АКЦИОНЕРНЫЙ БАНК РОССИЯ

ПРАВИЛА
дистанционного банковского обслуживания корпоративных клиентов АО «АБ «РОССИЯ»

действуют с «25» сентября 2025 г.

1. Термины, определения и сокращения

АБС «ЦФТ-Банк» (АБС) - используемая Банком автоматизированная банковская система «ЦФТ-Банк».

Авторизация – подтверждение полномочий (предоставление прав доступа) Клиента, успешно прошедшего Аутентификацию при входе в Систему ДБО, на получение услуг Банка, предусмотренных Договором ДБО.

Акцепт (визирование) – режим работы Системы ДБО, позволяющий получать авторизованное согласие на проведение ЭПД Клиента в Системе ДБО, совершённое Уполномоченным лицом с использованием Визирующей подписи. Порядок предоставления определён разделом 7 настоящих Правил.

Аутентификационные данные – совокупность Логина и Пароля, а также либо SMS-код при работе с Серверной ЭП, либо Ключ ЭП / Ключ PayControl при доступе к каналу «Клиент-Банк Онлайн», а также Пароль, PIN-код/ отпечаток пальца или изображение лица (TouchID/ FacelD), используемые для целей установления личности Уполномоченного лица Клиента при доступе к Мобильному устройству и/или Мобильному приложению PayControl и Мобильному приложению Банка.

Аутентификация - процедура проверки подлинности Аутентификационных данных Уполномоченного лица, позволяющая его идентифицировать.

База данных Банка России - база данных о случаях и попытках осуществления переводов денежных средств без добровольного согласия клиента, формируемая Банком России в соответствии с частью 5 ст. 27 Федерального закона от 27.06.2011 № 161-ФЗ «О национальной платежной системе» (далее - Федеральный закон № 161-ФЗ).

Банк - АО «АБ «РОССИЯ».

Банковская карточка - карточка с образцами подписей и оттиска печати.

Бенефициарный владелец – физическое лицо, которое, в конечном счёте, прямо или косвенно (через третьих лиц, в том числе через юридическое лицо, нескольких юридических лиц либо группу связанных юридических лиц) владеет (имеет преобладающее участие более 25 (двадцати пяти) процентов в капитале) Клиентом – юридическим лицом, либо прямо или косвенно контролирует действия Клиента, в том числе имеет возможность определять решения, принимаемые Клиентом. Бенефициарным владельцем Клиента - физического лица считается это лицо, за исключением случаев, если имеются основания полагать, что бенефициарным владельцем является иное физическое лицо.

Бланк ключа проверки электронной подписи (Бланк ключа ЭП) – документ на бумажном носителе или электронный документ, в формате, реализованном в Системе ДБО, удостоверяющий принадлежность приведенного в нем Ключа проверки электронной подписи и соответствующего ему Ключа электронной подписи Уполномоченному лицу. Подписанный Клиентом, переданный в Банк и активированный Банком Бланк ключа ЭП подтверждает факт наделения данного Уполномоченного лица правами на использование Системы ДБО в соответствии с Договором ДБО.

Браузер – программное обеспечение для просмотра веб-сайтов, для запроса веб-страниц, их обработки, вывода и перехода от одной веб-страницы к другой.

Визирующая подпись - подпись, которая предоставляется Уполномоченному лицу Клиента или юридического лица, отличного от Клиента и применяется в целях контроля за распоряжением денежными средствами, находящимися на Счёте(-ах) Клиента.

Выгодоприобретатель – лицо, не являющееся непосредственно участником операции, к выгоде которого действует Клиент, в том числе на основании агентского договора, договоров поручения, комиссии и доверительного управления, при проведении операций с денежными средствами и иным имуществом.

Выписка по счёту - документ, формируемый в АБС «ЦФТ-Банк» в электронном виде, передаваемый программным путём в Систему ДБО, в целях предоставления Клиенту сведений об операциях за период и остатках по Счёту Клиента в формате, установленном Системой ДБО, по факту отражения операций в бухгалтерском балансе Банка.

Дистанционное банковское обслуживание (ДБО) - комплекс услуг, предоставляемых Банком Клиенту, предназначенный для осуществления обмена электронными документами между Клиентом и Банком, в том числе при наличии открытого Счёта в Банке – для передачи Клиентом Банку Распоряжений на совершение одной или нескольких операций по Счёту Клиента, электронных документов по валютному контролю, и иных документов, необходимых для фиксирования информации в целях выполнения требований законодательства Российской Федерации и нормативных актов Банка России, электронных документов произвольного формата, а также предоставления Банком информации о Счёте Клиента (при его наличии), направления уведомлений, включая уведомления о приеме к исполнению, отказе от приема к исполнению(с указанием причины), о приостановлении исполнения, и об исполнении распоряжений и т.п. и иных сведений и документов.

Договор банковского счета - договор банковского счёта, определяющий порядок предоставления Банком услуг по расчётно-кассовому обслуживанию Клиента.

Договор ДБО – договор определяющий общие условия предоставления Клиенту услуг дистанционного банковского обслуживания с использованием Системы ДБО, заключенный с Банком путём присоединения к Правилам дистанционного банковского обслуживания корпоративных клиентов АО «АБ «РОССИЯ» (далее – Правила ДБО), размещённым на официальном сайте Банка в сети Интернет www.abr.ru.

Договор СБП - договор, заключенный между Клиентом и Банком, путем присоединения Клиента к условиям Правил предоставления услуги переводов денежных средств с использованием сервиса B2B Системы быстрых платежей для юридических лиц и индивидуальных предпринимателей в АО «АБ «РОССИЯ» (далее – Правила B2B) или Правил предоставления услуги переводов денежных средств юридическими лицами и индивидуальными предпринимателями в пользу физических лиц с использованием сервиса B2C через Систему быстрых платежей в АО «АБ «РОССИЯ» (далее – Правила B2C[1]), по которому Банк обязуется предоставлять Клиенту Услуги СБП.

Договор Транзит 2.0 – договор о предоставлении услуги обмена электронными документами с Системой Транзит НРД, заключаемый Сторонами в соответствии с законодательством Российской Федерации в порядке, предусмотренном Правилами предоставления услуги обмена электронными документами с Системой Транзит НРД (далее – Правила Транзит 2.0), с использованием Модуля Транзит 2.0. Договор Транзит 2.0 является неотъемлемой частью Договора ДБО.

Документы, подтверждающие полномочия - документы, подтверждающие предоставление Уполномоченным лицам Клиента /Банка /Контролирующей организации полномочий на распоряжение денежными средствами на Счёте/подписание ЭД/ акцепт расходных операций с использованием Электронной подписи, которые могут быть предоставлены различными способами, в том числе:

1) учредительными документами;
2) распорядительным актом, договором;
3) соответствующей доверенностью (в том числе машиночитаемой доверенностью), выдаваемой в порядке, установленном законодательством Российской Федерации.

Запрос на регистрацию Ключа проверки ЭП (ЗРКП ЭП) – запрос на регистрацию Ключа проверки ЭП в электронном виде, формируемый в Системе ДБО в процессе генерации Уполномоченным лицом Клиента Ключей ЭП, который средствами Системы ДБО или Мобильного приложения PayControl направляется в Банк.

[1] Доступно с момента технической реализации

Информационная система «Одно окно» (далее – ИС «Одно окно») – единая цифровая платформа для поддержки экспортеров, созданная Российским Экспортным Центром**.**

Канал «Клиент-Банк Онлайн» – канал отправки ЭД в Банк Системы ДБО, предоставляющий возможность обмена ЭД с Банком через официальный сайт Банка посредством Браузера, либо через Мобильное приложение Банка. Для подписания ЭД Клиента используется:

– УНЭП и УКЭП. Возможность подключения предоставляется в Системе «iBank» и ДБО «BS-Client (CORREQTS)»;

– ПЭП PayControl. Возможность использования предоставляется в Системе ДБО «BS-Client (CORREQTS)».

Для работы в Браузере с использованием СКЗИ на рабочее место Клиента требуется установка специализированного программного обеспечения, которое является частью Системы.

Канал «Интеграционный Клиент-Банк» - канал передачи данных (ЭД) Системы ДБО, предоставляющий возможность обмена ЭД между Банком и Клиентом с использованием УНЭП и УКЭП напрямую из Системы Клиента:

– посредством интеграции с системой 1С с применением модуля «Обмен с 1С по DirectBank/ DirectBank+»;

– посредством интеграции с модулем «Корпоративный автоклиент» Системы «iBank», позволяющим автоматизировать процесс подписи и отправки документов в Банк, получения из Банка Выписок по счетам, а также обеспечить интеграцию Системы Клиента с банковским сервером Системы «iBank»;

– посредством обмена информацией с Системой Транзит Небанковской кредитной организации акционерного общества «Национальный расчетный депозитарий» (НРД) с применением модуля взаимодействия с Системой Транзит НРД (Модуль Транзит 2.0) в соответствии с правилами предоставления услуги обмена электронными документами с Системой Транзит НРД;

– посредством интеграции с Системой Клиента с применением модуля «Интеграционный корпоративный шлюз» Системы ДБО «BS-Client (CORREQTS)»[2] в соответствии с форматами, определёнными пользовательской документацией, предоставляемой Банком Клиенту (размещена на сайте Банка по адресу: https://abr.ru/corp/remote-services/integration-client-bank/#user_docs);

– посредством интеграции через API (API Интеграция[3]) Системы iBank в соответствии с форматами, определёнными пользовательской документацией, предоставляемой Банком Клиенту (размещена на сайте Банка по адресу: https://abr.ru/corp/remote-services/integration-client-bank/#user_docs).

Порядок использования Канала «Интеграционный Клиент-Банк», за исключением модуля взаимодействия с Системой Транзит НРД, определён Приложением № 1 к настоящим Правилам. Предоставление услуг с использованием модуля взаимодействия с Системой Транзит НРД осуществляется на основании правил предоставления услуги обмена электронными документами с Системой Транзит НРД.

Канал ЭДО - канал связи, позволяющий использовать усиленную квалифицированную электронную подпись.

Клиент - юридическое лицо, иностранная структура без образования юридического лица, индивидуальный предприниматель, физическое лицо, занимающееся в установленном законодательством Российской Федерации порядке частной практикой, заключившее Договор ДБО.

[2] Подключается при наличии технической возможности у Банка

[3] Доступно с момента технической реализации

Клиентское рабочее место - индивидуальный комплекс технических и программных средств Клиента, обеспечивающий подготовку, редактирование, подписание, отправку, поиск, получение и печать электронного документа и справочной информации при взаимодействии с Банком.

Ключи инициализации PayControl - уникальные ключи, выдаваемые Банком каждому Уполномоченному лицу Клиента в закодированном виде двумя частями (QR-код и код в SMS-сообщении).

Ключ проверки электронной подписи (Ключ проверки ЭП) - уникальная последовательность символов, однозначно связанная с Ключом электронной подписи/ Ключом Серверной ЭП и предназначенная для проверки подлинности УНЭП, включая Серверную ЭП/ УКЭП.

Ключ Серверной ЭП[4] – Ключ ЭП, предназначенный для формирования Серверной ЭП, который хранится на Сервере Банка, доступ к Ключу Серверной ЭП осуществляется с помощью Пароля к Ключу Серверной ЭП.

Ключ электронной подписи (Ключ ЭП) – уникальная последовательность символов, предназначенная для создания УНЭП/ УКЭП.

Ключ проверки PayControl - уникальная последовательность символов, соответствующая Ключу PayControl, сформированному Клиентом с помощью Мобильного приложения PayControl, и предназначенная для проверки на стороне Банка ПЭП PayControl,

Ключ PayControl - уникальная последовательность символов, доступ к которым имеет Клиент посредством установленного мобильного приложения PayControl на мобильном устройстве Уполномоченного лица Клиента после прохождения процедуры инициализации, соответствующий Ключу проверки и предназначенный для создания ПЭП с помощью мобильного приложения PayControl

Ключи ЭП – при совместном упоминании Ключ ЭП (УНЭП, УКЭП), Ключ Серверной ЭП и Ключ PayControl.

Ключевая информация - обобщённое понятие информации, содержащей Ключи ЭП, Ключи проверки ЭП, Ключи инициализации PayControl, используемые для Аутентификации.

Ключевой носитель – носитель информации, предназначенный для записи, хранения, воспроизведения Ключей ЭП. Для целей настоящих Правил под Ключевым носителем понимается USB-Токен и Мобильное устройство с загруженными Ключами PayControl.

Код подтверждения – набор символов или сообщение, поступившие в Систему ДБО, используемые для подтверждения доступа к Системе ДБО в целях дополнительной/ обязательной при использовании Серверной ЭП Аутентификации Уполномоченного лица Клиента и/или одобрения перевода денежных средств Уполномоченным лицом Клиента, формируемые посредством:

- Мобильного устройства с установленным Мобильным приложением PayControl;
- Устройства подтверждения, выданного Банком[5];
- получения от Банка SMS-кода.

Компрометация - утрата доверия к тому, что используемый Логин, Пароль, Ключи ЭП недоступны третьим лицам, а также наличие оснований считать, что Мобильное устройство с активированным Мобильным приложением PayControl доступно неуполномоченным лицам, независимо от того, нанесён или нет ущерб Банку и/или Клиенту.

К событиям, связанным с Компрометацией или подозрениями на Компрометацию, относятся включая, но не ограничиваясь, следующие события:

[4] Серверная ЭП не применяется при работе в модуле ЦФК/РЦК и в Системе ДБО «BS-Client (CORREQTS).

[5]Услуга генерации Кода подтверждения с помощью Устройства подтверждения не предоставляется при использовании Мобильного приложения Банка и Канала «Интеграционный Клиент-Банк», за исключением интеграции с 1С с применением сервиса «Обмен с 1С по DirectBank» посредством модуля iBank для 1С.

−полная или временная утрата контроля доступа третьих лиц к программным средствам Системы ДБО, в том числе Мобильному устройству, Мобильному приложению Банка, Мобильному приложению PayControl, Устройству подтверждения;

−обнаружение попытки совершения каких-либо иных несанкционированных действий, которые могут привести к сбоям либо иным образом нанести ущерб Банку, либо другим пользователям Системы ДБО;

−обнаружение использования Системы ДБО без согласия Клиента, а также в случае если Клиент подозревает возможность возникновения подобных ситуаций;

−утеря Пароля, удаление Ключа ЭП и др. по вине Клиента;

−сбой (поломка) Ключевого носителя;

−утрата Ключевого носителя, в том числе с последующим обнаружением;

−возникновение подозрений на утечку информации или её искажение в Системе ДБО;

−нарушение целостности печатей на сейфах (металлических шкафах) с Ключевыми носителями, если используется процедура опечатывания сейфов;

−утрата ключей от сейфов (металлических шкафов) во время нахождения в них Ключевых носителей, в том числе с последующим обнаружением;

−временный доступ третьих лиц к Ключевому носителю;

−утрата Мобильного устройства УЛ, в том числе, с последующим обнаружением;

−заражение Мобильного устройства УЛ, Клиентского рабочего места вредоносными программами;

−несанкционированный перевыпуск SIM-карты с Номером телефона УЛ, сведения о котором были ранее предоставлены в Банк и содержатся в Системе ДБО, и на которые поступают Коды подтверждения/ SMS-сообщения/ PUSH-сообщения;

−нарушение правил хранения Мобильного устройства УЛ Клиента, предусмотренных Обязательствами по безопасной работе (Приложение № 2 к настоящим Правилам);

−Мобильное устройство УЛ Клиента вышло из строя и доказательно не опровергнута возможность того, что, данный факт произошёл в результате несанкционированных действий злоумышленника;

−иные обстоятельства, прямо или косвенно свидетельствующие о наличии возможности доступа третьих лиц к Ключевой информации.

Логин – уникальный идентификатор Уполномоченного лица Клиента в виде последовательности цифр и/или букв.

Мобильное приложение Банка[6] - канал отправки ЭД в Банк, требующий установки специализированного программного обеспечения на мобильное устройство Уполномоченного лица Клиента. Является неотделимой частью канала «Клиент-Банк Онлайн» Системы ДБО «BS-Client (CORREQTS)». Доступно для операционных систем iOS, Android.

Мобильное приложение PayControl - приложение для мобильных платформ iOS и Android, выполняющее функции управления Ключом PayControl (считывание, хранение, использование, обновление, удаление), получения информации для подтверждения от серверной части, отображения подтверждаемых данных (ЭД) на экране мобильного устройства, формирования Кода подтверждения на основе данных операции, Ключа PayControl, времени обработки, отправки Кода подтверждения в серверную часть в целях подтверждения входа в Мобильное приложение Банка**,** подтверждения и подписания ЭД ПЭП PayControl в Системе ДБО BS-Client (CORREQTS)».

Мобильное устройство - мобильное устройство (телефон, смартфон, планшет и т.д.), работающее под управлением операционной системы iOS / Android, на котором есть доступ в сеть Интернет, установлено и активировано Мобильное приложение PayControl и/или Мобильное приложение Банка.

[6] Предоставляется при наличии технической возможности у Банка в «ДБО BS-Client (CORREQTS).

Модуль «Центр финансового контроля/ Расчётный центр Корпорации» (далее – модуль ЦФК/РЦК[7]) – модуль Системы ДБО, при использовании которого Уполномоченному лицу Контролирующей организации предоставляется возможность получения информации о движении денежных средств по счетам Клиента и/или Подконтрольных организаций, открытым в Банке в режиме мониторинга, акцепта, управления счетами. Порядок использования модуля ЦФК/РЦК определён Приложением № 3 к настоящим Правилам, подключение осуществляется на основании Заявления о предоставлении модуля Системы ДБО Контролирующей организации (Приложение № 4 к настоящим Правилам).

Модуль «Электронный офис» / «Управление услугами» – модуль Системы ДБО, доступный в Канале доступа «Клиент-Банк Онлайн», обеспечивающий возможность Клиентам осуществлять самостоятельное подключение / отключение Сервисов Системы ДБО в случаях, предусмотренных программным комплексом Системы ДБО и заключённым между Банком и Клиентом договором. В интерфейсе Системы «ДБО «BS-Client (CORREQTS)» «Электронный офис» доступен в пункте меню «Продукты /услуги», в Системе iBank – пункт «Управление услугами» доступен на панели разделов главного экрана.

Номер телефона Уполномоченного лица (Номер телефона УЛ) - номер телефона сотовой связи Уполномоченного лица Клиента, зарегистрированный в Системе ДБО, указанный Клиентом при заполнении Заявления/ Заявлении об изменении данных и используемый Клиентом для получения от Банка SMS-сообщений/ PUSH-сообщений.

Операционный день - операционно-учётный цикл за соответствующую календарную дату, в течение которого все совершённые операции оформляются и отражаются в бухгалтерском учёте по балансовым и внебалансовым счетам с составлением ежедневного баланса.

Операционный день включает в себя операционное время, в течение которого совершаются банковские операции и другие сделки, а также период документооборота и обработки учётной информации, обеспечивающий оформление и отражение в бухгалтерском учёте операций, совершённых в течение операционного времени, календарной датой соответствующего операционного дня, и составление ежедневного баланса.

Пароль – уникальная алфавитно-цифровая последовательность символов, известная только Уполномоченному лицу Клиента, соответствующая присвоенному ему Логину и использующаяся для Аутентификации Уполномоченного лица Клиента в Системе ДБО.

Пароль к Ключу Серверной ЭП – пароль, самостоятельно устанавливаемый Уполномоченным лицом Клиента на каждый Ключ Серверной ЭП с целью ограничения доступа третьих лиц. Пароль должен соответствовать требованиям, установленным Обязательствами по безопасной работе.

Полномочия уполномоченного лица (Полномочия) - профиль, определяющий набор действий, которые Уполномоченное лицо вправе совершать в Системе ДБО: просмотр информации об операциях по Счету (-ам), подготовка проекта ЭД, подписание ЭД ЭП и отправка его в Банк. Полномочия конкретного Уполномоченного лица указываются в Заявлении/ Заявлении об изменения данных.

Порядок осуществления переводов – Порядок осуществления переводов денежных средств в валюте Российской Федерации по счетам корпоративных клиентов в АО «АБ «РОССИЯ», публикуемый на официальном сайте Банка в сети Интернет www.abr.ru в разделе «Открытие и ведение счетов».

Представитель Клиента – лицо, при совершении операции действующее от имени и в интересах или за счет Клиента, полномочия которого основаны на доверенности, договоре, акте уполномоченного государственного органа или органа местного самоуправления, законе, а также единоличный исполнительный орган юридического лица.

[7] Подключение модуля РЦК «ДБО BS-Client (CORREQTS) Контролирующим организациям не осуществляется.

Простая электронная подпись (ПЭП PayControl)[8] – электронная подпись, являющаяся простой электронной подписью в соответствии с требованиями Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи». Для целей настоящих Правил это ПЭП PayControl, формируемая УЛ в Мобильном приложении PayControl.

Рабочий ключ ЭП – Ключ ЭП/ Ключ Серверной ЭП, предназначенный для подтверждения авторства и обеспечения целостности ЭД, передаваемого в Системе ДБО, при этом Срок действия Ключа ЭП и Срок действия полномочий УЛ - владельца Ключа ЭП не истекли, Клиент не заявил в Банк о Компрометации.

Распоряжение на перевод (Распоряжение) – платёжное поручение или иной расчётный (платёжный) документ, форма которого определена либо Банком России, в том числе Положением Банка России от 29.06.2021 № 762-П «О правилах осуществления перевода денежных средств», документами, регламентирующими правила платежной системы Банка России, и/или Банком, закреплённый Банком и Клиентом в договоре, и принятый Банком в соответствии с Порядком переводов, на основании которого осуществляются расходные операции по Счёту.

Сайт Банка – официальный Web-сайт Банка в сети Интернет по адресу: www.abr.ru.

Серверная электронная подпись (Серверная ЭП)[9] – УНЭП, являющаяся аналогом собственноручной подписи Уполномоченного лица Клиента, созданная в Системе ДБО iBank при помощи Ключа Серверной ЭП. При её создании формируется учетная запись для входа в Систему iBank по Логину и Паролю с обязательным подтверждением входа SMS-кодом.

Сервер Банка – удаленный сервер, предназначенный для хранения Ключей Серверной ЭП.

Сервис «Личный кабинет юридического лица» (Сервис «Личный кабинет ЮЛ»)[10] – web-сервис, применяемый в Банке для обмена между Клиентом и Банком информацией и документами, подписанными ЭП, в электронной форме по сети Интернет, включая обмен юридически значимыми электронными документами, доступ к которому осуществляется по ссылке https://lk.abr.ru/ по защищённому соединению.

Сервисы Системы ДБО – функциональные возможности Системы ДБО, подключаемые по желанию Клиента либо на основании Договора ДБО, либо на основании отдельных договоров и оплачиваемые им в соответствии с Тарифами, утверждёнными в Банке. Перечень доступных Сервисов является Приложением № 5 к настоящим Правилам.

Сертификат ключа проверки электронной подписи (Сертификат ЭП) – ЭД или документ на бумажном носителе, выданный Удостоверяющим центром, и подтверждающий принадлежность Ключа проверки ЭП Уполномоченному лицу.

Система быстрых платежей (СБП) - сервис быстрых платежей платежной системы Банка России, позволяющий Клиенту в режиме реального времени совершать переводы денежных средств, порядок работы которого регламентирован нормативными актами Банка России, устанавливающими правила платежной системы Банка России, а также правилами и стандартами, установленными АО «Национальная система платежных карт», выполняющим функции операционного и платежного клирингового центра (ОПКЦ) при осуществлении переводов денежных средств в СБП (размещены на официальном сайте ОПКЦ СБП https://sbp.nspk.ru/)

Система «Клиент-Банк» (Система ДБО) - автоматизированная система обмена электронными документами (прием/передача документов и сообщений в электронном виде) между Банком и Клиентами, предоставляющая Клиентам возможность удалённого управления счетами, а также получения банковских Сервисов. Представлена в виде двух альтернативных Систем ДБО «BS-Client (CORREQTS)» и iBank и представляет собой

[8] Предоставляется при наличии технической возможности у Банка в ДБО BS-Client (CORREQTS).

[9] Серверная ЭП не применяется при работе в модуле ЦФК/РЦК и в Системе ДБО «BS-Client (CORREQTS).

[10] Сервис «Личный кабинет ЮЛ» обеспечивается в объеме технически реализованной и доступной в нем функциональности.

совокупность каналов дистанционного банковского обслуживания «Клиент-Банк Онлайн», «Интеграционный Клиент-Банк».

Система Клиента – программное обеспечение Клиента, используемое Клиентом для электронного документооборота между Клиентом и Банком (1С / иная бухгалтерская программа / система управления ресурсами предприятия / иное). При работе с Банком с использованием Канала доступа «Интеграционный Клиент-Банк» должна соответствовать требованиям Приложения № 2 к настоящим Правилам (Обязательства Клиента по выполнению правил безопасной работы при использовании клиентской части Системы ДБО).

Средства криптографической защиты информации (СКЗИ) - шифровальные (криптографические) средства защиты информации конфиденциального характера – аппаратные и (или) программные средства, обеспечивающие создание и проверку УНЭП/УКЭП, а также реализующие алгоритмы криптографического преобразования информации, и предназначенные для защиты информации при осуществлении электронного взаимодействия по каналам связи либо с использованием отчуждаемых носителей информации.

Срок действия Ключей ЭП:

– для УНЭП – максимальный срок, допустимый нормативной документацией разработчика к используемому СКЗИ, рассчитанный с момента создания Ключа ЭП в Системе ДБО. В случае если в эксплуатационной документации срок не указан, то он не превышает 3 (трёх) календарных лет;

– для Серверной ЭП - срок, составляющий 1 (один) календарный год и 3 (три) календарных месяца с момента создания Ключа Серверной ЭП в Системе ДБО;

– для УКЭП – срок, определяемый с момента регистрации Ключа ЭП в Системе ДБО до истечения срока действия Сертификата ЭП, выпущенного Удостоверяющим центром;

– для ПЭП PayControl - срок, составляющий 365 (триста шестьдесят пять) календарных дней с момента выдачи Клиенту Ключей инициализации PayControl.

Срок действия полномочий - срок действия предоставленных Уполномоченному лицу Клиента / Уполномоченному представителю Банка полномочий согласно Документам, подтверждающим полномочия. Пересечение Срока действия Ключа ЭП и Срока действия полномочий является необходимым условием для использования Ключа ЭП при подписи ЭД. В случае прекращения действия полномочий Уполномоченного лица действие Ключа ЭП в Системе ДБО приостанавливается до момента подтверждения факта продления полномочий Уполномоченным лицом. При продлении полномочий генерация новых Ключей ЭП не требуется.

Статус ЭД - параметр электронного документа, определяющий текущий статус его обработки.

Стороны - Банк и Клиент (совместно или по отдельности).

Счёт – счёт в валюте Российской Федерации или иностранной валюте, открываемый Банком Клиенту на основании заключенного Договора банковского счёта, в том числе счёт для расчётов с использованием корпоративных карт, предназначенный для совершения операций, связанных с предпринимательской деятельностью или частной практикой.

Тарифы - система ставок комиссионного вознаграждения, действующая в установленных Тарифных зонах, за услуги, оказываемые Банком Клиентам и порядок их взимания.

Удостоверяющий центр (УЦ) – организация, осуществляющая функции по созданию и выдаче Сертификатов ЭП, а также иные функции, предусмотренные законодательством Российской Федерации, аккредитованная в соответствии с требованиями Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи».

Уполномоченное лицо Клиента (Уполномоченное лицо, УЛ) - физическое лицо - Представитель Клиента, наделенный Клиентом определенными Полномочиями для работы в

Системе ДБО, а также подписания документов, связанных с обеспечением работы в Системе ДБО.

Уполномоченный представитель Банка - руководитель Банка или работник Банка, уполномоченный соответствующей доверенностью, заключать Договоры от имени Банка или подписывать иные документы в соответствии с предоставленными на основании доверенности полномочиями.

Усиленная квалифицированная электронная подпись (УКЭП)[11] - усиленная квалифицированная электронная подпись, Сертификат ЭП которой выдан Уполномоченному лицу Удостоверяющим центром.

Усиленная неквалифицированная электронная подпись (УНЭП) - усиленная неквалифицированная электронная подпись в соответствии с требованиями Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи», бланк ключа проверки которой выдан Банком в порядке, определённом настоящими Правилами.

УНЭП формируется либо на USB-токене[12], либо на Сервере Банка. Допускается формирование УНЭП с применением СКЗИ «Крипто Про CSP» в Системе ДБО «BS-Client (CORREQTS)» для работы в Модуле Транзит 2.0 (далее – УНЭП Транзит 2.0) в соответствии с Инструкцией по установке системы (Приложения №№ 6а/6б к настоящим Правилам). Ключ УНЭП, созданный с применением СКЗИ «Крипто Про CSP», применяется только в Модуле Транзит 2.0. Допускается использование УНЭП[13] для обмена и подписания ЭД посредством Сервиса «Личный кабинет ЮЛ».

Услуги СБП[14] – оказываемые Банком Клиенту услуги по регистрации Клиента, Счета и данных торгово-сервисного предприятия в операционном и платежном клиринговом центре СБП и проведению операций переводов денежных средств с использованием СБП (операции СБП), в порядке и на условиях, определенных Правилами B2B/Правилами B2C. Осуществление операций СБП доступно в Системе «iBank» с использованием функциональности СБП (разделы «СБП B2B», «СБП B2C») Системы «iBank». Услуги предоставляются при условии заключения Договора СБП.

Устройство подтверждения[15] - аппаратно-техническое устройство, отвечающее требованиям Положения Банка России от 17.08.2023 № 821-П «О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств», выдаваемое Клиенту и предназначенное при использовании Канала доступа «Клиент-Банк Онлайн» для дополнительной /обязательной при использовании Серверной ЭП Аутентификации Клиента при подтверждении доступа к Системе ДБО и/или для подтверждения ЭПД Клиента. Перечень разрешённых к использованию устройств устанавливается Банком.

Электронный документ (ЭД) - документированная информация, представленная в электронной форме, то есть в виде, пригодном для восприятия человеком с использованием электронных вычислительных машин, а также для передачи по информационно-телекоммуникационным сетям или обработки в информационных системах, в том числе Электронный платёжный документ и Электронный служебно-информационный документ. Виды ЭД, передаваемые Сторонами по Системе ДБО, определены в Приложении № 7 к настоящим Правилам.

Электронная подпись (ЭП) – информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или

[11] Не применяется при работе в модуле ЦФК/РЦК.

[12] Допускается использование USB-токена Клиента или USB-токена, предоставленного Банком, при наличии технической возможности у Банка.

[13] Использование УНЭП в Сервисе «Личный кабинет ЮЛ» доступно с момента технической реализации.

[14] Сервис Системы быстрых платежей обеспечивается в объеме технически реализованной и доступной в Системе ДБО функциональности.

[15] Предоставляется при наличии технической возможности

иным образом связана с такой информацией, и которая используется для определения лица, подписывающего информацию и целостности подписываемой информации. Для целей настоящих Правил в качестве ЭП Уполномоченного лица выступает УНЭП, включая Серверную ЭП, УКЭП или ПЭП.

Электронный платёжный документ (ЭПД) - ЭД, формат которого установлен Системой ДБО, подписанный УНЭП/ УКЭП/ ПЭП PayControl необходимого количества лиц, уполномоченных на подписание / акцепт ЭПД Клиента, и содержащий поручение/Распоряжение Клиента о совершении операции по Счету.

Электронный служебно-информационный документ (ЭСИД) - ЭД, не являющийся ЭПД (Выписки по счёту, запросы, отчёты, информационные текстовые сообщения в формате «Письмо», документы валютного контроля). ЭСИД также являются любые документы (заявления, подтверждения, уведомления, документы, приводящие к заключению договоров, в том числе в виде оферты, и т.п.), оформляемые на условиях и в рамках заключённых с Банком отдельных договоров / соглашений, предусматривающих порядок электронного обмена Сторонами с использованием Системы ДБО.

API-токен – токен доступа, используемый для авторизации при доступе к API Интеграция, выпускаемый Клиентом в Системе iBank для каждого Уполномоченного лица Клиента, который будет работать посредством API Интеграция.

USB-токен – носитель информации многократного использования со встроенным СКЗИ, обеспечивающий неизвлекаемость (невозможность считывания, закрытая Ключевая информация никогда не покидает пределы токена), размещенной на нем Ключевой информации. Разрешено использование USB-токена, предоставленного Банком или USB-токена, приобретенного Клиентом[16].

PIN-код – технология аутентификации с помощью комбинации из цифр, устанавливаемой Клиентом (и известной только Клиенту) в Мобильном приложении Банка/ Мобильном приложении PayControl после первой успешной Аутентификации.

PUSH-сообщение – сообщение, отправляемое Банком Клиенту с использованием сети Интернет на Мобильное устройство с установленным на нём Мобильным приложением PayControl и/или Мобильным приложением Банка.

SMS-код – определённый набор символов, направленных Банком в SMS-сообщении на Номер телефона УЛ, используемый для формирования Кода подтверждения.

SMS-сообщение – сообщение, направляемое Банком Клиенту на Номер телефона УЛ.

Формы документов и их сокращения, используемые по тексту Правил:

Акт возврата СКЗИ – Акт возврата средств криптографической защиты информации (Приложение № 8 к настоящим Правилам).

Акт приёма – передачи – Акт приёма – передачи ключевых носителей, программного обеспечения и средств криптографической защиты информации (для Клиентов) (Приложение № 9 к настоящим Правилам).

Доверенность – Типовая форма Доверенности (на получателя) (Приложение № 10 к настоящим Правилам).

Заявление – заявление, содержащее волеизъявление Клиента на заключение Договора ДБО и Договора Транзит 2.0, подключение Системы ДБО и параметры для подключения по форме Банка, размещённой на Сайте Банка.

Заявление об изменении данных – заявление, предназначенное для внесения изменений в информацию, предоставленную Клиентом в Заявлении, содержащее волеизъявление Клиента на заключение Договора Транзит 2.0, по форме Банка, размещённой на Сайте Банка.

Заявление о компрометации – Заявление о компрометации (Приложение № 11 к настоящим Правилам).

[16] Услуга предоставляется при наличии технической возможности у Банка.

Заявление о предоставлении модуля – Заявление о предоставлении модуля ЦФК/РЦК Системы ДБО Контролирующей организации (Приложение № 4 настоящим Правилам).

Заявления об установлении / снятии ограничений – Заявление об установлении / снятии ограничений на работу в Системе ДБО (Приложение № 12 к настоящим Правилам).

Инструкция по установке системы - Инструкция по установке Системы «iBank» (Приложение № 6а к настоящим Правилам), «ДБО BS-Client (CORREQTS)» (Приложение № 6б к настоящим Правилам).

Обязательства по безопасной работе - Обязательства клиента по выполнению правил безопасной работы при использовании Клиентской части Системы ДБО (Приложение № 2 к настоящим Правилам).

Перечень электронных документов - Перечень электронных документов, используемых в Системе ДБО (Приложение № 7 к настоящим Правилам).

Положение о технической экспертизе - Положение о порядке проведения технической экспертизы при возникновении спорных ситуаций (Приложение № 13 к настоящим Правилам).

Порядок обмена ЭД - Порядок обмена электронными документами с использованием Системы ДБО, размещенный на Сайте Банка.

Порядок обмена ЭД СБП - Порядок обмена электронными документами с использованием сервиса Системы быстрых платежей Системы ДБО iBank, размещенный на Сайте Банка.

Условия предоставления модуля ЦФК/РЦК - Условия предоставления модуля «Центр финансового контроля / Расчётный центр корпорации» в АО «АБ «РОССИЯ» (Приложение № 3 к настоящим Правилам).

Федеральный закон № 152-ФЗ - Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных».

2. Общие положения

2.1. Настоящие Правила дистанционного банковского обслуживания корпоративных клиентов АО «АБ «РОССИЯ» (далее – Правила) представляют собой условия Договора ДБО и регулируют отношения, возникающие при предоставлении Банком Клиенту услуг Дистанционного банковского обслуживания с использованием Системы ДБО и определяют порядок и условия:

- предоставления и обслуживания Системы ДБО;
- управления Сервисами Системы ДБО;
- обмена электронными документами в Системе ДБО.

Банк осуществляет предоставление услуг Дистанционного банковского обслуживания в соответствии с Правилами, действующими на момент оказания услуги. Действующая версия Правил размещается на Сайте Банка.

2.2. Дистанционное банковское обслуживание может предоставляться Клиентам с подключением или без подключения Счетов к Системе ДБО.

2.3. При наличии у Клиента Счета (-ов) в Банке исполнение обязательств путём обмена ЭД в соответствии с настоящими Правилами осуществляется по всем открытым в Банке Счетам.

2.4. Услуги Дистанционного банковского обслуживания предоставляются Клиентам на основании Договора ДБО.

2.5. Заключая Договор ДБО, Клиент подтверждает, что до заключения Договора ДБО:

- проинформирован об условиях использования Системы ДБО, об ограничениях способов, мест использования и случаях повышенного риска использования Системы ДБО;
- ознакомился с Правилами и Тарифами, согласен и обязуется их неукоснительно соблюдать их требования;
- Уполномоченные лица Клиента согласны получать от Банка на номера мобильных телефонов, предоставленные Клиентом в Банк, SMS-сообщения/ PUSH-сообщения, связанные с предоставлением Клиенту услуг по Договору ДБО, согласны с правилами использования ПЭП PayControl и обязуются при использовании Ключа PayControl соблюдать его конфиденциальность.

2.6. Заключение Договора ДБО осуществляется посредством присоединения Клиента к настоящим Правилам в целом в соответствии со ст. 428 Гражданского кодекса Российской Федерации на основании Заявления, надлежащим образом заполненного и подписанного Клиентом.

В случае использования Сервиса «Личный кабинет ЮЛ» для подачи Заявления, Клиент, подавая Заявление, присоединяется к «Пользовательскому соглашению о предоставлении услуг с использованием сервиса «Личный кабинет юридического лица»» в целом в соответствии со ст. 428 Гражданского кодекса Российской Федерации.

2.7. Договор ДБО заключается при условии предоставления Клиентом в Банк Документов, подтверждающих полномочия Уполномоченных лиц, документов (сведений), установленных действующим законодательством Российской Федерации и требованиями Банка России. При отсутствии в Банке указанных документов Клиента Договор ДБО не заключается, Заявление не принимается Банком к исполнению[17].

2.8. Подать Заявление и необходимые документы (сведения) для заключения Договора ДБО можно на бумажном носителе или с использованием Сервиса «Личный кабинет ЮЛ» [18] в электронном виде, подписанные УКЭП.

---

[17] Повторное представление документов, предоставленных Клиентом ранее, не требуется. Предоставляемые Клиентом документы должны быть актуальны на дату их предоставления.

[18] Функционал Сервиса «Личный кабинет ЮЛ» доступен с момента технической реализации.

2.9. Датой заключения Договора ДБО является дата, указанная в уведомлении Клиента о реквизитах заключенного Договора ДБО, направленном на адрес электронной почты,-указанный клиентом в Заявлении.

2.10. При исполнении Договора ДБО Стороны руководствуются нормами законодательства Российской Федерации, нормативными актами Банка России, настоящими Правилами, нормативными документами Банка. В случае изменения законодательства Российской Федерации, Правила применяются в части, не противоречащей требованиям законодательства Российской Федерации до момента их изменения.

2.11. Состав предоставляемых Банком Сервисов Системы ДБО определяется Приложением № 5 к настоящим Правилам. Банк вправе изменять состав услуг, предоставляемых посредством Системы ДБО, без предварительного уведомления Клиента, а также по своему усмотрению предоставлять полный или ограниченный набор услуг с использованием Системы ДБО в каждом из своих подразделений в конкретный период времени.

2.12. Клиент признаёт, что использование Системы ДБО влечёт дополнительные риски несанкционированного доступа к защищаемой информации с целью осуществления переводов денежных средств лицами, не обладающими правом распоряжения этими денежными средствами. Меры по снижению указанных рисков, а также требования к информационной безопасности изложены в Обязательствах по безопасной работе.

2.13. Клиенту известно, что электронная почта является незащищённым каналом связи, все риски, связанные с возможностью получения доступа неуполномоченных лиц к конфиденциальной информации Клиента (в том числе сведениям, составляющим банковскую тайну) при получении уведомлений об операциях поступления и/или списания по Счёту (ам) в соответствии с п. 2.9 Приложения № 5 к настоящим Правилам, Клиент принимает на себя.

2.14. Стороны подтверждают и соглашаются с тем, что:

2.14.1. Полномочия каждого УЛ в Системе ДБО определяются исходя из Срока действия полномочий, указанного в Документах, подтверждающих полномочия и данных, указанных в Заявлении, заполняемом Клиентом при первоначальной регистрации или в Заявлении об изменении данных, а также в электронном заявлении по форме Банка, реализованном в формате электронного документа в Системе ДБО для предоставления права на размещение средств в неснижаемые остатки, депозиты, в том числе подготовку, подписание, отправку ЭД в Банк и получение ЭД из Банка при условии наличии у Клиента заключённого договора на размещение средств в депозиты, неснижаемые остатки.

При выборе полномочий «Группа 1», «Группа 2» УЛ предоставляется право на просмотр информации по Счетам Клиента, право на распоряжение денежными средствами, находящимися на Счетах Клиента, в том числе подготовку, подписание, отправку ЭД в Банк и получение ЭД из Банка.

При выборе полномочий «Акцепт (визирование)» УЛ предоставляется право на подписание ЭД Визирующей подписью, отправку ЭД в Банк и получение ЭД из Банка.

При выборе полномочий «Просмотр» УЛ предоставляется право на просмотр информации по Счетам Клиента, на подготовку, подтверждение и отправку ЭД в Банк, получение ЭД из Банка.

2.14.2. Изменение полномочий Уполномоченного лица осуществляется путём предоставления в Банк Заявления об изменении данных или электронного заявления по форме Банка, реализованного в формате электронного документа в Системе ДБО для изменения прав на размещение средств в неснижаемые остатки, депозиты и Документов, подтверждающих полномочия.

2.14.3. Полномочия Уполномоченного лица могут быть ограничены на основании Заявления об установлении / снятии ограничений на работу в Системе ДБО в случае, если необходимо:

– установить по определённым Счетам ограниченный перечень УЛ, имеющих

право подписания или акцепта (визирования) ЭПД по Счёту;

– ограничить максимальную сумму платежа;

– подключить возможность устанавливать в Системе ДБО перечень получателей денежных средств.

2.14.4. Получение Клиентом запросов/ уведомлений Банка по Системе ДБО, предоставление Клиентом Банку по Системе ДБО запрошенных документов, а также направление по Системе ДБО ЭД, в том числе указанных в Приложении № 7 к настоящим Правилам, подписанных ЭП Стороны, юридически тождественно получению аналогичных документов на бумажном носителе, заверенных подписями и оттиском печати Стороны, оформленных в соответствии с действующим законодательством Российской Федерации и нормативными документами Банка России.

2.14.5. В качестве единой шкалы времени при работе в Системе ДБО принято московское время. Контрольным временем приёма / отправки ЭД является время системных часов сервера Банка.

2.14.6. Повреждение программного обеспечения средств электронной подписи, установленного у Клиента, в результате вмешательства третьих лиц через сеть Интернет или с использованием иных схем доступа, признаётся Сторонами как прекращение работоспособности Системы ДБО по вине Клиента.

2.14.7. ЭД, передаваемые Клиентом по Системе ДБО, должны быть подписаны ЭП Клиента. Подписание ЭД Уполномоченное лицо осуществляет в соответствии с Порядком обмена ЭД/ Порядком обмена ЭД СБП (в зависимости от используемых Сервисов Системы ДБО):

– УНЭП, включая Серверную ЭП;

– УКЭП;

– Простой ЭП в Системе «ДБО «BS-Client (CORREQTS)» (ПЭП PayControl).

которая позволяет определить Уполномоченное лицо, подписавшее ЭД и приравнивается к документу в письменной форме, оформленному в соответствии с действующим законодательством Российской Федерации.

2.14.8. ЭД, не подписанные ЭП в соответствии с настоящими Правилами, в обработку Банком не принимаются и не являются основанием для предоставления услуг по договору.

2.14.9. Если после подписания ЭП ЭД был изменён, то ЭП данного документа становится некорректной, т.е. проверка ЭП даёт отрицательный результат.

2.14.10. При использовании Клиентом для подписания ЭД двух и более ЭП, ЭД признаётся корректным, если корректны и принадлежат разным лицам, имеющим право подписи, все ЭП, которыми он подписан.

2.15. Применяемые в Системе ДБО механизмы защиты, при условии соблюдения Клиентом Обязательств клиента по выполнению правил безопасной работы при использовании Клиентской части Системы ДБО согласно Приложению № 2 к настоящим Правилам, являются достаточными для обеспечения конфиденциальности, авторства и целостности ЭД, а также обеспечивают невозможность их фальсификации.

2.16. В случае принятия Клиентом решения применять в Системе ДБО УКЭП, в том числе с применением машиночитаемой доверенности, актуализация информации Удостоверяющего центра об отозванных Ключах ЭП и машиночитаемых доверенностях обеспечивается Банком не реже, чем 1 (один) раз в сутки.

2.17. В случае обслуживания Клиента без подключения Счетов к Системе ДБО (без услуг расчетно-кассового обслуживания) или в случае предоставления УЛ полномочий «Просмотр» в Системе ДБО доступно использование:

– Серверной ЭП;

– УНЭП на USB-токене Клиента;

– УКЭП.

2.18. Подтверждение ЭПД в Системе ДБО Уполномоченное лицо осуществляет в

соответствии с Порядком обмена ЭД/ Порядком обмена ЭД СБП с применением Кода подтверждения. Банк обеспечивает направление Клиенту Кода подтверждения/ доведение до Клиента информации о способе получения Кода подтверждения с целью его обязательного применения для подтверждения ЭПД Клиента.

2.19. ЭПД, оформленные в соответствии с нормативными актами Банка России, Порядком переводов исполняются Банком в соответствии с Порядком обмена ЭД/ Порядком обмена ЭД СБП и действующим/ими договором/ми банковского счёта.

2.20. Замена Ключей ЭП с соблюдением требований настоящих Правил не влияет на юридическую силу ЭД, если он был подписан Рабочим ключом ЭП на момент подписания ЭД.

3. Порядок подключения к Системе ДБО

3.1. Банк предоставляет доступ к Системе ДБО после предоставления Клиентом:

– Заявления;

– документов, подтверждающих личность каждого УЛ, либо сведений о реквизитах документов, подтверждающих личность УЛ Клиента, установленных действующим законодательством Российской Федерации и требованиями Банка России;

– документов, подтверждающих полномочия каждого УЛ.

Документы, подтверждающие полномочия УЛ, которому в Системе ДБО предоставлены полномочия «Просмотр», не предоставляются.

При истечении Срока действия полномочий УЛ, которому в Системе ДБО предоставлены полномочия, отличные от полномочий «Просмотр», Клиент предоставляет новые Документы, подтверждающие полномочия, в случае не предоставлении новых документов Банк приостанавливает предоставленные УЛ полномочия в Системе ДБО.

3.2. В Заявлении Клиент определяет параметры подключения:

3.2.1. Уполномоченных лиц и предоставляемые им полномочия в Системе ДБО в соответствии с подп. 2.14.1 настоящих Правил.

3.2.2. Количество ЭП, используемых Клиентом для подписания передаваемых Банку ЭПД, в том числе использование Уполномоченными лицами УНЭП/ Серверной ЭП/ УКЭП/ПЭП PayControl.

3.3. После проверки Банком полноты и корректности указанных в п. 3.1 настоящих Правил документов:

– в зависимости от выбранного варианта защиты Системы и варианта подтверждения исполнения документов в Системе Банк передаёт Устройство подтверждения на основании Акта приёма-передачи, подписанного в порядке аналогичном изложенному в подп. 5.1.4 настоящих Правил;

– в зависимости от подключаемой Банком Клиенту Системы ДБО Клиент либо самостоятельно осуществляет предварительную регистрацию в Системе ДБО, либо получает в Банке Аутентификационные данные УЛ: Логин - на электронную почту (e-mail) УЛ Клиента, Пароль для первоначального входа - на Номер телефона УЛ Клиента, сведения о которых указаны в Заявлении[19].

3.4. Подключение к Системе ДБО производится Клиентом в соответствии с Инструкцией по установке системы.

3.5. Доступ к Системе ДБО «BS-Client (CORREQTS)» может осуществляться с Мобильных устройств через Мобильное приложение Банка. В целях обеспечения информационной безопасности Клиента Банк оставляет за собой право не предоставлять доступ к приложению.

[19] Допускается передача Логина, Пароля в непрозрачном конверте по запросу Клиента.

3.6. Перед подключением Мобильного приложения Банка Клиент обеспечивает работу Мобильного устройства в режиме, определённом Обязательствами по безопасной работе.

3.7. Для доступа к Системе ДБО «BS-Client (CORREQTS)» через Мобильное приложение Банка УЛ необходимо предварительно выполнить активацию Мобильного приложения Банка, для чего:

3.7.1. Установить на Мобильное устройство Мобильное приложение Банка, доступное на сайте Банка по адресу www.abr.ru для Android в соответствии с Инструкцией по установке системы.

3.7.2. Запустить на Мобильном устройстве Мобильное приложение Банка и ввести Аутентификационные данные (Логин и Пароль) от учётной записи Клиента, используемой при входе в Систему ДБО, добавить своё Мобильное устройство в список доверенных устройств, подтверждая действие Ключом ЭП или кодом, полученным от Банка в SMS-сообщении.

3.7.3. Создать в Мобильном приложении Банка пароль многоразового использования для Аутентификации в приложении (в зависимости от платформы и модели мобильного устройства возможно использование аутентификации по отпечатку пальца или изображению лица).

3.8. После совершения указанных действий подключение к Системе «ДБО BS-Client (CORREQTS)» через Мобильное приложение Банка считается завершённым.

4. Интеграция мобильного приложения PayControl с Системой ДБО «BS-Client (CORREQTS)». Регистрация Ключей PayControl. Правила использования ПЭП PayControl

4.1. Возможность подписания ЭД с помощью ПЭП PayControl может быть предоставлена Банком Клиентам, подключенным к Системе ДБО «BS-Client (CORREQTS)» и Мобильному приложению Банка.

4.2. Клиент и Банк признают ПЭП PayControl простой электронной подписью, равнозначной собственноручной подписи Клиента.

4.3. Применение ПЭП PayControl в Системе ДБО при условии соблюдения Клиентом Обязательств клиента по выполнению правил безопасной работы при использовании Клиентской части Системы ДБО согласно Приложению № 2 к настоящим Правилам является достаточным для обеспечения авторства и целостности передаваемой между Сторонами информации и невозможности её фальсификации после подписания.

4.4. Порядок подписания ЭД ПЭП PayControl определён подп. 13.1.7 Порядка обмена ЭД.

4.5. Обязательным условием использования ПЭП PayControl является соблюдение УЛ, использующим Ключ PayControl, его конфиденциальности.

4.6. В целях интеграции Мобильного приложения PayControl с Системой ДБО Уполномоченное лицо Клиента самостоятельно устанавливает Мобильное приложение PayControl, доступное в авторизованных магазинах приложений (AppStore или PlayMarket для iOS/Android соответственно) в соответствии с Инструкцией по установке Системы, на своё Мобильное устройство и производит его активацию.

4.7. УЛ вводит в приложение две части Ключа инициализации, полученного от Банка: QR-код (отображаемый в Системе ДБО «BS-Client (CORREQTS)» или передаваемый на бумажном носителе) и одноразовый SMS-пароль, направленный Банком на Номер телефона УЛ.

4.8. Мобильное приложение PayControl выполняет процедуры по генерации пары ключей (Ключ PayControl и Ключ проверки PayControl) и регистрации Ключа проверки

PayControl на стороне Банка[20]. Запись (сохранение) ключа ЭП осуществляется на Мобильное устройство УЛ.

4.9. УЛ создаёт в Мобильном приложении PayControl пароль многоразового использования для Аутентификации в приложении (в зависимости от платформы и модели мобильного устройства возможно использование аутентификации по отпечатку пальца или изображению лица).

4.10. Перед подключением Мобильного приложения PayControl Клиент обеспечивает работу Мобильного устройства в режиме, определённом Обязательствами по безопасной работе.

4.11. Банк вправе аннулировать выданные Банком Ключи инициализации PayControl в случае, если Клиент по истечении 2 (двух) месяцев с момента их получения от Банка не осуществил процедуру генерации Ключей ЭП в Мобильном приложении PayControl.

4.12. В случаях, когда использование Мобильного приложения PayControl предполагает передачу Клиенту либо хранение Банком конфиденциальной информации, Банк и Клиент обязуются принять все необходимые меры организационного и технического характера для предотвращения доступа третьих лиц к такой информации до передачи её Клиенту, а также во время её хранения Банком/Клиентом.

4.13. В случае отказа Клиента от использования Мобильного приложения PayControl, для перехода Клиента на подписание ЭД в Системе ДБО Ключом ЭП, Клиент предоставляет в Банк надлежащим образом оформленное Заявление об изменении данных.

5. Порядок регистрации Ключей ЭП (УНЭП, УКЭП) в Системе ДБО

5.1. **Регистрация Ключей ЭП, сформированных в Системе ДБО (УНЭП).**

5.1.1. Формирование Ключей ЭП осуществляется в Системе ДБО с сохранением Ключа ЭП / Ключа Серверной ЭП на USB-токен или на Сервере Банка соответственно с использованием СКЗИ.

Перечень СКЗИ, разрешенных к приему от Клиентов для использования в Системе ДБО, определяется Банком и размещается на Сайте Банка в сети Интернет по адресу: https://abr.ru/corp/remote-services/client-bank/;

Для использования СКЗИ на базе USB-токена Клиент может либо получить USB-токен в Банке[21], либо приобрести самостоятельно в соответствии с перечнем СКЗИ разрешенных к приему от Клиентов для использования в Системе ДБО.

5.1.2. Стороны согласны с тем, что использование в Системе ДБО СКЗИ является достаточным для Аутентификации и обеспечения целостности ЭД, т.е. обеспечивают защиту интересов Клиента и Банка.

5.1.3. Клиент в Заявлении / Заявлении об изменении данных при выборе типа ЭП для работы в Системе ДБО определяет необходимость выдачи Банком USB-токена, выбрав либо УНЭП на USB-токене Банка, либо УНЭП на USB-токене Клиента или Серверная ЭП.

5.1.4. Банк при выборе Клиентом в Заявлении / Заявлении об изменении данных УНЭП на USB-токене Банка[20] формирует для Уполномоченного лица конверт с USB-токеном, который передаёт Уполномоченному лицу или лицу, уполномоченному Клиентом на основании Доверенности. Уполномоченное лицо или лицо, уполномоченное на основании Доверенности, подписывает 2 (два) экземпляра Акта приёма-передачи. Один экземпляр Акта приёма-передачи после подписания Сторонами передаётся Клиенту.

5.1.5. Стороны договорились о том, что использование Уполномоченным лицом одного ранее выданного Банком USB-токена в рамках нескольких Клиентов, Представителем

[20] Количество Ключей PayControl (ПЭП (PayControl)) соответствует количеству Мобильных устройств, с которых Уполномоченное лицо планирует работать в Мобильном приложении Банка с возможностью подписания ЭД.

[21] Предоставляется при наличии технической возможности

которых он является, допускается при условии оформления Акта приема-передачи на выданный USB-токен[22] в рамках каждого такого Клиента.

5.1.6. Генерацию своих Ключей ЭП Уполномоченное лицо Клиента осуществляет самостоятельно.

В случае если Уполномоченное лицо Клиента является Представителем нескольких Клиентов разрешена генерация и хранение Ключей ЭП Уполномоченного лица на одном USB-токене, либо приобретенном Клиентом самостоятельно, либо ранее выданном Банком[20] данному Уполномоченному лицу.

5.1.7. Уполномоченное лицо после проведения самостоятельной предварительной регистрации[23] в Системе ДБО (в соответствии с п. 3.3 настоящих Правил) формирует свои Ключи ЭП и сохраняет Ключ ЭП/ Ключ Серверной ЭП на USB-токен или на Сервер Банка соответственно с применением СКЗИ в соответствии с Инструкцией по установке системы.

Для работы в Системе ДБО применяются СКЗИ, предусмотренные настройками используемой Системы ДБО.

Для работы в Модуле Транзит 2.0[24] применяются СКЗИ «КриптоПро CSP», предусмотренные настройками, реализованными в Системе ДБО «BS-Client (CORREQTS)».

В процессе генерации Ключей ЭП формируется электронный запрос на регистрацию Ключа проверки ЭП (далее - ЗРКП ЭП), который средствами Системы ДБО направляется в Банк и Бланк ключа ЭП с учетом подп. 5.1.8 настоящих Правил.

Бланк ключа ЭП необходимо предоставить в Банк:

– на бумажном носителе в 2 (двух) экземплярах. Бланк ключа ЭП подписывается Представителем Клиента, заверяется оттиском печати Клиента (при наличии);

– либо в электронном виде по Системе ДБО на отдельный адрес «Отдел открытия счетов» в виде вложения Бланка ключа ЭП в формате Word или в виде сканированного образа в ЭСИД «Письмо», подписанного ЭП Представителя Клиента, зарегистрированной в Системе ДБО.

Если ЭСИД «Письмо» подписано Представителем Клиента, действующим без доверенности, то Бланк ключа ЭП предоставляется в формате Word или в виде сканированного образа Бланка ключа ЭП.

Если ЭСИД «Письмо» подписано Представителем Клиента, действующим на основании доверенности, то Бланк ключа ЭП предоставляется в виде сканированного образа и ЭП в сообщении и подпись в сканированном образе Бланка ключа ЭП должны принадлежать одному лицу;

– либо в электронном виде с использованием Канала ЭДО[25]. Данный канал используется для передачи Бланка ключа ЭП, владельцем Ключа ЭП по которому является единоличный исполнительный орган (далее – ЕИО) Клиента - юридического лица, Клиент - иностранная структура без образования юридического лица/ индивидуальный предприниматель (далее – ИП) / физическое лицо, занимающееся в установленном законодательством Российской Федерации порядке частной практикой. Подписание Бланка Ключа ЭП осуществляется с использованием УКЭП в Канале ЭДО.

При этом Клиент обязан предоставить в Банк Документы, подтверждающие полномочия лица, подписавшего Бланк Ключа ЭП, если такие документы не были предоставлены Банку ранее.

5.1.8. Уполномоченное лицо при генерации Ключа Серверной ЭП безусловно соглашается на его хранение в закрытом контуре на Сервере Банка. Клиент и Уполномоченное лицо доверяют Банку хранение Ключа Серверной ЭП в закрытом контуре (защищённом

[22] Доступно при наличии технической возможности у Банка.
[23] Для Системы ДБО «BS-Client (CORREQTS)» Уполномоченное лицо использует Логин и Пароль, полученный в соответствии с п. 3.3 настоящих Правил.
[24] Ключ ЭП, созданный с применением СКЗИ «Крипто Про CSP», применяется только в Модуле Транзит 2.0.
[25] Доступно с момента технической реализации.

хранилище) на Сервере Банка и его использование для формирования Серверной ЭП под Электронными документами Системы iBank. Доверенность оформляется Клиентом и Уполномоченным лицом и предоставляется в Банк вместе с Бланком ключа ЭП.
Предоставление Бланка ключа ЭП и доверенности для Серверной ЭП в электронном виде по Системе ДБО в соответствии с подп. 5.1.7 настоящих Правил допускается только в виде вложения сканированного образа Бланка ключа ЭП и доверенности в ЭСИД «Письмо», подписанного ЭП Представителя Клиента, зарегистрированной в Системе ДБО.

5.1.9. Банк осуществляет прием и проверку Бланка Ключа ЭП. При условии положительного результата проверки Банк регистрирует Ключ проверки ЭП и активирует Ключ ЭП в Системе ДБО на основании ЗРКП ЭП и Бланка Ключа ЭП (в соответствии с реализованным форматом Бланка Ключа ЭП в Системе ДБО), при этом ограничивает возможность работы с Ключом ЭП сроком действия предоставленных Уполномоченному лицу полномочий.

При этом Банк не имеет доступа к Ключу ЭП Клиента:

– в случае использования USB-токена для хранения Ключей ЭП в Банке хранятся только Ключи проверки ЭП Клиента;

– в случае использования Серверной ЭП Ключи Серверной ЭП Клиента хранятся на Сервере Банка в контейнерах, зашифрованных Паролем к Ключу Серверной ЭП, установленным Уполномоченным лицом Клиента.

5.1.10. Подтверждением факта активации Ключа ЭП Банком является доступность работы с этим Ключом ЭП в Системе ДБО.

5.1.11. По факту регистрации Ключа проверки ЭП (активации Ключа ЭП/ Ключа Серверной ЭП) Система ДБО автоматически уведомляет УЛ о подключении к Системе ДБО посредством:

– направления уведомления на адрес электронной почты, зарегистрированной в Банке на основании Заявления;

– установки статуса ЗРКП ЭП «Исполнен», информация о котором доступна в разделе «Безопасность» / «Запросы на новый сертификат» интерфейса Системы ДБО «BS-Client (CORREQTS)»;

– обеспечения возможности просмотра, выгрузки и (при необходимости) печати Бланка ключа ЭП УЛ в меню «Настройки/ Безопасность/ Запросы на новый сертификат» интерфейса Системы ДБО «BS-Client (CORREQTS)»/ «Электронные подписи» интерфейса Системы iBank**.**

5.1.12. Срок действия ЗРКП ЭП, направленного в Банк в процессе генерации Ключа ЭП, составляет 15 (пятнадцать) рабочих дней с даты его формирования. По истечении указанного срока и при непредставлении Клиентом Бланка Ключа ЭП Банк вправе аннулировать ЗРКП ЭП. Для формирования нового Бланка Ключа ЭП Клиенту необходимо выполнить действия, предусмотренные подп. 5.1.7 - 5.1.9 настоящих Правил.

5.1.13. Клиент согласен с тем, что обмен документами с использованием Канала ЭДО, не является разглашением Банком сведений, составляющих персональные данные и банковскую тайну Клиента.

5.1.14. Стороны подтверждают, что в случае если услуги, связанные с использованием Канала ЭДО, предоставляются Клиенту третьим лицом, то Банк не несет какой-либо ответственности перед Клиентом, связанной с негативными последствиями для Клиента использования Канала ЭДО, в том числе, но не исключительно, Банк не несет какой-либо ответственности за ущерб, причиненный Клиенту и/или третьим лицам в результате:

– разглашения неуполномоченным лицам Ключа ЭП Клиента (его Уполномоченного лица), его утраты, передачи или иной формы Компрометации вне зависимости от причин;

– реализации угроз несанкционированного доступа неуполномоченных лиц к части Канала ЭДО, подлежащей использованию со стороны Клиента;

– неработоспособности оборудования и программных средств Клиента и третьих лиц, повлекшей за собой невозможность доступа Клиента к соответствующей системе электронного документооборота и получения Банком Бланка Ключа ЭП;

– каких-либо иных негативных последствий, возникших в результате использования Канала ЭДО.

Клиент согласен с тем, что обмен документами с использованием Канала ЭДО, не является разглашением Банком сведений, составляющих персональные данные и банковскую тайну Клиента.

Стороны подтверждают, что до начала использования Канала ЭДО, удостоверились в наличии технической возможности обмена ЭД через операторов электронного документооборота, используемых Сторонами.

5.2. **Регистрация Ключей ЭП, выпущенных Удостоверяющим центром (УКЭП).**

5.2.1. Клиент согласно внутреннему регламенту работы Удостоверяющего центра инициирует выпуск Ключей ЭП, предоставляет в Банк Сертификат ЭП, выданный Удостоверяющим центром на каждое Уполномоченное лицо, в электронном виде в файле с расширением *.cer в формате X509 и машиночитаемую доверенность (при предоставлении Сертификата ЭП на физическое лицо) в электронном виде (архив с двумя файлами, МЧД в XML-формате + файл подписи *.sig/*.sgn) на электронный адрес службы технической поддержки Системы ДБО certdbo@abr.ru, либо по Системе ДБО в формате «Письмо» на адрес операционного подразделения, осуществляющего обслуживание Клиента.

5.2.2. Банк на основании Заявления / Заявления об изменении данных и Сертификата ЭП, полученного в соответствии с подп. 5.2.1 настоящих Правил, регистрирует Ключи проверки ЭП в Системе ДБО на каждое Уполномоченное лицо, ограничивая возможность работы с Ключом ЭП сроком действия Сертификата ЭП, выданного Удостоверяющим центром.

6. Порядок перерегистрации Ключей ЭП (УНЭП, УКЭП, ПЭП PayControl) в Системе ДБО

6.1. Перерегистрация Ключей ЭП в Системе ДБО инициируется Уполномоченным лицом Клиента.

Контроль Срока действия Ключей ЭП Уполномоченное лицо Клиента осуществляет самостоятельно.

6.2. Плановая перерегистрация Ключей ЭП (УНЭП) осуществляется в связи с истечением Срока их действия.

6.3. Банк оповещает Уполномоченное лицо о необходимости перерегистрации Ключей ЭП (УНЭП)/ Ключей PayControl за 30 (тридцать) календарных дней до окончания Срока действия Ключей ЭП.

6.4. Если Уполномоченное лицо Клиента не произвело перерегистрацию Ключей ЭП до истечения их Срока действия, в Системе ДБО осуществляется автоматическая блокировка просроченных Ключей Клиента.

Блокировка Ключей ЭП также осуществляется по причине Компрометации/ подозрения о Компрометации, в случае изменения наименования или организационно-правовой формы Клиента / юридического лица, выполняющего функции единоличного исполнительного органа Клиента (ЕИО), либо в случае смены Мобильного устройства Уполномоченного лица, на котором установлено Мобильное приложение PayControl.

6.5. Особенности процесса перерегистрации Ключей ЭП:

6.5.1. Перегенерация Ключей ЭП (УНЭП) может осуществляться с использованием USB-токена, предоставленного Банком или USB-токена, приобретенного Клиентом/ Сервера

Банка. В случае изменения используемого Клиентом Ключевого носителя или типа ЭП Клиент подает в Банк Заявление об изменении данных.

6.5.2. Перерегистрация до истечения Срока действия Ключей ЭП, а также при изменении полномочий Уполномоченных лиц Клиента в Системе ДБО**,** ФИО Уполномоченных лиц Клиента, осуществляется:

– для Ключей ЭП (УНЭП) / Ключей PayControl - на основании электронного запроса на перегенерацию сертификата ключа ЭП/ продление ключей PayControl Уполномоченным лицом в Системе ДБО, при этом для Ключа ЭП (УНЭП) предоставление Бланка ключа проверки ЭП на бумажном носителе не требуется, для Ключей PayControl УЛ Клиента необходимо осуществить активацию нового Ключа PayControl в Мобильном приложении PayControl;

– для Ключей ЭП (УКЭП) - в порядке, определённом п. 5.2 настоящих Правил.

6.5.3. Перерегистрация после истечения Срока действия Ключей ЭП, а также в случае Компрометации/ подозрения о Компрометации, изменения наименования или организационно-правовой формы Клиента / юридического лица, выполняющего функции единоличного исполнительного органа Клиента (ЕИО), смены Мобильного устройства Уполномоченного лица, на котором установлено Мобильное приложение PayControl, требует осуществления перерегистрации:

– Ключей ЭП (УНЭП, включая Серверную ЭП) в соответствии с п. 5.1 настоящих Правил;

– Ключей ЭП (УКЭП) в соответствии с п. 5.2 настоящих Правил;

– Ключей PayControl в соответствии с подп. 6.5.4 настоящих Правил.

6.5.4. Перерегистрация Ключей PayControl после блокировки осуществляется по факту повторной активации Мобильного приложения PayControl в соответствии с пп. 4.7 - 4.8 настоящих Правил, для чего Клиент запрашивает в Банке новые Ключи инициализации PayControl:

– предоставив в Банк Заявление об изменении данных в порядке, определённом подп. 16.3.2 настоящих Правил;

– либо направив сообщение на электронный адрес службы технической поддержки Системы ДБО 3356525@abr.ru. Текст сообщения должен содержать наименование Клиента, ФИО заявителя, ФИО и должность Уполномоченного лица Клиента, которому необходимо предоставление новых Ключей инициализации PayControl.

По факту поступления сообщения Банк получает подтверждение необходимости направления новых Ключей инициализации PayControl по номеру телефона подтверждения экстренной блокировки Ключей ЭП и направляет Ключи инициализации PayControl Уполномоченному лицу Клиента. В случае если по факту телефонного звонка Клиенту подтверждение не получено Банк отказывает в отправке новых Ключей инициализации PayControl. Информация о номере телефона подтверждения экстренной блокировки Ключей ЭП указывается Клиентом в Заявлении. В случае если Клиент не представил в Банк номер телефона подтверждения экстренной блокировки Ключей ЭП, получение новых Ключей инициализации PayControl на основании сообщения на электронный адрес не осуществляется. Для их получения Клиенту необходимо предоставить в Банк Заявление об изменении данных в порядке, определённом подп. 16.3.2 настоящих Правил.

6.6. Продление полномочий Уполномоченного лица без изменения прав, установленных в Системе ДБО, в течение Срока действия Ключа ЭП не требует перерегистрации Ключей ЭП. Продление срока полномочий осуществляется на основании предоставленных в Банк Документов, подтверждающих полномочия.

6.7. Информация о факте перерегистрации Ключей ЭП Банком доступна Клиенту в меню «Настройки/ Безопасность/ Сертификаты» интерфейса системы «ДБО BS-Client (CORREQTS)» / «Электронная подпись» интерфейса системы iBank.

6.8. В случае перехода Клиента с одной Системы ДБО на другую по инициативе Банка действующие Уполномоченные лица Клиента осуществляют генерацию Ключей ЭП (УНЭП) в «новой» Системе ДБО в порядке, определенном п. 6.5.3 настоящих Правил ДБО, с предоставлением Бланка Ключа ЭП способами, определенными п. 5.1.8 настоящих Правил ДБО, при этом разрешено направить Бланк Ключа ЭП по «старой» Системе ДБО при наличии в ней Рабочего Ключа ЭП, подписав ЭСИД «Письмо» Ключом ЭП Представителя Клиента, действующего без доверенности или действующего на основании доверенности, либо Ключом ЭП Уполномоченного лица, на имя которого сформированы Ключи ЭП в «новой» Системе ДБО.

7. Предоставление режима работы «Акцепт (визирование)»

7.1. Режим работы «Акцепт (визирование)» предоставляется Банком с целью получения согласия на распоряжение денежными средствами, находящимися на Счёте(-ах) Клиента (далее – Контролируемый счет) с использованием Визирующей подписи в соответствии с законодательством Российской Федерации и/или на основании условий договора, заключённого между Клиентом и его контрагентом (третьим лицом) или Банком.

7.2. Режим работы «Акцепт (визирование)» предоставляется Банком только для Счетов в рублях Российской Федерации.

7.3. С целью установления режима работы «Акцепт (визирование)» Клиент в Заявлении/ Заявлении об изменении данных в разделе о порядке приёма электронных платёжных документов выбирает буллит «с визирующей подписью».

В случае если «Акцепт (визирование)» будет осуществлять представитель юридического лица, отличного от Клиента, то в указанном разделе заполняются поля, содержащие данные об организации, осуществляющей «Акцепт (визирование)», представителем которой является Уполномоченное лицо.

~~7.4.~~ Предоставление права Визирующей подписи Уполномоченным лицам для работы в режиме «Акцепт (визирование)» осуществляется на основании Заявления/ Заявления об изменении данных Клиента посредством выбора полномочий «акцепт (визирование)» с предоставлением Документов, подтверждающих полномочия.

7.5. Стороны договорились, что подача Заявления/ Заявления об изменении данных Клиентом – владельцем Контролируемых счетов с указанием перечня Уполномоченных лиц является выражением согласия Клиента на установление режима «Акцепт (визирование)» к Контролируемым счетам в случае, если получение согласия на распоряжение денежными средствами по Контролируемым счетам будет осуществляться на основании заключённого Клиентом договора.

7.6. Ограничение перечня Контролируемых счетов (при наличии необходимости) осуществляется на основании Заявления об установлении / снятии ограничений, поданного Клиентом.

7.7. Владельцем Визирующей подписи может быть УЛ Клиента, либо юридического лица, отличного от Клиента. Предоставляя право Визирующей подписи представителю юридического лица, отличного от Клиента, Клиент - владелец Контролируемых счетов выражает согласие на предоставление информации, составляющей банковскую тайну (информации об операции по Счетам), что рассматривается Сторонами, как предоставление информации уполномоченному представителю Клиента - владельца Контролируемых счетов.

7.8. В рамках работы в режиме «Акцепт (визирование)» Клиент поручает Банку:

7.8.1. Предоставить Уполномоченным лицам, имеющим на основании Заявления/ Заявления об изменении данных полномочия «акцепт (визирование)», возможность проставления Визирующей подписи под ЭПД на проведение расходных операций.

7.8.2. Принимать к исполнению ЭПД по Контролируемым счетам при условии получения Визирующей подписи Уполномоченного лица. В случае отсутствия Визирующей

подписи Уполномоченного лица Банк не принимает к исполнению ЭПД по Контролируемым счетам с уведомлением Клиента об отказе в приёме к исполнению ЭПД в порядке, установленном настоящим Договором.

7.9. В случае наличия у Клиента Визирующей подписи Банк не несёт ответственности за неисполнение распоряжений Клиента, не содержащих Визирующую подпись.

8. Права и обязанности Клиента

8.1. **Клиент имеет право:**

8.1.1. Использовать Систему ДБО для обмена электронными документами.

8.1.2. Выбрать вид ЭП для подписания ЭД в Системе ДБО[26].

8.1.3. Направлять в Банк посредством Системы ДБО документы согласно Перечню электронных документов (Приложение № 7 к настоящим Правилам), в том числе документы в соответствии с другими договорами, заключёнными между Сторонами. Оформление таких документов должно соответствовать требованиям, предусмотренным законодательством Российской Федерации, заключёнными договорами и настоящими Правилами.

8.1.4 Отзывать ЭД, переданные Банку, в соответствии с Порядком переводов, размещённом на официальном сайте Банка в сети Интернет www.abr.ru. Запрос на отзыв ЭД направляется в Банк с использованием Системы ДБО в соответствии с Порядком обмена ЭД.

8.1.4. Оформлять и передавать в Банк распоряжения на бумажных носителях в период неработоспособности (неисправности) Системы ДБО, а также при приостановлении обслуживания Клиента с использованием Системы ДБО в соответствии с положениями настоящих Правил.

8.1.5. Прекращать полномочия / осуществлять подключение/ изменение данных/ отключение/ блокировку Ключа ЭП Уполномоченного лица в Системе ДБО посредством направления Заявления об изменении данных / Заявления о предоставлении модуля в порядке, определённом подп. 16.3.2 настоящих Правил.

8.1.6. Устанавливать и снимать ограничения прав на работу в Системе ДБО и ограничение по параметрам операций в Системе ДБО при обслуживании с использованием Канала доступа «Клиент-Банк Онлайн» на основании Заявления об установлении / снятии ограничений.

8.1.7. Инициировать получение:

– дополнительного/ нового USB-Токена, Устройства подтверждения, в том числе в случае поломки, утраты,

– нового Пароля (смену Пароля), в том числе в случае утраты,

– новых Ключей инициализации PayControl для активации Мобильного приложения PayControl при смене Мобильного устройства и/или Номера телефона УЛ Клиента,

посредством предоставления в Банк Заявления об изменении данных / Заявления о предоставлении модуля в порядке, определённом подп. 16.3.2 настоящих Правил. Получение дополнительного USB-Токена, Устройства подтверждения осуществляется Клиентом в офисе Банка.

8.1.8. Подключать/отключать и пользоваться Сервисами Системы ДБО в соответствии с условиями их предоставления, в порядке, определённом Приложением № 5 к настоящим Правилам до момента их отключения Клиентом.

8.1.9. Получать у Банка консультации по обслуживанию через Систему ДБО.

8.1.10. Направлять в Банк в случае получения от Банка уведомления о приостановлении приема к исполнению Распоряжения (ЭПД) Клиента при выявлении Банком операции, соответствующей признакам осуществления перевода денежных средств без добровольного

[26] ПЭП PayControl предоставляется в системе «ДБО BS-Client (CORREQTS)».

согласия клиента в соответствии с требованиями Федерального закона № 161-ФЗ не позднее одного дня, следующего за днем приостановления приема к исполнению Распоряжения (ЭПД)

– подтверждение Распоряжения (ЭПД) либо в формате, определенном Банком в уведомлении о приостановлении приема к исполнению Распоряжения (ЭПД), либо в виде заявления в произвольной форме с указанием значимых реквизитов Распоряжения (ЭПД)

следующими способами:

– на бумажном носителе, подписанное Представителем Клиента и заверенное печатью (при наличии) по месту нахождения отделения Банка,

или

– по Системе ДБО (при наличии у Клиента нескомпрометированных Ключей ЭП) - на адрес «Приостановление по 161-ФЗ», в виде сканированного образа подписанного заявления в формате ЭСИД «Письмо».

8.1.11. Обратиться в Банк с заявлением об исключении сведений, относящихся к Клиенту и (или) его Системе ДБО, из Базы данных Банка России:

– на бумажном носителе, подписанным Представителем Клиента и заверенным печатью (при наличии) по месту нахождения отделения Банка,

или

– по Системе ДБО (при наличии у Клиента нескомпрометированных Ключей ЭП) - на адрес «Приостановление по 161-ФЗ» в виде сканированного образа подписанного заявления в формате ЭСИД «Письмо».

8.1.12. При смене Уполномоченных лиц использовать ранее выданный Банком Клиенту USB-токен новым Уполномоченным лицом. Стороны пришли к соглашению, что фактом согласия и волеизъявления Клиента на передачу[27] ранее выданного Банком USB-токена от одного Уполномоченного лица другому Уполномоченному лицу Клиента является факт подачи Клиентом Акта возврата и Заявления об изменении данных/Заявления о предоставлении модуля при подключении нового Уполномоченного лица. Информация об изменении данных об Уполномоченном лице фиксируется на основании Акта приема-передачи.

8.2. **Клиент обязуется:**

8.2.1. Организовать Клиентское рабочее место для работы в Системе ДБО в соответствии с Инструкцией по установке системы (Приложения №№ 6а/6б к настоящим Правилам) и поддерживать в рабочем состоянии свои программно-технические средства.

8.2.2. Соблюдать Порядок обмена ЭД, Порядок обмена ЭД СБП, размещенные на Сайте Банка.

8.2.3. Выполнять требования, указанные в Обязательствах по безопасной работе, а также по запросу Банка подтверждать выполнение указанных требований. Риски, возникающие в связи с невыполнением требований, указанных в Обязательствах по безопасной работе, несёт Клиент.

8.2.4. Использовать свои программно-технические средства в целях выполнения условий Договора.

8.2.5. Использовать Систему ДБО в соответствии с настоящими Правилами.

8.2.6. Оплачивать услуги ДБО в соответствии с Тарифами Банка в порядке, предусмотренном разделом 12 настоящих Правил.

8.2.7. По запросу Банка предоставить заверенные подписями и оттиском печати Клиента (при наличии) копии ЭД, принятых и/или исполненных Банком, в течение 2 (двух) рабочих дней с даты получения запроса Банка.

8.2.8. Не предоставлять третьим лицам, не являющимся УЛ Клиента, возможность распоряжения посредством Системы ДБО денежными средствами, находящимися на Счёте,

[27] Передача USB-токена новому Уполномоченному лицу возможна только после уничтожения с данного USB-токена Ключа ЭП прежнего владельца.

не предоставлять им право использования SMS-пароля, Логина, API-токена, Ключевого носителя с Ключами ЭП, Мобильного устройства с sim-картой Номера телефона УЛ Клиента, осуществляющей приём SMS-паролей, Мобильного устройства с активированным Мобильным приложением PayControl, Аутентификационных данных (Логин и Пароль) от учётной записи Клиента, с помощью которой осуществляется вход в Систему ДБО при использовании Серверной ЭП, Пароля к Ключу Серверной ЭП.

8.2.9. Завершить работу Системы ДБО на всех рабочих местах Клиента и уведомить Банк в порядке, определённом Приложением № 2 к настоящим Правилам, оформив Заявление о компрометации, в случае наличия подозрения о Компрометации, полной или временной утраты контроля доступа третьих лиц к программным средствам Системы ДБО, наступления иных случаев Компрометации (в день выявления факта Компрометации или возникновения подозрения о Компрометации). Риски, возникающие в связи с ненадлежащим исполнением обязанности, указанной в настоящем пункте, несёт Клиент. Любая передача ЭД, произведённая Клиентом с использованием скомпрометированного Ключа ЭП, освобождает Банк от любых видов ответственности.

8.2.10. Самостоятельно обращаться в Банк для получения сведений об изменениях и дополнениях, внесённых в настоящие Правила, с целью ознакомления (либо получать данную информацию в сети Интернет на официальном сайте Банка www.abr.ru).

8.2.11. Предоставлять Банку информацию, необходимую для исполнения Банком требований законодательства о противодействии легализации (отмыванию) доходов, полученных преступным путём, финансированию терроризма и финансированию распространения оружия массового уничтожения, включая информацию о своих выгодоприобретателях, учредителях (участниках) и бенефициарных владельцах, а также о своем статусе доверительного собственника (управляющего) иностранной структуры без образования юридического лица, протектора и иные документы по запросу Банка.

8.2.12. В случае изменения в течение срока действия Договора документов и сведений, необходимых для установления полномочий лиц, которым предоставлено право доступа в Систему ДБО, и их идентификации, отзыва доверенностей, в том числе машиночитаемых, и полномочий таких лиц, предоставить указанные сведения в Банк и провести, в случае необходимости, все необходимые мероприятия по смене Аутентификационных данных, перевыпуску Ключей ЭП не позднее следующего рабочего дня с даты возникновения указанных изменений.

8.2.13. Обеспечивать возможность круглосуточной связи по номеру телефона, указанному в Заявлении, для подтверждения необходимости экстренной блокировки Ключей ЭП.

8.2.14. Контролировать исполнение ЭД Банком, регулярно проверять движение денежных средств по Счетам.

В случае утраты доступа к Системе ДБО и (или) использования Системы ДБО без добровольного согласия клиента в соответствии с требованиями Федерального закона № 161-ФЗ незамедлительно, но не позднее дня, следующего за днем получения от Банка уведомления о совершенной операции, Клиент обязан направить в Банк уведомление об обнаружении факта утраты доступа к Системе ДБО и (или) использования Системы ДБО без добровольного согласия клиента в произвольной форме, а в случае Компрометации/ подозрения на Компрометацию Ключа (-ей) ЭП дополнительно Заявление о компрометации в соответствии с подп. 8.2.8 настоящих Правил, способами, определенными подп. 16.3.2 настоящих Правил.

При нарушении Клиентом срока информирования Банка в случае обнаружения факта утраты доступа к Системе ДБО и (или) использования Системы ДБО без добровольного согласия клиента, Банк не возмещает Клиенту сумму операции, совершенной без добровольного согласия Клиента с использованием Системы ДБО.

8.2.15. Инициировать на периодической основе сеанс связи с Банком (вход в Систему ДБО) в целях своевременного получения уведомлений об истечении Срока действия Ключей ЭП (УНЭП)/ Ключей PayControl.

8.2.16. По требованию Банка в течение 2 (двух) рабочих дней с даты получения такого требования предоставить достоверную информацию об использовании Системы ДБО Клиентом, в том числе информацию о Клиентских рабочих местах и использовании ЭП в формате, указанном в запросе Банка, информацию о подтверждении актуальности сведений об УЛ, указанных в Заявлении/ Заявлении об изменении данных, информацию об ЭД и расчётах по Счетам.

8.2.17. Оказывать содействие Банку в установлении фактов несанкционированного доступа к Системе ДБО (Компрометации). Обеспечивать доступ работников Банка к техническим средствам, на которых установлена клиентская часть Системы ДБО, для проведения работ по её установке и сопровождению.

8.2.18. В случае замены Банком программного обеспечения Системы ДБО, в течение 30 (тридцати) дней с даты получения уведомления Банка, получить у Банка и ввести в эксплуатацию необходимые программные средства.

В случае замены Банком СКЗИ, Ключевых носителей, используемых при работе в Системе ДБО, в течение 30 (тридцати) дней с даты получения уведомления Банка приобрести и установить необходимые средства или получить их в Банке на основании Заявления об изменении данных или в соответствии с процедурой, предусмотренной уведомлением Банка.

8.2.19. В случае получения от Банка уведомления по Системе ДБО об обновлении программного обеспечения Клиентского рабочего места в зависимости от используемого типа клиентского модуля и действий, указанных в полученном уведомлении, Клиент обязан либо скачать размещённую обновлённую версию программного обеспечения с официального сайта Банка и установить обновление на рабочее место Клиента, либо при очередном сеансе связи подтвердить установку пакета обновлений в автоматическом режиме.

8.2.20. Располагать согласием Уполномоченных лиц Клиента с правилами использования ПЭП PayControl, с получением SMS-сообщений/PUSH-сообщений, связанных с предоставлением услуг по Договору ДБО, на Номера мобильных телефонов, а также письменным обязательством Уполномоченных лиц при создании и использовании Ключа PayControl соблюдать его конфиденциальность. По требованию Банка предоставлять Банку указанные согласия и письменные обязательства.

8.2.21. Исполнять требования действующего законодательства Российской Федерации, в том числе Федерального закона № 152-ФЗ.

8.2.22. По требованию Банка обеспечить предоставление в Банк согласия на обработку (как с использованием средств автоматизации, так и без их использования) персональных данных Уполномоченных лиц Клиента, персональные данные которых содержатся в представляемых Клиентом Банку документах в целях заключения и исполнения Договора ДБО в соответствии с требованиями действующего законодательства Российской Федерации, в том числе Федерального закона № 152-ФЗ.

8.2.23. В течение срока действия Договора ДБО обеспечить либо сохранность полученных в рамках Договора ДБО программных СКЗИ, технологической документации и ключевой информации, либо контроль наличия действующего сертификата(-ов) соответствия требованиям ФСБ России на СКЗИ и последующий периодический контроль срока действия сертификата(-ов) соответствия требованиям ФСБ России на СКЗИ, при использовании USB-токена с СКЗИ, приобретенного Клиентом.

8.2.24. В случае расторжения Договора ДБО или отказа от использования Ключевого носителя, выданного Банком, осуществить возврат в Банк по Акту возврата СКЗИ Ключевых носителей, технологической документации и ключевой информации. В случае расторжения Договора ДБО возврат Ключевых носителей, выданных Банком, осуществить не позднее даты расторжения Договора ДБО.

9. Права и обязанности Банка[28]

9.1. **Банк имеет право:**

9.1.1. Требовать у Клиента документы и сведения, необходимые для осуществления функций, предусмотренных действующими законодательными и иными нормативными актами Российской Федерации, в том числе для выполнения Банком требований Федерального закона от 07.08.2001 № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» (далее – Федеральный закон № 115-ФЗ).

9.1.2. Блокировать использование Ключей ЭП Клиента после окончания срока их действия или блокировать доступ УЛ к Системе ДБО в случае истечения срока действия сертификата соответствия требованиям ФСБ России на СКЗИ, при использовании USB-токена с СКЗИ, приобретенного Клиентом, или в случае истечения Срока действия полномочий / отзыва полномочий Уполномоченного лица Клиента на основании данных предоставленных Клиентом в соответствии с подп. 8.2.12 настоящих Правил, либо на основании данных, полученных Банком из открытых официальных источников, подтверждающих истечение Срока действия полномочий или отзыв полномочий Уполномоченного лица Клиента (например, ЕГРЮЛ/ЕГРИП, исполнительные производства, арбитражные дела, бухгалтерская отчётность и т.д.).

9.1.3. В одностороннем порядке вводить лимиты/ограничения на совершение операций в Системе ДБО, а также другие меры безопасности, направленные на сокращение возможных потерь Клиента.

В случае введения Банком лимитов/ограничений Банк уведомляет Клиента любым доступным способом, в том числе по Системе ДБО, в виде SMS-сообщений по Номерам телефонов УЛ, телефонным номерам, указанным в разделе «Контактные данные клиента» Заявления или полученным Банком при идентификации Клиента, не позднее 5 (пяти) рабочих дней до введения указанных лимитов/ограничений.

9.1.4. Не принимать к исполнению полученные от Клиента ЭД в случае ненадлежащего их оформления согласно требованиям действующего законодательства Российской Федерации и настоящих Правил или при сомнении в подлинности ЭД. Об отказе в приеме к исполнению ЭД Банк сообщает Клиенту в течение 1 (одного) рабочего дня со дня получения Банком таких документов. Настоящая информация доводится до Клиента с использованием Системы ДБО.

9.1.5. При открытии новых Счетов Клиенту подключать их к Системе ДБО в автоматическом режиме без предоставления Клиентом заявления на их подключение.

В случае, если Клиент использует две Системы ДБО и в одной из Систем ДБО запрашивает установление режима «Акцепт» по Счёту (-ам), то в другой Системе ДБО такой Счет (-а) переводится в режим «Просмотр», исключающий проведение операций по Счёту (-ам), режим «Акцепт» не устанавливается.

9.1.6. Направлять Клиенту посредством Системы ДБО документы согласно Перечню ЭД, в том числе документы в соответствии с другими договорами, заключёнными между Сторонами. Оформление таких документов должно соответствовать требованиям, предусмотренным законодательством Российской Федерации, соответствующими договорами и настоящими Правилам.

9.1.7. Приостановить обслуживание Клиента по Системе ДБО, ограничив проведение расходных операций по Счету (-ам), с направлением уведомления Клиенту способами, определёнными подп. 16.3.1 настоящих Правил, в следующих случаях, включая, но не ограничиваясь:

[28] Права и обязанности Банка, относящиеся к обслуживанию расчётных счетов Клиента в Системе ДБО, не распространяются на Клиентов, не имеющих расчётных счетов в Банке.

– на время спорных ситуаций между Клиентом и Банком до урегулирования разногласий;

– при наличии подозрений о Компрометации;

– при возникновении однократной просрочки оплаты услуг Банка;

– в случае несоблюдения Клиентом требований настоящих Правил;

– на период нахождения сведений, относящихся к Клиенту и (или) его Системе ДБО, в Базе данных Банка России, уведомив о праве Клиента подать в порядке, установленном Банком России, заявление в Банк России, в том числе через Банк, об исключении сведений, относящихся к Клиенту и (или) его Системе ДБО, из Базы данных Банка России.

9.1.8. Приостановить предоставление услуг по Договору ДБО, заблокировав доступ Клиента к Системе ДБО, сроком до 3 (трех) календарных месяцев с последующим отказом от Договора ДБО в одностороннем порядке по истечении 6 (шести) и более календарных месяцев в соответствии с разделом 14 настоящих Правил.

9.1.9. Банк возобновляет обслуживание по Системе ДБО:

– незамедлительно по факту исключения из Базы данных Банка России, сведений, относящихся к Клиенту;

– по факту погашения всей суммы задолженности по оплате услуг Банка до наступления даты расторжения Договора ДБО;

– либо после устранения иных причин приостановления, указанных в уведомлении.

9.1.10. Осуществлять в операционное время Банка выполнение неотложных, аварийных и регламентных работ, связанных с обслуживанием Системы ДБО, уведомив Клиента посредством размещения информации на внешнем сайте Банка в разделе «Вход в Интернет-Банк» (окно входа в Систему ДБО) https://online.abr.ru или https://ibank.abr.ru/ibank2/#/).

9.1.11. Отказать Клиенту в обслуживании по Системе ДБО:

9.1.11.1. С переходом на прием от такого Клиента расчётных (платёжных) документов только на бумажном носителе, направив Клиенту уведомление способом, определённым подп. 16.3.1 настоящих Правил, в следующих случаях:

– непредставления/несвоевременного представления или представления Клиентом неполных сведений (документов) при идентификации/обновлении сведений о Клиенте, его Представителе, Выгодоприобретателе, Бенефициарном (ых) владельце (ах);

– возникновения подозрений, что разовая операция либо совокупность операций и (или) действий Клиента, связанных с проведением каких-либо операций, его Представителя в рамках обслуживания Клиента, осуществляются в целях легализации (отмывания) доходов, полученных преступным путем, или финансирования терроризма;

– отсутствия постоянно действующего исполнительного органа или представителя Клиента-юридического лица по адресу местонахождения юридического лица, указанному в Едином государственном реестре юридических лиц.

9.1.11.2. Направив Клиенту уведомление по установленной Банком форме по Системе ДБО не позднее 5 (пяти) рабочих дней, следующих за днем применения к Клиенту мер, установленных в п. 5 ст. 7.7 Федерального закона № 115-ФЗ, в случае их применения.

9.1.12. Запрашивать у Клиента подтверждение исполнения ЭПД при выявлении Банком операции, соответствующей признакам осуществления перевода денежных средств без добровольного согласия клиента, а также информацию, что перевод денежных средств не является переводом без добровольного согласия Клиента, и документы, подтверждающие обоснованность получения денежных средств.

9.1.13. Аннулировать выданные Банком Ключи инициализации PayControl в случае, если Клиент по истечение 2 (двух) месяцев с момента их получения от Банка не осуществил процедуру генерации Ключей ЭП в Мобильном приложении PayControl в порядке, определённом пп. 4.7 - 4.8 настоящих Правил.

9.1.14. Отказать Клиенту в подключении Системы ДБО и/или Мобильного приложения PayControl, если Клиентом не соблюдены требования действующего законодательства Российской Федерации, настоящих Правил, а также в случае, если Банком установлен факт предоставления Клиентом недостоверной информации, необходимой для подключения Системы ДБО и/или Мобильного приложения PayControl.

9.1.15. Осуществлять сбор информации о Мобильном устройстве для целей противодействия угрозам, возникающим при использовании Мобильного приложения PayControl, такой как геолокация, информация об устройстве, информация о подключении к сети, события, происходящие в Мобильном приложении PayControl, обнаруженное потенциально вредоносное программное обеспечение.

9.1.16. Взимать за оказываемые в соответствии с Правилами услуги ДБО в порядке заранее данного акцепта Клиента с любого Счёта Клиента, открытого в Банке или в другой кредитной организации, если это предусмотрено режимом счета, суммы комиссионного вознаграждения согласно действующим Тарифам Банка в соответствии с порядком, определённым п. 12.7 настоящих Правил.

9.1.17. Отказать Клиенту в предоставлении Сервисов Системы ДБО в случае отсутствия/ недостаточности денежных средств на Счёте Клиента, либо невнесения Клиентом наличных денежных средств в кассу Банка, для оплаты комиссионного вознаграждения Банка за предоставление таких сервисов в соответствии с Тарифами, действующими на момент обращения Клиента.

9.1.18. Запрашивать предоставление в Банк согласия на обработку (как с использованием средств автоматизации, так и без их использования) персональных данных Уполномоченных лиц Клиента, персональные данные которых содержатся в представляемых Клиентом Банку документах с целью исполнения Договора ДБО в соответствии с требованиями действующего законодательства Российской Федерации, в том числе Федерального закона № 152-ФЗ.

9.1.19. Производить замену:

– программного обеспечения Системы ДБО без согласия Клиента,

– СКЗИ, Ключевых носителей, используемых при работе в Системе ДБО,

уведомив об этом Клиента не менее чем за 30 (тридцать) календарных дней до ввода в эксплуатацию нового программного обеспечения Системы ДБО/ замены СКЗИ, Ключевых носителей, посредством направления информационного сообщения по Системе ДБО в формате «Письмо».

9.1.20. Вносить изменения в Правила и/или Тарифы в одностороннем порядке, уведомляя об этом Клиента в соответствии с пп. 12.4, 13.2 настоящих Правил.

9.1.21. Приостановить пересылку Клиенту Кодов подтверждения/ SMS-сообщений/ PUSH-сообщений и иной защищаемой информации, а также осуществление перевода денежных средств на основании Кодов подтверждения/ PUSH-сообщений без предварительного уведомления Клиента, в случае если Банку стало известно о признаках, указывающих на изменение получателя информации, направленной Банком и используемой при Аутентификации Клиента. К указанным признакам может быть отнесена информация о замене SIM-карты Клиента, прекращении обслуживания по Системе ДБО или смене Номера телефона УЛ.

9.1.22. Отказаться от Договора ДБО в одностороннем порядке в соответствии с разделом 14 настоящих Правил.

9.2. **Банк обязуется:**

9.2.1. Предоставить Клиенту программное обеспечение/инструкции по осуществлению доступа к программному обеспечению, а также программное средство контроля целостности этого программного обеспечения (включая инструкцию по применению) / информацию о порядке его получения у разработчика (при необходимости)), а

также инструкцию по эксплуатации/общедоступный ресурс, с использованием которого Клиент имеет возможность получить указанную инструкцию (эксплуатационную документацию).

9.2.2. Произвести предусмотренные настоящими Правилами действия, необходимые для предоставления Клиенту возможности работы с Системой ДБО, а также обеспечить установление ограничений прав на работу в Системе ДБО и ограничений по параметрам операций в Системе ДБО, указанных Клиентом в Заявлении об установлении / снятии ограничений, при обслуживании с использованием Канала «Клиент-Банк Онлайн».

9.2.3. Обеспечить конфиденциальность информации о Счёте (-ах) Клиента и защиту от несанкционированного доступа к операциям по Счёту (-ам) со стороны Банка при условии выполнения Клиентом условий Договора ДБО, касающихся защиты конфиденциальной информации от несанкционированного доступа, в том числе изложенных в Обязательствах по безопасной работе.

9.2.4. Обеспечить при использовании Клиентом Сервера Банка защиту от несанкционированного доступа и хранение Ключа Серверной ЭП в закрытом контуре на Сервере Банка, а также использование Ключа Серверной ЭП для формирования Серверной ЭП под Электронными документами Системы iBank по поручению Клиента и Уполномоченного лица, данному в соответствии с п. 5.1.8 настоящих Правил, при условии выполнения Клиентом условий Договора ДБО, касающихся защиты конфиденциальной информации от несанкционированного доступа, в том числе изложенных в Обязательствах по безопасной работе.

9.2.5. Приостановить прием к исполнению Распоряжения (ЭПД) при выявлении Банком операции, соответствующей признакам осуществления перевода денежных средств без добровольного согласия Клиента в соответствии с требованиями Федерального закона № 161-ФЗ на 2 (два) дня.

9.2.6. Уведомлять Клиента любым доступным способом, в том числе по Системе ДБО, на e-mail, в виде SMS-сообщений по телефонным номерам, указанным в Заявлении или полученным Банком при идентификации Клиента, о приостановлении приема к исполнению Распоряжения (ЭПД) Клиента и/или о приостановлении зачисления в случае выявления операции, соответствующей признакам осуществления перевода денежных средств без добровольного согласия клиента в соответствии с требованиями Федерального закона № 161-ФЗ, а также предоставлять Клиенту информацию о рекомендациях по снижению рисков повторного осуществления перевода денежных средств без добровольного согласия Клиента и о возможности подтвердить Распоряжение (ЭПД), прием к исполнению которого был приостановлен, не позднее одного дня, следующего за днем приостановления приема к исполнению указанного Распоряжения (ЭПД) в соответствии с подп. 9.2.4 настоящих Правил.

9.2.7. Незамедлительно принять к исполнению Распоряжение (ЭПД) Клиента, прием к исполнению которого был приостановлен при выявлении Банком операции, соответствующей признакам осуществления перевода денежных средств без добровольного согласия Клиента при получении от Клиента подтверждения посредством направления в Банк подтверждения Распоряжения (ЭПД) способом, предусмотренным подп. 8.1.11 настоящих Правил, при условии отсутствия в Базе данных Банка России, информации, относящейся к получателю средств по Распоряжению (ЭПД), а также при отсутствии иных установленных законодательством РФ и настоящими Правилами ДБО оснований не принимать Распоряжение (ЭПД) Клиента к исполнению.

9.2.8. Не принимать к исполнению Распоряжение (ЭПД) Клиента при неполучении от Клиента подтверждения Распоряжения (ЭПД) и/или информации, дополнительно запрошенной Банком в соответствии с подп. 9.1.12 настоящих Правил, способом, предусмотренным подп. 8.1.11 настоящих Правил, в случае если прием к исполнению ЭПД был приостановлен при выявлении Банком признаков осуществления перевода денежных средств без добровольного согласия клиента.

9.2.9. Приостановить прием к исполнению подтвержденного Распоряжения (ЭПД) на 2 (два) дня со дня направления Клиентом подтверждения Распоряжения (ЭПД) в порядке, предусмотренном подп. 8.1.11 настоящих Правил, в случае получения от Банка России информации, содержащейся в Базе данных Банка России, относящейся к получателю средств по подтвержденному Распоряжению (ЭПД), и уведомить Клиента любым доступным способом, в том числе по Системе ДБО, на e-mail, в виде SMS-сообщений по телефонным номерам, указанным в Заявлении или полученным Банком при идентификации Клиента, о приостановлении приема к исполнению подтвержденного Распоряжения (ЭПД) с указанием причины и срока приостановления.

9.2.10. Принять к исполнению подтвержденное Распоряжение (ЭПД) Клиента, прием к исполнению которого был приостановлен в соответствии с подп. 9.2.8 настоящих Правил, незамедлительно по истечении 2 (двух) дней со дня направления Клиентом подтверждения Распоряжения (ЭПД) в порядке, предусмотренном подп. 8.1.1 настоящих Правил, при отсутствии иных установленных законодательством и настоящими Правилами ДБО оснований не принимать Распоряжение (ЭПД) Клиента к исполнению.

9.2.11. Приостановить обслуживание Клиента по Системе ДБО, ограничив проведение расходных операций по Счету (-ам), на период нахождения в Базе данных Банка России, сведений, относящихся к Клиенту и (или) его Системе ДБО, в том числе сведений федерального органа исполнительной власти в сфере внутренних дел о совершенных противоправных действиях сведений, и уведомить Клиента способами**,** определёнными пп. 16.3.1 настоящих Правил, о приостановлении обслуживания по Системе ДБО, а также о праве Клиента подать в порядке, установленном Банком России, заявление в Банк России, в том числе через Банк, об исключении относящихся сведений, к Клиенту и (или) его Системе ДБО, из Базы данных Банка России.

Банк незамедлительно возобновляет обслуживание по Системе ДБО по факту исключения из Базы данных Банка Россия, сведений, относящихся к Клиенту, и уведомляет Клиента способами, определёнными Договором ДБО, о возобновлении обслуживания по Системе ДБО**.**

9.2.12. Уведомлять Клиента о совершении операции Клиента по Счёту (-ам) с использованием Системы ДБО путём предоставления Выписки по счёту, а также путём смены Статуса ЭД в Системе ДБО в соответствии с Порядком обмена ЭД/ Порядком обмена ЭД СБП. Уведомлять Клиента об отказе в совершении операции/ отказе от заключения договора /решении о расторжении договора банковского счета, с использованием Системы ДБО с формированием соответствующего уведомления по форме, установленной Банком[29]. Обязанность Банка по уведомлению Клиента считается исполненной в момент смены Статуса ЭД при обработке документа Банком в Системе ДБО. Статусы, присваиваемые ЭД, определены Порядком обмена ЭД/ Порядком обмена ЭД СБП.

9.2.13. По факту получения от Клиента информации о Компрометации в соответствии с подп. 8.2.8 настоящих Правил или в случае выявления Банком факта Компрометации/ любых подозрений на Компрометацию при наличии у Банка информации о событиях, относящихся к Компрометации, Банк незамедлительно блокирует скомпрометированный Ключ ЭП/ Ключ PayControl/ доступ УЛ Клиента к Системе ДБО, прекращает приём и исполнение любых ЭД, подписанных скомпрометированным Ключом ЭП/ Ключом PayControl.

Фактом уведомления Клиента является либо факт исполнения Заявления о компрометации, либо направление уведомления способом, определенным подп. 16.3.1 настоящих Правил.

9.2.14. Возместить Клиенту в течение 30 (тридцати) дней после получения от Клиента уведомления об обнаружении факта утраты доступа к Системе ДБО и (или) использования

[29] Уведомление формируется в случае, если решение об отказе от заключения договора банковского счета/о расторжении договора банковского счета принято Банком в соответствии с п. 5.2 ст. 7 Федерального закона № 115-ФЗ; решение об отказе в совершении операции принято Банком в соответствии с п. 11 ст. 7 Федерального закона № 115-ФЗ.

Системы ДБО без добровольного согласия клиента (далее – уведомление) в порядке, определённом подп. 8.2.14 настоящих Правил, сумму операции, совершённой без добровольного согласия Клиента с использованием указанной в уведомлении Системы ДБО после получения Банком указанного уведомления.

9.2.15. Осуществлять техническое сопровождение и консультирование Клиента в случаях и порядке, предусмотренных настоящими Правилами, и в соответствии с Тарифами Банка.

9.2.16. Обеспечить рассмотрение полученных заявлений Клиента и предоставить Клиенту возможность получать информацию о результатах рассмотрения заявлений, в том числе в письменной форме по требованию Клиента, в срок не более 15 (пятнадцати) рабочих дней с даты регистрации таких заявлений или в иные сроки, установленные законодательством Российской Федерации и настоящими Правилами.

9.2.17. Исполнять требования действующего законодательства Российской Федерации, в том числе Федерального закона № 152-ФЗ.

9.2.18. Обеспечить взаимодействие с ИС «Одно окно» в порядке, установленном Приказом Минфина России от 26.09.2022 № 142н «Об утверждении Порядка взаимодействия банков, иных кредитных организаций с информационной системой «Одно окно» в сфере внешнеторговой деятельности».

9.2.19. Предоставлять Клиенту информацию, полученную в результате взаимодействия с ИС «Одно окно», необходимую для перевода денежных средств, в неизменном виде посредством направления уведомления по Системе ДБО. Содержание уведомления определяется техническими настройками взаимодействия Банка с ИС «Одно окно».

В случае осуществления перевода денежных средств на основании распоряжения, составленного Клиентом в результате взаимодействия с ИС «Одно окно» при условии достаточности денежных средств на Счёте направить информацию о таком переводе денежных средств в ИС «Одно окно».

Вместе с тем, по поручению Клиента, полученному в результате взаимодействия с ИС «Одно окно», предоставить оператору ИС «Одно окно» информацию об исполнении указанного Клиентом Распоряжения о переводе. При этом при направлении посредством ИС «Одно окно» указанного Распоряжения Клиентом даётся согласие на предоставление информации, составляющей банковскую тайну, в соответствии с ч. 6 ст. 47.1 Федерального закона от 08.12.2003 № 164-ФЗ «Об основах государственного регулирования внешнеторговой деятельности».

9.2.20. Отказать Клиенту в заключении Договора ДБО в случае, если от Банка России получена информация, содержащаяся в Базе данных, которая содержит сведения, относящиеся к Клиенту и (или) его электронному средству платежа с незамедлительным уведомлением Клиента об отказе в заключении Договора ДБО с указанием причины такого отказа[30].

9.2.21. Информировать Клиента по основаниям, предусмотренным Федеральным законом № 115-ФЗ, в порядке, определенном Договором банковского счета.

10. Ответственность Сторон

10.1. Соблюдение положений настоящих Правил является обязательным для Банка и Клиента.

10.2. Клиент несёт ответственность за достоверность предоставляемых Банку сведений, послуживших основанием для заключения Договора.

10.3. Банк несёт ответственность за обеспечение конфиденциальности предоставленных Клиентом сведений, составляющих персональные данные и банковскую тайну. Сведения о проводимых операциях могут быть представлены третьим лицам в порядке, установленном действующим законодательством Российской Федерации.

[30] Требования, указанные в настоящем абзаце, вступают в силу с 01.09.2025.

10.4. Банк не несёт ответственность за сбой в работе Системы ДБО по вине Клиента, в том числе в случаях:

– самостоятельного внесения Клиентом изменений в программное обеспечение или настройки Системы ДБО, не согласованные с Банком;

– повреждения операционной системы Клиента вредоносными программами;

– нестабильной работы операционной системы или аппаратного обеспечения Клиентского рабочего места,

– несвоевременной смены Ключей ЭП Клиентом.

10.5. Банк не несёт ответственность за убытки, возникшие в результате:

– неисполнения клиентом правил безопасной работы при использовании клиентской части Системы ДБО, отражённых в Обязательствах по безопасной работе (Приложение № 2 к настоящим Правилам);

– умышленной или неосторожной утраты (порчи, передачи, утери, разглашения) клиентом применяемых в Системе ДБО паролей, Ключей ЭП, Ключевого носителя, Мобильных устройств, а также другой конфиденциальной информации и/или программного обеспечения, при условии исполнения Банком обязанности, предусмотренной подп. 9.2.13 настоящих Правил;

– несвоевременного сообщения Клиентом в Банк о Компрометации в соответствии с подп. 8.2.9 настоящих Правил;

– несанкционированного доступа третьих лиц к Клиентскому рабочему месту, Ключевому носителю, Мобильному устройству Клиента и/или Мобильному приложению PayControl, Мобильному приложению Банка при условии исполнения Банком обязанности, предусмотренной подп. 9.2.13 настоящих Правил;

– заражения рабочего места Клиента вредоносными программами;

– вследствие сбоев в работе линий связи, обрыва линий связи, выхода из строя оборудования у телефонного оператора и/или оператора доступа к сети Интернет;

– действий Банка, совершаемых в рамках исполнения Федерального закона № 115-ФЗ;

– действий Банка в результате надлежащего исполнения требований Федерального закона № 161-ФЗ.

10.6. Банк не несёт ответственность, если операции по Счёту задерживаются в результате ошибок Клиента и/или третьих лиц, допущенных при заполнении реквизитов документов при оформлении Клиентом и/или третьими лицами распоряжения на перевод денежных средств со Счёта и в других случаях, возникших не по вине Банка.

10.7. Банк не несёт ответственность за возможные технические помехи в работе линий связи, приводящие к невозможности получения SMS-сообщений Банка и передачи (приёма) Клиентом ЭД в соответствии с настоящими Правилами.

10.8. Банк не несёт ответственность за невозможность получения Клиентом Кода подтверждения в случае указания неверного номера телефона или не информирования Банка об его изменении.

10.9. Банк не несёт ответственности за исполнение /последствия обработки ЭД, являющихся основанием для проведения операций по Счёту Клиента/ полученных от Клиента в случае нарушения Клиентом своевременности информирования Банка об изменениях состава, полномочий, срока действия полномочий Уполномоченных лиц Клиента, на имя которых зарегистрированы Ключи проверки ЭП, отзыва доверенностей, в том числе машиночитаемых, и полномочий таких лиц.

10.10. Банк не несёт ответственности за актуальность, полноту и достоверность информации, размещённой в открытых официальных источниках, доступ к которой будет получен Клиентом с использованием Сервиса проверки контрагентов. Банк не несёт ответственности за убытки или ущерб Клиента, возникшие в результате использования данного сервиса, за любой прямой или косвенный ущерб и упущенную выгоду, вызванные

использованием информации сервиса, за иные последствия применения полученной информации.

10.11. Клиент несёт риск возникновения убытков и иных неблагоприятных последствий, возникших в результате неисполнения положений подп. 8.2.8 – 8.2.9 настоящих Правил, а также при выявлении Банком операции, имеющей признаки осуществления перевода денежных средств без добровольного согласия клиента в соответствии с требованиями Федерального закона № 161-ФЗ, в случае проведения такой операции после получения от Банка уведомления о приостановлении подтвержденного Распоряжения (ЭПД).

10.12. Клиент несёт ответственность за сохранность Аутентификационных данных при использовании Системы ДБО.

В случае использования Клиентом в Системе ДБО самостоятельно приобретенного USB-токена с СКЗИ за соответствие используемого СКЗИ требованиям ФСБ России к СКЗИ и перечню разрешенных к использованию СКЗИ, установленному Банком.

10.13. В случае нарушения Клиентом условий использования полученного в рамках настоящих Правил программного обеспечения (в том числе, но, не ограничиваясь случаями тиражирования и/или передачи программного обеспечения третьим лицам, вскрытия технологии и (или) дизассемблирование и(или) декомпиляции программного продукта), и предъявления третьими лицами требований к Банку, Клиент обязуется возместить Банку убытки в полном объёме.

10.14. Стороны обязуются за собственный счёт организовать рабочие места для работы в Системе ДБО в соответствии с настоящими Правилами и поддерживать в рабочем состоянии свои программно-технические средства.

10.15. Стороны взаимно освобождаются от имущественной ответственности за неисполнение или ненадлежащее исполнение обязательств по Договору ДБО, если оно вызвано факторами непреодолимой силы: чрезвычайными обстоятельствами, стихийными бедствиями, противоправными действиями третьих лиц, актами государственных или муниципальных органов власти и управления, обязательными для выполнения одной из Сторон, при условии, что Сторона, которая не в состоянии выполнить свои обязательства по Договору ДБО в силу вышеуказанных причин, предприняла все усилия для незамедлительного информирования другой Стороны в письменной форме о форс-мажорных обстоятельствах и о скорейшей ликвидации их последствий.

11.Разрешение споров и конфликтов

11.1. Все споры и разногласия, возникающие при исполнении Договора ДБО, Стороны будут стремиться разрешать путём переговоров.

На время разрешения спорной ситуации Стороны имеют право приостановить действие Договора ДБО, уведомив об этом другую Сторону посредством отправки соответствующего информационного сообщения с использованием Системы ДБО с обязательным его дублированием на бумажном носителе, направив его курьером или по почте заказным письмом в срок не позднее 1 (одного) рабочего дня, следующего за днём отправки такого информационного сообщения. Соответствующее уведомление (заявление) на бумажном носителе должно быть подписано представителем Банка и заверено оттиском печати соответствующей Стороны (при наличии).

11.2. При возникновении спорных /конфликтных ситуаций, связанных с использованием Системы ДБО при обмене ЭД, они рассматриваются в порядке, установленном Положением о порядке проведения технической экспертизы после подачи Клиентом заявления в Банк с указанием сути претензии. Результаты рассмотрения заявления доводятся до Клиента в установленные п. 11.3 настоящих Правил сроки.

11.3. Банк рассматривает заявление Клиента не более 15 (пятнадцати) рабочих дней с даты регистрации заявления или в иные сроки, установленные действующим законодательством Российской Федерации и настоящими Правилами.

11.4. Стороны признают, что:

11.4.1. Основополагающим документом при рассмотрении конфликтной ситуации, связанной с обменом ЭД посредством Системы ДБО, является протокол работы Системы ДБО, сформированный Банком.

11.4.2. ЭД, направленные Сторонами друг другу по Системе ДБО, а также журналы учёта ЭД, ведущиеся в Системе ДБО, могут быть представлены Банком в качестве доказательств в арбитражном суде.

11.5. В целях рассмотрения конфликтных ситуаций, связанных с подлинностью ЭД/ обменом ЭД с использованием Клиентом Системы ДБО, совместным решением Сторон может быть создана экспертная комиссия, задачей которой является проведение технической экспертизы в соответствии с Положением о порядке проведения технической экспертизы. Решение оформляется в виде акта(-ов) о результатах проведения технической экспертизы, в котором фиксируются выводы, к которым пришла экспертная комиссия в результате проведённых в соответствии с Положением о порядке проведения технической экспертизы мероприятий, который (-ые) подписывается (-ются) членами экспертной комиссии.

11.6. Стороны признают решение экспертной комиссии, оформленное актом, обязательным для участников конфликтной ситуации, и обязуются добровольно исполнять решение экспертной комиссии в установленные указанным актом сроки. В случае если одна из Сторон в результате работы экспертной комиссии признана виновной, то такая Сторона обязуется компенсировать другой Стороне причинённый реальный ущерб.

11.7. Расходы по формированию и работе экспертной комиссии (за исключением расходов на выплату вознаграждения за работу в составе экспертной комиссии экспертам, привлечённым по инициативе Клиента) возлагаются на Банк. В случае признания экспертной комиссией требований Клиента необоснованными, в течение 5 (пяти) рабочих дней с момента составления акта экспертной комиссии Банк предъявляет Клиенту требование о возмещении всех указанных расходов. Банк возмещает расходы путём списания денежных средств в порядке заранее данного договором банковского счёта акцепта со Счетов Клиента, открытых им в Банке, или указанные расходы оплачиваются Клиентом со Счетов, открытых в других кредитных организациях.

11.8. Уклонение какой-либо Стороны от участия в создании или работе экспертной комиссии может привести к невозможности её создания и работы, но не может привести к невозможности урегулирования конфликта в судебном порядке.

11.9. В случае не достижения соглашения Сторон, отсутствия согласия по спорным вопросам и добровольного исполнения решения экспертной комиссии споры и все материалы по Договору ДБО передаются на рассмотрение суда по месту нахождения Банка или его филиала.

11.10. Разбор спорных ситуаций, связанных с использованием Сервиса проверки контрагентов, осуществляется путём предоставления Банком информации об официальных открытых источниках информации, на основании которых работает Сервис проверки контрагентов, после подачи Клиентом заявления в Банк, в порядке, определённом п. 11.2 настоящих Правил.

12.Порядок оплаты услуг

12.1. Стоимость, порядок и сроки оплаты услуг Банка определяются Тарифами Банка, действующими в Тарифной зоне по месту нахождения подразделения Банка, в котором заключён Договор. Выбор Тарифа фиксируется Клиентом в Заявлении /Заявлении об изменении данных.

В случае закрытия Клиентом Счета в подразделении Банка, в котором с Клиентом был заключен Договор, и при наличии Счета (-ов) Клиента в иных подразделениях Банка, осуществляется перевод на обслуживание в подразделение Банка, в котором Клиент открыл второй Счет. Взимание комиссионного вознаграждения будет осуществляться по Тарифу Тарифной зоны по месту нахождения подразделения Банка, в который переведен Клиент, с первого числа месяца следующего за месяцем перевода Клиента на обслуживание в иное подразделение Банка.

12.2. Тарифы устанавливаются Банком для всех клиентов (групп клиентов) Банка или индивидуально в отношении Клиента (далее – Индивидуальные тарифы).

12.3. Информирование Клиентов о действующих Тарифах осуществляется всеми перечисленными способами или одним из них:

– на сайте Банка по адресу: www.abr.ru;

– в подразделениях Банка (с адресами мест нахождения Банка можно ознакомиться на сайте Банка);

– посредством Системы ДБО.

12.4. Банк вправе в одностороннем порядке вносить изменения в Тарифы. Об изменениях, внесенных в Тарифы, и дате вступления изменений в силу, Банк уведомляет Клиентов способами, указанными в п. 12.3 настоящих Правил не позднее, чем за 5 (пять) календарных дней до введения в действие новой редакции Тарифов, если иное не предусмотрено соглашением между Клиентом и Банком или Тарифами.

12.5. Об установлении / внесении изменений в Индивидуальные тарифы, их условиях, дате вступления в силу и сроке их действия, Банк уведомляет Клиентов по Системе ДБО. Изменение Тарифов, включая нумерацию пунктов, наименование услуги\операции, порядок и сроки оплаты, порядок налогообложения распространяется на действующие Индивидуальные тарифы с сохранением размера тарифных ставок, установленных Индивидуальными тарифами.

12.6. Стоимость неисключительного права на использование клиентской части Системы ДБО включена в стоимость услуг Банка по установке и эксплуатации Системы ДБО. Стороны вправе заключить дополнительное соглашение в целях фиксации стоимости неисключительного права на использование клиентской части Системы ДБО в пределах установленных Банком тарифов.

12.7. В случае если Счёт для взимания комиссионного вознаграждения, в том числе указанный в Заявлении /Заявлении об изменении данных, открыт в Банке, списание комиссионного вознаграждения со Счёта осуществляется в порядке, предусмотренном договором банковского счёта.

В случае если счёт для взимания комиссионного вознаграждения, открыт в другой кредитной организации Клиент:

– в целях предоставления права Банку взимать комиссионное вознаграждение со счёта, открытого в другой кредитной организации, обеспечивает заключение договора, соглашения (заявления и т.д.), на основании которого Банку предоставлено право списывать денежные средства со счёта;

– в целях самостоятельной оплаты комиссионного вознаграждения Банка вносит наличные денежные средства в рублях Российской Федерации в кассу Банка по месту обслуживания, либо осуществляет оплату по выставленному Банком счёту на сумму комиссии, подлежащей уплате.

Оплата комиссионного вознаграждения может осуществляться Клиентом в безналичном порядке по направленному Банком QR-коду через Систему быстрых платежей.

12.8. При использовании модуля ЦФК/РЦК для всех организаций, подключённых к модулю ЦФК/РЦК Контролирующей организации, применяется единый для всех Счетов принцип списания комиссий Банка за оказываемые услуги, установленный Контролирующей организацией в Заявлении о предоставлении модуля Контролирующей организации.

Изменение счёта для списания комиссий Банка осуществляется только для всех зарегистрированных в модуле ЦФК/РЦК Счетов.

13. Опубликование информации. Порядок внесения изменений и/или дополнений в Правила

13.1. Под опубликованием Правил понимается размещение Банком информации на официальном сайте Банка в сети Интернет www.abr.ru. Датой опубликования Правил считается дата первого размещения Правил на официальном сайте Банка в сети Интернет www.abr.ru.

13.2. Банк информирует Клиента об изменениях и/или дополнениях, вносимых в Правила, посредством размещения информации в подразделениях Банка, осуществляющих обслуживание Клиентов, и на официальном сайте Банка в сети Интернет www.abr.ru не позднее, чем за 5 (пять) календарных дней до вступления в силу новой редакции.

13.3. Банк не несёт ответственности, если информация об изменении и/или дополнении Правил, опубликованная в порядке и в сроки, установленные Правилами, не была получена и/или изучена и/или правильно истолкована Клиентом.

13.4. Банк вправе осуществлять дополнительное информирование об изменениях и/или дополнениях, вносимых в Правила в электронном виде по используемой Клиентом Системе ДБО.

13.5. Любые изменения и/или дополнения в Правила, в том числе утверждённая Банком новая редакция Правил, с момента вступления их в силу равно распространяются на всех лиц, заключивших Договор ДБО, в том числе ранее даты вступления в силу изменений и/или дополнений.

13.6. Отсутствие отказа Клиента от обслуживания по Системе ДБО (уведомления об отказе от Договора ДБО), а также проведение им операций, предусмотренных Системой ДБО, является согласием Клиента на присоединение к новой редакции Правил и с применением новых Тарифов.

14. Срок действия Договора ДБО, расторжение Договора ДБО

14.1. Договор ДБО вступает в силу с момента его заключения и действует в течение 1 (одного) года. Если ни одна из Сторон не заявит возражение о продлении срока его действия, уведомив об этом другую Сторону не менее чем за 3 (три) рабочих дня до даты окончания срока действия Договора ДБО, Договор ДБО автоматически продлевается (пролонгируется) на 1 (один) год. Срок действия Договора ДБО может продлеваться (пролонгироваться) неограниченное количество раз.

14.2. Любая из Сторон вправе отказаться от Договора ДБО полностью в одностороннем порядке путём предварительного уведомления другой Стороны в порядке, определённом п. 16.3 настоящих Правил. При этом Стороны проводят взаиморасчёты по обязательствам, возникшим из Договора ДБО до даты его расторжения.

14.3. Банк вправе отказаться от Договора ДБО в одностороннем порядке в случае неоплаты Клиентом предоставленных Банком услуг по Договору ДБО и/или в случае отсутствия операций по Счетам, а при использовании Системы ДБО без открытия счетов в Банке - в случае выявления факта неиспользования Системы ДБО, в течение 6 (шести) и более месяцев, направив Клиенту уведомление способами, определёнными подп. 16.3.1 настоящих Правил.

14.4. Договор ДБО расторгается при закрытии последнего открытого в Банке Счёта в соответствии с условиями заключенного с Банком Договора банковского счета при условии отсутствия у Клиента других банковских продуктов/ услуг, предоставляемых с использованием Системы ДБО, без дополнительного уведомления Клиента.

При наличии у Клиента других банковских продуктов/ услуг, предоставляемых с использованием Системы ДБО, основанием для расторжения Договора ДБО является отказ/расторжение договоров, обеспечивающих получение банковских продуктов/ услуг с использованием Системы ДБО.

При этом доступ к Системе ДБО для получения Выписки об операциях по Счёту и копий исполненных расчетных документов в электронном виде сохраняется в течение 3 (трёх) календарных дней со дня, следующего за днем закрытия счёта.

14.5. В случае расторжения Договора ДБО, Клиент обязан передать в Банк СКЗИ, полученные в рамках Договора ДБО, и подписать Акт возврата СКЗИ.

14.6. Расторжение Договора ДБО или односторонний отказ от Договора ДБО не влечёт прекращения обязательств по иным договорам (соглашениям), заключённым между Клиентом и Банком, за исключением договоров, которые не предполагают предоставление услуг Банка без использования Системы ДБО.

14.7. Клиент и Банк согласны с тем, что Договор ДБО в части неразглашения Ключей ЭП, продолжает действовать в течение 1 (одного) календарного года после его расторжения.

14.8. В случае если на дату заключения Договора ДБО между Клиентом и Банком имеется ранее заключённый действующий договор, определяющий порядок предоставления услуг электронного документооборота с использованием Системы ДБО, указанный договор считается изменённым в соответствии с содержащимися в нём требованиями и изложенным в редакции настоящих Правил с момента принятия Банком от Клиента Заявления. При этом соглашения/дополнительные соглашения, заключённые до даты заключения Договора ДБО, считаются изменёнными и изложенными в редакции Договора ДБО и продолжают действовать до истечения срока их действия.

15. Обработка персональных данных

15.1. Клиент фактом заключения настоящего Договора ДБО подтверждает получение им письменных согласий на передачу и обработку персональных данных своих Уполномоченных лиц, чьи персональные данные содержатся в представленных Клиентом в Банк документах, в соответствии с требованиями Федерального закона № 152-ФЗ. Клиент несёт все неблагоприятные последствия, связанные с неполучением указанных согласий.

15.2. Клиент проинформирован и понимает, что Банк получает, имеет доступ и обрабатывает персональные данные его Уполномоченных лиц для целей заключения и исполнения Договора ДБО, а также для целей исполнения требований применимого к Банку законодательства Российской Федерации, в частности требований об идентификации лиц, представляющих Клиента в соответствии с Федеральным законом № 152-ФЗ.

15.3. Обработка персональных данных осуществляется Акционерным обществом «Акционерный Банк «РОССИЯ», зарегистрированным по адресу: 191124, г. Санкт-Петербург, пл. Растрелли, д. 2, стр. 1, с целью исполнения Договора ДБО с использованием средств автоматизации и без их использования путём совершения следующих действий - сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных, а также передачу такой информации третьим лицам, если это необходимо для достижения целей их обработки в случаях, установленных действующим законодательством Российской Федерации при условии обеспечения конфиденциальности и безопасности персональных данных при их обработке.

15.4. Подтверждение на получение Клиентом письменных согласий своих Уполномоченных лиц, указанное в п. 15.1 настоящих Правил, действует с даты заключения Договора ДБО и по истечении 5 (пяти) лет после прекращения действия Договора ДБО.

15.5. Согласие на обработку персональных данных может быть отозвано путём предоставления в Банк письменного заявления Уполномоченного лица Клиента. В случае

отзыва согласия Банк уничтожает персональные данные в срок, не превышающий 30 (тридцати) дней, за исключением случаев, когда дальнейшая обработка персональных данных является обязанностью Банка, установленной законодательством Российской Федерации.

15.6. Срок обработки определяется достижением указанных в п. 15.2 настоящих Правил целей обработки, что определяется следующим событием - прекращение Договора ДБО (прекращение обслуживания Клиента). По достижении цели обработки Банк осуществляет архивное хранение данных и документов в соответствии с требованиями действующего законодательства Российской Федерации.

15.7. Банк обязуется:

– соблюдать принципы и правила обработки персональных данных, предусмотренные Федеральным законом № 152-ФЗ;

– соблюдать конфиденциальность, обеспечивать безопасность персональных данных при их обработке и не раскрывать персональные данные третьим лицам без согласия субъекта персональных данных, за исключением случаев, установленных законодательством Российской Федерации;

– соблюдать требования к защите обрабатываемых персональных данных в соответствии с Федеральным законом № 152-ФЗ, в том числе применять необходимые правовые, организационные и технические меры для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных и от иных неправомерных действий в отношении персональных данных.

16. Прочие условия

16.1. По всем вопросам, неурегулированным в Договоре ДБО, Стороны руководствуются законодательством Российской Федерации.

16.2. Стороны соблюдают конфиденциальность информации, в том числе персональных данных, переданных одной Стороной другой Стороне.

16.3. Уведомления (заявления) в рамках Договора ДБО могут быть направлены одним из следующих способов:

16.3.1. Банком Клиенту:

– под расписку уполномоченному представителю Клиента;

– по Системе ДБО либо путём размещения информации в разделе «Вход в Интернет-Банк» (окно входа в Систему ДБО);

– на адрес электронной почты Клиента, указанный в Заявлении, или полученный в рамках исполнения Банком требований законодательства о противодействии легализации (отмыванию) доходов, полученных преступным путём, финансированию терроризма и финансированию распространения оружия массового уничтожения, исключая сведения, содержащие банковскую, коммерческую тайны и персональные данные;

– по почте заказным письмом;

– с использованием Сервиса «Личный кабинет ЮЛ»[31].

16.3.2. Клиентом Банку:

– по Системе ДБО;

– представителем Клиента/курьером при личной явке в Банк;

– по почте заказным письмом;

– с использованием Сервиса «Личный кабинет ЮЛ»[25].

16.3.2.1. По Системе ДБО заявления (документы) в соответствии с настоящим Договором ДБО могут быть переданы в Банк одним из следующих способов в зависимости от реализации в Системе ДБО:

[31] Функционал Сервиса «Личный кабинет ЮЛ» доступен с момента технической реализации.

- в формате ЭД Системы ДБО с использованием меню пользовательского интерфейса Системы ДБО либо настроив виджет «Услуги» главного экрана в Системе «ДБО BS-Client (CORREQTS)»;
- если в формате ЭД в Системе ДБО заявление не предусмотрено - в виде вложения заявления в формате Word или в виде сканированного образа заявления в ЭСИД «Письмо» на адрес «Отдел открытия счетов» или на адрес «Приостановление по 161-ФЗ» (в соответствии с требованиями подп. 8.1.11 – 8.1.12 настоящих Правил) с указанием в поле «Тема» сообщения наименования вложенного заявления, наименования Клиента и наименования Системы ДБО. Если ЭСИД «Письмо» подписано Представителем Клиента, действующим без доверенности, то заявление предоставляется в формате Word или в виде сканированного образа. Если ЭСИД «Письмо» подписано Представителем Клиента, действующим на основании доверенности, то заявление предоставляется в виде сканированного образа и ЭП в сообщении и подпись в сканированном образе заявления должны принадлежать одному лицу.

Заявление оформляется либо по установленной Банком типовой форме, либо в произвольной форме с указанием в тексте заявления наименования Клиента, ИНН, номера Договора ДБО и предоставляемых/ изменяемых сведений в случае, если типовой формой заявления не предусмотрены поля для предоставления / изменения сведений, требующих информирования Банка с целью исполнения Сторонами обязательств по Договору ДБО;

- в случае необходимости внесения изменений в иные ранее предоставленные данные, Клиент передаёт в Банк Заявление об изменении данных, заполнив те разделы, в которых произошли изменения;
- в случае изменения контактных данных (по работе с Системой ДБО, по техническим вопросам) и номера телефона для обеспечения круглосуточной связи, указанных в Заявлении - в формате «Письмо» либо текстовым файлом, либо сообщением с указанием новых сведений.

16.4. Все приложения, на которые даны ссылки в тексте настоящих Правил, являются его неотъемлемыми частями.

17. Приложения

Приложение № 1 «Условия предоставления сервиса подключения Канала «Интеграционный Клиент-Банк»;

Приложение № 2 «Обязательства клиента по выполнению правил безопасной работы при использовании клиентской части Системы ДБО;

Приложение № 3 «Условия предоставления модуля «Центр финансового контроля / Расчетный центр корпорации» в АО «АБ «РОССИЯ»;

Приложение № 4 «Типовая форма Заявления о предоставлении модуля ЦФК/РЦК Системы ДБО Контролирующей организации»;

Приложение № 5 «Перечень Сервисов Системы ДБО»;

Приложение № 6а «Инструкция по установке Системы «iBank»;

Приложение № 6б «Инструкция по установке Системы «ДБО BS-Client (CORREQTS)» и Мобильного приложения Банка»;

Приложение № 7 «Перечень электронных документов, используемых в Системе ДБО;

Приложение № 8 «Типовая форма Акта возврата средств криптографической защиты информации»;

Приложение № 9 «Типовая форма Акта приема – передачи ключевых носителей, программного обеспечения и средств криптографической защиты информации (для Клиентов)»;

Приложение № 10 «Типовая форма Доверенности (на получателя)»;

Приложение № 11 «Типовая форма Заявления о компрометации»;

Приложение № 12 «Типовая форма Заявление об установлении/ снятии ограничений на работу в Системе ДБО»;

Приложение № 13 «Положение о порядке проведения технической экспертизы при возникновении спорных ситуаций»;

Приложение № 1

УСЛОВИЯ
предоставления сервиса подключения Канала «Интеграционный Клиент-Банк»

1. Банк предоставляет Клиенту Сервис подключения Канала «Интеграционный Клиент-Банк».

2. В рамках Канала «Интеграционный Клиент-Банк» доступна интеграция Системы Клиента с Системой ДБО посредством:

– интеграции с системой 1С (Сервис «Обмен с 1С по DirectBank»/ DirectBank+») - позволяет отправлять документы в Банк и получать документы из Банка непосредственно из программ системы «1С:Предприятие», нажатием одной кнопки в программе «1С». Реализованы две технологии интеграции с системой 1С: прямой обмен по технологии DirectBank и внешняя обработка - модуль «iBank для 1С»;

– интеграции с модулем «Корпоративный автоклиент» - для работы в «iBank» - позволяет автоматизировать процесс подписания и отправки документов в Банк, получения из Банка Выписок по счетам;

– интеграции с модулем «Интеграционный корпоративный шлюз»[1] - для работы в «ДБО BS-Client «CORREQTS» - представляет собой сервис, функционирующий на стороне Банка, и обеспечивающий возможность взаимодействия с Системой ДБО непосредственно из внешней Системы Клиента;

– интеграции через API (далее – API Интеграция[2]) - представляет собой сервис, обеспечивающий возможность взаимодействия с Системой ДБО непосредственно из внешней Системы Клиента.

3. Клиенту доступна возможность подключения «Канала «Интеграционный Клиент-Банк» посредством направления заявления на подключение в электронном виде по Системе ДБО для подключения следующих модулей/сервисов:

через «Электронный офис»	**через «Управление услугами»**
Сервисы интеграции с системой 1С	
• услуга Обмен с 1С по Directbank	• услуга DirectBank+
модуль «Корпоративный автоклиент»	
-	• Корпоративный автоклиент
модуль «Интеграционный корпоративный шлюз»	
• Интеграционный Корпоративный Шлюз	-
	через меню разделов интерфейса iBank
API Интеграция	
-	• API Интеграция

Отказ от использования модулей/сервисов Канала «Интеграционный Клиент-Банк» осуществляется на основании заявления Клиента, предоставленного либо в формате Системы ДБО, либо в произвольной форме с указанием в тексте заявления наименования Клиента, ИНН, номера Договора ДБО на бумажном носителе, или с использованием Системы ДБО в виде сканированного образа заявления в адрес «Отдел открытия счетов» операционного подразделения, осуществляющего обслуживание Клиента.

4. Необходимым условием для предоставления Банком Канала «Интеграционный Клиент-Банк» является:

– наличие у Клиента подключённого Канала «Клиент-Банк Онлайн»;

– наличие открытого в Банке Счета;

[1] Подключение модуля «Интеграционный Корпоративный Шлюз» Клиентам – владельцам учетной записи в модуле «Интеграционный Корпоративный Шлюз» не осуществляется.

[2] Доступно с момента технической реализации

– подача в модуле «Электронный офис» / «Управление услугами» заявления на подключение сервиса.

5. Банк осуществляет предоставление Канала «Интеграционный Клиент-Банк» в соответствии с пользовательской документацией, размещенной на сайте Банка по адресу: www.abr.ru в разделе «Интеграционный Клиент-Банк», действующей на момент оказания услуги. Подавая электронное заявление на услугу через Систему ДБО Клиент подтверждает, что он ознакомился с пользовательской документацией и обязуется соблюдать ее требования.

6. Для работы с использованием Канала «Интеграционный Клиент-Банк» Клиент самостоятельно производит настройки Системы Клиента и выполняет необходимые доработки своей Системы в зависимости от выбранного способа интеграции с Банком.

7. Клиенту рекомендуется обеспечить комплекс организационно-технических мер, направленных на выполнение следующих требований безопасности:

7.1. Обеспечить использование исключительно лицензионного программного обеспечения и операционной системы;

7.2. Организовать регулярную установку обновлений безопасности программного обеспечения и операционной системы;

7.3. Исключить использование средств удаленного администрирования;

7.4. Обеспечить применение лицензионного межсетевого экрана (допускается использование персонального межсетевого экрана);

7.5. Выполнить комплекс организационных мероприятий по обеспечению информационной безопасности (настройка безопасности операционной системы, ограничение прав доступа информационной системы, организация парольной защиты, подготовка процедур реагирования на инциденты и т.п.);

7.6. Контролировать соблюдение требований безопасности, установленных Приложением № 2 к настоящим Правилам, которые распространяются на стороне Клиента на все рабочие места Клиента, участвующие в обмене ЭД с Банком с использованием Канала «Интеграционный Клиент-Банк».

8. Обмен ЭД посредством Канала «Интеграционный Клиент-Банк» организуется по защищенному соединению на базе функционала сервисов интеграции Канала «Интеграционный Клиент-Банк» в поддерживаемых Банком форматах электронных документов в зависимости от выбранного варианта интеграции.

9. Безопасность обмена ЭД достигается за счет применения сертифицированных СКЗИ, протокола безопасности, обеспечивающего защищенный обмен данными при передаче по каналам связи, а также криптографических алгоритмов шифрования в соответствии с требованиями ГОСТ.

10. Стороны признают используемые ими при работе через Канал «Интеграционный Клиент-Банк» системы телекоммуникаций, обработки и хранения информации достаточными для обеспечения надежной и эффективной работы при приеме, передаче, обработке и хранении информации, а систему защиты информации, обеспечивающую разграничение доступа, формирование и проверку подлинности ЭП достаточной для защиты от несанкционированного доступа, подтверждения авторства и подлинности информации, содержащейся в получаемых ЭД и разбора конфликтных ситуаций.

11. При использовании Канала «Интеграционный Клиент-Банк» Банк не несёт ответственность за задержку и сбои при обмене документами с Системой Клиента, возникающие в сервисах интернет-провайдеров или Системе Клиента, за убытки Клиента, которые могут возникнуть в силу приостановления предоставления сервиса интеграции по причине неработоспособности Системы Клиента.

12. Особенности работы посредством интеграции с системой 1С:

12.1. Использование определённого типа ЭП Уполномоченным лицом Клиента:

в ДБО «BS-Client «CORREQTS»	в «iBank»

Необходим УКЭП, выпущенный УЦ	Необходим УНЭП, выданный Банком или Серверная ЭП

12.2. Отличия по функциональности, доступной в рамках услуги в Системах ДБО:

Система «ДБО BS-Client «CORREQTS»	**Система «iBank»**
Доступна стандартная функциональность услуги «Обмен с 1С по Directbank», позволяющая осуществлять: • отправку в Банк платежных документов • получение Выписки по счету • подписание документов • работу с платежными требованиями • отзыв документов • синхронизацию статусов по отправленным документам • отображение документов, созданных в 1С, в интерфейсе Системы ДБО	Доступна расширенная функциональность услуги «DirectBank+» с использованием модуля «iBank для 1С» («Стандартный» или «Премиум»), которая дополнительно позволяет использовать: • механизм дополнительного подтверждения платежных поручений (средства подтверждения: Устройство подтверждения, Код подтверждения в SMS); • справочник «Доверенные получатели» в платежных документах

12.3. Настройка Клиентом прямого обмена с 1С по технологии DirectBank или с использованием расширенной функциональности в СДБО iBank осуществляется в соответствии с пользовательской документацией, размещенной на сайте Банка по адресу: www.abr.ru в разделе «Интеграционный Клиент-Банк» и на странице входа в Систему ДБО, которая доступна через раздел «Вход в Интернет-Банк».

13. Особенности интеграции с Системой Клиента, отличной от платформы «1С».

В зависимости от используемой Клиентом Системы ДБО интеграция может осуществляться следующими способами:

13.1. С использованием модуля «Корпоративный автоклиент» Системы iBank – позволяет Клиенту автоматизировать процесс подписания и отправки ЭД в Банк и получения из Банка Выписок по счетам, а также обеспечить интеграцию Системы Клиента с банковским сервером Системы «iBank». Настройка работы модуля осуществляется в соответствии с пользовательской документацией, размещённой на сайте Банка в разделе «Интеграционный Клиент-Банк» по адресу: www.abr.ru и на странице входа в Систему ДБО, которая доступна через раздел «Вход в Интернет-Банк».

13.2. С использованием модуля «Интеграционный корпоративный шлюз» Системы «ДБО BS-Client (CORREQTS)».

13.2.1. Подключение новой учетной записи в модуле «Интеграционный Корпоративный Шлюз» Клиенту – головной организации не осуществляется. Подключение к действующей учетной записи в модуле «Интеграционный корпоративный шлюз» новых счетов Клиента – владельца счета Банк осуществляет на основании заявления на подключение в электронном виде в Системе ДБО в соответствии с п. 3 настоящего Приложения №1.

13.2.1. О факте подключения модуля «Интеграционный корпоративный шлюз» Банк уведомляет Клиента по Системе ДБО, что является основанием для взимания комиссионного вознаграждения в соответствии с Тарифами Банка.

13.3. С использованием API Интеграция.

13.3.1. При работе с использованием API Интеграция допускается использование Уполномоченным лицом Клиента УНЭП, включая Серверную ЭП.

13.3.2. API Интеграция подключается поэтапно: на первом этапе запрашивается тестовая среда для каждого участника взаимодействия, на втором этапе по факту готовности – доступ к промышленной среде, присоединение дополнительных участников интеграции происходит единовременно с предоставлением доступа к промышленной среде (подав заявление на подключение, включающего предоставление доступа к тестовой среде и подтверждение готовности к работе по API).

13.3.3. При подключении взаимодействия посредством API Интеграция Клиенту необходимо выполнить следующие условия:

– подать заявление в электронном виде о подключении API Интеграция с отметкой о предоставлении доступа к тестовой среде для настройки API Интеграции;

– самостоятельно осуществить доработку Системы Клиента в соответствии с требованиями Банка к форматам передаваемых документов, поддерживаемых в рамках API Интеграции в соответствии с пользовательской документацией, предоставляемой Банком / размещенной на сайте Банка в разделе «Интеграционный Клиент-Банк» по адресу: https://abr.ru/corp/remote-services/integration-client-bank/#user_docs;

– подтвердить готовность к проведению тестирования предложенных форматов обмена данными путём направления по электронной почте ответного сообщения на сообщение Банка, содержащее форматы обмена данными;

– при настройке взаимодействия посредством API Интеграция необходимо самостоятельно создать в Системе «iBank» API-токены для Уполномоченных лиц, которые будут работать через API Интеграция, и использовать их при формировании запросов к API из Системы Клиента с соблюдением требований Приложения №2 к Правилам;

– провести тестирование в части взаимодействия Системы Клиента и Системы ДБО на стороне Банка с участием представителя Банка с учётом согласованных Сторонами форматов передаваемых документов;

– по факту успешного завершения тестирования API Интеграция подать в Банк заявление в электронном виде с отметкой о подтверждении настройки интеграции и готовности к работе по API.

13.3.4. О факте завершения настройки API Интеграции Банк уведомляет Клиента по Системе ДБО. При подключении взаимодействия посредством API Интеграция основанием для взимания единовременного комиссионного вознаграждения за подключение является факт подачи по Системе ДБО заявления на подключение API Интеграция, содержащего запрос о предоставлении доступа к тестовой среде для настройки API Интеграции, основанием для взимания ежемесячного комиссионного вознаграждения за обслуживание является факт подачи по Системе ДБО заявления на подключение API Интеграция, содержащего подтверждение готовности к работе по API Интеграция, и направление уведомления.

Приложение № 2

Обязательства клиента
по выполнению правил безопасной работы при использовании клиентской части Системы ДБО

В соответствии с Договором ДБО Клиент подтверждает, что для обеспечения безопасной работы в Системы ДБО обязуется:

– обеспечить защиту от несанкционированного доступа к Клиентскому рабочему месту (АРМ Клиента), защиту от несанкционированного доступа и сохранность Ключей ЭП, Логинов и Паролей для входа в Систему ДБО, защиту от несанкционированного доступа к Мобильному устройству с активированным Мобильным приложением PayControl и Мобильным приложением Банка, а также защиту от несанкционированного доступа к другой конфиденциальной информации;

– в случае использования канала «Интеграционный Клиент-Банк» обеспечить защиту от несанкционированного доступа в Систему ДБО через рабочие места Клиента, которые участвуют в обмене ЭД с Банком, а также выполнение иных требований, установленных настоящим Приложением, на стороне Клиента;

– незамедлительно информировать Банк любым доступным способом обо всех случаях невозможности расшифровки ЭД, отрицательного результата проверки подлинности ЭП, нештатной работы Системы ДБО, неполучения информационных сообщений Банка;

– соблюдать следующие организационные меры:

☑ **Требования к сохранности Пароля/ Пароля к Ключу Серверной ЭП:**

– Пароль выбирается самостоятельно;

– если Пароль записан на бумаге, то хранится в месте, недоступном для неуполномоченных лиц, рекомендуется использовать надёжные металлические хранилища, оборудованные внутренними замками;

– запрещено записывать Пароль на съёмный носитель, монитор, клавиатуру и пр.;

– Пароль должен содержать не менее 8 различных символов (буквы, цифры, большой / малый регистр, спецсимволы);

– в качестве Пароля не должны быть использованы: ИНН и другие реквизиты Клиента, имена и фамилии, последовательности, состоящие из повторяющихся или одних цифр (в том числе номера телефонов, памятные даты, номера автомобилей и прочее, что можно связать с Клиентом);

– при Компрометации / подозрении на Компрометацию Пароля следует незамедлительно уведомить об этом Банк в соответствии с разделом Порядок действий при Компрометации / подозрении на Компрометацию настоящего Приложения;

– рекомендуемая периодичность смены пароля – не реже 1 (одного) раза в 3 (три) месяца.

☑ **Правила хранения и использования Ключевых носителей:**

– для хранения USB-Токенов необходимо использовать надёжные металлические хранилища, оборудованные внутренними замками, для исключения возможности несанкционированного доступа к ним неуполномоченных лиц;

– запрещается извлекать из хранилища носители с Ключами ЭП, если они не используются для работы с Системой ДБО;

– никогда не передавать Ключи ЭП третьим лицам для проверки работы Системы ДБО, проверки настроек взаимодействия с Банком и т.п. При необходимости таких проверок Уполномоченное лицо Клиента должно лично подключить носитель к рабочей станции,

убедиться, что пароль доступа к ключу вводится в интерфейс Системы ДБО, и лично ввести Пароль, исключая возможность его Компрометации;

– запрещается передавать Ключевые носители третьим лицам, оставлять без присмотра, а также (предпринимать попытки по проведению записи) записывать на USB-Токен постороннюю информацию;

– запрещается снятие несанкционированных копий с Ключевого носителя;

– при Компрометации / подозрении на Компрометацию среды исполнения (наличие в компьютере вредоносных программ), а также атрибутов доступа к Мобильному устройству (Логин, Пароль, графический ключ, PIN-код и т.д.) следует незамедлительно уведомить об этом Банк в соответствии с разделом Порядок действий при Компрометации / подозрении на Компрометацию настоящего Приложения;

– по требованию работника технической поддержки Системы ДБО в случае подозрения на Компрометацию выполнить антивирусную проверку АРМ Клиента;

– оказывать содействие Банку в установлении фактов несанкционированного доступа к Системе ДБО и Компрометации. Обеспечивать доступ работников Банка к техническим средствам, на которых установлена клиентская часть Системы ДБО для проведения работ по её установке и сопровождению;

☑ **Требования к выпуску и хранению API-токена при взаимодействии посредством API Интеграция в рамках канала «Интеграционный Клиент-Бак»:**

– выпустить API-токен в Системе iBank для Уполномоченных лиц, от имени которых будут формироваться запросы к API Интеграция;

– установить срок действия API-токена при его создании (по умолчанию 365 дней));

– срок действия API-токена может быть ограничен Банком исходя из срока действия полномочий Уполномоченного лица;

– в случае утери значения API-токена или изменения IP-адреса (если в процессе создания API-токена указывались IP-адреса) на стороне Клиента необходимо создание нового API-токена;

– запрещается передавать API-токен третьим лицам.

☑ **Соблюдение требований по обеспечению безопасности Ключевой информации:**

– все отчуждаемые (внешние) Ключевые носители должны учитываться поэкземплярно в специальных журналах согласно установленной нормативными актами Российской Федерации форме;

– учёт и хранение носителей СКЗИ, учёт Ключевых носителей должны быть поручены специально назначенным работником. Каждый владелец ЭП несёт персональную ответственность за его использование и сохранность;

– поэкземплярный учёт сформированных Уполномоченными лицами Клиента криптографических ключей осуществляется Клиентом;

– хранение Ключевых носителей допускается в одном хранилище с другими документами при условии, исключающем их непреднамеренное разрушение или уничтожение;

– Уполномоченными лицами или по поручению руководителя организации одним из работников из числа допущенных к эксплуатации СКЗИ, должен проводиться периодический контроль сохранности входящего в состав СКЗИ оборудования, а также всего используемого программного обеспечения для предотвращения внесения программно-аппаратных закладок и вредоносного программного обеспечения.

☑ **Правила хранения и использования Устройств подтверждения:**

– для хранения Устройств подтверждения необходимо использовать надёжные металлические хранилища, оборудованные внутренними замками, для исключения возможности несанкционированного доступа к нему неуполномоченных лиц и повреждение материального носителя;

– не извлекать из хранилища Устройство подтверждения, если оно не используются для работы с Системой ДБО;

– не раскрывать третьим лицам информацию об Устройстве подтверждения, находящемся в его распоряжении;

– не передавать его в пользование лицам, не являющимся Уполномоченными лицами Клиента, для распоряжения денежными средствами, находящихся на Счёте, или в иных целях, оставлять Ключевые носители без присмотра;

– в случае утраты или поломки Устройства подтверждения необходимо уведомить об этом Банк в соответствии с разделом Порядок действий при Компрометации / подозрении на Компрометацию настоящего Приложения.

☑ **Ограничение доступа и требования к рабочим местам, с которых осуществляется работа с Системой ДБО:**

– право доступа предоставляется только уполномоченным лицам, непосредственно осуществляющим работу с Системой ДБО. Исключить доступ к компьютерам неуполномоченных лиц, не имеющих отношения к работе с Системой ДБО;

– запрещается установка программных средств, не предназначенных для выполнения служебных обязанностей Уполномоченных лиц Клиента, допущенных к работе с Системой ДБО;

– применять на рабочем месте лицензионные ПО (операционные системы, офисные пакеты и пр.), лицензионные средства антивирусной защиты, обеспечить возможность регулярного автоматического обновления антивирусных баз;

– работа с Системой ДБО немедленно прекращается при подозрении, что компьютер заражен, а также в случае обнаружения незарегистрированных программ или нарушения целостности операционной системы – обязательно уведомить об этом Банк в соответствии с разделом Порядок действий при Компрометации / подозрении на Компрометацию настоящего Приложения;

– для работы в Системе ДБО крайне не рекомендуется выбирать переносной компьютер (ноутбук). Если Клиентом выбран ноутбук, запрещается подключать ноутбук к сетям общего доступа в местах свободного доступа в Интернет (Интернет-кафе, гостиницы, офисные центры и т.д.);

– в случае передачи (списание, выброс, ремонт) сторонним лицам компьютера (ноутбука), на котором ранее была установлена Система ДБО, необходимо гарантированно удалить с него всю информацию, использование которой третьими лицами может потенциально нанести вред финансовой деятельности или имиджу Клиента, в том числе следы работы в Системе ДБО;

– использовать дополнительное программное обеспечение, позволяющее повысить уровень защиты компьютера – персональные межсетевые экраны, программы поиска шпионских компонент, программы защиты от «спам»–рассылок и пр.;

– включить автоматическую блокировку экрана после ухода уполномоченного лица с рабочего места.

☑ **Соблюдение правил безопасной работы в сети интернет на рабочих местах Системы ДБО:**

– не открывать сайт Системы ДБО по ссылкам (особенно баннерным или полученным через электронную почту);

– не отвечать на подозрительные письма с просьбой выслать авторизационные и другие конфиденциальные данные;

– на компьютерах, используемых для работы с Системой ДБО, исключить посещение интернет-сайтов сомнительного содержания, загрузку и установку нелицензионного ПО и т.п.;

– не устанавливать и не сохранять подозрительные файлы, полученные из ненадежных источников, скачанные с неизвестных web-сайтов, присланные по электронной почте, полученные в телеконференциях;

– на компьютере запрещено запускать программы, полученные из ненадежных источников;

– если Клиент эксплуатирует выделенный высокоскоростной канал доступа в сеть интернет, ограничить диапазон IP-адресов, с которых разрешён доступ к Системе ДБО с использованием Ключей ЭП, зарегистрированных Банком по Заявлению, переданному Клиентом в Банк;

–обращать внимание на любые изменения в привычных процессах установления соединения с Системой ДБО или в функционировании Системы ДБО. При возникновении любых сомнений в правильности функционирования Системы ДБО незамедлительно обратиться в Банк по телефону службы технической поддержки, указанному на официальном сайте Банка в сети Интернет www.abr.ru;

–в случае появления предупреждений Браузера о перенаправлении Клиента на другой сайт при подключении к Системе ДБО Банка, отложите совершение операций и обратитесь в службу поддержки Банка по телефону службы технической поддержки, указанному на официальном сайте Банка в сети Интернет www.abr.ru.

☑ **Требования к сотрудникам Клиента:**

– Клиент обязан назначить Приказом уполномоченных лиц по работе с Системой ДБО, утвердить соответствующие должностные инструкции, исключить доступ к компьютерам неуполномоченных лиц, не имеющих отношения к работе с Системой ДБО;

– при регистрации в Системе ДБО в соответствии с разделом 5 настоящих Правил, руководствоваться Инструкцией по установке Системы ДБО;

– каждое уполномоченное лицо, имеющее доступ к Ключевым носителям, паролям и другой конфиденциальной информации, должно быть проинформировано об ответственности за разглашение конфиденциальной информации;

– при обслуживании компьютера Уполномоченного лица Клиента, на котором используется Система ДБО, третьими лицами – обеспечивать контроль над выполняемыми ими действиями;

– при увольнении Уполномоченного лица, имевшего доступ к Ключу ЭП, обязательно проинформировать об этом Банк в целях блокировки Банком Ключа ЭП/ Ключа PayControl;

– при увольнении Уполномоченного лица Клиента, имевшего технический доступ к секретному Ключу ЭП/ Ключу PayControl, обязательно проинформировать об этом Банк в целях блокировки Банком Ключа ЭП/ Ключа PayControl;

– при увольнении Уполномоченного лица, осуществлявшего обслуживание рабочей станции, используемой для работы с Системой ДБО, принять меры для обеспечения отсутствия вредоносных программ на компьютерах;

– при наличии Счёта в Банке:

- контролировать актуальность Номеров телефонов для направления Кодов подтверждения/SMS-сообщений/PUSH-сообщений, а в случае их изменения – незамедлительно информировать о таком изменении Банк по форме Заявления об изменении данных;

- информировать Уполномоченных лиц о недопущении ситуаций переполнения памяти Мобильных устройств, что может являться препятствием для приёма SMS-сообщений Банка с Кодами подтверждения/ PUSH-сообщений, а также о необходимости исключить передачу мобильного телефона, который используется для получения SMS-сообщений Банка, третьим лицам;
- в случае утраты телефона, на который приходят Коды подтверждения /SMS-сообщения/PUSH-сообщения, обеспечить немедленную блокировку номера телефона у оператора сотовой связи;
- информировать Банк о смене телефонного номера и SIM-карты Мобильного устройства, используемого для получения SMS-сообщений с Кодами подтверждения/ PUSH-сообщений от Банка;
- при поступлении на телефон Уполномоченного лица SMS-сообщений/ PUSH-сообщений, свидетельствующих о попытке входа в Систему ДБО или подтверждения отправки документов, которых данное лицо не совершало, немедленно уведомить об этом Банк в соответствии с разделом Порядок действий при Компрометации / подозрении на Компрометацию настоящего Приложения.

☑ **Требования по обеспечению безопасности использования Клиентом Мобильного устройства с Мобильным приложением PayControl, Мобильным приложением Банка.**

– мобильное устройство, предназначенное для использования Клиентом с Мобильным приложением PayControl, Мобильным приложением Банка, должно быть приобретено у официального продавца и быть сертифицировано по требованиям ГОСТ в соответствии с действующим законодательством для использования на территории Российской Федерации;

– мобильное устройство Клиента имеет поддерживаемую Мобильным приложением PayControl и Мобильным приложением Банка лицензионную версию операционной системы:

a) Android 5.0 и выше;

b) iOS 10.X и выше.

–не использовать Мобильное приложение PayControl и Мобильное приложение Банка на Мобильных устройствах с расширенными правами (Jailbreak, Root или иные операции, не поддерживаемые официально производителями);

– для операционной системы Мобильного устройства и приложений, установленных на Мобильное устройство, Клиентом установлены максимально возможные на текущее время обновления, рекомендованные производителем/разработчиком;

– мобильное приложение PayControl самостоятельно установлено Клиентом из одного из авторизованных магазинов приложений (AppStore или PlayМаркет для iOS/Android соответственно). Клиент не использовал переход к указанным сервисам и не совершал установку Мобильного приложения PayControl по ссылке из других источников;

– если при установке Мобильного приложения PayControl появились сообщения о необходимости удаления приложения/приложений, представляющих угрозу для Мобильного приложения PayControl, необходимо удалить представляющие угрозу приложение/приложения с Мобильного устройства.

1. для разблокировки Мобильного устройства использовать максимально возможный из доступных на данном Мобильном устройстве способ защиты от несанкционированного доступа к функциям устройства и хранящихся на нём данным (в порядке убывания стойкости защиты):

a) средство распознания радужной оболочки глаза;

b) средство распознавания отпечатка пальца или лица (TouchID, FaceID);

c) пароль длиною не менее 6 символов (включая буквы и цифры);

d) графический ключ;

e) PIN-код.

При использовании пароля или PIN-кода Клиент запомнил их и не сохранил в памяти Мобильного устройства.

– мобильное устройство настроить на автоматическую блокировку устройства по истечении определённого времени (не более 5 (пяти) минут);

– на Мобильном устройстве под управлением ОС Android используется средство защиты от вредоносного кода («антивирусное программное обеспечение»);

– на Мобильном устройстве под управлением ОС Android отключить возможность установки приложений из непроверенных источников;

– мобильное устройство с Ключами инициализации PayControl (направляются/передаются Банком каждому УЛ Клиента: QR-код + код в SMS-сообщении) и самостоятельно выработанными УЛ Клиента Ключами ЭП на основе средства PayControl, а также атрибуты доступа к Мобильному устройству (Логин, Пароль, графический ключ, PIN-код) никогда не передаётся Клиентом неуполномоченным лицам, включая руководство организации, коллег и членов семьи Уполномоченного лица Клиента и не оставляется им без присмотра;

– мобильное устройство, с установленным Мобильным приложением PayControl, использовать только для посещения сайтов и установки приложений, необходимых и достаточных Клиенту для ведения его коммерческой/уставной деятельности;

2. мобильное устройство не подключать к компьютерам, безопасность которых Клиент не может гарантировать, а именно:

a) обеспечение доверенной среды;

b) отсутствие удалённого управления;

c) отсутствие установленных/запущенных вредоносных программ.

3. мобильное устройство не подключать к общественным WI-FI сетям. Общественные WI-FI сети, как правило, плохо защищены, их настройки неизвестны;

4. никогда и никому не сообщать Пароль для Аутентификации при входе в Мобильное приложение PayControl и Мобильное приложение Банка;

–обеспечить использование Ключей PayControl в Системе ДБО только УЛ Клиента (с установленными правами подписи);

–в случае возникновения вопросов по работе в Системе ДБО с Мобильным приложением PayControl и Мобильным приложением Банка обратиться в службу поддержки Банка по телефону службы технической поддержки, указанному на официальном сайте Банка в сети Интернет www.abr.ru.

☑ **Дополнительные рекомендации для владельцев смартфонов:**

– установить на вашем Мобильном устройстве и регулярно обновлять мобильный антивирус (рекомендуется использовать антивирус российского производителя, так как он учитывает региональную специфику вредоносного ПО);

– своевременно устанавливать обновления для вашего Мобильного устройства и установленных на нём приложений. Установку производить только из авторизованных магазинов приложений (AppStore или PlayМаркет для iOS/Android соответственно, маркетов производителей устройств и т.п.). Иные способы установки приложений и обновлений небезопасны. Недопустима установка или обновление приложений по ссылке в e-mail / SMS-сообщении от имени Банка. Обратите внимание: Банк никогда не высылает писем и SMS-сообщений с прямыми ссылками на установку или обновление приложений;

– при установке на ваше Мобильное устройство дополнительного программного обеспечения обращайте внимание на полномочия, которые необходимы программе. Не допускать установки программ, которым требуются излишние полномочия, особенно в части чтения и отправки SMS-сообщений, доступа к сети Интернет, клавиатуре и т.п. При наличии

технической возможности рекомендуется включить на Мобильном устройстве режим установки только подписанных приложений с проверкой сертификата;

– если Вы заметили, что на ваше Мобильное устройство перестали приходить SMS-сообщения, в том числе перестали приходить Коды подтверждения/ PUSH-сообщения от Банка, необходимо прекратить использование Мобильного устройства. В данном случае возможно мошенничество с заражением вашего Мобильного устройства вирусом, перехватывающим SMS-сообщения. Для проверки рекомендуем установить SIM-карту в другое мобильное устройство, провести операцию в Системе ДБО и дождаться прихода Кода подтверждения/ PUSH-сообщения. Так же о заражении вирусом может свидетельствовать подозрительная работа устройства (самопроизвольные звонки и рассылки SMS-сообщений, несанкционированная загрузка и установка программного обеспечения). В случае выявления данных фактов рекомендуем обратиться за помощью в службу технической поддержки производителя Вашего мобильного устройства.

☑ **Порядок действий при Компрометации / подозрении на Компрометацию**

– Клиенту в целях информирования Банка о наступлении события Компрометации или подозрения о Компрометации в день выявления факта Компрометации/ подозрения о Компрометации необходимо оповестить об этом Банк по телефону службы технической поддержки Системы ДБО, указанному на официальном сайте Банка в сети Интернет www.abr.ru в разделе «Вход в Интернет-Банк» (окно входа в Систему ДБО).

Устное обращение по телефону службы технической поддержки Системы ДБО о временной блокировке скомпрометированного Ключа ЭП (УНЭП, УКЭП) / приостановлении использования Системы ДБО должно быть подтверждено письменным Заявлением о компрометации (Приложение № 11 к Правилам), форма которого размещена на официальном сайте Банка (www.abr.ru). Подать Заявление о компрометации в Банк можно способами, определёнными подп. 16.3.2 Правил, либо на бумажном носителе, подписанным Представителем Клиента и заверенным печатью (при наличии) по месту нахождения отделения Банка, либо по Системе ДБО (при наличии у Клиента нескомпрометированных Ключей ЭП) в формате ЭСИД «Письмо».

– При информировании Банка по телефону службы технической поддержки Системы ДБО:

- Представитель Клиента (заявитель) сообщает наименование Клиента (владельца Счёта), свои ФИО и должность, а также ФИО и должность Уполномоченного лица Клиента, в отношении которого выявлены события Компрометации или подозрения на Компрометацию;
- Банк по факту обращения представителя Клиента (заявителя) незамедлительно:

– обеспечивает временную блокировку скомпрометированного Ключа ЭП (УНЭП, УКЭП) УЛ Клиента в Системе ДБО. Временная блокировка Ключа PayControl/ Устройства подтверждения УЛ Клиента не осуществляется. Удаление Ключа PayControl/ Устройства подтверждения УЛ Клиента в Системе ДБО при обращении по телефону осуществляется после получения подтверждения по телефону подтверждения экстренной блокировки Ключей ЭП;

– обеспечивает совершение телефонного звонка Клиенту на номер телефона подтверждения экстренной блокировки Ключей ЭП. Информация о номере телефона подтверждения экстренной блокировки Ключей ЭП указывается Клиентом в Заявлении в целях получения подтверждения факта Компрометации/ подозрения на Компрометацию.

- Банк в случае, если по факту телефонного звонка Клиенту подтверждение необходимости блокировки Ключа ЭП/ удаления Ключа PayControl/ Устройства подтверждения УЛ не получено:

– снимает временную блокировку Ключа ЭП (УНЭП, УКЭП), установленную по факту входящего телефонного звонка заявителя, не удаляет Ключ PayControl/ Устройство

подтверждения. Иные действия в Системе ДБО в случае необходимости Банк совершает на основании предоставленного Клиентом Заявления о компрометации.

В случае не предоставления Клиентом в Банк номера телефона подтверждения экстренной блокировки Ключей ЭП, блокировка скомпрометированного Ключа ЭП, удаление Ключа PayControl/ Устройства подтверждения УЛ Клиента на основании входящего телефонного звонка Клиента не осуществляется.

– По факту получения от Клиента информации о Компрометации или в случае выявления Банком факта Компрометации/ любых подозрений на Компрометацию (при наличии у Банка информации о событиях, относящихся к Компрометации), Банк незамедлительно блокирует скомпрометированный Ключ ЭП, удаляет Ключ PayControl/ Устройство подтверждения УЛ Клиента в Системе ДБО, прекращает приём и исполнение ЭД, подписанных скомпрометированным Ключом ЭП/ Ключом PayControl.

– В целях получения нового Пароля, Ключевого носителя (USB-Токен), Устройства подтверждения Клиент либо запрашивает их в Заявлении о компрометации в момент уведомления Банка о наступлении случая Компрометации, либо подаёт в Банк Заявление об изменении данных в порядке, определённом подп. 16.3.2 Правил.

– Генерацию новых Ключей ЭП/ Ключей PayControl Клиент осуществляет в соответствии с разделом 6 Правил.

Не вносить исправления, изменения или дополнения в специализированное программное обеспечение и техническую документацию, предоставленные Банком по Договору ДБО, не передавать их третьим лицам, а также не передавать третьим лицам Ключевые носители, Устройства подтверждения, сведения по форматам ЭД и технологии их обработки Клиентом и Банком, а также прочие сведения, относящиеся к Договору ДБО.

Приложение № 3

УСЛОВИЯ
предоставления модуля «Центр финансового контроля / Расчётный центр корпорации»[3] в АО «АБ «РОССИЯ»

1. Используемые термины и определения

1.1. **Акцепт** – режим работы модуля «Центр финансового контроля/Расчётный центр Корпорации» (далее – модуль ЦФК/РЦК) Системы ДБО, позволяющий Контролирующей организации осуществлять финансовый контроль деятельности посредством:

– авторизированного согласия (акцепта) Уполномоченного лица Контролирующей организации на исполнение Банком ЭПД на проведение расходных операций по Контролируемым счетам;

– контроля бюджета/лимита по своим Счетам / Счетам Подконтрольных организаций.

В рамках режима работы «Акцепт» могут быть настроены опции:

- Сплошной акцепт - установка акцепта Контролирующей организации всех ЭПД Подконтрольных организаций, настройка осуществляется Банком;
- Выборочный акцепт - настройка автоматизированных правил контроля ЭПД Подконтрольных организаций (специальных критериев контроля / совокупности критериев контроля обязательных для проверки), устанавливаемых Уполномоченными лицами Контролирующей организации и дополнительный акцепт ЭПД по Контролируемым счетам, удовлетворяющих автоматизированным правилам контроля. Настройка осуществляется Контролирующей организацией в соответствии с эксплуатационной документацией, размещённой на Сайте Банка на странице входа в Систему ДБО, которая доступна через раздел «Вход в Интернет-Банк» (окно входа в Систему ДБО);
- Корпоративное бюджетирование – установление бюджета Подконтрольным организациям, автоматизация контроля бюджета/лимита Подконтрольными организациями.
- Многоуровневый акцепт - позволяет установить несколько уровней акцепта или акцепт несколькими Контролирующими организациями всех ЭПД Подконтрольной организаций.

1.2. **Контролирующая организация –** Клиент или стороннее юридическое лицо, иностранная структура без образования юридического лица, индивидуальный предприниматель или физическое лицо, занимающееся в установленном законодательством Российской Федерации порядке частной практикой, осуществляющий функции Мониторинга, Акцепта расходных операций по своим Счетам и/или Счетам Подконтрольных организаций, открытых в Банке, в силу требований законодательства Российской Федерации и/или на основании заключенного Клиентом договора, а также осуществляющее функции Мониторинга, контроля целевого использования денежных средств в рамках услуги банковского сопровождения контрактов.

1.3. **Мониторинг** - режим работы модуля ЦФК/РЦК, который обеспечивает возможность получения Контролирующей организацией в электронном виде детальной информации о движении денежных средств по своим Счетам и/или Счетам Подконтрольных организаций, зарегистрированным в модуле ЦФК/РЦК, в том числе:

– просмотр выписок;

– просмотр оборотно-сальдовой ведомости;

– просмотр отчета по остаткам;

– просмотр ЭПД по расходным операциям, предоставленным Подконтрольной организацией в Банк.

[3] Подключение модуля «Расчетный центр корпорации» Контролирующим организациям не осуществляется.

1.4. **Подконтрольная организация -** Клиент Банка (хозяйственное общество, индивидуальный предприниматель, обособленное/структурное подразделение Контролирующей организации), являющийся контролируемым со стороны Контролирующей организации в силу требований законодательства и/или на основании заключенного Клиентом договора, и предоставивший в Банк в предусмотренном настоящими Правилами порядке согласие на осуществление Контролирующей организацией контроля движения денежных средств по Счёту (функции Акцепта, Мониторинга, Управления счетами).

1.5. **Справочник статей /Справочник Кодов Бюджетного Классификатора (КБК) -** перечень кодов расходных статей (платежей)/ перечень кодов статей бюджета Клиента[4].

1.6. **Управление счетами (УС) –** режим работы «Мультиклиент» модуля ЦФК, позволяющий Контролирующей организации осуществлять формирование, подписание и передачу на исполнение в Банк ЭПД по своим Счетам и/или Счетам Подконтрольных организаций при наличии у Контролирующей организации соответствующих полномочий на распоряжение денежными средствами, находящимися на этих Счетах.

2. Общие положения

2.1. Предоставление модуля, позволяющего Контролирующей организации получать информацию по своим Счетам и/или Счетам Подконтрольных организаций (далее – Контролируемые счета) в режиме Мониторинг, осуществлять финансовый контроль деятельности в режиме Акцепт, формировать, подписывать и передавать на исполнение в Банк ЭПД по Счетам Подконтрольных организаций в режиме «Управление счетами» осуществляется на основании Заявления о предоставлении модуля Контролирующей организации.

В случае осуществления контроля за движением денежных средств по Счетам Подконтрольных организаций (режим Мониторинг, Акцепт, Управление счетами) необходимо предоставление Подконтрольной организацией Согласия на регистрацию Счетов в модуле ЦФК/РЦК по форме Приложения к Заявлению о предоставлении модуля (далее - Согласие на регистрацию счетов).

2.2. Согласие на регистрацию счетов от Подконтрольной организации принимается Банком только при наличии в Банке соответствующего Заявления о предоставлении модуля Контролирующей организации с отметкой Банка о приеме.

2.3. Предоставление Подконтрольной организацией Согласия на регистрацию счетов является поручением Банку на регистрацию Контролируемых счетов в модуле ЦФК/РЦК Контролирующей организации, а также подтверждением согласия Подконтрольной организации с порядком оплаты комиссионного вознаграждения Банка, установленным Контролирующей организацией в Заявлении о предоставлении модуля.

2.4. Предоставление Клиентам – Контролирующей и Подконтрольным организациям модуля ЦФК/РЦК осуществляется по месту обращения Клиента или по месту обслуживания Счета.

2.5. Использование модуля РЦК Контролирующей организацией осуществляется совместно с каналом «Клиент-Банк Онлайн» Системы ДБО «BS-Client (CORREQTS)».

Использование модуля ЦФК Контролирующей организацией возможно, как с одновременным подключением канала «Клиент-Банк Онлайн» Системы iBank, так и без его подключения. При использовании Контролирующей организацией модуля ЦФК совместно с каналом «Клиент-Банк Онлайн» Системы iBank требуется выпуск второго Ключа ЭП Уполномоченным лицам, которые будут дополнительно работать в канале «Клиент-Банк Онлайн» Системы iBank.

2.6. Фактом подключения Контролирующей организации к модулю ЦФК является предоставление Банком доступа к модулю ЦФК посредством регистрации Ключа проверки

[4] При использовании модуля ЦФК/РЦК в зависимости от типа Системы ДБО.

ЭП УЛ Контролирующей организации для работы в модуле ЦФК при подключении модуля ЦФК.

2.7. С использованием модуля ЦФК/РЦК предоставляются следующие возможности:

2.7.1. **Мониторинг** – базовый режим, предоставляемый Контролирующей организации при подключении модуля ЦФК/РЦК, позволяющий Контролирующей организации получать информацию по Контролируемым счетам путём формирования отчётов в меню «Оперативное управление» модуля РЦК и в меню «Отчеты» в режиме «Мультиклиент» модуля ЦФК.

2.7.2. **Акцепт** – дополнительно подключаемый к Мониторингу режим работы, позволяющий Контролирующей организации устанавливать правила и критерии контроля для акцепта платежей и бюджет Подконтрольным организациям.

2.7.2.1. Контролирующей организации в модуле ЦФК в режиме «Финансовый контроль», в модуле РЦК в меню «Оперативное управление / Расходы / Уведомление о лимитах» доступны следующие настройки:

– установка Многоуровневого акцепта ЭПД Подконтрольных организаций;

– настройка Выборочного акцепта;

– создание списков банков и контрагентов, на Счета и в адрес которых ЭПД направляются только после акцепта Контролирующей организации («чёрный список»), либо без дополнительного акцепта Контролирующей организацией («белый список»);

– формирование Справочника статей/Справочника КБК;

– настройка уведомлений о поступлении документов на акцепт в Системе ДБО в виде сообщения на электронную почту. Для указанного типа уведомления доступна настройка следующих полей: дата и время поступления документа, тип документа, номер документа, дата документа, наименование плательщика, причина попадания на акцепт. Настройку уведомлений осуществляет:

- в модуле ЦФК - Контролирующая организация самостоятельно в соответствии с эксплуатационной документацией, размещённой официальном Сайте Банка на странице входа в Систему ДБО, которая доступна через раздел «Вход в Интернет-Банк» (окно входа в Систему ДБО);
- в модуле РЦК - Банк (служба технической поддержки Системы ДБО).

2.7.2.2. Осуществление контроля исполнения бюджета / лимита обеспечивается Банком путём проверки на непревышение суммы ЭПД над суммой ограничения /лимита на расходные операции по каждой статье бюджета / статье расхода, установленной Контролирующей организацией в Справочнике статей / Справочнике КБК. Соответствующий операции код статьи/ код КБК из Справочника статей/ Справочника КБК указывается Подконтрольной организацией при формировании ЭПД в отдельном поле.

2.7.2.3. ЭПД Подконтрольной организации при направлении в Банк проходит все установленные автоматизированные правила контроля, результаты проверки каждого критерия контроля сохраняются в истории документа.

2.7.2.4. Особенности работы с автоматизированными правилам контроля:

- бюджеты/лимиты назначаются для каждой Подконтрольной организации индивидуально;
- невозможно использовать «белый» и «черный» список банков или получателей одновременно;
- реализован групповой акцепт нескольких документов;
- история изменений правил и критериев контроля сохраняется в системе.

2.7.2.5. ЭПД по Контролируемым счетам в рамках режима работы Акцепт поступают в Банк после прохождения проверки на соответствие автоматизированным правилам контроля, определенным Контролирующей организацией, или после осуществления акцепта Уполномоченным лицом Контролирующей организации.

2.7.2.6. В рамках работы в режиме Акцепт Клиент поручает Банку:

– предоставить Уполномоченным лицам, указанным в Заявлении о предоставлении модуля Контролирующей организации, доступ к модулю ЦФК/РЦК для просмотра информации об операциях по Контролируемым счетам и осуществления акцепта ЭПД на проведение расходных операций по Контролируемым Счетам;

– принимать к исполнению ЭПД по Контролируемым счетам при условии получения согласия (акцепта) Уполномоченного лица Контролирующей организации и/или наличии кода статьи /кода КБК, соответствующего бюджету, установленному Контролирующей организацией.

В случае отсутствия согласия Уполномоченного лица Контролирующей организации и/или кода статьи /кода КБК ЭПД не принимается к исполнению Банком, Клиент уведомляется в порядке, установленном Договором ДБО.

2.7.2.7. Реализована возможность акцепта следующих типов ЭД:

- в модуле ЦФК:

– Рублевые документы: Платежное поручение; Заявление об акцепте; Заявление о заранее данном акцепте; Заявление на аккредитив.

– Валютные документы: Заявление на перевод; Поручение на покупку иностранной валюты; Поручение на продажу иностранной валюты; Поручение на конвертацию валюты; Распоряжение о списании валюты с транзитного счета.

– Депозиты: Заявление на открытие депозита; Заявление на неснижаемый остаток; Заявление на возврат депозита; Заявление на закрытие неснижаемого остатка; Заявление на пополнение депозита.

- в модуле РЦК:

– Рублевые документы: Платежное поручение;

– Валютные документы: Валютный перевод.

2.7.3. **Управление счетами** – дополнительно подключаемый к Мониторингу режим работы «Мультиклиент», позволяющий в модуле ЦФК на стороне Контролирующей организации из единого рабочего места осуществлять формирование, подписание и передачу на исполнение в Банк ЭПД по Счетам Подконтрольных организаций.

2.7.3.1. Уполномоченное лицо Контролирующей организации формирует Ключи ЭП по Подконтрольным организациям, к Счетам которых ему предоставлен доступ. Для использования режима «Управление счетами» в модуле ЦФК Ключи ЭП Контролирующей и Подконтрольных организации должны храниться на одном носителе (токене), при этом пароли Ключа ЭП Контролирующей организации и Ключей ЭП Подконтрольных организаций должны совпадать.

2.7.3.2. Регистрация Ключей ЭП осуществляется в соответствии с процедурами, определёнными в Правилах.

2.7.3.3. Для создания ЭПД по Счетам Подконтрольных организаций Уполномоченное лицо Контролирующей организации формирует ЭПД в разделе Рублевые документы/Платежное поручение в модуле ЦФК, выбирая в окне «Выбор предприятия» Подконтрольную организацию, подписывает ключом ЭП соответствующей Подконтрольной организации и завершает оформление ЭПД выбором опции «отправить» в соответствии с эксплуатационной документацией, размещённой на официальном сайте Банка в сети Интернет www.abr.ru на странице входа в Систему ДБО, которая доступна через раздел «Вход в Интернет-Банк» (окно входа в Систему ДБО).

2.7.3.4. Подконтрольная организация получает информацию об ЭПД, созданных, подписанных и переданных на исполнение в Банк Уполномоченными лицами Контролирующих организаций, путём формирования Выписки по своим счетам.

2.8. В случае необходимости изменения параметров предоставления модуля ЦФК/РЦК:

2.8.1. Изменение режимов работы модуля ЦФК/РЦК, данных по Уполномоченным лицам, перечня Контролируемых счетов осуществляется на основании Заявления о предоставлении модуля Контролирующей организации.

Подконтрольная организация предоставляет Согласие на регистрацию счетов при регистрации каждого счета в перечне Контролируемых счетов.

2.8.2. Исключение закрываемого Счета из перечня зарегистрированных в модуле ЦФК/РЦК Счетов осуществляется на основании поданного в Банк заявления на закрытие счёта. В этом случае предоставление в Банк Заявления о предоставлении модуля или Согласия на регистрацию счетов для изменения перечня Контролируемых счетов не требуется.

2.9. При отказе Контролирующей организации от использования модуля ЦФК/РЦК, отключение зарегистрированных в модуле ЦФК/РЦК Контролируемых счетов осуществляется Банком на основании предоставленного Контролирующей организацией Заявления о предоставлении модуля, содержащего отметку об отключении модуля ЦФК/РЦК.

2.10. Банк вправе отказаться от предоставления модуля ЦФК/РЦК с отключением зарегистрированных в модуле ЦФК/РЦК Контролируемых счетов в одностороннем порядке в случае неоплаты предоставленных Банком услуг и/или в случае выявления факта неиспользования Контролирующей организацией модуля ЦФК/РЦК в течение 6 (шести) и более месяцев, направив Контролирующей организации уведомление способами, определёнными подп. 16.3.1 настоящих Правил.

Приложение № 4
Типовая форма Заявления о предоставлении модуля
ЦФК/РЦК Системы ДБО Контролирующей организации
(заполняется Контролирующей организацией)

ЗАЯВЛЕНИЕ О ПРЕДОСТАВЛЕНИИ МОДУЛЯ ЦФК/РЦК СИСТЕМЫ ДБО КОНТРОЛИРУЮЩЕЙ ОРГАНИЗАЦИИ

Клиент	
указывается наименование организации, включая организационно-правовую форму / ФИО индивидуального предпринимателя / физического лица, занимающегося частной практикой	
в лице	
действующий на основании	
ИНН	

НАСТОЯЩИМ ЗАЯВЛЕНИЕМ КЛИЕНТ ПРОСИТ:

1. ПРИ ОСУЩЕСТВЛЕНИИ ДИСТАНЦИОННОГО БАНКОВСКОГО ОБСЛУЖИВАНИЯ:

☐ подключить модуль ЦФК Системы **«iBank» (модуль ЦФК)**

☐ отключить модуль ЦФК/РЦК Системы ДБО *(выбрать Систему ДБО):*	☐ **«ДБО BS-Client (CORREQTS)» (модуль РЦК)** ☐ **«iBank» (модуль ЦФК)**

2. ПРЕДОСТАВИТЬ / ИЗМЕНИТЬ ДОСТУП к модулю ЦФК/РЦК следующим уполномоченным лицам:

(при необходимости добавить блоки об УЛ)

ВНИМАНИЕ! Доступ в Систему ДБО будет НЕВОЗМОЖЕН, в случае указания неверного / не существующего номера мобильного телефона или адреса электронной почты

ФИО (полностью) _____		**СНИЛС** _____		**e-mail и мобильный телефон**	_____@_____ +7 _____
☐	**отключить УЛ**	☐	**изменить пароль**	☐	**блокировать ключ**
При выборе буллитов «отключить УЛ», «изменить пароль», требуется только заполнение полей «ФИО» и «СНИЛС»					
☐	**подключить действующее УЛ**	☐	**подключить новое УЛ**	☐	**изменить данные**

Полномочия		**Тип ЭП**		**Дополнительно выдать**[5]		**Вариант защиты Системы и подтверждения исполнения документов (нужное отметить)**	
☐	просмотр[6]	**УНЭП**	☐ действующий УНЭП	☐	USB-токен	Обязательное подтверждение исполнения платежного документа[7]:	
☐	акцепт[8]		☐ на USB-токене Банка			☐	SMS-сообщение на номер +7 _____
☐	группа 1[3]		☐ на USB-токене Клиента, ранее выданном Банком[9]	☐	Устройство подтверждения[10]	☐	Устройство подтверждения[9]
☐	группа 2[3]		☐ на USB-токене Клиента, приобретенном Клиентом				

3. ПРОСИТ

☐ **выдать** по месту подачи заявления	☐ **направить** почтовой курьерской службой	☐ в подразделение Банка *(указать наименование)*		
		☐ по адресу Клиента:	Индекс:	
			Телефон	+ 7 - ___ - _____

USB-Токены, СКЗИ, Устройства подтверждения (в случае их выдачи) для Уполномоченных лиц, указанных в пункте V, программное обеспечение Клиентской части Системы ДБО и сопутствующую документацию **и доверяет совершать**[11] все юридические действия, связанные с их получением и обменом в АО АБ «РОССИЯ», с правом подписания необходимых документов, в том числе акта приема-передачи ключевых носителей, программного обеспечения и средств криптографической защиты информации

[5] Можно инициировать получение дополнительного USB-Токена, Устройства подтверждения.
[6] Применяется при выборе режима работы Мониторинг.
[7] Применяется при выборе режима работы Управление счетами в модуле ЦФК.
[8] Предоставляется при выборе режима работы Акцепт.
[9] Доступно с момента технической реализации
[10] Предоставляется при наличии технической возможности
[11] Не требуется предоставление отдельной доверенности на получателя, если настоящее заявление подписано ЕИО Клиента или представителем Клиента, имеющим доверенность с правом передоверия и являющимся руководителем филиала или представительства.

Фамилия, Имя, Отчество получателя		Реквизиты документа, удостоверяющего личность получателя)	
Настоящие полномочия получателя действуют в течение 60 календарных дней с даты приема Банком настоящего Заявления.			

Списание комиссионного вознаграждения Банка производить:	☐**изменить** *(заполняется при внесении изменений)*
☐ с Контролируемых счетов, подключенных к модулю	☐ Плата за установку модуля ☐ Плата за регистрацию и ведение счетов
☐ со счета Клиента	☐ Плата за установку модуля ☐ Плата за регистрацию и ведение счетов
№ счета	
открыт в[12]	

4. ОРГАНИЗОВАТЬ РАБОТУ в модуле ЦФК/РЦК Контролирующей организации со следующими Контролируемыми счетами:

(при необходимости в таблице добавить строки)

Наименование организации – владельца счета (ИНН)	**Номер счета**	Мониторинг	Акцепт			Управление счетами (iBank)
			Сплошной акцепт[13]	Выборочный акцепт[14]	Корп. бюджетирование	
	добавить ☐ исключить ☐	☐	☐	☐	☐	☐
	добавить ☐ исключить ☐	☐	☐	☐	☐	☐
	добавить ☐ исключить ☐	☐	☐	☐	☐	☐
	добавить ☐ исключить ☐	☐	☐	☐	☐	☐
	добавить ☐ исключить ☐	☐	☐	☐	☐	☐

Настоящим Клиент, в соответствии с Федеральным законом Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – Закон 152-ФЗ), подтверждает получение им в целях обмена электронными документами с использованием Системы ДБО всех требуемых в соответствии с действующим законодательством Российской Федерации (в том числе о персональных данных) согласий на передачу и обработку персональных данных субъектов персональных данных, упомянутых в любой из частей Заявления, а также направление в адрес таких субъектов персональных данных уведомлений об осуществлении обработки их персональных данных в АО «АБ «РОССИЯ», зарегистрированном по адресу: 191124, г. Санкт-Петербург, пл. Растрелли, д. 2, стр. 1, т.е. на совершение действий, предусмотренных п. 3. ст. 3. Закона 152-ФЗ.

К персональным данным, в отношении которых получено согласие субъекта персональных данных, относятся: фамилия, имя, отчество, дата и место рождения, паспортные данные, контактная информация, собственноручная подпись, иные персональные данные, упомянутые в любой из частей Заявления.

Перечень действий с персональными данными, в отношении которых получены согласия субъектов персональных данных, упомянутых в любой из частей Заявления, включает в себя - любое действие (операцию) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, в том числе сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных, а также передачу такой информации третьим лицам, в случаях, установленных действующим законодательством.

Настоящее подтверждение действует со дня его подписания в течение всего срока действия Договора. Условием прекращения обработки персональных данных является получение АО «АБ «РОССИЯ» письменного уведомления об отзыве согласия на обработку персональных данных.

ПОДПИСЬ КЛИЕНТА

Клиент подтверждает достоверность сведений, содержащихся в настоящем Заявлении о предоставлении модуля Системы ДБО

_____ _____

подпись дата

МП

ОТМЕТКИ БАНКА

Настоящее Заявление о предоставлении модуля Системы ДБО принято _____

дата

_____ _____

[12] В случае если счет открыт в другой кредитной организации в Банк предоставляется заверенная должным образом копия документа (договор, дополнительное соглашение, заявление и т.п.), заключенного с этой кредитной организацией, на основании которого Банку предоставлено право списывать денежные средства со счета.

[13] Режим работы «Сплошной акцепт» настраивает Банк.

[14] Режим работы «Выборочный акцепт», включающий настройку особого порядка и правил контроля, настраивает Контролирующая организация самостоятельно в модуле ЦФК/РЦК.

подпись ФИО

Приложение
к Заявлению о предоставлении модуля
Системы ДБО Контролирующей организации
(заполняется Подконтрольной организацией)

СОГЛАСИЕ НА РЕГИСТРАЦИЮ СЧЕТОВ В МОДУЛЕ ЦФК/РЦК
является неотъемлемой частью Заявления о предоставлении модуля Системы ДБО Контролирующей организации

Клиент	
указывается наименование организации, включая организационно-правовую форму / ФИО индивидуального предпринимателя / физического лица, занимающегося частной практикой.	
в лице	
действующий на основании	
ИНН	

НАСТОЯЩИМ ЗАЯВЛЕНИЕМ КЛИЕНТ – ПОДКОНТРОЛЬНАЯ ОРГАНИЗАЦИЯ

1. ВЫРАЖАЕТ СОГЛАСИЕ на осуществление в модуле ЦФК/РЦК Контролирующей организацией _____,
(указать наименование, организационно-правовую форму, ИНН Контролирующей организации)

контроля движения денежных средств по Контролируемым счетам. Настоящее согласие действует со дня его подписания в течение всего срока действия Договора или до момента исключения счета (-ов) из перечня Контролируемых счетов. Предоставление информации уполномоченному представителю Контролирующей организации рассматривается как предоставление информации Уполномоченному лицу Клиента (п. 4 ст. 185 ГК Российской Федерации).

2. ПРОСИТ ОРГАНИЗОВАТЬ РАБОТУ в модуле ЦФК/РЦК Контролирующей организации со следующими Контролируемыми счетами:
(при необходимости в таблице добавить строки)

Наименование организации – владельца счета (ИНН)	**Номер счета**	Мониторинг	Акцепт			Управление счетами (iBank)
			Сплошной акцепт[15]	Выборочный акцепт[16]	Корп. бюджетирование	
	добавить ☐ исключить ☐	☐	☐	☐	☐	☐
	добавить ☐ исключить ☐	☐	☐	☐	☐	☐
	добавить ☐ исключить ☐	☐	☐	☐	☐	☐
	добавить ☐ исключить ☐	☐	☐	☐	☐	☐
	добавить ☐ исключить ☐	☐	☐	☐	☐	☐
	добавить ☐ исключить ☐	☐	☐	☐	☐	☐

Настоящим Клиент, в соответствии с Федеральным законом Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – Закон 152-ФЗ), подтверждает получение им в целях обмена электронными документами с использованием Системы ДБО всех требуемых в соответствии с действующим законодательством Российской Федерации (в том числе о персональных данных) согласий на передачу и обработку персональных данных субъектов персональных данных, упомянутых в любой из частей Заявления, а также направление в адрес таких субъектов персональных данных уведомлений об осуществлении обработки их персональных данных в АО «АБ «РОССИЯ», зарегистрированном по адресу: 191124, г. Санкт-Петербург, пл. Растрелли, д. 2, стр. 1 , т.е. на совершение действий, предусмотренных п. 3. ст. 3. Закона 152-ФЗ.
К персональным данным, в отношении которых получено согласие субъекта персональных данных, относятся: фамилия, имя, отчество, дата и место рождения, паспортные данные, контактная информация, собственноручная подпись, иные персональные данные, упомянутые в любой из частей Заявления.
Перечень действий с персональными данными, в отношении которых получены согласия субъектов персональных данных, упомянутых в любой из частей Заявления, включает в себя - любое действие (операцию) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, в том числе сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных, а также передачу такой информации третьим лицам, в случаях, установленных действующим законодательством.

[15] Режим работы «Сплошной акцепт» настраивает Банк.
[16] Режим работы «Выборочный акцепт», включающий настройку особого порядка и правил контроля, настраивает Контролирующая организация самостоятельно в модуле ЦФК/РЦК.

Настоящее подтверждение действует со дня его подписания в течение всего срока действия Договора. Условием прекращения обработки персональных данных является получение АО «АБ «РОССИЯ» письменного уведомления об отзыве согласия на обработку персональных данных.

ПОДПИСЬ КЛИЕНТА

Клиент подтверждает достоверность сведений, содержащихся в настоящем Согласии на регистрацию счетов в модуле ЦФК/РЦК.

_____ _____

подпись дата

МП

ОТМЕТКИ БАНКА

Настоящее Согласие на регистрацию счетов в модуле ЦФК/РЦК принято _____

дата

_____ _____

подпись ФИО

Приложение № 5

Перечень Сервисов Системы ДБО

№ п/п	Наименование Сервиса	Способ подключения Сервиса
1.	**Сервисы Системы ДБО, доступные для использования независимо от наличия/ отсутствия открытого Счета в Банке:**	
1.1.	Обмен сообщениями между Банком и Клиентом в формате ЭСИД «Письмо», содержащего текст или файл установленного Банком формата (файлы в формате pdf, а при отсутствии такой возможности – в формате jpeg или tif), в том числе применяется в рамках заключённого между Банком и Клиентом отдельного договора/соглашения: – об оказании депозитарных услуг, – о перечислении заработной платы сотрудников на карточные счета, – о предоставлении услуги банковского сопровождения контрактов и иных услуг согласно заключаемым между Банком и Клиентом договорам.	Доступно при подключении СДБО
1.2.	Приём ЭД, необходимых для осуществления Банком функций агента валютного контроля, по установленным законодательством Российской Федерации и нормативными актами Банка России и/или Банком формам, предоставляемых: – в формате, определяемом Системой ДБО; – в формате ЭСИД «Письмо», содержащего вложенный сканированный графический образ (файлы в формате pdf, а при отсутствии такой возможности – в формате jpeg или tif), являющийся точным воспроизведением оригинала документа;	Доступно при подключении СДБО
1.3.	Сервис SMS-информирования - сервис Системы ДБО, в рамках которого Банк предоставляет Клиенту информацию по Счету (при наличии), информацию о поступлении в Банк/получении из Банка ЭД или о входе в Систему ДБО посредством направления Банком такой информации в виде SMS-сообщений на номера мобильных телефонов Клиента. Подключением услуги «SMS-информирование» Клиент поручает Банку осуществлять «SMS-информирование» посредством направления информации через операторов связи, обслуживающих Банк, в том числе в случаях, когда передаваемая информация содержит сведения, составляющие банковскую тайну.	Дистанционно
1.4.	Сервис по заключению договора присоединения к Условиям депозитных сделок/ НСО с использованием СДБО – сервис по предоставлению клиентам возможности заключения договора посредством направления в Банк электронного документа «Заявка на подключение услуги «Депозиты» / «НСО». Подачу Заявки на подключение услуги осуществляет единоличный исполнительный орган Клиента или лицо им уполномоченное.	Дистанционно
1.5.	Сервис предоставления сведений об Уполномоченных лицах для целей получения отчётности в рамках услуги банковского сопровождения контрактов и кэш-пулинга.	Дистанционно
1.6.	Сервис предоставления сведений об изменении личных данных Уполномоченных лиц для целей СДБО[17].	Дистанционно
1.7.	Сервис подключения Канала «Интеграционный Клиент-Банк» - сервис подключения канала отправки ЭД в Банк Системы ДБО, предоставляющий возможность обмена ЭД с Банком с	Дистанционно

[17] Сервис доступен с момента технической реализации.

№ п/п	Наименование Сервиса	Способ подключения Сервиса
	использованием УНЭП и УКЭП напрямую из Системы Клиента. Подключение канала осуществляется в соответствии с Приложением № 1 к настоящим Правилам для услуг Модуль «Интеграционный корпоративный шлюз», Обмен с 1С, Автоклиент, API Интеграция.	
1.8.	Сервис «Подписки» - сервис направления Клиенту уведомлений о наступлении определённых событий, параметры подписки настраиваются посредством изменения разрешённых настроек в пользовательском интерфейсе данного сервиса.	Дистанционно
1.9.	Модуль «Центр финансового контроля / Расчетный центр корпорации» - сервис контроля за расходованием денежных средств по своим Счетам и/или счетам Подконтрольных организаций, открытым в Банке. В рамках модуля доступна работа со счетами в режиме «Мониторинг», «Акцепт» («Сплошной акцепт», «Выборочный акцепт». «Корпоративное бюджетирование»), «Управление счетами». Подключение осуществляется Банком на основании Заявления о предоставлении модуля в порядке и на условиях, определённых Приложением № 4 к настоящим Правилам.	На основании заявления
1.10.	Модуль Транзит 2.0 - модуль взаимодействия с Системой Транзит Небанковской кредитной организации акционерного общества «Национальный расчетный депозитарий» (НРД) в соответствии с отдельными правилами правил предоставления услуги обмена электронными документами с Системой Транзит НРД.	На основании заявления
1.11.	Модуль «Кредиты»[18] - сервис по сопровождению кредитных договоров. Клиенту доступен функционал по: – просмотру информации по действующим кредитам (вид кредита, сумма, валюта, срок, процентная ставка, сумма задолженности и пр.); – формированию и направлению в Банк заявления на транш, заявления о досрочном погашении кредита, подписанного ЭП (УНЭП/ УКЭП/ ПЭП PayControl), в формате ЭД. Функционал доступен Уполномоченному лицу Клиента при условии подключении к модулю «Кредиты».	Дистанционно
1.12.	Сервис предоставления доступа к Модулю «Кредиты» и сведений об Уполномоченных лицах **(**Заявление на изменение перечня уполномоченных лиц**).**	Дистанционно
2.	**Сервисы Системы ДБО, доступные для использования только при наличии открытого Счета в Банке:**	
2.1.	Приём от Клиента ЭПД на выполнение операций по Счетам Клиента;	Доступно при подключении СДБО
2.2.	Сервис передачи Клиенту Выписок по Счетам Клиента и приложений к ним (в случае наличия открытого Счёта в Банке) за предыдущий Операционный день (включая обороты и сальдо по счёту). Обновление сведений происходит в автоматическом режиме при входе Клиента в Систему ДБО.	Доступно при подключении СДБО
2.3.	Сервис проверки контрагентов[19] - автоматизированный сервис, предназначенный для получения в режиме он-лайн аналитической информации о контрагентах (получателях	Дистанционно

[18] Сервис обеспечивается при наличии технической возможности.

[19] Услуга доступна при использовании Канала доступа «Клиент-Банк Онлайн» и в Мобильном приложении Банка.

№ п/п	Наименование Сервиса	Способ подключения Сервиса
	платежа) Клиента на основе официальных открытых источников информации федеральных органов власти (ФНС, ФССП, Росреестр, Генпрокуратура и др.). В интерфейсе Системы «ДБО «BS-Client (CORREQTS)» это «Светофор», в Системе iBank – «Индикатор». Получаемая по организации информация не является официальной, носит оценочный характер и не налагает на Банк каких-либо обязательств, не побуждает пользователя Сервиса проверки контрагентов к совершению каких-либо действий. Клиент, самостоятельно принимая решение об использовании Сервиса проверки контрагентов, соглашается с рисками, связанными с использованием указанной информации, актуальность которой соответствует моменту обработки запроса Клиента и её актуальности в открытом официальном источнике.	
2.4.	Сервис «Справочный конвейер»[20] – включает возможность запроса справок по Счетам Клиента, открытым в Банке, заказа дубликатов документов, включая копию Банковской карточки с образцами подписей. Справки и дубликаты документов (выписка, платежное поручение, копия Банковской карточки) предоставляются Клиенту в виде вложения в «Письмо», подписанного ЭП Банка.	Дистанционно
2.5.	Сервис «Электронная заявка на выдачу наличных денежных средств» - выдача денежных средств осуществляется со Счёта Клиента на основании расходного кассового ордера, оформленного Банком, без использования Клиентом чековой книжки. В целях получения денежных средств с использованием чековой книжки Клиент может направить заявку в формате «Письмо» в соответствии с подп. 16.3.2 настоящих Правил.	Дистанционно
2.6.	Сервис по заключению сделок на размещение денежных средств в неснижаемые остатки и депозиты онлайн с использованием Системы ДБО при условии заключения между Банком и Клиентом договора о присоединении к Условиям депозитных сделок/ НСО.	Дистанционно
2.7.	Сервис предоставления сведений об Уполномоченных лицах для целей размещения денежных средств в Депозиты и/или НСО.	Дистанционно
2.8.	Сервис направления Банком Клиенту уведомлений: – об операциях поступления и/или списания по Счету(ам) в валюте Российской Федерации в СДБО iBank в виде SMS-сообщений.	Дистанционно
2.9.	Сервис направления Клиентом из интерфейса Системы ДБО на электронный адрес контрагента Клиента: – информации об исполненном платеже. Сообщения направляются программным путем с электронного почтового ящика notification [mailto:ibank2@abr.ru] в Системе «iBank», с адреса online@abr.ru в Системе «ДБО BS-Client(CORREQTS)»; – реквизитов Счета. Сообщения направляются программным путем с электронного почтового ящика notification [mailto:ibank2@abr.ru] в Системе «iBank», с адреса online@abr.ru в Системе «BS-Client(CORREQTS)».	Дистанционно
2.10.	Сервис работы со Счетами в режиме «Акцепт (визирование)». Подключение осуществляется Банком на основании Заявления/ Заявления об изменении данных. Порядок предоставления указанных услуг определён разделом 7 настоящих Правил.	На основании заявления

[20] Перечень предоставляемых сведений может расширяться по мере технической реализации.

№ п/п	Наименование Сервиса	Способ подключения Сервиса
2.11.	Сервис акцепта оферты об установлении индивидуальных тарифов расчётно-кассового обслуживания (РКО) – автоматизированный сервис «Заявление на акцепт оферты об установлении индивидуальных тарифов РКО», позволяющий Клиентам заключать дополнительное соглашение к Договору банковского счёта о применении индивидуальных тарифов в формате акцепта оферты Банка.	Дистанционно
2.12.	Сервис предоставления информации об ограничениях /арестах и картотеке по Счету (-ам) Клиента. Обновление сведений происходит в автоматическом режиме. В интерфейсе СДБО реализовано отражение наличия действующих ограничений: – на стартовой странице по каждому расчётному счёту отображена информация о заблокированной сумме; – по нажатию открывается подробная информация о наложенных ограничениях.	Доступно при подключении СДБО
2.13.	Сервис переводов с использованием Системы быстрых платежей[21] (предоставляется при условии заключения Договора СБП) – может быть предоставлен доступ к разделу «B2B СБП» / разделу «B2C СБП».	На основании заявления/ дистанционно (с момента технической реализации)

В Системе ДБО подключение дополнительных Сервисов Системы ДБО доступно:

– с дистанционным подключением посредством Системы ДБО.

Для подключения Сервисов Системы ДБО используется:

- в Системе «ДБО BS-Client (CORREQTS)» - пункт меню «Продукты и услуги», в том числе модуль «Электронный офис», «Кассовые операции», «Депозиты», «Неснижаемые остатки», Заявление на изменение перечня УЛ, или виджет «Услуги» главного экрана;
- в Системе «iBank» - модуль «Управление услугами», «Депозиты», «Рублевые документы», меню разделов интерфейса iBank;
- изменение разрешённых Системой ДБО настроек.

Порядок дистанционного подключения сервисов определён инструкциями и/или пользовательской документацией, размещённой на сайте Банка по адресу: www.abr.ru.

– на основании заявления Клиента, по форме, установленной Правилами.

Предоставление Клиенту банковских услуг, не включённых в Договор ДБО, индивидуальных условий обслуживания регулируется дополнительными соглашениями к Договору ДБО, отдельными договорами, соглашениями и правилами (условиями) обслуживания, заключёнными / установленными как до, так и после заключения Договора ДБО.

[21] сервис Системы быстрых платежей обеспечивается в объеме технически реализованной и доступной функциональности.

Приложение № 6а

Инструкция по установке Системы «iBank»

1. Технические требования к оборудованию для работы в Системе «iBank»

Для работы с Системой «iBank» Клиент должен самостоятельно и за свой счёт обеспечить минимальные технические, программные и коммуникационные ресурсы.

Требования к аппаратному и программному окружению. Канал доступа «Клиент-Банк Онлайн».

Требования к программному окружению:

Вид ПО	Наименование ПО	Поддерживаемые версии ПО	Примечания
ОС	Windows	7 (x86/x64), 8 (x86/x64), 8.1 (x86/x64), 10 (x86/x64) и выше;	
	Apple	Apple Mac OS X: 10.12 и выше;	
	Linux	Ubuntu и прочие deb-дистрибутивы (последние версии x64)	
Веб-браузер	Internet Explorer, Firefox, Opera, Safari, Chrome, Яндекс.Браузер	Edge; Chrome (последняя версия); Firefox (последняя версия); Opera (последняя версия);	Web-браузер с поддержкой плагина «BifitSigner» для использования электронной подписи с применением аппаратных криптопровайдеров

Требования к аппаратному обеспечению

Любой современный компьютер с Web-браузером, наличием принтера, на котором будет распечатан сертификат ключа проверки ЭП Клиента, и USB-порта для использования съёмных USB-носителей: USB-токенов. Доступ в Интернет.

2. Порядок установки клиентской части системы «iBank»:

2.1. **Ссылки для скачивания программного обеспечения:**

– адрес для загрузки драйверов USB-токенов: https://ibank.abr.ru/makekeys.html

– адрес для загрузки инструкций: https://ibank.abr.ru/ibank2/#/

– адрес для загрузки сервиса и документации «iBank для 1С: https://ibank.abr.ru/ibank2/#/

2.2. **Порядок установки клиентского модуля «Internet-Банкинг для корпоративных клиентов (web-интерфейс)»**

Для работы в web-интерфейсе для корпоративных Клиентов необходимо:

– ознакомиться с руководством пользователя;

– установить плагин «BIFIT Signer» согласно инструкции (пункт 2.1);

– установить драйвер USB-токена при использовании USB-токена для хранения Ключа ЭП;

– самостоятельно провести предварительную регистрацию в Системе «iBank», запустив программу предварительной регистрации в разделе «Регистрация и ключи ЭП» на сайте https://ibank.abr.ru и сформировать Ключи ЭП;

– в разделе выбора типа ЭП установите отметку либо в поле «ЭП на аппаратном устройстве», либо в поле Облачная (Серверная) ЭП (в интерфейсе Системы iBank может применяться термин «Облачная ЭП» вместо «Серверная ЭП»):

– заполните данные на Уполномоченного лица (пользователя системы);

– укажите адрес электронной почты и мобильный телефон;

– при формировании Облачной (Серверной) ЭП подтвердите согласие с условиями доверенности, установив соответствующую отметку;

– при формировании Облачной (Серверной) ЭП придумайте название и пароль для своей Облачной (Серверной) ЭП и введите проверочный код;

– сохраните Бланк Ключа проверки ЭП (дополните бланк данными об организации или ИП)

– нажмите кнопку «Завершить»;

– подпишите распечатанный Бланк Ключа проверки ЭП Клиента и предоставьте бланк в Банк для окончательной регистрации в Системе **(срок предоставления документов в Банк – 15 (пятнадцать) рабочих дней с момента предварительной регистрации в Системе ДБО)**.

2.3. **Дополнительный модуль «iBank для 1С»**

Ссылка для загрузки модуля и документации «iBank для 1С» приведена в пункте 2.1 данного приложения.

Модуль совместим со следующими конфигурациями 1С:

– Бухгалтерия предприятия, редакция 2.0
– Бухгалтерия предприятия, редакция 3.0
– Управление торговлей, редакция 10.3
– Управление торговлей, редакция 11.1, редакция 11.2
– Управление производственным предприятием, редакция 1.3
– Комплексная автоматизация, редакция 1.1
– Управление небольшой фирмой, редакция 1.5
– 1С:ERP Управление предприятием 2.0
– Зарплата и управление персоналом 2.5
– Зарплата и управление персоналом 3.0

Для использования сервиса необходимо:

– иметь зарегистрированные в Банке ключи электронной подписи;
– подключить услугу в Банке;
– установить драйвер для USB-токенов (при необходимости);
– установить и настроить сервис (в соответствии с руководством пользователя сервиса);
– обеспечить доступ в Internet.

Приложение № 6б
(выдается при подписании Заявления и
выборе Системы «ДБО CORREQTS»)

ИНСТРУКЦИЯ
по установке Системы «ДБО BS-Client (CORREQTS)»
и Мобильного приложения Банка

1. Технические требования к оборудованию для работы в Системе «ДБО BS-Client (CORREQTS)».

Для работы с Системой **«ДБО BS-Client (CORREQTS)»** Клиент должен самостоятельно и за свой счет обеспечить следующие минимальные технические, программные и коммуникационные ресурсы:

Требования к аппаратному и программному окружению. Канал доступа «Клиент-Банк Онлайн».

Требования к программному окружению:

Вид ПО	**Наименование ПО**	**Поддерживаемые версии ПО**	**Примечания**
ОС	Windows	Windows 7, Windows 8 x86 и x64, Windows 8.1 x86 и x64, Windows 10 x86их64,	
	MacOS	10.12 (Sierra) и выше	
Веб-браузер	Microsoft Internet Explorer	10.0 и выше	
	Google Chrome	70.x	
	Mozilla Firefox	63.x	
	Opera	56.x	
	Safari	10, 11, 12	
Текстовый процессор	Microsoft Word	2007 и выше	Не обязательно. Для чтения RTF-файлов документов, сформированных с помощью подсистемы
	Office: Mac	2011	
Редактор электронных таблиц	Microsoft Excel	2007 и выше	
	Office: Mac	2011	
ПО для работы с документацией	Adobe Reader, Adobe Acrobat Standart, Adobe Acrobat Professional	5.0 и выше	Необходимо для чтения документации подсистемы

Требования к аппаратному обеспечению:

Любой современный компьютер с операционной системой семейства Windows, доступом в интернет, наличием принтера, на котором будет распечатан сертификат ключа

проверки ЭП Клиента, наличием в компьютере USB-порта для использования съёмных USB-носителей: USB-токенов.

2. **Порядок установки Системы «ДБО BS-Client (CORREQTS)»** (клиентский модуль «Интернет-Клиент»).

2.1. Для начала работы в Системе необходимо произвести следующие операции при использовании УНЭП/УКЭП:

2.1.1. Вставить USB-токен в рабочий компьютер;

2.1.2. Ввести Логин и Пароль на странице входа в Систему;

2.1.3. Установить криптоплагин. Подробная инструкция по установке криптоплагина доступна на сайте входа в Систему «ДБО BS-Client(CORREQTS)» в разделе «Как пользоваться системой» по адресу: https://online.abr.ru/ru/help/html/Basic/InstallCryptoPlagin.html.

2.1.4. Сгенерировать ключи ЭП и отправить запрос на регистрацию Ключа проверки ЭП в Банк, в том числе для работы в Модуле Транзит 2.0 с применением КриптоПро CSP в Системе ДБО «BS-Client (CORREQTS)». Подробная инструкция по формированию ключей ЭП и отправке запроса в Банк доступна по адресу: https://online.abr.ru/ru/help/html/Basic/certReq.html.

2.1.5. Заполнить, распечатать и предоставить Бланк ключа ЭП Клиента в Банк в случае его предоставления на бумажном носителе **(срок предоставления документов в Банк – 15 (пятнадцать) рабочих дней с момента** отправки электронного запроса на регистрацию Ключа проверки ЭП в Банк**);**

2.2. Инструкция по эксплуатации Системы «ДБО BS-Client (CORREQTS)» доступна на странице входа в Систему «ДБО BS-Client (CORREQTS)» в разделе «Как пользоваться системой» по адресу: https://online.abr.ru/ru/help/html/.

3. Технические требования к оборудованию для работы в Мобильном приложении.

Для работы в Мобильном приложении Банка Клиент должен самостоятельно и за свой счёт обеспечить следующие минимальные технические, программные и коммуникационные ресурсы.

Требования к программному окружению:

Вид ПО	**Наименование ПО**	**Поддерживаемые версии ПО**	**Примечания**
ОС	Android	5.x – 10.x	

Требования к аппаратному обеспечению:

Любой современный мобильный телефон с операционной системой Android доступом в интернет.

4. Порядок установки Мобильного приложения.

Для начала работы в Мобильном приложении Банка необходимо произвести следующие действия:

4.1. Скачать и установить приложение:

– Для устройств с ОС Android установочный файл доступен на официальном сайте Банка https://abr.ru/corp/remote-services/client-bank/.

Подробная инструкция по установке приложения доступна на сайте входа в Систему «ДБО BS-Client (CORREQTS)» в разделе «Как пользоваться системой», подраздел «Мобильное приложение».

4.2. Для работы в приложении необходимо ввести Логин и Пароль.

5. Технические требования к оборудованию для работы в Мобильном приложении PayControl.

Требования к программному окружению:

Вид ПО	**Наименование ПО**	**Поддерживаемые версии ПО**	**Примечания**
ОС	Android	4.4 и выше	

Требования к аппаратному обеспечению:

Любой современный мобильный телефон с операционной системой Android, доступом в интернет, камерой.

6. Порядок установки Мобильного приложения PayControl.

Для начала работы в Мобильном приложении PayControl необходимо произвести следующие действия:

6.1. Скачать и установить приложение PayControl производителя SafeTech Ltd.

– для устройств с ОС Android приложение PayControl доступно для скачивания и установки в магазине GooglePlay.

– для устройств с ОС iOS приложение PayControl доступно для скачивания и установки в магазине AppStore

6.2. Подробная инструкция по установке приложения доступна на сайте входа в Систему «ДБО BS-Client (CORREQTS)» в разделе «Как пользоваться системой», подраздел «PayControl».

Приложение № 7

Перечень[1]
электронных документов, используемых в Системе ДБО, использование ЭП в зависимости от типа ЭД

1. Электронные документы, направляемые Клиентом в Банк с использованием Канала «Клиент-Банк Онлайн»:

Тип документа	Возможность использования подписи			
	ПЭП PayControl	УНЭП/ Серверная ЭП[2]	УКЭП	Порядок подписания Клиентом
Платежное поручение	да	да	да	Кол-во подписей устанавливается Клиентом в Заявлении / Заявлении об изменении данных, либо определяется настройками Систем ДБО
Платежное требование, инкассовое поручение	да	да	да	
Массовый платёж (в Системе ДБО «BS-Client (CORREQTS)»)	нет	да	да	
Реестр на зачисление заработной платы (в рамках зарплатных проектов)	да	да	да	
Заявление на выдачу наличных денежных средств	да	да	да	
Заявление на размещение депозита	да	да	да	
Заявление на возврат депозита	да	да	да	
Заявление на пополнение депозита	да	да	да	
Заявление на частичный возврат депозита	да	да	да	
Заявление на установление неснижаемого остатка на счете/ Заявление на неснижаемый остаток (определяется Системой ДБО)	да	да	да	
Заявление на неснижаемый остаток. Отзыв[3]	да	да	да	
Постановка на учет договора/снятие с учета договора	да	да	да	
Сведения о валютной операции	да	да	да	
Запрос на получение справки о подтверждающих документах	да	да	да	
Изменение сведений о договоре	да	да	да	

[1]Перечень документов по мере расширения функционала Системы ДБО может изменяться, дополняться.
[2] Серверная ЭП не применяется при работе в модуле ЦФК/РЦК и в Системе ДБО «BS-Client (CORREQTS)
[3] Доступно с момента технической реализации

Тип документа	Возможность использования подписи			
	ПЭП PayControl	УНЭП/ Серверная ЭП[2]	УКЭП	Порядок подписания Клиентом
Распоряжение на списание денежных средств с транзитного валютного счета	да	да	да	
Поручение на перевод валюты	да	да	да	
Поручение на конвертацию валюты	нет	да	да	
Запрос на отзыв документа	да	да	да	
Запрос на выпуск сертификата ключа проверки ЭП	нет	да	да	
Запрос на продление Ключа PayControl	да	нет	нет	
Заявка на подключение услуги «Депозиты» / «НСО	да	да	да	
Заявление на изменение перечня уполномоченных лиц по сделкам НСО и депозитов	да	да	да	
Заявление на предоставление сведений об уполномоченных лицах для целей банковского сопровождения контрактов и кэш-пулинга	да	да	да	
Запрос на получение справки	да	да	да	
Заявка на Банковскую карточку	да	да	да	
Заявление на акцепт Оферты. Индивидуальный тариф РКО.	да	да	да	
Заявление на досрочное погашение кредита	да	да	да	
Заявление на транш	да	да	да	
Письмо / Произвольный документ – документ в системе ДБО «Письмо в Банк»/ «Письмо», в том числе с вложениями в виде файлов	да	да	да	

2. Электронные документы, получаемые Клиентом из Банка с использованием Канала «Клиент-Банк Онлайн»:

№п/п	Электронный документ	Вид ЭД	Порядок подписания Банком
1.	Выписка, содержащая информацию о движении средств по счетам (в том числе в виде сообщений в формате MT 940, MT 941, MT 942 /сообщений в формате ISO 20022)	формализованный	

№п/п	Электронный документ	Вид ЭД	Порядок подписания Банком
2.	Справка о подтверждающих документах, обработанная Банком	формализованный	Формируется АБС «ЦФТ-Банк» и отправляется шлюзом (без подписи Банка) / 1 ЭП уполномоченного лица Банка
3.	Сведения о валютной операции, обработанные Банком	формализованный	
4.	Заявление о постановке контракта на учет, обработанное Банком	формализованный	
5.	Документы, предусмотренные и составленные в соответствии с иными заключенными между Банком и Клиентом договорами и соглашениями	произвольный	
6.	Иные документы или письма, составленные в произвольной форме (в том числе содержащие вложенные копии документов валютного контроля, справки о наличии счета (счетов), о движении/ отсутствии движения средств по счету (счетам), об остатке средств на счете (счетах), о наличии/ отсутствии картотеки/ очереди распоряжений к счету/ счетам) - ЭСИД «Письмо»	произвольный	

3. Форматы электронных документов, передаваемых с использованием раздела «СБП B2B» / «СБП B2C» канала «Клиент-Банк Онлайн»:

Форматы передаваемых электронных документов определены требованиями документов, регулирующих порядок предоставления СБП, включая нормативные акты Банка России, устанавливающие правила платежной системы Банка России, а также правила, стандарты и требования, установленные АО «Национальная система платежных карт», выполняющим функции операционного и платежного клирингового центра при осуществлении перевода денежных средств в СБП (размещены на официальном сайте ОПКЦ СБП https://sbp.nspk.ru/).

Форматы передаваемых между Банком и ОПКЦ СБП документов определены Банком России в Альбоме распоряжений о переводе денежных средств, применяемых в платежной системе Банка России, публикуемом на официальном сайте Банка России по адресу: https://www.cbr.ru.

4. Электронные документы, направляемые в Банк и получаемые из Банка с использованием Канала «Интеграционный Клиент-Банк» [4]:

4.1. Сервис «Обмен с 1С по DirectBank».

Со стандартами обмена и форматами передаваемых документов при интеграции с программами на платформе «1С» можно ознакомиться на сайте фирмы «1С» и на сайте Банка по адресу www.abr.ru в разделе «Интеграционный Клиент-Банк».

4.2. Модуль «Корпоративный автоклиент» Системы «iBank».

Форматы передаваемых документов определены пользовательской документацией, которая размещена на сайте банка по адресу: www.abr.ru в разделе «Интеграционный Клиент-

[4] Перечень документов по мере расширения функционала модулей Системы ДБО может изменяться, дополняться.

Банк» и на странице входа в Систему ДБО, которая доступна через раздел «Вход в Интернет-Банк» (окно входа в Систему ДБО).

4.3. Модуль «Интеграционный Корпоративный шлюз» системы ДБО «BS-Client (CORREQTS)».

Стандарты обмена и форматы передаваемых документов определены пользовательской документацией, которая предоставляется Банком[5].

4.4. Модуль Транзит 2.0

Стандарты обмена и форматы передаваемых документов определены пользовательской документацией Модуля Транзит 2.0 и требованиями системы Транзит Небанковской кредитной организации Акционерное общество «Национальный расчетный депозитарий». Перечень передаваемых ЭД определен Договором Транзит 2.0.

4.5. API Интеграция[6]

Стандарты обмена и форматы передаваемых документов определены пользовательской документацией, которая размещена на сайте Банка по адресу: www.abr.ru в разделе «Интеграционный Клиент-Банк».

[5] Подключение новых учетных записей Клиентам – головным организациям в модуле «Интеграционный Корпоративный Шлюз» не осуществляется

[6] Доступно с момента технической реализации

Приложение № 8
(оформляется при расторжении (отказе от) Договора ДБО/ смене Уполномоченных лиц Клиента в случае наличия у Клиента СКЗИ, полученных в Банке)

АКТ
возврата средств криптографической защиты информации [7]

г._____ «_____» _____ 20____ г.

В соответствии с Договором №_____ (далее – Договор) Акционерное общество «Акционерный Банк «РОССИЯ», именуемое в дальнейшем «**Банк**», в лице _____, действующего на основании _____, и _____, именуемое в дальнейшем «**Клиент**», в лице _____, действующего на основании _____, именуемые далее «**Стороны**», составили настоящий Акт о том, что Клиент передал, а Банк принял в рамках оказания услуг, связанных с эксплуатацией Системы ДБО:

1. Средства криптографической защиты информации (СКЗИ) и носители:

№ п/п	Наименование СКЗИ	Идентификационный номер СКЗИ	Наименование и учетный номер носителя	ФИО владельца (Уполномоченное лицо Клиента)	Подпись владельца СКЗИ

2. Ключевые носители:
☐USB-Токен

№ п/п	Наименование носителя	Учетный номер носителя	ФИО владельца (Уполномоченное лицо Клиента)	Подпись владельца

Уничтожение ключевой информации (криптографических ключей) подтверждаем.
Достоверность сведений подтверждаем.
Настоящий Акт составлен в 2-х экземплярах, по одному для каждой из сторон, и является неотъемлемой частью Договора.

Подписи Сторон

Банк	**Клиент**
_____/_____/	_____/_____/

[7] Разделы Акта о наименовании и номере СКЗИ и номере носителя заполняются на основании данных Акта (-ов) приема-передачи ключевых носителей, программного обеспечения и средств криптографической защиты информации, подписанного (-ых) Клиентом, либо на основании Формуляра на средство криптографической защиты информации, выданное Клиенту в комплекте с СКЗИ. Формуляр подлежит передаче в Банк с возвращаемым СКЗИ.

Приложение № 9
(подписывается в обязательном порядке при передаче Клиенту ключевых носителей, ПО и СКЗИ)

АКТ
приема-передачи
ключевых носителей, программного обеспечения и
средств криптографической защиты информации

г._____ «_____» _____ 20____ г.

В соответствии с Договором от «___» _____ 20___г. №_____ (далее – Договор) Акционерное общество «Акционерный Банк «РОССИЯ», именуемое в дальнейшем «**Банк**», в лице _____, действующего на основании _____, и _____, именуемое в дальнейшем «**Клиент**», в лице _____, действующего на основании _____, именуемые далее «**Стороны**», составили настоящий Акт о том, что Банк передал, а Клиент принял в рамках оказания услуг, связанных с установкой и эксплуатацией Системы ДБО:

1. Программное обеспечение Клиентской части Системы ДБО:

При подключении «ДБО BS-Client (CORREQTS)» с интернет ресурса https://online.abr.ru	**При подключении «iBank»** с интернет ресурса https://ibank.abr.ru

2. Средства криптографической защиты информации (СКЗИ) и носители:

№ п/п	Наименование СКЗИ	Идентификационный номер СКЗИ	Наименование и учетный номер носителя	ФИО владельца (Уполномоченное лицо Клиента)	ФИО и подпись получателя СКЗИ

3. Ключевые носители:
☐USB-Токен

№ п/п	Наименование носителя	Учетный номер носителя	ФИО владельца (Уполномоченное лицо Клиента)	ФИО и подпись получателя

4. Устройства подтверждения:
☐ Генератор одноразовых кодов _____
_____, в кол-ве _____ шт.
☐ MAC-токен BIFIT_____
_____, в кол-ве _____ шт.

№ п/п	Наименование	Учетный номер	ФИО владельца (Уполномоченное лицо Клиента)	ФИО и подпись получателя

Достоверность сведений подтверждаем.
Настоящий Акт составлен в 2-х экземплярах, по одному для каждой из Сторон, и является неотъемлемой частью Договора.

Подписи Сторон

Банк	**Клиент**
_____/_____/	_____/_____/

При получении программного обеспечения, СКЗИ и ключевых носителей не Уполномоченными лицами, дополнительно предоставляется Доверенность на получателя от каждого Уполномоченного лица по форме, установленной АО «АБ «РОССИЯ».

Приложение № 10
Типовая форма Доверенности (на получателя)

Доверенность[8] №

г. _____ «___»_____ 20___ г.

Клиент	
указывается полное наименование организации, включая организационно-правовую форму / ФИО индивидуального предпринимателя / физического лица, занимающегося частной практикой	
в лице	
действующего на основании	
доверяет	
(фамилия, имя, отчество лица, которому выдается доверенность)	
данные документа, удостоверяющего личность:	
Тип документа	Серия, номер	Дата выдачи
Кем выдан	Код подразделения
совершать все юридические действия, связанные с получением и обменом программного обеспечения Клиентской части Системы ДБО, средств криптографической защиты информации (СКЗИ), Токенов (USB-Токен), Устройств подтверждения (в случае необходимости), а также сопутствующей документации, с правом подписания необходимых документов, в том числе акта приема-передачи ключевых носителей, программного обеспечения и средств криптографической защиты информации в	
АО «АБ «РОССИЯ» / наименование филиала АБ «РОССИЯ»)	

Образец подписи	
(подпись)	
	удостоверяю.
(фамилия, имя, отчество лица, которому выдается доверенность)	
Настоящая доверенность действует до	«___» _____ 20 ____ г. включительно.

(наименование должности руководителя)	*(подпись)*	*(фамилия, инициалы)*
МП		

[8] В соответствии с п. 3 ст. 187 Гражданского кодекса Российской Федерации Доверенность, выдаваемая в порядке передоверия, т.е. лицом, действующим на основании доверенности, должна быть нотариально удостоверена.

ЗАЯВЛЕНИЕ О КОМПРОМЕТАЦИИ

Клиент	
указывается наименование организации, включая организационно-правовую форму / ФИО индивидуального предпринимателя / физического лица, занимающегося частной практикой	
в лице	
действующий на основании	
ИНН	

НАСТОЯЩИМ ЗАЯВЛЕНИЕМ КЛИЕНТ

1. Уведомляет о наступлении события, связанного с Компрометацией или подозрением на Компрометацию:

☐	Ключа ЭП, указать идентификатор Ключа проверки ЭП[61] _____
☐	Ключа PayControl
☐	Ключа Серверной ЭП
☐	Ключевого носителя (USB-токена)
☐	Мобильного устройства (при использовании Ключа PayControl)
☐	Пароля
☐	Устройства подтверждения
☐	Иное _____

в отношении **Уполномоченного лица**

ФИО (полностью)	**СНИЛС**	**e-mail и телефон**	_____@_____
_____	_____		**+7** _____

2. Просит заблокировать скомпрометированные Ключ ЭП/Ключ Серверной ЭП/Ключ PayControl/устройство, указанные в п. 1 настоящего Заявления

3. Просит для возобновления работы в Системе ДБО выдать Уполномоченному лицу / принять от Уполномоченного лица (при необходимости):
В случае если у Уполномоченного лица (УЛ) несколько типов полномочий, заявление дополняется дополнительным блоком

Полномочия		**Дополнительно**		**Вариант защиты Системы и подтверждения исполнения документов (нужное отметить)**		
				Способ	**Обязательное подтверждение исполнения платежного документа[62]:**	**Дополнительно для входа в Систему[63]:**
☐	**группа 1**	☐	**выдать USB-токен Банка**			
☐	**группа 2**	☐	**зарегистрировать USB-токен Клиента**	**SMS-сообщение на номер +7** _____	☐	☐
☐	**просмотр**	☐	**выдать Устройство подтверждения[64]**			
☐	**акцепт (визирование)[65]**	☐	**выдать Ключи инициализации PayControl**	**Устройство подтверждения[5]**	☐	☐

Клиент подтверждает достоверность сведений, содержащихся в настоящем Заявлении о компрометации.

ПОДПИСЬ КЛИЕНТА

_____ подпись

_____ дата

МП

ОТМЕТКИ БАНКА

Настоящее Заявление принято _____

Дата

[61] Поле заполняется, если Уполномоченное лицо имеет несколько Ключей ЭП. Данные об идентификаторе Ключа проверки ЭП доступны Клиенту в разделе «Безопасность» / «Запросы на новый сертификат» Системы «ДБО «BS-Client CORREQTS»/ в разделе «Электронные подписи» Системы iBank или на бумажном экземпляре бланка Ключа проверки ЭП в поле «Идентификатор ключа».

[62] При выборе PayControl подтверждение платежа осуществляется в мобильном приложении PayControl.

[63] Не применяется при использовании Мобильного приложения Банка.

[64] Предоставляется при наличии технической возможности.

[65] Предоставляется уполномоченному лицу в случае указания порядка приема электронных платежных документов «с визирующей подписью.

Подпись фамилия, инициалы

ЗАЯВЛЕНИЕ ОБ УСТАНОВЛЕНИИ / СНЯТИИ ОГРАНИЧЕНИЙ
на работу в Системе ДБО Клиента

Клиент	
указывается наименование организации, включая организационно-правовую форму / ФИО индивидуального предпринимателя / физического лица, занимающегося частной практикой	
в лице	
действующий на основании	
ИНН	

НАСТОЯЩИМ ЗАЯВЛЕНИЕМ КЛИЕНТ при осуществлении дистанционного банковского обслуживания **ПРОСИТ установить следующие ограничения в Системе ДБО:**

	Варианты ограничений	**ФИО УЛ**
☐	Разрешить просмотр /подписание платежных поручений к счету (-ам) только указанным УЛ. №_____ №_____ *(указать счет (а))*	**ФИО (полностью)**_____ ☐ **просмотр** ☐ **группа 2** ☐ **группа 1** **ФИО (полностью)**_____ ☐ **просмотр** ☐ **группа 2** ☐ **группа 1** **ФИО (полностью)**_____ ☐ **просмотр** ☐ **группа 2** ☐ **группа 1**
	№_____ №_____ *(указать счет (а))*	**ФИО (полностью)**_____ ☐ **просмотр** ☐ **группа 2** ☐ **группа 1** **ФИО (полностью)**_____ ☐ **просмотр** ☐ **группа 2** ☐ **группа 1** **ФИО (полностью)**_____ ☐ **просмотр** ☐ **группа 2** ☐ **группа 1**
	№_____ №_____ *(указать счет (а))*	**ФИО (полностью)**_____ ☐ **просмотр** ☐ **группа 2** ☐ **группа 1** **ФИО (полностью)**_____ ☐ **просмотр** ☐ **группа 2** ☐ **группа 1** **ФИО (полностью)**_____ ☐ **просмотр** ☐ **группа 2** ☐ **группа 1**
☐	Акцепт (визирование) операций по счету (-ам) №_____ №_____ №_____ №_____ №_____ №_____ *(указать счета)*	**ФИО (полностью)**_____ **ФИО (полностью)**_____ **ФИО (полностью)**_____ **ФИО (полностью)**_____ **ФИО (полностью)**_____
☐	Ограничить максимальную сумму платежа[66] ☐ *на одну операцию (одно платежное поручение)* *и/или* ☐ *на сумму платежей за один Операционный день* _____*(руб.)* *(указать максимальную сумму платежа прописью)*	**ФИО (полностью)**_____ **ФИО (полностью)**_____ **ФИО (полностью)**_____ **ФИО (полностью)**_____ **ФИО (полностью)**_____
☐	Подключить возможность устанавливать в Системе ДБО перечень получателей денежных средств.	
☐	Снять все ранее установленные ограничения	

ПОДПИСЬ КЛИЕНТА

Клиент подтверждает достоверность сведений, содержащихся в настоящем Заявлении об установлении/снятии ограничений.

_____ _____
подпись дата

МП

[66] Ограничения для ДБО iBank устанавливается на Клиента в целом, заполнять поле с указанием ФИО не требуется.

ОТМЕТКИ БАНКА

Настоящее Заявление принято

Дата

подпись

фамилия, инициалы

ПОЛОЖЕНИЕ
о порядке проведения технической экспертизы при возникновении спорных ситуаций
(далее – Положение)

1. При возникновении разногласий Сторон в связи с обменом ЭД посредством Системы ДБО, а также в иных случаях возникновения спорных ситуаций, связанных с эксплуатацией Системы ДБО, обмен ЭД немедленно прекращается.
2. До разрешения спорной ситуации Клиенту рекомендуется не использовать в работе ПК, на который установлено программное обеспечение Системы ДБО.
3. В настоящем Положении под спорной ситуацией понимается возникновение у Сторон претензий, связанных с обменом ЭД посредством Системы ДБО, справедливость которых может быть однозначно установлена по результатам проверки корректности ЭП под оспариваемым ЭД. В рамках настоящего Положения рассматривается проверка корректности УНЭП/ УКЭП/ ПЭП PayControl. Под УНЭП понимается УНЭП, включая Серверную ЭП.
4. Спорные ситуации при эксплуатации Системы ДБО могут возникать в следующих случаях:
– не подтверждения подлинности ЭД средствами проверки ЭП принимающей Стороны;
– оспаривание факта формирования ЭД;
– оспаривание факта идентификации Уполномоченного лица Клиента/Банка, которому предоставлено право подписания от имени Банка направляемых Клиенту электронных документов, подписавшего ЭД;
– заявление Стороны об искажении ЭД;
– оспаривание факта отправления или доставки ЭД;
– оспаривание времени отправления или доставки ЭД;
– подозрение на несанкционированный доступ к Ключу Серверной ЭП;
– в иных случаях, связанных с функционированием Системы ДБО.
5. Клиент представляет Банку заявление по форме Банка либо заявление в свободной форме, подписанное представителем Клиента и заверенное печатью (при наличии) в срок не позднее дня, следующего за днём получения уведомления об исполнении Банком спорного ЭД.
Заявление в свободной форме должно содержать:
– наименование Клиента, включая ИНН;
– подробное изложение обстоятельств и предполагаемых причин возникновения спорной ситуации;
– ФИО представителя Клиента, уполномоченного от имени Клиента вести переговоры по урегулированию спорной ситуации, а также номер его контактного телефона, адрес.
6. До подачи в Банк заявления Клиенту рекомендуется убедиться в целостности своего программного обеспечения, неизменности используемой Ключевой информации, за исключением Серверной ЭП, а также отсутствия несанкционированных действий со стороны персонала Клиента, обслуживающего Клиентское рабочее место (АРМ Клиента).
7. Банк в течение 7 (семи) рабочих дней рассматривает заявление Клиента и либо удовлетворяет претензию Клиента, либо отказывает в её удовлетворении. Уведомление Клиента о принятом Банком решении по заявлению Клиента осуществляется путём направления Клиенту письменного ответа.
8. В случае несогласия с заключением Банка Клиент, не позднее 5 (пяти) рабочих дней с даты получения заключения Банка, направляет в Банк письменное уведомление о своём несогласии (далее – уведомление о несогласии).
9. В целях рассмотрения уведомления о несогласии Банком формируется

Экспертная комиссия, задачей которой является проведение технической экспертизы в порядке, установленном настоящим Положением.

10. Банк в течение 5 (пяти) рабочих дней с даты получения уведомления о несогласии, запрашивает у Клиента список лиц для включения в состав Экспертной комиссии со стороны Клиента, формирует в соответствии с п. 11 настоящего Положения Экспертную комиссию и направляет Клиенту уведомление о дате и месте проведения заседания Экспертной комиссии. Заседание Экспертной комиссии должно быть проведено не позднее 20 (двадцати) рабочих дней после даты получения уведомления о несогласии.

11. Экспертная комиссия состоит из равного числа представителей Сторон, в которую от каждой Стороны включается не более 3 (трёх) человек. Лица, входящие в состав Экспертной комиссии, должны обладать необходимыми знаниями в области обеспечения защиты информации и работы компьютерных информационных систем. По взаимной договорённости Стороны могут включить в состав Экспертной комиссии независимого эксперта. Оплата участия в разборе спорной ситуации независимого эксперта осуществляется Стороной, его пригласившей.

12. Процедура проверки подлинности ЭД проводится на оборудовании и в помещении Банка.

13. К заседанию Экспертной комиссии Клиент предоставляет Экспертной комиссии следующие материалы:

– заявление, предоставленное в соответствии с п. 5 настоящего Приложения;

– бумажную копию оспариваемого ЭД (при наличии);

– заверенные Банком копии заявлений об изменении состава Уполномоченных лиц Клиента, аннулировании действия Ключа ЭП Уполномоченных лиц Клиента по формам, определённым Банком в Правилах (при наличии);

– в случаях использования УКЭП – Сертификат ЭП, выданный Удостоверяющим центром, подтверждающий факт действительности ЭП под оспариваемым ЭД;

– выписку из протокола работы Системы ДБО, подтверждающую приём/отправку спорного ЭД, на бумажном носителе, за согласованный Сторонами период времени.

14. К заседанию Экспертной комиссии Банк предоставляет Экспертной комиссии следующие материалы:

– ЭД, на основании которого Банк совершил оспариваемые Клиентом действия (далее – оспариваемый ЭД), заверенный ЭП Клиента/Банка, в виде файла (или оспариваемый ЭД в виде файла и соответствующие этому документу ЭП в виде отдельных файлов);

– бумажную копию оспариваемого ЭД;

– Ключ проверки ЭП Уполномоченных лиц Клиента/Уполномоченного представителя Банка, с помощью которых проводилась проверка ЭП оспариваемого ЭД;

– распечатки Ключа проверки ЭП (УНЭП)/ Сертификата ЭП Уполномоченных лиц Клиента, распечатку Ключа проверки ЭП(УНЭП) Уполномоченного лица Банка на бумажном носителе;

– оригиналы заявлений об изменении состава Уполномоченных лиц Клиента, аннулировании действия Ключа ЭП Уполномоченных лиц Клиента по формам, определённым Банком в Правилах, данные об аннулировании действия Ключа ЭП Уполномоченного представителя Банка (при наличии);

– выписка из протокола работы Системы ДБО, подтверждающая приём/отправку спорного ЭД, на бумажном носителе, за согласованный Сторонами период времени;

– выписка из протокола работы Сервера подписи, фиксирующая обращения за получением Ключа Серверной ЭП;

– выписка из протокола работы Сервера подписи, фиксирующая аудит доступа к Серверу подписи.

15. Стороны могут передать Экспертной комиссии другие материалы, имеющие отношение к сути рассматриваемой претензии.

16. Стороны обязаны способствовать работе Экспертной комиссии и не допускать

необоснованного отказа от предоставления необходимых документов.

17. В случае непредоставления в установленный срок Экспертной комиссии одной из Сторон каких-либо из вышеперечисленных материалов к рассмотрению принимаются аналогичные материалы, предоставленные другой Стороной.

18. Процедура проверки Экспертной комиссией УНЭП (выпущенной Банком)/ УКЭП (выпущенной согласно внутреннему регламенту работы Удостоверяющего центра) под спорным ЭД включает следующие действия:

– установление времени подписания оспариваемого ЭД Уполномоченными лицами Клиента/Уполномоченным представителем Банка;

– установление времени направления/получения спорного ЭД Банку/Клиенту (Банком/Клиентом);

– сверку даты и времени регистрации, а также срока действия Ключей проверки ЭП Уполномоченных лиц Клиента/Уполномоченного представителя Банка, подписавших спорный ЭД, с датой и временем подписания спорного ЭД;

– сверку соответствия оригиналов Ключей проверки ЭП лиц, подписавших спорный ЭД, с УНЭП/ УКЭП под спорным ЭД;

– сверку даты и времени регистрации в Банке заявлений об изменении списка Уполномоченных лиц Клиента и аннулирования действия Ключа ЭП Уполномоченных лиц Клиента, подписавших спорный ЭД (при наличии), с датой и временем подписания спорного ЭД:

– сверку даты и времени регистрации в Банке заявлений об изменении списка Уполномоченных лиц Клиента и аннулирования действия Ключа ЭП Уполномоченных представителей Банка, подписавших спорный ЭД (при наличии), с датой и временем подписания спорного ЭД;

– проверку действительности полномочий лиц, подписавших ЭД, на дату подписания спорного ЭД, осуществляемую по результатам рассмотрения Документов, подтверждающих их полномочия;

– проверку подлинности и целостности Ключей проверки ЭП Уполномоченных лиц Клиента/Уполномоченного представителя Банка, с помощью которых проверялись УНЭП/ УКЭП Клиента/Банка:

- для УНЭП - файла Ключа проверки ЭП Клиента/Банка, полученного/направленного Клиентом/Банком по Системе ДБО, и Бланка Ключа ЭП Клиента/Банка, содержащего Ключ проверки ЭП, на бумажном носителе или электронного запроса на регистрацию Ключа проверки ЭП, направленного средствами Системы ДБО;
- для УКЭП - файла Сертификата ЭП с расширением *.cer в формате X509, направленного Клиентом в Банк;

– при необходимости подтверждения действительности УКЭП Экспертная комиссия направляет запрос в Удостоверяющий центр о подтверждении действительности УКЭП на дату подписания оспариваемого ЭД;

- проверку, с помощью эталонного программного обеспечения, УНЭП/ УКЭП под спорным ЭД. Подтверждением корректности УНЭП/ УКЭП под оспариваемым ЭД является одновременное выполнение следующих условий:
- Ключи проверки ЭП Уполномоченных лиц Клиента/Уполномоченного представителя Банка, с помощью которых проверялись УНЭП/ УКЭП, в момент поступления ЭД в Банк/Клиенту и его проверки являлись действующими, т.е. были зарегистрированы в установленном Банком или внутренним регламентом работы Удостоверяющего центра порядке, сроки их действия не истекли и они не были отменены;
- подтверждена подлинность и целостность Ключей проверки ЭП Уполномоченных лиц Клиента/Уполномоченного представителя Банка, с помощью которых проводилась проверка УНЭП/ УКЭП;
- проверка УНЭП/ УКЭП под спорным ЭД с использованием Ключей проверки ЭП Уполномоченных лиц Клиента/Уполномоченного представителя Банка дала

положительный результат, то есть подтвердила подлинность УНЭП/ УКЭП под спорным ЭД;

- действия Банка по обработке ЭД проведены в соответствии с информацией, содержащейся в ЭД.

– дополнительно процедура проверки Экспертной комиссией Серверной ЭП включает следующие действия:

- подтверждена подлинность собственноручной подписи руководителя и (или) Представителя Клиента на Бланке Ключа ЭП на бумажном носителе (при его наличии);
- признание или не признание Клиентом принадлежности ему Бланка Ключа ЭП на Серверную ЭП;
- проверка наличия доверенности от УЛ и Клиента на хранение и использование Банком Ключа Серверной ЭП УЛ Клиента. Доверенность оформляется и предоставляется Клиентом в Банк вместе с Бланком Ключа ЭП;
- Процедура проверки Экспертной комиссией ПЭП PayControl под спорным ЭД включает следующие действия:
- загрузку в специализированное программное обеспечение разработчика средства PayControl – АРМ РКС- файла спорного ЭД;
- загрузку в АРМ РКС файла со значением ЭП спорного ЭД;
- проверку ЭП выгруженного файла спорного ЭД с использованием значения Ключа проверки ЭП;
- печать протокола работы АРМ РКС.

19. Подтверждением корректности ПЭП PayControl под оспариваемым ЭД является следующее. В случае если:

– проверяемая ЭП для данного спорного ЭД верна;

– Ключ проверки ЭП, отобранный для разбора конфликтной ситуации, соответствует значению ключа, направленному в Банк при выполнении процедуры выработки Ключей ЭП на основе средства PayControl для его регистрации в Системе ДБО,

считается установленным:

– что проверяемый спорный ЭД был сформирован в соответствии с настоящими Правилами;

– проверяемый спорный ЭД был подписан Ключом ЭП, соответствующим зарегистрированному Банком Ключу проверки ЭП, использованному при проведении технической экспертизы;

– владельцем Ключа ЭП и Ключа проверки ЭП является представитель Клиента, зарегистрированный Банком.

20. В случае выполнения всех условий, перечисленных в пп. 18 или 19 настоящего Положения, Стороны соглашаются с тем, что корректность УНЭП/ УКЭП/ ПЭП PayControl под оспариваемым ЭД подтверждена, то есть проверяемый ЭД подписан корректными УНЭП/ УКЭП/ ПЭП PayControl.

21. В случае невыполнения любого из условий, перечисленных в п.п. 18 или 19 настоящего Положения, Стороны соглашаются с тем, что корректность УНЭП/УКЭП/ ПЭП PayControl не подтверждена, то есть проверяемый ЭД подписан некорректными УНЭП/ УКЭП/ ПЭП PayControl.

22. В том случае, если Банк принял к исполнению ЭД, подписанный УНЭП/ УКЭП/ ПЭП PayControl Уполномоченных лиц Клиента, корректность которых установлена Экспертной комиссией, Стороны соглашаются с тем, что претензии Клиента к Банку, связанные с последствиями исполнения указанного документа, являются необоснованными.

23. В том случае, если Банк принял к исполнению ЭД, подписанный УНЭП/ УКЭП/ ПЭП PayControl Уполномоченных лиц Клиента, корректность которых не подтверждена Экспертной комиссией, претензии Клиента к Банку, связанные с последствиями исполнения указанного документа, признаются обоснованными.

24. По итогам работы Экспертной комиссии составляется Акт о результатах проведения технической экспертизы, в котором фиксируются выводы Экспертной комиссии в

результате проведённых мероприятий, в 2 (двух) экземплярах, по одному экземпляру для каждой Стороны. Акт о результатах проведения технической экспертизы должен содержать следующую информацию:

- состав Экспертной комиссии;
- дата и место составления Акта;
- дата и время начала и окончания работы Экспертной комиссии;
- суть претензии;
- перечень мероприятий, проведённых Экспертной комиссией;
- фактические обстоятельства, установленные Экспертной комиссией;
- выводы, к которым пришла Экспертная комиссия в результате проведённых мероприятий;
- подписи членов Экспертной комиссии на каждом листе Акта.

25. Акт подписывается всеми членами Экспертной комиссии и является основанием для принятия Сторонами окончательного решения об урегулировании спорной ситуации.

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

27. Максимальный срок работы Экспертной комиссии составляет не более 30 (тридцати) календарных дней с даты её формирования, включая дату предоставления Акта.

В случае несогласия одной из Сторон с выводами Экспертной комиссии, отражёнными в Акте о результатах проведения технической экспертизы, уклонения от формирования Экспертной комиссии либо участия в её работе, препятствования участию второй Стороны в работе Экспертной комиссии, вторая Сторона вправе передать спор на рассмотрение в Арбитражный суд по месту нахождения Банка или его филиала/представительства.