Приложение 3 к Комплексному договору,
утвержденному Приказом от 20.10.2025 №938

УСЛОВИЯ ДИСТАНЦИОННОГО БАНКОВСКОГО ОБСЛУЖИВАНИЯ

(действуют с 27.10.2025)

ОГЛАВЛЕНИЕ

1. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Если иное не предусмотрено настоящими Условиями дистанционного банковского обслуживания (далее – Условия ДБО), используемые термины, определения и сокращения применяются в значении, определенном терминами, определениями и сокращениями Комплексного договора (Словарь терминов и сокращений). Термины и определения, значение которых не определено в Комплексном договоре, используются в значениях, установленных Законодательством.

Авторизация в ДБО – подтверждение полномочий (предоставление прав доступа) Клиента/УЛК, успешно прошедшего Аутентификацию входа, на получение услуг Банка, предусмотренных настоящими Условиями ДБО.

Авторство ЭД – принадлежность ЭП Клиенту/УЛК.

Защита информации от несанкционированного доступа – комплекс мероприятий, проводимых с целью предотвращения утечки, хищения, утраты, несанкционированного уничтожения, искажения, модификации (подделки), несанкционированного копирования информации, ее блокирования и т.п.

Ключ проверки электронной подписи (Ключ проверки ЭП) – ключ, автоматически формируемый программными средствами Системы ДБО при изготовлении ключа электронной подписи и однозначно зависящий (производный) от него. Ключ проверки предназначен для проверки ЭП ЭД, сформированной данным участником Системы ДБО при подписании ЭД. Ключ проверки считается принадлежащим абоненту, если он был зарегистрирован в установленном порядке.

Ключ электронной подписи (Ключ ЭП) – ключ, изготавливаемый УЛК - пользователем Системы ДБО и предназначенный для формирования им ЭП ЭД. Ключ ЭП хранится в цифровом виде, на специализированном носителе информации, именуемом в дальнейшем «ключевой элемент» или «носитель электронного ключа».

Ключевой элемент (Носитель электронного ключа) – специализированное программно-аппаратное устройство (USB-токен), подключаемое к компьютерному устройству Клиента через интерфейс USB, с интегрированной операционной системой со встроенным средством криптографической защиты информации (СКЗИ), сертифицированным в соответствии с Законодательством и разрешенным к применению для реализации функций формирования и проверки электронной подписи и шифрования информации.

Компрометация ключа – утрата доверия к тому, что используемые ключи обеспечивают безопасность информации.

К событиям, связанным с компрометацией ключей относятся, включая, но не ограничиваясь, следующие:

– утрата ключевых элементов;
– утрата ключевых элементов с последующим обнаружением;
– увольнение сотрудников, имевших доступ к ключевой информации;
– нарушение правил хранения и уничтожения (после окончания срока действия) ключа ЭП;
– несанкционированное копирование или подозрение на копирование информации с Носителя электронного ключа;
– возникновение подозрений на утечку информации или ее искажение в системе конфиденциальной связи;
– случаи, когда нельзя достоверно установить, что произошло с носителями электронных ключей, содержащими ключевую информацию (в том числе случаи, когда носитель вышел из строя и достоверно не опровергнута возможность того, что данный факт произошел в результате несанкционированных действий злоумышленника);

– несанкционированный доступ злоумышленников к рабочему месту Клиента, мобильному устройству УЛК в части использования Простой ЭП;
– утрата Мобильного устройства;
– утрата Пароля и (или) утрата контроля над сим-картой.

Облачная электронная подпись (облачная ЭП) – вычислительная система, предоставляющая через сеть доступ к возможностям создания, проверки ЭП и интеграции этих функций в бизнес-процессы других систем.

Подлинность ЭД – означает, что данный документ (экземпляр документа) создан в Системе ДБО без отступлений от принятой технологии. ЭД считается подлинным, если он был, с одной стороны, должным образом оформлен и подписан ЭП Клиента/УЛК и передан на обработку, а с другой – был принят к исполнению. Свидетельством того, что ЭД (кроме кредитных договоров) принят к исполнению, является уведомление «принят к исполнению» в строке статуса в соответствующем модуле, загруженном с Сайта.

Проверка ЭП ЭД – проверка соотношения, связывающего ЭП под этим ЭД и ключ проверки подписавшего абонента. Если рассматриваемое соотношение оказывается выполненным, то ЭП признается правильной, а сам ЭД – подлинным, в противном случае ЭД считается измененным, а ЭП под ним недействительной.

Сертификат ключа проверки подписи – электронный документ или документ на бумажном носителе, подтверждающий принадлежность ключа проверки участнику Системы ДБО, заверенный ЭП либо собственноручными подписями владельца соответствующего ключа электронной подписи, уполномоченного лица и печатью организации пользователя Системы ДБО.

Уполномоченные службы Банка – подразделения Банка, осуществляющие обслуживание Системы ДБО.

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

Электронная подпись (ЭП) – информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию. Средства ЭП обеспечивают формирование подписи ЭД, а также Пакета ЭД в соответствии с Законодательством при передаче на обработку, а также проверку наличия, аутентификации и не искаженности подписи при обработке ЭД, увязывая в одно целое содержание ЭД и Ключ ЭП Клиента/УЛК, и обеспечивают Целостность ЭД.

В целях применения настоящих Условий ДБО под Электронной подписью понимается Усиленная неквалифицированная ЭП, Облачная ЭП или Простая ЭП, в зависимости от вида подписи, фактически используемой Клиентом/УЛК.

Электронное средство платежа (ЭСП) – средство и (или) способ, позволяющие Клиенту Банка составлять, удостоверять и передавать распоряжения в целях осуществления перевода денежных средств в рамках применяемых форм безналичных расчетов с использованием Системы ДБО, электронных носителей информации, в том числе Карт и их преобразованных данных (токенизированных (цифровых) платежных карт), а также иных технических устройств.

Электронный служебно-информационный документ (ЭСИД) – ЭД, подписываемый ЭП Клиента/УЛК, не являющийся ЭПД (выписки по счету, запросы, отчеты, информационные сообщения, Документы валютного контроля).

ЭСИД также являются любые документы, приводящие к заключению договоров, в том числе в виде оферты, заключаемых путем обмена ЭД в соответствии с разделами Комплексного договора, а также документы (заявления, подтверждения, уведомления и т. п.), оформляемые на условиях и в рамках таких договоров, предусматривающих порядок обмена Сторонами с использованием Системы ДБО.

2. ОБЩИЕ ПОЛОЖЕНИЯ

2.1. Настоящие Условия ДБО регламентируют взаимодействие Сторон при предоставлении Банком услуг Клиенту с использованием Системы ДБО.

2.2. Настоящие Условия ДБО в совокупности с надлежащим образом заполненным и подписанным Клиентом Заявлением о присоединении/Заявлением на подключение к системе «Интернет Банк-Клиент» Клиента являются Договором ДБО, заключенным между Банком и Клиентом.

2.3. Условия ДБО, в том числе приложения к Условиям ДБО, являются неотъемлемой частью Комплексного договора.

2.4. Обслуживание Клиента в Системе ДБО в рамках настоящих Условий ДБО осуществляется Банком с даты подключения Клиента к Системе ДБО на основании Заявления на подключение к системе «Интернет Банк-Клиент», представленного Клиентом/УЛК в Банк.

2.5. Банк и Клиент договариваются об обмене распоряжениями, документами и информацией в электронной форме, подписанными ЭП, в соответствии с Регламентом обслуживания и применения системы дистанционного банковского обслуживания «Интернет Банк-Клиент» (далее – Регламент) (Приложение 2 к Условиям ДБО) и Порядком обмена между Банком и Клиентом в электронном виде документами и информацией, связанными с проведением валютных операций (далее – Порядок) (Приложение 6 к Условиям ДБО).

2.6. Стороны признают, что используемые во взаимоотношениях Сторон распоряжения, документы и информация, заверенные ЭП, подготовленные и переданные одной Стороной другой Стороне с посредством Системы ДБО, равнозначны документам на бумажном носителе и имеют юридическую силу наравне с документами, подписанными уполномоченными представителями Сторон и скрепленными печатью.

2.7. Стороны доверяют используемому программному обеспечению Системы ДБО.

2.8. Настоящие Условия ДБО регулируют отношения Сторон по обмену распоряжениями, документами и информацией, заверенными ЭП, подготовленными и переданными одной Стороной другой Стороне с помощью программного обеспечения Системы ДБО, в отношении счетов (далее счет или счета) и операций по счетам, открытым на основании Комплексного договора, а также счетов и операций по счетам, указанным в поданном Клиентом в Банк Заявлении на подключение к Системе ДБО.

2.9. Настоящие Условия ДБО устанавливают:

– порядок использования ЭП, которая посредством использования кодов, паролей или иных средств подтверждает факт формирования ЭП Клиентом/УЛК, а также определяет возникающие в связи с этим права, обязанности и ответственность Сторон;

– порядок использования Облачной ЭП, которая посредством использования Ключа проверки ЭП или иных средств подтверждает факт формирования ЭП Клиентом/УЛК, а также определяет возникающие в связи с этим права, обязанности и ответственность Сторон.

2.10. В сферу действия Условий ДБО также входят регламентированные в Порядке (Приложение № 6 к Условиям ДБО) отношения Сторон по обмену документами и информацией, предусмотренными Законодательством о валютном регулировании и валютном контроле.

2.11. В рамках настоящих Условий ДБО Банк предоставляет Клиенту следующие услуги с использованием функционала Системы ДБО:

– проведение операций по Счетам Клиента и их обслуживание (в том числе в рамках Законодательства о валютном регулировании и валютном контроле);
– передача между Сторонами ЭД, ЭСИД, в том числе в порядке, указанном в разделах Комплексного договора и в Договорах кредитно-обеспечительного характера;

2.12. Настоящие Условия ДБО и приложения к ним, перечисленные в п. 2.10, являются неотъемлемой частью Комплексного договора и распространяются на все счета Клиента, подключенные к Системе ДБО.

2.13. В составе Условий ДБО действуют следующие Приложения:

– Приложение №1 – Заявление на подключение к Системе ДБО.
– Приложение №2 - Регламент обслуживания с применением Системы «Интернет Банк-Клиент» ЦМРБанк (ООО).
– Приложение №3 - Перечень электронных документов, пересылаемых по Системе «Интернет Банк-Клиент», в соответствии с предоставляемыми Клиенту услугами.
– Приложение №4 - Сертификат ключа проверки подписи в Системе «Интернет Банк-Клиент» ЦМРБанк (ООО).
– Приложение №5 - Положение по разбору конфликтных ситуаций, связанных с подлинностью электронных документов.
– Приложение №6 – Порядок обмена между Банком и Клиентом в электронном виде документами и информацией, связанными с проведением валютных операций.
– Приложение №7 – Мобильное приложение «ЦМР Бизнес»
– Приложение №8 – Рекомендации по обеспечению информационной безопасности при использовании Мобильного приложения.
– Приложение №9 – Политика конфиденциальности при использовании Мобильного приложения.
– Приложение №10 – Заявление на подключение/отключение к Мобильному приложению «ЦМР Бизнес»

3. ПРАВА И ОБЯЗАННОСТИ СТОРОН

3.1. Банк обязуется:

3.1.1. Принимать к проверке и исполнению полученные по Системе ДБО электронные документы (ЭД), оформленные и заверенные в соответствии с Регламентом.

3.1.2. Предоставлять Клиенту документы и информацию в соответствии с Приложением №3 к настоящему Договору.

3.1.3. Консультировать персонал Клиента по вопросам обслуживания в Системе ДБО.

3.1.4. Обеспечивать защиту от несанкционированного доступа и сохранять конфиденциальность информации по счетам Клиента.

3.1.5. Сообщать Клиенту об обнаружении попытки несанкционированного доступа к Системе ДБО, если это затрагивало операции Клиента, в течение суток с момента обнаружения факта.

3.1.6. Предоставлять Клиенту возможность использования дополнительных услуг в рамках Системы ДБО.

3.1.7. Предоставлять Клиенту доступ к Системе ДБО только при использовании Клиентом средств и способов защиты передаваемой информации, указанных в Заявлении/Заявлениях.

3.1.8. Информировать клиента о совершении каждой операции с использованием ЭД. Информирование Клиента в Системе ДБО осуществляется путем изменения статуса обработки ЭД в Системе ДБО, а также отражением исполненного ЭД в выписке по счету (счетам).

3.1.9. Предоставлять по запросам другой Стороны подтверждения по ЭД, а также надлежащим образом оформленные бумажные копии ЭД.

3.2. Банк имеет право:

3.2.1. В одностороннем порядке изменять Тарифы Банка на обслуживание в Системе ДБО с предварительным уведомлением Клиента за 3 (три) календарных дня путем размещения информации на стендах в офисах Банка и/или на Сайте, и/или информационным сообщением по Системе ДБО.
3.2.2. Списывать без дополнительного распоряжения Клиента (на условиях заранее данного акцепта) со счетов Клиента сумму комиссионного вознаграждения за осуществление расчетов с применением Системы ДБО в соответствии с Тарифами Банка.
3.2.3. Без дополнительного распоряжения Клиента (на условиях заранее данного акцепта) списывать со Счетов Клиента, открытых в Банке и подключенных к Системе ДБО, денежные средства на оплату комиссии Банка в соответствии с действующими Тарифами в день совершения операции или иной срок, установленный Тарифами Банка.
3.2.4. В случае недостаточности денежных средств на Счетах Клиента, открытых в Банке и подключенных к Системе ДБО, для оплаты комиссионного вознаграждения за обслуживание с применением Системы ДБО в соответствии с Тарифами Банка, по истечении 7 (семи) календарных дней с момента возникновения задолженности Клиента прекратить предоставление соответствующей услуги Клиенту.
3.2.5. Не принимать к исполнению от Клиента ЭД, оформленные с нарушением Регламента, с уведомлением Клиента не позднее рабочего дня, следующего за днем получения ЭД, путем указания причин отказа в приеме на обработку ЭД в строке статуса в соответствующем модуле АБС, загруженном с Сайта.
3.2.6. Отказывать в приеме и оформлении документов, связанных с проведением валютных операций, по основаниям и в сроки, предусмотренные нормативными актами Банка России, с указанием причин отказа.
3.2.7. Не осуществлять операции по счету Клиента в случае недостатка средств на Счете, с уведомлением Клиента не позднее рабочего дня, следующего за днем получения распоряжения.
3.2.8. В случае необходимости затребовать от Клиента предоставления распоряжения на бумажных носителях, оформленных в соответствии с требованиями Банка России, и не производить платеж до предоставления данного документа, о чем Банк обязан сообщить Клиенту предварительно, но не позднее дня, следующего за днем получения распоряжения в электронной форме.
3.2.9. Отказать Клиенту в приёме от него ЭД, о чем Банк обязан сообщить Клиенту предварительно, но не позднее рабочего дня, следующего за днем получения документа в электронной форме с указанием причины отказа. В этом случае документы Клиента могут приниматься Банком оформленными надлежащим образом на бумажном носителе.
3.2.10. В случае наличия подозрений в совершении неправомерных действий в отношении Клиента приостановить расходные операции[1] по Счету Клиента в течение периода проведения проверки в порядке и сроки, установленные Законодательством.
3.3. Клиент обязуется:
3.3.1. Соблюдать требования Регламента и Порядка.
3.3.2. Соблюдать конфиденциальность информации, касающейся Системы ДБО. В случае обнаружения несанкционированного доступа к Системе ДБО в течение дня с момента обнаружения сообщить об этом Банку.
3.3.3. Обеспечить безопасность и целостность среды исполнения на своем компьютере и Мобильном устройстве (отсутствие вредоносного программного обеспечения и программ-закладок).
3.3.4. Соблюдать конфиденциальность информации, касающейся ключей и паролей, используемых в Системе ДБО.
3.3.5. Контролировать соответствие суммы платежа и остатка на начало операционного дня на Счетах, открытых в Банке, получать уведомления Банка о совершенных операциях с

[1] Ограничение распространяется на совершения расходных операций по Распоряжениям Клиента. Все иные операции по счету проходят в установленном порядке.

использованием ЭД и осуществлять платежи только в пределах остатка за исключением случаев предоставления Банком овердрафта по счету Клиента, условия которого оговариваются отдельным договором.
3.3.6. В случае компрометации ключа ЭП незамедлительно обращаться в Банк для принятия необходимых мер (в том числе блокирования работы Клиента в Системе ДБО).
3.3.7. По требованию Банка в соответствии с п. 2.3.4 Условий РКО предоставить Банку платежные и иные документы, оформленные на бумажном носителе в соответствии с требованиями Банка России.
3.3.8. Самостоятельно отслеживать уведомления Банка о процессе прохождения ЭД.
3.3.9. Оплачивать услуги Банка по осуществлению расчетов с применением Системы ДБО в соответствии с Тарифами Банка.

3.4. Клиент имеет право:
3.4.1. Получать из Банка справочную информацию в соответствии с Приложением №3 к Условиям ДБО.
3.4.2. Отзывать распоряжения, переданные в Банк, посредством передачи сообщения по Системе ДБО в форме запроса свободного формата в соответствии с Приложением №3 к Условиям ДБО, содержащего реквизиты отзываемого распоряжения и причины отзыва, подписанного ЭП уполномоченных лиц, указанных в КОП.
3.4.3. Отзыв распоряжений может быть осуществлён только до наступления безотзывности перевода денежных средств.
3.4.4. Направлять в Банк распоряжения, документы и информацию по Системе ДБО в соответствии с Условиями ДБО.
3.4.5. Установить в отношении операций, осуществляемых с использованием Системы ДБО, ограничения на осуществление операций либо ограничения максимальной суммы одной операции и (или) операций за определенный период времени путем подачи соответствующего заявления по форме Банка.

4. УРЕГУЛИРОВАНИЕ СПОРОВ И ОТВЕТСТВЕННОСТЬ СТОРОН

4.1. Все разногласия, споры и конфликтные ситуации, (далее – Споры) возникающие между Сторонами вследствие исполнения Условий ДБО, разрешаются с учетом взаимных интересов путем переговоров в порядке, установленным настоящими Условиями ДБО и Приложениями к ним.
4.2. В случае возникновения Споров между Клиентом и Банком по предмету настоящих Условий ДБО совместным решением обеих Сторон создается согласительная экспертная комиссия из равного количества представителей от каждой Стороны.
4.3. При рассмотрении Споров, связанных с подлинностью электронных документов, комиссия в своей работе руководствуется Положением по разбору конфликтных ситуаций, связанных с подлинностью электронных документов (Приложение №5 к Условиям ДБО). В ходе рассмотрения комиссией Спора о подлинности (наличии или отсутствии) документа, исполненного с помощью Системы ДБО или подписанного электронной подписью, каждая Сторона обязана доказать лишь то, что она своевременно и надлежаще выполнила обязанности, взятые на себя в соответствии с Условиями ДБО. Своевременным и надлежащим выполнением Стороной обязанностей признается соблюдение порядка и условий выполнения действий при обмене документами в электронном виде, закрепленных в Условиях ДБО и Приложениях к ним. При решении вопросов по всем остальным конфликтам Стороны руководствуются действующим Законодательством.
4.4. Свои решения комиссия оформляет в виде актов. Стороны признают решения комиссии, оформленные в соответствии с процедурами, установленными в Приложении №5 к Условиям ДБО обязательными для участников Споров, по которым они вынесены, и обязуются добровольно исполнять решения комиссии по указанным вопросам в установленные в них сроки.

4.5. Сторона, признанная виновной, возмещает убытки другой Стороне в соответствии с действующим Законодательством.
4.6. Уклонение какой-либо Стороны от участия в создании или работе согласительной экспертной комиссии может привести к невозможности ее создания и работы, но не может привести к невозможности урегулирования Спора в судебном порядке. В случае недостижения соглашения Сторон, отсутствия согласия по Спорам и добровольного исполнения решения комиссии, Споры по настоящему Договору рассматриваются в соответствии с действующим Законодательством.
4.7. Стороны несут ответственность за достоверность информации, предоставляемой друг другу.
4.8. За неисполнение или ненадлежащее исполнение обязательств, определенных в Условиях ДБО, Стороны несут ответственность в соответствии с действующим Законодательством.
4.9. Банк не несет ответственности за неисполнение или ненадлежащее исполнение распоряжений Клиента, подписанных ЭП Клиента/УЛК и направленных в Банк по Системе ДБО, произошедшее из-за нарушения Клиентом Условий ДБО, в том числе Приложений к ним.
4.10. Банк не несет ответственности за невыполнение или несвоевременное выполнение настоящих Условий ДБО в случае технических сбоев (отключения/повреждения электропитания и сетей связи, сбоев программного обеспечения, технических сбоев в работе Платежных систем), некорректного/неполного указания Клиентом/УЛК реквизитов при перечислении средств, возникновения обстоятельств непреодолимой силы (форс-мажор).
4.11. Банк не несет ответственности за ущерб, причиненный Клиенту в результате нарушения или ненадлежащего исполнения Клиентом/УЛК требований по защите от вредоносного кода рабочего места Системы ДБО.
4.12. Банк не несет ответственности за прием в обработку ЭД Клиента в случае наличия в Системе ДБО отдельных признаков возможной вредоносной активности на рабочем месте Клиента при одновременном подписании ЭД действующей ЭП Клиента/УЛК и отсутствии заявления Клиента/УЛК о Компрометации ключа ЭП.
4.13. Банк возмещает Клиенту убытки, произошедшие из-за нарушения системы защиты информации по вине Банка, в соответствии с действующим Законодательством.
4.14. Банк не несет ответственности за отказ в приеме и оформлении документов, связанных с проведением валютных операций, произошедший из-за несоблюдения Клиентом Порядка.

5. ОСОБЫЕ УСЛОВИЯ

5.1. Инициатором сеансов связи с Банком всегда является Клиент. В случае несвоевременного выполнения Банком своих обязательств из-за отсутствия инициативы Клиента в установлении сеанса связи с Банком, не влечет за собой ответственности Банка.
5.2. Клиент при подписании ЭД ЭП применяет свои Ключи ЭП, а Банк при проверке ЭП ЭД - Ключи проверки электронной подписи Клиента, являющиеся действующими на момент подписания и передачи документа на обработку соответственно.
5.3. Проверка поступающих от Банка ЭД осуществляется Клиентом в порядке аналогичном указанному в пункте 5.2 Условий ДБО.
5.4. Ключи ЭП и соответствующий ему Ключ проверки электронной подписи подписывающей Стороны становятся действующими только после завершения процедур регистрации Ключей проверки электронной подписи и ввода в действие Ключей ЭП. Ключи являются действующими на момент подписания, если они зарегистрированы, не отозваны подписывающей Стороной и срок действия их не окончен.
5.5. При регистрации нового Ключа проверки ЭП, регистрируемый Ключ проверки ЭП фиксируется и заверяется на бумажном носителе следующим образом: распечатывается на

бумаге в виде Сертификата ключа проверки подписи с контрольной записью с указанием даты его регистрации и Стороны, которой принадлежит этот ключ проверки, и заверяется подписями уполномоченных лиц и печатью Клиента. Порядок смены Ключа проверки ЭП и регистрируемого Ключа проверки ЭП без визита в Банк указан в Регламенте.

5.6. Смена Ключей ЭП может быть произведена в любой момент по желанию Стороны, которой принадлежат Ключи. Клиент обязан произвести смену принадлежащих ему ключей по требованию Банка.

5.7. Все процедуры генерации, обмена, регистрации, перерегистрации, ввода в действие и завершение действия Ключей ЭП производятся в соответствии с порядком, предусмотренным в Регламенте.

5.8. Обязательства Сторон по электронным документам, вытекающие из Договора ДБО, возникают после даты подписания Сертификата ключа проверки подписи в Системе ДБО и регистрации Клиента в Системе ДБО, а при смене Сертификата ключа проверки подписи без визита в Банк - в порядке, указанном Регламенте.

5.9. Стороны признают и руководствуются всеми терминами, понятиями, определениями и сокращениями, изложенными в Комплексном договоре, приложениях к нему и Условиях ДБО.

5.10. Сведения, содержащиеся в документах, переданных Сторонами друг другу по Системе ДБО, персональные электронные адреса, идентификационные параметры, регистрационные номера, пароли и ключи обеих Сторон, используемые для разграничения доступа, передачи и защиты передаваемой информации, а также материалы работы согласительной экспертной комиссии по разбору Споров являются конфиденциальными сведениями. Конфиденциальные сведения не подлежат разглашению третьим лицам ни при каких обстоятельствах, кроме установленного Законодательством порядка.

7. СРОК ДЕЙСТВИЯ И ПОРЯДОК РАСТОРЖЕНИЯ 7.1. Настоящие Условия ДБО прекращают свое действие при расторжении Комплексного договора (по любым основаниям) либо при предоставлении в Клиентом в Банк заявления на отключение от Системы ДБО.

7.2. В случае прекращения действия настоящих Условий ДБО Клиент обязуется уничтожить все принадлежащие ему Ключи ЭП и не передавать их третьим лицам.

Приложение 3 к Комплексному договору,
утвержденному Приказом от 20.10.2025 №938

Приложение 1
к Условиям дистанционного банковского обслуживания

ЗАЯВЛЕНИЕ НА ПОДКЛЮЧЕНИЕ К СИСТЕМЕ «ИНТЕРНЕТ БАНК-КЛИЕНТ»

(заполняется клиентом)	
1. Наименование организации	
2. Руководитель	Должность: _____ Ф.И.О. _____
3. Вид собственности организации	☐ Государственная ☐ Муниципальная ☐ Паевая или акционерная ☐ Частная ☐ Иная _____
4. Периодичность исходящих платежей (предположительно)	☐ Нерегулярно ☐ Еженедельно по дням: _____ ☐ Ежедневно ☐ Ежемесячно по дням: _____ ☐ Другая периодичность: _____
5. Максимальное количество расчетных документов в день (предположительно)	☐ Менее 10 ☐ 10-99 ☐ 100-999 ☐ Более (сколько) _____
6. Контактные лица по бухгалтерским вопросам	1. Ф.И.О. _____тел. _____ 2. Ф.И.О. _____тел. _____
7. Каким способом Вы хотели бы получать уведомления из БАНК?	☐ По телефону: _____ ☐ По электронной почте: _____ ☐ Другим способом: _____ Другая система_____
8. Укажите адрес электронной почты	(e-mail) _____
9. Сколько сотрудников будут пользоваться системой “Интернет Банк-Клиент”?	☐ Один ☐ Больше: укажите, сколько _____

10. IP фильтрация (необходимо выбрать первый или второй пункт)	
1. Просим не ограничивать доступ в систему Интернет Банк-Клиент определенными IP адресами [возможно только в том случае, когда у клиента все действующие ключи ЭЦП сгенерированы на USB-токене(ах)]	☐
2. Просим ограничить доступ в систему Интернет Банк-Клиент только следующими IP адресами	☐
№/№	IP адрес
11. Просим выдать USB-токен (-ы) в количестве:	_____ штук

Уполномочиваю ЦМРБанк (ООО) осуществить списание денежных средств в оплату за оказание услуги криптографической защиты путем безакцептного списания денежных средств в размере _____ руб., согласно тарифам со счета №_____.

12. Блокировочное слово:	

Информация об обслуживании клиента (заполняется сотрудниками отделения/филиала)	
1. Отделение БАНКа	
2. Руководитель БАНКа	Ф.И.О. _____ тел. _____
3. Специалист	Ф.И.О. _____ тел. _____
4. Код клиента в операционном дне	

	Счета клиента	Права доступа к указанным счетам	
		полное распоряжение счетом	просмотр и получение выписок по счету

5. Счета клиента и права доступа к ним	☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐ ☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐ ☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐ ☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐ ☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐ ☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐ ☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐	☐ ☐ ☐ ☐ ☐ ☐ ☐	☐ ☐ ☐ ☐ ☐ ☐ ☐
6. Срок подключения к системе “Интернет Банк-Клиент”	“_____” _____ 200___ г.		
7. Настоящее заявление является неотъемлемой частью Договора № ____ на обслуживание клиентов в системе «Интернет Банк-Клиент» от «___»_____20___г., заключенного в рамках Комплексного договора № от «___»_____20___г.			

Дата заполнения: “_____” _____200 ___ г.

Руководитель Банка “_____”_____/_____/
Клиент “_____”_____/_____/

Приложение 2

к Условиям дистанционного банковского обслуживания

РЕГЛАМЕНТ ОБСЛУЖИВАНИЯ И ПРИМЕНЕНИЯ СИСТЕМЫ ДИСТАНЦИОННОГО БАНКОВСКОГО ОБСЛУЖИВАНИЯ «ИНТЕРНЕТ БАНК-КЛИЕНТ»

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Система дистанционного банковского обслуживания «Интернет Банк-Клиент» предназначена для подготовки, учета и предварительной обработки распоряжений Клиентов, а также других ЭД Клиентов Банка. Система ДБО построена на основе технологии всемирной сети интернет, обеспечивает конфиденциальность, надежность и достоверность информации, установление подлинности отправителя, проверку целостности и авторства документа. Также реализована возможность доказательного разрешения споров на основе применения системы защиты, состоящей из специальных программных и технических средств, организационных мер и договорно-правовых норм.

1.2. Электронные документы, применяемые в Системе ДБО, юридически эквивалентны документам, предоставляемым на бумажном носителе, используемым в соответствии с нормативными актами Банка России и Комплексным договором и являются основанием для осуществления операций по счету (счетам) Клиента.

1.3. Стороны признают, что используемая в соответствии с Комплексным договором система телекоммуникации, обработки и хранения информации является достаточной для обеспечения надежной и эффективной работы при приеме, передаче, обработке и хранении информации, а система защиты информации, обеспечивающая разграничение доступа, шифрование, контроль целостности и электронную подпись, является достаточной для защиты от несанкционированного доступа, подтверждения авторства и подлинности информации, содержащейся в получаемых электронных документах, и для разрешения спорных ситуаций.

1.4. Электронный документ (ЭД) порождает обязательства Сторон по Комплексному договору, если он должным образом оформлен инициирующей Стороной, заверен ЭП и передан на обработку, а принимающей Стороной принят к исполнению. Свидетельством того, что ЭД принят к исполнению, является уведомление «принят к исполнению» в строке статуса в соответствующем модуле, загруженном с Сайта.

1.5. Готовность Сторон к работе по Системе ДБО оформляется подписанием Сертификата ключа проверки подписи в Системе «Интернет Банк-Клиент» (Приложение №4 Условиям ДБО) и регистрации Клиента в Системе ДБО.

1.6. В рамках настоящего Регламента Банк осуществляет следующие функции:

1.6.1. Прием от Клиента по электронным каналам связи должным образом оформленных ЭД с контролем их целостности и авторства.

1.6.2. Прием ЭД только с верной ЭП УЛК, регистрационный идентификационный номер и ключ проверки которых соответствует данным, указанным в Сертификате ключа проверки подписи в Системе «Интернет Банк-Клиент» (Приложение №4 к Условиям ДБО).

1.6.3. Обработку и исполнение полученных ЭД Клиента в строгом соответствии с установленными нормами, техническими требованиями, стандартами, инструкциями Банка России и Банка.

1.6.4. Предоставляет Клиенту информацию о результатах проверки и обработки (или отказе в приеме на обработку с указанием причин) принятого ЭД Клиента.

1.6.5. По результатам обработки и исполнения ЭД Клиента, а также по мере совершения иных операций по счету, в течение следующего дня после совершения операции, подготавливает и предоставляет Клиенту, в ответ на его запрос, выписки по счету с

указанием основных реквизитов платежного документа, на основании которого совершена операция по счету.

1.6.6. Своевременно информирует Клиента об изменениях порядка осуществления обработки ЭД и другой информации по Системе ДБО.

1.6.7. Оказывает консультационные услуги Клиенту по вопросам, необходимым для правильной эксплуатации Системы ДБО Клиентом, как-то: функционирование Системы ДБО, использования средств защиты и технологии обработки информации.

1.6.8. Осуществляет необходимую модернизацию программного обеспечения Системы ДБО и информирует Клиента о предстоящей модернизации за 10 (Десять) календарных дней, размещая информацию на Сайте/в Системе ДБО.

1.6.9. Сообщает Клиенту о непредвиденных сбоях в работе Системы ДБО для принятия им мер по своевременной доставке распоряжения на бумажном носителе в Банк. Доставка распоряжения, документов на бумажном носителе осуществляется Клиентом в течении действующего операционного дня Банка.

1.7. В соответствии с настоящим Регламентом Клиент обязуется

1.7.1. Осуществлять ввод документов (и осуществлять контроль введенной информации) в электронном виде, соблюдая порядок подготовки документов, обеспечивая заполнение форм в соответствии с требованиями Банка.

1.7.2. Осуществлять в течение любого рабочего дня не менее одного сеанса связи с Банком для получения возможных экстренных (технических) сообщений от Банка, либо другой актуальной информации.

1.7.3. Выполнять требования по оформлению и защите, передаваемой в виде ЭД информации, защите ключей ЭП, паролей доступа и другой информации, передаваемой и получаемой по Системе ДБО.

1.7.4. Соблюдать порядок осуществления приема и передачи ЭД и обеспечивать передачу только надлежащим образом оформленных документов.

1.8. Стороны обязуются соблюдать следующие условия:

1.8.1. Не осуществлять действий, наносящих ущерб другой Стороне вследствие использования Системы ДБО.

1.8.2. Поддерживать системное время компьютерного устройства своего абонентского пункта по местному времени с точностью до пяти минут. При обработке документов, полученных по Системе ДБО, определяющим временем является текущее время по системным часам аппаратных средств Банка.

1.8.3. Не осуществлять операцию по ЭД, заверенному ЭП, если программа проверки, используя действующий ключ проверки подписывающей Стороны, не подтвердила подлинность ЭП подписывающей Стороны под ЭД.

1.8.4. При осуществлении операций на основании полученных по Системе ДБО ЭД руководствоваться требованиями Законодательства и Договоров, заключенных между Банком и Клиентом.

1.8.5. Обеспечивать целостность и сохранность программных средств, ЭД, защиту ключей ЭП, паролей доступа и другой информации, передаваемой и получаемой по Системе ДБО.

1.8.6. Вести архивы документов на магнитных и бумажных носителях, хранить их в соответствии с порядком и сроками, установленными для хранения данного вида документов.

1.8.7. За собственный счет поддерживать в рабочем состоянии и при необходимости самостоятельно модернизировать свои помещения и технические средства обеспечения работоспособности вычислительной техники, средств связи, автоматизированного рабочего места, с которого осуществляется работа с Системой ДБО.

2. УСЛОВИЯ И ПОРЯДОК ОСУЩЕСТВЛЕНИЯ ЭЛЕКТРОННОГО ВЗАИМОДЕЙСТВИЯ

2.1. Общие положения

2.1.1. Программное обеспечение Банка настроено на взаимодействие с системой программного обеспечения ДБО, разработанной АО «БИФИТ», и предполагает использование этой Системы ДБО Клиентом.
2.1.2. Банк и Клиент взаимно признают достоверность ЭП, созданной программной Системой ДБО, разработанной АО «БИФИТ», на ЭД, передаваемых согласно условиям Комплексного договора.
2.1.3. После заключения Договора ДБО в рамках Комплексного договора Стороны проводят техническую и организационную подготовку, регистрацию ключей проверки ЭП.
2.1.4. Документы, переданные по Системе ДБО, приобретают юридическую силу после получения уполномоченными службами Банка должным образом оформленного и подписанного Сертификата ключа проверки подписи и регистрации Клиента в Системе ДБО.
2.1.5. ЭД представляют собой электронные бланки документов, заполняемые Клиентом на Сайте в соответствии с требованиями Банка. На экран компьютерного устройства Клиента выводится электронный бланк, который заполняется согласно наименованиям полей и правилам, принятым в Банке. Некоторые поля заполняются автоматически в соответствии со встроенными справочниками реквизитов. Заполнение документов возможно после установления, защищенного (с использованием алгоритмов шифрования и обеспечения целостности) соединения между Клиентом и Банком.
2.1.6. Заполняемые в Системе ДБО документы проходят предварительную автоматическую проверку (на датировку документа, на присутствие обязательной информации в полях документа, на соответствие вводимых данных - реквизитам, записанным во встроенном справочнике и иные проверки в соответствии с принятой технологией).
2.1.7. На этапе обработки документов в Банке осуществляется автоматический контроль (на соответствие электронной подписи содержимому документа, на правильность указанного номера счета Клиента, на соответствие реквизитов Банка и РКЦ получателя установленным Банком России и иные проверки в соответствии с принятой технологией). В случае выявления несоответствий в ходе проверки документа, операции по документу не проводятся, а Клиент получает информацию с указанием причин отказа в приеме на обработку ЭД в строке статуса в соответствующем модуле, загруженном с Сайта.
2.1.8. После заполнения электронной формы платежного или иного документа Клиентом осуществляется подписание документа. Подробности порядка работы с электронными документами описаны во встроенной в Систему ДБО документации.
2.1.9. Основанием для отказа Банком в исполнении ЭД служат:
- отрицательный результат проверки ЭП;
- недостаток денежных средств для проведения операций на счете Клиента (за исключением случаев предоставления овердрафта, оговоренных соответствующими договорами);
- несоответствие даты документа требованиям действующего Законодательства;
- неверно указанные реквизиты отправителя или получателя платежа;
- несоответствие ЭД требованиям Банка России и Банка.

2.1.10. Активной стороной при установлении связи является Клиент.

2.2. Сроки обработки платежей

Работа Системы ДБО обеспечивается Банком в течение времени, установленного Банком для обслуживания Клиентов. Информация о времени обслуживания Клиентов и приема расчетных документов доводится до сведения Клиента путем размещения на информационных стендах в офисах Банка и на Сайте.

2.3. Аварийный режим работы

При возникновении неисправности технических или программных средств Клиента, или других нештатных ситуаций, Клиент до 14 часов местного времени, того же дня, должен предупредить уполномоченных сотрудников Банка, и осуществить действия для доставки в Банк надлежащим образом оформленных распоряжений и других ЭД на бумажных носителях. Доставка распоряжения, документов на бумажном носителе осуществляется Клиентом в течении действующего операционного дня Банка.

3. ОБЕСПЕЧЕНИЕ ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

3.1. Общие положения

3.1.1. Защита информации в Системе ДБО является многоуровневой и задействует возможности операционной системы, прикладного программного обеспечения и специализированных программных и технических средств и организационных мер (наличие соответствующих администраторов), организации хранения ПО, используемого в Системе ДБО.

3.1.2. Система комплексной защиты информации, состоящая из набора аппаратно-программных средств и административных мер, обеспечивает:

- создание ключей шифрования и электронной подписи;
- электронную подпись под документами;
- шифрование передаваемой информации;
- аутентификацию Клиентов и разграничение их прав;
- достоверность факта получения документа получателем;
- подтверждение авторства и целостность электронных документов;
- выявление ошибок, сбоев и несанкционированных действий обслуживающего персонала;
- разбор конфликтных ситуаций.

3.1.3. Для разрешения возможных споров в Банке ведутся контрольные архивы ЭД подписанных ЭП, а также архивы ключей проверки электронной подписи. Хранение контрольных архивов ЭД осуществляется в течение пяти лет с момента проведения операции.

3.1.4. При проверке подписи под электронным документом используется соответствующий ключ подписи Клиента, подписавшего электронный документ.

3.2. Порядок генерации ключей ЭП

3.2.1. В процессе предварительной регистрации Клиент самостоятельно создает ключ ЭП и парный ему ключ проверки ЭП. Ключ ЭП Клиента сохраняется на Носитель электронного ключа Клиента. Ключ проверки ЭП по защищенному соединению передается в Банк и предварительно регистрируется. Также ключ проверки ЭП распечатывается Клиентом на бумажном носителе в виде Сертификата ключа проверки подписи в Системе ДБО, далее подписывается руководителем и главным бухгалтером Клиента, заверяется оттиском печати организации и регистрируется в Банке согласно п.3.2.5. данного Регламента. Распечатка Сертификата ключа проверки подписи хранится в Банке, а ее электронный аналог находится в каталоге ключей Банка и Клиента.

3.2.2. Все ключи ЭП защищаются паролями и данный пароль является конфиденциальной информацией соответствующей Стороны.

3.2.3. Владельцы Сертификатов ключа проверки подписи несут персональную ответственность за обеспечение сохранности ключевой информации и защиту Носителя электронного ключа от несанкционированного доступа.

3.2.4. Все процедуры окончательной регистрации Клиента и проверки ключей проверки ЭП происходят в помещении, на программном обеспечении и оборудовании Банка.

3.2.5. При регистрации ключа проверки ЭП Клиента в Банке производится сверка ключа проверки ЭП Клиента с ключом проверки, напечатанным в Сертификате ключа проверки подписи, и проверка данных лиц, на имя которых сформированы ключи, на соответствие

с именами, фамилиями, образцами подписей и оттиском печати, указанными в КОП Клиента, хранящейся в Банке.

3.2.6. При регистрации ключей без права подписи производится сверка Ф.И.О., подписи и должности Уполномоченных лиц Клиента, указанных в Сертификате, на соответствие данным представителей Клиента, содержащихся в документах, удостоверяющих личность, и документах, подтверждающих наличие соответствующих полномочий представителя Клиента без права электронной подписи (Доверенность).

3.2.7. Ключ активируется только после получения заверенного Клиентом Сертификата ключа проверки подписи и положительных результатов проверки данных, указанных в п. 3.2.5.

3.3. Порядок хранения и смены ключей ЭП

3.3.1. Порядок хранения ключей

3.3.1.1. Надежность средств криптозащиты и подлинность передаваемой по каналам связи информации обеспечивается только при условии сохранности от компрометации (утрата, копирование и т.п.) действующих ключей ЭП.

3.3.1.2. Клиент берет на себя полную ответственность и обязуется самостоятельно обеспечить сохранность, неразглашение и нераспространение своих ключей ЭП. В случае потери, кражи, несанкционированного копирования или любого подозрения о компрометации ключей Клиент обязан немедленно оповестить Банк, прислав в дальнейшем подтверждение в письменной форме.

3.3.1.3. Банк и Клиент обеспечивают сохранность ключей. При этом выведенные из употребления ключи проверки ЭП хранятся те же сроки, что и документы, подписанные и зашифрованные этими ключами.

3.3.2. Порядок смены ключей ЭП

3.3.2.1. Смена ключей производится при:

- Замене КОП Клиента.
- Истечении срока действия ключей.
- Компрометации ключей.
- Заявлении Клиента в письменной форме.

3.3.2.2. Срок действия ключей устанавливается в 365 календарных дней с момента их изготовления.

3.3.2.3. Смена ключей уполномоченных лиц Клиента производится в соответствии с п.3.2.1. данного Регламента.

3.3.2.4. ЭД, подписанный ЭП с использованием новых ключей, принимается Банком только после получения Сертификата ключа проверки подписи и проведения регистрации ключей в соответствии п. 3.2.5. данного Регламента.

3.3.3. Порядок смены ключей ЭП при истечении срока действия (без визита в БАНК)

3.3.3.1. Смена ключей ЭП без визита в БАНК доступна только уполномоченным лицам Клиента (владельцам действующих ключей ЭП) до окончания срока действия используемых ключей ЭП.

3.3.3.2. Смена ключей ЭП без визита в БАНК, у которых истек срок действия, невозможна.

3.3.3.3. Создание нового ключа ЭП и ключа проверки ЭП в Системе ДБО происходит в соответствии с п.3.2. данного Регламента за исключением необходимости предоставления в Банк Сертификата ключа проверки ЭП на бумажном носителе.

3.3.3.4. По результатам прохождения всех этапов создания ключа ЭП в Системе ДБО автоматически создается предзаполненное заявление на выпуск Сертификата ключа проверки ЭП, которое подписывается текущим ключом Клиента. Далее, в автоматическом режиме по защищенному соединению передается в Банк для проверки и регистрации.

3.3.3.5. После приема, успешной проверки, исполнения заявления и активации ключа ЭП на стороне Банка новый ключ ЭП может быть использован Клиентом для работы в Системе ДБО.

3.4. Порядок блокировки ключей ЭП

3.4.1. Банк блокирует (приостанавливает действие) ключа с момента получения уполномоченными службами Банка письменного заявления Клиента о блокировке ключа (содержащего причину блокировки), составленного в произвольной форме, подписанного руководителем и главным бухгалтером Клиента и заверенного оттиском печати организации. В экстренных случаях, блокировка может быть произведена при уведомлении иным способом (по телефону, по электронной почте, факсу и т.п.) с последующим предоставлением подписанного заявления на бумажном носителе в течение трех рабочих дней. После блокирования ключа, прием и обработка документов, подписанных данным ключом, прекращается.

3.4.2. Банк может блокировать ключ Клиента самостоятельно, в случае возникновения подозрений в компрометации ключа. В этом случае уполномоченный сотрудник Банка немедленно извещает Клиента о принятом решении и о приостановлении обработки ЭД, подписанных этим ключом по телефону или с использованием других средств связи.

3.4.3. Снятие блокировки производится на основании заявления Клиента, подписанного руководителем и главным бухгалтером и заверенного печатью организации, об устранении причин, приведших к блокированию ключа. В случае блокировки ключа по инициативе Банка снятие блокировки с ключа Клиента производится по согласованию с Клиентом и с его письменного разрешения.

3.5. Порядок исключения ключей ЭП

3.5.1. Банк исключает (блокирует, удаляет) ключ из каталога (базы) действующих ключей проверки, с момента получения уполномоченными службами Банка письменного заявления Клиента, составленного в произвольной форме и подписанного руководителем и главным бухгалтером и заверенного оттиском печати организации. Ключ исключается из каталога ключей проверки, прием и обработка ЭД, подписанных данным ключом прекращается.

3.5.2. Банк и Клиент обеспечивают сохранность исключенных ключей согласно п. 3.3.1. данного Регламента. При этом исключенные ключи хранятся в течение того же времени, что и документы, подписанные и зашифрованные этими ключами.

3.6. Порядок действий в случае компрометации ключей ЭП:

3.6.1. В случае компрометации или подозрения на компрометацию ключа Клиент должен незамедлительно известить уполномоченных сотрудников Банка для блокировки соответствующего ключа, в соответствии с порядком, установленным п. 3.4. данного Регламента.

3.6.2. В случае неподтверждения компрометации ключа, Банк производит снятие блокировки ключа в соответствии с п. 3.4.3. данного Регламента.

3.6.3. В случае подтверждения компрометации ключа Банк исключает скомпрометированный ключ в соответствии с п. 3.5. данного Регламента.

3.6.4. ЭД, подписанные скомпрометированным ключом, и ключ проверки ЭП хранятся в соответствии с п. 3.3.1.3. данного Регламента.

Приложение 3

к Условиям дистанционного банковского обслуживания

ПЕРЕЧЕНЬ ЭЛЕКТРОННЫХ ДОКУМЕНТОВ, ПЕРЕСЫЛАЕМЫХ ПО СИСТЕМЕ «ИНТЕРНЕТ БАНК-КЛИЕНТ» В СООТВЕТСТВИИ С ПРЕДОСТАВЛЯЕМЫМИ КЛИЕНТУ УСЛУГАМИ

Виды сообщений, которые Клиент передает в Банк по Системе ДБО:

№ п.п.	***Наименование ЭД***	***Вид сообщения***
1	***2***	***3***
Документы по счетам Клиента		
1	Платежное поручение в рублях	Формализованное
2	Заявление на аккредитив	Формализованное
3	Платежное требование	Формализованное
4	Инкассовое поручение	Формализованное
5	Заявление об акцепте / отказе от акцепта	Формализованное
6	Заявление на получение наличных денежных средств	Формализованное
7	Реестр переданных на инкассо платежных требований	Формализованное
8	Заявление на перевод средств в иностранной валюте	Формализованное
9	Заявление на открытие импортного аккредитива	Формализованное
10	Распоряжение на покупку иностранной валюты	Формализованное
11	Поручение на покупку валюты за другую валюту	Формализованное
12	Поручение на продажу иностранной валюты	Формализованное
13	Распоряжение на обязательную продажу валюты	Формализованное
14	Зарплатный реестр	Формализованное
15	Запросы по вопросам расчетов и другим видам услуг, предоставляемых в БАНК (в соответствии с адресной книгой)	Свободный формат
16	Прочие сообщения и запросы	Свободный формат
Документы для целей валютного контроля		
17	Паспорт сделки по контракту	Формализованное
18	Паспорт сделки по кредитному договору	Формализованное
19	Справка о валютных операциях	Формализованное
20	Справка о подтверждающих документах	Формализованное
21	Прочие сообщения и запросы	Свободный формат

Виды сообщений, которые Клиент получает по Системе ДБО из Банка:

№ п.п.	***Наименование ЭД***	***Вид сообщения***
1	***2***	***3***
Документы по счетам Клиента		

1	Выписки по рублевым счетам Клиента, включая остатки по счетам и приложения к выписке;	Формализованное
2	Выписки по валютным счетам Клиента, включая остатки по счетам и приложения к выписке;	Формализованное
3	Оборотно-сальдовая ведомость;	Формализованное
4	Платежное требование, выставленное Клиенту;	Формализованное
5	Прочие сообщения и запросы	Свободный формат

Перечень и формы ЭД могут меняться в связи с изменениями нормативных актов Банка России и с учетом развития системы и услуг, предоставляемых Клиентам Банка при использовании Системы «Интернет Банк-Клиент».

Приложение 4

к Условиям дистанционного банковского обслуживания

СЕРТИФИКАТ КЛЮЧА ПРОВЕРКИ ПОДПИСИ В СИСТЕМЕ «ИНТЕРНЕТ БАНК-КЛИЕНТ» ЦМРБАНК (ООО)

1. Наименование организации
_____
_____
_____
_____

2. Юридический адрес _____
3. Местонахождение _____
4. Наименование документа о регистрации, кем и когда выдан _____
_____

5. Тел. _____ 6. Факс _____7. E-mail _____
8. Примечания: _____
9.Сведения о владельце ключа:
Фамилия, имя, отчество _____
Должность _____
Паспорт: сер._____ № _____ выдан _____
дата выдачи "_____"_____ _____ г. код подразделения _____

Личная подпись владельца ключа

Информация о ключе проверки ЭП:

Идентификатор ключа проверки ЭП: _____ Идентификатор токена: _____

Наименование криптосредств:
_____

Алгоритм: _____

Представление ключа проверки ЭП в шестнадцатеричном виде:
_____
_____
_____
_____
_____
_____
_____

Дата начала действия ключа "___" _____ 20_ г.
Дата окончания действия ключа "___" _____ 20_ г.

Достоверность приведенных данных подтверждаю

Руководитель организации _____ (_____)
ФИО

Главный бухгалтер _____ (_____)
ФИО

Оттиск печати

"___"_____20_ г.

Уполномоченный представитель БАНК _____ (_____)
ФИО

Администратор системы/Уполномоченный контролер БАНК _____(_____)
ФИО

Оттиск печати Банка

"___"_____20_ г.

Приложение 5

к Условиям дистанционного банковского обслуживания

ПОЛОЖЕНИЕ ПО РАЗБОРУ КОНФЛИКТНЫХ СИТУАЦИЙ, СВЯЗАННЫХ С ПОДЛИННОСТЬЮ ЭЛЕКТРОННЫХ ДОКУМЕНТОВ

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. В данном Положении описан порядок разрешения конфликтных ситуаций между Банком и Клиентом, связанных с подлинностью электронных документов, исполненных в Системе ДБО.

1.2. Электронный документ считается подлинным, если он был, с одной стороны, надлежащим образом оформлен и подписан, а с другой - проверен и принят.

1.3. При наличии сомнений в подлинности ЭД или его содержания Сторона - инициатор спора обязана направить другой Стороне письмо с подробным изложением нарушения, обстоятельств происшедшего и предложением создать согласительную экспертную комиссию.

1.4. В случае согласия с претензией, содержащейся в письме, Сторона, получившая письмо, незамедлительно уведомляет другую Сторону и устраняет нарушения, описанные в письме. Согласительная экспертная комиссия в таком случае не создается.

1.5. До подачи письменного заявления сторонам рекомендуется проверить, что причиной возникновения Спора не является нарушение целостности программного обеспечения, целостности среды исполнения на компьютере Клиента, компрометация ключей ЭП или несанкционированный доступ к ресурсам.

2. РАБОТА СОГЛАСИТЕЛЬНОЙ ЭКСПЕРТНОЙ КОМИССИИ

2.1. Для рассмотрения Споров создается согласительная экспертная комиссия. Данная комиссия создается только по письменному заявлению одной из Сторон. Дата сбора комиссии назначается не позднее 15 (Пятнадцати) календарных дней с момента отправки предложения о ее создании. В состав комиссии входит равное количество представителей обеих Сторон. При необходимости, с согласия обеих Сторон, в состав комиссии могут быть дополнительно введены эксперты третьей стороны. Полномочия членов комиссии подтверждаются доверенностями, выданными в установленном порядке. Состав комиссии должен быть зафиксирован в итоговом документе (Акте), отражающем результаты работы комиссии.

2.2. Экспертная комиссия осуществляет свою работу на территории Банка, с использованием компьютерных устройств, программного обеспечения и ключевых элементов.

2.3. Срок работы комиссии – 5 (Пять) рабочих дней. В особо сложных случаях, по обоюдному письменному согласию Сторон, этот срок может быть увеличен, но не более чем до одного месяца.

2.4. Целью работы созданной комиссии является установление подлинности ЭД, исполненного в рамках Договора.

2.5. Стороны обязаны предоставить комиссии возможность ознакомиться с условиями и порядком работы Системы ДБО. Стороны способствуют работе комиссии и не допускают отказа от представления необходимых документов, имеющих отношение к рассматриваемому Спору.

2.6. В ходе рассмотрения комиссией Спора о подлинности (наличии или отсутствии) документа, исполненного с помощью Системы ДБО и подписанного ЭП, каждая Сторона

обязана доказать лишь то, что она своевременно и надлежащим образом выполнила обязательства, взятые на себя по Комплексному договору, в том числе его Разделам и Приложениям к ним.

2.7. По итогам работы комиссии составляется Акт, в котором в обязательном порядке отражаются:

- установленные обстоятельства;
- действия членов комиссии;
- выводы о подлинности предъявленного электронного документа;
- основания, послужившие для формирования выводов.

Акт подписывается уполномоченными представителями Сторон не позднее 10 (Десяти) календарных дней с момента окончания работы комиссии. В случае, если подписание Акта в этот срок не состоится, заинтересованная Сторона вправе обратиться в Арбитражный суд и без выработанного Сторонами решения, а в качестве доказательства в судебном споре представить Акт, составленный в соответствии с настоящим Положением.

2.8. В случае, если предложение о создании комиссии оставлено другой Стороной без ответа (по истечении 15 (Пятнадцати) календарных дней согласно п.2.1. данного Положения), либо Сторона отказывается от участия в комиссии, либо работе комиссии были учинены препятствия, которые не позволили комиссии оформить надлежащий Акт, заинтересованная Сторона составляет Акт в одностороннем порядке с указанием причины составления его в одностороннем порядке. В указанном Акте фиксируются обстоятельства, позволяющие сделать вывод о том, что оспариваемый электронный документ, произведенный в Системе ДБО в соответствии с Комплексным договором, является подлинным, либо формулируется вывод об обратном. Указанный Акт направляется другой Стороне для сведения.

3. РАССМАТРИВАЕМЫЕ СПОРЫ

Согласительная экспертная комиссия рассматривает споры следующего характера: Сторона-получатель ЭД утверждает, что инициирующая Сторона-отправитель должным образом оформила, заверила (подписала) ЭП и передала на обработку документ, а Сторона-отправитель отрицает факт подготовки, заверения (подписания) ЭП и передачи на обработку этого документа.

В этом случае Сторона-получатель предъявляет комиссии ключ проверки подписи Стороны-отправителя в электронном виде и файл, содержащий спорный ЭД, подписанный ЭП Стороны-отправителя.

На специально выделенном компьютере устанавливается эталонное программное обеспечение для проверки корректности ЭП под документом.

С помощью программы проверки ЭП проверяется корректность ЭП файла, содержащего оспариваемый ЭД.

В том случае, если корректность ЭП подтверждается программой, виновной признается Сторона-отправитель ЭД, в противном случае виновной признается Сторона-получатель ЭД.

Согласительная экспертная комиссия может рассматривать иные споры, связанные с вопросами подлинности ЭД.

4. ПОРЯДОК ФОРМИРОВАНИЯ И ПРОВЕРКИ ЭЛЕКТРОННЫХ ПОДПИСЕЙ ПОД ЭЛЕКТРОННЫМИ ДОКУМЕНТАМИ

4.1. Соблюдается следующая последовательность формирования электронной подписи под электронным документом:

4.1.1. Подписываемый электронный документ состоит из набора полей и представляется в виде:

<Наименование поля 1>=<Значение поля 1> <символ перевода строки>

<Наименование поля 2>=<Значение поля 2> <символ перевода строки>

……...

4.1.2. Подписываемый ЭД в виде набора полей, описанного в п. 4.1.1, преобразовывается в строку символов, и далее в соответствии с кодировкой UniCode преобразовывается в байтовый массив.

4.1.3. Электронная подпись формируется от указанного в п. 4.1.2 байтового массива в соответствии ГОСТ Р34.10-2001.

4.1.4. Публичные параметры P,Q,A и таблица подстановок для вычисления хеш-функции в соответствии с ГОСТ Р34.11-94 при контрольной проверке ЭП для указанного в п.4.1.2 байтового массива представляются в Банк в шестнадцатиричном виде по запросу согласительной экспертной комиссии.

4.2. Контрольная проверка электронной подписи Клиента под электронным документом, пришедшим в Банк, осуществляется в АРМе «Операционист», входящим в комплекс Системы ДБО или при помощи иного Программного обеспечения, применяемого в Банке на момент проведения контрольной проверки.

При проверке ЭП Клиента в АРМе «Операционист», отображается:

- содержание электронного документа
- идентификаторы ключей ЭП Клиента, которыми подписан ЭД
- время формирования ЭП (если документ подписан несколькими ЭП – время формирования каждой ЭП)
- результаты проверки каждой из ЭП под ЭД

Результат проверок ЭП Клиента под ЭД в АРМе «Операционист» или в ином Программном обеспечении, применяемом в Банке на момент проведения контрольной проверки, является подтверждением верности/неверности ЭП Клиента под ЭД.

Приложение 6

к Условиям дистанционного банковского обслуживания

ПОРЯДОК ОБМЕНА МЕЖДУ БАНКОМ И КЛИЕНТОМ В ЭЛЕКТРОННОМ ВИДЕ ДОКУМЕНТАМИ И ИНФОРМАЦИЕЙ, СВЯЗАННЫМИ С ПРОВЕДЕНИЕМ ВАЛЮТНЫХ ОПЕРАЦИЙ

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Предметом настоящего Порядка являются взаимоотношения Сторон по обмену в электронном виде документами и информацией, требование о представлении (направлении) которых предусмотрено Законодательством, в том числе нормативными актами Банка России, регламентирующими порядок осуществления функций агента валютного контроля (далее – документы валютного контроля).

1.2. Стороны соглашаются, что документы валютного контроля, направляемые по Системе «Интернет Банк-Клиент», подписываются усиленной неквалифицированной электронной подписью и признаются равнозначными документам на бумажном носителе, подписанным собственноручными подписями уполномоченных Сторонами лиц и заверенным печатью.

2. ПОРЯДОК ФОРМИРОВАНИЯ И ПЕРЕДАЧИ ДОКУМЕНТОВ И ИНФОРМАЦИИ

2.1. Формализованные документы валютного контроля, указанные в Приложении №3 к Порядку, формируются Сторонами в электронном виде с использованием программно-технических средств Системы ДБО и подписываются электронной подписью.

2.2. Документы, обосновывающие проведение валютных операций, оформление / переоформление / прием на обслуживание / закрытие паспортов сделок, а также документы, подтверждающие вывоз (ввоз) товара с территории (на территорию) Российской Федерации, выполнение работ, оказание услуг, передачу информации и результатов интеллектуальной деятельности, в том числе исключительных прав на них, предоставляются Клиентом в виде изображений документов, полученных с использованием сканирующих устройств.

Файлы изображений могут быть прикреплены как к указанным в Приложении №3 формализованным документам, так и к письму свободного формата, подписанному электронной подписью.

2.3. Ведомости контроля и паспорта сделок, предоставляемые Клиентом при переводе договоров на обслуживание в Банк из иных уполномоченных банков, а также направляемые Клиенту при закрытии в Банке паспортов сделок в связи с переводом в иные уполномоченные банки, при уступке резидентом требования по контракту (кредитному договору) другому лицу - резиденту либо при переводе долга резидентом по контракту (кредитному договору) на другое лицо – резидента, должны быть сформированы в виде файлов установленного Банком России формата XML. Для передачи по Системе ДБО файлы прикрепляются к письму свободного формата, подписанному электронной подписью.

2.4. Направление Сторонами запросов, разъяснений и иной информации, необходимой для целей валютного контроля, осуществляется посредством передачи писем свободного формата, подписанных электронной подписью.

2.5. Датой предоставления документов, направленных Клиентом по Системе ДБО в рамках установленного Банком операционного дня, считается текущая дата.

При направлении Клиентом по Системе ДБО документов после окончания установленного Банком операционного дня, датой предоставления данных документов считается следующий рабочий день.

2.6. Датой принятия Банком поступившего от Клиента ЭД является дата установления в Системе ДБО статуса данного документа «Исполнено» и подписания ЭП Банком. Датой возврата в Банк поступившего от Клиента ЭД является дата установления в Системе ДБО статуса данного документа «Отвергнуто» и подписания ЭП Банком.

2.7. Клиент вправе отозвать направленные ранее ЭД путем направления в Банк сообщения с учетом требований Законодательства о валютном регулировании и валютном контроле.

3. ВЗАИМОДЕЙСТВИЕ СТОРОН

3.1. В рамках настоящего Порядка Клиент:

− формирует и предоставляет в Банк по Системе ДБО документы и информацию, указанные в п.2.1-2.4 настоящего Порядка, в соответствии с требованиями нормативных актов Банка России, внутренних документов Банка и настоящего Договора;

− регулярно осуществляет сеансы связи с Банком с целью получения формализованных документов, подписанных электронной подписью Банка, с отметками о приеме/отказе в приеме электронных документов;

− в случае получения от Банка отказа в приеме электронных документов Клиент вправе после устранения выявленных недостатков повторно направить документы в Банк сроки, по возможности, не превышающие сроки, установленные Банком России для предоставления таких документов.

3.2. В рамках настоящего Порядка Банк:

− осуществляет проверку документов, полученных по Системе ДБО в порядке и в сроки, предусмотренные нормативными актами Банка России, внутренними документами Банка и настоящим Договором;

− редактирует полученные формализованные документы в части внесения информации в разделы, предназначенные для заполнения Банком;

− при положительном результате проверки проставляет на формализованных документах отметку о дате приема документа Банком и возвращает их Клиенту в электронном виде по Системе ДБО в срок не позднее 2-х рабочих дней после даты приема документов;

− при отрицательном результате проверки возвращает Клиенту непринятые формализованные документы в электронном виде с указанием даты возврата и причины отказа в их принятии. Банк отказывает Клиенту в приеме документов в сроки и по основаниям, установленным Законодательством, в том числе нормативными актами Банка России, внутренними документами Банка и настоящим Договором.

Приложение 7

к Условиям дистанционного банковского обслуживания

МОБИЛЬНОЕ ПРИЛОЖЕНИЕ «ЦМР БИЗНЕС»

1. Доступ в Систему ДБО может осуществляться Клиентом в том числе с Мобильных устройств через Мобильное приложение. Для доступа к Системе ДБО через Мобильное приложение необходимо оформить Заявление на подключение/отключение к Мобильному приложению (Приложение №9 к настоящему Договору) и установить Мобильное приложение на свое Мобильное устройство.
2. Работа в Мобильном приложении возможна только при условии подключения Клиента к Системе ДБО.
3. Мобильное приложение доступно для устройств на платформах Android (версия 5.0 и выше). С целью расширения функциональных возможностей Мобильного приложения Банк имеет право по своему усмотрению периодически выпускать обновления Мобильного приложения. Клиент самостоятельно выбирает режим установки обновлений на Мобильное устройство.
4. Для регистрации в Мобильном приложении используется номер мобильного телефона, указанный в «Заявлении на подключение/отключение к Мобильному приложению «ЦМР Бизнес»» (Приложение №9 к настоящему Договору). Дополнительно с целью повышения удобства и скорости использования Мобильного приложения может быть настроен вход по ПИН коду или иному доступному в Мобильном устройстве способу аутентификации. Настройка входа по ПИН коду осуществляется пользователем самостоятельно.
5. Мобильное приложение обеспечивает доступ к функциональности Системы ДБО. Состав банковских услуг, предоставляемых посредством Мобильного приложения и функциональность Мобильного приложения определены Руководством пользователя по работе в Мобильном приложении «ЦМР Бизнес», размещенном на Сайте.
6. Устанавливая Мобильное приложение на свое Мобильное устройство и вводя Аутентификационные данные, пользователь подтверждает свое согласие на использование Мобильного приложения.
7. Подписание документов в Мобильном приложении осуществляется с помощью облачной ЭП. Ограничения, установленные Договором на обслуживание клиентов в Системе ДБО для ЭП, также действуют и для Мобильного приложения.
8. Права и обязанности Сторон при работе с Мобильным приложением определяются Условиями ДБО.
9. Клиент уведомлен о необходимости до начала работы в Мобильном приложении ознакомиться с Рекомендациями по обеспечению информационной безопасности при использовании Мобильного приложения (Приложение №8 к Договору). Использование Мобильного приложения влечет за собой дополнительный риск мошеннических действий третьих лиц, в том числе в случае, если используется одно устройство для работы и получения кодов аутентификации.
10. В целях обеспечения безопасности работы Мобильного приложения, Банк оставляет за собой право не предоставлять (блокировать) доступ к приложению с использованием отдельных версий операционных систем, не отвечающих требованиям информационной безопасности. Доступ к Мобильному приложению прекращается при расторжении Договора на обслуживание клиентов в Системе ДБО.
11. Банк может получать данные Мобильного устройства, на котором установлено Мобильное приложение в порядке, установленном в Приложении №9 к Условиям ДБО.

Приложение 8

к Условиям дистанционного банковского обслуживания

РЕКОМЕНДАЦИИ ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ ИСПОЛЬЗОВАНИИ МОБИЛЬНОГО ПРИЛОЖЕНИЯ

1. Общие рекомендации:
   - не оставляйте Мобильное устройство без присмотра;
   - настройте блокировку экрана Мобильного устройства. При включении Мобильного устройства или при выходе из спящего режима блокировку необходимо будет снимать. Для этого потребуется ввести PIN-код, пароль, графический ключ или отпечаток пальца (наличие или отсутствие представленных способов снятие блокировки Мобильного устройства зависит от конфигурации вашего устройства). Рекомендуется использовать совместно с ограничением неверных попыток снятия блокировки Мобильного устройства;
   - используйте шифрование. Средствами операционной системы Мобильного устройства зашифруйте данные, которые хранятся на устройстве;
   - используйте только лицензионное программное обеспечение;
   - не устанавливайте на Мобильное устройство программное обеспечение, полученное из неизвестных источников;
   - на Мобильном устройстве всегда должны быть установлены все официальные обновления операционной системы и приложений;
   - не подключайте Мобильное устройство к чужим компьютерам и не заряжайте телефон в публичных местах зарядки мобильных устройств.
2. Дополнительные рекомендации для мобильных устройств с операционной системой Android:
   - используйте операционную систему Android версий 5.0 и выше;
   - отключите «Режим разработчика». Если был активирован режим разработчика и после этого включен режим отладки по USB, отключите его;
   - мобильное устройство не должно иметь прав суперпользователя (root) для приложений;
   - установите на Мобильном устройстве Антивирусную защиту;
   - отключите возможность установки программного обеспечения из неизвестных источников.

Приложение 9
к Условиям дистанционного банковского обслуживания

ПОЛИТИКА КОНФИДЕНЦИАЛЬНОСТИ ПРИ ИСПОЛЬЗОВАНИИ МОБИЛЬНОГО ПРИЛОЖЕНИЯ

1. СФЕРА ПРИМЕНЕНИЯ И ЦЕЛЬ ПУБЛИКАЦИИ

Настоящая Политика действует в отношении всей информации, относящейся к данным Мобильного устройства, на котором установлено Мобильное приложение, которую Банк может получить в процессе использования Мобильного приложения.

Банк собирает и обрабатывает только ту информацию, которая необходима для предоставления и оказания услуг.

Использование Мобильного приложения осуществляется на основании договоров и соглашений с Банком, которые в числе прочего регулируют все вопросы обработки и хранения Банком информации.

Настоящая Политика применима только к Мобильному приложению. Банк не контролирует и не несет ответственность за информацию (последствия её передачи), переданную пользователем третьей стороне, в случае если такая передача была выполнена на ресурсе третьей стороны, на который пользователь мог перейти по ссылкам из Мобильного приложения.

Целью настоящей Политики является информирование Клиента об условиях обработки данных Мобильного устройства при использовании Мобильного приложения.

2. ОСНОВАНИЯ ДЛЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Банк собирает и хранит только ту информацию пользователя, которая необходима для предоставления сервисов, входящих в состав Мобильного приложения.

3. СОСТАВ ОБРАБАТЫВАЕМЫХ ДАННЫХ МОБИЛЬНОГО УСТРОЙСТВА, НА КОТОРОМ УСТАНОВЛЕНО МОБИБИЛЬНОЕ ПРИЛОЖЕНИЕ

В процессе использования Мобильного приложения Банк может собирать разные виды информации об использовании Мобильного устройства, на котором установлено Мобильное приложение, в том числе сведения об оборудовании и программном обеспечении. К указанным сведениям относятся:

- Идентификаторы программного обеспечения, Мобильного приложения, субъекта данных и среды (идентификаторы устройств, IMSI, IMEI, идентификаторы прошивки устройства, идентификаторы установки программного обеспечения, версии программного обеспечения, операционная система, идентификатора пользователя Мобильного приложения);
- Данные об использовании функционала аутентификации на Мобильном устройстве по отпечатку пальца (данные о поддержке данного функционала Мобильным устройством, данные об активации/деактивации функционала, данные о факте смены отпечатка пальца, используемого для аутентификации на Мобильном устройстве);
- Данные об установленных Мобильных приложениях (имена файлов, имена пакетов, пути, разрешения, сертификаты, источник, используемые библиотеки, дата и время установки, репутация приложения);
- Данные о местоположении Мобильного устройства (координаты, точность координат);
- Активные сетевые подключения (GPRS, GPS, Wi-Fi);
- Роуминг Мобильного устройства;

- Данные о сетевых подключениях (IP-адреса, MAC-адреса, URL-адреса, данные HTTP-реферера, SSID, VPN подключения);
- Отпечаток свойств Мобильного устройства (свойства прошивки и оборудования устройства, характеристики дисплея, свойства датчиков, данные сетевого подключения, текущие настройки, текущие настройки безопасности, местоположение, системные настройки, настройки webView, данные webGI, отпечаток);
- Данные о файлах (размер, имя, путь, хэш-сумма файла, MD5);
- Данные SensorEvent.

4. ЦЕЛИ ОБРАБОТКИ ДАННЫХ МОБИЛЬНОГО УСТРОЙСТВА, НА КОТОРОМ УСТАНОВЛЕНО МОБИЛЬНОЕ ПРИЛОЖЕНИЕ

Банк обрабатывает данные Мобильного устройства для достижения следующих целей:

- **Обеспечение безопасности.** Банк обеспечивает безопасность в Мобильном приложения и конфиденциальность данных Мобильного устройства. Для этого Банк использует собранные сведения для разработки обновлений и исправлений систем безопасности. Для достижения этой цели Банк использует сведения о Мобильном устройстве и об использовании Мобильного приложения.
- **Предотвращение мошеннических действий.** Банк обеспечивает безопасность операций в Мобильном приложении. Для этого Банк использует сведения о Мобильном устройстве и использовании Мобильного приложения.

5. СПОСОБЫ ОБРАБОТКИ И ДЕЙСТВИЯ, СОВЕРШАЕМЫЕ С ДАННЫМИ МОБИЛЬНОГО УСТРОЙСТВА, НА КОТОРОМ УСТАНОВЛЕНО МОБИЛЬНОЕ ПРИЛОЖЕНИЕ

Банк осуществляет обработку и хранение информации в соответствии с внутренними регламентами и Условиями безопасной обработки данных, с сохранением ее конфиденциальности. При обработке данных Мобильное приложение не раскрывает личность пользователя третьим лицам.

При обработке идентификационных и платежных данных Мобильное приложение ни при каких обстоятельствах не публикует/не распространяет персональную информацию, личные и конфиденциальные данные пользователя.

Информация может быть предоставлена государственным органам по запросу в соответствии с требованиями Законодательства.

Действия, совершаемые Банком с данными Мобильного устройства: сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение.

6. МЕРЫ ДЛЯ ЗАЩИТЫ ДАННЫХ ПОЛЬЗОВАТЕЛЯ

Банк принимает все зависящие от него организационные и технические меры для защиты информации пользователя от неправомерного или случайного доступа третьих лиц, уничтожения, изменения, блокирования, использования, копирования и распространения, от иных неправомерных действий.

Приложение 10
к Условиям дистанционного банковского обслуживания

ЗАЯВЛЕНИЕ НА ПОДКЛЮЧЕНИЕ / ОТКЛЮЧЕНИЕ К МОБИЛЬНОМУ ПРИЛОЖЕНИЮ «ЦМР БИЗНЕС»

_____, ИНН _____
(указывается полное наименование организации/ФИО индивидуального предпринимателя, ИНН)
в лице
_____
(должность)
_____,
(Ф.И.О.)
действующего на основании
_____
просит Вас:
☐ Подключить к Услуге

☐ Отключить от Услуги

Номер мобильного телефона	Вид подключения Услуги (нужное отметить)	
_____		Информационный[2]
		Полнофункциональный[3]

С Тарифами и условиями обслуживания в ЦМРБанк (ООО) ознакомлен и полностью согласен.

Руководитель организации / Индивидуальный предприниматель

_____ _____ _____
М.П.

Дата: «_____» _____20 ___ г.

Заполняется работником Банка

Заявление проверено и принято к исполнению.

Дата: «_____» _____20 ___ г.

_____ _____ _____

М.П.

[2] Мобильное приложение доступно на просмотр информации.

[3] Полный доступ к Мобильному приложению, создание, подписание и подтверждение писем / платежных документов.

Приложение 11
к Условиям дистанционного банковского обслуживания

Заявление на выпуск сертификата ключа проверки ЭП

Банку_____

От
Клиента_____

Просим выпустить сертификат ключа проверки ЭП в соответствии с идентификационными данными:

1.Сведения об организации		
1.1	Наименование организации	
1.2	Место нахождения	
1.3	ОГРН	
1.4	Дата внесения в ЕГРЮЛ (ЕГРИП)	
1.5	ИНН (КИО)	
1.6	КПП	
1.7	Телефон	
2.Сведения о владельце ключа		
2.1	ФИО	
2.2	Должность	
2.3	Документ, удостоверяющий личность	
2.4	Серия	
2.5	Номер	
2.6	Дата выдачи	
2.7	Кем выдан	
2.8	Код подразделения	
3.Сведения о ключе проверки ЭП		
3.1	Идентификатор	
3.2	Наименование криптосредств	
3.3	Идентификатор устройства	
3.4	Алгоритм	
3.5	ID набора параметров алгоритма	
3.6	Представление ключа проверки ЭП	
3.7	Срок действия	

_____ Дата создания ключа ЭП: _____
_____

Приложение 12
к Условиям дистанционного банковского обслуживания

ПОРЯДОК ВЗАИМОДЕЙСТВИЯ ПРИ ОПЕРАЦИЯХ, СОВЕРШЕННЫХ БЕЗ ДОБРОВОЛЬНОГО СОГЛАСИЯ КЛИЕНТА

1. Общие положения

1.1. Настоящий Порядок разработан в соответствии с Федеральным законом от 27.06.2011 № 161-ФЗ «О национальной платежной системе», Федеральным законом от 02.12.1990 № 395-1 «О банках и банковской деятельности» и регулирует взаимодействие Банка и Клиента при выявлении операций по переводу денежных средств, а также операций внесения или выдачи наличных денежных средств с использованием банкоматов, совершенных без добровольного согласия Клиента или с согласием, полученным под влиянием обмана или при злоупотреблении доверием (далее — ОБДС).

1.2. Банк осуществляет мониторинг операций Клиента на наличие признаков ОБДС с использованием специализированных систем в соответствии с критериями, установленными Законодательством.

2. Действия Банка при выявлении подозрительной операции

2.1. При выявлении операции, соответствующей признакам ОБДС, Банк обязан:

2.1.1. В случае операции с использованием платежных карт, перевода электронных денежных средств или перевода с использованием Сервиса быстрых платежей платежной системы Банка России (СБП) — отказать в совершении такой операции до момента списания денежных средств клиента.
2.1.2. В иных случаях — приостановить прием к исполнению распоряжения Клиента на срок до 2 (двух) суток.

2.2. Банк незамедлительно уведомляет Клиента о приостановке или отказе в проведении операции способом, предусмотренным Комплексным договором (push-уведомление, СМС-информирование и т.п.), и предоставляет следующую информацию:

- причину приостановки/отказа;
- рекомендации по снижению рисков повторного осуществления ОБДС;
- о возможности Клиента подтвердить легитимность операции не позднее дня, следующего за днем приостановления;
- о возможности совершения Клиентом повторной операции, содержащей те же реквизиты получателя (плательщика) и ту же сумму перевода, способами, предусмотренными Комплексным договором, в случае отказа Банка в совершении Клиентом операции с использованием платежных карт, перевода электронных денежных средств или перевода денежных средств с использованием СБП.

2.3. При получении от Клиента подтверждения легитимности операции в течение 2 (двух) суток Банк осуществляет операцию. Если операция связана с получателем, сведения о котором имеются в Базе данных Банка России об ОБДС, Банк применяет «период охлаждения» — приостанавливает выполнение операции на 2 (два) дня с момента подтверждения Клиентом.

2.4. При неполучении подтверждения от Клиента в течение 2 (двух) суток распоряжение считается не принятым к исполнению.

3. Действия Клиента при выявлении ОБДС

3.1. При обнаружении операции, совершенной без его добровольного согласия, Клиент обязан:

3.1.1. Немедленно заблокировать Счет/Карту через Систему ДБО, Колл-центр Банка по телефону 8 (800) 25-00-922 , 8 (800) 23-44-300.

3.1.2. Направить Банку уведомление о несогласии с операцией (далее — Уведомление) незамедлительно, но не позднее дня, следующего за днем получения уведомления от Банка об операции или самостоятельного выявления ОБДС.

3.2. Уведомление направляется в Банк путем обращения в Колл-центр с последующим представлением письменного заявления в Подразделение Банка. В Уведомлении указываются: ФИО Клиента, реквизиты Счета/Карты, дата, сумма и реквизиты оспариваемой операции, обстоятельства ее выявления.

4. Рассмотрение Банком Уведомления Клиента и возмещение средств

4.1. При получении Уведомления Банк проводит проверку и в срок, не превышающий 30 (тридцати) календарных дней, принимает решение о возврате денежных средств или об отказе в возврате.

4.2. В случае принятия решения о возврате, Банк зачисляет денежные средства на Счет Клиента в срок, не превышающий 3 (трех) рабочих дней с даты принятия решения.

4.3. Банк обязан возместить Клиенту суммы ОБДС, за исключением случаев, когда докажет, что Клиент нарушил порядок использования Электронного средства платежа (ЭСП) по своей вине (умысел или грубая неосторожность).

4.4. Обязанность по возмещению не возникает, если Клиент не направил Уведомление в установленный срок.

5. Блокировка ЭСП в связи с наличием сведений в Базе данных Банка России

5.1. Банк вправе, а в случае поступления сведений от МВД России — обязан, приостановить использование Клиентом ЭСП при наличии сведений о Клиенте и (или) его ЭСП в Базе данных Банка России об ОБДС.

5.2. Банк уведомляет Клиента о блокировке и его праве подать заявление в Банк России об исключении сведений из Базы данных.

5.3. Банк вправе самостоятельно направить в Банк России мотивированное заявление об исключении сведений, если сочтет их включение необоснованным.

5.4. Банк незамедлительно возобновляет использование ЭСП после получения информации об исключении сведений из Базы данных.

6. Обжалование включения сведений в Базу данных Банка России

6.1. Клиент вправе подать заявление об исключении сведений через любой банк или напрямую в Банк России через Интернет-приемную.

6.2. Банк России рассматривает заявление в течение 15 (пятнадцати) рабочих дней. Решение направляется Клиенту или в Банк для последующего информирования Клиента.

7. Ответственность и обязанности Сторон

7.1. Клиент обязан предоставлять Банку достоверную контактную информацию и своевременно ее обновлять.

7.2. Риск убытков по ОБДС несет Банк, за исключением случаев, когда ОБДС произошла по вине Клиента.

7.3. Работники Банка при звонке Клиенту действуют только с номеров Банка, указанных на Сайте Банка в разделе «Контакты», и не запрашивают коды из СМС, номер Карты и иные конфиденциальные данные.