

**ПРАВИЛА
ОКАЗАНИЯ УСЛУГ ДИСТАНЦИОННОГО БАНКОВСКОГО ОБСЛУЖИВАНИЯ
ЮРИДИЧЕСКИХ ЛИЦ, ИНДИВИДУАЛЬНЫХ ПРЕДПРИНИМАТЕЛЕЙ, ФИЗИЧЕСКИХ ЛИЦ,
ЗАНИМАЮЩИХСЯ В УСТАНОВЛЕННОМ ЗАКОНОДАТЕЛЬСТВОМ РОССИЙСКОЙ
ФЕДЕРАЦИИ ПОРЯДКЕ ЧАСТНОЙ ПРАКТИКОЙ, В СИСТЕМЕ ДБО
В ООО «ВАЙЛДБЕРРИЗ БАНК»**

1. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Указанные в настоящих Правилах оказания услуг дистанционного банковского обслуживания юридических лиц, индивидуальных предпринимателей, физических лиц, занимающихся в установленном законодательством Российской Федерации порядке частной практикой, в Системе ДБО в ООО «Вайлдберриз Банк» (далее – Правила) термины и определения с прописной (заглавной) буквы применяются в определении, содержащемся в разделе «Термины и определения» Договора КБО, если иное прямо не оговорено в тексте настоящих Правил, за исключением следующих терминов, имеющих указанное ниже значение:

Аутентификация – процедура проверки соответствия предъявленных аутентификационных данных Клиента и аутентификационных данных, находящихся в организации.

Авторизация – процесс подтверждения полномочий Клиента на использование Системы ДБО. Авторизация проводится Банком с использованием программно-аппаратных средств путем анализа и сопоставления введенных (предоставленных) Клиентом Аутентификационных данных со сведениями об аналогичных данных, имеющимися в Банке. По результатам Авторизации определяется наличие у Клиента прав доступа к каналам Системы ДБО.

Асимметричный алгоритм (RSA) — это криптографический алгоритм, в котором для шифрования и расшифровки используется криптографическая пара ключей ЭП. Один из двух ключей ЭП является открытым (основным) (public key), которым подписывается электронный документ. Второй ключ — закрытый ключ проверки (private key), связанный с открытым (основным) ключом, который предназначен для проверки подлинности ЭП при подписании электронных документов Клиентом.

Банк – Общество с ограниченной ответственностью «Вайлдберриз Банк» (ООО «Вайлдберриз Банк»), лицензия Банка России № 841 от 06.08.2021.

Вредоносный код - компьютерная программа, предназначенная для внедрения в автоматизированные системы, программное обеспечение, средства вычислительной техники, телекоммуникационное оборудование Банка и/или Клиента, приводящего к уничтожению, созданию, копированию, блокированию, модификации и (или) передаче информации, а также к созданию условий для такого уничтожения, создания, копирования, блокирования, модификации и (или) передачи.

ДКБО - договор комплексного банковского обслуживания юридических лиц, индивидуальных предпринимателей, физических лиц, занимающихся в установленном законодательством Российской Федерации порядке частной практикой, в ООО «Вайлдберриз Банк», в котором установлены условия и порядок предоставления Клиенту банковских продуктов и услуг.

Клиент - юридическое лицо (за исключением кредитных организаций), иностранная структура без образования юридического лица, индивидуальный предприниматель или физическое лицо, занимающееся в установленном законодательством Российской Федерации порядке частной практикой.

Компрометация - утрата/хищение средства подтверждения, любые признаки осуществления несанкционированных действий в Системе ДБО, а также случаи, когда нельзя достоверно установить, что произошло со средством подтверждения, паролем.

Ключ ЭП – уникальная последовательность символов известная Клиенту и предназначенная для создания в Электронном документе Электронной подписи с использованием Ключа ЭП, а также расшифровывания Электронных документов.

Логин – номер мобильного телефона, указанный в Заявлении о присоединении к ДКБО и, который регистрируется Банком в Системе ДБО и используется Клиентом для Аутентификации входа.

Номер мобильного телефона – номер мобильного телефона Клиента, предоставленный оператором сотовой связи и указанный Клиентом в Заявлении о присоединении к ДКБО или при

регистрации Клиента в Системе ДБО (либо измененный Клиентом в установленном порядке), используемый в качестве логина для входа в Систему ДБО.

Обращение - обращения Клиентов, связанные с деятельностью Банка, направленные посредством почтовой связи на юридический адрес Банка, представленные нарочно на бумажном носителе в офис Банка, а также направленные на адрес электронной почты (адрес: feedback@wb-bank.ru) или по Системе ДБО или по телефону: +8 800 600 6 006. Ответ на обращение по результатам его рассмотрения направляется Банком Клиенту в течение 15 рабочих дней со дня регистрации обращения (если иной срок не предусмотрен федеральными законами для отдельной категории обращений). В случае необходимости запроса дополнительных документов и материалов в целях объективного и всестороннего рассмотрения обращения Банк вправе продлить срок рассмотрения обращения, но не более чем на 10 рабочих дней, если иное не предусмотрено федеральными законами. В указанном случае, Банк направляет Клиенту соответствующее уведомление о продлении срока рассмотрения обращения.

Пароль - аутентификационная информация, генерируемая Клиентом самостоятельно в Системе ДБО с целью проведения Банком Аутентификации входа Клиента в Систему ДБО.

Разовый СМС-пароль – уникальный набор символов, используемый при регистрации Клиента в Системе ДБО, при подтверждении простого ЭД / группы простых ЭД, аутентификации клиента и совершения иных действий. Разовый СМС-пароль направляется Клиенту на Номер мобильного телефона путем направления СМС-сообщения/Push-сообщения. Разовый СМС-пароль имеет ограниченный срок действия, определяемый Системой ДБО.

Система дистанционного банковского обслуживания (далее – Система ДБО) - информационная система, включающая сервисы «Интернет-Банк» и «Мобильный банк» и представляющая собой совокупность программного, информационного и аппаратного обеспечения, реализующая электронный документооборот между Банком и Клиентом.

Средство подтверждения - электронное средство (в т.ч. мобильный телефон), используемое для подтверждения электронного документа разовым СМС-паролем. Использование средств подтверждения является наиболее эффективной мерой защиты платежных документов от несанкционированного доступа в Систему ДБО посторонних лиц.

СКЗИ - сертифицированное средство криптографической защиты информации «КриптоПро CSP»), имеющее действующий сертификат соответствия.

Участник Системы ДБО (Участник) – Клиент, а также уполномоченное должностное лицо Клиента, при их совместном упоминании.

Чат Системы ДБО/ Чат – программное обеспечение, интегрированное с Системой ДБО, позволяющее Клиенту, авторизованному в Системе ДБО дистанционно, с использованием текстового интерфейса обмениваться сообщениями, заявлениями и файлами с Банком в Системе ДБО. Обмен сообщениями в Чате осуществляется с Банком круглосуточно. История переписки между Банком и Клиентом сохраняется в Системе ДБО автоматически и может быть использована в качестве подтверждающего документа при рассмотрении спорных ситуаций, в том числе в суде. Сервис предоставляется при наличии технической возможности.

Электронный документ (далее – ЭД) - информация, представленная в электронной форме, содержащая финансовый документ (платежное распоряжение) или распоряжение по подключению, отключению или изменению предоставляемых Банком услуг в рамках расчетного обслуживания, информационное сообщение в системе, заявления, учредительные документы, финансовая отчетность и иные документы в электронной форме, предоставляемые в Банк. Электронные документы хранятся в электронных системах Системы ДБО и/или Банка.

Электронная подпись (далее – ЭП) - информация в электронной форме, присоединенная к другой информации в электронной форме (подписываемой информации) или иным образом связанная с такой информацией, и используемая для определения лица, подписывающего информацию.

В настоящих Правилах используется Усиленная неквалифицированная электронная подпись (УНЭП) и/или усиленная квалифицированная электронная подпись (УКЭП).

УНЭП – вид электронной подписи, признаваемая цифровым аналогом собственноручной подписи Клиента в соответствии с Соглашением об использовании электронной подписи Сторон, заключенным на основании оферты, размещенной на Сайте Банка и/или в Системе ДБО с целью электронного взаимодействия Клиента с Банком в соответствии с ч. 2 ст. 6 Федерального закона № 63-ФЗ¹, обмена информацией в электронной форме с использованием Системы ДБО Клиента, в том числе, но не ограничиваясь в целях заключения, изменения, исполнения, прекращения Договора КБО, а также в иных целях, оговоренных Соглашением об использовании электронной подписи, которая:

¹ Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи».

- создается Банком в результате криптографического преобразования информации криптографическая пара ключей ЭП, которая содержит открытый (основной) и закрытый ключ проверки электронной подписи (специальных компьютерных программ-криптопровайдеров). Владелец сертификата ключа проверки электронной подписи (далее - владелец ЭП) осуществляет проверку в программе-криптопровайдере или на веб-сервисе. Закрытая часть проверки ключа генерируется на стороне Клиента и использует асимметричный алгоритм (RSA);

- получена в результате криптографического преобразования информации с использованием ключа электронной подписи;

- позволяет определить лицо, подписавшее электронный документ;

- позволяет обнаружить факт внесения изменений в электронный документ после момента его подписания;

- создается с использованием средств электронной подписи.

УКЭП – вид электронной подписи, цифровой аналог собственноручной подписи Клиента, усиленная квалифицированная электронная подпись, создаваемая при помощи криптографического кода, регулируемая Федеральным законом № 63-ФЗ.

2. ОБЩИЕ ПОЛОЖЕНИЯ

2.1. Настоящие Правила оказания услуг дистанционного банковского обслуживания юридических лиц и индивидуальных предпринимателей в системе ДБО, в ООО «Вайлдберриз Банк» (далее – Правила) определяют условия и порядок использования Системы ДБО Клиентом, устанавливают порядок обмена документами между Клиентом и Банком, в которых информация представлена в электронной форме и заверена ЭП с помощью Системы ДБО. С использованием Системы ДБО Банк оказывает Клиенту услуги по дистанционному банковскому обслуживанию Счета(-ов) Клиента, открытого(-ых) в Банке, а также по обмену электронными документами между Клиентом и Банком.

2.2. Обслуживание Клиентов в Системе ДБО осуществляется Банком на основании заключенного Договора комплексного банковского обслуживания, надлежащим образом оформленного Заявления о присоединении к ДКБО (Приложение №3 к Договору) и настоящих Правил. Клиент присоединяется к настоящим Правилам в соответствии со ст. 428 Гражданского кодекса Российской Федерации путем подписания ЭП Заявления о присоединении к ДКБО.

2.3. Обязательным условием подключения Клиента к Системе ДБО является наличие у Клиента, открытого в Банке Счета.

2.4. Электронный документооборот по обмену ЭД между Банком и Клиентом осуществляется в порядке и на условиях, определенных настоящими Правилами и внутренними документами Банка.

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

2.6. Для обеспечения конфиденциальности ЭД при его передаче по открытым каналам связи, а также для обеспечения авторства и целостности ЭД в Системе ДБО используются программные средства защиты информации, реализующие алгоритмы шифрования, формирования и проверки ЭП. Целостность, авторство и конфиденциальность ЭД, подписанных ЭП, обеспечивается СКЗИ и соблюдением требований настоящих Правил.

2.7. На основании настоящих Правил с использованием Системы ДБО осуществляется обмен следующими ЭД:

- заявление о присоединении к ДКБО;

- распоряжение о переводе денежных средств со Счета в рублях;

- заявления (заявки) о предоставлении выписок и справок;

- документы и информация, которые связаны с проведением валютных операций;

- информационные сообщения Клиентов с приложенными к ним файлами, хранящиеся в виде записи в контрольных архивах Системы ДБО, или извлеченные из нее в виде отдельного файла, в том числе направленные через Чат Системы ДБО.

- заявления (заявки) о предоставлении, изменений условий и отключении банковских и небанковских продуктов/услуг, в том числе и кредитных продуктов;

- заявления (заявки) о расторжении ДКБО/о закрытии Счет и другие заявления в рамках ДКБО.

- документы свободного формата (запросы, тексты, сообщения свободного формата);

- прочие документы и приложения к ним, определенные заключенными сторонами договорами или соглашениями, в том числе и по кредитным продуктам.

Вышеуказанный перечень ЭД может изменяться Банком в одностороннем порядке с последующим информированием Клиента.

Направление Клиентом Банку иных видов ЭД может осуществляться после предварительного согласования с Банком.

2.8. Согласием Банка является, в т.ч. принятие электронного документа, содержащегося в письме, к исполнению. В целях реализации настоящих Правил Система ДБО является электронным средством платежа - средством, позволяющим Клиенту Банка 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.

2.9. Клиентская часть Системы ДБО может быть представлена Клиенту в виде доступа к Web-серверу Системы ДБО или в виде мобильного приложения для мобильного устройства на базе Android и iOS.

2.10. При работе в Системе ДБО Клиент использует одновременно и логин, и пароль.

2.11. Использование ЭП:

2.11.1. ЭП может быть использована Клиентом для подписания ЭД (нескольких связанных между собой ЭД), в т.ч. для подписания в электронной форме Заявления о присоединении к ДКБО доверенности о представлении интересов Клиента в целях открытия банковского счета, согласия на обработку персональных данных, соглашения об использовании электронной подписи, в целях проведения Банком идентификации Клиента, формирования Банком для Клиента финансовых предложений, принятия Банком решения о предоставлении Клиенту продуктов, заключения с Клиентом и дальнейшего сопровождения (исполнения) договоров и сделок.

2.11.2. ЭП удостоверяет факт формирования и подписания Клиентом документа в электронном виде посредством использования Клиентом ЭП. ЭП представляет собой сгенерированный Банком посредством Системы ДБО уникальный код последовательности символов.

2.11.3. Документы, подписанные Клиентом ЭП, признаются равнозначными документам на бумажном носителе, подписанными собственноручной подписью Клиента. На ЭД, подписанном ЭП, по усмотрению Банка может проставляться отметка о подписании документа ЭП. Вид и содержание такой отметки определяются Банком.

2.11.4. Проверка ЭП осуществляется Банком с использованием его программно-технических и иных средств путем установления факта ввода Клиентом ЭП, а также в порядке, предусмотренном Соглашением об использовании ЭП. В случае отрицательного результата проверки ЭП, Банк отказывает Клиенту в приеме к исполнению ЭД. Факт создания, подписания и направления Клиентом в Банк ЭД, а также проверка ЭП и иные действия Банка и Клиента фиксируются и хранятся Банком в электронных журналах. Выписка из электронных журналов и лог-файлы² являются достаточным и допустимым, в том числе для предоставления в государственные и судебные органы, а также иные организации при разрешении спорных ситуаций, доказательством направления Клиенту разовых СМС-паролей, подписания Клиентом ЭД с использованием ЭП, а также доказательством содержания ЭД.

2.11.5. Клиент несет ответственность за возможные отрицательные последствия в случае предоставления доступа к Системе ДБО и возможности подписывать электронные документы ЭП третьим лицам.

2.11.6. Подписанные Клиентом ЭП документы хранятся Банком в электронном виде и предоставляются Клиенту посредством Системы ДБО.

2.11.7. Алгоритм ЭП (одноразовый ключ ЭП) используется RSA, со сроком службы активной сессии Клиента в Системе ДБО. Одноразовый ключ ЭП создается/перевыпускается при авторизации Клиента в Системе ДБО, и удаляется после полного разлогирования и выхода Клиента из Системы ДБО.

2.11.8. Выпуск, передача и хранение ключа ЭП осуществляется на устройстве Клиента и непосредственно связан с активной сессией Клиента в Системе ДБО.

3. УСЛОВИЯ РАБОТЫ В СИСТЕМЕ

3.1. Подключение к Системе ДБО производится Клиентом самостоятельно при наличии доступа к сети Интернет, обеспечиваемого Клиентом, и собственного комплекта технического оборудования, удовлетворяющего требованиям Системы ДБО.

3.2. Банк на основании Заявления о присоединении к ДКБО предоставляет Клиенту доступ в Систему ДБО. Для входа в Систему ДБО Клиент использует логин - номер мобильного телефона и разовый СМС-пароль, который направляется отдельными СМС-сообщениями на номер мобильного телефона Клиента, указанный в Заявлении о присоединении к ДКБО. После первичного входа в Систему ДБО с использованием разового СМС-пароля Клиент устанавливает постоянный пароль для входа в Систему ДБО и использует его в дальнейшей работе.

² Отчеты, создаваемые программно-техническими средствами Банка, в которых зафиксированы действия и события, совершаемые Клиентом посредством Системы ДБО.

Банк при этом не несет ответственности за доставку СМС - сообщения Клиенту по причине возможных сбоев у мобильных операторов и в самой Системе ДБО. В случае неполучения разового СМС - пароля Клиент должен связаться с Контакт-центром Банка.

3.3. После осуществления входа в Систему ДБО (идентификация и аутентификация) для подписания всех электронных документов, отправляемых в Банк, Клиент использует ЭП и разовый СМС - пароль.

3.4. Участниками Системы ДБО могут быть только уполномоченные должностные лица Клиента, в отношении которых Банком проведена идентификация и установлены их полномочия в соответствии с Заявлением о присоединении к ДКБО.

3.5. При этом Банк не несет ответственности за доставку СМС-сообщения Участникам Системы ДБО по причине возможных сбоев у мобильных операторов и в самой Системе ДБО. В случае неполучения СМС-сообщения с логином и/или одноразовым паролем в течение 2 (Двух) рабочих дней с момента заключения ДКБО/подключения услуги, Клиент должен обратиться в Банк с обращением на адрес электронной почты (адрес: feedback@wb-bank.ru) или по телефону: +8 800 600 6 006.

3.6. Начало работы уполномоченного должностного лица Клиента в Системе ДБО осуществляется посредством ввода его логина и пароля в Систему ДБО.

3.7. Изменение/дополнение в составе уполномоченных должностных лиц Клиента и/или изменение номеров телефона уполномоченных должностных лиц Клиента, а также изменение номера телефона действующего уполномоченного должностного лица Клиента, или индивидуального предпринимателя, или физического лица, занимающегося в установленном законодательством Российской Федерации порядке частной практикой в Системе ДБО осуществляется путем оформления Заявления об изменении/дополнении прав доступа в Системе ДБО/о замене мобильного телефона в Системе ДБО ООО «Вайлдберриз Банк» по форме Приложения № 7.5 к настоящим Правилам (далее – Заявление).

Заявление в Банк направляется/предоставляется Клиентом/Представителем Клиента следующими способами:

- направление Заявления, подписанного ЭП Клиента/Представителя Клиента, по системе ДБО;
- направление Заявления, подписанного УКЭП Клиента/Представителя Клиента по электронной почте;
- предоставление Заявления, подписанного собственноручной подписью Клиента/Представителя Клиента на бумажном носителе в подразделение Банка.

3.8. Исполнение Заявления осуществляется в течение 1 (одного) рабочего дня с даты получения Банком Заявления.

3.9. Клиент, при работе с Системой ДБО, принимает на себя следующие обязательства, связанные с информационной безопасностью:

- использовать в работе только лицензионные версии операционных систем и прикладного программного обеспечения;
- применять и своевременно обновлять средства антивирусной защиты;
- своевременно устанавливать обновления безопасности для используемого программного обеспечения, в том числе мобильных приложений;
- не передавать логин/пароль/СМС третьим лицам, обеспечить сохранность указанных сведений;
- не использовать неизвестные/сомнительные Wi-Fi сети для подключения к сети Интернет;
- не передавать мобильное устройство, которое используется в качестве рабочего места для работы в Системе/ получения СМС, либо Средство подтверждения третьим лицам;
- активировать на мобильном устройстве, либо на Средстве подтверждения встроенное средство безопасности – пин-код, графический рисунок, отпечаток пальца либо фейс-айди.
- обеспечить непрерывное нахождение мобильного устройства под контролем уполномоченного лица Клиента.

3.10. Запрещается использование Системы ДБО в следующих случаях (включая, но не ограничиваясь):

- Клиентом не выполнены организационные меры для обеспечения безопасной работы в Системе ДБО;
- Клиент не обеспечил надежное хранение и защиту от компрометации средств, использующихся для дистанционного распоряжения счетом Клиента. К указанным средствам относятся мобильное устройство, пароль, зарегистрированный в Системе ДБО номер мобильного телефона, Средство подтверждения.
- Клиентом не обеспечен запрет использования на рабочем месте средств удаленного управления (R-Admin, TeamViewer и аналоги), администрирования и модификации ОС и её настроек (службы терминалов, удаленных рабочих столов и аналоги);
- Клиент не настроил канал оповещения о совершенных операциях (для мобильных приложений).

3.11. Клиент уведомлен и согласен, что при использовании Системы ДБО он несет повышенные риски, связанные с несанкционированным списанием средств Клиента неуполномоченными лицами, в том числе и с использованием Вредоносного кода. Начиная работать с Системой ДБО, Клиент подтверждает, что он полностью принимает на себя указанные риски.

3.12. Клиент несет полную ответственность за действия, совершенные третьими лицами, в случае передачи Клиентом средств, использующихся для дистанционного распоряжения счетом Клиента указанным лицам и/или в случае создания Клиентом условий для несанкционированного использования третьими лицами средств, использующихся для дистанционного распоряжения счетом Клиента. Клиент также несет полную ответственность за ущерб, причиненный Банку, указанными действиями или бездействием.

3.13. Клиент согласен с использованием логов (журналов) Системы ДБО и журналов модуля Системы ДБО по детектированию вредоносного программного обеспечения в качестве доказательства при разбирательстве по факту нарушений настоящих Правил и организационных мер для обеспечения безопасной работы в Системе ДБО.

4. ПОРЯДОК ОБМЕНА СООБЩЕНИЯМИ ПОСРЕДСТВОМ ЧАТА СИСТЕМЫ ДБО

4.1. Клиент, авторизованный в Системе ДБО, посредством Чата имеет техническую возможность дистанционно, с использованием текстового интерфейса обмениваться текстовыми сообщениями, Обращениями, заявлениями и файлами с Банком в Системе ДБО по вопросам, касающимся порядка предоставления банковских продуктов (услуг), направлять в Банк заявления на изменение условий обслуживания по продуктам (услугам) / подключение и отключение продуктов (услуг), а также направлять файлы документов, в рамках обновления сведений..

4.2. Обмен информационными сообщениями в Чате в рамках ДКБО является юридически значимым документооборотом. Такие информационные сообщения Банк и Клиент (далее при совместном упоминании — Стороны) признают составленными в письменной форме. Сообщения, направленные через Чат в рамках ДКБО, признаются сообщениями, содержащими волеизъявление отправившей Стороны на установление, изменение или прекращение правоотношений Сторон в рамках ДКБО. Стороны признают получение такого сообщения юридическим фактом. Сообщения Клиента должны подписываться Электронной подписью уполномоченного лица Клиента в случаях, когда подписание таких сообщений является требованием норм законодательства Российской Федерации, правил Банка, а также условий ДКБО. Стороны согласились, что электронные документы Сторон в рамках ДКБО признаются электронными документами, подписанными ЭП, и являются равнозначными документам на бумажных носителях, подписанным собственноручной подписью уполномоченного лица Клиента. Электронный документ, отправленный Клиентом в Банк с заявленных Клиентом электронных контактных данных, считается направленным от уполномоченных лиц Клиента, создающих и/или использующих ключ ЭП.

4.3. Банк не несет ответственности в случае отказа Клиента от получения/просмотра информационных сообщений в Чате. Риск неполучения Клиентом информационного сообщения, включая запрос, предписание, требование и иного документа, направленного Банком через Чат в рамках ДКБО, несет Клиент, включая правовые последствия, связанные с неисполнением направленного Банком информационного сообщения, включая запросы, предписания, требования и иные документы.

4.4. Сообщения, предложения, документы, уведомления и любая информация от Банка считаются доставленными Клиенту с момента их направления или размещения посредством Чата.

4.5. Клиент и Банк обязаны вести переписку в Чате, соблюдая общепринятые морально-этические нормы общения, без использования оскорблений, нецензурных выражений, непристойных фраз и бранных слов. Не допускается в переписке намеренное или по неосторожности унижение чести и достоинства собеседника.

4.6. Системой ДБО осуществляется автоматическое сохранение всей истории переписки с Клиентом в Чате. История переписок в Чате предоставляется Банком в качестве подтверждающего документа при рассмотрении спорных ситуаций, в том числе в суде.

5. БЛОКИРОВКА/РАЗБЛОКИРОВКА СИСТЕМЫ ДБО

5.1. Блокировка Системы ДБО представляет собой процедуру установления ограничений на совершение операций в Системе ДБО.

5.2. По инициативе Клиента Банк производит блокировку Системы ДБО в следующих случаях:

- в случаях компрометации личного кабинета Системы ДБО;
- в иных случаях по усмотрению Клиента.

5.3. Блокировка Системы ДБО по инициативе Клиента осуществляется после успешного прохождения Клиентом Авторизации/Аутентификации на основании запроса на блокировку, оформленного Клиентом через каналы Системы ДБО, Службу поддержки.

5.4. Разблокировка Системы ДБО по инициативе Клиента осуществляется после успешного прохождения Клиентом Авторизации.

Разблокировка Системы ДБО осуществляется Банком по истечении 24 часов с момента ее блокировки, если в Банк не поступит от Клиента заявление о совершении операции без его добровольного согласия.

Разблокировка Системы ДБО осуществляется Клиентом самостоятельно путем повторной Авторизации с использованием приложения мобильного банка.

5.5. Банк вправе в одностороннем порядке заблокировать доступ к каналам Системы ДБО или ограничить Клиента в использовании Системы ДБО (для совершения операций) до выяснения причин, в следующих случаях:

- при наличии у Банка подозрений компрометации Системы ДБО;
- в случае нарушения Клиентом условий ДКБО и настоящих Правил или предоставления Банку недостоверной информации;
- при наличии у Банка информации о вероятных или действительных противозаконных операциях или операциях, которые могут повлечь за собой ущерб для Банка или Клиента;
- в случае наличия нестандартных или необычно сложных схем проведения операций, отличающихся от обычного порядка операций, характерных для клиентов, пользующихся Системой ДБО;
- при выполнении Банком требований Федерального закона от 07.08.2001 № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» (далее - Федеральный закон № 115-ФЗ), Федерального закона от 10.12.2003 № 173-ФЗ «О валютном регулировании и валютном контроле» (далее - Федеральный закон № 173-ФЗ), Федерального закона от 27.06.2011 № 161-ФЗ «О национальной платежной системе» (далее - Федеральный закон № 161-ФЗ); Федерального закона от 26.10.2002 № 127-ФЗ «О несостоятельности (банкротстве)» (далее - Федеральный закон № 127-ФЗ);
- в иных случаях, предусмотренных законодательством Российской Федерации и нормативными правовыми актами.

5.6. Банк информирует Клиента о блокировке доступа к Системе ДБО с указанием причин блокировки в день установления такой блокировки путем размещения информации в приложении мобильного банка и/или путем направления Клиенту Push-уведомления.

5.7. В случае блокировки доступа в Систему ДБО по инициативе Банка установлены следующие сроки блокирования в зависимости от основания блокирования:

- до момента полного устранения Клиентом допущенных им нарушений порядка использования Системы ДБО;
- до момента рассмотрения Банком, предоставленных Клиентом разъяснений и документов о совершаемой операции, затребованных Банком;
- до момента принятия Банком решения по последствиям выявленных фактов несанкционированного доступа, но не более 3 (Трех) месяцев с даты блокирования Системы ДБО;
- либо на срок, установленный законодательством Российской Федерации и нормативными правовыми актами.

5.8. Заблокированные по решению Банка, доступ в Системы ДБО могут быть разблокированы по инициативе Банка, после устранения нарушений порядка использования Системы ДБО или иных обстоятельств, повлекших блокировку.

5.9. В случае выявления Банком операции, соответствующей установленным Банком России признакам осуществления перевода денежных средств без добровольного согласия Клиента, а именно без согласия Клиента или с согласия Клиента, полученного под влиянием обмана или при злоупотреблении доверием (далее при совместном упоминании - перевод денежных средств без добровольного согласия Клиента) до момента списания денежных средств, Банк приостанавливает прием к исполнению распоряжения о переводе денежных средств Клиента на 2 (два) дня и осуществляет блокировку доступа в Систему ДБО с уведомлением Клиента в день такой блокировки с указанием причины путем направления СМС-сообщения или Push-уведомления.

Банк обязан осуществить проверку наличия признаков осуществления перевода денежных средств без добровольного согласия Клиента, до момента списания денежных средств Клиента (за исключением операции с использованием платежных карт, перевода электронных денежных средств или перевода денежных средств с использованием СБП) либо при приеме к исполнению распоряжения клиента (при осуществлении перевода денежных средств в иных случаях).

Проверка наличия признаков осуществления перевода денежных средств без добровольного согласия Клиента осуществляется с учетом информации, полученной от оператора по переводу денежных средств, обслуживающего получателя средств, при выявлении операции, соответствующей признакам осуществления перевода денежных средств без добровольного согласия Клиента, если это предусмотрено правилами платежной системы, в рамках которой осуществляется перевод денежных средств, оператору по переводу денежных средств, обслуживающему плательщика, о такой операции в рамках реализации мероприятий по противодействию осуществлению переводов денежных средств без добровольного согласия Клиента.

Банк при выявлении им операции, соответствующей признакам осуществления перевода денежных средств без добровольного согласия Клиента (за исключением операции с использованием платежных карт, перевода электронных денежных средств или перевода денежных средств с использованием СБП), приостанавливает прием к исполнению распоряжения Клиента на 2 (Два) дня и осуществляет блокировку доступа в Систему ДБО с уведомлением Клиента в день такой блокировки с указанием причины путем направления СМС-сообщения или Push-уведомления. Банк при выявлении им операции с использованием платежных карт, перевода электронных денежных средств или перевода денежных средств с использованием СБП, соответствующих признакам осуществления перевода денежных средств без добровольного согласия Клиента, отказывает в совершении соответствующей операции (перевода).

5.10. Банк информирует Клиента:

- о приостановлении исполнения распоряжения о совершении операции, соответствующей признакам осуществления перевода денежных средств без добровольного согласия Клиента;

- о рекомендациях по снижению рисков повторного осуществления перевода без добровольного согласия Клиента и незамедлительно запрашивает у Клиента подтверждение возобновления исполнения распоряжения;

- о возможности Клиента подтвердить распоряжение не позднее 1 (Одного) дня, следующего за днем приостановления Банком приема к исполнению указанного распоряжения, способами, предусмотренными настоящими Правилами или о возможности совершения Клиентом повторной операции, содержащей те же реквизиты получателя (плательщика) и ту же сумму перевода (далее – повторная операция), способами, предусмотренными настоящими Правилами, в случае отказа Банка в совершении Клиентом операции с использованием платежных карт, перевода электронных денежных средств или перевода денежных средств с использованием СБП платежной системы Банка России.

5.11. Банк при предоставлении Клиенту информации в соответствии с п. 5.10 настоящих Правил вправе в дополнение к подтверждению Клиента запросить у Клиента информацию, что перевод денежных средств не является переводом денежных средств без добровольного согласия Клиента, и (или) направить Клиенту информацию о необходимости совершить повторную операцию способом, который предусмотрен настоящими Правилами.

5.12. При получении от Клиента подтверждения распоряжения или осуществлении действий по совершению Клиентом повторной

операции Банк обязан разблокировать доступ в Систему ДБО и незамедлительно принять к исполнению подтвержденное распоряжение Клиента или совершить повторную операцию, при отсутствии иных установленных законодательством Российской Федерации оснований не принимать распоряжение Клиента к исполнению.

5.13. При неполучении от Клиента подтверждения распоряжения и (или) запрошенной Банком информации, указанное распоряжение считается не принятым к исполнению, а при осуществлении действий по совершению Клиентом повторной операции способом, не предусмотренным настоящими Правилами, повторная операция считается несовершенной.

5.14. В случае, если, несмотря на направление Клиентом подтверждения распоряжения или осуществление действий по совершению повторной операции, Банк получил от Банка России информацию, содержащуюся в базе данных о случаях и попытках осуществления переводов денежных средств без добровольного согласия Клиента, Банк приостанавливает прием к исполнению подтвержденного распоряжения Клиента на 2 (Два) дня со дня направления Клиентом подтверждения распоряжения или отказывает в совершении Клиентом повторной операции. Банк незамедлительно уведомляет Клиента о приостановлении приема к исполнению подтвержденного распоряжения Клиента или об отказе в совершении Клиентом повторной операции с указанием причины такого приостановления (отказа) и срока такого приостановления, а также о возможности совершения Клиентом последующей повторной операции.

5.15. В случае приостановления приема к исполнению подтвержденного распоряжения Клиента в соответствии с п. 5.14 настоящих

Правил по истечении 2 (Двух) дней со дня направления Клиентом подтверждения распоряжения Банк обязан незамедлительно принять к исполнению подтвержденное распоряжение Клиента при

отсутствии иных установленных законодательством Российской Федерации оснований не принимать подтвержденное распоряжение Клиента к исполнению. В случае отказа в совершении Клиентом повторной операции по истечении 2 (Двух) дней со дня осуществления действий по совершению Клиентом повторной операции Банк обязан совершить последующую повторную операцию Клиента при отсутствии иных установленных законодательством Российской Федерации оснований не совершать последующую повторную операцию Клиента.

5.16. В случае, если Банк получил от Банка России информацию, содержащуюся в базе данных о случаях и попытках осуществления переводов денежных средств без добровольного согласия Клиента, и после получения от Банка России указанной информации исполняет распоряжение Клиента об осуществлении перевода денежных средств или совершает операцию с использованием платежных карт, перевод электронных денежных средств или перевод денежных средств с использованием СБП, соответствующие признакам осуществления перевода денежных средств без добровольного согласия Клиента, Банк обязан возместить Клиенту сумму перевода денежных средств или операции с использованием платежных карт, перевода электронных денежных средств или перевода денежных средств с использованием СБП без добровольного согласия Клиента в течение 30 (тридцати) дней, следующих за днем получения соответствующего заявления Клиента.

5.17. В случае, если Банк получил от Банка России информацию, содержащуюся в базе данных о случаях и попытках осуществления переводов денежных средств без добровольного согласия Клиента, которая содержит сведения, относящиеся к Клиенту и (или) его электронному средству платежа (далее – ЭСП), и если отсутствуют сведения федерального органа исполнительной власти в сфере внутренних дел о совершенных противоправных действиях, получаемые Банком в соответствии с Федеральным законом от 27.06.2011 № 161-ФЗ, Банк в рамках реализуемой им системы управления рисками и в порядке, предусмотренном настоящими Правилами, вправе приостановить использование Клиентом ЭСП на период нахождения сведений, относящихся к Клиенту и (или) его ЭСП, в базе данных о случаях и попытках осуществления переводов денежных средств без добровольного согласия клиента. В случае, если использование Клиентом ЭСП не было приостановлено в соответствии с настоящей частью Правил, в период нахождения сведений, относящихся к Клиенту и (или) его ЭСП, в базе данных о случаях и попытках осуществления переводов денежных средств без добровольного согласия клиента Банк осуществляет переводы денежных средств с использованием ЭСП по распоряжению Клиента - физического лица в пользу получателей - физических лиц на сумму не более 100 тысяч рублей в месяц.

5.18. Банк обязан приостановить использование Клиентом ЭСП, 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 и (или) его ЭСП, в том числе сведения федерального органа исполнительной власти в сфере внутренних дел о совершенных противоправных действиях, на период нахождения указанных сведений в базе данных о случаях и попытках осуществления переводов денежных средств без добровольного согласия Клиента.

5.19. После приостановления использования Клиентом ЭСП Банк незамедлительно уведомляет Клиента о приостановлении использования ЭСП, а также о праве Клиента подать в порядке, установленном Банком России, заявление в Банк России, в том числе через Банк, об исключении сведений, относящихся к Клиенту и (или) его ЭСП, в том числе сведений федерального органа исполнительной власти в сфере внутренних дел о совершенных противоправных действиях, из базы данных о случаях и попытках осуществления переводов денежных средств без добровольного согласия Клиента.

5.20. В случае наличия у Банка оснований полагать, что включение сведений, относящихся к Клиенту и (или) его ЭСП, в базу данных о случаях и попытках осуществления переводов денежных средств без добровольного согласия Клиента является необоснованным, Банк вправе самостоятельно (без участия Клиента) направить в Банк России мотивированное заявление об исключении сведений, относящихся к Клиенту и (или) его ЭСП, в том числе сведений федерального органа исполнительной власти в сфере внутренних дел о совершенных противоправных действиях, из базы данных о случаях и попытках осуществления переводов денежных средств без добровольного согласия Клиента.

5.21. В случае получения в порядке, установленном Банком России, информации об исключении сведений, относящихся к Клиенту и (или) его ЭСП, из базы данных о случаях и попытках осуществления переводов денежных средств без добровольного согласия Клиента Банк незамедлительно возобновляет исполнение распоряжения Клиента и незамедлительно уведомляет Клиента о возможности исполнения ЭСП при отсутствии иных оснований для приостановления исполнения ЭСП Клиента в соответствии с законодательством Российской Федерации или настоящими Правилами.

6. СОГЛАШЕНИЯ СТОРОН

- 6.1. Для подписания ЭД стороны используют ЭП. Стороны признают, что применяемая в Системе ДБО защита информации, обеспечивающая шифрование, контроль целостности и создание ЭП, достаточна для защиты информации от несанкционированного доступа, подтверждения подлинности и авторства ЭД.
- 6.2. Клиент (представитель Клиента), создающий электронный документ в Системе ДБО и подписывающий такой электронный документ ЭП, определяется как лицо, авторизованное и идентифицированное Системой ДБО.
- 6.3. При работе в Системе ДБО разовый СМС-пароль генерируется Системой ДБО в момент подтверждения Клиентом факта отправки документа в Банк и отправляется Клиенту посредством СМС-сообщения на номер мобильного телефона Клиента, указанный в Заявлении о присоединении к ДБО.
- 6.4. Электронные документы, подтвержденные ЭП, считаются переданными Клиентом, и в случае доставки их в Банк, полученными Банком, а соответствующая операция подлежит исполнению и выполняется Банком от имени и по поручению Клиента, если Системой ДБО подтверждена передача.
- 6.5. Стороны договорились считать, что Клиент отказался от передачи электронного документа до его отправки в Банк, если он не подтвердил правильность ввода информации ЭП.
- 6.6. Электронные документы, заверенные ЭП Клиента, юридически эквивалентны соответствующим документам на бумажном носителе, подписанным лицом, которому предоставлено право распоряжаться денежными средствами на счете Клиента и имеющим оттиск печати Клиента (при наличии), обладают юридической силой и подтверждают наличие правовых отношений между Сторонами. Электронные документы без ЭП Клиента не имеют юридической силы, Банком не рассматриваются и не исполняются.
- 6.7. Электронные документы с ЭП Клиента, создаваемые Клиентом в Системе ДБО и полученные Банком, являются доказательным материалом для решения спорных вопросов в соответствии с «Положением о процедуре разбора конфликтной ситуации в рамках использования Системы ДБО» в ООО Вайлдберриз Банк» (Приложение № 7.1 к настоящим Правилам).
- 6.8. Электронные документы, принятые Банком по окончании операционного времени, исполняются на следующий рабочий день Банка.
- 6.9. При наличии технической возможности по заявлению Клиента в Системе ДБО могут быть установлены ежедневные лимиты на проведение операций по Системе ДБО. Заявление составляется по форме Приложения № 7.2 к настоящим Правилам.
- 6.10. Стороны признают в качестве единой шкалы времени при работе с Системой ДБО московское поясное время. Контрольным является время системных часов Системы ДБО.
- 6.11. Стороны признают, что подделка разового СМС-пароля, пароля, ключа ЭП, то есть подтверждение ЭД от имени Клиента, невозможна без владения соответствующим Средством подтверждения.
- 6.12. Стороны признают, что возможность воспроизведения в электронном виде принятого к исполнению и исполненного Банком платежного распоряжения Клиента с отметками Банка осуществляется с использованием Системы ДБО.
- 6.13. Стороны признают надлежащим уведомление Клиента о совершенных операциях в Системе ДБО посредством направления уведомлений одним из способов:
- 6.13.1. Путем отправки СМС-сообщения/ Push-сообщений на номер мобильного телефона Клиента, указанный Клиентом в Заявлении о присоединении к ДКБО. Обязанность Банка по информированию Клиента считается исполненной Банком с момента отправки Банком СМС-сообщения/Push-сообщений на номер мобильного телефона Клиента. Банк не несет ответственности в случае несвоевременного уведомления Банка Клиентом об изменении номеров телефонов, в том числе используемых для получения СМС-сообщений/Push-сообщений, а также за действия или бездействие третьих лиц, влияющих на время и возможность получения Клиентом уведомлений от Банка о совершении операции по счету Клиента.
- 6.13.2. Путем изменения статуса соответствующего электронного документа в Системе ДБО. Присвоение электронному документу в Системе ДБО статуса «Отправлен в банк» подтверждает, что документ отправлен в Банк, но еще не получен. Присвоение электронному документу в Системе ДБО статуса «Принят Банком» подтверждает прием Банком распоряжения Клиента к исполнению. Присвоение электронному документу статуса «Исполнен» подтверждает исполнение Банком распоряжения Клиента. Присвоение электронному документу статуса «В картотеке» подтверждает помещение распоряжения в картотеку документов Клиента. Присвоение электронному документу статуса «Возвращен» подтверждает аннулирование Банком распоряжения Клиента. Уведомление считается полученным Клиентом с момента изменения статуса ЭД в Системе ДБО.
- 6.13.3. Путем направления выписки по банковскому счету Клиента. Уведомление считается полученным Клиентом с момента отправки Банком выписки в Систему ДБО.

6.13.4. Банк обязан проинформировать Клиента о совершенных операциях в Системе ДБО не позднее дня, следующего за днем исполнения соответствующей операции.

7. ПРАВА И ОБЯЗАННОСТИ КЛИЕНТА

7.1. Клиент вправе:

7.1.1. В любой момент прекратить действие Средства подтверждения, направив уведомление по форме Приложения № 7.3 к настоящим Правилам.

7.1.2. Приостановить/прекратить использовать Систему ДБО, направив уведомление по форме Приложения № 7.3 к настоящим Правилам.

7.1.3. Обращаться за получением консультаций, связанных с обслуживанием Клиента, а также эксплуатацией Системы ДБО.

7.1.4. Получать от Банка всю публичную финансовую информацию о деятельности Банка, а также направлять Банку письменные запросы, Обращения и получать на них ответы по Системе ДБО, а также в порядке, установленном законодательством Российской Федерации и Договором КБО.

7.2. Клиент обязан:

7.2.1. Использовать только лицензионные операционные системы, поддерживаемые компанией производителем, для работы в Системе ДБО.

7.2.2. Обеспечивать информационную безопасность рабочих мест и мобильных устройств ответственных сотрудников, уполномоченных использовать Систему ДБО для взаимодействия с Банком. Клиент обязан исключить или максимально ограничить доступ к этим рабочим местам лиц, чья деятельность не связана с осуществлением электронного документооборота с Банком.

7.2.3. Ознакомиться с описанием механизмов защиты Системы ДБО и требованиями по обеспечению информационной безопасности своего рабочего места и соблюдать их (Приложение № 7.4 к настоящим Правилам).

7.2.4. Заполнять ЭД в Системе ДБО в соответствии с требованиями действующего законодательства РФ.

7.2.5. Хранить в секрете логин и пароль, не предоставлять непосредственный или удаленный доступ к Средству подтверждения, используемому в Системе ДБО, а также обеспечить их защиту от использования третьими лицами.

7.2.6. Обеспечивать использование логина, пароля, СМС-сообщения только их владельцами в соответствии с установленными правами подписи.

7.2.7. В случае изменения информации для связи своевременно предоставить Банку обновленную информацию. Обязанность Банка по направлению Клиенту уведомлений считается исполненной при направлении уведомления в соответствии с имеющейся у Банка информацией для связи.

7.2.8. В случае компрометации логина/пароля или Средства подтверждения Клиент обязан незамедлительно проинформировать Банк путем направления соответствующего сообщения на эл. адрес: feedback@wb-bank.ru или по телефону: +8 800 600 6 006.

7.2.9. Исполнять обязательства, возникшие до момента приостановления или прекращения использования Клиентом Системы ДБО.

8. ПРАВА И ОБЯЗАННОСТИ БАНКА

8.1. Банк вправе:

8.1.1. По своему усмотрению блокировать/ограничивать доступ к Системе ДБО, предварительно уведомив об этом Клиента.

8.1.2. В любое время потребовать от Клиента сменить пароль в целях защиты информации.

8.1.3. Заблокировать логин Клиента в случае отказа Клиента от использования СМС-подтверждения платежей, либо при наличии обоснованных подозрений в Компрометации.

8.1.4. Не производить исполнение полученных от Клиента ЭД при наличии обоснованных подозрений в нарушении Клиентом действующего законодательства РФ. Банк обязан незамедлительно, но не позднее 24 (Двадцати четырех) часов, любым способом сообщить Клиенту о возникновении подобных подозрений.

8.1.5. Приостановить использование Клиентом Системы ДБО до получения от Клиента достоверной информации в случае нарушения Клиентом обязанности по предоставлении Банку достоверной информации для связи с Клиентом или обновленной информации в случае ее изменения. При этом Банк прекращает обработку всех ЭД, полученных от Клиента и не исполненных до момента блокировки.

8.1.6. Не возмещать Клиенту сумму операции, совершенной без согласия Клиента, в случаях, когда: Банк исполнил обязанность по информированию Клиента о совершенной операции и/или Клиент не направил Банку уведомление о Компрометации.

8.1.7. В одностороннем порядке приостановить до момента устранения неисправности использование Системы ДБО Клиентом в случае возникновения технических неисправностей или других обстоятельств, препятствующих использованию Клиентом Системы ДБО.

8.1.8. При непогашении Клиентом задолженности перед Банком, Банк имеет право:

- ограничить перечень услуг, предоставляемых Системой ДБО;
- приостановить оказание услуг ДБО;
- прекратить оказание услуг ДБО.

8.1.9. После предварительного уведомления Клиента приостанавливать использование Системы ДБО при несоблюдении Клиентом настоящих Правил, а также в рамках исполнения рекомендаций/требований Банка России, норм действующего законодательства РФ, в том числе, в области противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансирования терроризма. Уведомление в форме электронного сообщения по Системе ДБО направляется Банком Клиенту в момент блокировки с указанием документов/информации, которой необходимо представить в Банк.

8.1.10. По своему усмотрению производить учет (логгирование) действий Клиента с целью их контроля и, при необходимости, для разрешения любых конфликтных ситуаций в соответствии, но не ограничиваясь положениями Приложения № 7.1 к настоящим Правилам.

8.2. Банк обязан:

8.2.1. Производить регистрацию Клиента в Системе ДБО в течение 1 (одного) рабочего дня с момента поступления в Банк Заявления о присоединении к ДКБО.

8.2.2. Принимать к исполнению ЭД, полученные по Системе ДБО от Клиента, подписанные необходимым количеством ЭП уполномоченных должностных лиц Клиента.

8.2.3. Информировать Клиента о совершенных операциях в Системе ДБО одним из способов, установленных настоящими Правилами.

8.2.4. Предоставлять Клиенту необходимые рекомендации для работы в Системе ДБО путем размещения на информационных стендах в операционных залах Банка, официальном интернет-сайте Банка в сети Интернет и/или путем направления информационных сообщений в Системе ДБО.

8.2.5. В случае получения от Клиента надлежащим образом заверенного Уведомления о прекращении действия и (или) об утрате и (или) об использовании без согласия Клиента Средства подтверждения и (или) Компрометации заблокировать логин Клиента в Системе ДБО, Средства подтверждения и прекратить обработку ЭД, подписанных/подтвержденных указанными средствами. Исполнение данного уведомления производится Банком в срок, указанный Клиентом в уведомлении, но не ранее дня, следующего за днем получения уведомления. При наличии технической возможности, Банк может исполнить указанное уведомление в более короткий срок.

8.2.6. Возместить Клиенту сумму операций в случае совершения Банком без согласия Клиента расходных операций по расчетному счету Клиента после получения Банком от Клиента Уведомления о прекращении действия и (или) об утрате и (или) об использовании без согласия Клиента средства подтверждения и/или Компрометации.

8.2.7. Возместить Клиенту сумму операции, о которой Клиент не был проинформирован и, которая была совершена без согласия Клиента в случае неисполнения Банком обязанности по информированию Клиента о совершенной операции.

8.2.8. Фиксировать факт получения от Клиента уведомления о прекращении действия и/или об утрате и (или) об использовании без согласия Клиента Средства подтверждения и (или) Компрометации, оформленного на бумажном носителе, с обязательным указанием даты и времени получения указанного уведомления на Клиентском и своем экземплярах.

8.2.9. Хранить направленные Клиенту и полученные от клиента Уведомления о прекращении действия и(или) об утрате, и (или) об использовании без согласия Клиента средства подтверждения и (или) Компрометации в течение срока не менее трех лет.

8.2.10. Рассматривать и принимать Обращения в сроки и порядке, установленном законодательством Российской Федерации, настоящими Правилами и Договором КБО.

9. ПОРЯДОК ПРЕДОСТАВЛЕНИЯ ДОКУМЕНТОВ И ИНФОРМАЦИИ, СВЯЗАННЫХ С ИСПОЛЬЗОВАНИЕМ СИСТЕМЫ

9.1. Клиент имеет право запрашивать у Банка документы, связанные с использованием Системы ДБО, в том числе копию Заявления о предоставлении доступа сотруднику организации в систему ДБО с помощью логина/пароля, копию акта разрешительной комиссии по разбору конфликтной ситуации (если

ранее между Клиентом и Банком проводилась процедура разбора конфликтной ситуации), копию экспертного заключения о подлинности ЭП (если ранее в рамках разбора конфликтной ситуации проводилась экспертиза подлинности ЭП), иные документы. При необходимости Клиент направляет в Банк заявление в письменном виде в свободной форме с требованием о предоставлении одного или нескольких указанных документов.

9.2. Банк в течение 5 (Пяти) рабочих дней направляет Клиенту запрашиваемые им документы по адресу, указанному в заявлении.

Приложение № 7.1

к Правилам оказания услуг дистанционного банковского обслуживания юридических лиц, индивидуальных предпринимателей, физических лиц, занимающихся в установленном законодательством Российской Федерации порядке частной практикой, в Системе ДБО в ООО «Вайлдберриз Банк»

**ПОЛОЖЕНИЕ О ПРОЦЕДУРЕ РАЗБОРА КОНФЛИКТНОЙ СИТУАЦИИ В РАМКАХ
ИСПОЛЬЗОВАНИЯ СИСТЕМЫ ДБО В
ООО «ВАЙЛДБЕРРИЗ БАНК»**

1. Настоящее положение о процедуре разбора конфликтной ситуации в рамках использования дистанционного банковского обслуживания системы (далее – Положение) разработано в соответствии с Гражданским кодексом Российской Федерации, Федеральным Законом от 27.06.2011 № 161-ФЗ «О национальной платежной системе» и Федеральным Законом от 06.04.2011 № 63-ФЗ «Об электронной подписи», является порядком досудебного урегулирования споров между Банком и Клиентом возникающих в рамках оказания услуг ДБО, в соответствии с Правилами оказания услуг дистанционного банковского обслуживания юридических лиц, индивидуальных предпринимателей, физических лиц, занимающихся в установленном законодательством РФ порядке частной практикой, в системе ДБО в ООО «Вайлдберриз Банк» (далее – Правила).

2. Термины, применяемые в рамках настоящего Положения, используются в следующих значениях:

Конфликтная ситуация – спор между Клиентом и Банком (далее – Стороны) по причине перевода денежных средств, в рамках которого Клиентом оспаривается факт перевода денежных средств, подлинность электронной подписи в электронном документе и (или) факт уведомления о переводе денежных средств, возникшие в результате воздействия вредоносного кода, компрометации Средства подтверждения платежа или по иным причинам.

Разрешительная комиссия – орган, формируемый Банком в соответствии с настоящим Положением с целью разбора Конфликтной ситуации, по существу, и документального оформления результатов работы.

3. Подлежат рассмотрению споры, связанные с наличием у Клиента к Банку претензий по поводу:
- факта передачи Клиентом Банку электронного документа;
 - дня и времени передачи Клиентом Банку электронного документа;
 - содержания, переданного Клиентом Банку электронного документа.

4. В случае возникновения конфликтной ситуации Сторона, обнаружившая возникновение Конфликтной ситуации, должна незамедлительно направить уведомление о Конфликтной ситуации другой Стороне. До направления уведомления иницилирующая Сторона должна убедиться, что причиной возникновения конфликта не является нарушение ей требований к защите Системы ДБО.

Уведомление о наличии Конфликтной ситуации должно содержать информацию о существовании Конфликтной ситуации и обстоятельствах, которые, по мнению уведомителя, свидетельствуют о наличии Конфликтной ситуации, а также все реквизиты соответствующего электронного документа, на основании которого Банк выполнил, не выполнил или выполнил ненадлежащим образом какую-либо операцию.

Уведомление также должно содержать фамилии, имена, отчества и должности представителей заявителя, уполномоченных вести от его имени переговоры по урегулированию Конфликтной ситуации, а также их контактные телефоны, факс, адрес электронной почты.

Уведомление о наличии Конфликтной ситуации оформляется и отправляется в виде электронного документа в Системе ДБО или в письменной форме, которое направляется нарочным либо иным способом, обеспечивающим подтверждение вручения корреспонденции адресату.

5. Сторона, которой направлено уведомление, обязана не позднее двух рабочих дней после его получения проверить наличие обстоятельств, свидетельствующих о возникновении Конфликтной ситуации, и направить уведомителю информацию о результатах проверки и, в случае необходимости, о мерах, принятых для разрешения возникшей Конфликтной ситуации.

6. Конфликтная ситуация признается разрешенной в рабочем порядке в случае, если уведомитель удовлетворен информацией, полученной от другой Стороны. В случае если уведомитель не удовлетворен информацией, полученной от другой Стороны, для рассмотрения Конфликтной ситуации формируется разрешительная комиссия.

7. Банк не позднее чем на следующий рабочий день после того, как принято решение о необходимости формирования разрешительной комиссии, но не позднее пяти рабочих дней после

получения уведомления о Конфликтной ситуации, в случае если конфликтная ситуация не была урегулирована в рабочем порядке:

- формирует состав разрешительной комиссии;
- определяет дату, время и место работы разрешительной комиссии;
- информирует Клиента о назначенной дате, времени, месте работы разрешительной комиссии и о ее составе.

Если Банк и Клиент не договорятся об ином, в состав разрешительной комиссии входит равное количество уполномоченных представителей каждой из Сторон (не более трех с каждой стороны, включая владельца оспариваемой электронной подписи).

Права лиц на представление Сторон в комиссии подтверждаются доверенностями, оформленными надлежащим образом, или распорядительными актами стороны, которую они представляют.

8. Заседание разрешительной комиссии должно быть организовано Банком не позднее 10 (Десяти) рабочих дней с момента получения заявления Клиента.

9. В случае если Клиент не направит своих представителей для участия в работе разрешительной комиссии, разбор Конфликтной ситуации осуществляется без представителей Клиента.

10. Максимальный срок работы разрешительной комиссии не может превышать 20 (Двадцать) рабочих дней с даты ее формирования.

11. При работе разрешительной комиссии, каждая из сторон обязуются способствовать работе комиссии и не допускать отказа от предоставления необходимых документов (информации), если предоставление таких документов (информации) будет допустимо в соответствии с действующим законодательством РФ. Стороны обязуются предоставить разрешительной комиссии возможность ознакомления с условиями и порядком работы своих программных и аппаратных средств, используемых для обмена ЭД по Системе ДБО.

12. Сформированная разрешительная комиссия при рассмотрении Конфликтной ситуации анализирует:

- предмет разногласий на основании претензии одной из сторон;
- банковскую операцию, относящуюся к предмету разногласий;
- факт входа под логином Уполномоченного должностного лица в Систему ДБО, предшествующий отправке спорного электронного документа в Банк;
- факт отправления разового СМС-пароля на зарегистрированный номер Уполномоченного должностного лица;
- дату и время введения разового СМС-пароля для подтверждения факта формирования электронной подписи Уполномоченного должностного лица.

13. Разрешительная комиссия вправе рассматривать любые иные технические вопросы, необходимые, по мнению комиссии, для выяснения причин и последствий возникновения Конфликтной ситуации.

14. Подтверждением правильности исполнения Банком спорного электронного документа является одновременное выполнение следующих условий:

- отправленный разовый СМС-пароль совпадает с введенным разовым СМС-паролем и время ввода не просрочено;
- установлен факт входа под Логин Уполномоченного должностного лица (лиц) в Систему ДБО, предшествующий отправке спорного электронного документа в Банк;
- установлен факт отправления разового СМС-пароля на зарегистрированный номер Уполномоченного должностного лица (лиц);
- установлен факт ввода разового СМС-пароля для подтверждения факта формирования электронной подписи Уполномоченного должностного лица или факт отправки разового СМС-пароля в Систему ДБО.

15. Разрешительная комиссия не вправе давать правовую или какую-либо иную оценку установленных ею фактов.

16. По итогам работы комиссии составляется Акт, в котором содержится:

- дата и место составления Акта;
- даты и время начала и окончания работы разрешительной комиссии;
- состав комиссии;
- суть претензии Стороны;
- действия разрешительной комиссии;
- установленные обстоятельства;
- выводы разрешительной комиссии;
- указание на особое мнение члена (членов) разрешительной комиссии, в случае его наличия.

- подписи членов разрешительной комиссии.

Члены комиссии, не согласные с выводами, отраженными в Акте, подписывают Акт с возражениями либо излагают свое несогласие и выводы в письменном виде в отдельном документе, который прилагается к Акту.

17. Акт составляется в двух экземплярах - по одному для каждой из Сторон не позднее 10 рабочих дней с момента окончания работы комиссии. По требованию члена разрешительной комиссии ему может быть выдана заверенная Банком копия Акта. Один из экземпляров Акта направляется Банком Клиенту по Системе ДБО, нарочным, либо иным способом, обеспечивающим подтверждение вручения корреспонденции адресату.

18. Выводы, содержащиеся в Акте, являются обязательными для Сторон. В случае если подписание Акта в установленный срок не состоится, заинтересованная Сторона вправе обратиться в Арбитражный суд и без выработанного Сторонами решения.

19. Результатом рассмотрения спорной ситуации разрешительной комиссией является определение Стороны, несущей ответственность согласно выводу о подлинности электронной подписи Клиента под электронным документом.

20. В случае подтверждения правильности исполнения Банком спорного электронного документа Клиента претензии Клиента к Банку, связанные с последствиями исполнения указанного электронного документа Клиента, признаются необоснованными.

21. В случае, если будет установлено, что правильность исполнения электронного документа Клиента не подтверждена, т.е. проверяемый электронный документ Клиента подтвержден некорректной электронной подписью, либо электронный документ Клиента не был правильно исполнен Банком. В этом случае претензии Клиента к Банку, связанные с последствиями исполнения указанного электронного документа Клиента, признаются обоснованными.

В случае принятия Банком решения о возмещении Банком Клиенту суммы операции, совершенной с использованием Системы ДБО и без согласия Клиента, сумма возмещения зачисляется на счет Клиента в течение 7 (семи) календарных дней с момента принятия решения.

ЗАЯВЛЕНИЕ

на настройку лимитов в Системе ДБО

1. Сведения о Клиенте

| | |
|-----------------------|--------------------------|
| Клиент ³ : | ИНН: |
| Номер телефона: + 7 | Адрес электронной почты: |

2. Заявление Клиента

Настоящим заявлением Клиент просит:

включить суточный лимит платежей на сумму платежей в течение одного дня (календарные сутки по московскому времени) в размере:

| | |
|----------------|-----------------|
| Сумма цифрами: | Сумма прописью: |
|----------------|-----------------|

3. Подпись Клиента

| | |
|---|--|
| <p>3.1. <input type="checkbox"/> Заполняется Клиентом⁴</p> <p>Дата подачи заявления:</p> <p>Подпись:</p> <p>Расшифровка подписи:</p> <p>М.П. (при наличии)</p> | <p>3.2. <input type="checkbox"/> Заявление подписано электронной подписью⁵:</p> |
|---|--|

³ Указывается полное наименование юридического лица; Ф.И.О. индивидуального предпринимателя; Ф.И.О. физического лица занимающегося в установленном законодательством Российской Федерации порядке частной практикой.

⁴ Подписывается Клиентом собственноручной подписью.

⁵ Подписывается Клиентом ЭП при подаче Заявления через дистанционные каналы связи.

Уведомление

**о прекращении действия и (или) об утрате/компрометации
средства подтверждения и(или) использовании средства подтверждения без согласия Клиента и(или) о приостановлении/прекращении
использования Системы ДБО в ООО «Вайлдберриз Банк»**

1. Сведения о Клиенте

| | |
|-----------------------|--------------------------|
| Клиент ⁶ : | ИНН: |
| Номер телефона: + 7 | Адрес электронной почты: |

2. Настоящим Клиент:

2.1. Уведомляет Банк:

- ☐ о прекращении действия средства подтверждения
- ☐ об утрате/компрометации средства подтверждения
- ☐ об использовании средства подтверждения без согласия Клиента

Прошу с даты направления настоящего уведомления заблокировать указанное ниже средство подтверждения, использовавшееся в соответствии с Правилам оказания услуг дистанционного банковского обслуживания юридических лиц, индивидуальных предпринимателей, физических лиц, занимающихся в установленном законодательством Российской Федерации порядке частной практикой, в Системе ДБО в ООО «Вайлдберриз Банк», и остановить обработку электронных документов, подписанных/подтвержденных указанным средством:

- ☐ мобильный телефон

2.2. Уведомляет Банк:

- | | |
|---|---|
| <input type="checkbox"/> о приостановлении использования Системы ДБО ООО «Вайлдберриз Банк» | <input type="checkbox"/> о прекращении использования Системы ДБО ООО «Вайлдберриз Банк» |
|---|---|
- Прошу с 00:00 даты направления настоящего уведомления заблокировать все средства подтверждения и прекратить обработку электронных документов, подписанных/подтвержденных средствами подтверждения.

3. Подпись Клиента

| | |
|---|--|
| 3.1. <input type="checkbox"/> Заполняется Клиентом⁷ Дата подачи заявления: Подпись: Расшифровка подписи: М.П. (при наличии) | 3.2. <input type="checkbox"/> Заявление подписано электронной подписью⁸: |
|---|--|

⁶ Указывается полное наименование юридического лица; Ф.И.О. индивидуального предпринимателя; Ф.И.О. физического лица занимающегося в установленном законодательством РФ порядке частной практикой.

⁷ Подписывается Клиентом собственноручной подписью.

⁸ Подписывается Клиентом ЭП при подаче Уведомления через дистанционные каналы связи.

ОРГАНИЗАЦИОННЫЕ МЕРЫ ДЛЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОЙ РАБОТЫ В СИСТЕМЕ ДБО

1. Требования по защите от вредоносного кода:

1.1. К средствам защиты от вредоносного кода относятся средства, используемые для:

- выявления и обезвреживания вредоносного кода (антивирусы);
- межсетевое экранирование рабочего места или корпоративной сети;
- Web-фильтрации;
- обнаружения и предотвращения вторжений;
- контроля выполнения приложений.

2. Для обеспечения надлежащей защиты от вредоносного кода Клиент обязан:

- обеспечить непрерывное использование средств защиты от вредоносного кода;
- обеспечить периодический контроль целостности системного, прикладного и специального программного обеспечения;
- ежедневно осуществлять проверку рабочего места на наличие вредоносного кода;
- обеспечить регулярное обновление средств защиты от вредоносного кода, обновление прикладного программного обеспечения, установку пакетов обновления безопасности операционной системы;
- использовать лицензионное программное обеспечение;
- использовать для работы в Системе учетную запись, не входящую в группу «Локальные администраторы» или аналогичную группу пользователей;
- на мобильном устройстве (смартфоне) не повышать полномочия до пользователя root;
- осуществлять вход в Систему с рабочего места, используемого исключительно для подключения к Системе;
- ограничивать по времени доступ ответственных лиц к ЭП и/или телефону, на который приходят СМС – подтверждения платежей;
- контролировать суммы переводов, реквизиты получателей.

1. Для защиты ЭП необходимо:

1.1. Для входа в Систему вводить логин и пароль только на сайте Системы, убеждаться в подлинности сайта Системы до ввода реквизитов доступа.

1.2. Никогда и ни при каких обстоятельствах не сообщать никому свои логины, пароли, СМС/Push коды.

1.3. Обязательно сверять текст СМС-сообщений, содержащий пароль, с деталями выполняемой операции. Если в СМС указан пароль для платежа, который вы не совершали или его предлагают ввести/назвать, чтобы отменить якобы ошибочно проведенный по счету платеж, ни в коем случае не вводить его и не сообщать его никому, в том числе сотрудникам Банка.

1.4. В случае утери мобильного телефона, на который приходят разовые пароли, немедленно заблокировать соответствующую SIM-карту у оператора сотовой связи.

1.5. Записать контактный телефон Банка в адресную книгу или запомнить его. В случае если в личном кабинете Системы вы обнаружите телефон, отличный от записанного, в особенности, если вас будут призывать позвонить по этому телефону для уточнения информации, либо по другому поводу, будьте бдительны и немедленно позвоните в Банк по ранее записанному вами телефону.

1.6. Устанавливать мобильные приложения Системы только из авторизованных магазинов. Использовать антивирусное программное обеспечение для смартфона.

1.7. Избегать регистрации номера мобильного телефона, на который приходят СМС-сообщения с разовым паролем, в социальных сетях и других открытых источниках.

2. Общие правила безопасности, применяющиеся для защиты любых данных, хранящихся на компьютерах:

2.1. Использовать только компьютеры с лицензионным программным обеспечением, установленным и запущенным антивирусным программным обеспечением и персональным межсетевым экраном, своевременно обновлять антивирусные базы. Регулярно проводить полную проверку

компьютера на предмет наличия вредоносного кода, своевременно обновлять лицензионную операционную систему и браузеры.

2.2. Проверять действительность сертификата веб-сайта Системы. При вводе личной информации, помнить, что любой веб-адрес в адресной строке Интернет-банка должен начинаться с «https». Если в адресе не указано «https», это значит, что вы находитесь на незащищенном веб-сайте, и вводить данные нельзя.

2.3. Использовать виртуальную клавиатуру для ввода пароля.

2.4. Быть внимательным: в случае возникновения подозрений на мошенничество необходимо максимально быстро сообщить о своих подозрениях в Банк с целью оперативного блокирования доступа к вашей учетной записи в Системе.

2.5. При работе с электронной почтой не открывать письма и вложения к ним, полученные от неизвестных отправителей, не переходить по содержащимся в таких письмах ссылкам.

2.6. Не работать с правами администратора при отсутствии необходимости. В повседневной практике входить в систему как пользователь, не имеющий прав администратора.

2.7. Включить системный аудит событий, регистрирующий возникающие ошибки, вход пользователей и запуск программ, периодически просматривать журнал и реагировать на ошибки.

2.8. Запретить в межсетевом экране соединения по неиспользуемым протоколам.

2.9. Не давать разрешения неизвестным программам выходить в Интернет.

2.10. При работе в Интернете не соглашаться на установку каких-либо дополнительных программ от недоверенных издателей.

Заявление

**об изменении/дополнении прав доступа в Системе ДБО/
о замене мобильного телефона в Системе ДБО ООО «Вайлдберриз Банк»**

1. Сведения о Клиенте

| | |
|-----------------------|--------------------------|
| Клиент ⁹ : | ИНН: |
| Номер телефона: | Адрес электронной почты: |

2. Изменение/дополнение прав доступа в Системе ДБО¹⁰:

2.1. Установление доступа в Системе ДБО:

| | Фамилия, имя, отчество | Номер мобильного телефона | Адрес электронной почты |
|---|------------------------|---------------------------|-------------------------|
| <input type="checkbox"/> Настоящим Заявлением прошу предоставить право использовать аналог собственноручной подписи, а также наделить полномочиями по доступу в Систему ДБО, подписанию электронной подписью, подтверждению одноразовым паролем и направлению в ООО «Вайлдберриз Банк» электронных документов, в том числе с целью распоряжения денежными средствами на Счете(ах) следующих должностных лиц: | | | |
| <input type="checkbox"/> Настоящим Заявлением наделю полномочиями по доступу в Систему ДБО без права использования аналога собственноручной подписи/распоряжения денежными средствами на Счете(-ах) следующих лиц: | | | |
| <input type="checkbox"/> Прошу отозвать ранее установленные полномочия по доступу в Систему ДБО с правом/без права использовать аналога собственноручной подписи следующих лиц: | | | |

3. Замена номера мобильного телефона Клиента¹¹ в Системе ДБО¹²:

| | |
|---|----|
| <input type="checkbox"/> Прошу отключить номер мобильного телефона: | +7 |
| <input type="checkbox"/> Прошу подключить новый номер мобильного телефона: | +7 |

4. Согласия Клиента, предоставленные ООО «Вайлдберриз Банк»

Настоящим Заявлением подтверждаю, что номер(-а) мобильного(-ых) телефона(-ов), указанный(-ые) в настоящем Заявлении, принадлежит(-ат) указанному(-ым) лицу(-ам) и будет(-ут) использован(-ы) в качестве зарегистрированного номера мобильного телефона в Системе ДБО.
Обязуюсь: в случае утраты/смены зарегистрированного номера мобильного телефона в порядке, установленном Правилами Системы ДБО, обратиться в Банк с целью уведомления о смене зарегистрированного номера; не разглашать третьим лицам СМС-сообщения с логином и/или одноразовым паролем. Риски неблагоприятных последствий, связанных с невыполнением указанных обязательств, принимаю на себя.

5. Подпись Клиента

| | |
|--|---|
| 3.1. <input type="checkbox"/> Заполняется Клиентом¹³ Дата подачи заявления: Подпись: Расшифровка подписи: М.П. (при наличии) | 3.2. <input type="checkbox"/> Заявление подписано электронной подписью¹⁴: |
|--|---|

⁹ Указывается полное наименование юридического лица; Ф.И.О. индивидуального предпринимателя; Ф.И.О. физического лица занимающегося в установленном законодательством Российской Федерации порядке частной практикой.

¹⁰ Раздел 2 заполняется в случае изменения/дополнения прав доступа в Системе ДБО уполномоченных должностных лиц Клиента.

¹¹ Изменение номера телефона действующего уполномоченного должностного лица Клиента; индивидуального предпринимателя; физического лица занимающегося в установленном законодательством Российской Федерации порядке частной практикой.

¹² Раздел 3 заполняется в случае изменения номера мобильного телефона Клиента.

¹³ Подписывается Клиентом собственноручной подписью.

¹⁴ Подписывается Клиентом ЭП при подаче Заявления через дистанционные каналы связи.