Приложение № 1 к Договору об
использовании системы дистанционного
банковского обслуживания «Клиент-Банк»

УСЛОВИЯ
предоставления и обслуживания
системы дистанционного банковского обслуживания «Клиент-Банк» для юридических лиц, индивидуальных предпринимателей и физических лиц, занимающихся в установленном законодательством Российской Федерации порядке частной практикой в АО «Банк ЧБРР»

ОГЛАВЛЕНИЕ

1. ОБЩИЕ ПОЛОЖЕНИЯ 2
2. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ 3
3. ПОДКЛЮЧЕНИЕ К СИСТЕМЕ ДБО ЮЛ 4
4. СМЕНА КЛЮЧЕЙ ВСЛЕДСТВИЕ КОМПРОМЕТАЦИИ 7
5. СОПРОВОЖДЕНИЕ АРМ КЛИЕНТОВ 7
6. ПОРЯДОК ВРЕМЕННОГО ПРИОСТАНОВЛЕНИЯ ИЛИ ВОЗОБНОВЛЕНИЯ ОБСЛУЖИВАНИЯ КЛИЕНТА В СИСТЕМЕ……..……8
7. ИЗМЕНЕНИЕ УПОНОМОЧЕННЫХ ЛИЦ КЛИЕНТА 9
8. ОРГАНИЗАЦИЯ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА 9
9. ОТКЛЮЧЕНИЕ ОТ СИСТЕМЫ ДБО ЮЛ 10
10. УСТАНОВЛЕНИЕ ЛИМИТА СПИСАНИЯ ДЕНЕЖНЫХ СРЕДСТВ СО СЧЕТА……..10
11. ОФОРМЛЕНИЕ И ОТПРАВКА ЭЛЕКТРОННОЙ ЗАЯВКИ НА ПОЛУЧЕНИЕ НАЛИЧНЫХ ДЕНЕЖНЫХ СРЕДСТВ ЧЕРЕЗ СИСТЕМУ ДБО ЮЛ……..11
Приложение № 1.Заявление на подключение к системе ДБО ЮЛ 12
Приложение № 1.2. Заявление на подключение к Мобильному приложению……..…..……13
Приложение № 2. Перечень электронных документов, передаваемых по системе ДБО ЮЛ 14
Приложение № 3. Перечень технических средств АРМ Клиента для установки и функционирования Системы ДБО ЮЛ 15
Приложение № 4. Требования к Клиенту по обеспечению информационной безопасности при эксплуатации Системы ДБО ЮЛ, ключевой информации и СКЗИ 16
Приложение № 5. Доверенность 18
Приложение № 6. Акт приема-передачи средств криптографической защиты информации 19
Приложение № 7. Уведомление о компрометации ключа ЭП 21
Приложение № 8. Заявление на приостановку/возобновление обслуживания в Системе ДБО ЮЛ…….. 22
Приложение № 9. Рекомендации по настройке и эксплуатации АРМ Клиента, на которых устанавливаются или используются клиентские части Системы ДБО ЮЛ 23
Приложение № 10. Заявление на подключение/отключение услуги, изменение номера(ов) телефона SMS-подтверждения 25
Приложение № 11. Образец Заявления о подтверждении использования ЭП в системе ДБО "iBank" 26
Приложение № 12. Заявление о расторжении Договора об использовании системы дистанционного банковского обслуживания «Клиент-Банк» 27
Приложение № 13. Сертификат ключа проверки электронной подписи сотрудника клиента в системе «iBank» АО «Банк ЧБРР» 28
Приложение № 14. Заявление на сброс PIN-кода 29
Приложение № 15. Рекомендации по безопасной работе Клиента в Мобильном приложении Системы ДБО ЮЛ.30
Приложение № 16. Заявление на установление/отмену лимита сумм платежных поручений 31
Приложение № 17. Заявление на предоставление доступа к меню «Мониторинг» Системы ДБО ЮЛ 32
Приложение № 18. Порядок оформления документа «Заявка на получение наличных денежных средств»……..……33

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Условия предоставления и обслуживания системы дистанционного банковского обслуживания «Клиент-Банк» в АО «Банк ЧБРР» (далее – Условия) являются неотъемлемой частью Договора об использовании системы дистанционного банковского обслуживания «Клиент-Банк», заключаемого между АО «Банк ЧБРР» (далее – Банк) и его Клиентами – юридическими лицами, индивидуальными предпринимателями, физическими лицами, занимающимися в установленном законодательством Российской Федерации порядке частной практикой (далее – Договор) и регламентируют порядок и условия:

1.1.1. предоставления и обслуживания Системы дистанционного банковского обслуживания «Клиент-Банк» (далее – Система, либо Система ДБО ЮЛ);

1.1.2. документооборота в Системе.

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

1.3. Клиентская часть Системы представлена Клиенту в виде:

– доступа к Системе ДБО ЮЛ («Интернет-Банк») на сайте https://cb.chbrr.crimea.com в информационно-телекоммуникационной сети «Интернет» (предназначенном для работы с Системой ДБО ЮЛ). Требуется дополнительная установка ПО компании БИФИТ – BIFIT Signer, который Клиент самостоятельно скачивает и устанавливает при перовом входе в ДБО ЮЛ;

– мобильного приложения Системы дистанционного банковского обслуживания «Клиент-Банк» для юридических лиц, индивидуальных предпринимателей и физических лиц, занимающихся в установленном действующим законодательством Российской Федерации порядке частной практикой для мобильных устройств (смартфоны) на операционной системе Android (далее – Мобильное приложение Системы ДБО ЮЛ). ВАЖНО – для полнофункционального режима работы с возможностью наложения электронной подписи на электронные документы в Мобильном приложении Системы ДБО ЮЛ используется только защищенный носитель ключевой информации USB-токен с USB-адаптером.

1.4. Средствами защиты информации, используемыми в Системе для обеспечения конфиденциальности Электронного Документа (ЭД) при его передаче по открытым каналам связи, а также для обеспечения авторства и целостности ЭД, являются сертифицированные ФСБ России средства криптографической защиты информации (СКЗИ), реализующие алгоритмы шифрования, формирования и проверки Электронной Подписи (ЭП) и имеющие действительный сертификат соответствия ФСБ. К таким относятся программные СКЗИ – криптографические библиотеки, и съемный защищенный носитель ключевой информации – аппаратные СКЗИ – USB-токен.

1.5. Хранение ключей ЭП допускается только на:

– защищенном ключевом носителе USB-токен, тип которого устанавливается Банком самостоятельно в одностороннем порядке;

– съемном носителе USB-flash накопитель, в случае использования файлового ключа ЭП, сформированного при помощи криптографических библиотек;

далее совместно упоминаемые – съемные носители ключевой информации.

1.6. При использовании СКЗИ USB-токен, Клиент приобретает в Банке необходимое количество USB-токенов, предназначенных для генерации и хранения криптографических ключей электронной подписи и формирования ключа проверки ЭП. При использовании USB-flash накопителя, Клиент самостоятельно обеспечивает себя необходимым количеством съемных носителей для каждого владельца ключа ЭП. Клиент самостоятельно генерирует секретный ключ на USB-токен или USB-flash накопитель. Съемные носители ключевой информации необходимо использовать лишь при наложении электронной подписи (ЭП) на персональном компьютере с Системой ДБО ЮЛ или мобильном устройстве для работы в Мобильном приложении. Категорически запрещается использовать носитель ключевой информации в других целях и на других устройствах, не предназначенных для работы в Системе ДБО ЮЛ. Ключи ЭП каждого пользователя должны храниться на персональном устройстве хранения ключевой информации USB-токен или USB-flash накопитель.

1.7. Полномочия использовании программных СКЗИ (криптографические библиотеки), Клиент самостоятельно скачивает с сайта https://cb.chbrr.crimea.com в информационно-телекоммуникационной сети «Интернет» (предназначенного для работы с Системой ДБО ЮЛ) инструкцию по установке криптобиблиотек и установочный комплект – архив с криптобиблиотеками, документацией и программным обеспечением контроля целостности. Пароль на распаковку архива клиент получает в Банке при заключении Договора об использовании системы дистанционного банковского обслуживания «Клиент-Банк». Далее Клиент осуществляет контроль целостности скачанных криптобиблиотек и установку их на свой ПК. При использовании программных СКЗИ, ключи ЭП необходимо хранить только на персональных USB-flash накопителях. **В целях обеспечения конфиденциальности средств электронной подписи, категорически запрещается хранение Ключей ЭП на жестком магнитном диске персонального компьютера, ноутбука, либо других устройствах, предназначенных для широкого пользования.**

1.8. Стороны согласны, с тем, что использование в Системе СКЗИ, указанных в п. 1.4 Условий, является достаточным для обеспечения конфиденциальности, аутентификации и целостности ЭД, и, обеспечивает защиту интересов Сторон.

1.9. Стороны признают, что получение Банком по Системе ДБО ЮЛ ЭД, указанных в Перечне электронных документов, передаваемых по Системе ДБО ЮЛ (Приложение № 2 к Условиям), подписанных ЭП Клиента, юридически тождественны получению аналогичных документов на бумажном носителе, заверенных собственноручной подписью Уполномоченных лиц и печатью Клиента, соответствующими указанным в карточке с образцами подписей и оттиска печати Клиента, и оформленных в соответствии с действующим законодательством Российской Федерации, в том числе нормативным правовыми актами Банка России (далее – действующее

законодательство). Клиент дает право Банку использовать ЭД наравне с заверенными собственноручной подписью документами на бумажном носителе.
1.10. Клиент признает, что ЭД, направленные Сторонами друг другу по Системе ДБО ЮЛ, а также файлы учета ЭД, ведущиеся в Системе, могут быть представлены Банком в качестве доказательств в Арбитражном суде в случае рассмотрения спора, возникшего в результате применения Системы ДБО ЮЛ.
1.11. Любые ЭД, передаваемые Клиентом в Системе, должны быть заверены ЭП Клиента.
1.12. Ключи с правом подписи ЭД предоставляются Владельцам ЭП, обладающим правом распоряжаться денежными средствами на Счете (Счетах), на период действия их полномочий, указанных в Карточке с образцами подписей и оттиска печати. Информационный ключ (без права подписи ЭД) может быть предоставлен представителю Клиента, не указанному в Карточке с образцами подписей и оттиска печати, после предоставления Клиентом Сертификата ключа проверки электронной подписи сотрудника клиента в системе «iBank» АО «Банк ЧБРР» (Приложение № 13 к Условиям) на указанного представителя Клиента.
1.13. Замена ключей с соблюдением требований настоящих Условий не влияет на юридическую силу ЭД, если он был подписан действующим на момент подписания ключом ЭП.
1.14. Обслуживание Клиента в Системе начинается с момента подключения к Системе ДБО ЮЛ.
1.15. Одновременное хранение ключей ЭП нескольких владельцев ключей ЭП, например, руководителя и главного бухгалтера, руководителя и его заместителя, на одном носителе запрещено. Для каждого ключа ЭП, в том числе "информационный", необходимо использовать отдельный носитель USB-токен или USB-flash накопитель.

2. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Банк – Акционерное общество «Черноморский банк развития и реконструкции», АО «Банк ЧБРР».

Владелец Сертификата ключа проверки ЭП – уполномоченное лицо Клиента, на имя которого выдан Сертификат ключа проверки ЭП и которое владеет соответствующим закрытым ключом ЭП, позволяющим с помощью средств электронной подписи создавать свою электронную подпись в электронных документах (подписывать электронные документы).

Договор – договор об использовании системы дистанционного банковского обслуживания «Клиент-Банк».

Договор банковского счета – Договор банковского счета, заключенный между Банком и Клиентом, в соответствии с которым открыт счет (а) и осуществляется его (их) обслуживание.

Клиент – юридическое лицо, индивидуальный предприниматель, физическое лицо, занимающееся в установленном законодательством Российской Федерации порядке частной практикой, имеющее(ий) в Банке банковский счет и заключивший с Банком Договор.

Клиентское автоматизированное рабочее место (далее – АРМ Клиента) – индивидуальный комплекс технических и программных средств Клиента, предназначенный для подключения к Системе и обеспечивающий подготовку, редактирование, подписание, отправку, поиск, получение и печать документов и справочной информации при взаимодействии с Банком.

Ключ электронной подписи (далее – Ключ ЭП) – число, представленное в виде уникальной последовательности символов, известное только Владельцу Ключа ЭП и предназначенное для создания в ЭД электронной подписи с использованием средств электронной подписи либо для дополнительной авторизации в Системе.

Ключ ЭП действует на определенный момент времени (действующий ключ ЭП) если:

– наступил момент времени начала действия ключа ЭП;

– срок действия ключа ЭП не истек;

– ключ проверки ЭП, соответствующий данному Ключу ЭП не аннулирован (отозван) и действие его не приостановлено. Ключ ЭП должен храниться владельцем в тайне.

В Системе ДБО ЮЛ также может использоваться (в т.ч. одновременно с ключом ЭП Банка) квалифицированный ключ электронной подписи, который выдан Клиенту удостоверяющим центром Федеральной Налоговой Службы Российской Федерации (далее – Ключ ЭП ФНС), Данная возможность предоставляется Клиенту при условии проведения Банком соответствующих процедур проверки сертификата ключа проверки электронной подписи и активации Ключа ЭП ФНС в Системе ДБО ЮЛ.

Ключ проверки электронной подписи – уникальная последовательность символов, однозначно связанная с закрытым Ключом ЭП и предназначенная для проверки подлинности электронной подписи (далее – проверка электронной подписи);

Ключевая информация – совокупность закрытого Ключа ЭП и Сертификата ключа проверки ЭП.

Ключевой носитель – аппаратный криптопровайдер USB-токен или USB-flash накопитель, предназначенный для хранения ключевой информации;

Ключевой документ – это Ключевая информация, записанная на Ключевой носитель.

Компрометация Ключа ЭП – событие, в результате которого возможно несанкционированное использование Ключа ЭП. К событиям, связанным с компрометацией ключей, относятся, включая, но не ограничиваясь, следующие:

– утрата ключевых носителей, с последующим обнаружением или без обнаружения;

– увольнение, либо смена участка работы сотрудников, имевших доступ к ключевой информации;

– нарушение правил хранения Ключа ЭП;

– возникновение подозрений на несанкционированный доступ к месту хранения или использования ключевых носителей, утечку информации или ее искажение.

Сертификат ключа проверки электронной подписи электронный документ или документ на бумажном носителе, выданные удостоверяющим центром либо доверенным лицом удостоверяющего центра и подтверждающие

принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи;

Система дистанционного банковского обслуживания «Клиент-Банк» (Система или Система ДБО ЮЛ) – комплекс программно-технических средств и организационных мероприятий для обеспечения электронного документооборота между Банком и Клиентом, включающий в себя подготовку, передачу и обработку документов в электронном виде с использованием электронно-вычислительных средств обработки информации, а также разбор конфликтных ситуаций.

SMS-подтверждение – услуга SMS-подтверждения электронных платежей в Системе ДБО ЮЛ.

Средство Криптографической Защиты Информации (далее – СКЗИ) – это сертифицированное ФСБ России программное обеспечение или аппаратное устройство, предназначенное для защиты информации от искажения в процессе ее хранения и передачи, и используемое в Системе для генерации Ключа ЭП, формирования электронной подписи, шифрования данных при передаче по каналам связи.

Стороны – Банк и Клиент при совместном упоминании.

Счет – банковский счет, открытый в соответствии с законодательством Российской Федерации и на основании заключенного с Банком Договора банковского счета.

Тарифы – установленный размер оплаты по осуществлению операций с использованием Системы ДБО ЮЛ, взимаемый Банком с Клиента за оказываемые ему услуги в рамках Договора, а также иные условия, которые устанавливаются в Тарифах. Тарифы Банка размещены на Официальном сайте Банка и в подразделениях Банка (в местах, доступных для Клиентов) по месту обслуживания Клиента (раздел 2 «Обслуживание счетов с использованием системы ДБО» Тарифов АО «Банк ЧБРР» на расчетно-кассовое обслуживание в валюте РФ и иностранной валюте юридических лиц, индивидуальных предпринимателей и физических лиц, занимающихся в установленном законодательством Российской Федерации порядке частной практикой).

Мобильное приложение (Мобильный Банк) – канал дистанционного доступа в Системе ДБО ЮЛ к расчетным счетам Клиентов, открытым в Банке, который позволяет им осуществлять расчетные операции, а также получать другие доступные услуги по указанным счетам посредством использования мобильного устройства (смартфона), подключенного к информационно-телекоммуникационной сети «Интернет».

Меню «Мониторинг» – интерфейс в Системе ДБО ЮЛ, позволяющий Клиенту самостоятельно подключить услугу SMS-оповещения и (либо) E-mail-оповещения, с целью получения информации об остатках денежных средств, операциях, совершенных по счетам в Системе ДБО ЮЛ.

Уполномоченное лицо – физическое лицо, имеющее право распоряжаться денежными средствами, находящимися на Счете(ах) Клиента, и указанное в карточке с образцами подписей и оттиска печати, действующее на основании учредительных документов Клиента и (или) выданной Клиентом доверенности, оформленной в соответствии с Договором банковского счета.

Целостность ЭД – означает, что после его создания и заверения ЭП в его содержание не вносилось никаких изменений.

Электронный документооборот - это способ обмена документами в электронном виде с помощью Системы.

Электронная подпись (далее – ЭП) – реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием Ключа ЭП и позволяющий идентифицировать владельца сертификата ключа проверки ЭП, а также установить отсутствие искажения информации в электронном документе.

Электронный документ (далее – ЭД) – документ, представляющий собой расчетный документ Клиента на совершение операций по его Счету, составленный в электронном виде и содержащий все предусмотренные законодательством Российской Федерации реквизиты, подписанный ЭП и имеющий равную юридическую силу с аналогичным документом на бумажном носителе, подписанным собственноручными подписями уполномоченных лиц и заверенным оттиском печати (при наличии) Клиента. Достоверность и конфиденциальность ЭД обеспечивается средствами ЭП, при соблюдении установленного режима эксплуатации Системы.

Электронный информационный документ (ЭИД) – электронный документ, не являющийся расчетным документом и обеспечивающий обмен информацией при совершении расчетов и проведении операций по Счету Клиента (выписки по счету, справки по счету, запросы, отчеты, информационные сообщения), а также иные документы, предоставляемые Клиентом в Банк, в т.ч. с целью заключения договоров с Банком и (или) исполнения условий заключенных договоров с Банком.

Электронное средство платежа (в контексте настоящего документа – АРМ Клиента (персональный компьютер, ноутбук, смартфон) – средство и (или) способ, позволяющие клиенту составлять, удостоверять и передавать распоряжения в целях осуществления перевода денежных средств в рамках применяемых форм безналичных расчетов с использованием информационно-коммуникационных технологий, электронных носителей информации, а также иных технических устройств.

Лимит списания денежных средств со счета – лимит сумм платежных поручений, ограничивающий максимально возможную сумму списания денежных средств с расчетного счета Клиента, с использованием Системы ДБО ЮЛ.

3. ПОДКЛЮЧЕНИЕ К СИСТЕМЕ ДБО ЮЛ

3.1. **Условия допуска Клиента к осуществлению документооборота в Системе ДБО ЮЛ:**

3.1.1. Документооборот в Системе доступен Клиенту только после выполнения Клиентом всех следующих условий:

– наличие АРМ Клиента в соответствии с Перечнем технических средств АРМ Клиента для установки и функционирования Системы ДБО ЮЛ (Приложение № 3 к Условиям), Требованиями к Клиенту по обеспечению информационной безопасности при эксплуатации системы дистанционного банковского обслуживания «Клиент-Банк», ключевой информации и СКЗИ (Приложение № 4 к Условиям);

– получения всех аппаратных или программных компонентов, необходимых для функционирования Системы ДБО ЮЛ;

– генерации ключей ЭП, создания технологических паролей и идентификаторов для доступа к Системе;

– получения Банком полного пакета документов, надлежащим образом оформленных и подписанных Клиентом.

3.2. **Порядок подключения Клиента к Системе ДБО ЮЛ:**

3.2.1. Подключение к Системе производится Клиентом самостоятельно путем регистрации на сайте https://cb.chbrr.crimea.com в информационно-телекоммуникационной сети «Интернет», предназначенном для работы с Системой ДБО ЮЛ.

3.2.2. **Клиент предоставляет в Банк:**

– Заявление на подключение к Системе ДБО ЮЛ (Приложение № 1 к Условиям) (все поля Заявления должны быть заполнены);

– Заявление на подключение к Мобильному приложению Системы ДБО ЮЛ (Приложение № 1.2 к Условиям)[1], оформляется Клиентами, которые только подключаются к Системе ДБО ЮЛ, а также действующими Клиентами, которые изъявили желание использовать Мобильное приложение.

! При указании номеров счетов, указывается режим обслуживания:

- «Полный» – указывается для расчетных счетов, специальных банковских счетов и депозитных счетов с возможностью проведения расчетных операций;
- «Получение выписки» – указывается для карточных счетов и депозитных счетов без возможности проведения расходных операций.

– Сертификат ключа проверки электронной подписи сотрудника клиента в системе «iBank» АО «Банк ЧБРР» (Приложение № 13 к Условиям), распечатывается Клиентом самостоятельно и предоставляется в Банк в 2-х экземплярах для каждой ЭП, один из которых после активации возвращается Клиенту;

– Заявление о подтверждении использования Ключа ЭП ФНС (Образец заявления указан в Приложении № 11 к Условиям) (предоставляется Клиентом при активации Ключа ЭП ФНС) формируется автоматически в Системе ДБО ЮЛ, при регистрации Ключа ЭП ФНС в Системе ДБО ЮЛ, распечатывается и подписывается Клиентом собственноручно и предоставляется в Банк в 2-х экземплярах, один из которых, после активации Ключа ЭП ФНС в Системе ДБО ЮЛ, возвращается Клиенту.

3.2.3. Направляемые в Банк сертификаты ключей проверки ЭП должны содержать достоверную информацию о владельце ключа ЭП и организации. При первичной регистрации в Системе, все поля, в том числе отмеченные звездочкой (*), должны быть обязательно заполнены. При повторной генерации (продлении) ключа ЭП, поля, отмеченные звездочкой (*) могут не заполняться. Не допускается внесение исправлений. В случае обнаружения Клиентом ошибочно введенных данных на распечатанном сертификате, рекомендуется провести повторную генерацию ключа ЭП.

3.2.4. Предоставление в Банк сертификата/Заявления о подтверждении использования ключа ЭП ФНС в Системе ДБО ЮЛ осуществляется лично Уполномоченным лицом предприятия, индивидуальным предпринимателем либо доверенным лицом, действующим на основании доверенности, оформляемой Клиентом в Банке по форме Приложения № 5 к Условиям. В случае возникновения у Клиента необходимости оформить и предоставить в Банк нотариально удостоверенную либо удостоверенную руководителем Клиента – юридического лица доверенность по форме отличной от формы, указанной в Приложении № 5 к Условиям, то в такую доверенность должны быть включены все действия, предусмотренные в доверенности по форме Приложения № 5 к Условиям. В противном случае Клиент обязан оформить в Банке доверенность по форме Приложения № 5 к Условиям.

3.2.5. В случае выявления неполной, недостоверной информации в сертификатах/Заявлении о подтверждении использования ключа ЭП ФНС в Системе ДБО ЮЛ или наличия исправлений, данные документы не принимаются работниками Банка в работу и возвращаются Клиенту/представителю Клиента.

3.2.6. При предоставлении в Банк сертификатов на руководителя и главного бухгалтера организации, право подписи будет предоставляться, на основании карточки образцов подписей. При этом подписи будут взаимосвязаны, т.е. главный бухгалтер не сможет отправить платежи в Банк без подписи руководителя организации и наоборот.

3.2.7. При необходимости активации дополнительного ключа ЭП для Уполномоченного лица организации, на двух экземплярах сертификата каждого ключа ЭП Уполномоченного лица, руководителем организации ставится пометка «Дополнительный». В случае отсутствия такой пометки, Банк активирует в Системе предоставленный сертификат на новый ключ ЭП, при этом все предыдущие действующие ключи ЭП Уполномоченного лица будут заблокированы. Дополнительный ключ ЭП возможно сгенерировать только на персональный носитель ключевой информации Уполномоченного лица.

3.2.8. В случае необходимости создания информационного ключа (просмотр/печать выписок, набор платежных документов, и т.д.), без права подписи, руководителем предприятия на сертификате ключа ЭП сотрудника организации проставляется отметка «Информационный».

3.3. При получении аппаратных ключевых носителей (USB-токен) в Банке, Клиент подписывает 2 экземпляра Акта приема-передачи средств криптографической защиты информации (Приложение № 6 к Условиям без Приложения к Приложению № 6). После внесения работниками Банка необходимых отметок в Акт и учета носителей USB-токен в журнале поэкземплярного учета СКЗИ, один экземпляр подписанных документов остается в Банке, второй передается Клиенту.

3.4. При получении установочного комплекта программных СКЗИ (криптобиблиотек) с сайта https://cb.chbrr.crimea.com в информационно-телекоммуникационной сети «Интернет» (предназначенного для работы с

[1] *Рекомендации по безопасной работе Клиента в Мобильном приложении Системы ДБО ЮЛ приведены в Приложении № 15 к Условиям.*

Системой ДБО ЮЛ) по защищенному каналу связи, Клиент подписывает 2 экземпляра Акта приема-передачи средств криптографической защиты информации (Приложение № 6 к Условиям) и 2 экземпляра Приложения к Акту (Приложение к Приложению № 6). После внесения работниками Банка необходимых отметок в Акт и учета криптографических библиотек в журнале поэкземплярного учета СКЗИ, один экземпляр подписанных документов остается в Банке, второй передается Клиенту. Обязательным условием подключения к Системе ДБО ЮЛ с использованием программных СКЗИ (криптобиблиотек), является подключение услуги SMS-подтверждения электронных платежей в Системе ДБО ЮЛ (на основании оформленного Заявления на подключение/отключение услуги, изменение номера(ов) телефона SMS-подтверждения (Приложение № 10 к Условиям)). В дальнейшем, при необходимости, и при условии оформления Заявления на подключение/отключение услуги, изменение номера(ов) телефона SMS-подтверждения (Приложение № 10 к Условиям), Клиент может изменять номер телефона(ов) для услуги SMS-подтверждения (часть 3 Приложения № 10 к Условиям), либо отключить услугу SMS-подтверждения (часть 2 Приложения № 10 к Условиям). Ввозможность отключения услуги SMS-подтверждения не распространяется на вариант подключения к Системе ДБО ЮЛ с помощью программных СКЗИ (криптографических библиотек). Услуга SMS-подтверждения подключается и предоставляется в соответствии с тарифами, опубликованными на Официальном сайте Банка. При этом плата взимается отдельно за каждый подключенный Клиентом номер телефона для услуги SMS-подтверждения (допускается подключать не более 2-х номеров телефона). В случае генерации и использования нескольких ключей ЭП на программных СКЗИ (криптобиблиотеки), комиссия взимается за второй и последующие ключи ЭП, согласно действующим тарифам, опубликованным на Официальном сайте Банка.

3.5. При отказе от использования аппаратных СКЗИ (USB-токен), предложенных Банком и использовании собственных аппаратных средств криптографической защиты и аутентификации (носитель ключевой информации USB-токен, идентичный, используемым в Банке), Клиент выбирает вариант подключения к Системе ДБО ЮЛ с использованием собственного аппаратного СКЗИ USB-токен клиента, идентичного, используемому в АО «Банк ЧБРР» и вносит соответствующие отметки в разделе «Подключение к системе ДБО ЮЛ Заявления на подключение к Системе ДБО ЮЛ (Приложение № 1 к Условиям) и указывает идентификатор устройства.

3.6. С целью получения информации об остатках денежных средств, операциях, совершенных по счетам в Системе ДБО ЮЛ, Клиент может подключить услугу SMS-оповещения и (либо) E-mail-оповещения, путем оформления Заявления на предоставление доступа в меню «Мониторинг» (Приложение № 17 к Условиям). Функцию SMS-оповещения и (либо) E-mail-оповещения Клиент имеет возможность включать и отключать самостоятельно, в меню «Мониторинг» Системы ДБО ЮЛ. Инструкция по подключению услуги SMS-оповещения и (либо) E-mail-оповещения расположена на *сайте* Банка по адресу https://чбрр.рф/corporate/remote-services/documents/в информационно-телекоммуникационной сети «Интернет» в разделе «Документация»/«Дополнительные инструкции»: «Инструкция по настройке SMS и E-mail оповещений в Клиент-Банке», либо на Сайте СДБО ЮЛ https://cb.chbrr.crimea.com в разделе «Документация».

Услуга SMS-оповещения предоставляется в соответствии с тарифами, опубликованными на Официальном сайте Банка**. <u>При этом плата взимается отдельно за каждый подключенный Клиентом номер телефона для услуги SMS-оповещения.</u>** В случае, если Клиент, с целью получения информации об остатках денежных средств, операциях, совершенных по счетам в Системе ДБО ЮЛ, **<u>подключил в меню «Мониторинг» только функцию E-mail-оповещения</u>**, то плата за получение информации об остатках денежных средств, операциях, совершенных по счетам в Системе ДБО ЮЛ, **<u>с Клиента не взимается.</u>**

Услуги SMS-подтверждения и SMS-оповещения (далее, при совместном упоминании – услуги SMS сервиса) подключаются и предоставляется на следующих условиях:

3.6.1. Комиссия за предоставление услуги списывается в последний рабочий день месяца с основного расчетного счета независимо от наличия операций по счету.

3.6.2. В случае подключения нескольких номеров телефонов SMS-оповещения дополнительно взимается комиссия за каждый подключенный номер, согласно тарифам Банка.

3.6.3. В случае наличия у Клиента нескольких (подключенных к услуге) счетов комиссия взимается с основного счета независимо от количества счетов.

3.6.4. В случае если сумма задолженности за предоставление услуги SMS сервиса составит 1 (один) месяц – данная услуга отключается без предварительного уведомления Клиента.

3.6.5. Повторное подключение услуги будет произведено после полного погашения задолженности.

3.6.6. Клиент подтверждает, что ознакомлен с Тарифами Банка на предоставление услуг SMS-подтверждения и SMS-оповещения.

3.6.7. Банк не несет ответственности в случае неполучения Клиентом SMS-сообщения в связи с техническими проблемами, в том числе по вине лиц, оказывающих услуги сотовой связи либо доставки электронных сообщений, а также в иных случаях, произошедших не по вине Банка.

3.6.8. В случае утери SIM-карты и/или телефона, который используется для SMS-подтверждения, Клиент обязан уведомить об этом Банк для блокирования доступа к сервису, а также предоставить Заявление на подключение/отключение услуги, изменение номера(ов) телефона SMS-подтверждения с заполненными соответствующими графами раздела 3 заявления (Приложение № 10 к Условиям). Изменить номер телефона SMS-оповещения в меню «Мониторинг», Клиент может самостоятельно, согласно Инструкции по настройке SMS и E-mail-оповещений в Клиент Банке, указанной п. 3.6 Условий).

3.6.9. Все рассылаемые посредством интерфейса Системы ДБО ЮЛ меню «Мониторинг» SMS-оповещения и (либо) E-mail-оповещения носят информационный характер.

3.6.10. Предоставление доступа в меню «Мониторинг» и (либо) подключение услуги SMS-подтверждения происходит не позднее следующего дня, за днем соответствующего оформления Клиентом Заявления на предоставление доступа в меню «Мониторинг» (Приложение № 17 к Условиям)/Заявления на подключение/отключение услуги, изменение

номера(ов) телефона SMS-подтверждения (Приложение № 10 к Условиям), соответственно.
3.6.11. Отключение от услуги SMS-оповещения и (либо) E-mail-оповещения Клиент производит самостоятельно в меню «Мониторинг».
3.7. В случае отказа от услуг SMS-подтверждения (но не в случае работы в Системе с программными СКЗИ – криптобиблиотеки) электронных платежей, Клиент заполняет соответствующие графы раздела 2 Заявления на подключение/отключение услуги, изменение номера(ов) телефона SMS-подтверждения (Приложение № 10 к Условиям).
3.8. Работа в Системе производится в браузере, посредством WEB-интерфейса при условии готовности АРМ Клиента в соответствии с Перечнем технических средств АРМ Клиента для установки и функционирования Системы ДБО ЮЛ (Приложение № 3 к Условиям), Требованиями к Клиенту по обеспечению информационной безопасности при эксплуатации системы дистанционного банковского обслуживания «Клиент-Банк», ключевой информации и СКЗИ (Приложение № 4 к Условиям) и Рекомендациями по настройке и эксплуатации АРМ Клиента, на которых устанавливаются или используются клиентские части Системы ДБО ЮЛ (Приложение № 9 к Условиям).
3.9. Банк осуществляет действия по подключению Клиента к Системе ДБО ЮЛ в течение 5 (пяти) рабочих дней от даты подачи полного пакета документов, в том числе, указанных в п. 3.2.2 Условий.
3.10. Для подключения дополнительных счетов, а также в случае изменения параметров подключения, Клиент оформляет Заявление на подключение к Системе ДБО ЮЛ (Приложение № 1 к Условиям), при этом в разделе «БАНКОВСКИЕ СЧЕТА» указываются новые Счета для подключения, в разделе *«Предоставить право подписи электронных документов следующим уполномоченным лицам, внесенным в карточку с образцами подписей и оттиска печати»* – новые параметры подключения и передает его в Банк на бумажном носителе в 2-х экземплярах. Один экземпляр Заявления на подключение к Системе ДБО ЮЛ с отметкой о приеме Банк передает Клиенту.
3.11. В случае подключения счетов с различным уровнем полномочий представителей Клиента (в соответствии с карточками с образцами подписей и оттиска печати), счета группируются в соответствующих Заявлениях на подключение к Системе ДБО ЮЛ по указанным полномочиям.

4. СМЕНА КЛЮЧЕЙ ВСЛЕДСТВИЕ КОМПРОМЕТАЦИИ

4.1. Ключ ЭП является средством подтверждения права Уполномоченного лица Клиента на использование Системы как электронного средства платежа. При утрате или компрометации ключа ЭП, а также в случае перевода денежных средств без добровольного согласия Клиента, Уполномоченное лицо Клиента обязано незамедлительно приостановить любую работу в Системе ДБО ЮЛ, в том числе остановить операции с электронными документами, при нетипичной (подозрительной) работе ПК, извлечь из него ключевой носитель, незамедлительно сообщить по телефону в обслуживающее Клиента подразделение Банка (в соответствии с режимом работы подразделения) о случившемся инциденте, предварительно пройдя идентификацию, для принятия мер по блокировке ключа ЭП, после чего подойти в Банк и оформить Уведомление о компрометации ключа ЭП (Приложение № 7 к Условиям) (далее – Уведомление).

Банк оставляет за собой право проверить достоверность полученной информации путем совершения контрольного звонка по Телефону Клиента для экстренной связи.

4.2. Уполномоченное лицо Клиента, не позднее дня, следующего за днем совершения телефонного звонка с предоставлением информации о компрометации, либо в день выявления компрометации ключа ЭП, оформляет в Банке Уведомление на бумажном носителе, заверенное печатью (при наличии) и подписанное собственноручной подписью уполномоченного лица Клиента – 1 (Один) экземпляр. Документ должен быть доставлен в Банк нарочно. Направление Уведомления о компрометации ключа означает требование Клиента прекратить прием и исполнение любых ЭД, подписанных ЭП, сформированных на скомпрометированном ключе.
4.3. При получении от Клиента (уполномоченного лица Клиента) Уведомления на бумажном носителе, все ЭД, подписанные скомпрометированным ключом ЭП, считаются недействительными и Банком не принимаются.
4.4. Клиент самостоятельно производит замену ключей ЭП. Клиент обязан предоставить в Банк после смены ключей ЭП оригиналы сертификатов ключей проверки ЭП в 2 (Двух) экземплярах для регистрации сертификатов ключей проверки ЭП клиента на сервере Банка или Заявление о подтверждении использования ЭП в Системе ДБО ЮЛ. Сертификаты ключей проверки ЭП/Заявление о подтверждении использования ЭП в Системе ДБО ЮЛ передаются в Банк лично Уполномоченным лицом Клиента или представителем Клиента, действующим на основании доверенности, оформленной в порядке, указанном в пп. 3.2.4 Условий.
4.5. Банк оставляет за собой право заблокировать Ключ ЭП Уполномоченного лица Клиента с последующим уведомлением, при выявлении или подозрении факта компрометации ключа ЭП, выявлении факта несоответствия Уполномоченного лица Клиента с лицами, указанными в карточке образцов подписей, выявлении несоответствия реквизитов организации Клиента с данными в Системе, подозрении или выявлении несанкционированного списания денежных средств.
4.6. Разблокирование (возобновление действия) ключа ЭП Уполномоченных лиц Клиента осуществляется Банком не позднее дня, следующего за днем устранения выявленных нарушений и представления актуальных данных, и документов, указанных в п. 4.5 настоящих Условий.

5. СОПРОВОЖДЕНИЕ АРМ КЛИЕНТОВ

5.1. При возникновении вопросов по работе программного обеспечения Системы или сбоев в ее работе на стороне Клиента, Клиент обращается (в соответствии с режимом работы подразделения) за консультацией в службу технической поддержки Банка по телефонам: +7 (978) 835-21-12, +7 (978) 835-22-11, +7 (3652) 605-805. Если в процессе консультации возникает необходимость раскрытия конфиденциальной информации о данном Клиенте, работник службы технической поддержки Банка обязан идентифицировать Клиента запросив блокировочное слово (указанное в Системе при первоначальной регистрации Клиента). Отсутствие правильного ответа со стороны Клиента

и/или обоснованные подозрения о наличии угрозы нанесения убытков Клиенту или Банку являются основанием для отказа в раскрытии конфиденциальной информации на основании подпункта 3.2.2 Договора.
5.2. Оплата услуг по сопровождению Системы производится согласно Тарифам, размещенным на Официальном сайте Банка**.**
5.3. При блокировке аппаратного носителя ключевой информации USB токен вследствие неверного указания Клиентом PIN-кода на устройство, блокированный носитель ключевой информации USB-токен передается в Банк на основании его Заявления на сброс PIN-кода (Приложение № 14) для организации его разблокирования. При этом в подразделении Банка оформляется Акт приема-передачи СКЗИ от Клиента Банку. После возвращения работоспособного USB-токена, оформленного Актом приема-передачи СКЗИ между Банком и Клиентом, Клиент обязан сгенерировать новый ключ ЭП, в соответствии с п. 3.2.3–3.2.7 настоящих Условий.
5.4. При блокировке ключа ЭП вследствие неверного указания Клиентом пароля на ключ ЭП, Системой не предусмотрена возможность разблокирования. Клиент обязан сгенерировать новый ключ ЭП, в соответствии с п. 3.2.3–3.2.7 настоящих Условий.

6. ПОРЯДОК ВРЕМЕННОГО ПРИОСТАНОВЛЕНИЯ ИЛИ ВОЗОБНОВЛЕНИЯ ОБСЛУЖИВАНИЯ КЛИЕНТА В СИСТЕМЕ

6.1. Банк имеет право в одностороннем порядке приостановить обслуживание и (или) ограничить доступ Клиента в Системе ДБО ЮЛ с уведомлением Клиента об этом[2]:
− на время спорных ситуаций;
− для выполнения неотложных, аварийных, технических и регламентных работ, связанных с обслуживанием Системы с уведомлением Клиента о сроках проведения этих работ;
− при наличии у Банка оснований полагать, что по Системе ДБО ЮЛ, возможна попытка несанкционированного доступа или совершения противоправных действий, нарушающих законодательство Российской Федерации, в том числе нарушения целостности ЭД и (либо) компрометация Ключа ЭП;
– неисполнения Клиентом обязательств, предусмотренных Договором;
– несвоевременного предоставления Банку сведений (документов), предусмотренных Договором, и (либо) истребованных по письменному запросу Банка. Банк имеет право отказать, либо приостановить прием от Клиента распоряжений о совершении операций по Счету по Системе ДБО ЮЛ, в случаях, если у Банка возникают подозрения, что операции осуществляются Клиентом с целью легализации (отмывания) доходов, полученных преступным путем, финансирования терроризма и финансированию распространения оружия массового уничтожения;
– совершения Клиентом других нарушений условий Договора и/или действующего законодательства, которые могут повлечь (повлекших) за собой ущерб для Банка;
– в иных случаях угрозы нанесения убытков Клиенту или Банку;
– не поступления от Клиента оплаты за обслуживание в Системе в течение 2-х (Двух) месяцев подряд;
– если по банковским счетам Клиента, обслуживающимся в Системе, в течение более 3-х (Трех) месяцев не проводятся операции, в т.ч. операции по зачислению денежных средств;
– в случае выявления Банком операций, соответствующих признакам осуществления перевода денежных средств без согласия Клиента;
– в случае получения от Банка России информации, содержащейся в базе данных о случаях и попытках осуществления переводов денежных средств без добровольного согласия Клиента, которая содержит сведения, относящиеся к Клиенту и (или) его электронному средству платежа;
– в иных случаях, предусмотренных действующим законодательством Российской Федерации.
Банк **обязан** в одностороннем порядке приостановить использование Клиентом Системы ДБО ЮЛ, с уведомлением Клиента об этом, в случае получения от Банка России информации, содержащейся в базе данных о случаях и попытках осуществления переводов денежных средств без добровольного согласия Клиента, которая содержит сведения, относящиеся к Клиенту и (или) его электронному средству платежа, в том числе сведения федерального органа исполнительной власти в сфере внутренних дел о совершенных противоправных действиях, на период нахождения таких сведений в указанной базе данных.
6.1.1. При выявлении операции, соответствующей признакам осуществления перевода денежных средств без добровольного согласия Клиента и после выполнения действий, предусмотренных подпунктом 3.1.8 настоящего Договора, Банк предоставляет Клиенту информацию:
− о выполнении Банком действий, предусмотренных подпунктом 3.1.8 настоящего Договора;
– о возможности подтвердить распоряжение не позднее одного дня, следующего за днем приостановления Банком приема к исполнению указанного распоряжения посредством телефонной связи.
6.1.2. При получении от Клиента подтверждения распоряжения, Банк в установленные сроки принимает к исполнению подтвержденное распоряжение Клиента, при отсутствии иных установленных законодательством Российской Федерации оснований не принимать распоряжение Клиента к исполнению.
6.1.3. При неполучении от Клиента подтверждения распоряжения (указанного в абзаце третьем подпункта 6.1.1) и (или) информации, запрошенной в соответствии подпунктом 3.1.8 настоящего Договора, указанное распоряжение считается не принятым к исполнению.
6.1.4. В случае, если, несмотря на направление Клиентом подтверждения распоряжения, Банк получил от Банка России информацию, содержащуюся в базе данных о случаях и попытках осуществления переводов денежных средств

[2] *За исключением случаев, когда в соответствии с действующим законодательством Российской Федерации дальнейшее использование Клиентом Системы ДБО ЮЛ недопустимо.*

без добровольного согласия Клиента, Банк приостанавливает прием к исполнению подтвержденного распоряжения Клиента на два дня со дня направления Клиентом подтверждения распоряжения. Банк в порядке, установленном в п. 6.1.7 настоящего Договора, незамедлительно уведомляет Клиента о приостановлении приема к исполнению подтвержденного распоряжения Клиента, с указанием причины такого приостановления и срока такого приостановления.
6.1.5. В случае приостановления приема к исполнению подтвержденного распоряжения Клиента в соответствии с п. 6.1.4 настоящего Договора по истечении двух дней со дня направления клиентом подтверждения распоряжения в соответствии с подпунктом 6.1.4 настоящего Договора, Банк обязан в установленные сроки принять к исполнению подтвержденное распоряжение Клиента при отсутствии иных установленных законодательством Российской Федерации оснований не принимать подтвержденное распоряжение Клиента к исполнению.
6.1.6. Рассматривать заявления Клиента, в том числе при возникновении споров, связанных с использованием Клиентом его электронного средства платежа, а также предоставить Клиенту возможность получать информацию о результатах рассмотрения заявлений, в том числе в письменной форме по требованию Клиента, в срок установленный ст.30.1 Федерального закона от 02.12.1990 № 395-1 «О банках и банковской деятельности», а также не более 60 дней со дня получения заявлений в случае использования электронного средства платежа для осуществления трансграничного перевода денежных средств.
6.1.7. В случаях, предусмотренных Федеральным законом от 27.06.2011 № 161-ФЗ «О национальной платежной системе» способом информационного взаимодействия между Банком и Клиентом являются: электронные сообщения по Системе ДБО ЮЛ либо через средства телефонной/мобильной связи, SMS-оповещение.
6.2. Клиент имеет право приостановить обслуживание в Системе по собственному желанию, при этом Клиент оформляет Заявление на приостановку/возобновление обслуживания в Системе «Клиент-Банк» (Приложение № 8 к Условиям) и передает его в Банк. Заявление на приостановку обслуживания является основанием прекращения взимания с Клиента абонентской платы за обслуживание в Системе с месяца, следующего за месяцем приостановки обслуживания. После получения указанного Заявления Банк на следующий рабочий день осуществляет приостановку обслуживания Клиента по Системе ДБО ЮЛ.
6.3. Для возобновления обслуживания в Системе Клиент оформляет Заявление на приостановку/возобновление обслуживания в Системе ДБО ЮЛ (Приложение № 8 к Условиям) и передает его в Банк. Заявление на приостановку/возобновление обслуживания в Системе является основанием возобновления взимания с Клиента абонентской платы за обслуживание в Системе. Возобновление обслуживания производится на следующий рабочий день, следующий за днем приема Заявления на возобновление обслуживания в Системе Банком.
6.4. Возобновление обслуживания в Системе, в связи с невыполнением Клиентом пункта 1.11 Условий осуществляется на следующий рабочий день после продления срока полномочий Владельца ЭП для работы с ключами ЭП согласно Заявления на приостановку/возобновление обслуживания в Системе ДБО ЮЛ (Приложение № 8 к Условиям).
6.5. Банк прекращает обслуживание Клиента с использованием Системы ДБО ЮЛ в случае расторжения с Клиентом Договора банковского счета.

7. ИЗМЕНЕНИЕ УПОЛНОМОЧЕННЫХ ЛИЦ КЛИЕНТА

7.1. В случае изменений в составе Уполномоченных лиц Клиента, указанных в карточке с образцами подписей и оттиска печати, Клиент оформляет Уведомление о компрометации ключа ЭП (Приложение № 7 к Условиям), после чего производит новую генерацию Ключа ЭП, распечатывает сертификат КПЭП на бумажном носителе в 2 (Двух) экземплярах или Заявление о подтверждении использования ключа ЭП ФНС в Системе ДБО, и предоставляет его в Банк лично Уполномоченным лицом Клиента или представителем Клиента, действующим на основании доверенности, оформленной в порядке, указанном в пп. 3.2.4 Условий. Второй экземпляр Сертификата/Заявления с отметкой о приеме Банк передает Клиенту.

8. ОРГАНИЗАЦИЯ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА

8.1. Этапы электронного документооборота:
– формирование ЭД, заверение его ЭП;
– отправка и доставка ЭД;
– проверка подлинности ЭД;
– подтверждение получения ЭД Банком;
– отзыв ЭД;
– учет ЭД (регистрацию входящих и исходящих ЭД);
– хранение ЭД (ведение архивов ЭД).
8.2. Формирование ЭД осуществляется в следующем порядке:
8.2.1. Список видов документов, принимаемых Банком к исполнению в Системе указан в Перечне электронных документов, передаваемых по Системе ДБО ЮЛ (Приложение № 2 к Условиям). Доступ к видам документов, перечисленных в пунктах 1.2, 1.3 Приложения № 2 к Условиям, предоставляется Клиентам по дополнительному запросу в обслуживающий Офис Банка.
8.2.2. ЭД оформляется путем заполнения стандартной формы документа, предусмотренной в Системе для данного вида ЭД, т.е. внесения данных в форму документа согласно наименованиям полей. При оформлении ЭД, Система 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.
8.2.3. Сформированный ЭД подписывается личным ключом ЭП каждого из Уполномоченных лиц Клиента.

8.3. Отправка и доставка электронного документа:
8.3.1. ЭД считается исходящим от Клиента, если:
– ЭД подписан действующим Ключом (ключами) ЭП Клиента;
– Банк не уведомлен о компрометации действующего Ключа (ключей) ЭП Клиента;
– ЭД передан получателю средствами Системы ДБО ЮЛ.
8.3.2. ЭД не считается исходящим от Клиента, если:
– ЭД не прошел проверку на целостность документа и подлинность ЭП Клиента;
– Банк уведомлен о компрометации Ключа (ключей) ЭП Клиента.
8.4. Проверка подлинности доставленного ЭД включает:
– проверку подлинности ЭП электронного документа;
– расшифровку ЭД;
– проверку ЭД на соответствие установленному формату для данного вида ЭД;
– проверку соответствия параметров ЭД требованиям Договора между Банком и Клиентом, а также требованиям законодательства Российской Федерации, в том числе нормативных документов Банка России. В случае положительного результата проверки, ЭД принимается к исполнению. В случае если ЭД не проходит контроль правильности оформления, или не подтверждается его ЭП, Банк не принимает данный ЭД к исполнению/сведению, о чем Клиент видит в Системе статус ЭД «Отвергнут».
8.5. Отзыв электронного документа:
8.5.1. Участник Системы вправе отозвать отправленный ЭД. Для отзыва ЭД Участник Системы должен выполнить следующие действия:
1) позвонить работнику обслуживающего подразделения Банка в Системе, сообщить свои Ф.И.О. и наименование Участника Системы;
2) назвать реквизиты ЭД, который необходимо отозвать;
3) направить сообщение через Систему, подписанное электронной подписью, с указанием об отмене ЭД и реквизитов ЭД.

Работник обслуживающего подразделения Банка, после получения по телефону от Участника Системы требования об отмене ЭД (в порядке, указанном в частях 1 и 2 подпункта 8.5.1 настоящих Условий), не проводит исполнение (отправку) ЭД в Системе до момента получения от Участника Системы сообщения, указанного в части 3 подпункта 8.5.2. настоящих Условий. После получения сообщения и проверки электронной подписи участника Системы, ЭД удаляется.
8.5.3. ЭД может быть отозван только до начала его исполнения получателем. Банк вправе отказать в отзыве отправителю, в случае невозможности отзыва ЭД.
8.6. Учет ЭД:
8.6.1. Учет ЭД, отправленных через Систему, осуществляется Банком в базе данных Системы. При отправке ЭД Система автоматически осуществляет учет отправленного ЭД.
8.7. Хранение ЭД:
8.7.1. Архивное хранение ЭД осуществляется в течение установленных сроков, предусмотренных действующим законодательством.
8.8. При направлении в Банк текстовых сообщений, уведомление о регистрации обращения производится путем изменений статуса письма.

9. ОТКЛЮЧЕНИЕ ОТ СИСТЕМЫ ДБО ЮЛ

9.1. Отключение от услуги использования Системы ДБО ЮЛ по инициативе Клиента происходит путем подачи Заявления о расторжении Договора об использовании системы дистанционного банковского обслуживания «Клиент-Банк» (Приложение № 12 к Условиям) в то подразделение Банка, в котором Клиент подключался к услуге Системы ДБО ЮЛ.
9.2. Работник подразделения Банка подписывает у клиента Заявление в 2-х экземплярах, проставляет свои отметки, после чего один экземпляр возвращает Клиенту.
9.3. Обслуживание в Системе ДБО ЮЛ прекращается на следующий рабочий день после дня приема заявления о расторжении Договора с Банком.
9.4. Отключение от услуги использования Системы ДБО ЮЛ по инициативе Банка происходит в случае отсутствия у Клиента действующих банковских продуктов – Счета (Счетов) Клиента, открытых в Банке на основании Договора(ов) банковского счета, и подключенных к Системе ДБО ЮЛ, в соответствии с настоящим Договором. Договор считается расторгнутым со дня следующего за днем закрытия крайнего Счета Клиента. При этом дополнительные уведомления не отправляются, заявления не оформляются.
9.5. При заключении и расторжении Договора об использовании Системы ДБО ЮЛ оплата за эксплуатацию Системы взимается за полный месяц.
9.6. Вся информация о работе Клиента в Системе ДБО ЮЛ переносится в Архив и хранится в соответствующих регистрах Системы в течение срока, оговоренного в Договоре, но не менее 5 (пяти) лет с даты осуществления последнего платежа/перевода.

10. УСТАНОВЛЕНИЕ ЛИМИТА СПИСАНИЯ ДЕНЕЖНЫХ СРЕДСТВ СО СЧЕТА

10.1. Клиент может установить лимит списания денежных средств с расчетного счета на основании оформленных платежных поручений в Системе ДБО ЮЛ (далее – Лимит). Для этого Клиенту необходимо обратиться в обслуживающее подразделение Банка и оформить Заявление об установлении/отмене лимита сумм платежных поручений (Приложение № 16 к настоящим Условиям).

10.2. Лимит может быть установлен на разовый платеж, на день и на месяц:
– для АРМ Клиента (заполняется пп. 1.1 Приложения № 16 к настоящим Условиям – «Общий лимит на платежные поручения»);
– для Мобильного приложения (заполняется пп. 1.2 Приложения № 16 к настоящим Условиям – «Лимит на платежные поручения Мобильного Банка»).
В случае установления Клиентом различных размеров Лимитов, приоритетным будет Лимит, установленный для АРМ Клиента.
10.3. Установленный Лимит действует бессрочно, либо до момента его изменения/отмены путем оформления Клиентом соответствующего Заявления об установлении/отмене лимита сумм платежных поручений (Приложение № 16 к настоящим Условиям).

11. ОФОРМЛЕНИЕ И ОТПРАВКА ЭЛЕКТРОННОЙ ЗАЯВКИ НА ПОЛУЧЕНИЕ НАЛИЧНЫХ ДЕНЕЖНЫХ СРЕДСТВ ЧЕРЕЗ СИСТЕМУ ДБО ЮЛ

11.1. Клиент, с целью получения наличных денежных средств в российских рублях в учреждении Банка по расходному кассовому ордеру 0402009 (без оформления денежного чека), вправе осуществлять формирование и отправку через Систему ДБО ЮЛ в электронном виде Заявки на получение наличных денежных средств.
11.2. Для формирования Заявки на получение наличных денежных средств Клиент в разделе «Рублевые документы» Системы ДБО ЮЛ заходит в документ «Заявка на наличные» и заполняет ее в соответствии с рекомендациями по заполнению документа, приведенными в Приложении № 18 к Условиям. Заявка подается не позднее, чем за один рабочий день до даты получения денежных средств, но не ранее, чем за 10 (Десять) рабочих дней до получения денежных средств. После чего осуществляет подписание и отправку в Банк документа «Заявка на наличные» через Систему ДБО ЮЛ.

Приложение № 1
к Условиям предоставления и обслуживания
системы дистанционного банковского обслуживания «Клиент-Банк»
для юридических лиц, индивидуальных предпринимателей и физических лиц,
занимающихся в установленном законодательством
Российской Федерации порядке частной практикой в АО «Банк ЧБРР»

Заявление на подключение к Системе ДБО ЮЛ

НАИМЕНОВАНИЕ КЛИЕНТА	
ИНН	

БАНКОВСКИЕ СЧЕТА

НОМЕР СЧЕТА						
НА ОСНОВАНИИ ДОГОВОРА БАНКОВСКОГО СЧЕТА	ОТ		№		РЕЖИМ ОБСЛУЖИВАНИЯ	☐ ПОЛНЫЙ[3] ☐ ПОЛУЧЕНИЕ ВЫПИСКИ
НОМЕР СЧЕТА						
НА ОСНОВАНИИ ДОГОВОРА БАНКОВСКОГО СЧЕТА	ОТ		№		РЕЖИМ ОБСЛУЖИВАНИЯ	☐ ПОЛНЫЙ ☐ ПОЛУЧЕНИЕ ВЫПИСКИ
НОМЕР СЧЕТА						
НА ОСНОВАНИИ ДОГОВОРА БАНКОВСКОГО СЧЕТА	ОТ		№		РЕЖИМ ОБСЛУЖИВАНИЯ	☐ ПОЛНЫЙ ☐ ПОЛУЧЕНИЕ ВЫПИСКИ

ПРЕДОСТАВИТЬ ПРАВО ПОДПИСИ ЭЛЕКТРОНЫХ ДОКУМЕНТОВ СЛЕДУЮЩИМ УПОЛНОМОЧЕННЫМ ЛИЦАМ, ВНЕСЕННЫМ В КАРТОЧКУ С ОБРАЗЦАМИ ПОДПИСЕЙ И ОТТИСКА ПЕЧАТИ:

Должность	Фамилия, Имя, Отчество (при наличии) полностью	Ключ ЭП
		☐ С ПРАВОМ ПОДПИСИ ЭД ☐ ИНФОРМАЦИОННЫЙ
		☐ С ПРАВОМ ПОДПИСИ ЭД ☐ ИНФОРМАЦИОННЫЙ
		☐ С ПРАВОМ ПОДПИСИ ЭД ☐ ИНФОРМАЦИОННЫЙ
		☐ С ПРАВОМ ПОДПИСИ ЭД ☐ ИНФОРМАЦИОННЫЙ

ПОДКЛЮЧЕНИЕ К СИСТЕМЕ ДБО ЮЛ ПРОИЗВОДИТСЯ С ИСПОЛЬЗОВАНИЕМ:

АППАРАТНОГО СКЗИ USB-ТОКЕН, ПРЕДОСТАВЛЯЕМОГО АО «БАНК ЧБРР»	☐
СОБСТВЕННОГО АППАРАТНОГО СКЗИ USB-ТОКЕН КЛИЕНТА, ИДЕНТИЧНОГО, ИСПОЛЬЗУЕМОМУ В АО «БАНК ЧБРР» идентификатор № ☐☐☐☐☐☐	☐
ПРОГРАММНОГО СКЗИ, ПРЕДОСТАВЛЯЕМОГО АО «БАНК ЧБРР» (БЕЗ USB-ТОКЕНА)	☐
СОБСТВЕННОГО СКЗИ USB-ТОКЕН. КЛЮЧА ЭП И СЕРТИФИКАТА КЛЮЧА ПРОВЕРКИ ЭП, ПОЛУЧЕННЫХ В УЦ ФНС РОССИИ	☐

КОНТАКТНОЕ ЛИЦО КЛИЕНТА ДЛЯ ВЗАИМОДЕЙСТВИЯ ПО СИСТЕМЕ ДБО ЮЛ

Ф.И.О.		ТЕЛЕФОН	

РУКОВОДИТЕЛЬ ОРГАНИЗАЦИИ

ДОЛЖНОСТЬ	ПОДПИСЬ	ИНИЦИАЛЫ, ФАМИЛИЯ	ДАТА		

М.П.

ОТМЕТКИ БАНКА

С КЛИЕНТОМ ЗАКЛЮЧЕН ДОГОВОР ОБ ИСПОЛЬЗОВАНИИ СИСТЕМЫ ДИСТАНЦИОННОГО БАНКОВСКОГО ОБСЛУЖИВАНИЯ «КЛИЕНТ-БАНК»	ОТ		№	

ЗАЯВЛЕНИЕ ПРИНЯТО, ПОЛНОМОЧИЯ ПРЕДСТАВИТЕЛЯ КЛИЕНТА ПРОВЕРЕНЫ.

НАЧАЛЬНИК ДО № /ОООК ОУ

ПОДПИСЬ	ИНИЦИАЛЫ, ФАМИЛИЯ	ДАТА		

М.П.

[3] *«Полный» – указывается для расчетных счетов, специальных банковских счетов и депозитных счетов с возможностью проведения расчетных операций; «Получение выписки» – указывается для карточных счетов и депозитных счетов без возможности проведения расходных операций.*

Приложение № 1.2
к Условиям предоставления и обслуживания
системы дистанционного банковского обслуживания «Клиент-Банк»
для юридических лиц, индивидуальных предпринимателей и физических лиц,
занимающихся в установленном законодательством
Российской Федерации порядке частной практикой в АО «Банк ЧБРР»

АО «Банк ЧБРР»

_____

_____

_____

(должность, название Клиента, ФИО полностью)

Заявление на подключение к Мобильному приложению

На основании настоящего заявления, прошу произвести подключение услуги по работе в системе ДБО ЮЛ посредством Мобильного приложения
Клиенту_____
ИНН_____

Номер телефона для регистрации:

+	7										

Клиент заполняет собственноручно

Канал взаимодействия «Базовый» ☐
Канал взаимодействия «Информационный»[4] ☐

РУКОВОДИТЕЛЬ ОРГАНИЗАЦИИ

ДОЛЖНОСТЬ	ПОДПИСЬ	ИНИЦИАЛЫ, ФАМИЛИЯ	ДАТА		

М.П.

[4] *В режиме просмотра (с закрытым доступом на выполнение расходных операций по счетам) без использования USB-токена.*

Приложение № 2
к Условиям предоставления и обслуживания
системы дистанционного банковского обслуживания «Клиент-Банк»
для юридических лиц, индивидуальных предпринимателей и физических лиц,
занимающихся в установленном законодательством
Российской Федерации порядке частной практикой в АО «Банк ЧБРР»

Перечень электронных документов, передаваемых по Системе ДБО ЮЛ

1. В рамках Системы, Клиент и Банк имеют возможность обмениваться следующими видами документов (указаны наименования внешних видов форм документов в Системе ДБО ЮЛ), к которым предоставлен доступ:

1.1. Рублевые документы:
- Платежное поручение;
- Платежное требование;
- Заявка на наличные.

1.2. Валютные документы:
- Заявление на перевод;
- Межбанковский перевод;
- Поручение на покупку иностранной валюты;
- Поручение на продажу иностранной валюты;
- Конверсионная операция по on-line курсу;
- Поручение на конвертацию валюты;
- Уведомление о зачислении валюты на транзитный счет;
- Распоряжение о списании валюты с транзитного счета;
- Распоряжение на обязательную продажу иностранной валюты;
- Поручение на обратную продажу иностранной валюты.

1.3. Валютный контроль:
- Сведения о валютных операциях;
- Справка о подтверждающих документах;
- Заявление о постановке на учет контракта (кредитного договора);
- Заявление о снятии с учета контракта (кредитного договора);
- Заявление о внесении изменений в раздел I ведомости банковского контроля;
- Справка о поступлении валюты РФ.

1.4. Зарплатный проект:
- Зарплатный реестр (ведомость);
- Присоединение к зарплатному проекту;
- Открепление от зарплатного проекта;
- Изменение сведений о сотруднике.

1.5. Входящие документы:
- Подтверждение сделки;
- Входящее платежное требование;
- Подтверждение остатков;

1.6. Прочие права на документы:
- Рублевые выписки;
- Валютные выписки;
- Оборотно-сальдовая ведомость;
- Приложения к выпискам
- Справочник сотрудников.

1.7. Письма.

1.8. Система быстрых платежей:
- Регистрация клиента в СБП;
- Регистрация QR - кода в СБП;
- Активация QR - кода в СБП;
- Возврат средств по операции СБП;
- Подключение внешнего устройства или системы.

1.9. Автоматизированная упрощенная система налогообложения.

1.10. Электронные информационные документы, не являющиеся расчетными документами и обеспечивающие обмен информацией при совершении расчетов и проведении операций по Счету Клиента (выписки по счету, справки по счету, запросы, отчеты, информационные сообщения).

1.11. Иные документы, предоставляемые Клиентом в Банк в т.ч. с целью заключения договоров с Банком/ исполнения условий заключенных договоров с Банком.

Приложение № 3
к Условиям предоставления и обслуживания
системы дистанционного банковского обслуживания «Клиент-Банк»
для юридических лиц, индивидуальных предпринимателей и физических лиц,
занимающихся в установленном законодательством
Российской Федерации порядке частной практикой в АО «Банк ЧБРР»

Перечень технических средств АРМ Клиента для установки и функционирования Системы ДБО ЮЛ

Для установки и функционирования Системы ДБО ЮЛ, АРМ Клиента (персональный компьютер, на который устанавливается Система), должен удовлетворять следующим требованиям:

1. Современный компьютер с операционной системой. Работа в Системе возможна на следующих ОС:
   - Microsoft Windows: 10 (x86/x64) и выше;
   - Apple Mac OC X: 10.12 и выше;
   - Linux x64.

Для доступа к Системе ДБО ЮЛ посредством смартфона необходимо устройство с ОС Android с версией ОС не ниже 8.0.

2. Наличие под Систему свободного места на диске не менее 1 Гб.

3. Web-браузер с поддержкой плагина «BIFIT Signer» для использования электронной подписи с применением аппаратных устройств USB-токен. Поддержка плагина обеспечена в следующих браузерах:
   - Microsoft Edge;
   - Firefox - последняя версия;
   - Opera - последняя версия;
   - Chrome - последняя версия;
   - Safari - при условии совместного использования с Mac OS X.

4. Установленное, подключенное и настроенное коммуникационное оборудование (модем, сетевая карта и др.) обеспечивающее возможность установления соединения с Банком по информационно-коммуникационной сети «Интернет».

5. Наличие USB-порта, для подключения защищенного ключевого носителя USB-токен.

6. Персональный аппаратный криптопровайдер в виде USB-токена, в количестве, соответствующему п. 1.15 Условий к Договору, для хранения ключа электронной подписи (ЭП). Аппаратный криптопровайдер (USB-токен) предназначен для генерации ключей ЭП внутри самого устройства и обеспечения их защищенного неизвлекаемого хранения. Формирование ЭП под электронным документом происходит внутри самого устройства. Аппаратный криптопровайдер в виде USB-токена предоставляется Банком.

7. Доступ в информационно-телекоммуникационную сеть «Интернет». Минимальная скорость соединения – 33,6 Кбит/сек и выше.

8. Для обеспечения защиты конфиденциальной информации необходимо наличие СКЗИ на компьютере пользователя. Средства криптографической защиты информации используется для реализации функций формирования ключей шифрования и электронной подписи, выработки и проверки электронной подписи, шифрования и имитозащиты информации, шифрования трафика. При работе с модулем для криптографической защиты информации используются аппаратные криптопровайдеры (USB-токен).

9. Компьютер должен быть оборудован лицензионным программным средством антивирусной защиты с ежедневным обновлением базы данных сигнатур вирусов.

Если используемые программные или технические средства не соответствуют данным требованиям, то **Вы подвержены дополнительным рискам информационной безопасности и Банк не гарантирует возможность подключения или правильную работу в Системе ДБО ЮЛ**.

Приложение № 4
к Условиям предоставления и обслуживания
системы дистанционного банковского обслуживания «Клиент-Банк»
для юридических лиц, индивидуальных предпринимателей и физических лиц,
занимающихся в установленном законодательством
Российской Федерации порядке частной практикой в АО «Банк ЧБРР»

Требования к
Клиенту по обеспечению информационной безопасности при эксплуатации Системы ДБО ЮЛ, ключевой информации и СКЗИ

1. Требования по организационному обеспечению безопасности АРМ Клиента с Системой ДБО ЮЛ.

1.1. В организации Клиента назначаются (определяются) должностные лица, ответственные за обеспечение информационной безопасности и эксплуатацию Системы ДБО ЮЛ.

1.2. В организации Клиента разрабатываются нормативные документы, регламентирующие вопросы информационной безопасности и эксплуатации Системы ДБО ЮЛ.

1.3. К работе с Системой допускаются работники, имеющие навыки работы на персональном компьютере, ознакомленные с Условиями.

1.4. Работа в информационно-телекоммуникационной сети «Интернет» на ПК пользователя Системы не должна допускать посещения сайтов сомнительного содержания, развлекательных ресурсов, сайтов социальных сетей, игровых интернет-ресурсов. Рекомендуется на таких АРМ предоставлять доступ к информационно-телекоммуникационной сети «Интернет» только для соединения с Официальным сайтом Банка для работы в Системе.

1.5. Не допускается запуск на АРМ пользователя Системы программ несанкционированного снятия защиты с программного обеспечения.

1.6. Не допускается установка программного обеспечения, позволяющая осуществлять перехват, преобразование данных Системы.

1.7. Обеспечить своевременную установку обновлений безопасности операционной системы и прикладных программ на АРМ.

1.8. В настройках операционной системы АРМ Клиента необходимо отключить автозапуск программ с внешних носителей.

2. Требования по размещению АРМ Клиента с Системой ДБО ЮЛ и режиму охраны.

2.1. Помещения, в которых размещаются АРМ Клиента и используются средства криптографической защиты информации, должны иметь ограниченный доступ и обеспечивать конфиденциальность проводимых работ.

2.2. Размещение помещений с ограниченным доступом и их оборудование должны исключать возможность бесконтрольного проникновения в них посторонних лиц, и обеспечивать сохранность находящихся в этих помещениях конфиденциальных документов и технических средств.

2.3. Размещение оборудования, технических средств, предназначенных для обработки конфиденциальной информации, должно соответствовать требованиям техники безопасности, санитарным нормам и требованиям пожарной безопасности.

2.4. Входные двери помещений с ограниченным доступом должны быть оборудованы механическим и кодовым замками, или хотя бы одним из них, обеспечивающими надежное закрытие помещений, а также местом для опечатывания двери в нерабочее время.

2.5. Окна и двери должны быть оборудованы охранной сигнализацией, связанной с пультом централизованного наблюдения за сигнализацией.

2.6. Размещение технических средств в помещении с ограниченным доступом должно исключать возможность визуального просмотра конфиденциальных документов и экранов мониторов, на которых она отражается через окна.

2.7. В помещения с ограниченным доступом допускаются руководитель организации Клиента, технические сотрудники, сопровождающие работу Системы и ответственные за работу с ключевой информацией (Уполномоченные лица) на АРМ Клиента для работы в Системе. При этом, право самостоятельной работы на АРМ в Системе разрешено только Уполномоченным лицам Клиента, техническим сотрудникам только в присутствии Уполномоченных лиц.

2.8. Системные блоки АРМ Клиента с Системой ДБО ЮЛ, оборудуются средствами контроля вскрытия (пломба, голографическая наклейка на местах вскрытия крышек корпуса).

2.9. При передаче в ремонт АРМ Клиента, должно быть удалено программное обеспечение, предназначенное для работы в Системе. В случае невозможности удаления, из системного блока должен быть изъят жесткий диск.

2.10. По возврату АРМ Клиента из ремонта, перед началом эксплуатации, ПК должен быть проверен лицензионными средствами антивирусной защиты с актуальными базами данных сигнатур вирусов, а также обследован на наличие стороннего/неизвестного программного обеспечения, не предназначенного для работы в Системе ДБО ЮЛ.

3. Требования по обеспечению безопасности при работе с ключевой информацией.

3.1. Порядок хранения и использования ключевых документов должен исключать возможность несанкционированного доступа к ним.

3.2. Все носители ключевой информации должны быть зарегистрированы в журнале поэкземплярного учета с указанием даты постановки на учет, даты генерации секретного ключа, номера ключа, фамилии ответственного исполнителя и его подписи.

3.3. Учет и обеспечение хранения ключевой информации, носителей, поручается руководством Клиента сотруднику, ответственному за информационную безопасность в организации либо ответственным за работу с ключевой информацией в Системе ДБО ЮЛ, каждый из которых несет персональную ответственность за ее сохранность. Доступ неуполномоченных лиц к носителям ключевой информации должен быть исключен.

3.4. В случае сменного режима работы, отпуска, болезни и т.п., ответственных, передача носителей ключевой информации осуществляется по акту или журналу приема-передачи, с указанием даты и времени передачи, номера ключевого носителя, идентификатора Ключа ЭП, ФИО сотрудников и подписей.

3.5. Для хранения ключевых носителей, предназначенных для работы в Системе, выделяются сейфы или металлические хранилища для каждого ответственного, которые оборудованы внутренними замками и имеют место для опечатывания в конце рабочего дня. Сейф должен быть надежно закреплен к полу или стене. Вторые экземпляры ключей от сейфа или металлического хранилища должны храниться в службе безопасности или у руководителя организации, не имеющих права его опечатывания. Дубликаты должны быть помещены в боксы или конверты, опечатаны, с проставлением печати или подписи на месте склеивания конверта. Хранение ответственным носителей ключевой информации в сейфе или металлическом хранилище, закрепленном за другим, не допущенным к ключевой информации лицом, разрешается только в отдельно опечатанном пользователем боксе, пакете, которое имеет место для опечатывания.

3.6. Подключать съемные носители с ключевой информацией необходимо только в момент начала работы с Системой и обязательно извлекать его из ПК сразу после окончания работы в Системе. В остальных случаях, по завершении работы в Системе, ключевые носители должны находиться в сейфе.

3.7. При транспортировке ключевых носителей с ключевой информацией создавать условия, обеспечивающие защиту от физических повреждений и внешнего воздействия на ключевую информацию.

3.8. Запрещается снимать несанкционированные копии ключевой информации с носителей, знакомить с содержанием ключевых носителей, передавать лицам, не допущенным к работе с ними, хранить ключевую информацию на жестких дисках ПК, устанавливать носитель в порты ПК, не предназначенных для работы в Системе ДБО ЮЛ записывать на носители постороннюю информацию.

3.9. Уничтожение выведенных из действия закрытых ключей ЭП производить путем двойного форматирования по истечении одного рабочего дня с момента генерации и ввода в действие нового ключа ЭП, при условии, что новый ключ ЭП записан на другой носитель ключевой информации, с отметкой в журнале учета и хранения ключевой информации.

3.10. Своевременно проводить смену ключевой информации при окончании срока действия, смене Уполномоченных лиц, имеющих право подписи, а также при обнаружении факта компрометации ключей ЭП.

4. Требования по обеспечению безопасности при использовании услуги SMS-подтверждения и SMS-оповещения

4.1. Необходимо ограничить доступ к телефону, на номер которого приходят SMS с кодами подтверждения платежей.

4.2. При смене номера телефона SMS-подтверждения или его утере, незамедлительно обращайтесь в Банк для его замены в Системе ДБО ЮЛ. Добавление/Изменение номера телефона SMS-оповещения выполняется Клиентом самостоятельно (без обращения в Банк) в меню «Мониторинг» Системы ДБО ЮЛ, при условии полученного в установленном порядке доступа.

4.3. Перед вводом кода для подтверждения платежа, полученного по SMS, убедитесь, что информация, полученная в SMS, соответствует фактическим реквизитам платежа (проверяйте счет, сумму, БИК и т.д.)

4.4. Для SMS-услуг не рекомендуется использовать модели телефонов с операционными системами iOS и Android, которые подвержены компрометации и взлому, в следствие чего, злоумышленник может получить возможность перехвата SMS сообщений.

5. При этом обязательным условием предоставления Банком SMS-подтверждения и SMS-оповещения является наличие технической возможности у оператора сотовой связи, осуществляющего обслуживание телефонного номера, принимать и отправлять SMS-сообщения между SMS-Центром Банка и Клиентом с использованием данного номера.

Приложение № 5
к Условиям предоставления и обслуживания
системы дистанционного банковского обслуживания «Клиент-Банк»
для юридических лиц, индивидуальных предпринимателей и физических лиц,
занимающихся в установленном законодательством
Российской Федерации порядке частной практикой в АО «Банк ЧБРР»

ДОВЕРЕННОСТЬ № ___

_____
(город (село, поселок, район), край, область, республика, автономная область, автономный округ полностью)

_____
(дата, месяц, год прописью)

_____
(полное наименование организации Клиента)

_____, ИНН _____

Адрес местонахождения (юридический и фактический (при расхождении адресов): _____,
(индекс)

Российская Федерация, _____
(край, область, республика, автономная область, автономный округ полностью, район)

_____
(город (село, поселок), улица, номер дома)

в лице _____
(должность Уполномоченного лица, владельца ключа ЭП)

_____

_____
(ФИО и паспортные данные (год рождения, адрес регистрации, реквизиты паспорта полностью)

действующего на основании _____
(Устав, Положение, иной документ, нужное указать)

уполномочивает_____
(должность)

_____

_____
(ФИО и паспортные данные (год рождения, адрес регистрации, реквизиты паспорта полностью
уполномоченного представителя организации)

телефон представителя для связи: _____

на выполнение следующих действий:

1. Предоставлять и получать от моего имени на бумажном носителе сертификат ключа проверки электронной подписи в АО «Банк ЧБРР».
2. Подписывать от моего имени Акт приема-передачи средств криптографической защиты информации.
3. Получать от моего имени программные и аппаратные средства криптографической защиты информации для работы в Системе ДБО ЮЛ.

Подпись _____ удостоверяю:
(полностью ФИО уполномоченного представителя организации)

_____
(подпись уполномоченного представителя организации)

Настоящая доверенность выдана сроком до _____
(дата, месяц, год прописью)

включительно. Полномочия по доверенности не могут быть переданы другим лицам.

_____	_____	_____
(должность руководителя)	(подпись)	(И.О. Фамилия)

М.П.

Приложение № 6
к Условиям предоставления и обслуживания
системы дистанционного банковского обслуживания «Клиент-Банк»
для юридических лиц, индивидуальных предпринимателей и физических лиц,
занимающихся в установленном законодательством
Российской Федерации порядке частной практикой в АО «Банк ЧБРР»

Акт приема-передачи средств криптографической защиты информации

г. Симферополь «____» _____ 202__г.

Мы, нижеподписавшиеся, представитель АО «Банк ЧБРР» в лице _____
(должность, ФИО полностью)

действующего на основании доверенности № _____ от «___» _____ 202__ г. с одной стороны,
и _____,
(название Клиента, ИНН)

в лице_____ действующего на основании _____,
(должность, ФИО полностью)

с другой стороны, составили настоящий Акт о том, что в рамках Договора об использовании системы дистанционного банковского обслуживания «Клиент-Банк» от _____ № _____ и Условиями предоставления и обслуживания системы дистанционного банковского обслуживания «Клиент-Банк» клиентам АО «Банк ЧБРР», Банк передал, а Клиент принял:

I. ---------- заполняется при передаче аппаратного СКЗИ USB-токен

1. Аппаратный(е) ключевой(ые) носитель(и) USB-токен, не содержащий(е) Ключи электронной подписи, в количестве ____ (_____) штук.
(прописью)

В случае отказа от USB-токена – поставить прочерки в таблице Раздела I.

№	ID (s/n) аппаратного носителя	Название аппаратного носителя (например, РУТОКЕН или MS_KEY K - Ангара)
1.		
2.		
3.		
4.		

Аппаратный(е) ключевой(ые) носитель(и) USB-токен передан Клиенту в индивидуальном пакете, в опечатанном виде без надрывов и повреждений, и при его передаче Сторонами приняты меры по обеспечению конфиденциальности.

II. ---------- заполняется при передаче программных СКЗИ (криптобиблиотеки)

1. Архив в электронном виде, переданный по защищенному каналу связи, содержащий программные криптобиблиотеки СКЗИ «Крипто-КОМ 3.5», документацию и ПО контроля целостности. Криптобиблиотеки предназначены для использования только в составе Системы ДБО ЮЛ «iBank 2».

№ п/п	Наименование СКЗИ	Учетный номер СКЗИ
1.	Крипто-КОМ 3.5	№2424/230726/ (указать номер договора)

Получен	
Нет	

– поставить отметку V при работе с криптобиблиотеками и отказе от USB-токена, в поле «Нет» поставить прочерк

– поставить отметку V при получении USB-токена и отказа от работы с криптобиблиотеками, в поле «Получен» поставить прочерк

Установочный комплект СКЗИ в электронном виде получен Клиентом по защищенному каналу связи и при его передаче Сторонами приняты меры по обеспечению конфиденциальности.

Настоящий Акт составлен в двух экземплярах для каждой из сторон, является неотъемлемой частью Договора и имеет одинаковую юридическую силу.

Клиент (владелец ключа ЭП или лицо по доверенности):

АО «Банк ЧБРР»[1]

_____ (должность)

/ _____ (подпись) (Инициалы, Фамилия)

М.П.

_____ (должность)

/ _____ (подпись) (Инициалы, Фамилия)

М.П.

Ответственный исполнитель[2]

Передачу аппаратного носителя USB-токен подтверждаю

_____ (должность, № Дополнительного офиса)

/ _____ (подпись) (Инициалы, Фамилия)

М.П.

[1] *Заполняется уполномоченным работником Банка*

[2] *Заполняет начальник ДО (лицо его замещающее).*

Приложение
к Приложению № 6
Акт приема-передачи средств
криптографической защиты информации

программные СКЗИ «Крипто-КОМ 3.5» (вариант исполнения 1, 2) – криптографические библиотеки (опись установочного комплекта) *

Программа для ЭВМ «Средство криптографической защиты информации «Крипто-КОМ 3.5», все исключительные права на которую принадлежат ЗАО «Сигнал-Ком», имеет Сертификаты соответствия ФСБ России рег. №СФ/114-4579 от 16.05.2023, рег. №СФ/124-4580 от 16.05.2023, является неотчуждаемой компонентой ПрЭВМ «iBank 2» и предназначена для использования только в составе ПрЭВМ «iBank 2». Регистрационный номер эталонного экземпляра криптобиблиотеки, переданной Клиенту 2424/230726.

Имя	Контрольная сумма GOSTH	Описание
Программное обеспечение контроля целостности (rush), утилита для удаления файлов (wipe), программное обеспечение регламентного контроля ДСЧ (ccrandreg)		
\bin\ccom_3_5_0_0_linux_gnu_x86_64:		
ccrandreg	28d9c5c8458c1cd4883d6a7718b57e473ed7b05c5b75e6ec6345a4430a964556	Для ОС Linux (64 бит)
rush	a328898f88a0318383957a0a9978ae58e80edfa8b63eabafa7b47446bcc60bc4	
wipe	962019f9018e2e0eb54fd823240fae672b53c49b78c41e7f86b65ae59d9ad391	
\bin\ccom_3_5_0_0_win32_x86:		
ccrandreg.exe	cb6ed19bb7281c44b0798d0f4fb85a21af598a06bacbb2776996a5449a143384	Для ОС Windows (32 бит)
rush.exe	e930aa2d7518a93248248ccc743e3e4bbdabee5f27ea56d3e7689e64abcd2fd2	
wipe.exe	4d8f4fc7c348023e34d1613dc613294ead7d6cf589a911cacbc19105b3b09c80	
\bin\ccom_3_5_0_0_win64_x86_64:		
ccrandreg.exe	49ae7ff8d75575faa88a234c01b534364a4664231f601d9fd110c723f7bca4f6	Для ОС Windows (64 бит)
rush.exe	562235e45048a227ab2b929f85ac2c31ecddf22c92b0e65c84724a1a6443b7a8	
wipe.exe	443fc035419608bdd3a4b89182599dfd53afb8babb23f9d085f8bf2611fb371a	
Модуль СКЗИ «Крипто-КОМ 3.5» (вариант исполнения 1, 2) Для ПрЭВМ «iBank 2»		
\lib\ccom_3_5_0_0_linux_gnu_x86_64:		
libccom.so	e2796abfc19a102076f4ba3f72c0f36cf4277a6d55b42220f3540214ff565848	Для ОС Linux (64 бит)
libccom.so.sig	d584b1896a61b2377924302865c4a70cfa991e84d774e29d011ffee5154b0e58	
libscbrng.so	82cb91ffcb1e74f2c4ac6f28f36d1554887532c0682c3da5cac22342071274bd	
\lib\ccom_3_5_0_0_win32_x86:		
ccom.dll	a35a5dc15d839f5fa24f467ac2320df6b162682b57dc7065c9ec4c1f60ff2937	Для ОС Windows (32 бит)
ccom.dll.sig	12a6b507c169b82547d2ccf71138fd91915d87ceb403e00d9a0750996e1b1661	
scbrng.dll	5482d8dfaad2969b4f7eee4970874e1232ee00418b2805739c6fd2a0e94011e0	
\lib\ccom_3_5_0_0_win64_x86_64:		
ccom.dll	74fc695301ff976cc387b796c5aa4753a534e432f7d0c51766a887a2261a14dc	Для ОС Windows (64 бит)
ccom.dll.sig	0f88c8ab47d9c49ca98564ceb22a4994cb9294795148752c5cc2a31f6c8a9e5b	
scbrng.dll	0c6e2793c1fbedf6471ed236f6f4b18ed8e2649e8cbec2b9815354591f9c3f02	

АО «Банк ЧБРР» **

(должность)

/

(подпись) (Инициалы, Фамилия)

Клиент (владелец ключа ЭП или лицо по доверенности):

(должность)

/

(подпись) (Инициалы, Фамилия)

* *Заполняется в случае подключения к Системе «Клиент-Банк» с использованием программных СКЗИ.*

** *Заполняется уполномоченным работником Банка*

Приложение № 7
к Условиям предоставления и обслуживания
системы дистанционного банковского обслуживания «Клиент-Банк»
для юридических лиц, индивидуальных предпринимателей и физических лиц,
занимающихся в установленном законодательством
Российской Федерации порядке частной практикой в АО «Банк ЧБРР»

Уведомление о компрометации ключа ЭП
от «____» _____ 202__г.

Я, _____
_____
(должность, название организации, ФИО владельца[5] ключа ЭП полностью)

настоящим уведомляю о компрометации ключа ЭП, предназначенного для подписи электронных документов в Системе ДБО ЮЛ «iBank2».

ИНН Организации				
Договор об использовании системы дистанционного банковского обслуживания «Клиент-Банк»	от	«____» _____ 202__г.	№	
Причина компрометации	☐	Смена владельца ключа ЭП		
	☐	Утеря ключевого носителя		
	☐	Вышел из строя ключевой носитель		
	☐	Сбой аппаратно-программного обеспечения		
	☐	Утрата ключевых носителей, с последующим обнаружением или без обнаружения		
	☐	Увольнение, либо смена участка работы сотрудников, имевших доступ к ключевой информации		
	☐	Нарушение правил хранения Ключа ЭП		
	☐	Возникновение подозрений на несанкционированный доступ к месту хранения или использования ключевых носителей, утечку информации или ее искажение		
	☐	Другое (указать)		

_____ _____ _____
(должность) (подпись) (И.О. Фамилия владельца ключа ЭП)

М.П.

ОТМЕТКИ БАНКА:

О получении Уведомления работником Банка:

должность, отдел	подпись	И.О. Фамилия	дата	время

Отметка Администратора информационной безопасности Системы ДБО ЮЛ iBank2:

Уведомление получил

дата	время

Ключ электронной подписи Клиента заблокировал	подпись	И.О. Фамилия	дата	время

[5] *При смене владельца ключа ЭП – указывается ФИО нового владельца.*

Приложение № 8
К Условиям предоставления и обслуживания
системы дистанционного банковского обслуживания «Клиент-Банк»
для юридических лиц, индивидуальных предпринимателей и физических лиц,
занимающихся в установленном законодательством
Российской Федерации порядке частной практикой в АО «Банк ЧБРР»

Заявление
на приостановку/возобновление обслуживания в Системе ДБО ЮЛ

ДАТА			№

НАИМЕНОВАНИЕ КЛИЕНТА				
ИНН				
ДОГОВОР ОБ ИСПОЛЬЗОВАНИИ СИСТЕМЫ ДБО ЮЛ	ОТ		№	

1. ПРИОСТАНОВЛЕНИЕ ОБСЛУЖИВАНИЕ В СИСТЕМЕ ДБО ЮЛ

☐	ПРОСИМ ПРИОСТАНОВИТЬ ОБСЛУЖИВАНИЕ В СИСТЕМЕ ДБО ЮЛ
ДАТА ПРИОСТАНОВЛЕНИЯ ОБСЛУЖИВАНИЯ	

2. ВОЗОБНОВЛЕНИЕ ОБСЛУЖИВАНИЯ В СИСТЕМЕ ДБО ЮЛ:

☐	ПРОСИМ ВОЗОБНОВИТЬ ОБСЛУЖИВАНИЕ В СИСТЕМЕ ДБО ЮЛ
ДАТА ВОЗОБНОВЛЕНИЯ ОБСЛУЖИВАНИЯ	
ПРИЧИНА ПРЕРЫВАЕНИЯ ОБСЛУЖИВАНИЯ	☐ БАНКОМ В СООТВЕТСТВИИ С НАСТОЯЩИМИ УСЛОВИЯМИ ☐ ПО ЗАЯВЛЕНИЮ ОТ « » _20 Г №

Клиент

ДОЛЖНОСТЬ	ПОДПИСЬ	И.О. ФАМИЛИЯ
руководитель		

М.П.

ОТМЕТКИ БАНКА:

О получении Заявления работником Банка:

должность, отдел	подпись	И.О. Фамилия	дата			время	

Отметка Администратора информационной безопасности системы ДБО ЮЛ iBank2:

Заявление получил

дата			время	

Ключ электронной подписи Клиента заблокировал/разблокировал **(нужное подчеркнуть)**							
	подпись	И.О. Фамилия	дата			время	

Приложение № 9
к Условиям предоставления и обслуживания
системы дистанционного банковского обслуживания «Клиент-Банк»
для юридических лиц, индивидуальных предпринимателей и физических лиц,
занимающихся в установленном законодательством
Российской Федерации порядке частной практикой в АО «Банк ЧБРР»

Рекомендации
по настройке и эксплуатации АРМ Клиента, на которых устанавливаются или используются клиентские части Системы ДБО ЮЛ

С целью минимизации рисков, связанных с подключением и использованием клиентской части Системы ДБО ЮЛ, Банк рекомендует:

1. Относительно организации доступа к операционной системе АРМ Клиента.

1.1. Учетная запись, под которой осуществляется работа в Системе ДБО ЮЛ, не должна иметь права доступа «Администратор» к операционной системе ("Администратор" в Windows). Учетная запись пользователя Системы ДБО ЮЛ должна быть уровня «пользователь» "User".

1.2. Учетная запись «Гость» должна быть отключена.

1.3. Не допускается автоматический вход пользователя в Систему ДБО ЮЛ (без ввода логина и пароля).

1.4. Пароли учетных записей и доступа в Систему ДБО ЮЛ должны соответствовать следующим требованиям:

- Содержать не менее восьми символов
- Включать буквы разных регистров (A, a,)
- Включать цифры (0-9)
- Включать специальные символы (@#$%&)

1.5. Запрещается оставлять пароли учетных записей пользователей в доступном месте, разглашать и передавать их другим лицам.

1.6. Пароли должны быть изменены в случае подозрения относительно их компрометации.

2. Относительно организации антивирусной защиты АРМ Клиента.

2.1. На АРМ Клиента должно быть установлено и настроено лицензионное антивирусное программное обеспечение актуальной версии, которая включает следующие компоненты:

- Файловый антивирус;
- Почтовый антивирус;
- Веб-антивирус;
- Защита от сетевых атак (Антихакер);
- Компонент защиты от рекламы (adware) и шпионского программного обеспечения (spyware);
- Программный межсетевой экран (firewall).

В случае отсутствия компонента "Программный межсетевой экран" необходимо установить отдельное программное дополнение с аналогичным функционалом.

2.2. Антивирусное ПО должно проводить активный мониторинг всех внешних носителей, которые подключаются к системе.

2.3. Антивирусное ПО должно проводить полную проверку жесткого диска компьютера на наличие вредоносного ПО не реже, чем один раз в неделю.

2.4. Почтовый антивирус должен проверять все входящие и исходящие сообщения.

2.5. Межсетевой экран должен быть настроен по принципу "минимизации" ресурсов.

2.6. Антивирусное ПО должно быть настроено таким образом, чтобы обеспечивать надежную защиту без участия пользователя.

2.7. Антивирус обязательно должен быть обновлен до актуальной версии, и обеспечивать ежедневное обновление базы данных сигнатур вирусов.

2.8. Если возникло подозрение, что АРМ заражен (нетипичная реакция на выполняемые команды пользователя, появляющиеся непонятные окна, получение незапрашиваемых SMS с ключом для входа или для проведения операции и т.п.) - немедленно прекратите работу в Системе, извлеките USB-токен и обратитесь к своему ИТ-специалисту для выяснения причин происходящего. До выяснения причин пользоваться Системой ДБО ЮЛ крайне не рекомендуется.

3. Относительно организации эксплуатации системного ПО

3.1. Все программное обеспечение (ПО) на АРМ Клиента (включая операционную систему), должно быть лицензионное, и получено из достоверных источников.

3.2. При распределении доступа к локальным ресурсам на АРМ Клиента должен быть применен принцип "минимизации" ресурсов:

– устанавливать только ПО для взаимодействия с Системой ДБО ЮЛ, и ПО системы защиты информации;

– установка иного ПО должно быть четко контролируемо и регламентировано только в случае крайней необходимости;

– пользователь системы должен осуществлять личный контроль за нетипичной робой компьютера и ПО (появление всплывающих окон, которых не было, изменение шрифтов Интернет-страницы Клиент-банка, появление ПО, которого он не устанавливал, и т. п.)

3.3. Все ресурсы общего пользования на АРМ Клиента должны быть отключены.

3.4. Не допускается установка на рабочие станции, которые задействованы при работе в Системе ДБО ЮЛ, программного обеспечения типа "удаленного администрирования" (TeamViewer, RemoteDesktop, Radmin, DameWare, VNC, Hamachi, RemoteOfficeManager и другие).

3.5. Все программное обеспечение должно постоянно обновляться.

3.6. Не устанавливайте и не сохраняйте подозрительные файлы, полученные из ненадежных источников, неизвестных web-сайтов, присланные по электронной почте и т.д. Такие файлы необходимо немедленно удалять. В случае необходимости загрузки файла, обязательно проверьте его антивирусным ПО перед использованием.

4. Относительно организации безопасной работы в Системе ДБО ЮЛ посредством Web-интерфейса

4.1. Не проводить работу в Системе ДБО ЮЛ с рабочих станций, которые находятся в "не доверенной" зоне (Интернет-кафе, в местах, где установлено видео наблюдение, на домашнем ПК).

4.2. При необходимости доступа сотрудников к другим ресурсам сети Internet, отправки/получения электронной почты, пользования социальными сетями и прочее, необходимо использовать отдельный ПК.

4.3. Держать в тайне пароль. При подозрении, относительно компрометации пароля следует немедленно его изменить. При вводе пароля убедитесь, что за Вами никто не наблюдает.

4.4. Не допускается хранение носителей ключевой информации в доступном месте без визуального присмотра.

4.5. Не допускается передача носителей ключевых данных посторонним лицам.

4.6. Запрещается оставлять без присмотра АРМ Клиента с авторизованной (запущенной к исполнению) Системой ДБО ЮЛ. При необходимости покинуть рабочее место АРМ, произвести блокирование учетной записи, путем одновременного нажатия комбинации клавиш Win+L, или Ctrl+Alt+Del, после чего выбрать «Блокировка».

4.7. При завершении работы выполнить выход из Системы ДБО ЮЛ, отсоединить носитель ключевой информации USB-токен.

4.8. Не используйте функцию хранения паролей, которое предлагается браузером или другим ПО.

4.9. Не допускается осуществлять доступ к Системе ДБО ЮЛ с использованием общедоступных беспроводных сетей. Если Ваша организация использует корпоративную беспроводную сеть, доступ к ней должен быть организован по "белым спискам" MAC адресов и строго ограничен. Должен быть установлен уровень шифрования сессии WPA2 с шифрованием по стандарту AES.

4.10. Для хранения секретных ключей следует использовать защищенные носители ключевой информации, которые рекомендуются Банком.

4.11. О любых замеченных значительных и/или нетипичных изменениях в работе Системы ДБО ЮЛ, таких например как изменение интерфейса сайта https://cb.chbrr.crimea.com или его частей, появление необходимости выполнения новых, ранее не используемых действий при работе с Системой, следует воздержаться от введения данных для авторизации в Системе ДБО ЮЛ и сообщить об этом в Банк по известным Вам телефонам.

4.12. При увольнении или смене должностных обязанностей Уполномоченных лиц, которые имели доступ к ключевым данным и Системе ДБО ЮЛ, выполните изменение паролей и перегенерацию ключей ЭП.

4.13. Необходимо обеспечить безопасную работу с Системой ДБО ЮЛ. Внимательно контролируйте состояние Ваших счетов (рекомендуется 1–2 раза в день), даже если Вы не проводите платежные операции в Системе.

Кроме этого, стоит обратить внимание:

Банк ни в коем случае не станет осуществлять запрос с использованием электронной почты, SMS сообщений или телефонной связи Ваших паролей, номеров счетов и т.д. Банк не высылает своим Клиентам ссылки для осуществления обновлений, или загрузки и установки ПО (в том числе мобильного). При получении сообщений такого содержания ни в коем случае не раскрывайте конфиденциальные данные и известите об этом Банк.

В случае возникновения подозрения, относительно факта или попытки несанкционированного доступа к АРМ Клиента, Системе ДБО ЮЛ, немедленно прекратите работу с скомпрометированным компьютером, отсоедините его от сети и сообщите об этом по телефону в обслуживающее Клиента подразделение Банка (в соответствии с режимом работы подразделения) или в Службу поддержки Клиентов: +7 (3652) 605-805; +7 (978) 835-21-12; +7 (978) 835-22-11; +7 (978) 099-03-80 (в соответствии с режимом работы подразделения).

Придерживайтесь дальнейших рекомендаций Банка.

Приложение № 10
к Условиям предоставления и обслуживания
системы дистанционного банковского обслуживания «Клиент-Банк»
для юридических лиц, индивидуальных предпринимателей и физических лиц,
занимающихся в установленном законодательством
Российской Федерации порядке частной практикой в АО «Банк ЧБРР»

Заявление на подключение/отключение услуги, изменение номера(ов) телефона SMS-подтверждения[6]

☐ 1. На основании настоящего заявления, по счету №_____ Договор об использовании системы дистанционного банковского обслуживания «Клиент-Банк» №_____ от «___» _____202__г., с «___» _____202_г. прошу **произвести подключение услуги SMS-подтверждения электронных платежей в Системе ДБО ЮЛ** (ОБЯЗАТЕЛЬНАЯ опция при подключении к Системе ДБО ЮЛ с помощью программных СКЗИ (криптографических библиотек))

+ 7										
+ 7										

☐ 2. На основании настоящего заявления, по счету №_____ Договор об использовании системы дистанционного банковского обслуживания «Клиент-Банк» №_____ от «___» _____202__г., с «___» _____202_г. **прошу произвести отключение услуги SMS-подтверждения электронных платежей в Системе ДБО ЮЛ** (не распространяется на вариант подключения к Системе ДБО ЮЛ с помощью программных СКЗИ (криптографических библиотек)).

☐ 3. На основании настоящего заявления, по счету №_____ Договор об использовании системы дистанционного банковского обслуживания «Клиент-Банк» №_____ от «___» _____202__г., с «___» _____202_г. прошу произвести **изменение номера(ов) телефона** для **услуги SMS-подтверждения электронных платежей в Системе ДБО ЮЛ**

+ 7										
+ 7										

РУКОВОДИТЕЛЬ ОРГАНИЗАЦИИ

ДОЛЖНОСТЬ	ПОДПИСЬ	ИНИЦИАЛЫ, ФАМИЛИЯ	ДАТА		

М.П.

[6] *Необходимо заполнить соответствующую часть Приложения № 10.*

Приложение № 11
к Условиям предоставления и обслуживания
системы дистанционного банковского обслуживания «Клиент-Банк»
для юридических лиц, индивидуальных предпринимателей и физических лиц,
занимающихся в установленном законодательством
Российской Федерации порядке частной практикой в АО «Банк ЧБРР»

Заявление о подтверждении использования ЭП в системе ДБО "iBank"
от 14.04.2025

Банку АО "БАНК ЧБРР"

Подтверждаем правомочность использования ключа проверки электронной подписи для работы в системе ДБО "iBank" нашего представителя

1. Владелец ключа проверки ЭП		
1.1	**ФИО**	ИВАНОВ ИВАН ИВАНОВИЧ
1.2	**Должность**	ГЕНЕРАЛЬНЫЙ ДИРЕКТОР
1.3	**Подразделение**	
1.4	**СНИЛС**	184- .
1.5	**Организация**	ООО " "
1.6	**ИНН**	910
2. Издатель сертификата		
2.1	**Организация**	Федеральная налоговая служба
2.2	**ИНН**	7707329152
2.3	**ОГРН**	1047707030513
3. Сертификат ключа проверки ЭП		
3.1	**Серийный номер**	02 25 00 B1 73 48 A4 17 65 84
3.2	**Срок действия по UTC**	с 05.03.2024 11:12:59 по 05.06.2025 11:22:59
3.3	**Отпечаток**	60 51 81 49 64 C1 AA D9 68 90 3E
4. Ключ проверки ЭП		
4.1	**Алгоритм ключа**	GOST R 34.10-2012-256
4.2	**Значение**	04 40 4d 46 ac 9a e9 ac 24 dd de 26 e3 38 1a e5 4e 90 eb a1 74 47 1b 8f a9 3f 9e 7a 88 30 3f 7f 0a 94 35 13 67 e0 76 ab 30 45 f7 42 44 07 37 8f 95 76 9b 38 da f9
4.3	**Идентификатор в системе "iBank"**	174400 63

☆_____

_____

_____/_____

(подпись, Ф.И.О. Уполномоченного представителя Банка)

Оттиск штампа Банка

Дата приема Заявления о подтверждении использования ключа ЭП в Системе ДБО ЮЛ и проверки сведений о ключе ЭП Клиента, указанных в Заявлении о подтверждении использования ключа ЭП в Системе ДБО ЮЛ

«_____» _____ 20___ г.

_____/_____

(подпись, Ф.И.О. Администратора безопасности системы)

Оттиск штампа Банка

Дата активации ключа ЭП в Системе ДБО ЮЛ

«_____» _____ 20___ г.

☆ *Владелец ключа ЭП указывает должность, ФИО и проставляет свою подпись, и печать.*

Ниже под подписью Владельца ключа ЭП работники Банка (Уполномоченный представитель Банка и Администратор безопасности системы) ставят штампы, Ф.И.О. и подписи о проверке сведений в данном Заявлении (на бумажном носителе) с информацией о ключе ЭП Клиента в Системе ДБО ЮЛ и об активации ключа ЭП в Системе ДБО ЮЛ.

Приложение № 12
к Условиям предоставления и обслуживания
системы дистанционного банковского обслуживания «Клиент-Банк»
для юридических лиц, индивидуальных предпринимателей и физических лиц,
занимающихся в установленном законодательством
Российской Федерации порядке частной практикой в АО «Банк ЧБРР»

В АО «Банк ЧБРР»

ЗАЯВЛЕНИЕ
о расторжении Договора об использовании системы дистанционного банковского обслуживания «Клиент-Банк»

_____

полное наименование юридического лица и его организационно-правовая форма, ИНН; ФИО индивидуального предпринимателя (адвоката, нотариуса), ИНН:

Настоящим заявлением прошу расторгнуть Договор об использовании системы дистанционного банковского обслуживания «Клиент-Банк».

_____ _____ _____
Руководитель (должность) (подпись) (И.О. Фамилия)

М.П.

«____» _____ 202__ г.

Заполняется Банком*

Уведомление получено работником Банка:

должность, отдел	подпись	И.О. Фамилия	дата		

_____
** Заполняется работником Банка, принявшим заявление.*

Приложение № 13.
к Условиям предоставления и обслуживания
системы дистанционного банковского обслуживания «Клиент-Банк»
для юридических лиц, индивидуальных предпринимателей и физических лиц,
занимающихся в установленном законодательством
Российской Федерации порядке частной практикой в АО «Банк ЧБРР»

СЕРТИФИКАТ КЛЮЧА ПРОВЕРКИ ЭЛЕКТРОННОЙ ПОДПИСИ СОТРУДНИКА КЛИЕНТА
В СИСТЕМЕ "iBank"
АО "БАНК ЧБРР"

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

* необязательно для заполнения

Ключ проверки ЭП сотрудника клиента (создан г.)

Идентификатор ключа проверки ЭП _____ Идентификатор устройства _____
Наименование криптосредств _____
Алгоритм ГОСТ Р 34.10-2012 256 бит (1.2.643.7.1.1.1.1) ID набора параметров алгоритма 1.2.643.2.2.35.1

Представление ключа проверки ЭП в шестнадцатеричном виде

```
57 D2 C2 B6 51 63 98 75 0A A5 05 51 BA AE 60 4E
5F                                             D6
F3                                             91
E0 C1 62 5B E9 90 26 8F 76 53 52 02 92 FF E2 6C
```

Личная подпись владельца ключа проверки ЭП

Срок действия (заполняется банком):
с "___" _____ ___г. _____
по "___" _____ ___г. _____

Сертификат ключа проверки ЭП сотрудника клиента действует в рамках договора на обслуживание в системе "iBank 2" N_____ от ___ _____ 20___.

Достоверность приведенных данных подтверждаю

Руководитель организации
_____/_____/
подпись Ф.И.О.

Оттиск печати

Уполномоченный представитель банка
_____/_____/
подпись Ф.И.О.

Оттиск печати Банка

Дата приема сертификата ключа проверки ЭП
"___" _____ 20___г.

Администратор безопасности системы
_____/_____/
подпись Ф.И.О.

Оттиск печати

Дата регистрации сертификата ключа проверки ЭП
"___" _____ 20___г.

Приложение № 14.
к Условиям предоставления и обслуживания
системы дистанционного банковского обслуживания «Клиент-Банк»
для юридических лиц, индивидуальных предпринимателей и физических лиц,
занимающихся в установленном законодательством
Российской Федерации порядке частной практикой в АО «Банк ЧБРР»

АО «Банк ЧБРР»

_____

_____

_____,

(название Клиента, ИНН)

Заявление на сброс PIN-кода

Я, _____,

(должность, название Клиента, ФИО полностью)

установил(а) PIN-код на аппаратное средство криптографической защиты информации MS_KEY K - «Ангара», ID (s/n): 650G1-_____, приобретенный в АО «Банк ЧБРР», который не могу вспомнить.

Прошу сбросить PIN-код на USB-токене "MS_KEY K" - "АНГАРА".

При этом, я проинформирован(а) о том, что на моем USB-токене будут деактивированы все имеющиеся ключи электронной подписи, сброшены PIN-коды и удалены данные пользователя USB-токена, на что даю свое полное согласие.

_____ _____ _____

(дата) (подпись) (И.О. Фамилия)

Приложение № 15.
к Условиям предоставления и обслуживания
системы дистанционного банковского обслуживания «Клиент-Банк»
для юридических лиц, индивидуальных предпринимателей и физических лиц,
занимающихся в установленном законодательством
Российской Федерации порядке частной практикой в АО «Банк ЧБРР»

РЕКОМЕНДАЦИИ
по безопасной работе Клиента в Мобильном приложении Системы ДБО ЮЛ

1. ПОДКЛЮЧЕНИЕ МОБИЛЬНОГО ПРИЛОЖЕНИЯ:

1.1. Подключение Мобильного приложения выполняется Клиентом на своем средстве доступа (смартфоне на операционной системе Android), самостоятельно и за свой счет.

1.2. Для этого средство доступа должно быть подключено к информационно-телекоммуникационной сети «Интернет».

1.3. Клиенту рекомендуется обеспечивать безопасность и целостность программных средств на своем средстве доступа посредством:

– использования средств защиты от вирусов с актуальными антивирусными базами;

– исключения использования на своем средстве доступа программ-закладок и прочего опасного и потенциально опасного программного обеспечения;

– обеспечить установку программ из достоверных источников;

– не допускать несанкционированного доступа третьих лиц к программным средствам и средствам защиты информации, с помощью которых осуществляется обмен электронными документами с Банком.

1.4. В качестве достоверного источника понимается использование Официального сайта Банка в Сети интернет, при этом скачивая установочные файлы с Официального сайта Банка, Клиент обязуется сверить контрольную сумму скачиваемого файла с аналогичной информацией, размещенной на Официальном сайте Банка, а также самостоятельно выполнить необходимые настройки на своем средстве доступа по установке такого типа файлов, если того требует операционная система средства доступа.

2. МЕРЫ БЕЗОПАСНОСТИ ПРИ РАБОТЕ В МОБИЛЬНОМ ПРИЛОЖЕНИИ:

2.1. Для полнофункционального режима работы с возможностью наложения электронной подписи на электронные документы в Мобильном приложении используется только защищенный носитель ключевой информации USB-токен с USB-адаптером. Без применения USB-токена, работа в Мобильном приложении возможна только в режиме просмотра информации (с закрытым доступом на осуществление расходных операций по Счетам).

2.2. Хранение ключей ЭП допускается только на защищенном носителе ключевой информации.

2.3. Категорически запрещается использовать носитель ключевой информации в других целях и на других устройствах, не предназначенных для работы в Мобильном приложении или Web-версии («Интернет-Банк»)

2.4. При утрате или компрометации ключа ЭП Уполномоченное лицо Клиента обязано незамедлительно приостановить любую работу в Мобильном приложении, в том числе остановить операции с электронными документами, при нетипичной (подозрительной) работе средства доступа, извлечь из него ключевой носитель, сообщить в Банк о случившемся инциденте в порядке, указанном в Договоре об использовании системы дистанционного банковского обслуживания «Клиент-Банк».

2.5. При утрате или подозрении на компрометацию средства доступа (смартфон) с подключенным Мобильным приложением, Клиент обязан обратиться в Банк для временного приостановления (блокировки) доступа к Системе ДБО ЮЛ.

2.6. Банк оставляет за собой право заблокировать ключ ЭП Уполномоченного лица Клиента с последующим уведомлением, при выявлении или подозрении факта компрометации ключа ЭП, выявлении факта несоответствия Уполномоченного лица Клиента с лицами, указанными в карточке образцов подписей, выявлении несоответствия реквизитов организации Клиента с данными в Мобильном приложении, подозрении или выявлении несанкционированного списания денежных средств.

2.7. Разблокирование (возобновление действия) ключа ЭП Уполномоченных лиц Клиента осуществляется Банком не позднее дня, следующего за днем устранения выявленных нарушений и представления Клиентом в Банк необходимых актуальных данных и документов.

3. ХРАНЕНИЕ ИНФОРМАЦИИ ПО СФОРМИРОВАННЫМ И ПРОВЕДЕННЫМ ДОКУМЕНТАМ ЧЕРЕЗ МОБИЛЬНОЕ ПРИЛОЖЕНИЕ:

3.1. Информацию о платежах и переводах через Мобильное приложение можно получить в меню «Платежи»: «В работе», «В Банке», «Исполнено».

3.2. Для формирования выписки по счету необходимо зайти в меню «Счета».

3.3. Информация о работе Мобильного приложения хранится в соответствующих регистрах Системы ДБО ЮЛ в течение пяти лет.

Приложение № 16.
к Условиям предоставления и обслуживания
системы дистанционного банковского обслуживания «Клиент-Банк»
для юридических лиц, индивидуальных предпринимателей и физических лиц,
занимающихся в установленном законодательством
Российской Федерации порядке частной практикой в АО «Банк ЧБРР»

Заявление на установление/отмену лимита сумм платежных поручений

1. На основании настоящего заявления, по счету №_____ Договор об использовании системы дистанционного банковского обслуживания «Клиент-Банк» №_____ от «___» _____202__г., с «___» _____202_г. прошу, начиная с __:__ час. __.__.20__, установить следующий размер сумм платежных поручений:

1.1. Общий лимит на платежные поручения:			
☐	Лимит на разовый платеж	_____(_____)	рублей
☐	Лимит на день	_____(_____)	рублей
☐	Лимит на месяц	_____(_____)	рублей

1.2. Лимит на платежные поручения Мобильного Банка:			
☐	Лимит на разовый платеж	_____(_____)	рублей
☐	Лимит на день	_____(_____)	рублей
☐	Лимит на месяц	_____(_____)	рублей

---

2. На основании настоящего заявления, по счету №_____ Договор об использовании системы дистанционного банковского обслуживания «Клиент-Банк» №_____ от «___» _____202__г., с «___» _____202_г. прошу, начиная с __:__ час. __.__.20__, отменить установленный общий лимит на платежные поручения/лимит на платежные поручения Системы «Клиент-Банк»[7].

РУКОВОДИТЕЛЬ ОРГАНИЗАЦИИ

ДОЛЖНОСТЬ	ПОДПИСЬ	ИНИЦИАЛЫ, ФАМИЛИЯ	ДАТА		

М.П.

[7] *Нужное подчеркнуть.*

Приложение № 17.
к Условиям предоставления и обслуживания
системы дистанционного банковского обслуживания «Клиент-Банк»
для юридических лиц, индивидуальных предпринимателей и физических лиц,
занимающихся в установленном законодательством
Российской Федерации порядке частной практикой в АО «Банк ЧБРР»

Заявление на предоставление доступа к меню «Мониторинг» Системы ДБО ЮЛ

1. На основании настоящего заявления, по счету №_____ Договор об использовании системы дистанционного банковского обслуживания «Клиент-Банк» №_____ от «___» _____202__г., с «___» _____202_г. прошу **предоставить мне доступ к меню «Мониторинг» в Системе ДБО ЮЛ** для самостоятельного подключения услуги SMS-оповещения и (либо) услуги оповещения на электронную почту в информационно-телекоммуникационной сети «Интернет» (E-mail), с целью оповещения о движении денежных средств и операциях, совершенных в Системе ДБО ЮЛ по счету.

2. Настоящим подтверждаю тот факт, что я осведомлен с тем, что канал оповещения на E-mail в информационно-телекоммуникационной сети «Интернет является незащищенным (нешифрованным) каналом связи, и я соглашаюсь нести все риски, связанные с возможным нарушением конфиденциальности и целостности информации (возможным несанкционированным доступом третьих лиц) при ее передаче с использованием информационно-телекоммуникационной сети «Интернет». Принимаю на себя полную ответственность за отключение оповещения или изменения в меню «Мониторинг» номера телефона SMS-оповещения и (либо) адреса электронной почты в информационно-телекоммуникационной сети «Интернет» (E-mail).

3. Я обязуюсь, при первичном предоставлении мне доступа к меню «Мониторинг» в Системе ДБО ЮЛ, а также в дальнейшем, при изменении номера телефона SMS-оповещения и (либо) адреса электронной почты в информационно-телекоммуникационной сети «Интернет» (E-mail), производить установленные Банком процедуры подтверждения Банку номера телефона SMS-оповещения и (либо) адреса электронной почты в информационно-телекоммуникационной сети «Интернет» (E-mail)[8].

РУКОВОДИТЕЛЬ ОРГАНИЗАЦИИ

ДОЛЖНОСТЬ	ПОДПИСЬ	ИНИЦИАЛЫ, ФАМИЛИЯ	ДАТА		

М.П.

[8] *Для подтверждения владения (использования) Клиентом адреса электронной почты в информационно-телекоммуникационной сети «Интернет» (E-mail), на указанный адрес (E-mail) направляется письмо с уникальной ссылкой для подтверждения. Клиенту необходимо перейти по уникальной ссылке подтверждения. Срок действия ссылки подтверждения 24 часа, с момента ее направления.*

Приложение № 18.
к Условиям предоставления и обслуживания
системы дистанционного банковского обслуживания «Клиент-Банк»
для юридических лиц, индивидуальных предпринимателей и физических лиц,
занимающихся в установленном законодательством
Российской Федерации порядке частной практикой в АО «Банк ЧБРР»

Порядок заполнения документа «Заявка на получение наличных денежных средств»

Внешний вид формы документа «**Заявка на получение наличных»** представлен на рис. 1.

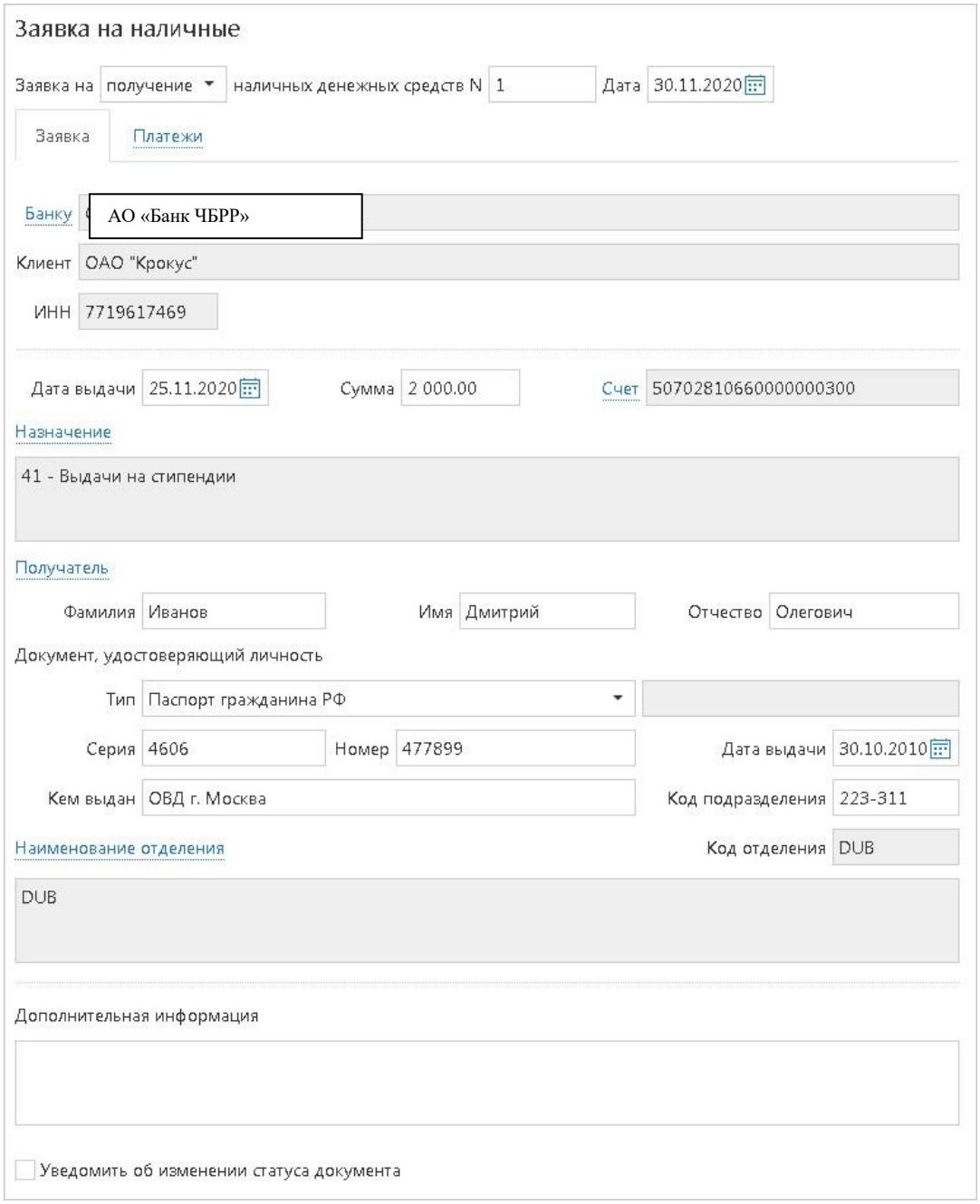

Рис. 1. Заявка на получение наличных. Вкладка "Заявка"

Для заполнения полей вкладки **Заявка на получение наличных (далее - Заявка)** используйте приведенные ниже рекомендации:

1. В поле **Сумма** укажите сумму денежных средств, которую вы хотите получить в виде наличных денег.
2. В поле **Дата выдачи** укажите дату получения денежных средств.
3. В поле **Счет** выбрать счет с которого будут выдаваться денежные средства.

4. Поля формы **Получатель** заполняются данными получателя (ФИО, данные документа, удостоверяющего личность). В данном поле, указываются только данные получателей физических лиц, имеющих право распоряжения расчетным счетом либо имеющих действующую доверенность в Банке. Если у Клиента заключен Договор о порядке выпуска и обслуживания банковских карт работников Предприятия (Организации) или учащихся/студентов/аспирантов/работников Учебного заведения (для взаимодействия посредством системы Клиент - Банк), то возможно выбрать получателя - физическое лицо из справочника.
5. Выбрать из справочника **Наименование отделения,** в котором обслуживается Клиент. Код отделения и его название отобразятся в соответствующих полях формы. Получение денежных средств в других ДО, осуществляется только по предварительному согласованию в Банком.
6. Нажмите ссылку **Назначение** и в отобразившемся диалоге (см. рис. 2) выберите цель получения денежных средств.

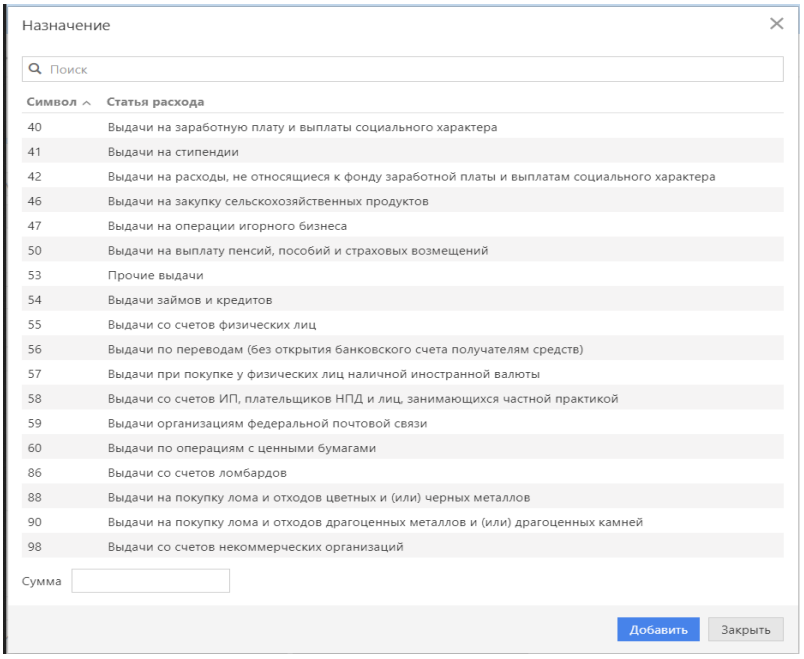

Рис. 2. Диалог "Назначение"

Возможно указать несколько **Статей расхода**, в диалоге **Назначение** укажите сумму для каждой выбранной статьи (см. рис. 3)

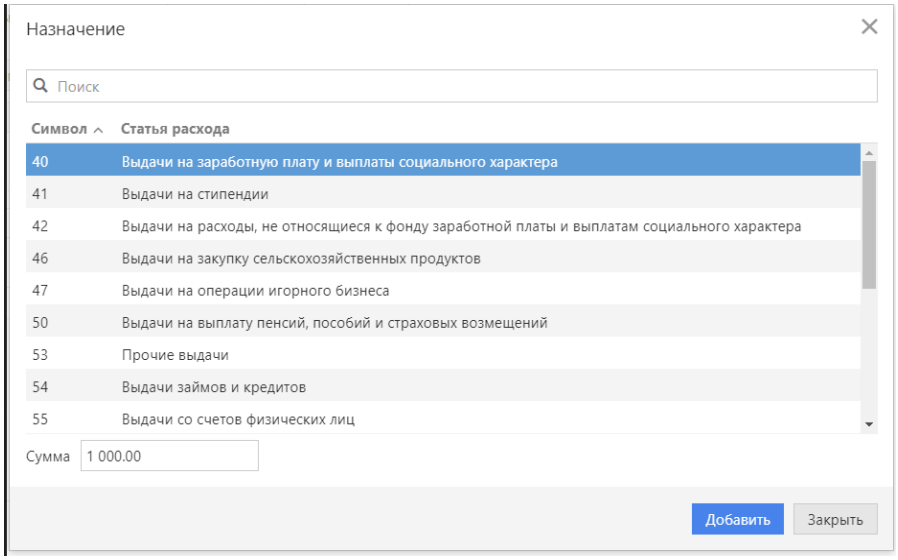

Рис. 3. Диалог "Назначение". Указание сумм для отдельных статей расхода

В поле **Сумма** отображается общая сумма по всем указанным статьям расхода (см. рис. 4).

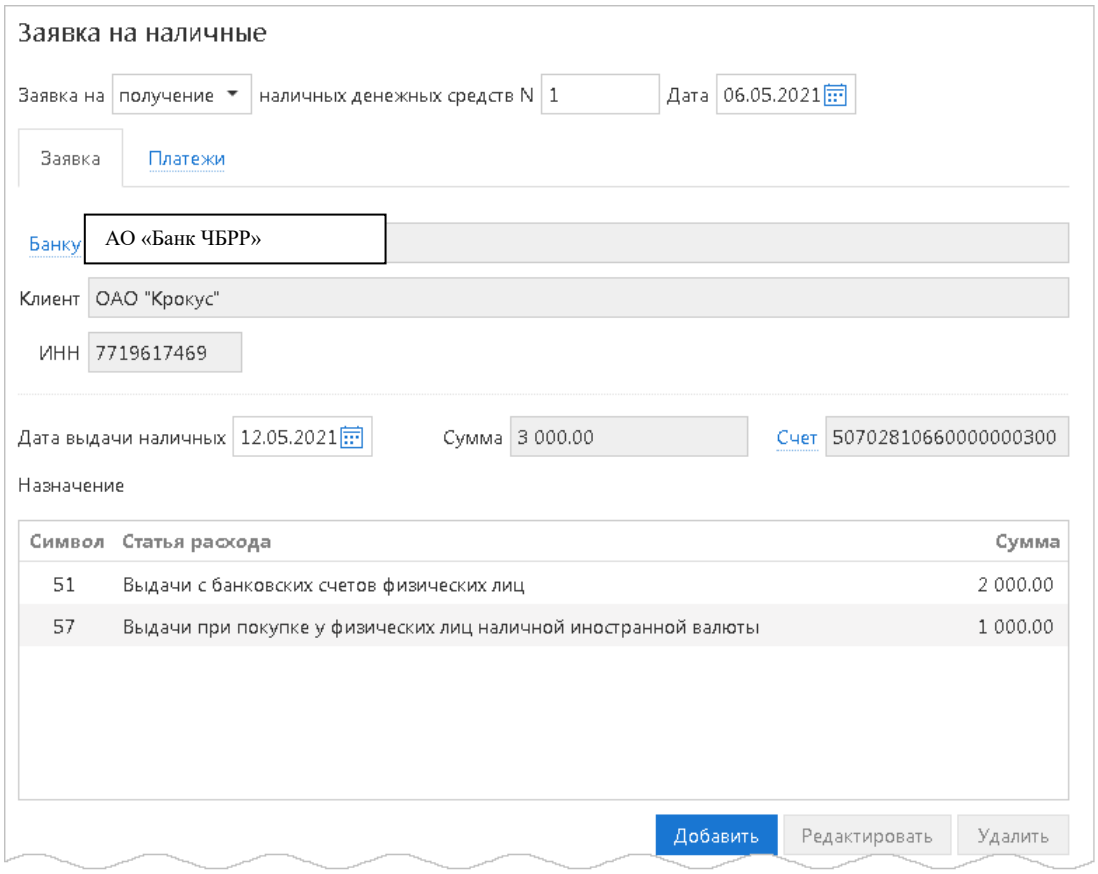

Рис. 4. Заявка на получение наличных. Вкладка "Заявка". Несколько статей расхода

7. В поле **Дополнительная информация** указывается полное назначение платежа, расшифровка сути операции, для ее однозначного понимания, исключающего двусмысленность.

Например: Заработная плата за 00.0000; Выдача по договору займа № ___ от _____; Доход ИП; ГСМ, стройматериалы; Дивиденды, согл. Протокола/Решения № __ от_____ и др.

Оформленную Заявку необходимо подписать (электронными подписями лиц, уполномоченных распоряжаться денежными средствами, находящимися на счете), и направить в Банк в стандартном порядке.
Изменение данных подписанной ЭЦП Заявки не предусмотрено. При возникновении необходимости изменить сумму выдачи или назначение выдачи, или других данных, клиент должен сначала отозвать неправильную Заявку (для этого в СДБО ЮЛ необходимо написать письмо в Банк об аннулировании Заявки), а затем создать новую с правильными данными.
В день, указанный в Заявке, получатель обращается в Банка и получает денежные средства. При этом дополнительно представлять в Банк денежный чек не требуется. Выдача денежных средств на основании Заявки оформляется расходным кассовым ордером, который составляет работник Банка.
В случае неполучения денежной наличности в установленный день - Заявка аннулируется.