



АКЦИОНЕРНЫЙ БАНК РОССИЯ

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

действует с «26» мая 2022г.

1. Термины, определения и сокращения

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 8 настоящих Правил.

Аутентификационные данные – совокупность Логина и Пароля при доступе к каналу доступа «Клиент-Банк Онлайн» / «Клиент-Банк», а также Ключ ЭП / Ключ PayControl при доступе к каналу доступа «Клиент-Банк Онлайн», а также Пароль, PIN-код/ отпечаток пальца или изображение лица (TouchID/ FaceID), 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 в Системе ДБО, позволяющая его идентифицировать.

Банк - АО «АБ «РОССИЯ».

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) – ЭД или документ на бумажном носителе, подтверждающий принадлежность Ключа проверки ЭП Уполномоченному лицу по форме Приложения №№ 19/ 20 к настоящим Правилам.

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 Счете(-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 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 действующего законодательства Российской Федерации и нормативных актов Банка России, электронных документов произвольного формата, а также предоставления Банком информации о Счёте Клиента (при его наличии) и иных сведений и документов.

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

Договор ДБО - договор, определяющий порядок предоставления услуг дистанционного банковского обслуживания с использованием Системы ДБО, заключённый в соответствии со ст. 428 Гражданского кодекса Российской Федерации, который представляет собой совокупность Правил дистанционного банковского обслуживания корпоративных клиентов АО «АБ «РОССИЯ» (далее – Правила) и Заявления о присоединении, размещённые на официальном сайте Банка в сети Интернет www.abr.ru.

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, 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.

Канал «Клиент-Банк» – канал отправки ЭД в Банк Системы ДБО, требующий локальной установки специализированного программного обеспечения на рабочее место Клиента. Для подписания ЭД Клиента используется УНЭП. Обслуживание канала осуществляется в Системе «iBank» и Системе «ДБО BS-Client».¹

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 отправки ЭД в Банк Системы ДБО, предоставляющий возможность обмена ЭД с Банком с использованием УНЭП и УКЭП напрямую из Учётной системы Клиента:

- посредством интеграции с системой 1С с применением сервиса «Обмен с 1С по DirectBank»/ «DirectBank+» в Системе «ДБО BS-Client (CORREQTS)» и в Системе «iBank»;
- 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 Учётной системы Клиента с банковским сервером Системы «iBank»;

¹ Банк не осуществляет подключение новых Клиентов к Каналу «Клиент-Банк».

- посредством интеграции с модулем «Интеграционный корпоративный шлюз» Системы «ДБО BS-Client (CORREQTS)» в соответствии с форматами, определёнными пользовательской документацией, предоставляемой Банком Клиенту.

Порядок использования Канала «Интеграционный Клиент-Банк» определён Приложением № 15 к настоящим Правилам.

Клиент - юридическое лицо, иностранная структура без образования юридического лица, индивидуальный предприниматель, физическое лицо, занимающееся в установленном законодательством Российской Федерации порядке частной практикой, присоединившееся к настоящим Правилам.

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 и предназначенная для проверки подлинности УНЭП/ УКЭП.

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

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

Ключевой носитель – носитель информации, содержащий Ключи ЭП, либо предназначенный для записи, хранения, воспроизведения Ключей ЭП.

Код подтверждения – набор символов или сообщение, поступившие в Систему ДБО, используемые для подтверждения доступа к Системе ДБО в целях дополнительной 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 Банком²,
- 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:

²Услуга генерации Кода подтверждения с помощью Устройства подтверждения не предоставляется при использовании Мобильного приложения Банка и Канала «Интеграционный Клиент-Банк».

- 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 Уполномоченного лица, в том числе, с последующим обнаружением;
- 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 № 4 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 Банка³ - 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

³ Возможность обмена электронными документами между Клиентом и Банком, в том числе создание, подписание ЭП и отправка ЭД в Банк на исполнение, доступна клиентам – субъектам микро- и малого предпринимательства.

доступ в сеть Интернет, установлено и активировано Мобильного приложения PayControl и/или Мобильное приложение Банка.

Модуль «Центр финансового контроля/ Расчётный центр Корпорации» (далее –модуль ЦФК/РЦК)⁴ – 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 (бюджетирования), управления счетами. Порядок использования модуля ЦФК/РЦК определён Приложением № 13 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 о присоединении / Заявлении об изменении данных и используемый Клиентом для получения от Банка SMS-сообщений/ PUSH-сообщений.

Операционный день - операционно-учетный цикл за соответствующую календарную дату, в течение которого все совершенные 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 используемая для Аутентификации Уполномоченного лица Клиента в Системе ДБО.

Порядок переводов - Порядок осуществления переводов денежных средств в валюте Российской Федерации Клиентов – юридических лиц, иностранных структур без образования юридического лица, индивидуальных предпринимателей и физических лиц, занимающихся в установленном законодательством Российской Федерации порядке частной практикой, в АО «АБ «РОССИЯ», размещённый на официальном сайте Банка в сети Интернет www.abr.ru.

Простая электронная подпись (ПЭП PayControl) – 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.

Распоряжение на перевод (Распоряжение) – платёжное поручение или иной расчётный (платёжный) документ, форма которого определена Положением Банка России от 29.06.2021 № 762-П «О правилах осуществления перевода денежных

⁴ Услуга предоставляется при условии подключения модуля ЦФК/РЦК по заявлению по форме Приложения № 17 к настоящим Правилам.

средств» 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.

Полномочия уполномоченного лица - 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 о присоединении/ Заявлении об изменении данных.

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 № 1 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 ДБО (Система) - 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 совокупность каналов дистанционного банковского обслуживания «Клиент-Банк Онлайн», «Интеграционный Клиент-Банк», «Клиент-Банк».

Средства криптографической защиты информации (СКЗИ) - шифровальные (криптографические) средства защиты информации конфиденциального характера – аппаратные и (или) программные средства, обеспечивающие создание и проверку УНЭП/УКЭП, создание Ключей ЭП, 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 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 по Договору 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, утверждённая в соответствии с действующим в Банке порядком и действующая на дату оказания услуги в ГО/ ВСП Банка по месту обращения Клиента.

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) - единоличный исполнительный орган юридического лица, лицо, действующее от имени и в интересах или за счёт Клиента, полномочия которого основаны на доверенности, договоре, распорядительном акте Клиента, уполномоченного государственного органа или органа местного самоуправления, законе, уполномоченный на работу в Системе ДБО в рамках, установленных для данного УЛ полномочий.

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) - усиленная квалифицированная электронная подпись, Сертификат ключа проверки 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 Уполномоченному лицу Банком и удовлетворяет требованиям настоящих Правил.

Устройство подтверждения - аппаратно-техническое устройство, отвечающее требованиям Положения Банка России от 04.06.2020 № 719-п, выдаваемое Клиенту и предназначенное при использовании Канала доступа «Клиент-Банк Онлайн» для дополнительной Аутентификации Клиента при подтверждении доступа к Системе ДБО и/или для подтверждения ЭПД Клиента. Перечень разрешённых к использованию устройств устанавливается Банком.

Учётная система Клиента - программное обеспечение Клиента, принадлежащее Клиенту и используемое Клиентом для автоматизации бухгалтерского и управленческого учёта, подготовки бухгалтерских документов и финансовой отчётности. При работе с Банком с использованием Канала доступа «Интеграционный Клиент-Банк» должна соответствовать требованиям Приложения № 4 к настоящим Правилам (Обязательства Клиента по выполнению правил безопасной работы при использовании клиентской части Системы ДБО).

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 № 15 к настоящим Правилам.

Электронная подпись (ЭП) – информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется

для определения лица, подписывающего информацию и целостности подписываемой информации. Для целей настоящих Правил в качестве ЭП Уполномоченного лица выступает УНЭП, 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, подписываемый ЭП Стороны и не являющийся ЭПД (Выписки по счету, 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.

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 нем 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.

1.1. **Формы документов и их сокращения, используемые по тексту Правил.**

Акт возврата СКЗИ – Акт возврата средств криптографической защиты информации (Приложение № 12 к настоящим Правилам).

Акт выполненных работ – Акт выполненных работ (Приложение № 10 к настоящим Правилам).

Акт приёма – передачи – Акт приёма – передачи ключевых носителей, программного обеспечения и средств криптографической защиты информации (для Клиентов) (Приложение № 6 к настоящим Правилам).

Доверенность – Типовая форма Доверенности (на получателя) (Приложение № 9 к настоящим Правилам).

Заявление на выезд специалиста – Заявление на выезд специалиста Банка на территорию Клиента (Приложение № 7 к настоящим Правилам).

Заявление о компрометации – Заявление о компрометации (Приложение № 15 к настоящим Правилам).

Заявление о предоставлении модуля ЦФК/РЦК – Заявление о предоставлении модуля ЦФК/РЦК Системы ДБО Контролирующей организации (Приложение № 14 к настоящим Правилам).

Заявление о присоединении – заявление Клиента, содержащее волеизъявление Клиента на заключение договора в форме присоединения к Правилам дистанционного банковского обслуживания корпоративных клиентов АО «АБ «РОССИЯ» в соответствии со ст. 428 ГК РФ, размещённое на официальном сайте Банка www.abr.ru.

Заявление об изменении данных – Заявление об изменении данных по форме, установленной Банком и размещённой на сайте Банка по адресу: www.abr.ru.

Заявления об установлении / снятии ограничений – Заявление об установлении / снятии ограничений на работу в Системе ДБО (Приложение № 16 к настоящим Правилам).

Заявление о предоставлении третьим лицам выписки по счетам – Заявление о предоставлении третьим лицам выписки по счетам Клиента (подключение/отключение) (Приложение № 17 к настоящим Правилам)

Заявление о расторжении договора - Заявление о расторжении Договора ДБО (Приложение № 11 к настоящим Правилам).

Инструкция по установке системы - Инструкция по установке Системы «iBank» (Приложение № 5 к настоящим Правилам), «ДБО BS-Client (CORREQTS)» (Приложение № 5а к настоящим Правилам).

Обязательства Клиента по безопасной работе - Обязательства Клиента по выполнению правил безопасной работы при использовании Клиентской части Системы ДБО (Приложение № 4 к настоящим Правилам).

Перечень электронных документов - Перечень электронных документов, используемых в Системе ДБО (Приложение № 12 к настоящим Правилам).

Положение о технической экспертизе - Положение о порядке проведения технической экспертизы при возникновении спорных ситуаций (Приложение № 3 к настоящим Правилам).

Порядок электронного документооборота - Порядок электронного документооборота с использованием Системы ДБО (Приложение № 2 к настоящим Правилам).

Условия предоставления модуля ЦФК/РЦК - Условия предоставления модуля «Центр финансового контроля / Расчётный центр корпорации» в АО «АБ «РОССИЯ» (Приложение № 13 к настоящим Правилам).

2. Общие положения

- 2.1. Настоящие Правила определяют положения Договора ДБО, заключаемого между Банком и Клиентом в соответствии с п. 1 ст. 428 Гражданского кодекса Российской Федерации.
- 2.2. Заключение Договора ДБО осуществляется путём присоединения Клиента к настоящим Правилам на основании Заявления о присоединении, надлежащим образом заполненного и подписанного Клиентом 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 Заявление о присоединении не принимается Банком к исполнению.⁵
- 2.3. 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.
- 2.4. Информирование Клиента о реквизитах заключённого Договора ДБО осуществляется Банком посредством направления уведомления по Системе ДБО.
- 2.5. При исполнении Договора ДБО Стороны руководствуются нормами законодательства Российской Федерации, нормативными актами Банка России,

⁵ Повторное представление документов, предоставленных Клиентом ранее не требуется. Предоставляемые Клиентом документы должны быть актуальны на дату их предоставления.

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.

- 2.6. Настоящие Правила определяют порядок и условия:
 - предоставления и обслуживания Системы ДБО;
 - управления Сервисами Системы ДБО;
 - обмена электронными документами в Системе ДБО.
- 2.7. Дистанционное банковское обслуживание может предоставляться Клиентам с подключением или без подключения Счетов к Системе ДБО.
- 2.8. 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.
- 2.9. Состав предоставляемых Банком Сервисов Системы ДБО определяется Приложением № 1 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.
- 2.10. 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 клиента по безопасной работе.
- 2.11. 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 Счету (ам) в соответствии с п. 2.8 Приложения № 1 к настоящим Правилам, Клиент принимает на себя.
- 2.12. Стороны подтверждают и соглашаются с тем, что:
 - 2.12.1. Полномочия каждого УЛ в Системе ДБО определяются в Заявлении о присоединении, заполняемом Клиентом при первоначальной регистрации или в Заявлении об изменении данных.

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 «Заключение сделок (депозиты)/ Заключение сделок (НСО)» УЛ предоставляется право на размещение средств в неснижаемые остатки, депозиты, в том числе подготовку, подписание, отправку ЭД в Банк и получение ЭД из Банка при условии наличия у Клиента заключённого договора на размещение средств в депозиты, неснижаемые остатки.

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, подготовку ЭД, отправку подписанных ЭД в Банк и получение ЭД из Банка.

Изменение полномочий Уполномоченного лица осуществляется путём предоставления в Банк Заявления об изменении данных.

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.
- 2.12.2. Применяемые механизмы защиты Системы ДБО в соответствии с настоящими Правилами достаточны для обеспечения конфиденциальности, авторства и целостности ЭД, а также невозможности их фальсификации без нарушения настоящих Правил.
- 2.12.3. Получение Клиентом запросов Банка по Системе ДБО, предоставление Клиентом Банку по Системе ДБО запрошенных документов, а также направление по Системе ДБО ЭД, указанных в Приложении № 12 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.
- 2.12.4. В качестве единой шкалы времени при работе в Системе ДБО принято московское время. Контрольным временем приёма / отправки ЭД является время системных часов сервера Банка.
- 2.12.5. 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.
- 2.12.6. Любые ЭД, передаваемые Клиентом по Системе ДБО, должны быть подписаны ЭП Клиента. Подписание ЭД может осуществляться:
- Усиленной неквалифицированной ЭП;
 - Усиленной квалифицированной ЭП;
 - Простой ЭП в Системе «ДБО «BS-Client (CORREQTS)» (ПЭП PayControl) и позволяет определить Уполномоченное лицо, подписавшее ЭД.
- 2.12.7. ЭД, не подписанные ЭП в соответствии с настоящими правилами, в обработку Банком не принимаются и не являются основанием для предоставления услуг по договору.
- 2.12.8. Если после подписания ЭП ЭД был изменён, то ЭП данного документа становится некорректной, т.е. проверка ЭП даёт отрицательный результат.
- 2.12.9. 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.
- 2.13. В случае принятия Клиентом решения применять в Системе ДБО УКЭП (Ключ ЭП, выпущенный сторонним Удостоверяющим центром), актуализация информации Удостоверяющего центра об отозванных Ключах ЭП обеспечивается Банком не реже, чем 1 (один) раз в сутки.
- 2.14. Подтверждение ЭПД в Системе ДБО Уполномоченное лицо осуществляет в соответствии с Порядком электронного документооборота (Приложение № 2 к настоящим Правилам) 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.
- 2.15. ЭПД, оформленные в соответствии с нормативными актами Банка России, Порядком переводов исполняются Банком в соответствии с Порядком электронного документооборота и действующим/ими договором/ми банковского счёта.
- 2.16. Замена Ключей ЭП с соблюдением требований настоящих Правил не влияет на

юридическую силу ЭД, если он был подписан рабочим на момент подписания ключом.

- 2.17. 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 от 27.07.2006 № 152-ФЗ «О персональных данных» (далее - Федеральный закон № 152-ФЗ). Клиент несёт все неблагоприятные последствия, связанные с неполучением указанных согласий.

Обработка персональных данных осуществляется Акционерным обществом «Акционерный Банк «РОССИЯ», зарегистрированным по адресу: 191124, г. Санкт-Петербург, пл. Растрелли, д. 2, лит. А, с целью исполнения настоящего Договора 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, в случаях, установленных действующим законодательством Российской Федерации.

Настоящее подтверждение действует с даты заключения Договора ДБО и по истечении 5 (пяти) лет после прекращения действия Договора ДБО. Согласие 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.

Банк обязуется соблюдать принципы и правила обработки персональных данных, предусмотренные Федеральным законом № 152-ФЗ, обеспечивать конфиденциальность и безопасность персональных данных при их обработке, а именно: принимать необходимые и достаточные правовые, организационные и технические меры для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления персональных данных и от иных неправомерных действий в отношении персональных данных, а также соблюдать все требования к защите персональных данных, установленные Федеральным законом № 152-ФЗ и принятыми в соответствии с ним нормативными правовыми актами.

3. Порядок подключения к Системе ДБО

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

- Заявления о присоединении;
- Документов, подтверждающих личность и полномочия на каждое УЛ, либо сведений о реквизитах документов, подтверждающих личность и полномочия УЛ Клиента, установленных действующим законодательством Российской Федерации и требованиями Банка России.

По истечении срока полномочий УЛ для продления полномочий Клиент предоставляет новые Документы, подтверждающие полномочия. По истечении срока действия полномочий УЛ и при не предоставлении новых документов Банк приостанавливает полномочия УЛ. Документы, подтверждающие полномочия, для УЛ, не имеющего права подписи ЭД в Системе ДБО, не предоставляются.

- 3.2. В Заявлении о присоединении Клиент определяет параметры подключения:

- 3.2.1. Систему ДБО. В процессе работы возможна одновременная эксплуатация нескольких Систем ДБО, а также изменение эксплуатируемой Системы ДБО.
- 3.2.2. Уполномоченных лиц и предоставляемые им полномочия в Системе ДБО в

соответствии с пп. 2.12.1 настоящих Правил.

- 3.2.3. Количество ЭП, используемых Клиентом для подписания передаваемых Банку ЭПД, в том числе использование Уполномоченными лицами УНЭП/УКЭП/ПЭП PayControl.
- 3.3. После проверки Банком полноты и корректности указанных в пп. 3.1 настоящих Правил документов:
- при подключении Системы «ДБО BS-Client (CORREQTS)» Банк регистрирует Клиента в Системе ДБО и направляет Аутентификационные данные УЛ: Логин - на электронную почту (e-mail) Уполномоченного лица Клиента, Пароль для первоначального входа - на Номер телефона Уполномоченного лица Клиента, сведения о которых указаны в Заявлении о присоединении.⁶
 - при подключении Системы «iBank» Клиент самостоятельно осуществляет предварительную регистрацию в Системе «iBank».
 - 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 пп. 5.1.5 настоящих Правил.
- 3.4. Подключение к Системе ДБО производится Клиентом самостоятельно или с привлечением работника Банка по Заявлению на выезд специалиста.
- 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.
- 3.6. Перед подключением Мобильного приложения Банка Клиент обеспечивает работу Мобильного устройства в режиме, определённом Обязательствами безопасной работы (Приложение № 4 к настоящим Правилам).
- 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 в авторизованном магазине приложений AppStore для iOS и на сайте Банка по адресу www.abr.ru для Android в соответствии с Инструкцией по установке системы (Приложение № 5а к настоящим Правилам).
- 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 в Системе «ДБО BS-Client (CORREQTS)» и Мобильном приложении Банка.
- 4.2. Клиент и Банк признают ПЭП PayControl простой электронной подписью,

⁶ Допускается передача Логина, Пароля в непрозрачном конверте по запросу Клиента.

- равнозначной собственноручной подписи Клиента.
- 4.3. Стороны признают применение ПЭП PayControl в Системе ДБО достаточным для обеспечения авторства и целостности передаваемой между Сторонами информации и невозможности её фальсификации после подписания.
 - 4.4. Порядок подписания ЭД ПЭП PayControl определен пп. 13.1.7 Приложения № 2 к настоящим Правилам.
 - 4.5. Обязательным условием 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 (Приложение № 5а к настоящим Правилам), 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 Банка⁷. 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 безопасной работы (Приложение № 4 к настоящим Правилам).
 - 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. Для формирования и проверки Ключей ЭП в Системе ДБО применяется СКЗИ. 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.

⁷ Количество Ключей PayControl (ПЭП (PayControl)) соответствует количеству Мобильных устройств, с которых Уполномоченное лицо планирует работать в Мобильном приложении Банка с возможностью подписания ЭД.

- 5.1.2. При работе в Системе ДБО используется Ключевой носитель USB-токен, который предоставляется Банком.
- 5.1.3. Для получения Ключевого носителя Клиент предоставляет в Банк надлежащим образом оформленное и подписанное Заявление о присоединении / Заявление об изменении данных.
- 5.1.4. На основании Заявления о присоединении / Заявления об изменении данных Банк формирует для Уполномоченного лица конверт с Ключевым носителем, который передаёт Уполномоченному лицу или лицу, уполномоченному Клиентом на основании Доверенности (Приложение № 8 к настоящим Правилам).
- 5.1.5. Уполномоченное лицо или лицо, уполномоченное на основании Доверенности (Приложение № 8 к настоящим Правилам), подписывает 2 (два) экземпляра Акта приёма-передачи (Приложение № 6 к настоящим Правилам). Один экземпляр Акта приёма-передачи после подписания Сторонами передаётся Клиенту.
- 5.1.6. Генерацию своих ключей Клиент осуществляет самостоятельно.
- 5.1.7. Уполномоченное лицо, используя Логин и Пароль, полученный в соответствии с п. 3.3 настоящих Правил, авторизуется в Системе ДБО и формирует свой Ключ ЭП на предоставленный Банком Ключевой носитель в соответствии с Инструкцией по установке системы (Приложения №№ 5/ 5а к настоящим Правилам). В процессе генерации Ключа ЭП формируется электронный запрос на регистрацию Ключа проверки ЭП (далее - ЗРКП ЭП), который средствами Системы ДБО направляется в Банк.
- 5.1.8. Банк регистрирует Ключ проверки ЭП в Системе ДБО и ограничивает возможность работы с Ключом сроком действия предоставленных Уполномоченному лицу полномочий на основании ЗРКП ЭП и Бланка ключа ЭП, который необходимо предоставить в Банк в 2 (двух) экземплярах на бумажном носителе. Бланк ключа ЭП подписывается Уполномоченным лицом, представителем Клиента, заверяется оттиском печати Клиента (при наличии).
- 5.1.9. По факту регистрации Ключа проверки ЭП (активации Ключа ЭП) Система ДБО автоматически уведомляет УЛ о подключении к Системе ДБО посредством:
- направления уведомления на адрес электронной почты, зарегистрированной в Банке на основании Заявления о присоединении;
 - 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)»/ «Электронная подпись» интерфейса Системы iBank.
- 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 на электронный адрес службы технической поддержки Системы ДБО certdbo@abr.ru.
- 5.2.2. Банк на основании Заявления о присоединении / Заявления об изменении данных и Сертификата ЭП, полученного в соответствии с пп. 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. Смена Ключей ЭП (УНЭП, УКЭП, PayControl) в Системе ДБО

- 6.1. Смена (регенерация) Ключей ЭП производится Уполномоченным лицом самостоятельно.

- 6.2. Плановая смена Ключей ЭП осуществляется в связи с истечением Срока их действия.
- 6.3. При использовании в Системе ДБО УНЭП, ПЭП PayControl Клиент обязан инициировать сеанс связи с Банком не реже 2 (двух) раз в месяц для своевременного получения уведомлений об истечении Срока действия Ключей ЭП. Банк оповещает Уполномоченное лицо о необходимости смены Ключей ЭП за 30 (тридцать) календарных дней до окончания Срока действия Ключей ЭП.
- 6.4. В целях плановой смены Ключей ЭП (УНЭП), Ключей PayControl Клиент не позднее чем за 5 (пять) рабочих дней до даты фактического истечения Срока действия Ключа ЭП в Системе ДБО производит действия, направленные на смену Ключей ЭП.
- 6.5. Плановая смена Ключа ЭП (УНЭП) осуществляется на основании электронного запроса на регенерацию сертификата ключа ЭП, сформированного УЛ в Системе ДБО. По факту обработки запроса Банком активный Бланк ключа ЭП будет доступен Клиенту в меню «Настройки/ Безопасность/ Сертификаты» интерфейса системы «ДБО BS-Client (CORREQTS)» / «Электронная подпись» интерфейса системы iBank. После получения Бланка Ключа ЭП новый Ключ ЭП становится рабочим, и УЛ далее осуществляет работу в Системе ДБО с новым Ключом ЭП.
- 6.6. Плановая смена Ключей PayControl осуществляется на основании электронного запроса на продление Ключа PayControl, сформированного УЛ в Системе ДБО. После обработки запроса Банком необходимо осуществить активацию Ключа PayControl в Мобильном приложении PayControl в соответствии с п.п. 4.7 - 4.8 настоящих Правил, после чего новый Ключ PayControl становится рабочим.
- 6.7. При использовании в Системе ДБО УКЭП Клиент самостоятельно осуществляет контроль срока действия Сертификатов ЭП, выпущенных Удостоверяющим центром, и регистрацию нового Ключа ЭП (УКЭП) в порядке, определённом п. 5.2 настоящих Правил.
- 6.8. Если Клиент не произвёл своевременно плановую смену Ключей ЭП (УНЭП, УКЭП), Ключей PayControl, Система ДБО блокирует их доступ с даты окончания срока действия рабочих Ключей ЭП/ Ключей PayControl (осуществляется автоматическая блокировка просроченных Ключей ЭП/ Ключей PayControl Клиента, т.е. документы, подписанные с использованием Ключей ЭП/ Ключей PayControl, срок действия которых истёк, Банком не принимаются).
- 6.9. Возобновление обслуживания Клиента после автоматической блокировки просроченных Ключей ЭП (УНЭП, УКЭП) осуществляется после регистрации Банком новых Ключей ЭП в порядке, определённом п.п. 5.1, 5.2 настоящих Правил.
- 6.10. Возобновление обслуживания Клиента после автоматической блокировки просроченных Ключей PayControl осуществляется после повторной активации Мобильного приложения PayControl в соответствии с п.п. 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 пп. 16.3.2.1 настоящих Правил;
 - либо направив сообщение на электронный адрес службы технической поддержки Системы ДБО 3356525@abr.ru. Текст сообщения должен содержать наименование Клиента, ФИО и должность Уполномоченного лица Клиента, которому необходимо предоставление новых Ключей инициализации PayControl.
- 6.10.1. По факту получения сообщения на электронный адрес службы технической поддержки Системы ДБО Банк осуществляет / обеспечивает:
 - совершение телефонного звонка Клиенту на номер телефона подтверждения экстренной блокировки Ключей ЭП в целях получения подтверждения необходимости направления новых Ключей инициализации PayControl Уполномоченному лицу Клиента. Информация о номере телефона подтверждения экстренной блокировки Ключей ЭП указывается Клиентом в Заявлении о присоединении. 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, определенном пп. 16.3.2.1 настоящих Правил;

- направление Ключей инициализации PayControl Уполномоченному лицу Клиента;
- отказ в отправке новых Ключей инициализации PayControl в случае, если по факту телефонного звонка Клиенту подтверждение необходимости направления новых Ключей инициализации PayControl не получено.

6.11. При возникновении причин, требующих внеплановой смены Ключа ЭП/ Ключа PayControl, Клиенту необходимо зарегистрировать новые Ключи ЭП/ Ключи PayControl:

- 6.11.1. По причинам, не связанным с истечением Срока действия Ключей ЭП⁸ (при наличии рабочих Ключей ЭП/ Ключей PayControl) - в порядке, предусмотренном п.п. 6.5 - 6.7 настоящих Правил;
- 6.11.2. В случае Компроматации/ подозрения на Компроматацию - в порядке, предусмотренном п.п. 5.1, 5.2, 6.10 настоящих Правил.

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

7. Порядок временного приостановления и возобновления обслуживания клиента в Системе ДБО по инициативе Клиента

7.1. Для временного приостановления обслуживания по Системе ДБО Клиент оформляет Заявление об изменении данных и передает его в Банк в порядке, определенном пп. 16.3.2.1 настоящих Правил.

Банк не позднее рабочего дня, следующего за днём получения Заявления об изменении данных от Клиента или с даты, указанной в Заявлении об изменении данных, приостанавливает доступ Клиента к Системе ДБО, при этом сохраняется возможность отправки ЭСИД «Письмо».

7.2. Для возобновления обслуживания в Системе ДБО (после временного приостановления доступа по собственной инициативе) Клиент оформляет Заявление об изменении данных и передает его в Банк в порядке, определенном пп. 16.3.2.1 настоящих Правил. Возобновление обслуживания производится не позднее рабочего дня, следующего за днём приёма Банком заявления Клиента.

8. Предоставление режима работы «Акцепт (визирование)»

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

⁸ К причинам, связанным со сменой Ключей ЭП, включая, но не ограничиваясь, относятся следующие случаи:

- смена программного обеспечения Банка (в случае необходимости и при наличии соответствующего уведомления от Банка);
- изменение полномочий Уполномоченных лиц Клиента в Системе ДБО с предоставлением документов (сведений), установленных действующим законодательством Российской Федерации и требованиями Банка России и Заявления об изменении данных;
- внесение изменений в ранее предоставленные в Банк сведения, в том числе:
 - изменение личных данных Уполномоченных лиц Клиента, в том числе ФИО, паспортных данных,
 - смена наименования или организационно-правовой формы Клиента / юридического лица, выполняющего функции единоличного исполнительного органа Клиента (далее – ЕИО).

- 8.2. Режим работы «Акцепт (визирование)» предоставляется Банком только для счетов в рублях Российской Федерации.
- 8.3. С целью установления режима работы «Акцепт (визирование)» Клиент в Заявлении о присоединении/ 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.
- 8.4. Предоставление права Визирующей подписи Уполномоченным лицам для работы в режиме «Акцепт (визирование)» осуществляется на основании Заявления о присоединении/ Заявления об изменении данных Клиента посредством выбора полномочий «акцепт (визирование)» с предоставлением Документов, подтверждающих полномочия.
- 8.5. Стороны договорились, что подача Заявления о присоединении/ 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.
- 8.6. Ограничение перечня Контролируемых счетов (при наличии необходимости) осуществляется на основании Заявления об установлении / снятии ограничений, поданного Клиентом.
- 8.7. 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.
- 8.8. В рамках работы в режиме «Акцепт (визирование)» Клиент поручает Банку:
 - 8.8.1. Предоставить Уполномоченным лицам, имеющим на основании Заявления о присоединении/ Заявления об изменении данных полномочия «акцепт (визирование)», возможность проставления Визирующей подписи под ЭПД на проведение расходных операций.
 - 8.8.2. 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 порядке, установленном настоящим Договором.
- 8.9. В случае наличия у Клиента Визирующей подписи Банк не несёт ответственности за неисполнение распоряжений Клиента, не содержащих Визирующую подпись.

9. Права и обязанности клиента

9.1. Клиент имеет право:

- 9.1.1. Использовать Систему ДБО для обмена электронными документами с использованием Системы ДБО.
- 9.1.2. Выбрать вид ЭП для подписания ЭД в Системе ДБО⁹.
- 9.1.3. Направлять в Банк посредством Системы ДБО документы согласно Перечню электронных документов (Приложение № 12 к настоящим Правилам), в том числе

⁹ ПЭП PayControl предоставляется в системе «ДБО BS-Client (CORREQTS)»

документы в соответствии с другими договорами, заключёнными между Сторонами. Оформление таких документов должно соответствовать требованиям, предусмотренным законодательством Российской Федерации, заключёнными договорами и настоящим Договором.

- 9.1.4. Отзывать ЭД, переданные Банку, до начала их обработки Банком. Запрос на отзыв ЭД направляется в Банк с использованием Системы ДБО в соответствии с Порядком электронного документооборота
- 9.1.5. В период неработоспособности Системы ДБО, в случае отказа Банка в выполнении распоряжения Клиента на проведение операции по списанию денежных средств со Счета, подписанного ЭП, а также при приостановлении обслуживания Клиента с использованием Системы ДБО оформлять и передавать в Банк распоряжения на бумажных носителях.
- 9.1.6. Приостанавливать / возобновлять обслуживание по Системе ДБО, предварительно письменно уведомив об этом Банк не менее чем за 1 (один) рабочий день до даты приостановления/возобновления обслуживания Системы ДБО в порядке, определённом в разделе 7 настоящих Правил.
- 9.1.7. Прекращать полномочия / осуществлять подключение/ изменение данных/ отключение/ блокировку Ключа ЭП Уполномоченного лица в Системе ДБО путем направления Заявления об изменении данных / Заявления о предоставлении модуля ЦФК/РЦК в порядке, определённом пп. 16.3.2.1 настоящих Правил.
- 9.1.8. Устанавливать и снимать ограничения прав на работу и ограничение по параметрам операций в Системе ДБО при обслуживании с использованием Канала доступа «Клиент-Банк Онлайн» на основании Заявления об установлении / снятии ограничений. При использовании Канала «Клиент-Банк» установка ограничений выполняется администратором Системы ДБО Клиента самостоятельно.
- 9.1.9. Инициировать получение:
 - дополнительного/ нового Ключевого носителя (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 Клиентапутём предоставления в Банк Заявления об изменении данных / Заявления о предоставлении модуля ЦФК/РЦК в порядке, определённом пп. 16.3.2.1 настоящих Правил. Получение дополнительного Ключевого носителя (USB-Токена), Устройства подтверждения осуществляется Клиентом в офисе Банка.
- 9.1.10. Подключать/отключать и пользоваться Сервисами Системы ДБО в соответствии с условиями их предоставления, в порядке, определённом Приложением № 1 к настоящим Правилам до момента их отключения Клиентом.
- 9.1.11. Получать у Банка консультации по обслуживанию через Систему ДБО.
- 9.1.12. Уполномочить Банк на предоставление Выписок по своим счетам иному юридическому лицу, отличному от Клиента, которому Клиентом предоставлены полномочия, путём выражения своего согласия в Заявлении о предоставлении выписки по счетам после присоединения указанных организаций (иного юридического лица) к Правилам путём подачи Заявления о присоединении.
- 9.1.13. Направлять в Банк, в случае выявления операции /получения уведомления об операции, соответствующей признакам осуществления перевода денежных средств без согласия клиента в соответствии с требованиями Федерального закона от 27.06.2011 № 161-ФЗ «О национальной платежной системе» (далее - Федеральный закон № 161-ФЗ), заявление о несогласии с операцией в произвольной форме с указанием значимых реквизитов ЭПД на проведении операции:
 - на бумажном носителе, подписанное представителем Клиента и заверенное печатью (при наличии),

или

– по Системе ДБО (при наличии у Клиента нескомпрометированных Ключей ЭП) - в виде сканированного образа подписанного заявления в формате «Письмо» на адреса, определённые пп. 16.3.2.1 настоящих Правил.

В случае необходимости досрочной блокировки Ключей ЭП в Системе ДБО при несогласии с операцией Клиент дополнительно направляет в Банк Заявление о компрометации в соответствии с пп. 9.2.9 настоящих Правил.

9.2. Клиент обязуется:

- 9.2.1. Организовать Клиентское рабочее место для работы в Системе ДБО в соответствии с Инструкцией по установке системы (Приложение № 5/5а к настоящим Правилам) и поддерживать в рабочем состоянии свои программно-технические средства.
- 9.2.2. Соблюдать Порядок электронного документооборота в соответствии с Приложением № 2 к настоящим Правилам.
- 9.2.3. Выполнять требования, указанные в Обязательствах Клиента по безопасной работе (Приложение № 4 к настоящим Правилам), а также по запросу Банка подтверждать выполнение указанных требований. Риски, возникающие в связи с невыполнением требований, указанных в Обязательствах Клиента по безопасной работе, несёт Клиент.
- 9.2.4. Использовать свои программно-технические средства в целях выполнения условий Договора.
- 9.2.5. Использовать Систему ДБО в соответствии с настоящими Правилами.
- 9.2.6. Оплачивать услуги в соответствии с Тарифами Банка в порядке, предусмотренном п. 12.2 настоящих Правил. При наступлении срока взимания вознаграждения, предусмотренного Тарифами Банка, действующими на день совершения операции, обеспечить на Счёте остаток денежных средств, достаточный для уплаты сумм, причитающихся Банку.
- 9.2.7. Предоставить заверенные подписями и оттиском печати Клиента принятые и/или исполненные (в том числе проведённые по Счетам Клиента) копии документов в бумажном/электронном виде или оригиналы указанных документов (в офис Банка или по Системе ДБО) в течение 2 (двух) рабочих дней с даты получения запроса Банка.
- 9.2.8. Не предоставлять третьим лицам, не являющимся УЛ Клиента, возможность распоряжения посредством Системы ДБО денежными средствами, находящимися на Счёте, не предоставлять им право использования SMS-пароля, Логина, 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.
- 9.2.9. Завершить работу Системы ДБО на всех рабочих местах Клиента и уведомить Банк в порядке, определённом Приложением № 4 к настоящим Правилам, оформив Заявление о компрометации, в случае полной или временной утраты контроля доступа третьих лиц к программным средствам Системы ДБО, наступления иных случаев Компрометации (в день утраты). 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.
- 9.2.10. 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).
- 9.2.11. Предоставлять Банку информацию, необходимую для исполнения Банком требований законодательства о противодействии легализации (отмыванию) доходов, полученных преступным путем, финансированию терроризма и

финансированию распространения оружия массового уничтожения, включая информацию о своих выгодоприобретателях, учредителях (участниках) и бенефициарных владельцах, а также иные документы по запросу Банка.

- 9.2.12. 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, 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.
- 9.2.13. Обеспечивать возможность круглосуточной связи по номеру телефона для подтверждения необходимости экстренной блокировки Ключей ЭП, указанному в Заявлении о присоединении.
- 9.2.14. Контролировать исполнение ЭД Банком, регулярно проверять движение денежных средств по Счетам. При несогласии с исполненным ЭД или при получении уведомления об операции, соответствующей признакам осуществления перевода денежных средств без согласия клиента в соответствии с требованиями Федерального закона № 161-ФЗ обратиться в Банк в порядке, определённом пп. 9.1.13 настоящих Правил, с заявлением о несогласии с операцией не позднее, чем на следующий рабочий день после совершения операции / получения от Банка уведомления об операции, совершение которой не было санкционировано Клиентом.
При нарушении Клиентом срока информирования Банка о несогласии с операцией, Банк не возмещает Клиенту сумму операции, совершенной с использованием Системы ДБО без согласия Клиента.
- 9.2.15. 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 о присоединении/ Заявлении об изменении данных, информацию об ЭД и расчётах по Счетам.
- 9.2.16. 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.
- 9.2.17. 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.
- 9.2.18. 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.
- 9.2.19. 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, и по требованию Банка Клиент обязан предоставить их в Банк.
- 9.2.20. Исполнять требования действующего законодательства Российской Федерации, в том числе Федерального закона № 152-ФЗ.

- 9.2.21. 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.
- 9.2.22. В течение срока действия Договора ДБО обеспечить сохранность полученных в рамках Договора ДБО программных СКЗИ, технологической документации и ключевой информации.
- 9.2.23. 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.

10. Права и обязанности Банка¹⁰

10.1. Банк имеет право:

- 10.1.1. Требовать у Клиента документы и сведения, необходимые для осуществления функций, предусмотренных действующими законодательными и нормативными актами Российской Федерации, в том числе для выполнения Банком требований Федерального закона № 115-ФЗ.
- 10.1.2. Блокировать использование Ключей ЭП Клиента после окончания срока их действия или блокировать доступ УЛ к Системе ДБО в случае истечения Срока действия полномочий / отзыва полномочий Уполномоченного лица Клиента на основании данных предоставленных Клиентом в соответствии с пп. 9.2.12 настоящих Правил, либо на основании данных полученных Банком из открытых официальных источников (например, ЕГРЮЛ/ЕГРИП, исполнительные производства, арбитражные дела, бухгалтерская отчётность, государственные контракты и т.д.).
- 10.1.3. В одностороннем порядке вводить лимиты/ ограничения на совершение операций в Системе ДБО, а также другие меры безопасности, направленные на сокращение возможных потерь Клиента от неправомерных действий третьих лиц.
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 о присоединении или полученным Банком при идентификации Клиента, в срок не позднее 5 (пяти) рабочих дней до введения указанных лимитов/ограничений.
- 10.1.4. 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 принятии 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.
- 10.1.5. При открытии новых счетов Клиенту подключать их к Системе ДБО в автоматическом режиме без предоставления Клиентом заявления на их подключение.
Исключением является случай, когда Клиент использует две Системы ДБО и в одной из Систем ДБО запрашивает установление режима «Акцепт (бюджетирование)» по Счёту (-ам), тогда в другой Системе ДБО такой Счёт (-а) Банк переводит в режим

¹⁰ Права и обязанности Банка, относящиеся к обслуживанию расчётных счетов Клиента в Системе ДБО, не распространяются на Клиентов, не имеющих расчётных счетов в Банке.

работы «просмотр».

- 10.1.6. Направлять Клиенту посредством Системы ДБО документы согласно Перечню ЭД (Приложение № 12 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, соответствующими договорами и настоящим Правилам.
- 10.1.7. Приостановить обслуживание Клиента по Системе ДБО, уведомив Клиента путём направления уведомления в порядке, определённом п. 16.3 настоящих Правил, в следующих случаях, включая, но не ограничиваясь:
- на время спорных ситуаций между Клиентом и Банком до урегулирования разногласий;
 - для выполнения неотложных, аварийных и регламентных работ, связанных с обслуживанием Системы ДБО, с уведомлением Клиента о сроках проведения этих работ посредством размещения информации в разделе «Вход в Интернет-Банк» (окно входа в Систему ДБО);
 - при наличии подозрений о Компрометации;
 - при возникновении просрочки оплаты услуг Банка;
 - при выявлении ЭПД, соответствующего признакам осуществления перевода денежных средств без согласия Клиента, установленным Банком России, до подтверждения возобновления исполнения ЭПД Клиентом. При неполучении подтверждения возобновления исполнения ЭПД в порядке, определённом пп. 10.2.7 настоящих Правил Банк действует в соответствии с требованиями Федерального закона № 161-ФЗ;
 - при непредставлении документов и/или информации, необходимых для фиксирования информации в целях противодействия легализации (отмывания) доходов, полученных преступным путем, финансирования терроризма или финансирования распространения оружия массового уничтожения, в том числе:
 - непредставления/несвоевременного представления или представления Клиентом неполных сведений (документов) в части идентификации, в том числе при обновлении сведений о Клиенте, его представителе, выгодоприобретателе, бенефициарном (ых) владельце (ах);
 - возникновения подозрений, что операция осуществляется в целях легализации (отмывания) доходов, полученных преступным путём, финансирования терроризма и финансирования распространения оружия массового уничтожения;
 - отсутствия постоянно действующего исполнительного органа или представителя Клиента – юридического лица по адресу местонахождения, указанному в Едином государственном реестре юридических лиц.
- 10.1.8. 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 в порядке, определённом п. 4.7 - 4.8 настоящих Правил.
- 10.1.9. 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.
- 10.1.10. 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.

- 10.1.11. Взимать за оказываемые в соответствии с Правилами услуги в порядке заранее данного акцепта Клиента со Счета Клиента, открытого в Банке на основании договора банковского счёта суммы комиссионного вознаграждения согласно действующим Тарифам Банка в соответствии с порядком, определённым с п. 12.2 настоящих Правил.
- 10.1.12. Отказать Клиенту в предоставлении Сервисов Системы ДБО в соответствии с Правилами в случае отсутствия/ недостаточности денежных средств на оплату комиссионного вознаграждения Банка за её предоставление в соответствии с Тарифами, действующими на момент обращения Клиента.
- 10.1.13. 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.
- 10.1.14. Производить замену программного обеспечения Системы ДБО без согласия Клиента, уведомив об этом Клиента не менее чем за 30 (тридцать) календарных дней до ввода в эксплуатацию нового программного обеспечения Системы ДБО посредством направления информационного сообщения по Системе ДБО в формате «Письмо».
- 10.1.15. Вносить изменения в Договор ДБО и/или Тарифы в одностороннем порядке, уведомляя об этом Клиента в соответствии с п. 14.2 настоящих Правил.
- 10.1.16. 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 или смене Номера телефона УЛ.
- 10.1.17. Отказаться от Договора ДБО в одностороннем порядке на основании п. 15.3 настоящих Правил при выявлении факта неиспользования Клиентом Системы ДБО (не проведение Клиентом сеансов связи с Банком) в течение срока, превышающего 6 (шесть) календарных месяцев.

10.2. Банк обязуется:

- 10.2.1. 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).
- 10.2.2. Произвести предусмотренные настоящими Правилами действия, необходимые для предоставления Клиенту возможности работы с Системой ДБО, а также обеспечить установление ограничений прав на работу и ограничений по параметрам операций в Системе ДБО, указанных Клиентом в Заявлении об установлении / снятии ограничений, при обслуживании с использованием Канала «Клиент-Банк Онлайн».
- 10.2.3. Обеспечить конфиденциальность информации о Счете (-ах) Клиента и защиту от несанкционированного доступа к операциям по Счету (-ам) со стороны Банка при условии выполнения Клиентом условий Договора ДБО, касающихся защиты конфиденциальной информации от несанкционированного доступа, в том числе

изложенных в Обязательствах Клиента по безопасной работе (Приложение № 4 к настоящим Правилам).

- 10.2.4. Приостановить исполнение ЭПД при выявлении Банком операции, соответствующей признакам осуществления перевода денежных средств без согласия Клиента в соответствии с требованиями Федерального закона № 161-ФЗ на срок не более 2 (двух) рабочих дней, следующих за днём поступления в Банк Распоряжения Клиента.
- 10.2.5. Уведомлять Клиента любым доступным способом, в том числе по Системе ДБО, в виде SMS-сообщений по телефонным номерам, указанным в разделе «Контактные данные клиента» Заявления о присоединении или полученным Банком при идентификации Клиента, о приостановлении исполнения ЭПД и/или о приостановлении зачисления в случае выявления операции /получении уведомления об операции, соответствующей признакам осуществления перевода денежных средств без 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 согласия Клиента.
- 10.2.6. Запрашивать у Клиента подтверждение возобновления исполнения ЭПД при выявлении Банком операции, соответствующей признакам осуществления перевода денежных средств без согласия Клиента.
- 10.2.7. Возобновлять исполнение ЭПД Клиента по операции, соответствующей признакам осуществления перевода денежных средств без согласия Клиента:
 - незамедлительно при получении от Клиента подтверждения посредством направления в Банк заявления о согласии с операцией способом, предусмотренным пп. 9.1.13 настоящих Правил;
 - по истечении 2 (двух) рабочих дней после совершения действий, указанных в пп. 10.2.5 настоящих Правил, в случае неполучения от Клиента заявления о согласии/несогласии с операцией.
- 10.2.8. Уведомлять Клиента о совершении/отказе (с указанием причины отказа) в проведении операции Клиента по Счету (-ам) с использованием Системы ДБО путём предоставления Выписки по счёту, а также путём смены Статуса ЭД в Системе ДБО в соответствии с Порядком электронного документооборота. Обязанность Банка по уведомлению Клиента считается исполненной в момент смены Статуса ЭД при обработке документа Банком в Системе ДБО. Статусы, присваиваемые ЭД, определены Порядком электронного документооборота.
- 10.2.9. По факту получения от Клиента информации о Компрометации в соответствии с пп. 9.2.9 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.
- 10.2.10. Возместить Клиенту сумму операции, совершённой с использованием Системы ДБО без согласия Клиента на основании полученного от Клиента заявления о несогласии с операцией в порядке, определённом пп. 9.2.14 настоящих Правил.
- 10.2.11. Осуществлять техническое сопровождение и консультирование Клиента в случаях и порядке, предусмотренных настоящими Правилами, и в соответствии с Тарифами Банка.
- 10.2.12. 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 30 (тридцати) дней с даты получения таких заявлений или в иные сроки, установленные законодательством Российской Федерации и настоящими Правилами.

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

11. Ответственность сторон

- 11.1. Соблюдение положений настоящих Правил является обязательным для Банка и Клиента.
- 11.2. Клиент несёт ответственность за достоверность предоставляемых Банку сведений, послуживших основанием для заключения Договора.
- 11.3. 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.
- 11.4. 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.
- 11.5. Банк не несёт ответственность за убытки, возникшие в результате:
- неисполнения клиентом правил безопасной работы при использовании клиентской части Системы ДБО, отражённых в обязательствах клиента по безопасной работе (Приложение № 4 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;
 - несвоевременного сообщения Клиентом в Банк о Компрометации;
 - несанкционированного доступа третьих лиц к Клиентскому рабочему месту, Ключевому носителю, Мобильному устройству Клиента и/или Мобильному приложению PayControl, Мобильному приложению Банка;
 - 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.
- 11.6. 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.
- 11.7. 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.
- 11.8. Банк не несёт ответственность за невозможность получения Клиентом Кода подтверждения в случае указания неверного номера телефона или не информирования Банка об его изменении.
- 11.9. 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.
- 11.10. 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.

- 11.11. Клиент несёт риск возникновения убытков и иных неблагоприятных последствий в случае не направления в Банк заявления о несогласии с операцией в соответствии с пп. 9.1.13 настоящих Правил при получении уведомления об операции, соответствующей признакам осуществления перевода денежных средств без согласия Клиента в соответствии с требованиями Федерального закона № 161-ФЗ, а также риски, возникающие в связи получением доступа третьих лиц к указанным в пп. 9.2.8 настоящих Правил устройствам.
- 11.12. Клиент несёт ответственность за сохранность Аутентификационных данных при использовании Системы ДБО.
- 11.13. 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.
- 11.14. 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.
- 11.15. 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.

12. Порядок оплаты услуг

- 12.1. Стоимость услуг Банка устанавливается Тарифами Банка. 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.
- 12.2. В случае если Счёт для взимания комиссионного вознаграждения, указанный в Заявлении о присоединении/ 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, указанный в Заявлении о присоединении/ Заявлении об изменении данных, открыт в другой кредитной организации, Клиент предоставляет в Банк заверенную должным образом копию документа (договор, соглашение, заявление и т.д.), заключённого с этой кредитной организацией, на основании которого Банку предоставлено право списывать денежные средства со счёта.
Клиент также может оплатить комиссионное вознаграждение Банка посредством внесения наличных денежных средств в рублях Российской Федерации в кассу Банка по месту обслуживания.

- 12.3. При использовании модуля ЦФК/РЦК для всех организаций, подключённых к модулю ЦФК/РЦК Контролирующей организации, применяется единый принцип списания комиссий Банка за оказываемые услуги, установленный Контролирующей организацией в Заявлении о предоставлении модуля ЦФК/РЦК Контролирующей организации. Изменение счёта для списания комиссий Банка осуществляется только для всех зарегистрированных в модуле ЦФК / РЦК счетов.

13. Разрешение споров и конфликтов

- 13.1. Все споры и разногласия, возникающие при исполнении Договора ДБО, Стороны будут стремиться разрешать путём переговоров.
- 13.2. 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 в срок не позднее рабочего дня, следующего за днём отправки такого информационного сообщения, или предоставления оригинала письма непосредственно по местонахождению Стороны. Соответствующее уведомление (заявление) на бумажном носителе должно быть подписано представителем Банка и заверено оттиском печати соответствующей Стороны.
- 13.3. При возникновении спорных /конфликтных ситуаций, связанных с использованием Системы ДБО при обмене ЭД, они рассматриваются в порядке, установленном Положением о порядке проведения технической экспертизы (Приложение № 3 к настоящим Правилам) после подачи Клиентом заявления в Банк с указанием сути претензии. Результаты рассмотрения заявления доводятся до Клиента, в установленные п. 13.4 настоящих Правил сроки.
- 13.4. Банк рассматривает заявление Клиента в срок не более 30 (тридцати) дней с даты получения заявления или в иные сроки, установленные действующим законодательством Российской Федерации и настоящими Правилами.
- 13.5. Стороны признают, что
- 13.5.1. Основополагающим документом при рассмотрении конфликтной ситуации, связанной с обменом ЭД посредством Системы ДБО, является протокол работы Системы ДБО, сформированный Банком.
- 13.5.2. 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.
- 13.6. 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.
- 13.7. 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.
- 13.8. 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.

- 13.9. 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.
- 13.10. 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.
- 13.11. Разбор спорных ситуаций, связанных с использованием Сервиса проверки контрагентов, осуществляется путём предоставления информации об официальных открытых источниках информации, на основании которых работает Сервис проверки контрагентов, после подачи Клиентом заявления в Банк, в порядке, определённом п. 13.3 настоящих Правил.

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

- 14.1. Под опубликованием Правил понимается размещение Банком информации на официальном сайте Банка в сети Интернет www.abg.ru. Датой опубликования Правил считается дата первого размещения Правил на официальном сайте Банка в сети Интернет www.abg.ru.
- 14.2. Банк информирует Клиента об изменениях и/или дополнениях, вносимых в Тарифы в соответствии с пп. 10.1.15 Правил посредством размещения информации в подразделениях Банка, осуществляющих обслуживание Клиентов, и на официальном сайте Банка в сети Интернет www.abg.ru, не позднее, чем за 20 (двадцать) календарных дней до введения в действие изменённых Банком Тарифов.
- 14.3. Банк не несёт ответственности, если информация об изменении и/или дополнении Правил и/или Тарифов, опубликованная в порядке и в сроки, установленные Правилами, не была получена и/или изучена и/или правильно истолкована Клиентом.
- 14.4. Банк в праве осуществлять дополнительное информирование об изменениях и/или дополнениях, вносимых в Правила и/или Тарифы в электронном виде по используемой Клиентом Системе ДБО.
- 14.5. Любые изменения и/или дополнения в Правила и/или Тарифы, 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.
- 14.6. Отсутствие отказа Клиента от обслуживания в Системе (уведомления об отказе от Договора ДБО), а также проведение им операций, предусмотренных Системой, является согласием Клиента на присоединение к новой редакции Правил и с применением новых Тарифов.

15. Срок действия Договора ДБО, расторжение Договора ДБО

- 15.1. Договор ДБО вступает в силу с даты принятия Банком от Клиента надлежаще оформленного Заявления о присоединении и действует до 31 декабря текущего года. По истечении указанного срока Договор ДБО пролонгируется на каждый следующий календарный год, если ни одна из Сторон не уведомит другую в письменной форме о своём намерении отказаться от настоящего Договора ДБО в одностороннем порядке не менее чем за 30 (тридцать) календарных дней до истечения срока действия.

- 15.2. Стороны вправе отказаться от Договора ДБО в одностороннем порядке при условии уведомления об этом другой Стороны не позднее, чем за 30 (тридцать) календарных дней до предполагаемой даты отказа от Договора и проведения взаиморасчётов по обязательствам, вытекающим из Договора ДБО.
- 15.2.1. В случае отказа от Договора ДБО по инициативе Банка последний уведомляет об этом Клиента посредством направления уведомления по установленной Банком форме в порядке, определённом пп. 16.3.1 настоящих Правил. Обязательства Банка по приёму и исполнению электронных документов с использованием Системы ДБО считаются прекращёнными с даты, указанной в уведомлении. Все надлежащим образом оформленные ЭД Клиента, направленные Клиентом в Банк до даты, указанной в уведомлении, подлежат исполнению Банком в соответствии с условиями Правил.
- 15.2.2. В случае расторжения /отказа от Договора ДБО по инициативе Клиента, последний предоставляет в Банк:
- в случае наличия у Клиента Сервисов Системы ДБО - Заявление о расторжении договора;
 - в случае отсутствия у Клиента Сервисов Системы ДБО на момент закрытия Счёта Клиента - Заявление на закрытие банковского счёта установленного Банком образца, предоставление Заявления о расторжении договора не осуществляется. Обслуживание с использованием Системы ДБО прекращается с момента получения Банком такого заявления Клиента. Все надлежащим образом оформленные ЭД Клиента, направленные Клиентом в Банк до момента получения Банком заявления Клиента подлежат приёму /исполнению Банком в соответствии с условиями настоящих Правил. С момента получения Банком заявления Клиента, Банк прекращает приём и завершает исполнение ранее принятых ЭД Клиента.
- 15.3. Отказ от Договора ДБО в случаях, определённых пп. 10.1.17 настоящих Правил осуществляется в одностороннем порядке без соблюдения срока, установленного п. 15.2 настоящих Правил. При этом Банк направляет Клиенту письменное уведомление об отказе от Договора ДБО по установленной Банком форме.
- 15.4. В случае возврата уведомления Банка об отказе от Договора ДБО, направленного Банком по последнему известному адресу Клиента, уведомление считается врученным Клиенту, что влечёт прекращение прав и обязанностей Сторон и является основанием для расторжения Договора ДБО.
- 15.5. В случае расторжения или одностороннего отказа от Договора ДБО, Клиент обязан передать в Банк средства криптографической защиты информации, полученные в рамках Договора ДБО, и Акт возврата СКЗИ.
- 15.6. Расторжение Договора ДБО или односторонний отказ от Договора ДБО не влечёт прекращения обязательств по иным договорам (соглашениям), заключённым между Клиентом и Банком, за исключением договора банковского счёта для идентификации платежа (в рублях Российской Федерации), обслуживание счёта по которому не предполагает предоставление услуги по идентификации платежа без использования Системы ДБО.
- 15.7. 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.
- 15.8. При изменении, исполнении и расторжении/ одностороннем отказе от настоящего Договора ДБО Стороны могут использовать документооборот с применением электронной подписи в соответствии с законодательством Российской Федерации. Документ, подписанный электронной подписью в соответствии с законодательством Российской Федерации, признается Сторонами достаточным доказательством волеизъявления Сторон и приравнивается к документу в письменной форме.
- 15.9. 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 о присоединении. 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.

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, указанной в Заявлении о присоединении, исключая сведения, содержащие банковскую, коммерческую тайны и персональные данные;
 - по почте заказным письмом.
- 16.3.2. Клиентом Банку:
- по Системе ДБО;
 - представителем Клиента/курьером под расписку ответственному представителю Банка;
 - по почте заказным письмом.
- 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 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 сканированного образа заявления в «Письмо» на отдельный адрес «Отдел открытия счетов» с указанием в поле «Тема» сообщения наименования вложенного заявления, при этом 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 о присоединении - 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 «Перечень Сервисов Системы ДБО»;
- Приложение № 2 «Порядок электронного документооборота с использованием Системы ДБО»;
- Приложение № 3 «Положение о порядке проведения технической экспертизы при возникновении спорных ситуаций»;
- Приложение № 4 «Обязательства Клиента по выполнению правил безопасной работы при использовании клиентской части Системы ДБО»;
- Приложение № 5 «Инструкция по установке Системы «iBank»»;
- Приложение № 5а «Инструкция по установке Системы «ДБО BS-Client (CORREQTS)» и Мобильного приложения Банка»;
- Приложение № 6 «Типовая форма Акта приема – передачи ключевых носителей, программного обеспечения и средств криптографической защиты информации (для Клиентов)»;
- Приложение № 7 «Типовая форма Заявления на выезд специалиста Банка на территорию Клиента»;
- Приложение № 8 «Типовая форма Акта выполненных работ»;
- Приложение № 9 «Типовая форма Доверенности (на получателя)»;
- Приложение № 10 «Типовая форма Акта возврата средств криптографической защиты информации»;
- Приложение № 11 «Типовая форма Заявления о расторжении Договора присоединения»;
- Приложение № 12 «Перечень электронных документов, используемых в Системе ДБО»;
- Приложение № 13 «Условия предоставления модуля «Центр финансового контроля / Расчетный центр корпорации» в АО «АБ «РОССИЯ»»;
- Приложение № 14 «Типовая форма Заявления о предоставлении модуля ЦФК/ РЦК Системы ДБО Контролирующей организации»;
- Приложение № 15 «Условия предоставления сервиса подключения Канала «Интеграционный Клиент-Банк»»;
- Приложение № 16 «Типовая форма Заявления о компрометации»;
- Приложение № 17 «Типовая форма Заявление об установлении/ снятии ограничений на работу в Системе ДБО»;
- Приложение № 18 «Типовая форма Заявления о предоставлении третьим лицам выписки по счетам Клиента»;
- Приложение № 19 «Ключ проверки электронной подписи сотрудника клиента в системе «iBank»»;
- Приложение № 19а «Рекомендации по заполнению бланка Ключа проверки ЭП в Системе «iBank»»;
- Приложение № 20 «Ключ проверки электронной подписи сотрудника клиента в Системе «ДБО BS-Client»»;
- Приложение № 20а «Рекомендации по заполнению бланка Ключа проверки ЭП Клиента в Системе «ДБО BS-Client»».

Перечень Сервисов Системы ДБО

№ п/п	Наименование Сервиса	Способ подключения Сервиса	Необходимость наличия открытого счета в банке (да/нет)
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 заключаемых между Банком и Клиентом договоров.	Доступно при подключении СДБО	НЕТ
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	НЕТ
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	НЕТ
1.4.	Сервис по заключению Договора присоединения к Условиям депозитных сделок/ НСО с использованием СДБО – сервис по предоставлению клиентам возможности заключения Договора присоединения к Условиям депозитных сделок/ НСО посредством направления в Банк электронного документа «Заявка	Дистанционно	НЕТ

	на подключение услуги «Депозиты» / «НСО». Подачу Заявки на подключение услуги осуществляет единоличный исполнительный орган Клиента или лицо им уполномоченное.		
1.5.	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	НЕТ
1.6.	Сервис предоставления сведений об Уполномоченных лицах для целей размещения денежных средств в Депозиты и/или НСО.	Дистанционно	НЕТ
1.7.	Сервис предоставления сведений об Уполномоченных лицах для целей получения отчётности в рамках услуги банковского сопровождения контрактов.	Дистанционно	НЕТ
1.8.	Модуль «Тикер для корпоративных клиентов» Системы «iBank» - сервис информирования Клиента о движении денежных средств по Счетам в режиме онлайн, просмотра Выписки по счёту, а также поступления и просмотра входящих документов из Банка. В случае возникновения события поступления или списания по Счёту, поступления входящего документа из Банка модуль информирует Клиента о данном событии с помощью всплывающего сообщения. Доступно для подключения в Модуле «Управление услугами».	Дистанционно	НЕТ
1.9.	Сервис подключения Канала «Интеграционный Клиент-Банк» - сервис подключения канала отправки ЭД в Банк Системы ДБО, предоставляющий возможность обмена ЭД с Банком с использованием УНЭП и УКЭП напрямую из Учетной системы Клиента. Подключение канала осуществляется в соответствии с Приложением № 15 к настоящим Правилам.	Дистанционно	НЕТ
1.10.	Сервис «Подписки» - сервис направления Клиенту уведомлений о наступлении определённых событий, параметры подписки настраиваются посредством изменения разрешённых настроек в пользовательском интерфейсе данного сервиса.	Дистанционно	НЕТ
1.11.	Сервис настройки механизмов защиты системы и подтверждения исполнения ЭПД - автоматизированный сервис «Заявления о настройке способа защиты системы и подтверждения исполнения документов», обеспечивающий возможность Клиентам подавать в виде электронного документа заявление о выдаче Устройства подтверждения и настройке механизмов защиты системы и подтверждения исполнения ЭПД ¹ .	Дистанционно	НЕТ
1.12.	Сервис информирования Банка о Компрометации или подозрениях на Компрометацию – автоматизированный сервис, обеспечивающий возможность Клиентам подавать в виде электронного документа Заявления о компрометации. Сервис доступен только УЛК с полномочиями единоличного исполнительного органа ¹ .	Дистанционно	НЕТ

¹ Сервис доступен с момента технической реализации

1.13.	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 (бюджетирование)», «Управление счетами». Подключение осуществляется Банком на основании Заявления о предоставлении модуля ЦФК/РЦК в порядке и на условиях, определенных Приложением № 13 к настоящим Правилам.	На основании заявления	НЕТ
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 (при наличии);	Доступно при подключении СДБО	ДА
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	ДА
2.3.	Сервис проверки контрагентов ² - автоматизированный сервис, предназначенный для получения в режиме онлайн аналитической информации о контрагентах (получателях 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.	Дистанционно	ДА
2.4.	Сервис «Электронная справка» ³ . Справки предоставляются по Счетам Клиента, открытым в Банке, в виде вложения в «Письмо», подписанного УНЭП Банка.	Дистанционно	ДА
2.5.	Сервис «Заказ Банковской карточки». Копия Банковской карточки предоставляется Клиенту в виде вложения в «Письмо», подписанного УНЭП Банка.	Дистанционно	ДА
2.6.	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	Дистанционно	ДА

² Услуга доступна при использовании Канала доступа «Клиент-Банк Онлайн» и Мобильном приложении Банка.

³ Перечень предоставляемых сведений может расширяться по мере технической реализации.

	получения денежных средств с использованием чековой книжки Клиент может направить заявку в формате «Письмо» в соответствии с пп. 16.3.2 настоящих Правил.		
2.7.	Сервис направления Банком Клиенту уведомлений: – об ограничениях по Счету(ам) с использованием Системы ДБО в формате «Письмо»; – об операциях поступления и/или списания по Счету(ам) в валюте Российской Федерации в СДБО iBank в виде SMS-сообщений.	Дистанционно	ДА
2.8.	Сервис направления Клиентом из интерфейса Системы ДБО на электронный адрес контрагента Клиента: – информации об исполненном платеже. Сообщения направляются программным путем с адреса 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 адреса notification [mailto:ibank2@abr.ru] в Системе «iBank», с адреса online@abr.ru в Системе «BS-Client(CORREQTS)».	Дистанционно	ДА
2.9.	Сервис работы со Счетами в режиме «Акцепт (визирование)». Подключение осуществляется Банком на основании Заявления о присоединении/ Заявления об изменении данных. Порядок предоставления указанных услуг определен разделом 8 настоящих Правил.	На основании заявления	ДА
2.10.	Сервис передачи Выписок по своим счетам единоличному исполнительному органу (ЕИО) Клиента, иному юридическому лицу, отличному от Клиента. Подключение услуги осуществляется Банком на основании Заявления о предоставлении третьим лицам выписки по счетам.	На основании заявления	ДА

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»;
- изменение разрешённых Системой ДБО настроек.

Порядок дистанционного подключения сервисов определен 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.

**Порядок
электронного документооборота с использованием Системы ДБО**

1. Банк осуществляет приём ЭД, передаваемых по Системе ДБО, круглосуточно, кроме времени необходимого для установки обновлений или профилактических работ. Активной Стороной в установлении соединения (сеансов связи) и в процессе приёма-передачи ЭД, информации об их статусах, Выписок по счёту и сообщений является Клиент.
2. Банк обрабатывает принятые ЭД в течение Операционного дня. Банк имеет право изменять время приёма и обработки документов, о чём Клиент оповещается не позднее, чем за 1 (один) день до наступления изменений путём направления сообщения по Системе ДБО. В процессе обработки ЭД программным путём фиксируются дата и время его поступления и исполнения /возврата (аннулирования) Банком.
3. Система ДБО состоит из следующих компонентов:
 - сервер, расположенный на территории Банка;
 - клиентская часть, расположенная на компьютерах Клиента и/или Мобильном устройстве Уполномоченного лица Клиента (Клиентское рабочее место).
4. В Системе ДБО все действия по формированию, редактированию и подписанию ЭД производятся в клиентской части. Клиент несёт полную ответственность за действия лиц, получивших по любым основаниям (в том числе противоправным) доступ к клиентской части Системы ДБО, Ключам ЭП/ Ключам PayControl и иным техническим и информационным средствам, обеспечивающим возможность формирования и направления в Банк ЭД.
5. Для защиты ЭД, передаваемых по Системе ДБО, Стороны используют ЭП и Коды подтверждения.

ЭД (в том числе оформляемый и/или представляемый в соответствии с Инструкцией Банка России от 16.08.2017 № 181-И «О порядке представления резидентами и нерезидентами уполномоченным банкам подтверждающих документов и информации при осуществлении валютных операций, о единых формах учета и отчетности по валютным операциям, порядке и сроках их представления» и/или ЭД для целей валютного контроля) порождает обязательства Сторон в рамках настоящих Правил, если он надлежащим образом оформлен, заверен корректной (-ыми) ЭП Уполномоченных лиц (в случае необходимости контроля Банком операций по Счетам Клиента - заверен ЭП Уполномоченного лица, имеющего полномочия на согласование расходных операций по Счетам Клиента), зашифрован и передан по Системе ДБО, получен, расшифрован, проверен и принят к исполнению.

ЭД (в том числе вложение в «Письмо») порождает права и обязанности Сторон по Договору ДБО, договорам банковского счета, другим соглашениям, в рамках которых происходит взаимодействие с использованием Системы ДБО, если передающей Стороной ЭД оформлен надлежащим образом и передан по Системе ДБО, а принимающей Стороной - получен, проверен и принят в соответствии с Порядком электронного документооборота.
6. Передаваемые при взаимодействии Сторон ЭД, заверенные ЭП, имеют равную юридическую силу с документами на бумажном носителе, подписанными уполномоченными представителями и скреплёнными печатями Сторон (независимо от того, существуют такие документы на бумажных носителях или нет). В том числе Стороны признают, что переданные Клиентом по Системе ДБО и подписанные ЭП в формате «Письмо», вложения в «Письмо», являются эквивалентными подобным

документам на бумажных носителях и влекут аналогичные им права и обязанности Сторон.

7. Банк принимает ЭПД к обработке в соответствии с Порядком переводов, размещённом на официальном сайте Банка в сети Интернет www.abr.ru.
8. Основанием для исполнения Банком ЭПД Клиента является соответствие ЭПД Клиента требованиям оформления платёжных документов, установленным законодательством Российской Федерации, нормативными документами Банка России, Порядком переводов, размещённом на официальном сайте Банка в сети Интернет www.abr.ru. В случае если ЭПД оформлен с нарушениями требований действующего законодательства Российской Федерации, расчётная операция не соответствует действующему законодательству Российской Федерации и Правилам переводов, Клиент уведомляется об отказе в исполнении ЭПД в порядке, установленном пп. 13.3.1 настоящего Приложения.
9. Приём и обработка в Системе ДБО ЭД, связанных с проведением валютных операций, осуществляется в соответствии с Правилами взаимодействия АО «АБ «РОССИЯ» с клиентами при осуществлении операций, подлежащих валютному контролю, размещёнными на официальном сайте Банка в сети Интернет www.abr.ru.
10. В случае установления Клиентом ограничений прав на работу по какому-либо из Уполномоченных лиц Клиента и/или ограничений по параметрам операций в Системе ДБО на основании Заявления об установлении/снятии ограничений, Банк принимает к исполнению ЭПД Клиента с учётом установленных ограничений.
11. Используя возможности Системы ДБО и программное обеспечение, предоставленное Банком, Уполномоченные лица самостоятельно выполняют регистрацию Ключей PayControl /Ключей ЭП в порядке, определённом разделами 4 - 5 настоящих Правил (для новых Уполномоченных лиц Клиента), либо разделом 6 настоящих Правил (при смене Ключей ЭП) или Приложением № 4 к настоящим Правилам (при Компрометации).
12. Генерация Ключей ЭП, а также хранение Ключей ЭП осуществляется Клиентом в условиях, обеспечивающих невозможность Компрометации. Клиент не вправе раскрывать третьим лицам информацию о Ключе ЭП/ Ключе PayControl, находящемся в его распоряжении, и должен хранить и использовать его способами, обеспечивающими невозможность несанкционированного использования третьими лицами.
13. **Этапы электронного документооборота:**
 - формирование ЭД, подписание ЭП;
 - передача и приём ЭД;
 - проверка ЭД;
 - подтверждение получения ЭД Банком;
 - отзыв ЭД;
 - хранение и учёт ЭД (ведение архивов ЭД);
 - исполнение ЭД.

13.1. Формирование и подписание ЭД ЭП осуществляется в следующем порядке:

- 13.1.1. Список видов документов, которые могут быть переданы по Системе ДБО, указан в Перечне электронных документов.
- 13.1.2. При использовании Канала «Клиент-Банк Онлайн», Канала «Клиент-Банк», Мобильного приложения банка ЭД оформляется либо путём заполнения стандартной (экранной) формы документа, предусмотренной в Системе ДБО для данного вида ЭД, т.е. внесения данных в форму документа согласно наименованиям полей, либо в виде произвольного документа («Письмо»). При оформлении ЭД Система ДБО осуществляет автоматический контроль присутствия обязательной информации в соответствующих полях формы документа. Ключевыми полями ЭД являются все обязательные для данного вида ЭД реквизиты, без наличия которых надлежащее исполнение ЭД является невозможным. При использовании Канала доступа «Интеграционный Клиент-Банк» для формирования ЭД применяются форматы,

согласованные Сторонами в соответствии с Приложением № 18 к настоящим Правилам.

- 13.1.3. Сформированный ЭД подписывается ЭП Уполномоченных лиц Клиента в количестве, определённом в Заявлении о присоединении / Заявлении об изменении данных, при необходимости сформированный ЭД подписывается Визирующей подписью Уполномоченного лица в любой последовательности и передаётся в Банк с использованием Системы ДБО.
- 13.1.4. При каждом подписании ЭПД в Канале «Клиент-Банк Онлайн», Канале «Клиент-Банк», Мобильном приложении банка Система ДБО запрашивает подтверждение ЭПД, которое осуществляется с применением Кода подтверждения. Подтверждение Кодом подтверждения может быть осуществлено как отдельного ЭПД, так и нескольких ЭПД. Клиент самостоятельно принимает решение о выполнении подтверждения одного или нескольких ЭПД, за исключением Мобильного приложения банка, в котором Клиент подтверждает каждый ЭПД отдельно. Клиент в случае использования Кода подтверждения для подтверждения нескольких ЭПД принимает на себя риск отсутствия полноты информации по каждому подтверждаемому ЭПД в SMS-сообщении Банка.
- 13.1.5. Код подтверждения действителен для применения в течение 5 (пяти) минут с момента получения. В случае необходимости для подтверждения ЭПД требуется повторить процедуру получения Кода подтверждения.
- 13.1.6. Выбор способа подтверждения ЭПД осуществляется Клиентом в Заявлении о присоединении/ Заявлении об изменении данных путём проставления отметок в поле «Код подтверждения в SMS-сообщении»/ «Устройство подтверждения» в разделе «Вариант защиты системы и подтверждения исполнения документов» в разрезе каждого Уполномоченного лица, либо посредством Сервиса настройки механизмов защиты системы и подтверждения исполнения ЭПД Системы ДБО⁴. Банк в выбранной Клиентом Системе ДБО осуществляет настройку способа подтверждения ЭПД, определённого Клиентом.
- 13.1.7. Особенности подписания ЭД с помощью ПЭП PayControl.
- 13.1.7.1. После формирования ЭД в Системе «ДБО BS-Client (CORREQTS)» Клиент посредством Системы «ДБО BS-Client (CORREQTS)» делает запрос на подписание ЭД с помощью ПЭП PayControl и его отправку в Банк на исполнение.
- 13.1.7.2. На Мобильное устройство УЛ Клиента поступает PUSH-сообщение о необходимости подтверждения операции (ЭД) в Мобильном приложении PayControl. После прохождения Аутентификации при входе в Мобильное приложение PayControl в соответствии с установленным в п. 4.9 настоящих Правил способом, Клиенту предоставляется возможность подтвердить подписание ЭД, информация о котором отражается в Мобильном приложении PayControl, или отклонить подтверждение подписания.
- 13.1.7.3. Применение Мобильного приложения PayControl позволяет реализовать технологические меры по использованию отдельных технологий для подготовки электронных сообщений, содержащих распоряжения Клиента на перевод денежных средств, и передачи Клиентами подтверждений об исполнении распоряжений на перевод денежных средств в Банк.

13.2. Передача и прием ЭД:

- 13.2.1. ЭД считается исходящим от Отправителя (Уполномоченное лицо Клиента/работник Банка, производящий обработку ЭД), если:
- ЭД подписан с использованием Ключа ЭП Отправителя;
 - Срок действия Ключа ЭП, использованного (использованных) для подписания ЭД на момент проверки не истёк;
 - Банк не уведомлён о Компрометации Ключа (-ей) ЭП Отправителя;
 - срок действия полномочий лица, подписавшего ЭД ЭП не истёк.

⁴ Сервис доступен с момента технического внедрения.

- 13.2.2. ЭД не считается исходящим от Отправителя (Уполномоченное лицо Клиента/работник Банка, производящий обработку ЭД), если:
- ЭД не прошел проверку на целостность текста и подлинность ЭП;
 - Банк уведомлен о Компрометации Ключа ЭП Отправителя, с использованием которого был подписан ЭД.
- 13.3. **Проверка подлинности доставленного ЭД** включает:
- расшифровку ЭД;
 - проверку ЭД на соответствие установленному формату для данного вида ЭД;
 - проверку подлинности ЭП, которыми подписан ЭД;
 - контроль полноты и целостности ЭД.
- 13.3.1. Уведомлением Клиента о совершении/ отказе (с указанием причины отказа) в проведении операции Клиента по Счету (-ам) с использованием Системы ДБО, а также о принятии или непринятии (с указанием причины отказа) поступивших от Клиента в виде ЭД документов для целей валютного контроля в соответствии с Правилами взаимодействия АО «АБ «РОССИЯ» с клиентами при осуществлении операций, подлежащих валютному контролю, размещёнными на официальном сайте Банка в сети Интернет www.abr.ru, является предоставление Выписки по счёту и смена Статуса ЭД в Системе ДБО в соответствии с п. 13.4 настоящего Приложения. Изменение Статуса ЭД о принятии/непринятии ЭД осуществляется Банком. При этом изменение Статуса ЭД в Системе ДБО признается электронным сообщением о принятии/непринятии документа Банком. Исполненные операции Клиента по Счету (-ам) отражаются в Выписке по счёту.
- 13.3.2. В случае положительного результата проверки, ЭД принимается к исполнению или к сведению в зависимости от типа ЭД или подлежит дальнейшей обработке. Отправителю направляется подтверждение о получении ЭД в форме Смены статуса ЭД в Системе ДБО.
- 13.3.3. В случае ошибки при дешифрации, либо неудовлетворительном результате проверки ЭП, Отправитель получает по Системе ДБО формируемое программным путем служебное электронное сообщение об отрицательном результате проверки, то есть об отказе в сохранении и/или приёме ЭД.
- 13.3.4. Банк осуществляет проверку корректности составления ЭПД и подлинности ЭП Клиента после подтверждения Уполномоченным лицом Клиента отправки соответствующего ЭПД Кодом подтверждения в соответствии с требованиями пп. 13.1.4 настоящего Приложения.
- 13.3.5. В случае прохождения ЭД для целей валютного контроля проверки ЭП Банк осуществляет проверку правильность заполнения документа валютного контроля в соответствии с требованиями валютного законодательства Российской Федерации и его соответствие сведениям, содержащимся в комплекте документов, представленных для целей валютного контроля, а также полноту такого комплекта. В сроки, установленные валютным законодательством Российской Федерации, Банк принимает или отказывает в принятии документа валютного контроля (с указанием причин отказа), информируя Клиента о принятии/непринятии каждого документа валютного контроля при обработке ЭД путём смены Статуса ЭД в Системе ДБО в соответствии с пп. 13.3.1 настоящего Приложения. В процессе обработки документа валютного контроля программным путём фиксируются дата и время его поступления и принятия/или отказа в принятии Банком.
- 13.4. **Подтверждение получения ЭД** при использовании Канала «Клиент-Банк Онлайн» и Канала «Клиент-Банк»:
- 13.4.1. Свидетельством того, что ЭД принят/ непринят Банком к исполнению, является изменение Статуса ЭД в Системе ДБО.
- 13.4.2. ЭД считается полученным Банком только в случае, если он имеет статус⁵:
- для ЭПД – «Принят АБС» / «На исполнении»;

⁵ Здесь и далее по тексту: Статусы ЭД по мере расширения функционала Системы могут изменяться, дополняться.

- для ЭД по валютному контролю – «Принят» («Принят АБС»)/ «Доставлен» («На исполнении»);
 - для ЭСИД «Письмо» – «Принят» / «Доставлен» / «Обработан» / «Исполнен». По ЭСИД «Письмо» может быть отправлено ответное сообщение Клиенту по Системе ДБО, включающее текст следующего содержания: «Заявление принято Банком».
- 13.4.3. ЭД считается полученным Банком и не принятым к исполнению (отказанным в исполнении) в случае, если он имеет статус:
- для ЭПД – «Не принят АБС» («ЭП не верна» / «Ошибка реквизитов»/ «Отозван»/ «Не подтвержден»/ «Отказан АБС»/ «Отказан РЦК»)/ «Отвергнут»;
 - для ЭД по валютному контролю – «Не принят АБС» («ЭП не верна» / «Ошибка реквизитов»/ «Отозван»/ «Отказан АБС»/ «Отказан ВК»/ «Не принят»)/ «Отвергнут»;
 - для ЭСИД «Письмо» – «Не принят» («ЭП не верна» «Отозван»/ «Отказан АБС»)/ «Отвергнут». По ЭСИД «Письмо» может быть отправлено ответное сообщение Клиенту по Системе ДБО, включающее текст следующего содержания: «Заявление не принято Банком» (с указанием причины отказа в приёме).
- 13.4.4. При отсутствии изменения статуса отправленного ЭД/ неполучения сообщения от Банка по ЭСИД «Письмо» отправляющая Сторона должна уведомить принимающую Сторону о данном факте в день отправки ЭД любым доступным способом. Принимающая Сторона не несёт ответственности за неисполнение не полученных или не принятых ЭД⁶.
- 13.4.5. Информация о Статусе ЭД доступна Клиенту для просмотра во время сеансов связи с использованием Системы ДБО. Статусы ЭД, однозначно отражающие их текущее состояние, автоматически отображаются в Системе ДБО и синхронизируются во время сеансов связи, проводимых Клиентом.
- 13.5. Подтверждение получения ЭД при использовании Канала «Интеграционный Клиент-Банк»:**
- 13.5.1. Свидетельством того, что ЭД принят и подтверждён, является полученная отправляющей Стороной информация в электронной форме в ответ на запрос о статусе отправленного ЭД, содержащая данные о факте доставки отправленного ЭД (далее – Квитанция).
- 13.5.2. При наличии ошибок ЭД Банком не принимаются, а Клиенту отправляется Квитанция об отказе.
- 13.6. Отзыв ЭД:**
- 13.6.1. Клиент вправе отозвать отправленный ЭД путём направления получателю ЭД «Запрос на отзыв документа», если иное не предусмотрено отдельным договором между Банком и Клиентом.
- 13.6.2. В Запросе на отзыв документа должно указываться основание отзыва ЭД.
- 13.6.3. ЭД может быть отозван только до начала его исполнения получателем. Банк вправе отказать в отзыве Отправителю в случае невозможности отзыва ЭД.
- 13.6.4. Отказ Банка в принятии/ исполнении ЭД, отзыв ЭД, возврат ЭД осуществляется в соответствии с Порядком переводов, размещённом на официальном сайте Банка в сети Интернет www.abr.ru.
- 13.7. Хранение и учет ЭД:**
- 13.7.1. Банк обязан хранить полученные от Клиента ЭД в течение предусмотренных действующим законодательством Российской Федерации сроков хранения для аналогичных по смыслу документов на бумажном носителе. Способ и формат хранения определяются Банком.
- 13.7.2. Все операции, производимые Сторонами в Системе ДБО, в том числе Системой ДБО, автоматически фиксируются в протоколах работы программы, хранящихся в

⁶Уведомление может быть получено только во время сеанса связи с Банком.

электронном виде в Банке. В случае разногласия между Банком и Клиентом Стороны признают в качестве доказательств записи в протоколе работы программы, хранящиеся на сервере Банка.

13.7.3. Система ДБО ведёт учёт действий, производимых Сторонами в ней, включая автоматические действия самой Системы ДБО (регистрация учётной записи Клиента в Системе ДБО, проверка средств доступа, средств подтверждения при входе в Систему ДБО, вход/выход из Системы, создание ЭД, проверка средств подтверждения при обработке документов), в том числе при смене Статусов ЭД.

В протоколах Системы ДБО осуществляется регистрация следующей информации о действиях Клиентов, выполняемых с использованием Системы ДБО:

- дата (день, месяц, год) и время (часы, минуты, секунды) осуществления действия Клиента;
- идентификатор Клиента;
- код, соответствующий выполняемому действию Клиента;
- идентификатор устройства Клиента, с которого осуществлялось действие.

Хранение в протоколах Системы ДБО зарегистрированной информации о действиях Клиентов, выполненных с использованием Системы ДБО, осуществляется не менее 5 (пяти) лет, начиная с даты осуществления действия.

13.7.4. Сформированные Банком посредством Системы ДБО отчёты по произведённым операциям (действиям) в Системе ДБО и распечатанные на бумажных носителях по форме Банка, подписанные Уполномоченным представителем Банка и скреплённые печатью Банка, являются достаточными доказательствами фактов совершения Сторонами операций и действий (в том числе Системой ДБО автоматически), предусмотренных Договором, и могут быть использованы при разрешении любых споров, а также предоставлены в судебные органы.

13.8. **Исполнение ЭД:**

При исполнении Банком поступившего ЭД в Системе ДБО отображается отметка об исполнении в виде смены Статуса ЭД в соответствии с п. 13.4 настоящего Приложения или осуществляется направление Квитанции в соответствии с п. 13.5 настоящего Приложения.

В случае установления Клиентом ограничений прав на работу и ограничение по параметрам операций в Системе ДБО по какому-либо из Уполномоченных лиц Клиента, Банк исполняет ЭПД, подписанные ЭП данного Уполномоченного лица с учётом установленных ограничений.

14. **Предоставление Выписки по счёту:**

14.1. Выписка по счёту Клиента за предыдущий Операционный день (включая обороты и сальдо по счёту) формируется не позднее следующего Операционного дня.

Выписка об операциях по счетам Клиента, переданная Клиенту, идентична выписке, выдаваемой Банком на бумажном носителе, и является исполнением обязательства по договору банковского счёта, и не влечёт обязанности для Сторон по получению/предоставлению Выписок по счетам Клиента на бумажном носителе. Выписки об операциях по счетам могут предоставляться Клиенту или исполнительному органу Клиента, либо иному юридическому лицу, отличному от Клиента, которому Клиентом в соответствии с Договором присоединения предоставлены полномочия на получение информации по счетам Клиента в формате Выписки по счёту.

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.
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;
 - 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 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, а также отсутствия несанкционированных действия 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, в срок 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 срок, не превышающий 5 (пять) 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 с изложением сути претензии;
 - бумажную копию оспариваемого ЭД (при наличии);
 - заверенные Банком копии заявлений об изменении состава Уполномоченных лиц Клиента, аннулировании действия Ключа ЭП Уполномоченных лиц Клиента, приостановлении/возобновлении доступа Клиента к Системе ДБО 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 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, приостановлении/возобновлении доступа Клиента к Системе ДБО (при наличии) по формам, определённым Банком в Правилах, данные об аннулировании действия Ключа ЭП Уполномоченного представителя Банка (при наличии);
 - выписка протокола работы Системы ДБО, подтверждающая приём/отправку спорного ЭД, на бумажном носителе, за согласованный Сторонами период времени.
15. По взаимной договорённости Стороны могут передать Экспертной комиссии другие материалы, имеющие отношение к сути рассматриваемой претензии.
16. Стороны обязаны способствовать работе Экспертной комиссии и не допускать отказа от предоставления необходимых документов.
17. В случае не предоставления 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 спорного 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, приостановлении/возобновлении доступа Клиента к Системе ДБО, 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, приостановлении/возобновлении доступа Клиента к Системе ДБО, 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 проверки 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.

19. 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.
20. 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.
21. 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.
22. В случае выполнения всех условий, перечисленных в п.п. 18 или 20 настоящего Положения, Стороны соглашаются с тем, что корректность УНЭП/ УКЭП/ ЭП PayControl под оспариваемым ЭД подтверждена, то есть проверяемый ЭД подписан корректными УНЭП/ УКЭП/ ЭП PayControl.
23. В случае невыполнения любого из условий, перечисленных в п.п. 18 или 20 настоящего Положения Стороны соглашаются с тем, что корректность УНЭП/ УКЭП/ ПЭП PayControl не подтверждена, то есть проверяемый ЭД подписан некорректными УНЭП/ УКЭП/ ПЭП PayControl.
24. 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.
25. 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.
26. По итогам работы Экспертной комиссии составляется Акт о результатах проведения технической экспертизы, в котором фиксируются выводы, к которым пришла Экспертная комиссия в результате проведённых мероприятий в 2 (двух) экземплярах, по одному экземпляру для Стороны, который 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.

27. Акт подписывается всеми членами Экспертной комиссии и является основанием для принятия Сторонами окончательного решения об урегулировании спорной ситуации.
28. 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.
29. Максимальный срок работы Экспертной комиссии составляет не более 30 (тридцать) календарных дней с даты её формирования, включая дату предоставления Акта.
30. В случае несогласия одной из Сторон с решением Экспертной комиссии, 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.

Обязательства Клиента по выполнению правил безопасной работы при использовании Клиентской части Системы ДБО

(заполняется в обязательном порядке при подписании Заявления о присоединении к Правилам)

**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 клиентской части 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, защиту от несанкционированного доступа в Систему ДБО при использовании Канала доступа «Интеграционный Клиент-Банк», а также защиту от несанкционированного доступа к другой конфиденциальной информации;
- 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:

- 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);
- 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 сменить Пароль и обратиться в Банк по телефону службы технической поддержки, указанному на официальном сайте Банка в сети Интернет по адресу www.abr.ru;
- 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;
 - при Компрометации / подозрении на Компрометацию или Компрометацию среды исполнения (наличие в компьютере вредоносных программ), а также атрибутов доступа к Мобильному устройству (Логин, Пароль, графический ключ, PIN-код, отпечаток пальца или изображение лица (TouchID/ FaceID)) следует незамедлительно обратиться в Банк по телефону службы технической поддержки, указанному на официальном сайте Банка в сети Интернет www.abr.ru, и заблокировать Ключ ЭП/ Ключ PayControl в порядке, предусмотренном настоящим Приложением;
 - 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.

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 используется 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, находящимися на Счёте, или в иных целях, оставлять Ключевые носители без присмотра;

- в случае утраты или поломки Устройства подтверждения необходимо уведомить об этом Банк посредством личного обращения в Банк или путём обращения по телефону службы технической поддержки Системы ДБО 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 заражён, а также в случае обнаружения незарегистрированных программ или нарушения целостности операционной системы – обязательно позвонить в Банк и заблокировать Ключ ЭП/ Ключ PayControl в порядке, предусмотренном разделом 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 ненадёжных источников, скачанные с неизвестных web-сайтов, присланные по электронной почте, полученные в телеконференциях;
- на компьютере запрещено запускать программы, полученные не из доверенных 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 письму, переданному Клиентом на бумажном носителе 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 3 настоящих Правил, руководствоваться Инструкцией по установке Системы ДБО (Приложения №№ 5 - 5а к настоящим Правилам);
- каждое уполномоченное лицо, имеющее доступ к Ключевым носителям, паролям и другой конфиденциальной информации, должно быть проинформировано об ответственности за разглашение конфиденциальной информации и подписать соответствующие обязательства;
- 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 и заблокировать Ключ ЭП/ Ключ PayControl;
- при увольнении Уполномоченного лица Клиента, имевшего технический доступ к секретному Ключу ЭП/ Ключу PayControl, обязательно проинформировать об этом Банк и заблокировать Ключ ЭП/ Ключ PayControl;
- при увольнении Уполномоченного лица, осуществлявшего обслуживание рабочей станции, используемой для работы с Системой ДБО, принять меры для обеспечения отсутствия вредоносных программ на компьютере;
- 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 обратиться в Банк и инициировать приостановление доступа к Системе ДБО в порядке, установленном Договором присоединения.

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:
 - а) Android 5.0 и выше;
 - б) 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 PlayMarket 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):
- а) средство распознавания радужной оболочки глаза;
 - б) средство распознавания отпечатка пальца или лица (TouchID, FaceID);
 - в) пароль длиной не менее 6 символов (включая буквы и цифры);
 - г) графический ключ;
 - д) 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:
 - а) обеспечение доверенной среды;
 - б) отсутствие удалённого управления;
 - с) 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 устанавливайте обновления для вашего Мобильного устройства и установленных на нём приложений. Установку производить только из авторизованных магазинов приложений (AppStore или PlayMarket 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 экстренного временного блокирования в Системе ДБО действия скомпрометированного Ключа ЭП необходимо оповестить об этом Банк любым доступным способом:
 - устно 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 приостановлении использования Системы ДБО должно быть подтверждено письменным Заявлением о компрометации, форма которого размещена на официальном сайте Банка (www.abr.ru);
 - дистанционно с использованием канала «Клиент-Банк Онлайн» посредством Сервиса информирования Банка о Компрометации или подозрениях на Компрометацию¹. Функционал доступен только Уполномоченным лицам Клиента с полномочиями единоличного исполнительного органа.
- При информировании Банка по телефону службы технической поддержки Системы ДБО, представитель Клиента (заявитель) должен сообщить наименование Клиента (владельца Счёта), свои ФИО и должность, а также ФИО и должность Уполномоченного лица Клиента, действие Ключа ЭП которого следует заблокировать.
- По факту обращения представителя Клиента (заявителя) Банк:
 - незамедлительно обеспечивает временную блокировку Ключа ЭП Уполномоченного лица Клиента в Системе ДБО;
 - при информировании по телефону незамедлительно обеспечивает совершение телефонного звонка Клиенту на номер телефона подтверждения экстренной блокировки Ключей ЭП в целях получения подтверждения необходимости блокировки Ключа ЭП Уполномоченного лица Клиента. Информация о номере телефона подтверждения экстренной блокировки Ключей ЭП указывается Клиентом в Заявлении о присоединении. В случае если Клиент не представил в Банк номер телефона подтверждения экстренной блокировки Ключей ЭП, приостановление действия (блокировка) Ключей ЭП Уполномоченных лиц Клиента на основании входящего телефонного звонка не осуществляется;
 - в случае если по факту телефонного звонка Клиенту подтверждение необходимости блокировки Ключа ЭП Уполномоченного лица Клиента не получено, снимает блокировку Ключа ЭП, заблокированного по факту поступления в Банк входящего телефонного звонка заявителя.
- 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/ Ключ PayControl/ доступ УЛ Клиента к Системе ДБО, прекращает приём и исполнение ЭД, подписанных скомпрометированным Ключом ЭП/ Ключом PayControl.

¹ Сервис доступен с момента технической реализации.

- в целях получения новых Аутентификационных данных и Ключевых носителей (USB-Токен), Генератора одноразовых кодов, MAC-токена ВІFІТ 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 пп. 16.3.2.1 настоящих Правил.
- генерацию новых Ключей ЭП Клиент осуществляет в соответствии с разделом 6 настоящих Правил.

Не вносить исправления, изменения или дополнения в специализированное программное обеспечение и техническую документацию, предоставленные Банком по Договору присоединения, 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 присоединения.

Требования, установленные настоящим Приложением, в случае использования Клиентом Канала «Интеграционный Клиент-Банк» распространяются на стороне Клиента на все рабочие места Клиента, которые участвуют в обмене ЭД с Банком с использованием Канала «Интеграционный Клиент-Банк».

При невыполнении или неполном выполнении требований настоящего Приложения к правилам по обеспечению информационной безопасности рабочих мест принимаю на себя риски возможных потерь (ущерба).

Инструкция по установке Системы «iBank»

(выдается при подписании Заявления о присоединении к Правилам при выборе Системы «iBank»)

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: 10.7 и выше;	
	Linux	Ubuntu и прочие deb-дистрибутивы (последние версии x64)	
Веб-браузер	Internet Explorer, Firefox, Opera, Safari, Chrome	Internet Explorer версия 11; 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/docs/client_doc.zip

– адрес для загрузки сервиса и документации «iBank для 1С»:

<https://ibank.abr.ru/docs/1C.zip>

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;

- Самостоятельно провести предварительную регистрацию в Системе «iBank», запустив программу предварительной регистрации на сайте <https://ibank.abr.ru> и сформировать Ключи ЭП;
- Заполнить и предоставить в Банк бланк Ключа проверки ЭП Клиента 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 № 5а

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

(выдается при подписании Заявления о присоединении к Правилам 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 x86иx64,	
	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 <https://online.abr.ru/ru/help/html/Basic/InstallCryptoPlugin.html> на сайте входа в Систему «ДБО BS-Client(CORREQTS)» в разделе «Как пользоваться системой» по адресу: <https://online.abr.ru/ru/help/html/Basic/InstallCryptoPlugin.html>.
 - 2.1.4. Сгенерировать ключи ЭП и отправить запрос на регистрацию Ключа проверки ЭП в Банк. 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 сайте 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 Банка (Канал доступа «Мобильный Бизнес-Клиент»).**

Для работы в Мобильном приложении Банка (Канал доступа «Мобильный Бизнес-Клиент» Клиент должен самостоятельно и за свой счёт обеспечить следующие минимальные технические, программные и коммуникационные ресурсы:

Требования к аппаратному и программному окружению. Клиентский модуль «Мобильный Бизнес-Клиент».

Требования к программному окружению.

Вид ПО	Наименование ПО	Поддерживаемые версии ПО	Примечания
ОС	Android	5.x – 10.x	
	iOS	11, 12, 13	

Требования к аппаратному обеспечению.

Любой современный мобильный телефон с операционной системой Android или iOS, доступом в интернет.

4. **Порядок установки Мобильного приложения Банка (Канал доступа «Мобильный Бизнес-Клиент»).**

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/>.
 - Для устройств с ОС iOS приложение ABR Бизнес Онлайн доступно для скачивания и установки в магазине AppStore.

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 аппаратному и программному окружению.

Требования к программному окружению.

Вид ПО	Наименование ПО	Поддерживаемые версии ПО	Примечания
ОС	Android	4.4 и выше	
	iOS	iOS 10 (arm64) и выше	

Требования к аппаратному обеспечению.

Любой современный мобильный телефон с операционной системой Android или iOS, 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».

Типовая форма Акта приема-передачи ключевых носителей, программного обеспечения и средств криптографической защиты информации»
(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. № _____, 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:				
<input type="checkbox"/> USB-Токен				
№ п/п	Наименование носителя	Учетный номер носителя	ФИО владельца (Уполномоченное лицо Клиента)	ФИО и подпись получателя

4. Устройства подтверждения:				
<input type="checkbox"/> Генератор одноразовых кодов _____, в кол-ве _____ шт.				
<input type="checkbox"/> MAC-токен VIFIT _____, 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».

Типовая форма Заявления на выезд специалиста Банка на территорию Клиента

(заполняется при выезде специалиста Банка по инициативе Клиента)

ЗАЯВЛЕНИЕ НА ВЫЕЗД СПЕЦИАЛИСТА БАНКА НА ТЕРРИТОРИЮ КЛИЕНТА

Клиент											
<i>указывается полное наименование организации, включая организационно-правовую форму / ФИО индивидуального предпринимателя / физического лица, занимающегося частной практикой</i>											
в лице											
действующий на основании											
ИНН											
НАСТОЯЩИМ ЗАЯВЛЕНИЕМ КЛИЕНТ ПРОСИТ предоставить услугу выезда специалиста Банка на территорию Клиента:											

Цель выезда:											
---------------------	--	--	--	--	--	--	--	--	--	--	--

Дата выезда специалиста (желаемая):	«		»		20		г.				
--	---	--	---	--	----	--	----	--	--	--	--

Адрес местонахождения											
------------------------------	--	--	--	--	--	--	--	--	--	--	--

Контактное (ответственное) лицо данные Клиента:															
Фамилия, Имя, Отчество (при наличии)															
Телефон	+	7	-					-					e-mail		

ПОДПИСЬ КЛИЕНТА

Клиент подтверждает достоверность сведений, содержащихся в настоящем Заявлении.

_____ Подпись _____ дата

МП

ОТМЕТКИ БАНКА

Настоящее Заявление принято _____
Дата

_____ подпись _____ фамилия, инициалы

Типовая форма Акта выполненных работ
(заполняется при выезде специалиста Банка на территорию
Клиента)

Акт выполненных работ

г. _____ «___» _____ 20__ г.

Настоящим подтверждается, что работник АО «АБ «РОССИЯ»

(ФИО и должность работника)

проводил следующие работы: _____

в _____
(наименование Клиента)

с _____ по _____ (итого полных _____ дней) _____ 20__ года.

Указанные работы приняты: _____
(должность и ФИО полностью сотрудника Клиента)

Настоящий Акт составлен в 2-х экземплярах, один для Банка, другой передается Клиенту.

Подписи Сторон

Банк

Клиент

МП

МП

Типовая форма Доверенности (на получателя)

Доверенность¹ №

г. _____

«__» _____ 20__ г.

Клиент			
<i>указывается полное наименование организации, включая организационно-правовую форму / ФИО индивидуального предпринимателя / физического лица, занимающегося частной практикой</i>			
в лице			
действующий на основании			
доверяет			
<i>(фамилия, имя, отчество лица, которому выдается доверенность)</i>			
данные документа, удостоверяющего личность:			
Тип документа		Серия, номер	Дата выдачи
Кем выдан		Код подразделения	
совершать все юридические действия, связанные с получением и обменом в			
<i>АО «АБ «РОССИЯ» / наименование филиала АО «АБ «РОССИЯ»</i>			
<input type="checkbox"/> программного обеспечения Клиентской части Системы ДБО, <input type="checkbox"/> средств криптографической защиты информации (СКЗИ) <input type="checkbox"/> Токенов (USB-Токен) <input type="checkbox"/> Устройств подтверждения			
а также сопутствующей документации, с правом подписания необходимых документов, в том числе акта приема-передачи ключевых носителей, программного обеспечения и средств криптографической защиты информации.			
Образец подписи			
<i>(подпись)</i>			
			удостоверяю.
<i>(фамилия, имя, отчество лица, которому выдается доверенность)</i>			
Настоящая доверенность действует до	«__»	20__	г. включительно.
<i>МП</i>	<i>(наименование должности руководителя)</i>	<i>(подпись)</i>	<i>(фамилия, инициалы)</i>

¹ В соответствии с п. 3 ст. 187 ГК РФ Доверенность, выдаваемая в порядке передоверия, т.е. лицом, действующим на основании доверенности, должна быть нотариально удостоверена.

Типовая форма Акта возврата средств
криптографической защиты информации

(оформляется при расторжении (отказе от) Договора
присоединения/ смене Уполномоченных лиц Клиента в случае
наличия у Клиента СКЗИ, полученных в Банке)

Акт возврата средств криптографической защиты информации¹

г. _____ « ____ » _____ 20__ г.

В соответствии с Договором № _____ 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 присоединения.

Подписи Сторон

Банк

Клиент

МП

МП

¹ 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 № 11

Типовая форма Заявления о расторжении Договора ДБО
(предоставляется при отказе от Договора ДБО по инициативе Клиента в случае обслуживания без открытия Счета)

ЗАЯВЛЕНИЕ О РАСТОРЖЕНИИ ДОГОВОРА ДБО

Клиент	
	<small>указывается полное наименование организации, включая организационно-правовую форму / ФИО индивидуального предпринимателя / физического лица, занимающегося частной практикой</small>
в лице	
действующий на основании	
ИНН	
НАСТОЯЩИМ ЗАЯВЛЕНИЕМ КЛИЕНТ ПРОСИТ прекратить предоставление услуг с использованием Системы ДБО и расторгнуть Договор ДБО.	

ПОДПИСЬ КЛИЕНТА

Клиент подтверждает достоверность сведений, содержащихся в настоящем Заявлении.

Подпись

дата

МП

ОТМЕТКИ БАНКА

Настоящее Заявление принято _____.

Дата

подпись

фамилия, инициалы

Перечень электронных документов, используемых в Системе ДБО, использование ЭП в зависимости от типа ЭД.

**Перечень¹
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» или «Клиент-Банк»:

Тип документа	Возможность использования подписи			Порядок подписания Клиентом
	ПЭП PayControl	УНЭП	УКЭП	
Платежное поручение	да	да	да	Кол-во подписей устанавливается Клиентом в Заявлении о присоединении / Заявлении об изменении данных
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	
Заявка на выдачу наличных денежных средств (Заявление на выдачу наличных денег/ Заявка на наличные)	да	да	да	
Заявление на размещение депозита /возврат депозита	да	да	да	1 подпись
Заявление на возврат депозита	да	да	да	
Заявление на пополнение депозита	да	да	да	
Заявление на частичный возврат депозита	да	да	да	
Заявление о поддержании НСО	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	
Заявка на выдачу наличных денежных средств (Заявление на выдачу наличных денег/ Заявка на наличные)	да	да	да	

¹Перечень документов по мере расширения функционала Системы ДБО может изменяться, дополняться.

Тип документа	Возможность использования подписи			
	ПЭП PayControl	УНЭП	УКЭП	Порядок подписания Клиентом
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	
Запрос на получение справки	да	да	да	
Заявка на подключение к услуге «Размещение депозитов посредством Системы ДБО»	да	да	да	1 подпись (единоличный исполнительный орган Клиента/индивидуального предпринимателя или лицо им уполномоченное на заключение договоров)
Заявление на изменение перечня уполномоченных лиц по сделкам НСО и депозитов	да	да	да	1 подпись
Заявка на Банковскую карточку	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 SWIFT-сообщения в формате MT 940 / MT 942)	формализованный	Формируется АБС и отправляется шлюзом (без подписи Банка) / 1 ЭП уполномоченного лица Банка
2.	Справка о подтверждающих документах, обработанная Банком	формализованный	
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	произвольный	

№п /п	Электронный документ	Вид ЭД	Порядок подписания Банком
	средств на счете (счетах), о наличии/отсутствии картотеки/ очереди распоряжений к счету/ счетам) - ЭСИД «Письмо»		

3. Электронные документы, направляемые в Банк и получаемые из Банка с использованием Канала «Интеграционный Клиент-Банк»²:

3.1. 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».

3.2. 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-Банк» и на странице входа в Систему ДБО, которая доступна через раздел «Вход в Интернет-Банк» (окно входа в Систему ДБО).

3.3. Модуль «Интеграционный Корпоративный шлюз» системы ДБО «BS-Client (CORREQTS)».

Стандарты обмена и форматы передаваемых документов определены пользовательской документацией, которая размещена на сайте банка по адресу: www.abr.ru в разделе «Интеграционный Клиент-Банк».

² Перечень документов по мере расширения функционала модулей Системы ДБО может изменяться, дополняться.

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

1. Используемые термины и определения

- 1.1. **Акцепт (бюджетирование)** – режим работы модуля «Центр финансового контроля/Расчётный центр Корпорации» (далее – модуль ЦФК/РЦК) Системы ДБО, позволяющий Контролирующей организации осуществлять финансовый контроль деятельности посредством:
- авторизованного 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 (бюджетирование)» может быть подключена опция многоуровневый акцепт, позволяющая 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 (бюджетирования) 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 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.
- 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 (бюджетирования)), Мониторинга, Управления счетами).
- 1.5. **Справочник статей /Справочник Кодов Бюджетного Классификатора (КБК)** - перечень кодов расходных статей (платежей)/ перечень кодов статей бюджета Клиента¹.

¹ При подключении модуля ЦФК/РЦК в зависимости от типа используемой Системы ДБО.

- 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 ЦФК/РЦК, 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 (бюджетирование), формировать, подписывать и передавать на исполнение в Банк ЭПД по Счетам Подконтрольных организаций в режиме «Управление счетами» осуществляется на основании Заявления о предоставлении модуля ЦФК/РЦК Контролирующей организации.
В случае осуществления контроля за движением денежных средств по счетам Подконтрольных организаций (режим Мониторинг, Акцепт (бюджетирование), Управление счетами) необходимо предоставление Согласия на регистрацию счетов в модуле ЦФК/РЦК по форме Приложения № 1 к Заявлению о предоставлении модуля ЦФК/РЦК (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 ЦФК/РЦК Контролирующей организации с отметкой Банка о приеме.
- 2.3. Предоставление Клиентам – Контролирующей и Подконтрольным организациям модуля ЦФК/РЦК осуществляется по месту обращения Клиента или по месту обслуживания Счета.
- 2.4. Использование модуля РЦК Контролирующей организацией осуществляется совместно с Системой ДБО «BS-Client (CORREQTS)».
Использование модуля ЦФК Контролирующей организацией возможно, как с одновременным подключением Системы iBank, так и без её подключения. При использовании Контролирующей организацией модуля ЦФК совместно с Системой iBank требуется выпуск второго Ключа ЭП Уполномоченным лицам, которые будут дополнительно работать в Системе iBank.
- 2.5. Готовность Сторон к работе в модуле ЦФК/РЦК оформляется подписанием Акта сдачи-приемки работ по подключению к модулю ЦФК/РЦК Системы ДБО (Приложение № 1 к настоящему Приложению) между Банком и Контролирующей организацией.
- 2.6. С использованием модуля ЦФК/РЦК предоставляются следующие возможности:
- 2.6.1. **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.
- 2.6.2. **Акцепт (бюджетирование)** – дополнительно подключаемый к Мониторингу режим работы, позволяющий Контролирующей организации устанавливать правила и критерии контроля для акцепта платежей.
- 2.6.2.1. Контролирующей организации в модуле ЦФК в режиме «Финансовый контроль», в модуле РЦК в меню «Оперативное управление / Расходы / Уведомление о лимитах» доступны следующие настройки:
- установка акцепта Контролирующей организацией всех ЭПД Подконтрольных организаций;
 - установка многоуровневого акцепта ЭПД Подконтрольных организаций;
 - настройка специальных критериев контроля / совокупности критериев контроля обязательных для проверки, 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).

- 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 на официальном сайте Банка в сети Интернет www.abg.ru 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).

2.6.2.2. Осуществление контроля исполнения бюджета / лимита обеспечивается Банком путём проверки на превышение 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.

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

2.6.2.4. Особенности работы с критериями контроля:

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

2.6.2.5. ЭПД по Контролируемым счетам в рамках режима работы Акцепт (бюджетирование) поступают в Банк после прохождения проверки на соответствие критериям контроля, определенным Контролирующей организацией, или после осуществления акцепта Уполномоченным лицом Контролирующей организации.

2.6.2.6. В рамках работы в режиме Акцепт (бюджетирование) Клиент поручает Банку:

- предоставить Уполномоченным лицам, указанным в Заявлении о предоставлении модуля ЦФК/РЦК Контролирующей организации, доступ для просмотра информации об операциях по Контролируемым счетам, устанавливать правила и критерии контроля для акцепта платежей, а также осуществлять акцепт ЭПД на проведение расходных операций по счетам.
- принимать к исполнению ЭПД по Контролируемым счетам при условии получения согласия (акцепта) Уполномоченного лица Контролирующей организации и/или кода статьи /кода КБК. 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 присоединения.

2.6.3. **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.

- 2.6.3.1. 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.
 - 2.6.3.2. Регистрация Ключей ЭП осуществляется в соответствии с процедурами, определёнными в Правилах.
 - 2.6.3.3. 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).
 - 2.6.3.4. Подконтрольная организация получает информацию о ЭПД, созданных, подписанных и переданных на исполнение в Банк Уполномоченными лицами Контролирующих организаций путём формирования Выписки по своим счетам.
- 2.7. В случае необходимости изменения параметров предоставления модуля ЦФК/РЦК:
- 2.7.1. Изменение режимов работы модуля ЦФК/РЦК, данных по Уполномоченным лицам, перечня Контролируемых счетов осуществляется на основании Заявления о предоставлении модуля ЦФК/РЦК Контролирующей организации. Если Контролируемые счета принадлежат Подконтрольной организации, то необходимо предоставление Согласия на регистрацию счетов от Подконтрольной организации, чей счёт регистрируется / исключается из перечня Контролируемых счетов.
 - 2.7.2. Исключение закрываемого счета из перечня зарегистрированных в модуле ЦФК/РЦК счетов осуществляется на основании заявления на закрытие счёта. Предоставление в Банк Заявления о предоставлении модуля ЦФК/РЦК Контролирующей организации, Согласия на регистрацию счетов не требуется.
- 2.8. При отказе Контролирующей организацией от использования модуля ЦФК/РЦК, отключение зарегистрированных в модуле ЦФК/РЦК Контролируемых счетов осуществляется Банком на основании предоставленного Контролирующей организацией Заявления о предоставлении модуля ЦФК/РЦК, содержащего отметку об отключении модуля ЦФК/РЦК.

Приложение № 1
к Условиям предоставления услуг с использованием
модуля «Центр финансового контроля / Расчётный
центр корпорации» в АО «АБ «РОССИЯ»
(подписывается с Контролирующей организацией)

**АКТ сдачи-приёмки работ по подключению к модулю ЦФК/РЦК
Системы ДБО**

г. _____ «____» _____ 20__ г.

АО «АБ «РОССИЯ», именуемый в дальнейшем «Банк», в лице _____, действующего на основании _____, с одной Стороны, и _____, именуемое в дальнейшем «Клиент», в лице _____, действующего на основании _____, с другой Стороны составили настоящий Акт о том, что Банком проведены мероприятия по подключению Клиента к модулю ЦФК/РЦК Системы ДБО _____.
(указать наименование Системы ДБО)

Настоящий Акт составлен в 2-х экземплярах, имеющих равную юридическую силу, по одному для каждой из Сторон и является неотъемлемой частью Договора № _____

Подписи Сторон

Банк

Клиент

_____/_____/

_____/_____/

МП

МП

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											
<i>указывается полное наименование организации, включая организационно-правовую форму / ФИО индивидуального предпринимателя / физического лица, занимающегося частной практикой</i>											
в лице											
действующий на основании											
ИНН											
НАСТОЯЩИМ ЗАЯВЛЕНИЕМ КЛИЕНТ ПРОСИТ:											

1. ПРИ ОСУЩЕСТВЛЕНИИ ДИСТАНЦИОННОГО БАНКОВСКОГО ОБСЛУЖИВАНИЯ:
 подключить модуль ЦФК/РЦК Системы ДБО (выбрать Систему ДБО):
 «ДБО BS-Client (CORREQTS)» (модуль РЦК) «iBank» (модуль ЦФК)
 отключить модуль ЦФК/РЦК Системы ДБО

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 телефона или адреса электронной почты

ФИО (полностью)	Действия		Полномочия		Ключ ЭП (выбрать один вариант)	Вариант защиты системы и подтверждения исполнения документов (нужное отметить)		Срок полномочий (в соответствии с доверенностью / Уставом)		
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
	<input type="checkbox"/>	подключить УЛ	<input type="checkbox"/>	просмотр ¹	<input type="checkbox"/>	USB-Токен	Обязательное подтверждение исполнения платежного документа ² :		<input type="checkbox"/>	по _____
	<input type="checkbox"/>	отключить УЛ	<input type="checkbox"/>	акцепт (бюджетирование)	<input type="checkbox"/>	дополнительный USB-Токен	<input type="checkbox"/>	SMS-сообщение на номер +7 _____		
	<input type="checkbox"/>	изменить данные	<input type="checkbox"/>	группа 1 ²	<input type="checkbox"/>	действующий Ключ ЭП	<input type="checkbox"/>	Устройство подтверждения ³		
e-mail и номер телефона для направления Логина и Пароля ⁴ _____ @_____ +7 _____	<input type="checkbox"/>	блокировать Ключ ЭП	<input type="checkbox"/>	группа 2 ²	<input type="checkbox"/>	ключ ЭП стороннего УЦ			<input type="checkbox"/>	не ограничен
	<input type="checkbox"/>	изменить Пароль								

ФИО (полностью)	Действия		Полномочия		Ключ ЭП (выбрать один вариант)	Вариант защиты системы и подтверждения исполнения документов (нужное отметить) / Номер телефона УЛ		Срок полномочий (в соответствии с доверенностью / Уставом)		
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
	<input type="checkbox"/>	подключить УЛ	<input type="checkbox"/>	просмотр ¹	<input type="checkbox"/>	USB-Токен	Обязательное подтверждение исполнения платежного документа ² :		<input type="checkbox"/>	по _____
	<input type="checkbox"/>	отключить УЛ	<input type="checkbox"/>	акцепт (бюджетирование)	<input type="checkbox"/>	дополнительный USB-Токен	<input type="checkbox"/>	SMS-сообщение на номер +7 _____		
	<input type="checkbox"/>	изменить данные	<input type="checkbox"/>	группа 1 ²	<input type="checkbox"/>	действующий Ключ ЭП	<input type="checkbox"/>	Устройство подтверждения ³		
e-mail и номер телефона для направления Логина и Пароля ⁴ _____ @_____ +7 _____	<input type="checkbox"/>	блокировать Ключ ЭП	<input type="checkbox"/>	группа 2 ²	<input type="checkbox"/>	ключ ЭП стороннего УЦ			<input type="checkbox"/>	не ограничен
	<input type="checkbox"/>	изменить Пароль								

¹ Применяется при выборе режима работы Мониторинг
² Применяется при выборе режима работы Управление счетами в модуле ЦФК
³ Разрешено использование устройств: ключ OTP eToken Pass Event (в системе «ДБО BS-Client (CORREQTS)») и MAC-токен BIFIT (в системе «iBank»)
⁴ Для «ДБО BS-Client (CORREQTS)».

+7 _____@_____	<input type="checkbox"/>	изменить Пароль								
ФИО (полностью)	Действия		Полномочия		Ключ ЭП (выбрать один вариант)		Вариант защиты системы и подтверждения исполнения документов (нужное отметить) / Номер телефона УЛ		Срок полномочий (в соответствии с доверенностью / Уставом)	
	<input type="checkbox"/>	подключить УЛ	<input type="checkbox"/>	просмотр ¹	<input type="checkbox"/>	USB-Токен	Обязательное подтверждение исполнения платежного документа ² :		<input type="checkbox"/>	по _____
	<input type="checkbox"/>	отключить УЛ	<input type="checkbox"/>	акцепт (бюджетирование)	<input type="checkbox"/>	дополнительный USB-Токен	<input type="checkbox"/>	SMS-сообщение на номер +7 _____		
	<input type="checkbox"/>	изменить данные	<input type="checkbox"/>	группа 1 ²	<input type="checkbox"/>	действующий Ключ ЭП	<input type="checkbox"/>	Устройство подтверждения ³		
e-mail и номер телефона для направления Логина и Пароля⁴	<input type="checkbox"/>	блокировать Ключ ЭП	<input type="checkbox"/>	группа 2 ²	<input type="checkbox"/>	ключ ЭП стороннего УЦ			<input type="checkbox"/>	не ограничен
_____@_____ +7 _____	<input type="checkbox"/>	изменить Пароль								

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 в⁵ _____

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

Наименование организации и – владельца счета (ИНН)	Номер счета	Добавить	Исключить	Мониторинг	Акцепт (бюджетирование)	Управление счетам и (ЦФК)
		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

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, лит. А, 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.

ПОДПИСЬ КЛИЕНТА

Клиент подтверждает достоверность сведений, содержащихся в настоящем Заявлении о предоставлении модуля ЦФК/РЦК Системы ДБО.

_____ дата _____

подпись _____

МП _____

ОТМЕТКИ БАНКА

Настоящее Заявление о предоставлении модуля ЦФК/РЦК Системы ДБО принято _____ дата _____

⁵ 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.

ПОДПИСЬ

ФИО

УСЛОВИЯ предоставления сервиса подключения Канала «Интеграционный Клиент- Банк»

1. Банк предоставляет Клиенту Сервис подключения Канала «Интеграционный Клиент-Банк» с целью интеграции Учетной системы Клиента с Системой ДБО посредством:
 - интеграции с системой 1С (Сервис «Обмен с 1С по 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» - для работы в «CORREQTS» - представляет собой сервис, функционирующий на стороне Банка, и обеспечивающий возможность взаимодействия с Системой ДБО непосредственно из внешней Учетной системы.

2. Клиенту доступна возможность подключения и отключения сервиса интеграции Учетной системы Клиента в Системе ДБО посредством направления заявления на подключение / отключение сервиса, автоматически формируемого в электронном виде и подписываемого ЭП Клиента. Подача электронного заявления на услугу осуществляется в следующих модулях Системы ДБО:

Модуль «Электронный офис» Системы «ДБО BS-Client «CORREQTS»	Модуль «Управление услугами» Системы «iBank»
<i>Интеграция с системой 1С (Сервис «Обмен с 1С по DirectBank»)</i>	
• Подключение 1С Direct bank (Обмен с 1С по Directbank)	• Direct bank+
<i>Интеграция с модулем «Корпоративный автоклиент»</i>	
-	• Корпоративный автоклиент
<i>Интеграция с модулем «Интеграционный корпоративный шлюз»</i>	
• Интеграционный Клиент-Банк	-

3. Необходимым условием для предоставления Банком Канала «Интеграционный Клиент-Банк» является:
 - наличие у Клиента подключённого Канала «Клиент-Банк Онлайн»;
 - наличие открытого в Банке Счета;
 - подача в модуле «Электронный офис» / «Управление услугами» заявления на подключение сервиса.
4. При использовании Канала «Интеграционный Клиент-Банк» Банк не несёт ответственность за задержку и сбой при обмене документами с Учётной системой Клиента, возникающие в сервисах интернет-провайдеров или Учётной системе Клиента, за убытки Клиента, которые могут возникнуть в силу приостановления предоставления сервиса интеграции по причине неработоспособности Учётной системы Клиента.
5. Особенности работы посредством интеграции с системой 1С:
- 5.1. Использование определенного типа ЭП Уполномоченным лицом Клиента:

в ДБО «BS-Client «CORREQTS»	в «iBank»
Необходим УКЭП, выпущенный УЦ	Необходим УНЭП, выданный Банком

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

Система «ДБО BS-Client «CORREQTS»	Система «iBank»
<p>Доступна стандартная функциональность услуги «1С Directbank», позволяющая осуществлять:</p> <ul style="list-style-type: none"> • 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 	<p>Доступна расширенная функциональность с использованием модуля «iBank для 1С» («Стандартный» или «Премиум»), которая дополнительно позволяет использовать:</p> <ul style="list-style-type: none"> • механизм дополнительного подтверждения платежных поручений (средства подтверждения: Устройство подтверждения, Код подтверждения в SMS); • справочник «Доверенные получатели» в платежных документах

5.3. Настройка Клиентом прямого обмена по технологии DirectBank или с использованием дополнительного модуля «iBank для 1С» в системе «1С» 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».

6. Особенности интеграции с Учётной системой Клиента отличной от платформы «1С». В зависимости от используемой Клиентом Системы ДБО может осуществляться двумя способами:

6.1. 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 Учётной системы Клиента с банковским сервером Системы «iBank». Настройка работы модуля 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».

6.2. С использованием модуля «Интеграционный Корпоративный Шлюз» Системы «ДБО BS-Client (CORREQTS)».

6.2.1. При подключении к модулю «Интеграционный Корпоративный Шлюз» Клиенту необходимо выполнить следующие условия:

- самостоятельно осуществить доработку Учётной системы в соответствии с требованиями Банка к схеме подключения и форматам передаваемых документов, поддерживаемых в рамках модуля «Интеграционный Корпоративный Шлюз»;
- согласовать форматы передаваемых документов и подтвердить готовность к проведению тестирования предложенных форматов обмена данными путем направления по электронной почте ответного сообщения на сообщение Банка, содержащее спецификацию и форматы обмена данными;
- провести тестирование в части взаимодействия Учётной системы и Системы ДБО на стороне Банка с участием представителя Банка с учётом согласованной Сторонами спецификации обмена, которая может быть изменена по соглашению Сторон.

По факту завершения тестирования Банк уведомляет/ направляет уведомление Клиенту по Системе ДБО о факте/ дате подключения модуля, что является основанием для взимания комиссионного вознаграждения в соответствии с Тарифами Банка.

ЗАЯВЛЕНИЕ О КОМПРОМЕТАЦИИ

Клиент		
<small>указывается полное наименование организации, включая организационно-правовую форму / ФИО индивидуального предпринимателя / физического лица, занимающегося частной практикой</small>		
в лице		
действующий на основании		
ИНН		
НАСТОЯЩИМ ЗАЯВЛЕНИЕМ КЛИЕНТ уведомляет о Компрометации в соответствии с требованиями Договора присоединения и просит Банк		
совершить следующие действия в отношении Уполномоченного лица		

(указать ФИО всех УЛ, в отношении которых выявлены случаи Компрометации)

(выбрать нужное)

<input type="checkbox"/>	заблокировать Ключ ЭП, указать идентификатор Ключа проверки ЭП ¹	
<input type="checkbox"/>	заблокировать Ключ PayControl	
<input type="checkbox"/>	отключить УЛ	
<input type="checkbox"/>	исключить Мобильное устройство из перечня доверенных (при использовании ПЭП PayControl)	
<input type="checkbox"/>	выдать новый USB-Токен	
<input type="checkbox"/>	изменить Пароль	
<input type="checkbox"/>	выдать Ключи инициализации PayControl (при использовании ПЭП PayControl)	
<input type="checkbox"/>	выдать новое Устройство подтверждения	

ПОДПИСЬ КЛИЕНТА

Клиент подтверждает достоверность сведений, содержащихся в настоящем Заявлении о компрометации.

подпись

дата

МП

ОТМЕТКИ БАНКА

Настоящее Заявление принято _____.

дата

Подпись

фамилия, инициалы

¹ 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»

**ЗАЯВЛЕНИЕ ОБ УСТАНОВЛЕНИИ / СНЯТИИ ОГРАНИЧЕНИЙ
 на работу в Системе ДБО**

Клиент	
указывается полное наименование организации, включая организационно-правовую форму / ФИО индивидуального предпринимателя / физического лица, занимающегося частной практикой	
в лице	
действующий на основании	
ИНН	
<p>НАСТОЯЩИМ ЗАЯВЛЕНИЕМ КЛИЕНТ при осуществлении дистанционного банковского обслуживания ПРОСИТ установить следующие ограничения в Системе ДБО:</p>	

Варианты ограничений	ФИО УЛ
<input type="checkbox"/> Разрешить подписывать платежные поручения к счету (-ам) только указанным УЛ. № _____ № _____ (указать счет (а))	_____ (указать ФИО УЛ) _____ указать ФИО УЛ) _____ (указать ФИО УЛ)
№ _____ № _____ (указать счет (а))	_____ (указать ФИО УЛ) _____ указать ФИО УЛ) _____ (указать ФИО УЛ)
№ _____ № _____ (указать счет (а))	_____ (указать ФИО УЛ) _____ указать ФИО УЛ) _____ (указать ФИО УЛ)
<input type="checkbox"/> Акцепт (визирование) операций по счету (-ам) № _____ № _____ № _____ № _____ № _____ (указать счета)	_____ (указать ФИО УЛ) _____ указать ФИО УЛ) _____ (указать ФИО УЛ) _____ (указать ФИО УЛ)
<input type="checkbox"/> Ограничить максимальную сумму платежа* <input type="checkbox"/> на одну операцию (одно платежное поручение) и/или <input type="checkbox"/> на сумму платежей за один Операционный день _____ (руб.) (указать максимальную сумму платежа прописью)	_____ (указать ФИО УЛ) _____ указать ФИО УЛ) _____ (указать ФИО УЛ) _____ (указать ФИО УЛ)
<input type="checkbox"/> Подключить возможность устанавливать в Системе ДБО перечень получателей денежных средств.	
<input type="checkbox"/> Снять все ранее установленные ограничения	

*Ограничения для ДБО iBank устанавливаются на Клиента в целом, заполнять поле с указанием ФИО не требуется.

ПОДПИСЬ КЛИЕНТА

Клиент подтверждает достоверность сведений, содержащихся в настоящем Заявлении об установлении/снятии ограничений.

_____ подпись

_____ дата

МП

ОТМЕТКИ БАНКА

Настоящее Заявление принято

дата

подпись

фамилия, инициалы

Типовая форма Заявления о предоставлении третьим лицам выписки по счетам Клиента

(предоставляется головной организацией – получателем выписок и организацией – владельцем счета)

ЗАЯВЛЕНИЕ О ПРЕДОСТАВЛЕНИИ ТРЕТЬИМ ЛИЦАМ ВЫПИСКИ ПО СЧЕТАМ КЛИЕНТА

Клиент			
	<i>указывается полное наименование организации, включая организационно-правовую форму / ФИО индивидуального предпринимателя / физического лица, занимающегося частной практикой</i>		
в лице			
действующий на основании			
ИНН			
НАСТОЯЩИМ ЗАЯВЛЕНИЕМ КЛИЕНТ ПРОСИТ в рамках оказания услуги «Предоставление третьим лицам выписки по счетам Клиента» ² совершить следующие действия:			
Подключить услугу	Изменить параметры	Отключить услугу	
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

1. ОРГАНИЗОВАТЬ РАБОТУ СО СЛЕДУЮЩИМИ СЧЕТАМИ путем предоставления информации по счетам Клиента - головной организации

(указать наименование, организационно-правовую форму, ИНН Головной организации)

(при необходимости добавить строки)

Наименование организации – владельца счета (ИНН)	Номер счета	Добавить счет	Исключить счет
		<input type="checkbox"/>	<input type="checkbox"/>
		<input type="checkbox"/>	<input type="checkbox"/>
		<input type="checkbox"/>	<input type="checkbox"/>

Настоящим Заявлением Клиент – владелец счета выражает согласие на предоставление информации по своим счетам, указанным в настоящем пункте, Контролирующей организации. Предоставление информации уполномоченному представителю Контролирующей организации рассматривается как предоставление информации Уполномоченному лицу Клиента (п. 4 ст. 185 ГК РФ)

ПОДПИСЬ КЛИЕНТА

Клиент подтверждает достоверность сведений, содержащихся в настоящем Заявлении.

_____ дата

_____ подпись

МП

ОТМЕТКИ БАНКА

Настоящее Заявление принято _____ дата _____

_____ подпись _____ фамилия, инициалы

²При подключении услуги предоставления выписки третьим лицам заполнение раздела следует осуществлять с учетом следующего:

- при подаче заявления организацией, дающей согласие на предоставление выписки по своим счетам третьему лицу, заполняются данные о номере(-ах) банковского (-их) счета (-ов) и проставляется отметка о добавлении счета, по которому необходимо предоставление выписки. Данная организация в обязательном порядке предоставляет согласие на передачу сведений третьему лицу путем заполнения раздела о согласии в настоящем пункте.
- при подаче заявления организацией, запрашивающей получение выписки по счетам третьего лица, заполняются данные о номере(-ах) банковского (-их) счета (-ов), проставляется отметка о добавлении счета, по которому необходимо предоставление выписки, указываются наименования юридических лиц, по счетам которых требуется предоставление выписки.

При оказании услуги с использованием Канала доступа «Интеграционный Клиент-Банк» Системы «ДБО BS-Client (CORREQTS)» его подключение осуществляется посредством модуля «Электронный офис» организацией, запрашивающей получение выписки по счетам третьего лица.

Приложение № 19
Бланк Ключа проверки электронной подписи сотрудника
Клиента в Системе «iBank»

КЛЮЧ ПРОВЕРКИ ЭЛЕКТРОННОЙ ПОДПИСИ СОТРУДНИКА КЛИЕНТА В СИСТЕМЕ «iBank»

1. Наименование организации _____
2. Место нахождения юр. лица _____
3. ОГРН _____ дата внесения в ЕГРЮЛ (ЕГРИП) «__» _____ года
4. Тел. _____ 5. ИНН (КИО) _____ 6. КПП _____
7. Факс* _____ 8. E-mail* _____
9. Сведения о владельце ключа
 Фамилия, Имя, Отчество _____
 Должность _____
 Документ, удостоверяющий личность _____, серия _____
 номер _____, дата выдачи «__» _____ г,
 кем выдан _____
10. Примечания* _____
* обязательно для заполнения

Ключ проверки ЭП сотрудника Клиента

Идентификатор ключа проверки ЭП _____ Идентификатор ключевого носителя _____
Наименование криптосредств _____
Алгоритм ГОСТ Р 34.10-2012 ID набора параметров алгоритма 1.2.643.7.1.1.1.1
Дата начала действия «__» _____ 20__ г. (заполняется Банком)
Дата окончания действия «__» _____ 20__ г. (заполняется Банком)
Представление Ключа проверки ЭП в шестнадцатеричном виде
XX
XX
XX
XX
Личная подпись Владельца ключа проверки ЭП
[]
Ключ проверки ЭП Клиента действует в рамках
Договора присоединения от «__» _____ 20__ г. № _____

Достоверность приведенных данных подтверждаю Уполномоченный представитель Банка

Руководитель организации

Оттиск печати

Оттиск печати
Банка

/ /
Дата приема ключа проверки ЭП
«__» _____ 20__ г.

Приложение № 19а

Рекомендации по заполнению Бланка Ключа проверки
электронной подписи сотрудника Клиента в Системе
«iBank»

**Рекомендации по заполнению Бланка Ключа проверки электронной подписи сотрудника Клиента
в Системе «iBank»**

Ключ проверки ЭП сотрудника Клиента в Системе ДБО (далее – Ключ проверки ЭП) – бумажный документ, предназначенный для аутентификации сотрудников Клиента, имеющих право работы с документами по Системе ДБО.

При оформлении аналога сертификата Ключа проверки ЭП часть сведений «предзаполняется» Банком. Клиент должен в блоках информации, обведенных в примере жирной чертой, заполнить пустые поля:

КЛЮЧ ПРОВЕРКИ ЭЛЕКТРОННОЙ ПОДПИСИ СОТРУДНИКА КЛИЕНТА В СИСТЕМЕ «iBank»

1. Наименование организации _____	
2. Место нахождения юр. лица _____	
3. ОГРН _____	дата внесения в ЕГРЮЛ (ЕГРИП) “__” _____ года
4. Тел. _____	5. ИНН (КИО) _____
7. Факс* _____	8. E-mail* _____
9. Сведения о владельце ключа	
Фамилия, Имя, Отчество _____	
Должность _____	
Документ, удостоверяющий личность _____, серия _____	
номер _____, дата выдачи “__” _____ г.,	
кем выдан _____	
10. Примечания* _____	

* обязательно для заполнения

Ключ проверки ЭП сотрудника Клиента

Идентификатор ключа _____ Идентификатор ключевого носителя _____
 Наименование криптосредств _____
 Алгоритм ГОСТ Р 34.10-2012 ID набора параметров алгоритма 1.2.643.7.1.1.1.1 _____
 Дата начала действия «__» _____ 20__ г. (заполняется Банком)
 Дата окончания действия «__» _____ 20__ г. (заполняется Банком)

Представление Ключа проверки ЭП в шестнадцатеричном виде
 XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
 XXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
 XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
 XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

**Личная подпись владельца ключа
проверки ЭП**

Ключ проверки ЭП сотрудника действует в рамках
 Договора присоединения от «__» _____ 20__ г. № _____

Достоверность приведенных данных подтверждаю

Руководитель организации _____ / _____ /
 _____ / _____ /
подпись фио

Оттиск печати

Уполномоченный представитель Банка

_____/_____/_____/

Оттиск печати

Дата приема ключа проверки ЭП
 «__» _____ 20__ г.

Блок № 1 – блок общей информации об организации и владельце ключа.

В данном блоке указываются реквизиты организации – Клиента, а в случае если бланк Ключа ЭП оформляется для организации, выполняющей функции исполнительного органа Клиента – указываются реквизиты данной организации. Так же указываются персональные данные уполномоченного сотрудника Клиента, которому выдан Ключ ЭП.

Поля №№ 7, 8 – заполняются по желанию.

Поле № 10 – заполняется по желанию, но является обязательным для заполнения в случае, если бланк Ключа проверки ЭП оформляется для организации, выполняющей функции исполнительного органа Клиента. При этом в поле № 10 «Примечания» включается следующая фраза «с правом единоличного исполнительного органа в соответствии правоустанавливающими документами, предоставленными в Банк».

Остальные поля должны быть заполнены.

В поле № 3 должны быть указаны «ОГРН» и «дата внесения в ЕГРЮЛ (ЕГРИП)» – единый государственный реестр юридических лиц (единый государственный реестр индивидуальных предпринимателей).

Блок № 2

В поле «**Личная подпись**» необходимо поставить личную подпись **Владельца ключа проверки ЭП** (см. пункт № 9 – «Сведения о владельце ключа»).

В поле «**Достоверность приведённых данных подтверждаю**» указываются ФИО руководителя организации – Клиента, проставляется его подпись и оттиск печати.

Таким образом, на бланке Ключа проверки ЭП Клиентом должна быть заполнена следующая информация:

- полное наименование юридического лица;
- юридический адрес;
- номер ОГРН;
- дата внесения записи в ЕГРЮЛ (ЕГРИП);
- телефон;
- ИНН;
- КПП;
- факс (не обязательно);
- e-mail (не обязательно);
- сведения о владельце ключа – полностью;
- примечания (при наличии);
- личная подпись (подпись владельца ключа);
- подпись и ФИО руководителя юридического лица;
- оттиск печати юридического лица.

На бланке Ключа проверки ЭП работник Банка заполняет поля:

- номер договора;
- дата подписания договора;
- подпись и ФИО Уполномоченного представителя Банка;
- дата приёма Ключа проверки ЭП;
- оттиск печати Банка.

Приложение № 20
Бланк Ключа проверки электронной подписи сотрудника
клиента в Системе «ДБО «BS-Client» / «ДБО BS-
Client(CORREQTS)»

**КЛЮЧ ПРОВЕРКИ ЭЛЕКТРОННОЙ ПОДПИСИ СОТРУДНИКА КЛИЕНТА В СИСТЕМЕ «ДБО BS-Client»/
«ДБО BS-Client(CORREQTS)»**

1. Наименование организации _____
2. Юридический адрес _____
3. ОГРН _____ дата регистрации «__» _____ года
4. Тел. _____ 5. ИНН _____ 6. КПП _____
7. Факс* _____ 8. E-mail* _____
9. Сведения о владельце ключа
Фамилия, Имя, Отчество _____
Дата и место рождения «__» _____ г. _____
Должность _____
Документ, удостоверяющий личность _____, серия _____
номер _____, дата выдачи «__» _____ г.,
кем выдан _____
10. Примечания* _____
- * обязательно для заполнения

Ключ проверки ЭП сотрудника клиента

Идентификатор ключа _____

Идентификатор ключевого носителя _____

Наименование криптосредств _____

Алгоритм ГОСТ Р34.10-2012 ID набора параметров алгоритма _____

Дата начала действия «__» _____ 20__ г. (заполняется банком)

Дата окончания действия «__» _____ 20__ г. (заполняется банком)

Представление ключа проверки ЭП в шестнадцатеричном виде

**Личная подпись владельца
ключа проверки ЭП**

Ключ проверки ЭП клиента действует в рамках

Договора присоединения от «__» _____ 20__ г. № _____

Достоверность приведенных данных подтверждаю

Уполномоченный представитель банка

Руководитель организации

_____/_____
подпись / ФИО

_____/_____
подпись / ФИО

Оттиск печати

Оттиск печати

Дата приема
ключа проверки ЭП
«__» _____ 20__ г.

Приложение № 20а
Рекомендации по заполнению Бланка Ключа
проверки электронной подписи сотрудника клиента
в Системе «ДБО BS-Client»/«ДБО BS-Client
CORREQTS»

**Рекомендации по заполнению Бланка Ключа проверки электронной подписи сотрудника
клиента в Системе «ДБО BS-Client» / «ДБО BS-Client(CORREQTS)»**

Ключ проверки ЭП сотрудника Клиента в Системе ДБО (далее – Ключ проверки ЭП) – бумажный документ, предназначенный для аутентификации сотрудников Клиента, имеющих право работы с документами по Системе ДБО.

При оформлении аналога сертификата Ключа проверки ЭП часть сведений «предзаполняется» Банком. Клиент должен в блоках информации, обведенных в примере жирной чертой, заполнить пустые поля:

КЛЮЧ ПРОВЕРКИ ЭЛЕКТРОННОЙ ПОДПИСИ СОТРУДНИКА КЛИЕНТА В СИСТЕМЕ «ДБО BS-Client» / «ДБО BS-Client(CORREQTS)»

1. Наименование организации _____
2. Место нахождения юр. лица _____
3. ОГРН _____ дата внесения в ЕГРЮЛ (ЕГРИП) “__” _____ года
4. Тел. _____ 5. ИНН (КИО) _____ 6. КПП _____
7. Факс* _____ 8. E-mail* _____
9. Сведения о владельце ключа Фамилия, Имя, Отчество _____ Должность _____ Документ, удостоверяющий личность _____, серия _____ номер _____, дата выдачи “__” _____ г., кем выдан _____
10. Примечания* _____

* обязательно для заполнения

Ключ проверки ЭП сотрудника Клиента

Идентификатор ключа _____ Идентификатор ключевого носителя _____
Наименование криптосредств _____
Алгоритм ГОСТ Р34.10-2012 ID набора параметров алгоритма _____
Дата начала действия «__» _____ 20__ г. (заполняется Банком)
Дата окончания действия «__» _____ 20__ г. (заполняется Банком)
Представление Ключа проверки ЭП в шестнадцатеричном виде

PublicKey:

pub:

Parameters OID:

Ключ проверки ЭП сотрудника действует в рамках
Договора присоединения от «__» _____ г. № _____

Личная подпись владельца ключа ЭП

Достоверность приведенных данных подтверждаю

Руководитель организации

_____ / _____

подпись

фио

Оттиск печати

Уполномоченный представитель Банка

_____ / _____

подпись

фио

Дата приема

ключа проверки ЭП

«__» _____ 20__ г.

Оттиск печати

Блок № 1 – блок общей информации об организации и владельце ключа.

В данном блоке указываются реквизиты организации – Клиента, а в случае если бланк Ключа ЭП оформляется для организации, выполняющей функции исполнительного органа Клиента Банка - указываются реквизиты данной организации. Так же указываются персональные данные уполномоченного сотрудника Клиента, которому выдан Ключ ЭП.

Поля №№ 7, 8 – заполняются по желанию.

Поле № 10 – заполняется по желанию, но является обязательным для заполнения в случае, если бланк Ключа проверки ЭП оформляется для организации, выполняющей функции исполнительного органа Клиента. При этом в поле № 10 «Примечания» включается следующая фраза «с правом единоличного исполнительного органа в соответствии правоустанавливающими документами, предоставленными в Банк».

Остальные поля должны быть заполнены.

В поле № 3 должны быть указаны «ОГРН» и «дата внесения в ЕГРЮЛ (ЕГРИП)» – единый государственный реестр юридических лиц (единый государственный реестр индивидуальных предпринимателей).

Блок № 2

В поле «**Личная подпись**» необходимо поставить личную подпись **Владельца ключа проверки ЭП** (см. пункт № 9 – «Сведения о владельце ключа»).

В поле «**Достоверность приведённых данных подтверждаю**» указываются ФИО руководителя организации – Клиента, проставляется его подпись и оттиск печати Клиента.

Таким образом, в бланке Ключа проверки ЭП Клиентом должна быть заполнена следующая информация:

- полное наименование юридического лица;
- юридический адрес;
- номер ОГРН;
- дата внесения записи в ЕГРЮЛ (ЕГРИП);
- телефон;
- ИНН;
- КПП;
- факс (не обязательно);
- e-mail (не обязательно);
- сведения о владельце ключа – полностью;
- примечания (при наличии);
- личная подпись (подпись владельца ключа);
- подпись и ФИО руководителя юридического лица;
- оттиск печати юридического лица.

В бланке Ключа проверки ЭП работник Банка заполняет поля:

- номер договора;
- дата подписания договора;
- подпись и ФИО Уполномоченного представителя Банка;
- дата приёма Ключа проверки ЭП;
- оттиск печати Банк.