС Банк Рус.

Приложение № 18. Перечень подтверждающих документов.

Приложение №19. Заявление на конфигурирование Системы ДБО.

Приложение №20. Заявление на создание Единого окна ДБО для Клиента и его обособленных подразделений

Приложение №21. Порядок взаимодействия Банка и Клиента с ИС «Одно окно»

Приложение № 1 к Правилам дистанционного банковского обслуживания АО МС Банк Рус

Перечень электронных документов, направляемых Сторонами.

1.1. Перечень электронных документов, направляемых Клиентом Банку:

- платежное поручение (в рублях РФ);
- заявление на перевод иностранной валюты;
- поручение на перевод по СБП;
- заявление на регистрацию QR;
- поручение на конверсию иностранной валюты;
- поручение на покупку иностранной валюты;
- поручение на продажу иностранной валюты;
- запрос на получение выписки о состоянии счетов;
- справка о подтверждающих документах;
- сведения о валютных операциях;
- контракт для постановки на учет;
- кредитный договор для постановки на учет;
- заявление об изменении сведений о контакте(кредитном договоре)
- заявление о снятии с учета контракта (кредитного договора);
- распоряжение на обязательную продажу иностранной валюты;
- письмо (документ свободного формата, в котором информация представлена в электронном виде);
- отзыв электронного документа;
- другой документ по запросу Банка либо возникающий в связи с необходимостью осуществления Клиентом операций и сделок;
- любые документы в рамках исполнения кредитных договоров и договоров обеспечения, в том числе, но не исключительно, заявление о предоставлении кредита, а также дополнительные соглашения к кредитным договорам и/или договорам обеспечения;
- документы, оформленные по форме Банка;
- отдельные документы для получения/обновления сведений о Клиенте, его представителях, выгодоприобретателях и бенефициарных владельцах в соответствии с порядком, определенным Банковскими правилами.

При этом Стороны признают, что использование документов в электронном виде не исключает возможность использования документов на бумажном носителе.

1.2. Перечень электронных документов, направляемых Банком Клиенту:

- выписки о состоянии любых счетов Клиента, имеющих у него в Банке;
- любые документы в рамках исполнения кредитных договоров и договоров обеспечения, в том числе, но не исключительно, уведомление о повышении или понижении процентной ставки по кредитному договору, требование о досрочном погашении кредита, запросы о предоставлении документов и информации, требование о страховании предмета залога, документы в связи с обращением взыскания на предмет залога, а также дополнительные соглашения к кредитным договорам и/или договорам обеспечения;
- другие документы, необходимые для передачи.

Приложение № 2 к Правилам дистанционного банковского обслуживания АО МС Банк Рус

ПОРЯДОК РЕГИСТРАЦИИ УПОЛНОМОЧЕННЫХ ПРЕДСТАВИТЕЛЕЙ В СИСТЕМЕ ДБО

Настоящий Порядок устанавливает правила регистрации Уполномоченных представителей в системе ДБО и формирования КЭП, КПЭП и Акта признания КПЭП.

1. В течение 5 (Пяти) рабочих дней после подписания и направления Клиентом в Банк Заявления Банк предоставляет, а Клиент или его представитель, действующий на основании доверенности, оформленной в соответствии с требованиями действующего законодательства, может получить в Банке Установочный комплект для каждого Уполномоченного представителя, 2 (Два) экземпляра Акта признания КПЭП Банка
2. Получив Установочные комплекты, Клиент или его представитель должен подписать «Акт приема-передачи» (Приложение №8 к Правилам).
3. Каждый Пользователь системы ДБО, получив конверт, содержащий Носитель ключевой информации, логин и пароль для первоначального входа в систему ДБО, должен:
 - 3.1 войти в Систему ДБО, указав присвоенный ему логин и пароль;
 - 3.2 после первого входа в Систему ДБО, сменить пароль для входа, сформировать на Носителе ключевой информации пару КЭП и КПЭП и направить запрос на регистрацию КПЭП через Систему ДБО в Банк т.е. сформировать свой закрытый ключ (КЭП), соответствующий ему открытый ключ (КПЭП) отправить на регистрацию в Банк;
 - 3.3 распечатать в 2 (Двух) экземплярах Акт признания КПЭП, заверить подписью Пользователя и передать их в Банк.
4. Получив от клиента надлежащим образом оформленный Акт признания КПЭП, Банк производит сверку текста КПЭП (открытого ключа) Пользователя и КПЭП, указанного в запросе на регистрацию. При положительном результате сверки Банк обрабатывает запрос на регистрацию КПЭП, заверяет Акт признания КПЭП Пользователя и возвращает 1 экземпляр акта Клиенту, изготавливает и направляет через Систему ДБО сертификат КПЭП Клиенту, в противном случае банк уведомляет клиента о выявленных нарушениях.
5. После обработки Банком запроса на регистрацию КПЭП, каждый Пользователь в Системе ДБО должен принять сертификат КПЭП, после чего новые КЭП и КПЭП вводятся в эксплуатацию.

ПОРЯДОК ОБСЛУЖИВАНИЯ ПО ДОГОВОРУ БАНКОВСКОГО СЧЕТА С ПРИМЕНЕНИЕМ ЭЛЕКТРОННЫХ ДОКУМЕНТОВ

Обмен ЭД между Банком и Клиентом осуществляется по Системе ДБО, которая состоит из 2-х частей. Со стороны Банка – сервер, где установлена банковская часть системы (далее – абонентский пункт Банка), со стороны Клиента – персональный компьютер (один или несколько), где установлено рабочее место пользователя системы (далее – абонентский пункт Клиента).

Абонентский пункт Клиента должен удовлетворять следующим требованиям к программному обеспечению:

- операционная система из следующего перечня
 - Windows 10 x32/x64; Windows 11 x32/x64;
 - Astra Linux: Common Edition версии orel-2.12.45, ядро linux-5.* и выше. Special Edition "Воронеж" v.1.
- браузер из следующего перечня
 - Chrome;
 - Firefox;
 - Edge;
 - Safari;
 - Яндекс.Браузер.

Абонентский пункт Клиента должен находиться в помещении с ограниченным доступом персонала.

Порядок подготовки, передачи и приёма ЭД

Сторона-отправитель с использованием своего абонентского пункта готовит Электронный документ для передачи. Перечень ЭД, разрешенных к обмену по Системе ДБО, указан в Приложении №1 настоящих Правил.

Сторона-отправитель с использованием своего абонентского пункта проставляет под документом необходимое количество своих ЭП в соответствии с информацией, представленной по форме Приложения №9 настоящих Правил.

Сторона-получатель с использованием своего абонентского пункта осуществляет все виды контроля полученного ЭД:

- подтверждение подлинности ЭД;
- логический контроль ЭД;
- проверка ЭД на возможность исполнения.

Контроль подтверждения подлинности ЭД состоит из проверки правильности всех ЭП, которыми подписан ЭД, и проверки соответствия зарегистрированных владельцев КЭП отправителю ЭД.

ЭД, подлинность которых подтверждена, принимаются в дальнейшую обработку.

Подлинные ЭД участников подвергаются процедуре логического контроля, которая состоит в проверке правильности составления ЭД и в установлении соответствия реквизитов ЭД нормативно - справочной информации.

При успешном завершении всех этапов контроля ЭД Клиента выполняется Банком в соответствии с законодательством и условиями Договора о предоставлении услуг/ Договоров банковского счета.

На всех этапах обработки ЭД получает статус, однозначно отражающий его состояние в Системе ДБО.

Приложение № 4
к Правилам дистанционного банковского обслуживания АО МС Банк Рус

ОБРАЗЕЦ

АКТ
О ПОДКЛЮЧЕНИИ КЛИЕНТА К СИСТЕМЕ ДБО № _____ от « ____ » _____ 20__ г.

Акционерное общество МС Банк Рус, именуемое в дальнейшем «Банк», в лице _____, действующего на основании _____, с одной стороны, и _____, именуемый в дальнейшем «Клиент» в лице _____, действующего на основании _____, с другой стороны, вместе именуемые «Стороны», составили настоящий Акт о нижеследующем:

В соответствии с Правилами дистанционного банковского обслуживания АО МС Банк Рус с использованием Системы ДБО Сторонами проведены следующие мероприятия по подключению Клиента к Системе ДБО:

- Банком передано, а Клиентом получено программное обеспечение (дистрибутив) и комплект документации, необходимые для подключения и работы в Системе ДБО;
- на автоматизированном рабочем месте Клиентом проведена установка и настройка программного обеспечения;
- Клиентом сгенерированы и зарегистрированы в Банке криптографические ключи должностных лиц Клиента, уполномоченных подписывать электронными подписями (ЭП) передаваемые в Банк электронные документы (ЭД);
- проверена работа в Системе ДБО с автоматизированного рабочего места Клиента в режимах передачи и приема ЭД.

Мероприятия по подключению к Системе ДБО выполнены Сторонами в полном объеме, система ДБО полностью работоспособна и вводится в эксплуатацию с момента подписания настоящего Акта.

Настоящий Акт составлен в двух экземплярах, имеющих равную юридическую силу, по одному для каждой из Сторон.

ПОДПИСИ СТОРОН:

БАНК:

М.П.

КЛИЕНТ:

Руководитель

М.П.

ПОРЯДОК СОЗДАНИЯ И РАБОТЫ СОГЛАСИТЕЛЬНОЙ КОМИССИИ

При возникновении разногласий между Банком и Клиентом, связанных с обменом ЭД, заявитель обязан в пятидневный срок со дня обнаружения разногласий подготовить и направить другой Стороне письменный документ, подписанный уполномоченным должностным лицом, с изложением существенных обстоятельств случившегося. При нарушении срока подачи письменного заявления данный документ не рассматривается.

Примечание: До подачи заявления заявителю рекомендуется убедиться в целостности своего программного обеспечения, неизменности используемых КЭП и КПЭП, а также отсутствии несанкционированных действий со стороны собственного персонала.

Документ должен быть рассмотрен стороной - ответчиком не позднее трех рабочих дней со дня получения.

В случае отказа стороны-ответчика от удовлетворения заявления, для рассмотрения конфликтных ситуаций в недельный срок совместным решением обеих Сторон создается согласительная комиссия в количестве не менее 3 человек, в следующем составе: Пользователи Системы ДБО со стороны Клиента и представители Банка.

Кроме того, в случае необходимости, могут привлекаться независимые эксперты и технические специалисты сторонних организаций, в том числе, изготовителей программного обеспечения и средств защиты информации.

Состав комиссии согласовывается Сторонами и утверждается двухсторонним актом.

В ходе разбора конфликта согласительной комиссией проверяется соответствие изготовления и передачи спорного ЭД Правилам и Договору банковского счета, а также подлинность ЭП под спорным ЭД.

При разрешении разногласий используются эталонные программно-аппаратные средства. Держателем эталонных программно-аппаратных средств признается Банк.

Комиссия в двухнедельный срок на территории Банка проводит разбор конфликтной ситуации, результаты которого оформляются Актом с изложением сути конфликта, определением виновной Стороны и возможных сроков устранения причин возникновения конфликта. Стороны предоставляют документы, являющиеся надлежащими доказательствами соответствующих фактов при рассмотрении споров.

Банк предоставляет следующие документы:

- Акт о начале использования Системы ДБО Клиентом;
- спорный ЭД в виде файла, экспортированного из базы данных, входящих ЭД Системы ДБО;
- журналы работы и протоколы операций Системы ДБО;
- Акты признания и сертификаты КПЭП Клиента;
- иные документы при необходимости.

Клиент предоставляет следующие документы:

- Заявления с отметками Банка о принятии;
- Акты признания и сертификаты КПЭП Банка;
- Заявления Клиента, в т.ч. заявления о компрометации КПЭП с отметками Банка о принятии;
- документы, свидетельствующие о расторжении Договора о предоставлении услуг;
- иные документы при необходимости.

Подлинность ЭД Клиента проверяется в следующем порядке:

- Установление факта соответствия спорного ЭД, представленного Банком, предмету спора.
- Установление круга лиц, уполномоченных на подписание ЭП спорного ЭД на момент генерации ЭП спорного ЭД.
- Проверка действительности КПЭП на момент выработки каждой ЭП.
- Проверка корректности всех ЭП спорного ЭД.
- Установление соответствия шестнадцатеричных значений КПЭП соответствующим значениям, указанными в Актах признания КПЭП.

Спорный ЭД признается подлинным тогда и только тогда, когда одновременно выполнены все следующие условия:

- представлен ЭД, соответствующий предмету спора;
- КПЭП действовали в момент генерации соответствующих ЭП;
- спорный ЭД содержит необходимое количество корректных ЭП лиц, имеющих надлежащие полномочия;
- шестнадцатеричные значения КПЭП соответствуют значениям, указанным в Актах признания КПЭП.

Решения комиссии, отраженные в Акте, являются обязательными для Сторон.

Приложение № 6
к Правилам дистанционного банковского обслуживания АО МС Банк Рус

Доверенность

г. _____

(дата прописью)

(наименование организации)

ОГРН _____, место нахождения: _____,
в лице _____,

(наименование должности и ФИО руководителя)

действующего на основании _____, настоящей доверенностью уполномочивает

(Фамилия Имя Отчество Доверенного лица)

Дата рождения: _____ Место рождения: _____ Гражданство: _____

Паспорт: _____ Серия _____ Номер _____ выдан _____

код подразделения _____ Дата выдачи « _____ » _____ года

Адрес места жительства (регистрации) или места пребывания: _____

Для иностранных граждан: данные миграционной карты, документа, подтверждающего право иностранного гражданина на пребывание (проживание) в Российской Федерации

Получить в АО МС Банк Рус:

•

(указывается только нужное).

Доверенность выдана без права передоверия на _____.

Подпись _____ удостоверяю.
(ФИО доверенного лица) (подпись Доверенного лица)

М.П.

Руководитель

Подпись

ФИО

Главный бухгалтер

Подпись

ФИО

Приложение № 7
к Правилам дистанционного банковского обслуживания АО МС Банк Рус

ФОРМА

АКТ

ПРИЗНАНИЯ ОТКРЫТОГО КЛЮЧА ЭП
ДЛЯ ОБМЕНА СООБЩЕНИЯМИ

Настоящим Актом признается ключ проверки электронной подписи, принадлежащий уполномоченному представителю:

ФИО владельца сертификата:

Организация:

Ключ ЭП создан с использованием СКЗИ:

Идентификатор ключа:

Местонахождение:

Хранилище ключевой информации:

Момент генерации ключа:

Открытый ключ:

Достоверность приведенных данных подтверждаем

Владелец сертификата

/ /

0

Отметка о принятии Банком

Дата

подпись

ФИО

Должность

Правила безопасного использования Системы дистанционного банковского обслуживания АО МС Банк Рус

После того, как Банк передал Вам средства доступа (логин / пароль и Носители) к Системе дистанционного банковского обслуживания АО МС Банк Рус (далее – «Система ДБО»), конфиденциальность данных полностью зависит от того, насколько ответственно Вы отнесётесь к их использованию и хранению.

Для снижения риска несанкционированного доступа к Системе ДБО необходимо соблюдать следующие меры предосторожности:

1. Обеспечить безопасность Носителей с Ключами ЭП, используемых в Системе ДБО:

1.1. Для хранения Ключей ЭП используются только Носитель. При этом владелец Носителя должен хранить его в условиях, исключающих доступ к нему третьих лиц (например, использовать для хранения личный сейф).

1.2. Извлекать Носители с Ключами ЭП из компьютера каждый раз после завершения их использования. Не допускать нахождение Носителей с Ключами ЭП:

- подключенными к компьютеру, если Вы их не используете;
- в открытом доступе (например, на столе) в тот момент, когда они не находятся в зоне прямой видимости. В случае необходимости отлучиться от рабочего места, поместите Носители с Ключами ЭП в защищённое место (например, в личный сейф).

1.3. Не передавать Ключи ЭП третьим лицам.

1.4. Пин-код Носителя должен быть известен только владельцу ключа ЭП.

1.4. Пин-код Носителя и пароль доступа к Системе ДБО следует помнить и вводить вручную, не запоминая его в компьютере. Допускается хранение пин-кода или пароля на листе бумаги (например, в сейфе), отдельно от Носителя.

1.5. Осуществлять ежегодную смену Ключей ЭП, используемых при работе с ЭСП.

2. Обеспечить безопасность доступа к системе дистанционного банковского обслуживания:

2.1. Не допускать использования простых паролей (123456, qwerty и др.), а использовать различные сложные комбинации из букв (в т.ч. в разных регистрах), цифр, не расположенных на клавиатуре последовательно, и специальных символов (!, @, ?, < и т.д.). Настоятельно рекомендуется использовать специализированные программы-генераторы паролей.

2.2. Осуществлять периодическую смену паролей (не реже, чем раз в 3 месяца), используемых в системе дистанционного банковского обслуживания.

2.3. Не назначать пароль, используемый при работе с Системой ДБО, в любых других системах и сервисах.

2.4. Не сообщать логин или пароль, используемый при работе с Системой ДБО, третьим лицам.

2.5. Незамедлительно изменить пароль и обратиться в Банк за повторной выдачей средств доступа следует в следующих случаях:

- при возникновении любых подозрений на компрометацию ключей и/или средств доступа;
- в случае обнаружения каких-либо вредоносных программ на компьютере, используемом для работы с Системой ДБО;
- при смене ответственных исполнителей, имеющих непосредственный доступ к Ключам ЭП.

Рекомендуем Вам незамедлительно обратиться в Банк в случае обнаружения отсутствия возможности подключения к Системе ДБО.

2.6. Не использовать функцию запоминания логина и пароля в браузерах.

3. Обеспечить безопасность компьютера, с которого осуществляется работа с ЭСП:

3.1. Применять только лицензионное программное обеспечение.

3.2. Использовать средства антивирусной защиты, обеспечивая при этом регулярное, не реже одного раза в день, обновление антивирусных баз, а также еженедельную полную антивирусную проверку.

3.3. Установить межсетевой экран. При этом межсетевой экран следует настроить таким образом, чтобы заблокировать входящие соединения. Разрешены должны быть только исходящие соединения с Банком и ограниченным числом сайтов сети Интернет для работы в Системе ДБО и проведения обновлений программного обеспечения.

3.4. Обеспечивать своевременную (по возможности, автоматическую) загрузку и установку всех последних обновлений операционных систем, а также регулярное обновление другого системного и прикладного программного обеспечения, в т.ч. браузеров, по мере появления новых версий, свободных от выявленных уязвимостей.

3.5. Исключать возможность посещения сайтов сети Интернет сомнительного содержания, загрузку и установку нелицензионного программного обеспечения.

3.6. Не использовать ссылки, указанные в подозрительных письмах, полученных по электронной почте, всегда вводить адрес через браузер. Одним из способов мошеннических действий является рассылка писем с указанием ссылок на поддельные Web-сайты, имеющие похожие адреса, к примеру, mcbankrus.ru вместо истинного mcbankrus.ru.

3.7. Осуществлять антивирусную проверку любых файлов и программ, загружаемых из сети Интернет.

3.8. На компьютере, предназначенном для работы с Системой ДБО, из числа съемных носителей информации следует использовать только Носители, а также использовать строго ограниченный перечень программного обеспечения, необходимый для работы с Системой ДБО.

3.9. Отключить «автоматическое выполнение» для подключаемых к компьютеру флеш-карт и компакт-дисков, поскольку значительная часть вредоносных программ распространяется именно этим способом.

3.10. Не допускать работу под учётной записью операционной системы, имеющей права администратора - использовать учётную запись с ограниченными правами.

3.11. Не допускать использования «пустых» или простых паролей (123456, qwerty и др.) для всех учётных записей, а также осуществлять периодическую смену паролей. Рекомендуется использовать пароли, содержащие не менее 12 символов.

3.12. Не использовать любые средства удалённого (дистанционного) доступа. Заблокировать возможность использования таких средств с помощью межсетевого экрана (программного и/или аппаратного).

3.13. Не запускать на компьютере программы, полученные из не заслуживающих доверия источников.

3.14. Обеспечить возможность доступа к компьютеру только уполномоченных лиц.

3.15. Ограничить передачу файлов и обмен сообщениями электронной почты на компьютере, используемом для работы с Системой ДБО.

3.16. Периодически контролировать целостность исполняемых файлов и файлов конфигураций.

3.17. Использовать решение для мониторинга и выявления киберугроз и оперативного реагирования на инциденты.

3.18. Исключить использование компьютера для личных целей пользователей, в том числе посещения развлекательных ресурсов, личной электронной почты или общения в мессенджерах.

4. Обращаем Ваше внимание:

1) АО МС Банк Рус не осуществляет рассылку электронных писем с просьбой прислать Ключи ЭП и/или пароль доступа к Системе ДБО и никогда не запрашивает у Вас эту информацию.

2) Рассылка программ (или ссылок на них) по электронной почте для установки на Вашем компьютере может осуществляться только службой поддержки клиентов и Системы ДБО Банка и только по предварительной договоренности с Вами.

3) Никогда не отвечайте на письма, запрашивающие конфиденциальную информацию.

Вы должны помнить, что Банк никогда не будет связываться с Вами по электронной почте с целью запроса каких-либо паролей, данных счетов, персональной информации. Вам следует удалять любые полученные сообщения, запрашивающие личную информацию или содержащие ссылку на Web-страницу, где Вам предлагается эти данные ввести. Вероятнее всего, такие сообщения являются мошенничеством.

4) При плановом длительном неиспользовании Системы ДБО следует блокировать возможность использования Системы ДБО до предоставления в Банк письма на бумажном носителе.

5) Рекомендуется осуществить разделение прав доступа в Систему ДБО между двумя разными изолированными друг от друга рабочими местами: например, на одном рабочем месте осуществляется ввод документов в систему и установка электронной подписи, а на другом месте, другим работником - проверка и отправка платежей в Банк. Такой подход существенно снижает риски, связанные с осуществлением операций без Вашего согласия.

6) Если Ваша организация эксплуатирует выделенный высокоскоростной канал доступа в сеть Интернет, рекомендуется ограничить диапазон ip-адресов, с которых разрешён доступ к ЭСП с использованием ключей, зарегистрированных для Вашей организации.

7) При неожиданном «зависании» компьютера в момент работы с Системой ДБО, с последующим полным отказом в работе, **СЛЕДУЕТ НЕЗАМЕДЛИТЕЛЬНО** позвонить в операционный отдел Банка и убедиться, что по Вашему счёту от Вашего имени не отправлен платёж.

8) Риск хищения и дальнейшего неправомерного использования Ключа ЭП и другой аутентификационной информации увеличивается при доступе к Системе ДБО с гостевых рабочих мест (интернет-кафе и т.д.). Осуществление подобного доступа, в т.ч. с целью просмотра данных, запрещено.

9) Банк рекомендует отслеживать информацию по вопросам информационной безопасности в связи с видоизменением способов мошеннических посягательств и информационных угроз.

Вам могут быть полезны следующие ресурсы:

- «Управление «К» предупреждает: будьте осторожны и внимательны!»:

http://mvd.ru/upload/site1/mvd/mvd2/mvd3/broshyura_k_01_02_20121.pdf

- «Вредоносные программы в интернете»: http://mvd.ru/upload/site1/mvd/mvd2/mvd3/liflets_out_1.pdf

- «Пользователям интернета»: http://mvd.ru/upload/site1/mvd1/liflets_out_3.pdf

- «Телефонные мошенники»: http://mvd.ru/upload/site1/mvd1/liflets_out_4.pdf

Регламент действий клиентов АО МС Банк Рус в случае несанкционированного доступа или попытки несанкционированного доступа в Систему ДБО

1. Общие положения

1.1. Реагирование Клиента АО МС Банк Рус на инциденты, возникающие при использовании Системы ДБО, включает в себя технические и организационные мероприятия, которые следует проводить параллельно друг с другом.

1.2. Сущностью технических мероприятий является немедленное обеспечение целостности данных, потенциально имеющих отношение к инциденту, путем отключения, упаковки и опечатывания, должного хранения соответствующих носителей информации.

1.3. Организационные мероприятия заключаются в уведомлении Банка, уведомление подразделений информационной безопасности (Банка и Клиента) о факте инцидента, о реквизитах переданных платежных поручений.

1.4. В целях проведения технических мероприятий Банк рекомендует привлекать независимого специалиста и лиц, не являющихся работниками Клиента. Независимый специалист должен обладать опытом реагирования на инциденты информационной безопасности.

При невозможности привлечения независимого специалиста, технические мероприятия могут быть проведены работниками Клиента, ответственными за обеспечение информационной безопасности или иными лицами, обладающими соответствующими знаниями (например, системными администраторами).

2. Технические мероприятия

2.1. Выявление автоматизированных рабочих мест (далее – АРМ), которые использовались для работы с Системой ДБО, и составление их перечня. В перечень следует также вносить АРМ, которые на момент инцидента были выключены.

2.2. Немедленное выключение работающих АРМ (из составленного перечня) методом принудительного прерывания электропитания в обход штатной процедуры завершения работы. Например, извлечь аккумуляторную батарею из ноутбука и отключить от кабелей информационных сетей (если было подключение).

2.3. Извлечение энергонезависимых носителей информации (жесткий диск, USB-накопители) из АРМ, на которых осуществлялась работа с Системой ДБО.

2.4. Упаковка и опечатывание энергонезависимых носителей информации.

2.5. Упаковка и опечатывание Носителей ключей, используемых для подписи платежных поручений.

2.6. Копирование журналов систем контроля доступа в помещения на территории Клиента, копирование видеопотока систем видеонаблюдения в офисе или офисном центре за максимально возможный промежуток времени. Запись соответствующих журналов и видеопотоков на компакт-диски, их упаковка и опечатывание.

2.7. Составление акта лицами, указанными в п. 1.4, в котором отражаются характеристики упакованных и опечатанных Носителей и иная значимая информация (по форме Приложения 12 к Правилам).

2.8. Передача упакованных и опечатанных Носителей информации на хранение в специальное помещение или сейф.

2.9. Сбор журналов межсетевых экранов, серверов баз данных и иных компонентов клиентского приложения электронного средства платежа, систем авторизации пользователей, АРМ, используемых для управления денежными средствами через Систему ДБО, устройств, которые могут использоваться для удаленного управления указанными АРМ.

2.10. Направление письменного заявления Интернет-провайдеру (по форме Приложения 13 к Правилам) для получения в электронной форме журналов соединений с Интернет с электронного устройства Клиента или из его локальной вычислительной сети как минимум за три месяца, предшествовавшие факту хищения денежных средств.

3. Организационные мероприятия

3.1. Незамедлительно сообщить в Банк на адрес dbosupport@mcbankrus.ru, а также по телефону (495) 287-04-80 о факте несанкционированной Клиентом передачи платежных поручений (с указанием их номеров, сумм, получателей, назначений платежей) и потребовать отмены указанных платежных поручений и аннулирования действующего сертификата КПЭП Клиента.

3.2. Обратиться в Банк с письменным заявлением о блокировании учетной записи и отзыве сертификата КПЭП, используемых при работе с Системой ДБО (по форме Приложения 14 к Правилам).

Копии вышеуказанных заявлений должны быть отправлены в Банк незамедлительно по электронной почте (скан-копии) на адрес: dbosupport@mcbankrus.ru, а оригиналы заявлений должны быть доставлены в Банк в течение одного рабочего дня.

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

3.4. В случае если на момент обращения в Банк платежное поручение уже было исполнено, в течение одного рабочего дня обратиться в Банк с письменным заявлением об отзыве платежа, возврате денежных средств (по форме Приложения 15 к Правилам).

3.5. Подготовить документы для правоохранительных органов (описание инцидента в письменной форме, договор на предоставление услуг по использованию Системы ДБО, договор на предоставление услуги доступа в сеть Интернет, копии несанкционированных платежных поручений, заявление о преступлении). Примерный перечень вопросов, на которые необходимо дать ответ при описании инцидента, приведен в Приложении 16 к Правилам.

Заявление о преступлении оформляется с учетом требований статьи 141 Уголовно-процессуального кодекса РФ и передается в орган МВД России для регистрации и последующей проверки. Обращаем Ваше внимание, что если заявление о преступлении подается при личном обращении заявителя, то ему выдается талон-уведомление (пункт 68 приложения к приказу МВД России от 01.03.2012 №140).

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

3.6. Копии вышеуказанных документов (Приложения 12-15 к Правилам), направить в Банк с приложением Справки по факту инцидента информационной безопасности, возникшего при использовании электронного средства платежа (по форме Приложения 17 к Правилам), а также подтверждающих документов (согласно перечню, указанному в Приложении 18 к Правилам).

4. Типовые ошибки при реагировании на инциденты, возникающие при использовании электронного средства платежа

Банк обращает Ваше внимание на то, что процесс реагирования на инциденты, возникающие при использовании Системы ДБО, должен исключить совершение следующих ошибок:

- антивирусная проверка файловых систем носителей информации АРМ, на которых работали с электронным средством платежа, после обнаружения инцидента. Проверка приводит к изменению временных меток файлов вредоносных программ, перемещению или удалению файлов вредоносных программ;
- переустановка операционных систем АРМ, на которых работали с электронным средством платежа, после обнаружения признаков инцидента. Переустановка приводит к удалению файлов вредоносных программ, следов их работы и усложняет расследование инцидента за счет необходимости восстановления данных;

- продолжение работы пользователей с АРМ, имеющими отношение к инциденту, после обнаружения инцидента; необоснованный перенос выключения АРМ на более поздний срок. Продолжение работы дает возможность злоумышленнику удалить следы несанкционированной активности;
- несвоевременное информирование Банка о факте несанкционированной передачи платежных поручений. Несвоевременное информирование приводит к исполнению платежных поручений, переданных злоумышленником, а также к возможности передачи новых платежных поручений без согласия Клиента;
- необоснованное отклонение от рекомендуемой последовательности действий, зафиксированной в настоящем приложении; медленное реагирование на инцидент, что приводит к снижению юридической значимости собираемых материалов, перезаписи криминалистически значимых данных.

Приложение № 12

к Правилам дистанционного банковского обслуживания АО МС Банк Рус

АКТ ОБ ИЗЪЯТИИ НОСИТЕЛЕЙ ИНФОРМАЦИИ

«__» _____ 20__ года в офисе _____,
(сокращенное наименование юр. лица)

расположенном по адресу: г. _____, ул. _____, д. _____, строение _____, в присутствии следующих лиц:

1. ФИО (генеральный директор _____)
2. ФИО (системный администратор _____)
3. ФИО (независимое лицо, привлеченное для удостоверения проводимых действий)
4. ФИО (независимое лицо, привлеченное для удостоверения проводимых действий) специалистом _____
ФИО

было произведено изъятие носителей информации и копирование их содержимого с целью дальнейшего исследования.

Были изъяты следующие носители информации:

1. накопитель _____ из компьютера _____
тип _____ накопителя идентификатор компьютера _____

производитель: «_____», модель: «_____», серийный номер: «_____», заявленная емкость: _____;

2. накопитель _____ из компьютера _____
тип _____ накопителя идентификатор компьютера _____

производитель: «_____», модель: «_____», серийный номер: «_____», заявленная емкость: _____;

Содержимое изъятых носителей информации было скопировано на накопитель на жестких магнитных дисках специалиста (производитель: «_____», модель: «_____», серийный номер: «_____», заявленная емкость: _____).

После копирования изъятые носители информации были упакованы и опечатаны способом, обеспечивающим невозможность доступа к носителю без видимого нарушения целостности упаковки.

Специалист _____ ФИО
(подпись)

Генеральный директор _____ ФИО
(подпись)

Системный администратор _____ ФИО
(подпись)

Независимое лицо _____ ФИО

(подпись)

Независимое лицо _____ ФИО

(подпись)

_____._____._____

Приложение № 13

к Правилам дистанционного банковского обслуживания АО МС Банк Рус

ФОРМА ПИСЬМА ИНТЕРНЕТ-ПРОВАЙДЕРУ О ПРЕДОСТАВЛЕНИИ ЖУРНАЛОВ СОЕДИНЕНИЙ (ЛОГОВ)

должность руководителя

наименование организации

ФИО

Уважаемый (ая) _____
имя, отчество руководителя

« ____ » _____ 20 ____ года в ____:____ по московскому времени со счета _____ с использованием Системы дистанционного банковского обслуживания АО МС Банк Рус («Система ДБО») был осуществлен несанкционированный перевод денежных средств. Компьютер, с которого осуществляется подключение к Системе ДБО, располагается по адресу _____ и использует IP-адрес _____. _____. _____. _____. _____.

Вероятной причиной несанкционированного перевода могло послужить заражение компьютера вредоносным программным обеспечением, кража логина, пароля и закрытых ключей Системы ДБО.

« ____ » _____ 20 ____ года между _____ и Вами был заключен договор № _____ об оказании _____ услуг.

Для выявления обстоятельств несанкционированного перевода прошу предоставить информацию из журналов (логов) о входящем и исходящем трафике за период с « ____ » _____ 20 ____ года по « ____ » _____ 20 ____ года с указанием времени соединения, IP адресов.

должность подпись

расшифровка подписи

« ____ » _____ 20 ____

Исп. _____
Фамилия И.О.

тел. _____

Приложение № 14

к Правилам дистанционного банковского обслуживания АО МС Банк Рус

ЗАЯВЛЕНИЕ О БЛОКИРОВАНИИ ДОСТУПА К СИСТЕМЕ ДИСТАНЦИОННОГО БАНКОВСКОГО ОБСЛУЖИВАНИЯ (Системе ДБО)

в АО МС Банк Рус

31 из 40

АО МС Банк Рус

ул. Обручева, д. 30/1 стр.2, Москва, 117485, Россия
Тел. +7 (495) 287-04 80

www.mcbankrus.ru

ОГРН 1027739094250 ИНН 7744001105 КПП 997950001

должность руководителя

Фамилия И.О.

1. Клиент: _____
наименование организации

Местонахождение Клиента: _____
адрес местонахождения организации

ИНН: _____ ОГРН: _____

Расчетный счет Клиента: _____

Представитель Клиента: _____
должность, Фамилия, Имя, Отчество представителя (указываются полностью)

действующий на основании _____
наименование документа – Устав, Доверенность (указываются номер доверенности и дата ее совершения), иной соответствующий документ

2. По причине _____ прошу Вас заблокировать
учетную запись в Системе ДБО, а также ключи электронной подписи следующих работников:

Должность, Ф.И.О. представителя Клиента (указываются полностью)	Логин в системе

Подпись Представителя Клиента: _____ Печать Клиента
Дата: _____ 20__ года

ОТМЕТКИ БАНКА:				
Электронный ключ: ☐ утрачен ☐ скомпрометирован ☐ имеются физические повреждения ☐ был использован без согласия Клиента				
Заявление принял и проверил: _____ / _____ / «____» _____ 20__ г.				
(должность работника Банка)	(Подпись)	(ФИО)	(Дата)	(Время)

Приложение № 15
к Правилам дистанционного банковского обслуживания АО МС Банк Рус

В АО МС БАНК РУС

ЗАЯВЛЕНИЕ ОБ ОТЗЫВЕ ПЛАТЕЖА, ВОЗВРАТЕ ДЕНЕЖНЫХ СРЕДСТВ И БЛОКИРОВАНИИ ДО-
СТУПА К СИСТЕМЕ ДИСТАНЦИОННОГО БАНКОВСКОГО ОБСЛУЖИВАНИЯ АО МС БАНК РУС

«___» _____ 20__ года с нашего расчетного счета

по Системе дистанционного банковского обслуживания АО МС Банк Рус были похищены денежные средства, которые, по имеющейся информации, были переведены со следующими реквизитами платежа:

Дата платежа: _____ Время _____
Номер платежного поручения: _____
Наименование банка плательщика: _____
Наименование плательщика: _____
ИНН плательщика: _____
Номер счета плательщика: _____
Наименование банка получателя: _____
Наименование получателя: _____
ИНН получателя: _____
Номер счета получателя: _____
Сумма платежа: _____
Назначение платежа: _____

Прошу Вас заблокировать нашу учетную запись в Системе дистанционного банковского обслуживания АО МС Банк Рус, провести процедуру компрометации всех ключей электронной подписи и оказать содействие в возврате денежных средств.

_____ должность подпись

_____ расшифровка подписи

«___» _____ 20__

Исп. _____
Фамилия И.О.

тел. _____

Отметки Банка:

Дата регистрации _____ Время регистрации _____

Зарегистрировал сотрудник Банка _____
(ФИО, должность)

ПРИМЕРНЫЙ ПЕРЕЧЕНЬ ВОПРОСОВ, НА КОТОРЫЕ НЕОБХОДИМО ДАТЬ ОТВЕТ ПРИ ОПИСАНИИ ИНЦИДЕНТА

1. Когда и как вы обнаружили передачу несанкционированных (мошеннических) платежных поручений?
2. Отображались ли вам какие-нибудь необычные сообщения при работе с электронным средством платежа непосредственно до инцидента (сообщения о технических работах, об ошибках)? Если да, то какие это были сообщения?
3. Замечали ли вы какие-нибудь необычные события при работе с компьютером непосредственно до инцидента (беспричинные движения курсора мыши, ввод текста, запуск программ)? Если да, то какие это были события?
4. Поступали ли вам звонки от лиц, представившихся работниками Банка, непосредственно до инцидента? Если да, то о чем вы говорили?
5. Какие носители ключей электронной подписи необходимы для корректного подписания платежного поручения? За какими лицами они закреплены?
6. Как организована работа с носителями ключей электронной подписи? Как и где они хранятся в нерабочее (ночное, обеденное) время? Какие лица имеют к ним доступ?
7. Принято ли в организации передавать свой ключ электронной подписи другому лицу?
8. Как организовано хранение резервных копий ключей электронной подписи? Какие лица имеют к ним доступ?
9. Какие действия производились с носителями ключей электронной подписи и их резервными копиями непосредственно до инцидента?
10. Применяется ли компьютер в целях, отличных от работы с электронным средством платежа? Если да, то в каких?
11. Как часто производится обновление программного обеспечения, установленного на компьютере? Когда было последнее обновление?
12. Какие антивирусные программы установлены на компьютере? Как часто они обновляются?
13. Какие программные межсетевые экраны установлены на компьютере? Какие правила сетевых взаимодействий они реализуют?
14. Какие программные средства удаленного (сетевого) управления установлены на компьютере? Для каких целей они используются?
15. Производилось ли антивирусное сканирование компьютера после обнаружения инцидента? Если да, то какие оно дало результаты?
16. Производилась ли переустановка операционной системы компьютера после обнаружения инцидента?
17. Как организован доступ организации в сеть интернет? Какие правила сетевых взаимодействий реализуются межсетевыми экранами? При ответе на этот вопрос желательно нарисовать карту сети.
18. Установлена ли в офисе система контроля и управления доступом в помещения? Если да, то ведет ли она журналы доступа?
20. Ведется ли в офисе или бизнес-центре видеонаблюдение? Как долго хранится видеоряд?

СПРАВКА ПО ФАКТУ ИНЦИДЕНТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ, ОБНАРУЖЕННОМ ПРИ ИСПОЛЬЗОВАНИИ СИСТЕМЫ ДИСТАНЦИОННОГО БАНКОВСКОГО ОБСЛУЖИВАНИЯ АО МС БАНК РУС

«__» _____ 20__ неустановленным лицом через Систему дистанционного банковского обслуживания АО МС Банк Рус была совершена несанкционированная операция по переводу денежных средств со следующими реквизитами:

Дата платежа: _____
Номер платежного поручения: _____
Наименование банка плательщика: _____
Наименование плательщика: _____
ИНН плательщика: _____
Номер счета плательщика: _____
Наименование банка получателя: _____
Наименование получателя: _____
ИНН получателя: _____
Номер счета получателя: _____
Сумма платежа: _____
Назначение платежа: _____

Дополнительно сообщая:

Количество автоматизированных рабочих мест (далее – АРМ), настроенных для доступа к Системе дистанционного банковского обслуживания АО МС Банк Рус (далее – Система ДБО):

_____.

Для доступа к Системе ДБО хотя бы раз использовались

- ☐ корпоративные АРМ
- ☐ личные АРМ
- ☐ АРМ, находящиеся в общественном пользовании

Периодичность смены пароля в Системе ДБО: _____

Применяемые элементы безопасности АРМ включают:

- ☐ используется только программное обеспечение для работы с Системой 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 АРМ используются только ключевые носители

тели

- ☐ передача файлов и обмен сообщениями электронной почты на АРМ ограничены
- ☐ целостность исполняемых файлов и файлов конфигураций контролируется с периодично-

стью _____

- ☐ используются средства сетевой защиты: _____
- ☐ на АРМ запрещены входящие соединения из сети Интернет
- ☐ с АРМ разрешены исходящие соединения с Банком и ограниченным числом сайтов сети

Интернет для проведения обновлений программного обеспечения, число разрешенных сайтов составляет _____

- ☐ обеспечивается возможность доступа к АРМ только уполномоченных лиц
- ☐ обеспечивается возможность доступа к ключевым носителям только уполномоченных лиц

Иная информация, имеющая отношение к инциденту: _____

Подтверждаю отсутствие у меня претензий к _____
наименование банка плательщика

подпись плательщика

☐ 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 _____

☐ 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.

Заявитель: _____/_____

Дата: _____/Телефон: _____

ПЕРЕЧЕНЬ ПОДТВЕРЖДАЮЩИХ ДОКУМЕНТОВ

1. Копия лицензии на операционную систему персонального компьютера (далее – ПК), на котором установлено электронное средство платежа.
2. Копия документов на приобретение операционной системы ПК.
3. Описание используемого программного обеспечения (далее – 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 платежного документа за предоставление доступа в сеть Интернет на повременной основе.
7. Копия заявления в правоохранительные органы.
8. Копия лицензии на антивирусное ПО.
9. Копия документов о приобретении антивирусного 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 – сведения о порядке хранения и использования ключевых носителей).

Приложение № 19
к Правилам дистанционного банковского обслуживания АО МС Банк Рус

ЗАЯВЛЕНИЕ^{*1}
на установление лимитов на исходящие платежи через систему ДБО
в АО МС Банк Рус № ____ от ____/____/20__ г.

Наименование Клиента (полное в соответствии с учредительными документами):

ИНН Клиента:

Просим установить ограничения/снять ранее установленные ограничения при переводах через систему ДБО (выбрать требуемое) по счету _____:

1. Ограничения по сумме переводов:

1.1. На сумму одной операции, не более _____ руб.	
☐ Установить лимит	☐ Отменить установленный лимит
1.2. На сумму всех операций в день , не более _____ руб.	
☐ Установить лимит	☐ Отменить установленный лимит

2. Ограничения по времени переводов (ежедневно):

2.1. Разрешить проведение операций в интервале с _____ ч. _____ мин. по _____ ч. _____ мин.	
☐ Установить ограничение	☐ Отменить ограничение

3. Установить идентификаторы устройств, с которых возможен вход в ДБО:

3.1. IP устройства _____ и ФИО подписанта _____	
☐ Установить ограничение	☐ Отменить установленное ограничение
3.2. IP устройства _____ и ФИО подписанта _____	
☐ Установить ограничение	☐ Отменить установленное ограничение
3.3. IP устройства _____ и ФИО подписанта _____	
☐ Установить ограничение	☐ Отменить установленное ограничение
3.4. IP устройства _____ и ФИО подписанта _____	
☐ Установить ограничение	☐ Установить ограничение

Подписи(-ь) уполномоченных(-ого) лиц(-а)
Клиента^{*2}

_____/_____
(подпись) (фамилия и инициалы)

^{*1} Каждое новое заявление отменяет ранее оформленное заявление.

^{*2} Заполняется в соответствии с карточкой с образцами подписей и оттиском печати.

на создание Единого окна ДБО для
Клиента и его обособленных подразделений

ИНН Клиента

ФНО

Перечень доступных обособленных подразделений:

Наименование обособленного подразделения	ИНН/КПП

_____/_____ / _____

Руководитель Подпись ФИО

« » 20 Г.

Отметки Банка

Заявление принято _____
(Дата) (Подпись) (ФИО и должность сотрудника, принявшего заявление)

Предоставить доступ к Системе ДБО

Председатель Правления _____ / _____ /

Приложение № 21

к Правилам дистанционного банковского обслуживания АО МС Банк Рус

Порядок взаимодействия Банка и Клиента с ИС «Одно окно»

Банк обеспечивает взаимодействие с ИС "Одно окно" в соответствии с Порядком взаимодействия банков, иных кредитных организаций с ИС «Одно окно» в сфере внешнеторговой деятельности, утверждённого приказом Министерства финансов Российской Федерации от 26.09.2022 №142н и действующим законодательством.

1. При получении через ИС «Одно окно» следующих видов сведений Банк направляет Клиенту уведомление через Систему ДБО до 18:00 текущего Операционного дня, если виды сведений были получены Банком до 18:00 этого дня либо не позднее следующего Операционного дня, если виды сведений были получены после 18:00 текущего Операционного дня:
 - 1) Получение информации, необходимой для перевода денежных средств, или информации о начислении;
 - 2) Получение информации, необходимой для перевода денежных средств с акцептом плательщика.
2. Клиент при получении уведомления от Банка, указанного в п.1 настоящего Порядка, самостоятельно создает расчетный документ в Системе ДБО, при этом уведомляет Банк по телефону или электронной почте о создании такого распоряжения.
3. По факту приема к исполнению распоряжений Клиента, указанных в п. 2 настоящего Порядка, Банк направляет в ИС «Одно окно» вид сведений «Получение информации о приеме к исполнению распоряжения о переводе денежных средств».
4. При необходимости Банк может проверить статус счета или актуальность распоряжения Клиента перед его исполнением путем направления в ИС «Одно окно» вида сведений «Получение запроса на предоставление информации».
5. При получении из ИС «Одно окно» вида сведений «Предоставление запроса на получение информации об исполнении» Банк направляет запрашиваемую информацию об исполнении распоряжения Клиента в форме уведомления об исполнении распоряжения или сообщение об ошибке до 18:00 текущего Операционного дня, если данный вид сведений был получен Банком до 18:00 этого дня, либо не позднее следующего Операционного дня, если данный вид сведений был получен Банком после 18:00 текущего Операционного дня.