

УТВЕРЖДЕНО:
приказом Председателя Правления
ООО Банк Оранжевый
от 04.04.2024 г. №97-П-А

ПРАВИЛА ДИСТАНЦИОННОГО БАНКОВСКОГО ОБСЛУЖИВАНИЯ

ЮРИДИЧЕСКИХ ЛИЦ, ИНДИВИДУАЛЬНЫХ ПРЕДПРИНИМАТЕЛЕЙ И ФИЗИЧЕСКИХ ЛИЦ,
ЗАНИМАЮЩИХСЯ В УСТАНОВЛЕННОМ ЗАКОНОДАТЕЛЬСТВОМ РОССИЙСКОЙ
ФЕДЕРАЦИИ ПОРЯДКЕ ЧАСТНОЙ ПРАКТИКОЙ, В ООО БАНК ОРАНЖЕВЫЙ

(Договор присоединения)

(версия 1, редакция 2, действует с 08.04.2024)

Разработчик:	Отдел методологии Департамента банковских технологий и методологии
Ограничение доступа:	Открытый доступ

ОГЛАВЛЕНИЕ

1. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ	3
2. ОБЩИЕ ПОЛОЖЕНИЯ	7
3. ПОРЯДОК ОСУЩЕСТВЛЕНИЯ ПЕРЕВОДОВ С ИСПОЛЬЗОВАНИЕМ СИСТЕМЫ ДБО	11
4. ПРАВА И ОБЯЗАННОСТИ СТОРОН	14
5. ПОРЯДОК РАБОТЫ В СИСТЕМЕ ДБО С ИСПОЛЬЗОВАНИЕМ УЭП.....	19
6. ПОРЯДОК РАБОТЫ В СИСТЕМЕ ДБО С ИСПОЛЬЗОВАНИЕМ ЛОГИНА И ПАРОЛЯ	21
7. ПОРЯДОК РАБОТЫ В СИСТЕМЕ ДБО С ИСПОЛЬЗОВАНИЕМ ПЭП РАУСCONTROL	23
8. ПОРЯДОК ИСПОЛЬЗОВАНИЯ МОБИЛЬНОГО ПРИЛОЖЕНИЯ.....	25
9. ОТВЕТСТВЕННОСТЬ СТОРОН И ПОРЯДОК РАЗРЕШЕНИЯ СПОРОВ	25
10. ПОРЯДОК РАЗРЕШЕНИЯ СПОРОВ, СВЯЗАННЫХ С ПОДТВЕРЖДЕНИЕМ АВТОРСТВА ЭЛЕКТРОННОГО ДОКУМЕНТА И (ИЛИ) ДОСТОВЕРНОСТЬ ЭЛКТРОННОЙ ПОДПИСИ	27
11. СРОК ДЕЙСТВИЯ И ПОРЯДОК ДОСРОЧНОГО РАСТОРЖЕНИЯ ДОГОВОРА ДБО	29
12. ДОПОЛНИТЕЛЬНЫЕ УСЛОВИЯ	30

1. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Авторизация – подтверждение полномочий (предоставление прав доступа) Клиента/ его Уполномоченного лица/Пользователя, успешно прошедшего Аутентификацию входа, на получение услуг Банка в Мобильном приложении на протяжении одного Сеанса соединения.

Аутентификация – автоматическая процедура проверки соответствия Средств аутентификации, используемых Уполномоченным лицом для входа в Систему.

Банк - общество с ограниченной ответственностью Банк Оранжевый.

Владелец сертификата ключа проверки УЭП (Владелец УЭП) – физическое лицо, на имя которого Удостоверяющим центром выдан сертификат ключа проверки электронной подписи, и которое владеет соответствующим ключом УЭП, позволяющим с помощью средств УЭП создавать УЭП в электронных документах (подписывать электронные документы). Владельцами сертификатов ключей проверки УЭП являются уполномоченные лица Сторон, имеющие право подписывать электронные документы своей ЭП от имени Стороны в Системе ДБО.

Временный пароль – уникальная комбинация цифр и (или) букв и (или) символов, направляемая Банком Клиенту и (или) Уполномоченному лицу Клиента в SMS-сообщении, для осуществления первичной Аутентификации входа в Систему в сочетании с Логинном. Срок действия Временного пароля ограничен тремя календарными днями с даты направления SMS на Зарегистрированный номер.

Договор, Договор ДБО – "Договор дистанционного банковского обслуживания юридических лиц, индивидуальных предпринимателей и физических лиц, занимающихся в установленном законодательством Российской Федерации порядке частной практикой", заключаемый между Банком и Клиентом (далее при совместном упоминании – Стороны) путем присоединения Клиента к настоящим Правилам в порядке, определенном настоящими Правилами.

Дистанционное банковское обслуживание (ДБО) – услуга дистанционного банковского обслуживания, позволяющая Клиенту удаленно осуществлять комплекс операций в порядке, предусмотренном настоящими Правилами, посредством Системы ДБО на основании заключенного с Банком Договора ДБО.

Клиент - юридическое лицо/ индивидуальный предприниматель/ физическое лицо, занимающееся в установленном законодательством Российской Федерации порядке частной практикой, которое (-ый) обслуживается в Банке на основании Договора ДБО.

Код подтверждения – уникальный разовый код в виде комбинации цифр, генерируемый Системой и направляемый Банком Клиенту в SMS – сообщении/ PUSH - уведомлении для подтверждения каждой операции, выполняемой Клиентом в Системе. В сочетании с Логинном и Паролем Код подтверждения является простой ЭП Клиента.

Компрометация – событие и (или) ситуация, в результате которой происходит либо может произойти ознакомление неуполномоченным лицом (неуполномоченными лицами) с Ключом УЭП, Логинном, Паролем, Кодом подтверждения.

К компрометации относятся следующие события и (или) ситуации:

- получение несанкционированного доступа третьих лиц к носителю Ключа УЭП (закрытого ключа), телефону и (или) SIM-карте с номером телефона Уполномоченного лица Клиента/Пользователя, используемого в целях подписания документов в Системе ДБО ПЭП и (или) получения доступа к Системе ДБО в результате утраты, хищения (в т.ч. кражи или разбоя), изъятия, передачи третьему лицу, в том числе с последующим обнаружением (возвратом);
- несанкционированное копирование Ключа УЭП (закрытого ключа);
- увольнение работника, имевшего доступ к носителю Ключа УЭП (закрытого ключа) и (или) паролю для доступа к Системе ДБО;
- нарушение правил хранения и уничтожения (после окончания срока действия) носителя Ключа УЭП (закрытого ключа);
- возникновение подозрений на утечку информации или её искажение в Системе ДБО;
- нарушение печати на сейфе или пенале (контейнере) с носителем Ключа УЭП (закрытого ключа);
- случаи, когда невозможно достоверно установить, что произошло с носителем Ключа УЭП (закрытого ключа), в том числе случаи, когда носитель Ключа УЭП (закрытого ключа)

- вышел из строя и доказательно не опровергнута возможность того, что данный факт произошел в результате несанкционированных действий злоумышленника;
- несанкционированное использование Зарегистрированного номера, технических, программных и коммуникационных ресурсов, используемых для доступа в Систему ДБО;
 - возникновение подозрений о доступе неуполномоченных лиц к информации в Системе ДБО или об ее искажении в Системе ДБО, когда нельзя достоверно установить, что произошло с техническими, программными, коммуникационными ресурсами, используемыми для доступа в Систему (в том числе, выход из строя, когда доказательно не опровергнута возможность того, что данный факт произошел в результате несанкционированных действий третьих лиц);
 - любые иные события и (или) ситуации, по причине которых у Владельца УЭП/Уполномоченного лица Клиента/Пользователя возникают сомнения в сохранении тайны Ключа УЭП, Логина, Пароля, Кода подтверждения.

Ключ УЭП (закрытый ключ) – уникальная последовательность символов, предназначенная для создания в электронном документе ЭП, а также преобразования полученной закрытой информации в открытую с использованием сертифицированных средств криптографической защиты информации в Системе ДБО, доступная только Клиенту (Уполномоченному лицу Клиента), наделенному правом использования УЭП.

Ключ проверки ЭП (открытый ключ) – уникальная последовательность символов, однозначно связанная с Ключом ЭП и предназначенная для проверки подлинности УЭП, а также преобразования передаваемой открытой информации в закрытую в Системе ДБО.

Ключевой носитель (Смарт-ключ) – USB-токен или иное аппаратное устройство для хранения закрытого ключа электронной подписи УЭП для Системы ДБО.

Проверка электронной подписи (УЭП) документа – проверка соотношения, связывающего хэш-функцию документа, подпись под этим документом и открытый ключ подписавшего абонента в Системе ДБО. Если рассматриваемое соотношение оказывается выполненным, то подпись признается правильной, а сам документ – подлинным, в противном случае документ считается измененным, а подпись под ним – недействительной.

Логин – уникальная комбинация букв, цифр и символов, предоставляемая Банком Клиенту и (или) Уполномоченному лицу Клиента в порядке, установленном [разделом 6](#) Правил, для осуществления Аутентификации входа в Систему в сочетании с Временным паролем, Паролем.

Мобильное приложение – мобильная версия Системы ДБО, созданная для установки на мобильных устройствах под управлением операционных систем Android, iOS и позволяющая Клиентам осуществлять доступ к Системе ДБО с данных устройств с использованием сети "Интернет".

Зарегистрированный номер телефона – абонентский номер сотовой связи (мобильного телефона) Уполномоченного лица Клиента/Пользователя Системы ДБО, указанный в заявлении на заключение Договора ДБО и (или) иных заявлениях, предоставленных Банку в целях получения доступа в Систему ДБО и (или) формирования и использования ПЭП.

Операционный день – часть рабочего дня Банка, в течение которого все совершенные операции оформляются и отражаются в бухгалтерском учете Банка за соответствующую календарную дату.

Операционное время – часть Операционного дня Банка, в течение которого производится обслуживание Клиентов, совершение операций, прием и обработка документов для отражения в бухгалтерском учете текущим Операционным днем Продолжительность Операционного дня (времени) (время начала и окончания) определяется Банком. Банк информирует Клиентов об Операционном времени приема и обработки документов, а также его изменении, посредством размещения соответствующей информации способом, обеспечивающим ее доведение неограниченному количеству лиц на официальном сайте Банка в сети Интернет www.bankorange.ru, в местах обслуживания клиентов, и, при необходимости, любым иным способом, установленным договором с Клиентом.

Пароль – уникальная комбинация букв и (или) цифр и (или) символов, самостоятельно сформированная Уполномоченным лицом Клиента в соответствии с требованиями, установленными Системой ДБО, после получения от Банка Временного пароля, известная только указанному Уполномоченному лицу и используемая им для Аутентификации входа в Систему ДБО в сочетании с Логинем.

Правила ДБО (Правила) – настоящие "Правила дистанционного банковского обслуживания юридических лиц, индивидуальных предпринимателей и физических лиц, занимающихся в установленном законодательством Российской Федерации порядке частной практикой, в ООО Банк Оранжевый", представляющие собой договор присоединения о предоставлении Клиенту услуги дистанционного банковского обслуживания с использованием Системы ДБО на условиях, перечисленных в Правилах (на основании статьи 428 Гражданского кодекса Российской Федерации).

Подтверждение подлинности УЭП в электронном документе – положительный результат проверки средствами ЭП с использованием сертификата ключа подписи принадлежности ЭП в ЭД Владельцу сертификата ключа подписи УЭП и отсутствия искажений в подписанном данной ЭП ЭД в Системе ДБО посредством проверки соотношения, связывающего хэш-функцию документа, подпись под этим документом и открытый ключ подписавшего абонента в Системе ДБО.

Пользователь – физическое лицо, наделенное Клиентом полномочиями (правами) доступа в Систему ДБО и уполномоченное Клиентом просматривать информацию в Системе ДБО и/или давать Банку распоряжения о совершении операций по Счетам Клиента с использованием Системы и наделенное правом подписания ЭД ЭП в соответствии с заявлениями для предоставления доступа к Системе ДБО, предусмотренными настоящими Правилами.

Простая электронная подпись (ПЭП) – электронная подпись, которая посредством использования кодов, паролей или иных средств подтверждает факт формирования электронной подписи Пользователем или Уполномоченным лицом Клиента в Системе ДБО. В рамках настоящих Правил Простой электронной подписью является одноразовый код (Код подтверждения), формируемый Банком и направляемый на Зарегистрированный номер Пользователя/Уполномоченного лица Клиента для однократного использования при передаче пароля для первичного входа Клиента в Систему и для каждого подписываемого ЭД Клиента, и средство ЭП PayControl.

Представитель Клиента - единоличный исполнительный орган Клиента - юридического лица, а также лицо, действующее от имени Клиента, полномочия которого подтверждены доверенностью, договором, законом либо актом уполномоченного на то государственного органа или органа местного самоуправления (в том числе арбитражный управляющий (внешний, конкурсный, финансовый), действующий на основании решения (определения) арбитражного суда в целях проведения процедур, предусмотренных в деле о банкротстве Клиента).

Распоряжение – распоряжение о переводе денежных средств, составляемое, удостоверяемое и передаваемое Клиентом в Банк в электронном виде в целях осуществления перевода денежных средств в рамках форм безналичных расчетов в соответствии с Положением Банка России "О правилах осуществления перевода денежных средств" от 25.08.2021 № 762-П. Банк определяет формат Распоряжений в соответствии с требованиями действующего законодательства Российской Федерации, нормативных актов Банка России и внутренних нормативных актов Банка, определяющих порядок оформления распоряжений и выполнения процедур приема к исполнению и исполнения распоряжений.

Сайт Банка – официальный сайт Банка в информационно-телекоммуникационной сети "Интернет", находящийся по адресу: www.bankorange.ru.

Сертификат ключа проверки УЭП (Сертификат ключа подписи, Сертификат) – электронный документ, выданный Удостоверяющим центром либо доверенным лицом Удостоверяющего центра, подтверждающий принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи.

Смарт-ключ (USB-токен) – компактное программно - аппаратное устройство, используемое как персональное средство аутентификации и защищённого хранения данных, аппаратно поддерживающее работу с сертификатами и УЭП.

Средства криптографической защиты информации (СКЗИ) – программно-технические средства, осуществляющие криптографическое преобразование информации для обеспечения неизменности содержания и установления Авторства электронных документов, а также конфиденциальности и контроля целостности информации в Системе ДБО при использовании УЭП.

Счет – банковский счет Клиента, счет депозита, открытый Банком Клиенту на основании договора банковского счета, договора депозита в соответствии с требованиями законодательства Российской Федерации в рублях или иностранной валюте.

Система ДБО (Система) – информационно - технологический комплекс дистанционного банковского обслуживания, позволяющий Сторонам организовать формирование и обмен Электронными документами и информацией (передачу Электронных документов и информации), имеющей значение для Сторон, в том числе составлять, удостоверить и передавать Клиентом распоряжения в Банк в целях осуществления перевода денежных средств в рамках применяемых форм безналичных расчетов ¹.

Средства ЭП – шифровальные (криптографические) средства, используемые для реализации хотя бы одной из следующих функций – создание ЭП, проверка ЭП, создание ключа ЭП и ключа проверки ЭП для Системы ДБО. Для целей настоящих Правил предусмотрена возможность использования ПЭП, УНЭП и/или Средство ЭП PayControl.

Стороны – Банк и Клиент при совместном упоминании.

Средства аутентификации – Сертификат, хранящийся на Смарт-ключе, Логин, Пароль, а также в случае использования Уполномоченным лицом Мобильного приложения - короткий код доступа и (или) отпечаток пальца.

Уполномоченное лицо – должностное лицо Клиента и (или) Представитель Клиента, полномочия которых подтверждены доверенностью, договором, законом либо актом уполномоченного на то государственного органа или органа местного самоуправления, наделенные правами использования ЭП при работе с Электронными документами в Системе ДБО.

Удостоверяющий центр – в целях настоящих Правил - юридическое лицо, осуществляющие функции по созданию и выдаче сертификатов ключей проверки электронных подписей (УЭП), в том числе изготовление и выдачу сертификатов ключей подписей, создание (генерация) закрытых и открытых ключей, установление сроков действия сертификатов ключей подписей, приостановление и возобновление действия сертификатов ключей подписей, а также их аннулирование, ведение Реестра Сертификатов. Банк вправе осуществлять функции (часть функций) Удостоверяющего центра при наличии соответствующих полномочий и необходимых разрешений (лицензий).

Усиленная электронная подпись (далее – УЭП) – электронная подпись, полученная в результате криптографического преобразования информации, позволяющая определить лицо, подписавшее Электронный документ, а также обеспечивающая возможность контроля целостности и подтверждения подлинности Электронных документов, исходящих от каждой из Сторон в Системе ДБО.

Тарифы – "Сборник тарифов на услуги, предоставляемые клиентам – юридическим лицам и индивидуальным предпринимателям ООО Банк Оранжевый".

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, и позволяющая однозначно идентифицировать Уполномоченное лицо, подписывающее Электронный документ, а также установить отсутствие утраты, искажения или подделки содержащейся в Электронном документе информации. В целях настоящих Правил под ЭП понимается усиленная ЭП (в случае Аутентификации в Системе ДБО и подписании ЭД с использованием Сертификата, хранящегося на Смарт-ключе), простая ЭП (в случае Аутентификации и подписании ЭД с использованием Логина и Пароля, одноразовых кодов и паролей).

Электронный документ – документ (в том числе Распоряжение) и (или) сообщение, информация в которых представлена в электронно-цифровой форме, в том числе в виде файла или записи базы данных, которые соответствуют установленным в Системе ДБО

¹ Банк предоставляет сервисы дистанционного банковского обслуживания с использованием программных решений - технологических комплексов дистанционного банковского обслуживания "Faktura.ru" и технологического комплекса дистанционного банковского обслуживания Digital2Go. Функциональность Системы ДБО в рамках каждой из используемых программных решений устанавливается на усмотрение Банка и может различаться.

В целях применения Тарифов Система ДБО может быть также поименована как "Клиент-Банк"

форматам и заверены Электронной подписью, подготовленный и переданный с помощью программного обеспечения Системы ДБО в соответствии со всеми процедурами защиты информации. Электронный документ в форме сообщения может содержать вложенные файлы, в том числе созданные с использованием сканирующих устройств изображения документов, оформленных на бумажном носителе², которые также считаются заверенными Электронной подписью.

Push-уведомление – сообщение, направляемое Банком Клиенту на Номер телефона посредством информационно-телекоммуникационной сети "Интернет", всплывающее на экране мобильного устройства Клиента при условии наличия на указанном мобильном устройстве установленного Мобильного приложения. Банк использует Push-уведомления наряду с SMS – сообщениями для направления Клиенту Кодов подтверждения, а также сообщений информационного характера.

SMS – сообщение – короткое текстовое сообщение, направляемое Банком на Зарегистрированный номер телефона и содержащее уникальную последовательность символов, предназначенных для однократного использования в целях проведения Аутентификации Клиента для работы в Системе ДБО, в том числе в целях первичного входа в Систему ДБО, подтверждения факта формирования ПЭП. Банк использует SMS – сообщения для направления Временного пароля, а также наряду с Push-уведомлениями для направления Клиенту Кодов подтверждения и сообщений информационного характера.

PayControl – программный комплекс в виде отдельного мобильного приложения для мобильного устройства, предназначенный для подтверждения пользователем операций в Системе ДБО и/или формирования электронной подписи в Системе ДБО.

2. ОБЩИЕ ПОЛОЖЕНИЯ

2.1. Настоящие Правила представляют собой договор о предоставлении Клиенту услуг Банка по дистанционному банковскому обслуживанию, который регулирует условия и порядок заключения, исполнения, изменения и расторжения Договора ДБО между Клиентом и Банком, условия и порядок использования Системы ДБО, определяют возникающие в этой связи права, обязанности и ответственность Сторон и является договором присоединения на основании статьи 428 Гражданского кодекса Российской Федерации.

2.2. Действовавшие до введения в действие настоящих Правил "Правила дистанционного банковского обслуживания юридических лиц, индивидуальных предпринимателей и физических лиц, занимающихся в установленном законодательством Российской Федерации порядке частной практикой, в системе "Интернет-Банк (Faktura.ru)" в ООО Банк Оранжевый" изложены в редакции настоящих Правил и применяются для всех ранее присоединившихся к ним Клиентов в соответствии с положениями пункта 1 статьи 428 Гражданского кодекса Российской Федерации.

2.3. Дистанционное банковское обслуживание Клиента с использованием Системы ДБО осуществляется Банком в соответствии с законодательством Российской Федерации и Правилами. В случае изменения законодательства Российской Федерации Правила, до момента их изменения Банком, применяются в части, не противоречащей требованиям законодательства Российской Федерации.

2.4. До заключения Договора ДБО Банк информирует Клиента об условиях использования Системы ДБО, в том числе о возможных ограничениях способов и мест использования Системы ДБО, случаях повышенного риска использования Системы ДБО путем опубликования на Сайте Банка и размещения в клиентских зонах подразделений Банка соответствующей информации, Правил и Тарифов.

2.5. Заключение Договора ДБО осуществляется путем присоединения Клиента к условиям настоящих Правил на основании:

- подписанного Клиентом заявления установленной Банком формы на заключение Договора ДБО, при этом Договор ДБО считается заключенным с момента подписания указанного заявления Клиентом/Представителем Клиента и уполномоченным сотрудником Банка,

² Максимальный объем вложения для служебно-информационных документов и для Документов свободного формата 10мб. Рекомендованные настройки для качественного сканирования документов больших объемов: качество 150 Dpi, монохромное сканирование.

либо посредством направления Банком Клиенту отдельного уведомления о заключения Договора ДБО;

- волеизъявления Клиента, выраженного в форме оферты и указанного в иных заявлениях (обращениях) Клиента, отличных от заявления установленной Банком формы на заключение Договора ДБО - при условии принятия Банком данной оферты. Способ акцептования Банком оферты на заключение Договора отражается в условиях оферты.

2.6. Банк вправе отказать Клиенту в заключении Договора ДБО.

2.7. Подписание Клиентом (Представителем Клиента) заявления на заключение Договора ДБО по форме Банка и (или) осуществление иных действий, поименованных в п. 2.5 настоящих Правил и направленных на заключение Договора ДБО, подтверждает ознакомление и согласие Клиента с условиями настоящих Правил и действующих Тарифов.

2.8. Клиент и Банк признают используемые ими в рамках настоящих Правил системы обработки, хранения, защиты и передачи информации достаточными для обеспечения надежной, эффективной и безопасной работы и защиты от несанкционированного доступа, а также для подтверждения авторства и подлинности ЭД.

2.9. Стороны признают, что направление и получение Сторонами любых Электронных документов посредством Системы ДБО, заверенных ЭП уполномоченных лиц Банка и Клиента, в том числе обмен между Банком и Клиентом документами (заявлениями, уведомлениями, пр.) в целях заключения, изменения и расторжения любых видов договоров и дополнительных соглашений к указанным договорам, равнозначно направлению и получению Банком и Клиентом документов на бумажных носителях, заверенных необходимым количеством собственноручных подписей уполномоченных лиц Банка и Клиента и печатями Банка и Клиента (при использовании Клиентом печати).

В случае если действующие договоры, заключенные между Банком и Клиентом, в которые вносятся изменения либо которые расторгаются по соглашению Сторон путем обмена Сторонами посредством Системы соответствующими документами, заверенными ЭП уполномоченных лиц Банка и Клиента, не содержат положения о возможности применения в указанных целях такого способа обмена документами и равнозначности таких документов документам на бумажных носителях, заверенным подписями уполномоченных лиц и печатями Сторон, Стороны руководствуются положениями настоящих Правил.

При этом Электронные документы, в том числе содержащие в виде вложенных файлов сканированные копии документов, оформленных на бумажных носителях и заверенных подписями Уполномоченных лиц и печатью Клиента (при использовании печати), направленные в Банк Клиентом в целях заключения, изменения и расторжения любых видов договоров и дополнительных соглашений к указанным договорам, должны быть заверены ЭП только Уполномоченных лиц Клиента, наделенными соответствующими полномочиями на осуществление заключения, изменения и расторжения договоров и дополнительных соглашений к указанным договорам.

2.10. Банк предоставляет Клиенту следующие услуги с использованием Системы ДБО:

- прием от Клиента Распоряжений по Счету(-ам) Клиента в виде Электронных документов;
- предоставление Клиенту возможности формирования выписок по Счету Клиента в виде Электронных документов;
- возможность обмена иными Электронными документами с Банком;
- возможность обмена электронными копиями документов, полученными с использованием сканирующих устройств, изначально оформленных на бумажном носителе, в виде вложенных в Электронные документы файлов;
- иные услуги, предоставление которых предусмотрено функционалом Системы ДБО.

2.11. Подробная информация о функционале и порядке работы в Системе, в том числе порядок подготовки, контроля и отправки Электронных документов в Банк приведена в инструкции пользователя, доступной при входе в Систему ДБО, а также на Сайте Банка. В случае приостановления работы Системы или ее элементов, а также в иных случаях невозможности предоставления услуг, предусмотренных настоящими Правилами, обслуживание Клиента осуществляется в порядке, установленном соответствующими договорами банковских счетов, договорами депозитов, а также другими договорами, заключенными между Банком и Клиентом, в том числе, но не исключительно, договорами о

предоставлении банковских продуктов и услуг, небанковских услуг, а также о заключении иных сделок.

2.12. Клиент поручает, а Банк принимает на себя обязательство выполнять операции на основании распоряжений Клиента в соответствии с условиями настоящих Правил, условиями соответствующих договоров, заключенных между Банком и Клиентом, требованиями законодательства Российской Федерации, функционалом Системы.

2.13. За предоставление услуги обслуживания Клиентов с использованием Системы в соответствии с настоящими Правилами Банк удерживает комиссионное вознаграждение в размере, установленном Тарифами.

2.14. Банк с целью ознакомления Клиента с условиями настоящих Правил размещает Правила путем их опубликования в порядке, предусмотренном п. 2.15 Правил.

2.15. Банк имеет право вносить изменения в настоящие Правила и Тарифы, информируя Клиентов об изменениях одним из указанных способов:

- путем размещения на информационных стендах в клиентских зонах подразделений Банка;
- путем размещения на Сайте Банка;
- путем рассылки Клиентам писем по электронной почте, текстовых SMS-сообщений на номера мобильных телефонов Клиентов, зафиксированных в автоматизированных банковских системах Банка на основании соответствующих заявлений Клиентов;
- путем направления (размещения) информации посредством Системы ДБО.

Изменения становятся обязательными для Банка и Клиента с момента размещения Банком указанных изменений. Использование Системы после утверждения Банком измененных Правил и (или) Тарифов означает согласие Клиента на их применение. Моментом ознакомления Клиента с информацией об изменении Договора и (или) Тарифов считается момент, с которого информация доступна для Клиентов. Банк не несет ответственность, если размещенная информация не была получена, и (или) не была изучена, и (или) была неправильно понята Клиентом.

Банк не несет ответственности, если информация об изменении и (или) дополнении Правил и (или) Тарифов на услуги, опубликованная в порядке и в сроки, установленные Правилами, не была получена и/или изучена и/или правильно истолкована Клиентом.

В случае несогласия Клиента с изменениями и (или) дополнениями, внесенными Банком в Правила или Тарифы, новой редакцией Правил, Клиент имеет право расторгнуть Договор в порядке, предусмотренном [разделом 11](#) настоящих Правил.

2.16. Банк принимает Электронные документы Клиента в случае их соответствия условиям договора, заключенного между Банком и Клиентом, в рамках действия которого применяются указанные Электронные документы, действующему законодательству Российской Федерации, внутренним нормативным документам Банка, условиям настоящих Правил, ежедневно в круглосуточном режиме, за исключением:

- технологических временных интервалов, связанных с завершением и (или) открытием текущего Операционного дня;
- случаев приостановления или прекращения использования Клиентом Системы ДБО, предусмотренных законодательством Российской Федерации и настоящими Правилами;
- перерывов в работе Системы ДБО по техническим причинам - в случае возникновения проблем технического характера и (или) проведения Банком технических работ, необходимых для обеспечения надлежащего функционирования Системы ДБО (в указанных случаях Клиент уведомляется Банком путем оповещения в Системе ДБО в процессе попытки совершения операции (действия), а также в разделе уведомлений Системы ДБО.

Принятые Банком Распоряжения и иные Электронные документы Клиента исполняются не позднее Операционного дня, следующего за днем их поступления. В случае необходимости представления Клиентом подтверждающих документов, требуемых для исполнения Распоряжения в соответствии с законодательством Российской Федерации, Банк исполняет распоряжение Клиента не позднее Операционного дня, следующего за днем представления указанных документов.

2.17. В случае обмена Электронными документами между Банком и Клиентом в целях заключения, изменения, расторжения договора, в том числе, но не исключительно, в

офертно-акцептной форме, данный договор считается заключенным, измененным, расторгнутым с даты, указанной в соответствующем подтверждении заключения, изменения, расторжения договора, направляемом Банком Клиенту.

2.18. Банк информирует Клиента о совершении каждой операции с использованием Системы ДБО, в том числе об этапах приема, контроля и прохождения ЭД, посредством создания и изменения в клиентской части Системы ДБО комплекса статусов, автоматически присваиваемых таким операциям и отражающих ход их исполнения Банком.

Клиент обязан не реже чем раз в 7 (семь) дней проверять состояние счета посредством Системы ДБО. Уведомление о совершении каждой операции по Счету считается полученным Клиентом с момента изменения в клиентской части Системы ДБО комплекса статусов.

2.19. Банк обеспечивает возможность направления ему Клиентом уведомления об использовании Системы ДБО без согласия Клиента (компрометации).

2.20. Банк фиксирует направленные Клиенту и полученные от Клиента уведомления, а также хранит соответствующую информацию не менее трех лет.

2.21. Банк предоставляет Клиенту документы и информацию, которые связаны с использованием Клиентом его электронного средства платежа, в порядке, установленном Правилами.

2.22. Банк рассматривает заявления Клиента, в том числе при возникновении споров, связанных с использованием Клиентом Системы ДБО, а также предоставляет Клиенту возможность получать информацию о результатах рассмотрения заявлений, в том числе в письменной форме по требованию Клиента, в срок, установленный договором, но не более 30 дней со дня получения таких заявлений, а также не более 60 дней со дня получения заявлений в случае использования Системы ДБО для осуществления трансграничного перевода денежных средств.

2.23. Использование Клиентом Системы ДБО может быть приостановлено или прекращено Банком на основании полученного от Клиента уведомления или по инициативе Банка при нарушении Клиентом порядка использования электронного средства платежа в соответствии с договором.

2.24. В случаях выявления Банком операций, соответствующих признакам осуществления перевода денежных средств без согласия Клиента, Банк приостанавливает использование Клиентом Системы ДБО в целях составления, удостоверения и передачи Клиентом Распоряжений в Банк. При получении от Клиента подтверждения возобновления исполнения распоряжения, Банк незамедлительно возобновляет использование клиентом Системы ДБО в целях составления, удостоверения и передачи Клиентом Распоряжения в Банк. При неполучении от Клиента подтверждения возобновления исполнения распоряжения, Банк возобновляет использование Клиентом Системы ДБО по истечении двух рабочих дней после дня приостановления использования Клиентом Системы ДБО.

2.25. При приостановлении или прекращении использования Клиентом Системы ДБО в случаях, предусмотренных Федеральным законом №161-ФЗ, Банк в день такого приостановления или прекращения в порядке, установленном Правилами, предоставляет Клиенту информацию о приостановлении или прекращении использования Системы ДБО с указанием причины такого приостановления или прекращения.

2.26. Приостановление или прекращение использования Клиентом Системы ДБО не прекращает обязательств Клиента и Банка, возникших до момента приостановления или прекращения указанного использования.

2.27. В случае утраты средств аутентификации Системы ДБО либо использования Системы ДБО без согласия Клиента, Клиент обязан направить соответствующее уведомление Банку незамедлительно после обнаружения факта утраты средств аутентификации Системы ДБО и (или) использования Системы ДБО без согласия Клиента, но не позднее дня, следующего за днем получения от Банка уведомления о совершенной операции.

2.28. Банк в случае получения от налогового органа сведений о снятии физического лица с учета в налоговых органах в связи со смертью прекращает исполнение Распоряжений о перечислении соответствующих сумм со Счета Клиента - индивидуального предпринимателя или физического лица, занимающегося в установленном законодательством Российской Федерации порядке частной практикой, за исключением завещательных распоряжений, иных распоряжений в случаях, предусмотренных законодательством Российской Федерации, а также распоряжений, возможность исполнения которых подтверждена получателю денежных

средств и (или) обслуживающему его банку в соответствии с законодательством Российской Федерации, банковскими правилами и договором, если такое подтверждение представлено до получения Банком сведений о снятии физического лица с учета в налоговых органах в связи со смертью.

2.29. В отношении условий, не урегулированных настоящими Правилами, Стороны руководствуются соответствующими договорами, заключенными между Банком и Клиентом, и законодательством Российской Федерации.

2.30. В случае участия Клиента в отдельных фокус-группах с целью использования Системы ДБО в режиме опытного использования, либо опытного использования отдельного функционала Системы ДБО, устанавливаемого Банком, если ни одна из Сторон не заявит обратное до завершения периода использования Системы ДБО/части функционала Системы ДБО в режиме опытного использования, все правоотношения между Банком и Клиентом, возникшие вследствие волеизъявлений об использовании Системы ДБО/ части функционала Системы ДБО в режиме опытного использования продолжают действие после завершения периода использования Системы ДБО/ части функционала Системы ДБО в режиме опытного использования и ввода Системы ДБО и (или) отдельной функциональности Системы ДБО в промышленную эксплуатацию, продолжают свое действие и определяются в дальнейшем действующими правилами использования Системы ДБО, публикуемых Банком.

3. ПОРЯДОК ОСУЩЕСТВЛЕНИЯ ПЕРЕВОДОВ С ИСПОЛЬЗОВАНИЕМ СИСТЕМЫ ДБО

3.1. Банк осуществляет перевод денежных средств по Распоряжению Клиента, оформленному в рамках применяемой формы безналичных расчетов.

3.2. Перевод денежных средств осуществляется за счет денежных средств Клиента, находящихся на его банковском счете, либо за счет средств Банка в случаях, когда в соответствии с договором банковского счета Банк осуществляет платежи со счета несмотря на отсутствие денежных средств (кредитование счета).

3.3. Перевод денежных средств осуществляется Банком в рамках применяемых форм безналичных расчетов посредством зачисления денежных средств на банковский счет получателя средств.

3.4. Если иное не обусловлено применяемой формой безналичных расчетов или федеральным законом, безотзывность перевода денежных средств, наступает с момента списания денежных средств с банковского счета плательщика.

Безотзывность перевода денежных средств на единый казначейский счет наступает с момента представления плательщиком в Банк распоряжения о переводе денежных средств при условии достаточности денежных средств для его исполнения.

Распоряжение Клиента может быть отозвано Клиентом до наступления безотзывности перевода денежных средств в порядке, предусмотренном законодательством Российской Федерации и Правилами, посредством создания в Системе ДБО соответствующего запроса на отзыв распоряжения.

3.5. Безусловность перевода денежных средств наступает в момент выполнения определенных Клиентом и (или) получателем средств либо иными лицами условий осуществления перевода денежных средств, в том числе осуществления встречного перевода денежных средств в иной валюте, встречной передачи ценных бумаг, представления документов, либо при отсутствии указанных условий.

3.6. В случае если Клиента (плательщика средств) и получателя средств обслуживает Банк, окончательность перевода денежных средств, наступает в момент зачисления денежных средств на банковский счет получателя средств или обеспечения получателю средств возможности получения наличных денежных средств.

3.7. В случае если Клиента (плательщика средств) и получателя средств обслуживают разные операторы по переводу денежных средств, окончательность перевода денежных средств наступает в момент зачисления денежных средств на банковский счет оператора по переводу денежных средств, обслуживающего получателя средств, с учетом требований статьи 25 Федерального закона №161-ФЗ.

3.8. При переводе денежных средств обязательство Банка перед Клиентом (плательщиком) прекращается в момент наступления его окончательности.

3.9. Банк до осуществления перевода денежных средств предоставляет Клиентам возможность ознакомления в доступной для них форме с условиями осуществления перевода денежных средств в рамках применяемой формы безналичных расчетов, в том числе:

1) с размером вознаграждения и порядком его взимания в случае, если оно предусмотрено договором;

2) со способом определения обменного курса, применяемого при осуществлении перевода денежных средств в иностранной валюте (при различии валюты денежных средств, предоставленных плательщиком, и валюты переводимых денежных средств);

3) с порядком предъявления претензий, включая информацию для связи с оператором по переводу денежных средств;

4) с иной информацией, обусловленной применяемой формой безналичных расчетов.

Распоряжение Клиента должно содержать информацию, позволяющую осуществить перевод денежных средств в рамках применяемых форм безналичных расчетов (далее - реквизиты перевода). Перечень реквизитов перевода устанавливается нормативными актами Банка России, Министерством финансов Российской Федерации по согласованию с Банком России (в части перечня реквизитов перевода, кодирования реквизитов перевода, необходимых для учета поступления платежей, являющихся источниками формирования доходов бюджетов бюджетной системы Российской Федерации, иных платежей, поступающих на счета органов Федерального казначейства, и платежей за выполнение работ, оказание услуг бюджетными и автономными учреждениями). За правильное заполнение платежных и иных реквизитов документа несет ответственность Клиент.

3.10. Распоряжение Клиента, составленное и удостоверенное с использованием Системы ДБО, передается, принимается к исполнению, исполняется и хранится в электронном виде.

3.11. Банк вправе составить распоряжение от своего имени для исполнения Распоряжения Клиента.

3.12. При приеме к исполнению Распоряжения Клиента Банк осуществляет все необходимые процедуры приема Распоряжения к исполнению, предусмотренные законодательством Российской Федерации, в том числе удостоверяется права распоряжения денежными средствами, проверяет реквизиты перевода, целостность распоряжения, достаточность денежных средств для исполнения распоряжения, а также выполняет иные процедуры приема к исполнению распоряжений клиентов, предусмотренные законодательством Российской Федерации.

Банк не принимает к исполнению Распоряжение при отрицательных результатах процедур контроля при приеме к исполнению распоряжений установленных действующим законодательством Российской Федерации и направляет Клиенту уведомление об этом не позднее дня, следующего за днем получения распоряжения Клиента, в порядке, определенном настоящими Правилами.

3.13. Распоряжения, прошедшие все процедуры приема к исполнению, исполняются Банком не позднее рабочего дня, следующего за днем поступления в Банк соответствующего Распоряжения, если иной срок не предусмотрен законом, изданными в соответствии с ним банковскими правилами или договором, заключенным между Клиентом и Банком. Перевод денежных средств осуществляется Банком в срок не более трех рабочих дней начиная со дня списания денежных средств с банковского счета Клиента.

3.14. Банк при выявлении операции, соответствующей признакам осуществления перевода денежных средств без согласия Клиента, до осуществления списания денежных средств с банковского счета Клиента на срок не более двух рабочих дней приостанавливает исполнение Распоряжения о совершении операции, соответствующей признакам осуществления перевода денежных средств без согласия Клиента.

Банк после выполнения действий, указанных в настоящем пункте, в порядке, установленном настоящими Правилами:

1) предоставляет Клиенту информацию:

а) о совершении им действий, предусмотренных абзацем 1 настоящего пункта;

б) о рекомендациях по снижению рисков повторного осуществления перевода денежных средств без согласия Клиента;

2) незамедлительно запрашивает у Клиента подтверждение возобновления исполнения Распоряжения.

При получении от Клиента подтверждения, Банк незамедлительно возобновляет исполнение Распоряжения. При неполучении от Клиента подтверждения, указанного в настоящем пункте, Банк возобновляет исполнение распоряжения по истечении двух рабочих дней после дня совершения им действий по приостановлению исполнения Распоряжения.

3.15. Достаточность денежных средств, находящихся на банковском счете Клиента, для исполнения его Распоряжения определяется Банком в порядке, установленном нормативными актами Банка России. При недостаточности денежных средств, находящихся на банковском счете Клиента, Банк не принимает распоряжение клиента к исполнению, если иное не предусмотрено законодательством Российской Федерации и договором, а также направляет Клиенту уведомление об этом не позднее дня, следующего за днем получения распоряжения клиента в порядке, определенном настоящими Правилами.

3.16. Прием распоряжения Клиента к исполнению подтверждается Банком Клиенту в порядке, определенном настоящими Правилами.

3.17. Распоряжение Клиента исполняется Банком в рамках применяемых форм безналичных расчетов в размере суммы, указанной в распоряжении Клиента. Вознаграждение Банка (при его взимании) не удерживается из суммы перевода денежных средств, за исключением случаев осуществления трансграничных переводов денежных средств.

3.18. Исполнение Распоряжения Клиента подтверждается Банком Клиенту в порядке, предусмотренном настоящими Правилами.

3.19. Положения настоящего раздела применяются также в случае составления Банком распоряжений от своего имени в целях исполнения распоряжений Клиентов в рамках применяемых форм безналичных расчетов с учетом особенностей, предусмотренных законодательством Российской Федерации.

3.20. Списание средств со Счета плательщика и зачисление средств на Счет получателя осуществляется программным способом в соответствии со значениями цифровых реквизитов плательщика и получателя в Распоряжении (БИК кредитной организации, обслуживающей плательщика либо получателя, номер корреспондентского счета кредитной организации, обслуживающей плательщика либо получателя, номер лицевого счета плательщика либо получателя). Указанные операции выполняются независимо от значений (содержания) текстовых реквизитов Распоряжения (наименования плательщика либо получателя, назначения платежа). Претензии, возникающие при неверном зачислении средств на Счета получателей из-за несоответствия цифровых и текстовых реквизитов, должны регулироваться между плательщиком и получателем непосредственно, минуя Банк.

3.21. Банк возмещает Клиенту сумму операции, совершенной с использованием Системы ДБО, в случаях, если:

- Банк получил от Клиента уведомление о факте утраты средств аутентификации Системы ДБО, и (или) использовании Системы ДБО без согласия Клиента, и операция с использованием Системы ДБО совершена после получения Банком указанного уведомления - при условии признания такой операции совершенной без согласия Клиента;
- Банк не проинформировал Клиента о совершении операции с использованием Системы ДБО в соответствии с Правилами - при условии признания такой операции совершенной без согласия Клиента, за исключением случаев, когда информирование не было осуществлено по причинам, не зависящим от Банка, и (или) если Клиент своевременно не воспользовался способами получения указанной информации от Банка, предусмотренными Правилами;
- Банк проинформировал Клиента о совершении операции с использованием Системы ДБО, и Клиент направил Банку уведомление об утрате средств аутентификации Системы ДБО, и (или) использовании Системы ДБО без его согласия незамедлительно после обнаружения факта утраты и (или) неправомерного использования Системы ДБО, но не позднее дня, следующего за днем информирования Банком о совершенной операции, - за исключением случая, когда причиной совершения операции без согласия Клиента является доказанное Банком нарушение Клиентом порядка использования Системы ДБО, установленного Правилами.

Признание операции совершенной без согласия Клиента осуществляется Банком по итогам претензионной работы, проведенной в соответствии с требованиями внутренних нормативных документов Банка и законодательства Российской Федерации.

4. ПРАВА И ОБЯЗАННОСТИ СТОРОН

4.1. Банк вправе:

4.1.1. В одностороннем порядке вносить изменения в функционал Системы ДБО, в том числе в связи с обновлением пользовательского интерфейса, аппаратных и (или) программных составляющих Системы ДБО, в том числе внедрять новые программные решения для предоставления услуг ДБО и (или) формирования средств ЭП и осуществлять перевод на них Клиентов.

4.1.2. В одностороннем порядке определять (изменять, дополнять) перечень доступной функциональности Системы ДБО в части перечня доступных Клиенту услуг в различных Системах ДБО и (или) различных пользовательских интерфейсах (web-интерфейс, Мобильное приложение, в том числе в Мобильных приложениях, разрабатываемых для различных операционных систем), заключать и расторгать договоры с Удостоверяющими центрами в целях выпуска и использования УЭП для работы в Системе ДБО.

4.1.3. Отказать в приеме Электронных документов Клиента, формат и (или) оформление которых не соответствует требованиям законодательства Российской Федерации и (или) Системы ДБО.

4.1.4. Отказать в исполнении Распоряжения при наличии у Банка подозрений о том, что данная операция совершается в целях легализации (отмыванию) доходов, полученных преступным путем, финансированию терроризма и финансированию распространения оружия массового уничтожения", а также в совершении операции, по которой Клиентом не представлены документы, необходимые для фиксации информации в соответствии с положениями федерального закона от 07.08.2001 № 115-ФЗ "О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма".

4.1.5. Осуществлять без распоряжений Клиента (в порядке заранее данного акцепта) безналичное списание денежных средств с любого из Счетов Клиента в целях оплаты комиссионного вознаграждения Банка в соответствии с Тарифами.

4.1.6. Приостановить обслуживание Клиента с использованием Системы в случае неоплаты Клиентом комиссионного вознаграждения Банка (отсутствия денежных средств для оплаты комиссионного вознаграждения на Счете(-ах) Клиента) в соответствии с Тарифами. Банк возобновляет обслуживание Клиента с использованием Системы не позднее следующего рабочего дня после поступления в Банк указанной оплаты.

4.1.7. Приостановить или прекратить обслуживание Клиента с использованием Системы ДБО при наличии у Банка сведений о введении в отношении Клиента арбитражным судом процедуры, применяемой в деле о банкротстве, в соответствии с требованиями федерального закона от 26.10.2002 г. № 127-ФЗ "О несостоятельности (банкротстве)".

4.1.8. Требовать от Клиента в рамках мероприятий по реализации положений Федерального закона от 07.08.2001 № 115-ФЗ "О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма" предоставления в срок, указанный Банком, документов, связанных с проведением Клиентом банковских операций и подтверждающих их действительность и экономическую обоснованность (в т.ч. заверенные надлежащим образом копии договоров, на основании которых производится перевод денежных средств, счетов-фактур, спецификаций и др.), а также копий документов, заверенных надлежащим образом, содержащих сведения о выгодоприобретателях и бенефициарных владельцах Клиента.

4.1.9. Приостановить или прекратить обслуживание Клиента с использованием Системы ДБО при наличии у Банка подозрений о неисполнении клиентом обязанности по выполнению требований действующего законодательства, в том числе положений федерального закона от 07.08.2001 № 115-ФЗ "О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма".

4.1.10. Приостановить обслуживание Клиента с использованием Системы ДБО в случае наличия у Банка информации об арестах денежных средств на Счетах Клиента, приостановлениях операций по Счетам Клиента, наложенных уполномоченными органами.

4.1.11. Приостановить обслуживание Клиента с использованием Системы ДБО при наличии у Банка информации об истечении срока полномочий Уполномоченного лица Клиента до

момента предоставления Клиентом в Банк документального подтверждения продления указанных полномочий либо наделения полномочиями иного лица.

4.1.12. Приостановить или прекратить использование Клиентом Системы ДБО как электронного средства платежа в случае нарушения Клиентом порядка использования Системы ДБО, установленного Договором ДБО.

4.1.13. Проводить в установленном в Банке порядке служебное расследование ставшего известным факта несанкционированного доступа к счету Клиента, в том числе в результате компрометации одноразового кода, с привлечением Клиента; привлекать к экспертизе третьих лиц (представителей удостоверяющего центра, разработчика и (или) лица, обеспечивающего работоспособность Системы ДБО) при проведении технической экспертизы в случаях возникновения спорной ситуации, связанной с отказом Клиента от авторства или содержания Электронного документа или связанной с отказом Банка от факта приема или исполнения Электронного документа. Порядок проведения экспертизы устанавливается определен в [разделе 10](#) Правил.

4.1.14. В одностороннем порядке приостановить работу с Клиентом через Систему ДБО в случае возникновения у Банка технических неисправностей или других обстоятельств, препятствующих использованию Системы ДБО, до момента устранения неисправностей. Все платежные документы в этом случае принимаются от Клиента на бумажных носителях в порядке, установленном договором банковского счета, заключенном между Банком и Клиентом.

4.1.15. При наличии у Банка сомнений в подлинности (аутентичности) платежного документа, поступившего с использованием Системы ДБО, направить письменный запрос Клиенту (с курьером/ посредством факсимильной связи/ по Системе ДБО) или провести переговоры с Клиентом по телефону о подтверждении подлинности документа. В случае подтверждения Клиентом подлинности платежного документа, Банк выполняет операцию по нему не позднее банковского дня, следующего за днем получения Банком платежного документа.

4.1.16. Приостановить или прекратить использование Клиентом Системы ДБО в случаях выявления фактов Компрометации и (или) получения несанкционированного доступа к Системе ДБО третьих лиц.

4.1.17. Приостановить использование Клиентом Системы ДБО в случае поступления информации о зачислении на банковский счет Клиента денежных средств, списанных в результате несанкционированного доступа к счетам третьих лиц в Банке или в других кредитных организациях и совершения переводов без согласия клиентов.

4.1.18. Приостановить или прекратить обслуживание Клиента в Системе ДБО в одностороннем порядке в случае неисполнения Клиентом обязательств по замене Ключей УЭП в течение 2 (Двух) месяцев и более при условии отсутствия иных действующих сертификатов ключа проверки ЭП, либо средств электронной подписи ПЭП.

4.1.19. Приостановить или ограничить доступ Клиента к средствам электронной подписи (в т.ч. PayControl) или отключить возможность использования ПЭП для целей подтверждения ЭД при наличии у Банка оснований считать, что по используемому Клиентом каналу доступа возможна попытка несанкционированного доступа от имени Клиента или в иных случаях по усмотрению Банка, либо в случае выявления Банком неактуальных контактных данных и сведений об Уполномоченных лицах/Пользователях, ранее предоставленных Клиентом Банку.

4.1.20. Осуществлять сбор информации о мобильных устройствах, на которых установлены Мобильное приложение PayControl и (или) Мобильное приложение Системы ДБО для целей противодействия угрозам информационной безопасности, включая сведения о геолокации, информации об устройстве, информации о подключении к сети, событиях, происходящих в мобильном приложении PayControl, обнаружении потенциально вредоносного программного обеспечения.

4.1.21. Приостановить и (или) прекратить доступа к Системе ДБО в случаях, указанных в Правилах, без предварительного уведомления Клиента (Уполномоченного лица, Пользователя), за исключением случаев, когда требование направления соответствующего уведомления определено действующим законодательством Российской Федерации.

4.2. Банк обязуется:

- 4.2.1. Принимать и обрабатывать полученные по Системе ДБО Электронные документы (пакеты Электронных документов), оформленные в соответствии с настоящими Правилами.
- 4.2.2. Информировать Клиента о совершении каждой операции с использованием Системы ДБО, в том числе об этапах приема, контроля и прохождения ЭД, посредством создания и изменения в клиентской части Системы ДБО комплекса статусов, автоматически присваиваемых таким операциям и отражающих ход их исполнения Банком.
- 4.2.3. Не позднее Операционного дня, следующего за днем проведения операции, при получении запроса от Клиента предоставить Клиенту возможность формирования выписок по Счету(-ам) в электронном виде.
- 4.2.4. Незамедлительно прекратить прием Электронных документов в случае поступления в Банк соответствующего требования Клиента.
- 4.2.5. В течение не более чем 3 (трех) банковских дней с момента получения письменного запроса от Клиента предоставить копии платежных документов на бумажном носителе по операциям, выполненным Банком по Счетам Клиента с использованием Системы.
- 4.2.6. Уведомить Клиента (Представителя Клиента) о приостановлении или прекращении использования Клиентом Системы ДБО в случаях, указанных в п. 2.23 и п. 2.24 Правил, в день такого приостановления или прекращения доступным способом в соответствии с имеющейся у Банка информацией для связи с Клиентом, с указанием причины такого приостановления или прекращения.
- 4.2.7. Возобновить использование Клиентом Системы ДБО, приостановленное Банком в случае, указанном в п.2.24 Правил, незамедлительно в случае получения от Клиента подтверждения исполнения операции, до истечения 2 (двух) рабочих дней после дня приостановления использования Клиентом Системы ДБО по инициативе Банка, а в случае неполучения указанного подтверждения - по истечении 2 (двух) рабочих дней после дня приостановления использования Системы ДБО.
- 4.2.8. Фиксировать направленные Клиенту и полученные от Клиента уведомления, связанные и (или) направленные с использованием Системы ДБО, а также хранить соответствующую информацию не менее 3 (трех) лет.
- 4.2.9. Консультировать представителей Клиента по работе в Системе ДБО и использования СКЗИ в период операционного обслуживания Клиентов.
- 4.2.10. Обеспечивать защиту информации в Системе ДБО от несанкционированного доступа посредством принятия следующих мер:
- Сохранение конфиденциальности и подлинности используемых ключей ЭП, паролей и одноразовых кодов;
 - Протоколирование всех случаев и попыток нарушения безопасности Системы ДБО и принятие всех возможных мер для предотвращения и ликвидации их последствий вплоть до приостановления функционирования Системы ДБО;
 - Обеспечение сохранности и конфиденциальности информации, доверенной ему Клиентом в рамках Договора ДБО, в соответствии с действующим законодательством.
- 4.2.11. Соблюдать положения законодательных документов Российской Федерации, нормативных документов Банка России, регламентирующих функционирование Системы, а также настоящих Правил.
- 4.2.12. Предоставлять Клиенту новые версии программного обеспечения Системы ДБО в случае их замены без дополнительной оплаты, а также консультировать Клиента по телефону в случаях сбоев используемой Клиентом Системы ДБО в целях устранения последствий сбоев и восстановления нормального функционирования Системы ДБО.
- 4.2.13. Предоставить Уполномоченным лицам Клиента права доступа к Системе ДБО в соответствии с предоставленными правами не позднее следующего рабочего дня после получения от Клиента необходимых документов.
- 4.2.14. При получении от Клиента письменной информации об ошибочном списании со Счета Клиента в Банке, либо случае совершения перевода денежных средств без согласия клиента, осуществленного в результате несанкционированного доступа к банковскому счету Клиента, информировать банк-корреспондент о списании денежных средств Клиента с предложением (просьбой) оказать содействие по возврату денежных средств (как ошибочно перечисленных, необоснованно списанных при несанкционированном доступе к счету).

4.2.15. В установленном в Банке порядке провести служебное расследование ставшего известным факта несанкционированного доступа к счету Клиента, в том числе в результате компрометации Кода подтверждения, с привлечением Клиента, проинформировать Клиента о результатах расследования.

4.2.16. В целях противодействия осуществлению переводов денежных средств без согласия Клиента установить ограничения на осуществление операций клиентами либо ограничения максимальной суммы одной операции и (или) операций за определенный период времени, а также установить ограничения на подключение к Системе ДБО по сетевым адресам при получении соответствующего заявления Клиента.

4.3. Клиент вправе:

4.3.1. В любой момент в рамках действия настоящего Договора изменить используемый способ Аутентификации, обратившись в подразделение Банка с заявлением об изменении средств доступа к Системе ДБО по форме Банка.

4.3.2. Обратиться в Банк с целью приостановления или прекращения его работы в Системе ДБО.

4.3.3. В рамках обмена ЭД и информацией в Системе ДБО на основании Договора ДБО обратиться в Банк с целью оспаривания авторства и (или) содержания ЭД.

4.3.4. Взаимодействовать с Банком в ходе расследования факта несанкционированного доступа к счету Клиента, получать от Банка информацию о результатах расследования.

4.3.5. Вносить изменения в перечень Уполномоченных лиц и (или) состав их полномочий путем предоставления в подразделение Банка заявления об изменении полномочий по форме Банка.

4.3.6. В случае невозможности направления в Банк платежных документов посредством Системы ДБО по причине технического сбоя, действия непреодолимой силы, влияющей на функционирование Системы ДБО, представить в Банк платежные документы на бумажных носителях, заверенные собственноручными подписями Уполномоченных лиц Клиента и оттиском печати Клиента (при использовании печати) в соответствии с карточкой с образцами подписей и оттиска печати.

4.3.7. В случае Компрометации либо утраты Логина, Пароля получить новые Логин, Пароль для работы в Системе ДБО, обратившись в Банк с заявлением об изменении средств доступа к Системе ДБО на бумажном носителе в подразделение Банка, либо посредством системы электронного документооборота, заверенное усиленной квалифицированной подписью единоличного исполнительного органа Клиента – юридического лица, либо лично Клиентом – индивидуальным предпринимателем или физических лиц, занимающихся в установленном законодательством Российской Федерации порядке частной практикой.

4.3.8. В целях противодействия осуществлению переводов денежных средств без согласия Клиента направить в Банк заявление об установлении ограничения на осуществление операций клиентами либо ограничения максимальной суммы одной операции и (или) операций за определенный период времени, а также об установлении ограничения на подключение к Системе ДБО по сетевым адресам.

4.3.9. Взаимодействовать с Банком в ходе расследования факта несанкционированного доступа к счету Клиента, получать от Банка информацию о результатах расследования.

4.4. Клиент обязуется:

4.4.1. Представить Банку материалы и информацию, необходимые для подключения к Системе ДБО.

4.4.2. Назначить и наделить необходимыми полномочиями лиц, имеющих право работать с Системой ДБО и средствами ЭП.

4.4.3. Строго соблюдать предусмотренные настоящими Правилами требования к подготовке и передаче ЭД.

4.4.4. Самостоятельно контролировать и расставлять приоритеты платежей в соответствии с требованиями действующего законодательства Российской Федерации. Банк не контролирует правильность расстановки приоритетов. При недостаточности денежных средств на Счете

Клиента в каждом приоритете платежные поручения исполняются в порядке возрастания их номеров.

4.4.5. В случае работы в Системе ДБО с использованием Сертификата, размещенного на Смарт-ключе, назначить лиц, ответственных за сохранность физических носителей ключей ЭП и принять меры для обеспечения их безопасного хранения, хранить Смарт-ключ в надежном месте, исключая его повреждение, а также доступ к нему лиц, не имеющих соответствующих полномочий.

4.4.6. Незамедлительно уведомить Банк в случае несанкционированного доступа к счету и списания денежных средств и (или) Компрометации, в том числе возникновения угрозы использования (копирования) Ключа ЭП и (или) угрозы доступа к Системе с использованием Ключа ЭП лицами, не имеющими соответствующих полномочий, либо Уполномоченными лицами в противозаконных целях; утери Смарт-ключа; прекращения полномочий Уполномоченного лица, имеющего право на использование Ключа ЭП; утраты Логина и (или) Пароля; изменении Зарегистрированного номера телефона; ошибок в работе Системы, в том числе возникающих в связи с попытками нарушения информационной безопасности.

Бремя доказывания надлежащего исполнения обязательств по обеспечению сохранности и конфиденциальности средств ЭП, средств Аутентификации и недопущению Компрометации, несанкционированного доступа третьих лиц, предусмотренных Правилами, возлагается на Клиента.

4.4.7. Обеспечивать все возможные меры для предотвращения несанкционированного доступа к Системе ДБО и (или) Компрометации, соблюдать конфиденциальность информации, касающейся Системы, в том числе в случае работы в Системе с использованием Логина и Пароля обеспечивать хранение и использование Логина, Пароля, Кодов подтверждения способом, исключая доступ к указанным Средствам аутентификации лиц, не имеющих соответствующих полномочий, а также защиту от несанкционированного доступа третьих лиц к компьютеру, мобильному устройству, иному устройству, посредством которого осуществляется работа в Системе ДБО, обеспечить сохранность и недоступность третьим лицам мобильных устройств с установленным Мобильным приложением, приложением PayControl, а также мобильных устройств и (или) SIM-карт, номера которых зарегистрированы в Банке для целей получения Кода подтверждения кода в виде SMS сообщения (Зарегистрированный номер), а при работе в Системе ДБО с использованием УЭП - обеспечить соблюдение порядка хранения защищенных носителей с ключевой информацией СКЗИ и условия хранения и использования программного обеспечения СКЗИ, исключая порчу и утрату защищенного носителя, а также их использование любыми другими лицами.

4.4.8. В случае Компрометации, утраты Логина и (или) Пароля, изменении Зарегистрированного номера телефона, утери мобильного устройства и (или) SIM-карты с Зарегистрированным номером, несанкционированного доступа третьих лиц к мобильному устройству или иному устройству, посредством которого осуществляется работа в Системе ДБО, осуществления операций по счетам Клиента без согласия Клиента, незамедлительно уведомить об этом Банк.

4.4.9. Своевременно оплачивать сумму комиссионного вознаграждения Банка в соответствии с Тарифами за оказание Банком Клиенту услуг с использованием Системы ДБО в рамках настоящих Правил, в том числе посредством обеспечения на банковском счете, открытом в Банке, суммы денежных средств в размере комиссии за сопровождение и обслуживание Системы ДБО в соответствии с Тарифами.

4.4.10. Предоставить Банку достоверную информацию для связи с Клиентом, а в случае ее изменения своевременно предоставить обновленную информацию.

4.4.11. Самостоятельно и своевременно отслеживать результаты совершения операций по Счетам путем проверки соответствующих статусов данных операций в клиентской части Системы ДБО. Клиент считается проинформированным о совершении операции по Счету с момента автоматического изменения в клиентской части Системы ДБО комплекса статусов в отношении указанной операции.

4.4.12. По первому требованию Банка представлять информацию, подтверждающую подлинность (аутентичность) платежного документа, направленного с использованием Системы ДБО (в том числе, предоставлять платежный документ, направленный с

использованием Системы ДБО, на бумажном носителе с подписями лиц, уполномоченных распоряжаться счетом, и оттиском печати Клиента (при наличии)).

4.4.13. Использовать предоставленные Банком средства Системы ДБО только для целей, определенных настоящими Правилами.

4.4.14. Использовать шифровальные (криптографические) средства (СКЗИ), предоставленные в целях работы в Система ДБО, только в Системе ДБО и только на территории Российской Федерации, без права их продажи или передачи каким-либо другим способом третьим лицам. Все исключительные права на программное обеспечение СКЗИ, его модификации и переводы сохраняются за правообладателем программного обеспечения.

4.4.15. В случае уведомления Банком Клиента о смене программного обеспечения и/или смене сертификатов ключей обеспечить меры для их своевременного получения и применения в соответствии с Правилами.

4.4.16. При использовании ПЭП PayControl в случае смены Мобильного устройства и/или Зарегистрированного номера телефона Клиент обязан обратиться в Банк для получения новых ключей ЭП PayControl.

4.4.17. Предоставлять информацию, необходимую для исполнения Банком требований Федерального закона от 07.08.2001 № 115-ФЗ "О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма", включая информацию о своих выгодоприобретателях и бенефициарных владельцах.

4.4.18. Уведомлять Банк о случаях и (или) попытках переводов денежных средств без согласия Клиента способами, определенными Правилами.

4.4.19. Не передавать третьим лицам и сохранять конфиденциальность информации, направленной Банком на Зарегистрированный номер телефона до момента ее применения.

4.4.20. Обеспечить доступы в помещения и к рабочим местам, с которых осуществляется работа в Системе ДБО с целью проведения расследования (экспертизы) участникам комиссии при разрешении споров, связанных с подтверждением авторства ЭД и (или) достоверности ЭП в Системе ДБО.

5. ПОРЯДОК РАБОТЫ В СИСТЕМЕ ДБО С ИСПОЛЬЗОВАНИЕМ УЭП

5.1. Доступ к Системе ДБО Клиенту (Уполномоченному лицу Клиента) предоставляется с момента первичного входа в Систему ДБО с момента активации Ключа УЭП.

5.2. При подключении Клиенту Системы ДБО с использованием УЭП доступ к Системе ДБО предоставляется с момента активации Ключа УЭП.

5.3. В целях получения доступа к Системе ДБО Клиент самостоятельно создает Ключ ЭП и Сертификат с использованием Системы ДБО, руководствуясь порядком создания Сертификата, приведенным на Сайте Банка (при наличии такой технологической возможности в программном решении Системы ДБО)³, либо обращается в Банк или аккредитованный Банком Удостоверяющий центр с целью изготовления и выдачи Сертификата⁴.

5.4. В процессе изготовления и выдачи Сертификата Банк/Удостоверяющий центр:

- осуществляет проверку документов, подтверждающих полномочия Клиента и (или) Уполномоченных лиц Клиента;
- инициирует выдачу Клиенту Сертификата для обмена Электронными документами с использованием Электронной подписи в соответствии с правилами Удостоверяющего центра;
- подписывает с Клиентом заявление на выдачу Сертификата и акт приема-передачи сертификата и Смарт-ключа по установленным формам.

³ Самостоятельная генерация ключей УЭП доступна в Системе ДБО на базе технологического комплекса дистанционного банковского обслуживания "Faktura.ru". Сертификаты изготавливаются и выдаются удостоверяющим центром "AUTHORITY". Банк от лица Удостоверяющего центра осуществляет проверку Клиентов, необходимую для создания Сертификата и регистрацию Сертификата в Системе.

⁴ Генерация ключей УЭП для Системы ДБО на базе технологического комплекса дистанционного банковского обслуживания Digital2Go осуществляется удостоверяющим центром ООО "Айтиком". Банк от лица Удостоверяющего центра осуществляет проверку Клиентов, необходимую для создания Сертификата.

5.5. Изготовление и передача Сертификата ключа проверки УЭП Клиенту подтверждает использование УЭП электронных документов и их шифрования и признание документов, подписанных УЭП Уполномоченных лиц Клиента юридически равнозначно получению документа на бумажном носителе, заверенного собственноручными подписями Уполномоченных лиц Клиента и оттиском печати Клиента (при использовании печати) в течение периода действия Ключей УЭП.

5.6. В рамках настоящих Правил Стороны (Участники Системы) признают, что:

5.6.1. созданный в единственном экземпляре в соответствии с настоящими Правилами Ключ ЭП Клиента (Уполномоченного лица Клиента) уникален, создание дубликата Ключа ЭП возможно только Клиентом (Уполномоченным лицом Клиента) при нарушении условий хранения и (или) использования Ключа ЭП, предусмотренных настоящими Правилами;

5.6.2. подделка ЭП, то есть создание корректной ЭП Электронного документа, невозможна без использования Ключа ЭП Участника;

5.6.3. при произвольном изменении Электронного документа, заверенного ЭП, подпись становится некорректной, то есть проверка подписи дает отрицательный результат, при этом Банк отказывает в приеме Электронных документов, подписанных такой ЭП.

5.7. Банк представляет Клиенту рекомендации по комплектации рабочего места техническими и программными средствами, а Клиент самостоятельно и за свой счет обеспечивает комплектование аппаратного обеспечения для работы программного комплекса Системы ДБО с использованием Ключей УЭП, предоставляет каналы связи и выделяет помещение, осуществляет настройку своего рабочего места, согласно требованиям настоящих Правил.

5.8. Для обеспечения защиты Системы ДБО от несанкционированного доступа используются средства криптографической защиты информации, сертифицированные ФСБ России - СКЗИ "КриптоПро CSP"⁵. Размещение и установка СКЗИ осуществляется в соответствии с требованиями эксплуатационной документации на СКЗИ. Техническое обслуживание сертифицированных ФСБ России шифровальных средств могут осуществлять только организации, имеющие соответствующие лицензии ФСБ.

5.9. Факты невыполнения Клиентом рекомендаций Банка по комплектации рабочего места техническими и программными средствами⁶, либо факты обнаружения в результате проверки неработоспособности (несовместимости (несовместимость) технических или программных средств, или низкое качество линий связи, которое явилось причиной неработоспособности Системы ДБО, являются основанием для применения Банком права на приостановление и (или) прекращение доступа Клиента к Системе ДБО и (или) расторжение Договора ДБО.

5.10. В целях противодействия получению несанкционированного доступа к Ключам УЭП, Ключи УЭП должны находиться только на защищенных носителях (Смарт-ключках/USB-токенах) у ответственных лиц и подлежать обязательному учету (к примеру, в специально выделенных для этих целей журналах).

5.11. Клиент назначает ответственных должностных лиц из числа сотрудников Клиента, ответственных за сохранность Ключей УЭП и имеющих право работать с Системой ДБО или из числа сотрудников сторонней организации, а также определяет порядок допуска в помещения, в которых размещены СКЗИ, с учетом специфики и условий функционирования конкретной структуры Клиента.

5.12. До наделения Уполномоченных лиц/Пользователей правами работы в Системе ДБО и до начала работы указанных лиц с Ключами УЭП/СКЗИ Клиент должен обеспечить ознакомление (обучение) указанных лиц с правилами пользования Ключами УЭП/СКЗИ, в том числе о возможных угрозах утечки секретной информации при ее обработке, передаче, хранении, методах и средствах защиты информации, эксплуатационной документацией и настоящими Правилами.

⁵ Устанавливается для Системы ДБО на базе технологического комплекса дистанционного банковского обслуживания Digital2Go.

⁶ Рекомендованный набор оборудования и программного обеспечения для использования Системы ДБО с использованием ключей УЭП - персональный компьютер со следующими характеристиками: доступом к сети Интернет; операционная система Microsoft Windows версии 7 и выше (при условии совместимости соответствующей версии ОС с сертифицированной версией СКЗИ); интернет-браузер Microsoft Internet Explorer версии 9.0 или выше; объем доступной памяти на жестком диске не менее 3 ГБ; наличие свободного USB-порта; установленное и работающее лицензионное антивирусное программное обеспечение.

5.13. Клиент обязан не допускать появления в персональном компьютере, с которого осуществляется доступ к Системе ДБО, компьютерных вирусов, программ-шпионов и других вредоносных программ для исключения несанкционированного перехвата ключевой информации и передачи ее третьим лицам. Для выполнения данного требования не рекомендуется с ЭВМ, с которой осуществляется доступ к Системе ДБО, осуществлять незащищенное подключение к сети Интернет и использовать электронную почту.

5.14. Системные блоки персональных компьютеров с СКЗИ должны быть оборудованы средствами контроля за их вскрытием.

5.15. Специальное оборудование, охрана и режим в помещениях, в которых размещены СКЗИ должны обеспечивать безопасность информации⁷, СКЗИ и ключей УЭП, сведение к минимуму возможности неконтролируемого доступа к СКЗИ, просмотра процедур работы с СКЗИ посторонними лицами. Порядок охраны таких помещений должен предусматривать периодический контроль технического состояния средств охранной и пожарной сигнализации и соблюдения режима охраны.

5.16. Для хранения носителей Ключей УЭП, нормативной и эксплуатационной документации, помещения обеспечиваются хранилищами (металлическими шкафами либо сейфами), оборудованными внутренними замками с двумя экземплярами ключей. Дубликаты ключей от хранилищ и входных дверей должны храниться в сейфе ответственного лица, назначаемого распорядительным документом Клиента.

5.17. Учет и хранение носителей Ключей УЭП осуществляется Владельцами УЭП. Хранение носителей Ключей УЭП допускается в одном хранилище с другими документами при условиях, исключающих их непреднамеренное уничтожение или иное, не предусмотренное правилами пользования СКЗИ, применение (к примеру, посредством помещения носителей Ключей УЭП в отдельные опечатываемые контейнеры – закрывающиеся пеналы, тубусы). В случае отсутствия индивидуального хранилища у Владельцев УЭП, Ключи УЭП по окончании сессии работы с Системой ДБО должны передаваться на хранение лицу, назначенному ответственным за их хранение.

5.18. Размещение (копирование, сохранение) ключей на незащищенном носителе и (или) в реестре операционной системы недопустимо. В случае размещения (копирования, сохранения) ключа на незащищенный носитель и (или) в реестре операционной системы, Клиент обязан выполнить внеплановую смену ключа и отозвать сертификат, сохраненный на незащищенный носитель, направив в Банк соответствующее заявление.

5.19. При транспортировке Ключей УЭП Клиентом должны быть обеспечены условия транспортировки, исключающие возможность физических повреждений и внешнего воздействия на записанную ключевую информацию.

5.20. Клиент, допустивший утрату контроля за носителем с ключевой информацией СКЗИ (Ключа УЭП), независимо от наличия или отсутствия сведений о его несанкционированном использовании, незамедлительно сообщает об этом УЦ и Банку и прекращает работу с использованием СКЗИ до момента регистрации и ввода в действие новых ключей. Вышедший из-под контроля защищенный носитель с ключевой информацией СКЗИ не подлежит дальнейшему использованию.

5.21. Клиент обязан обеспечивать замену Ключей УЭП до истечения срока действия Сертификата, и каждый раз при изменении состава Уполномоченных лиц/Пользователей – Владельцев Ключа УЭП.

6. ПОРЯДОК РАБОТЫ В СИСТЕМЕ ДБО С ИСПОЛЬЗОВАНИЕМ ЛОГИНА И ПАРОЛЯ

6.1. Доступ к Системе ДБО Клиенту (Уполномоченному лицу Клиента) предоставляется с момента первичного входа в Систему ДБО с использованием Логина и Временного пароля и (или) ПЭП, предоставляемого на Зарегистрированный номер телефона, в том числе PayControl.

⁷ В рамках настоящих Правил - состояние информации, информационных ресурсов и информационных систем, при котором с требуемой вероятностью обеспечивается защита информации (данных) от утечки, хищения, утраты, несанкционированного уничтожения, искажения, модификации (подделки), копирования, блокирования и т.п., и состояние защищенности информации, обрабатываемой средствами вычислительной техники или автоматизированной системы, от внутренних или внешних угроз.

6.2. Каждое Уполномоченное лицо/Пользователь Клиента может иметь только один уникальный Логин и Пароль, Зарегистрированный номер телефона для работы в Системе ДБО.

6.3. Для работы в Системе с использованием ПЭП Клиент (Представитель Клиента) обращается непосредственно в подразделение Банка и оформляет заявление на заключение Договора ДБО.

6.4. Банк предоставляет Клиенту (Уполномоченному лицу Клиента) Логин для доступа к Системе ДБО после заключения Договора ДБО. По заявлению Клиента Логин может быть направлен Клиенту по электронной почте. После подключения Клиента (Уполномоченному лицу Клиента) к Системе ДБО, Клиент получает на Зарегистрированный номер телефона SMS сообщение с одноразовым паролем для первичного входа в Систему ДБО (Временный пароль), который Клиент Уполномоченному лицу Клиента обязан использовать одноразовый пароль для первичного входа в Систему ДБО в течение 3 (Трех) календарных дней с даты получения SMS с одноразовым паролем.

6.5. С момента направления Банком Временного пароля/ Временных паролей Стороны признают, что получение Банком документа, подписанного ЭП Клиента, юридически равнозначно получению документа на бумажном носителе, заверенного собственноручными подписями Уполномоченных лиц Клиента и оттиском печати Клиента (при использовании печати).

6.6. При первичной Аутентификации с использованием Логина и Временного пароля каждому Уполномоченному лицу Клиента необходимо заменить Временный пароль на постоянный Пароль, сформированный Клиентом по своему усмотрению, с целью дальнейшего применения для Аутентификации в Системе.

6.7. Смена Логина и (или) Пароля Уполномоченного лица в случае их Компрометации либо утраты осуществляется на основании соответствующего заявления по форме, установленной Банком, оформленного и представленного в подразделение Банка Клиентом/ Представителем Клиента.

6.8. В случае изменения лица, уполномоченного подписывать ЭД ПЭП PayControl и/или мобильного устройства, Зарегистрированного номера телефона Уполномоченного лица (пользователя), Клиент предоставляет в Банк новое заявление о регистрации Уполномоченных лиц по форме Банка с уточненными данными и приложением документов, подтверждающих полномочия Уполномоченного лица (Пользователя).

6.9. Процедура контроля наличия в ЭД ПЭП обеспечивает наличие в созданном и (или) подписанном ЭД информации, указывающей на логин Уполномоченного лица Клиента, от имени которого был создан и подписан ЭД.

6.10. Порядок подписания ЭД и факт формирования ПЭП с использованием одноразовых кодов, направляемых с использованием SMS, подтверждается путем ввода Уполномоченным лицом Клиента одноразового кода, направленного на Зарегистрированный номер в виде SMS сообщения.

6.11. Одноразовый код для подтверждения факта формирования ПЭП генерируется в привязке к Зарегистрированному номеру и самому подтверждаемому ЭД. ЭД считается подписанным Клиентом (Уполномоченным лицом) в случае если одновременно выполняются следующие условия:

- установлен факт входа под логином Уполномоченного лица в Систему ДБО (с том числе в Мобильное приложение), предшествующий отправке ЭД в Банк;
- установлен факт отправления SMS сообщения с одноразовым кодом на Зарегистрированный номер Уполномоченного лица;
- установлен факт ввода одноразового кода для подтверждения факта формирования ЭП Уполномоченным лицом;
- отправленный Банком SMS сообщением одноразовый код совпадает с введенным Уполномоченным лицом в Систему кодом и время ввода не просрочено.

6.9. Пользователь Системы ДБО обязуется не допускать переполнение памяти мобильных устройств с Зарегистрированными номерами, что может стать препятствием для приема SMS-сообщений с одноразовыми кодами.

7. ПОРЯДОК РАБОТЫ В СИСТЕМЕ ДБО С ИСПОЛЬЗОВАНИЕМ ПЭП PAYCONTROL⁸

7.1. В рамках настоящего подраздела в дополнение к общему перечню терминов и определений, приведенных в [разделе 1](#) Правил, используются следующие определения и сокращения:

Ключ ЭП PayControl – уникальная последовательность данных, используемая для формирования ЭП документа Клиентом. Вырабатывается на Мобильном устройстве Клиента одновременно с Ключом проверки ЭП с использованием Средства ЭП PayControl при выполнении процедуры Активации, а также при плановой смене ключей ЭП. Однозначно соответствует Ключу проверки ЭП. Хранится на Мобильном устройстве Клиента и защищается средствами Мобильного приложения PayControl, средствами операционной системы и аппаратными средствами Мобильного устройства.

Ключ проверки ЭП PayControl – уникальная последовательность данных, служащая для проверки значения ЭП документа. Вырабатывается на Мобильном устройстве Клиента одновременно с Ключом ЭП с использованием Средства ЭП PayControl при выполнении процедуры Активации, а также при проведении плановой смены ключей ЭП. Однозначно соответствует Ключу ЭП. Хранится на Мобильном устройстве Клиента, а также передается на сервер PayControl, для целей обеспечения процедуры проверки ЭП.

Акт признания ключа проверки ЭП – электронный документ, подтверждающий принадлежность Ключа проверки ЭП PayControl владельцу.

Аутентификация входа PayControl – процедура проверки соответствия предъявленных Аутентификационных данных Аутентификационным данным, установленным при активации Мобильного приложения PayControl.

Мобильное приложение PayControl – мобильное приложение для операционных систем iOS и Android, разработанное ООО "СэйфТек" (SafeTech LTD), предназначенное для формирования ЭП.

7.2. Предоставление возможности работы в Системе ДБО Клиенту (Уполномоченному лицу Клиента) с использованием PayControl осуществляется в рамках работы в Системе ДБО с использованием Логина и Пароля в порядке, определенном в [разделе 6](#) Правил, после подписания со стороны Клиента Акта признания ключа проверки ЭП ПЭП PayControl, сформированного Уполномоченным лицом Клиента в Системе ДБО.

7.3. Подписание Акта признания Ключа проверки ЭП ПЭП PayControl осуществляется с использованием одноразовых кодов в виде SMS сообщений, формируемых и направляемых Банком по запросу Клиента на Зарегистрированный номер. Для подтверждения Аутентификации и совершения (подтверждения) операций, Клиент использует одноразовый код, содержащийся в SMS сообщении, правильность которого проверяется Банком.

7.4. Право на подписание Акта признания ключа проверки ЭП ПЭП PayControl может быть предоставлено только одному Уполномоченному лицу Клиента.

7.5. Банк осуществляет подключение и возможность получения доступа к Системе ДБО Уполномоченному лицу Клиента/Пользователям в рамках предоставленных им полномочий (прав) использования PayControl в срок не позднее следующего рабочего дня после получения соответствующего заявления по форме Банка и документов, подтверждающих соответствующие полномочия.

7.6. Для получения доступа к Системе ДБО Клиенту к использованию PayControl Уполномоченное лицо/Пользователь в обязательном порядке проходит процедуру активации Мобильного приложения PayControl, состоящую из следующих шагов по персонализации Уполномоченного лица/Пользователя:

- успешный ввод/передача в Мобильное приложение PayControl QR-кода/ключа инициализации;
- формирование в Мобильном приложении PayControl и регистрации на сервере PayControl набора уникальных признаков Мобильного устройства Клиента;
- создание Ключей ЭП в Мобильном приложении PayControl;

⁸ Применяется с 26.02.2024 для Системы ДБО на базе технологического комплекса дистанционного банковского обслуживания Digital2Go. Банк от лица Удостоверяющего центра осуществляет проверку Клиентов, необходимую для создания Сертификата и регистрацию Сертификата в Системе.

- регистрация Ключа проверки ЭП на сервере PayControl с целью дальнейшей проверки ЭП Клиента;
- создание Клиентом Пароля/TouchID/FaceID для дальнейшего использования в качестве аутентификационных данных для доступа к Ключу ЭП в Мобильном приложении PayControl.

7.7. ЭД Клиента, подписанный PayControl, считается подписанным с помощью Ключа ЭП, принадлежащего Клиенту, для которого Банком зарегистрирован Ключ проверки ЭП в Мобильном приложении PayControl и (или) подтвержден при помощи кода подтверждения, выработанного на симметричных ключах.

7.8. Порядок подписания ЭД в Мобильном приложении PayControl:

- Уполномоченное лицо (Пользователь) в интерфейсе Системы ДБО формирует ЭД в соответствии с установленными форматами и предоставленными полномочиями;
- Банк на основании созданного ЭД Уполномоченного лица (Пользователя) формирует и направляет Уполномоченному лицу (Пользователю), наделенному правом подписи с использованием ПЭП PayControl, электронное сообщение с шаблоном ЭД из Системы ДБО;
- После поступления Клиенту от Банка через Мобильное приложение PayControl электронного сообщения с шаблоном ЭД на мобильное устройство Клиента с Зарегистрированным номером телефона поступает PUSH-сообщение о необходимости подписания ЭД;
- Уполномоченное лицо (Пользователь) проходит Аутентификацию входа в Мобильном приложении PayControl с использованием ранее созданных аутентификационных данных для доступа к Ключу ЭП;
- В Мобильном приложении PayControl Клиент ознакомливается с Электронным сообщением Банка по шаблону ЭД;
- Клиенту предоставляется возможность подписать ЭД Средством ЭП PayControl или отклонить подписание посредством нажатия (активации) соответствующих активных полей (кнопок) в интерфейсе Мобильного приложения PayControl.
- В случае решения Клиента не подписывать ЭД, Клиент нажимает соответствующую кнопку для отклонения подписания ЭД, в этом случае ЭД не будет подписан ЭП и не будет направлен на исполнение в Банк.
- В случае решения Клиента подписывать ЭД, Клиент нажимает соответствующую кнопку для подтверждения подписания ЭД, в этом случае с помощью Мобильного приложения PayControl ЭД подписывается ЭП и направляется на исполнение в Банк.
- Банк выполняет проверку ЭП посредством проверки соответствия предъявленной ЭП данным документа, времени формирования ЭП и набору уникальных признаков Мобильного устройства с использованием Ключа проверки ЭП на сервере PayControl.

Если Клиент не подписал ЭД и не отклонил подписание ЭД в течение установленного времени с момента получения соответствующего Электронного сообщения от Банка, такое Электронное сообщение исчезает из списка ЭД в Мобильном приложении PayControl и аннулируется на сервере PayControl.

7.9. В случае изменения лица, уполномоченного подписывать ЭД ПЭП PayControl и/или мобильного устройства, Зарегистрированного номера телефона Уполномоченного лица (пользователя), Клиент предоставляет в Подразделение Банка новое заявление о регистрации Уполномоченных лиц по форме Банка с уточненными данными и приложением документов, подтверждающих полномочия Уполномоченного лица (Пользователя).

7.10. Банк осуществляет отключение возможности подписания документов ПЭП PayControl на основании предоставленного Клиентом заявления на отключение использования ПЭП PayControl не позднее следующего рабочего дня после его получения.

7.11. Банк осуществляет отключение возможности подписания документов ПЭП PayControl в одностороннем порядке в случае выявления Банком неактуальности сведений о Клиенте (Уполномоченных лицах/Пользователях), ранее предоставленных Клиентом в целях предоставления возможности подписания документов ПЭП PayControl.

7.12. Клиент принимает меры для предотвращения несанкционированного доступа третьих лиц к конфиденциальной информации, связанной с использованием Клиентом PayControl.

Любая информация такого рода может быть предоставлена третьим лицам не иначе как в порядке, установленном законодательством Российской Федерации.

8. ПОРЯДОК ИСПОЛЬЗОВАНИЯ МОБИЛЬНОГО ПРИЛОЖЕНИЯ ⁹

8.1. Банк в рамках Договора ДБО, заключенного с Клиентом, предоставляет Клиенту возможность работы в Системе с использованием Мобильного приложения.

8.2. Установка Мобильного приложения на мобильном устройстве осуществляется из официальных магазинов приложений "Google Play" и "App Store" в информационно – телекоммуникационной сети "Интернет", а также по ссылке, приведенной на странице входа в сервис "Интернет-Банк" Системы. Банк не использует иные ресурсы для распространения Мобильного приложения.

8.3. В Мобильном приложении подписание электронных документов возможно исключительно с использованием ПЭП. Интерфейс и (или) прикладной функционал Системы ДБО, предоставляемый Банком Клиенту с использованием Мобильного приложения, может отличаться от интерфейса и (или) прикладного функционала Системы ДБО, доступного через web-интерфейс. Мобильное приложение размещается Банком только в официальных магазинах приложений GooglePlay, AppStore.

8.4. Для регистрации в Мобильном приложении Уполномоченное лицо Клиента вводит Логин и Пароль, используемые для входа в сервис "Интернет-Банк" Системы, при этом при первом входе в Мобильное приложение и вводе Логина и Пароля Клиент получает от Банка SMS – сообщение/ Push - уведомление, содержащее разовый пароль для регистрации мобильного устройства в целях использования Мобильного приложения.

8.5. После регистрации в Мобильном приложении Клиент имеет возможность настроить использование в качестве Средства аутентификации в Мобильном приложении короткого кода доступа и (или) отпечатка пальца, заданных Клиентом после первого входа в Мобильное приложение с использованием Логина и Пароля.

8.6. В Мобильном приложении Системы ДБО подписание распоряжений и иных ЭД возможно только с использованием ПЭП в порядке, определенном в [разделе 6](#) Правил.

8.7. При использовании Клиент поставлен в известность и в полной мере осознает, что использование Мобильного приложения несет риск несанкционированного доступа от имени Клиента к Системе ДБО и конфиденциальной информации Клиента третьих лиц в случае утери или передачи третьим лицам Мобильного устройства и/или компрометации Мобильного приложения.

9. ОТВЕТСТВЕННОСТЬ СТОРОН И ПОРЯДОК РАЗРЕШЕНИЯ СПОРОВ

9.1. Стороны несут ответственность за нарушение условий настоящего Договора и (или) требований законодательства Российской Федерации.

9.2. Стороны не несут ответственность за частичное или полное неисполнение предусмотренных настоящими Правилами обязательств, если исполнение данных обязательств стало невозможным вследствие обстоятельств непреодолимой силы (в случае действия непреодолимой силы, влияющей на функционирование Системы, в виде стихийных бедствий, отключения электроэнергии, повреждения линий связи, общественных явлений, воздействия на Систему вредоносных программ, решений органов власти), наступление которых Стороны не могли предвидеть и на которые Стороны не могли оказать влияние. Сторона, подверженная действию обстоятельств непреодолимой силы, незамедлительно известить любым доступным способом другую Сторону о наступлении обстоятельств непреодолимой силы.

9.3. Клиент несет ответственность:

9.3.1. за указание в Электронных документах недостоверных реквизитов, несоблюдение требований законодательства Российской Федерации к оформлению платежных документов

⁹ Доступно только для Системы ДБО на базе технологического комплекса дистанционного банковского обслуживания "Faktura.ru". Сервис предоставляется при наличии у Банка соответствующей технологической возможности. Банк самостоятельно определяет требования к версии операционных систем мобильных устройств Android и (или) iOS в целях возможности установки и функционального использования мобильного приложения.

и осуществлению операций с денежными средствами, а также документов, определяющих полномочия Уполномоченных лиц (Пользователей) для работы в Системе ДБО;

9.3.2. за действия и операции, осуществленные в Системе с использованием Логина, Пароля, Кодов подтверждения либо Ключа УЭП, ПЭП PayControl Уполномоченного лица (Пользователя), за обеспечение конфиденциальности используемых Уполномоченным лицом (Пользователем) средств аутентификации для доступа к Системе ДБО и (или) средств ЭП во избежание их Компрометации, а также за последствия, возникшие вследствие Компрометации Средств аутентификации и (или) средств ЭП или несанкционированного доступа к Системе ДБО, в том числе посредством мобильного устройства, на котором установлено Мобильное приложение Системы ДБО или Мобильное приложение PayControl, или SIM-карты с Зарегистрированным номером;

9.3.3. за несвоевременное уведомление либо неуведомление Банка о Компрометации Средств аутентификации;

9.3.4. за несвоевременное уведомление Банка об изменении Номера телефона Уполномоченного лица, прекращении срока полномочий Уполномоченного лица.

9.3.5. за несанкционированный доступ третьих лиц к Системе ДБО, средствам аутентификации для доступа к Системе ДБО и (или) средствам ЭП и несвоевременное информирование Банка и таких случаях.

9.4. Клиент несет ответственность и риск убытков и иных неблагоприятных последствий вследствие передачи ЭД, подтвержденных ПЭП.

9.5. Банк несет ответственность:

9.5.1. за достоверность данных Клиента, используемых Банком в процессе Аккредитации Клиента;

9.5.2. за сохранность Электронных документов и своевременное исполнение платежных документов.

9.6. Банк не несет ответственность:

9.6.1. за последствия возможного несанкционированного доступа к SMS-сообщениям/ Push-уведомлениям, направляемым Банком на Номер телефона Уполномоченного лица Клиента и содержащим Коды подтверждения, несанкционированного использования ЭП Уполномоченного лица;

9.6.2. за задержку или недоставку SMS-сообщений/ Push-уведомлений Клиенту по причине сбоев в сетях операторов сотовой связи и сервисах провайдеров информационно-телекоммуникационной сети "Интернет";

9.6.3. за задержку или недоставку SMS-сообщений по причине переполненной памяти мобильного устройства Клиента (Уполномоченного лица, Пользователя);

9.6.4. за возможные неблагоприятные последствия для Клиента в связи с выявлением Банком неактуальности ранее представленных Клиентом контактных данных, а также несвоевременным сообщением Клиентом Банку актуальных данных, в том числе используемых в целях направления Банком Кодов подтверждения, паролей (в том числе Временных паролей);

9.6.5. за неисполнение или ненадлежащее исполнение поручений Клиента из-за нарушения Клиентом положений настоящих Правил, а также в случаях, предусмотренных законодательством Российской Федерации;

9.6.6. за списание средств со счета Клиента в случае, если по причинам, не зависящим от Банка, Распоряжения были отправлены в Банк лицами, не несущими ответственность за сохранность ключей ЭП, не имеющими право работать с Системой ДБО, при условии, что электронные платежные документы были составлены правильно и соответствовали требованиям системы защиты от несанкционированного доступа и содержали правильные ЭП, а также если Банк не был своевременно информирован о случаях несанкционированного доступа к счету, списания денежных средств и о фактах Компрометации, в случае возникновения у Клиента технических неисправностей или других обстоятельств, препятствующих использованию ЭД;

9.6.7. за убытки, понесенные Клиентом в связи с указанием Уполномоченным лицом / Пользователем Системы неверного номера телефона при оформлении прав на использование ПЭП, либо в связи с исполнением Банком ЭД, направленных с номера телефона, который более не принадлежит Уполномоченному лицу / Пользователю Системы, как следствие

неисполнения или ненадлежащего исполнения Клиентом обязанности, предусмотренной настоящими Правилами в части своевременного предоставления информации об изменении реквизитов доступа;

9.6.8. за невыполнение обязательств, предусмотренных настоящими Правилами в случае сбоев, возникших по причинам, независящим от Сторон.

9.7. При совершении конверсионных операций в иностранной валюте Клиент понимает и принимает на себя риск, связанный с колебаниями курсов валют, в результате которого Клиент может заключить Конверсионную сделку по невыгодному для себя курсу.

9.8. Претензии рассматриваются Сторонами на основании официально врученных уведомлений в письменном виде уведомлений.

9.9. Все споры и разногласия, возникающие в рамках Договора, заключенного в соответствии с настоящими Правилами, или в связи с ним, разрешаются Сторонами путем принятия мер к их разрешению на взаимоприемлемой основе - переговоров и иных действий в соответствии с законодательством Российской Федерации, а в случае невозможности разрешения путем переговоров иных действий во внесудебном порядке - в Арбитражном суде г. Санкт-Петербурга и Ленинградской области.

10. ПОРЯДОК РАЗРЕШЕНИЯ СПОРОВ, СВЯЗАННЫХ С ПОДТВЕРЖДЕНИЕМ АВТОРСТВА ЭЛЕКТРОННОГО ДОКУМЕНТА И (ИЛИ) ДОСТОВЕРНОСТЬ ЭЛЕКТРОННОЙ ПОДПИСИ

10.1. Разбор конфликтной ситуации, связанной с подтверждением авторства ЭД и (или) достоверность ЭП, выполняется по инициативе любого участника Системы на основании письменной претензии одной из Сторон, и проводится специально сформированной для этой цели комиссией (рабочей группой), в которую включаются представители каждой из Сторон, и, при необходимости, с привлечением независимых экспертов и (или) третьих лиц, представителя разработчика (лицензиара) программного обеспечения Системы ДБО, представителя организации, которой Банк поручает технологическую поддержку (сопровождение) Системы ДБО, представитель разработчика СКЗИ. Оплата участия в работе комиссии независимых экспертов и (или) третьих лиц производится за счет Стороны, предъявляющей претензию.

10.2. Конфликтные ситуации, связанные с подтверждением авторства ЭД и (или) достоверность ЭП при использовании УЭП разбираются Сторонами с учетом требований Удостоверяющего центра, выдавшего соответствующий сертификат УЭП.

10.3. Право представлять соответствующую Сторону в комиссии должно подтверждаться доверенностью, выданной каждому представителю на согласованный Сторонами срок работы комиссии.

10.4. Комиссия определяет, включая, но, не ограничиваясь, следующее: предмет разногласий на основании письма Стороны-инициатора разбирательства и разъяснений Сторон; правомерность предъявления претензии на основании текста Договора ДБО и иных неразрывно связанных документов; документы в электронной форме, относящиеся к предмету разногласий; идентичность открытых ключей Клиента или Банка (в случае оспаривания ЭД, подписанного УЭП); идентичность ключей Клиента (в случае оспаривания ЭД, подписанного ПЭП PayControl); идентичность электронного документа документу на бумажном носителе, сформированному в Банке; истинность электронной подписи электронного документа; наличие и содержание подтверждения по электронному документу; даты и время поступления, отправки электронного документа и подтверждения по нему; исправность используемых ключевых носителей в случае оспаривания ЭД, подписанного УЭП.

10.5. Для разбора конфликтных ситуаций комиссия принимает на рассмотрение электронные документы и подтверждения по ним и обязана использовать следующие, признаваемые сторонами, эталонные данные: данные электронного архива принятых, отправленных документов; данные базы данных регистрационных записей (журнал регистрации приема и отправки электронных документов); подписанные Клиентом оригиналы заявлений на изготовление ключей ЭП; хранимое у Банка программное обеспечение Системы ДБО.

10.6. Экспертиза оспариваемого электронного документа осуществляется в присутствии всех членов экспертной комиссии.

10.7. В целях подтверждения подлинности оспариваемого ЭД, подписанного Клиентом с использованием ПЭП (Кодом подтверждения), комиссия осуществляет проверку подлинности оспариваемого ЭД и (или) достоверности ЭП путем установления и проверки следующих фактов: идентификации и Аутентификации клиента в Системе ДБО; направления Банком QR-сообщения с Кодом подтверждения на Зарегистрированный номер при подписании Акта признания ключа проверки ЭП; ввода корректного Кода подтверждения; положительного результата проведения проверки введенного Кода подтверждения на правильность и неистечения срока его действия для ввода; совпадения даты в ЭД, сформированном в Системе ДБО, а также даты и времени ввода Кода подтверждения.

10.8. В целях подтверждения подлинности оспариваемого ЭД, подписанного Клиентом с использованием УЭП, комиссия осуществляет проверку подлинности оспариваемого ЭД и (или) достоверности ЭП путем проведения экспертизы, состоящей из следующих этапов:

Этап 1. Подготовка оборудования и программного обеспечения и тестирование их работоспособности, которая проводится в следующем порядке:

производится конфигурирование операционной системы, осуществляется проверка предоставленного Банком персонального компьютера на предмет отсутствия вирусов и программных закладок;

производится установка эталонного программного обеспечения СКЗИ. Для установки эталонного программного обеспечения СКЗИ используется дистрибутив, представленный разработчиком СКЗИ;

членам экспертной комиссии предоставляется возможность убедиться в работоспособности установленного программного обеспечения путем проведения тестов, в порядке, предусмотренном документацией на СКЗИ.

Этап 2. Контроль целостности оспариваемого электронного документа путем проверки ЭП при помощи Сертификата открытого ключа ЭП, представленного Банком.

Контроль целостности оспариваемого электронного документа производится посредством стандартной процедуры проверки ЭП, предусмотренной СКЗИ и (или) эксплуатационной документацией УЦ. Проверка осуществляется на Сертификате ЭП, файл которого предъявляется Банком комиссии на защищенном носителе.

Этап 3. Аутентификация отправителя оспариваемого электронного документа путем проверки подлинности (принадлежности, актуальности и целостности) Сертификата, использованного комиссией для проверки ЭП.

Для доказательства подлинности (принадлежности, актуальности и целостности) Сертификата, использованного для проверки ЭП, которой подписан оспариваемый документ, Банк предъявляет членам комиссии заверенное уполномоченным лицом Клиента заявление на изготовление сертификата УЭП.

Проверка принадлежности, актуальности и целостности Сертификата, подтвержденного письменным документом, проводится путем визуальной сверки членами экспертной комиссии распечатки файла Сертификата, записанного на представленном Банком съемном носителе и реквизитов ключа проверки ЭП заявления на изготовление сертификата пользователя УЦ, зафиксированных в бумажном документе.

Подтверждением подлинности оспариваемого ЭД, и (или) и (или) достоверности ЭП подписанного Клиентом с использованием УЭП, является единовременное наличие следующих условий:

положительный результат проверки ЭП оспариваемого электронного документа на Сертификате, файл которого предъявлен Банком;

подтверждение принадлежности, актуальность и целостность Сертификата открытого ключа Клиента, с помощью которого проводится проверка ЭП оспариваемого ЭД.

10.9. В целях подтверждения подлинности оспариваемого ЭД, подписанного Клиентом с использованием ЭП PayControl, комиссия осуществляет проверку подлинности оспариваемого ЭД и (или) достоверности ЭП путем проведения технической экспертизы с использованием специализированного ПО разработчика ПЭП PayControl – ПО АРМ РКС; и следующих данных и (или) документов: идентификатора пользователя; файла спорного ЭД и/или данных транзакции; кода подтверждения, выработанный на симметричных ключах; ЭП, выработанной на

асимметричных ключах (при оффлайн-подтверждении отсутствует); время выработки ЭП; наличия Акта признания ключа проверки ЭП, достоверность и работоспособность которого установлена на время совершения оспариваемого ЭД.

Проведение технической экспертизы включает в себя выполнение следующих действий:

- загрузка в АРМ РКС идентификатора пользователя; файла спорного ЭД и/или данных транзакции; Кода подтверждения, выработанного на симметричных ключах; ЭП, выработанной на асимметричных ключах (при оффлайн-подтверждении отсутствует); времени выработки ЭП.
- проверка результатов разбора в АРМ РКС;
- печать протокола работы АРМ РКС.

Спор решается в пользу Банка в случае если владельцем Ключа ЭП и Ключа проверки ЭП является Представитель Клиента, зарегистрированный Банком; ЭП и (или) Код подтверждения для оспариваемого ЭД верны (ключ проверки ЭП, отобранный для разбора конфликтной ситуации, соответствует значению ключа в Акте признания ключа проверки ЭП, что подтверждает подписание проверяемого (оспариваемого) ЭД Ключом ЭП, соответствующим зарегистрированному Банком Ключу проверки ЭП, использованным при проведении технической экспертизы и (или) предоставление Кода подтверждения, выработанного на симметричном ключе, владельцем которого является Клиент, зарегистрированный Банком).

Спор решается в пользу Клиента в случае если владельцем Ключа ЭП и Ключа проверки ЭП не является Представитель Клиента, зарегистрированный Банком; ЭП и (или) Код подтверждения для оспариваемого ЭД не верны (ключ проверки ЭП, отобранный для разбора конфликтной ситуации, не соответствует значению ключа в Акте признания ключа проверки ЭП, что не подтверждает подписание проверяемого (оспариваемого) ЭД Ключом ЭП, соответствующим зарегистрированному Банком Ключу проверки ЭП, использованным при проведении технической экспертизы и (или) предоставление Код подтверждения, выработанного на симметричном ключе, владельцем которого не является Клиент, зарегистрированный Банком)

10.10. Результаты экспертизы оформляются в виде письменного заключения – Акта экспертной комиссии, подписываемого всеми членами комиссии. Акт составляется немедленно после завершения всех этапов экспертизы. В Акте фиксируются результаты всех этапов проведенной экспертизы, а также все существенные реквизиты оспариваемого электронного поручения. Акт составляется в двух экземплярах - по одному для представителей Банка и Клиента. Акт комиссии является окончательным и пересмотру не подлежит.

10.11. Подтверждение подлинности электронного документа, зафиксированное в Акте, будет означать, что этот документ имеет юридическую силу и является законным основанием для осуществленных Банком операций по счету Клиента. Не подтверждение подлинности электронного документа, зафиксированное в Акте, будет означать, что этот документ не имеет юридической силы и не является законным основанием для осуществленных Банком операций по счету Клиента.

10.12. В случае последующего судебного разбирательства об оспаривании электронного документа, акт, составленный комиссией, используется в качестве доказательства при дальнейшем разбирательстве спора в суде.

11. СРОК ДЕЙСТВИЯ И ПОРЯДОК ДОСРОЧНОГО РАСТОРЖЕНИЯ ДОГОВОРА ДБО

11.1. Договор ДБО действует до его расторжения по любым основаниям.

11.2. Клиент имеет право при отсутствии задолженности перед Банком расторгнуть Договор ДБО, предупредив об этом Банк письменно за 10 (десять) рабочих дней.

11.3. Банк вправе расторгнуть Договор ДБО с Клиентом в одностороннем порядке с направлением Клиенту письменного уведомления о расторжении Договора ДБО, в том числе нарушения Клиентом условий настоящего Договора и (или) требований законодательства Российской Федерации, а также в случае неоплаты Клиентом услуг Банка по сопровождению Системы ДБО, несоблюдения Клиентом рекомендаций Банка по укомплектованию рабочего места для использования Системы ДБО при использовании СКЗИ. В указанных случаях Договор ДБО считается расторгнутым с даты, указанной в уведомлении.

11.4. Банк в одностороннем порядке расторгает Договор ДБО с момента получения Банком информации о смерти Клиента - индивидуального предпринимателя или физического лица, занимающегося в установленном законодательством Российской Федерации порядке частной практикой, а также в случае прекращения действия всех договоров банковского счета, договоров депозита, заключенных с Клиентом.

11.5. Прекращение Договора не влечет прекращения обязательств по взаиморасчетам Сторон и возмещению убытков, возникших до момента расторжения. Неисполненные обязательства Клиента по выплате вознаграждения за фактически оказанные Банком услуги до момента расторжения Договора, сохраняются после расторжения Договора до момента полного их исполнения Клиентом.

12. ДОПОЛНИТЕЛЬНЫЕ УСЛОВИЯ

12.1. Стороны согласились считать, что использование Банком факсимильного воспроизведения подписи должностного лица Банка с помощью средств механического или иного копирования (факсимиле подписи) и (или) факсимильного воспроизведения оттиска печати Банка (факсимиле печати) допускается для подписания документов (актов, заявлений, соглашений, пр.) в рамках Договора ДБО, заключенного в соответствии с настоящими Правилами, и факсимиле подписи должностного лица Банка, факсимиле печати Банка равнозначны собственноручной подписи должностного лица Банка и оттиску печати Банка.

12.2. Любое уведомление или сообщение, направляемое Сторонами друг другу, за исключением уведомлений или сообщений Банка, определенных в п. 2.15 Банка, должно быть совершено в письменной или приравненной к письменной форме.

12.3. Обязанность Банка по направлению Клиенту уведомлений и (или) сообщений, предусмотренных Договором ДБО и действующим законодательством Российской Федерации, считается исполненной при направлении уведомления в соответствии с имеющейся у Банка информацией для связи с Клиентом, предоставленной Клиентом при заключении Договора ДБО, или предоставленной отдельным заявлением Клиента, способом, предусмотренным Правилами.

12.4. Стороны договорились, что уведомления и (или) сообщения, предусмотренные Договором ДБО, и направленные с использованием предусмотренных в настоящем пункте способов направления информации, считают полученными адресатом:

– при использовании почтовой связи - в дату вручения письма адресату. Если письмо не было вручено адресату, письмо считается полученным адресатом независимо от причин его невручения (в том числе в случае отказа адресата от получения письма, отсутствия адресата по указанному адресу (в частности, непроживании/ ненахождении адресата по указанному адресу, выбытии адресата, сноса дома (здания) и т.п., истечения срока хранения письма и т.п.) на 6 (Шестой) календарный день со дня направления письма (включая день направления);

– при использовании телеграфной связи - в дату вручения телеграммы адресату. Если телеграмма не была вручена адресату, телеграмма считается полученной адресатом независимо от причин её невручения (в том числе в случаях отказа адресата от получения телеграммы, отсутствия адресата по указанному адресу (в частности, при непроживании/ ненахождении адресата по указанному адресу, выбытии адресата, сноса дома (здания) и т.п.), истечения срока хранения телеграммы и т.п.) в первый рабочий день, следующий за днем направления телеграммы;

– при использовании курьерской связи - в дату вручения Стороне (в дату, проставленную Стороной или представителем на копии полученного сообщения); при этом полномочия представителя Стороны следуют из обстановки;

– при использовании системы ДБО, факса или электронной почты — в дату направления уведомления или сообщения;

– при использовании sms-сообщений (может использоваться Банком в целях уведомления Клиента о приостановке или прекращении использования Системы ДБО: информировании о внесении изменений в Правила и (или) Тарифы) - в дату направления такого уведомления.

12.5. Банк осуществляет хранение и обработку персональных данных Клиента (Представителя Клиента), в том числе содержащихся в заявлениях и (или) иных документах,

представляемых в Банк Клиентом (Представителем Клиента) в связи с заключением Договора в целях исполнения договорных обязательств и (или) предоставления банковских услуг, в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ "О персональных данных", включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных. Банк вправе использовать при обработке персональных данных Клиента (Представителя Клиента) автоматизированный и неавтоматизированный способы по усмотрению Банка.

12.5.1. Банк имеет право осуществлять передачу персональных данных Клиента (Представителя Клиента) третьим лицам на основании заключенных между Банком и указанными третьими лицами соответствующих договоров, при условии обеспечения данными третьими лицами конфиденциальности и безопасности при обработке персональных данных Клиента (Представителя Клиента):

- ПАО "МТС", адрес: 109147, г. Москва, ул. Марксистская, д.4 - в целях предоставления Банком Клиенту (Представителю Клиента) услуг дистанционного банковского обслуживания с использованием средств телефонной связи посредством контактного центра Банка;
- ООО "КАРТЛАВКА", адрес: 117342, г. Москва, Новоясеневский пр-кт, д. 6 к. 2 - в целях приема за пределами подразделений Банка и передачи в Банк документов Клиента, необходимых для принятия Клиента на обслуживание и в рамках обслуживания Клиента в Банке.

12.6. В случае изменения законодательства Российской Федерации и нормативных актов Банка России, затрагивающих условия настоящих Правил, положения Правил действуют в части, не противоречащей законодательству Российской Федерации и нормативным актам Банка России.

12.7. Ни одна из Сторон не может передавать свои права и обязательства по Договору, заключенному в соответствии с настоящими Правилами, третьим лицам.