**Договор №\_\_\_\_\_/iBank от «\_\_\_» \_\_\_\_\_\_\_\_\_\_\_2022 г.**

**дистанционного банковского обслуживания юридических лиц по Системе «iBank»**

**ООО «ЗЕМКОМБАНК»**, именуемый в дальнейшем «Банк», в лице \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, действующего на основании \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, с одной стороны, и \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, именуемое в дальнейшем «Клиент», в лице \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, действующего/ей на основании \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, с другой стороны, вместе именуемые «Стороны», заключили настоящий Договор дистанционного банковского обслуживания юридических лиц и обмена электронными документами с юридическими лицами в Системе «iBank» (далее по тексту – **«Договор»**) о нижеследующем.

1. **Термины и определения**
   1. **АРМ** – автоматизированное рабочее место Клиента, с которого осуществляется вход в Систему «iBank».
   2. **Аутентификация** – подтверждение факта обращения непосредственно Клиента в Банк посредством Системы «iBank», в котором корректно были введены Аутентификационные данные, для предоставления и/или получения информации, совершения сделок, операций и иных действий, предусмотренных функционалом Системы «iBank».
   3. **Аутентификационные данные** – данные, которыми обладает легальный субъект доступа (Клиент), используемые для выполнения процедуры аутентификации при осуществлении логического доступа и совершения операций с использованием Системы «iBank» (факторами аутентификации: пароль, пин-код, смс-код, средства криптографической защиты информации на носителе» (далее – «ТОКЕН»).
   4. **Антифрод (или фрод-мониторинг)** — система, предназначенная для оценки финансовых и не финансовых событий (карточных транзакций, действий пользователя в ДБО, операций с баллами лояльности и проч.) на предмет подозрительности с точки зрения мошенничества и предлагающая рекомендации по их дальнейшей обработке.
   5. **Владелец Сертификата ключа проверки электронной подписи** – физическое лицо (сотрудник/ доверенное лицо Клиента, уполномоченный сотрудник Банка), на имя которого Удостоверяющим центром выдан Сертификат ключа проверки электронной подписи и которое владеет соответствующим Ключом электронной подписи, позволяющим создавать ЭП в Электронных документах (подписывать Электронный документ).
   6. **Вредоносный код (ВК) –** компьютерная программа, предназначенная для внедрения в автоматизированные системы, программное обеспечение, средства вычислительной техники, телекоммуникационное оборудование Банка и его Клиентов, пользователей систем дистанционного банковского обслуживания (в т.ч. Системы «iBank»), приводящего к его уничтожению, созданию, копированию, блокированию модификации и (или) передаче информации, а также к созданию условий для такого уничтожения, создания, копирования, блокирования, модификации и (или) передачи.
   7. **Зарегистрированный номер** – номер мобильного телефона, указанный в соответствующем заявлении Клиента.
   8. **Ключ электронной подписи** – уникальная последовательность символов, предназначенная для создания ЭП.
   9. **Ключ проверки электронной подписи** – уникальная последовательность символов, однозначно связанная с Ключом электронной подписи и предназначенная для проверки подлинности ЭП.
   10. **Подтверждение подлинности ЭП в ЭД (Проверка ЭП)** – положительный результат проверки принадлежности ЭП в ЭД Клиенту и отсутствия искажений в данном ЭД. Подтверждение подлинности ЭП должно осуществляться соответствующим средством ЭП с использованием Сертификата ключа проверки электронной подписи.
   11. **Распоряжение** – электронный документ, созданный и направленный в электронной форме по Системе «iBank» и являющийся расчетным (платежным) документом Клиента.
   12. **Сертификат ключа проверки электронной подписи (Сертификат)** – 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.
   13. **Счет –** расчетный счет в рублях РФ и/или депозитный счет в рублях РФ и/или иной банковский счет в рублях РФ (в т.ч. специальный), открытый Банком Клиенту на основании соответствующего договора с Банком, обслуживание которого осуществляется с использованием Системы «iBank».
   14. **Система «iBank»** – информационно-технологическая система дистанционного банковского обслуживания (веб-версия), используемая Банком для обслуживания Клиентов в сети Интернет, являющаяся электронным средством платежа, и позволяющая Клиенту использовать Систему «iBank» в соответствии с настоящим Договором.
   15. **ТОКЕН** (USB – ключ / ключевой носитель) – компактное сертифицированное в ФСБ России программно-аппаратное устройство, предназначенное для хранения Ключа электронной подписи, Ключа проверки электронной подписи, Сертификата, а также другой электронно-цифровой информации.
   16. **Средства электронной подписи (Средства ЭП)** - аппаратные и /или программные средства, являющиеся частью Средств криптографической защиты информации и реализующие хотя бы одну из следующих функций при организации электронного документооборота: создание Электронной подписи в Электронном документе с использованием Ключа электронной подписи; подтверждение подлинности Электронной подписи, содержащейся в Электронном документе, с использованием Ключа проверки электронной подписи; создание Ключа электронной подписи и Ключа проверки электронной подписи.
   17. **Средства криптографической защиты информации (СКЗИ) / Криптографические средства** – аппаратные и(или) программные средства, обеспечивающие применение ЭП и Шифрования при организации ЭД. Средства криптографической защиты информации могут применяться как в виде самостоятельных программных модулей, так и в виде инструментальных средств, встраиваемых в прикладное программное обеспечение. В Системе «iBank» допускается использование только Средств криптографической защиты информации, разрешённых к использованию Оператором сервиса и имеющих соответствующие сертификаты.
   18. **Тарифы -** тарифы комиссионных вознаграждений по операциям в рублях в части открытия и обслуживания банковских счетов юридических лиц (некредитных организаций) в ООО «ЗЕМКОМБАНК», размещенных на сайте Банка и/или направленные Клиенту по Системе «iBank».
   19. **Шифрование** – криптографическое преобразование данных, позволяющее предотвратить доступ неуполномоченных лиц к содержимому зашифрованного Электронного сообщения.
   20. **Удостоверяющий Центр** – удостоверяющий центр который осуществляет изготовление Сертификатов ключей проверки электронных подписей для юридических и физических лиц для возможности осуществления электронного документооборота в рамках Системы iBank.
   21. **ФСБ** - Федеральная служба безопасности Российской Федерации.
   22. **Электронный документ (ЭД**) – любой документ, предусмотренный функционалом Системы «iBank», в том числе Распоряжение, оформленный Клиентом в электронном виде и удостоверенный ЭП.
   23. **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 Владельца сертификата ключа проверки ЭП, подписывающего информацию. В рамках настоящего Договора ЭП является усиленной неквалифицированной электронной подписью (УНЭП), созданная в соответствии со стандартами ГОСТ 34.10-2012/ ГОСТ 34.11-2012.
   24. **Электронное сообщение** – информация в электронной форме, переданная или полученная Клиентом/Банком с использованием Системы «iBank».

1. **Предмет Договора**
   1. Настоящий Договор устанавливает порядок дистанционного банковского обслуживания (далее – «ДБО») Клиентов с использованием Системы «iBank» в целях предоставления услуг по ДБО, обмену ЭД между Банком и Клиентом, и определяет возникающие в этой связи права, обязанности и ответственность Сторон.
   2. Предметом настоящего Договора являются: определение условий и порядка обмена Электронными документами между Банком и Клиентом по Системе «iBank».
   3. На основании настоящего Договора, при выполнении его условий, и с учетом технических возможностей Банка с использованием Системы «iBank» осуществляются:
      1. получение Клиентом информации о состоянии Счета/Счетов Клиента, открытых в Банке, включая, прием/передачу выписок и приложений к ним, информации о банковских услугах и продуктах, информации о режиме осуществления операций.
      2. прием к исполнению от Клиента Распоряжений в целях осуществления переводов денежных средств со Счета/ Счетов Клиента в рамках применяемых форм безналичных расчетов.
      3. заключение договоров/соглашений Клиента с Банком, подписание заявлений, приложений, изменений и дополнений к ним, иных документов, связанных с их оформлением, заключением, подписанием, исполнением, прекращением, расторжением, приемом/передачей указанных ЭД (если иное не предусмотрено действующим законодательством РФ и внутренними документами Банка).
      4. прием/передача иных ЭД, связанных с использованием Клиентом услуг Банка и проведением соответствующих операций, включая запросы о предоставлении информации и документов, касающихся операций по Счету/Счетам Клиента.
2. **Общие условия обмена Электронными документами**

Стороны подтверждают, что:

* 1. способы защиты информации и Криптографические средства, используемые в Системе «iBank» при передаче ЭД, достаточны для защиты информации, для подтверждения авторства и подлинности документов, и обязуются выполнять режим обеспечения безопасности, установленный *Регламентом обеспечения информационной безопасности в системах дистанционного банковского обслуживания ООО «ЗЕМКОМБАНК»*, размещается на сайте ООО «ЗЕМКОМБАНК» К исполнению документы принимаются только после их Аутентификации в соответствии с разделом 6 настоящего Договора;
  2. Банк обеспечивает:

- защиту Электронных сообщений от искажения, фальсификации, переадресации, несанкционированного ознакомления и (или) уничтожения, ложной авторизации.

- контроль (мониторинг) соблюдения установленной технологии подготовки, обработки, передачи и хранения Электронных сообщений и ЭД и защищаемой информации на объектах информационной инфраструктуры;

- Аутентификацию входных Электронных сообщений и ЭД в соответствии с разделом 6 настоящего Договора;

- взаимную (двустороннюю) Аутентификацию участников обмена Электронными сообщениями и ЭД;

- восстановление информации об остатках денежных средств на Счете/Счетах, информации об остатках электронных денежных средств в случае умышленного (случайного) разрушения (искажения) или выхода из строя средств вычислительной техники;

- сверку выходных Электронных сообщений с соответствующими входными и обработанными Электронными сообщениями при осуществлении расчетов в платежной системе;

- выявление фальсифицированных Электронных сообщений, в том числе имитацию третьими лицами действий клиентов при использовании электронных средств платежа, и осуществление операций, связанных с осуществлением переводов денежных средств, злоумышленником от имени авторизованного Клиента (подмена авторизованного Клиента) после выполнения процедуры авторизации.

* 1. в Системе «iBank» используется ЭП, в связи с чем, Стороны признают, что получение документа, подписанного ЭП Стороны при соблюдении условий раздела 7 Договора, юридически эквивалентно получению документа на бумажном носителе, подписанного собственноручными подписями уполномоченных лиц и оттиском печати (при наличии) Стороны, подписавшей ЭД. Проверка ЭП в Системе «iBank» осуществляется в соответствии с разделами 6 и 7 настоящего Договора. Обязательства, предусмотренные настоящим пунктом, действительны при условии, что Ключ электронной подписи, ЭП, Сертификат Стороны созданы с использованием технологии с использованием СКЗИ Крипто-Ком (сертифицирован ФСБ России);
  2. хранение Ключа электронной подписи допускается только на ключевом носителе, сертифицированном ФСБ. Банк передает Клиенту необходимое количество ключевых носителей по акту приема-передачи;
  3. созданный в единственном экземпляре в рамках настоящего Договора Ключ электронной подписи Клиента уникален, создание дубликата Ключа электронной подписи возможно только Клиентом или при нарушении Клиентом условий хранения и/или использования Ключа Электронной подписи, предусмотренных настоящим Договором;
  4. Каждая сторона несет ответственность за сохранение в тайне своих Ключей электронной подписи, за правильность заполнения и оформления ЭД и за действия своего персонала при работе с Системой «iBank» в рамках исполнения обязательств по настоящему Договору.
  5. при возникновении конфликтных ситуаций и споров, связанных с формированием, доставкой, получением, подтверждением получения ЭД, а также использованием в данных документах ЭП, данные конфликтные ситуации разрешаются в порядке в соответствии с законодательством РФ.

1. **Порядок подключения Клиента к Системе «iBank»**
   1. В соответствии с настоящим Договором и на основании заявления Клиента на доступ к Системе «iBank» ***(Приложение № 1 к настоящему Договору)*,** Банк предоставляет доступ в Систему «iBank» после заключения с Клиентом договора банковского (расчетного счета) с правом распоряжаться денежными средствами, находящимися на Счете, используя ЭП.
   2. Клиент для работы в Системе «iBank» должен обеспечить наличие технического, программного обеспечения, оборудования и операционных систем, удовлетворяющих требованиям Банка в соответствии с настоящим Договором.
   3. Ключевые носители ТОКЕНы клиент получает при подписании настоящего Договора и акта приема-передачи к настоящему Договору **(*Приложение № 2 к настоящему Договору).***
   4. Изготовление Ключей электронной подписи Сертификата, осуществляется Клиентом самостоятельно посредством Сервиса банка по адресу <https://dbo-zemcombank.ru>.
   5. Подключение Клиента к Системе «iBank» производится Банком на основании настоящего Договора:

- подключение осуществляется в течение 3 (Трех) рабочих дней с момента предоставления Клиентом в Банк подписанных актов приема-передачи *(Приложение № 2 к настоящему Договору)* и Сертификатов ключей выпущенных на лиц, наделенных правом распоряжения денежными средствами, находящимися на Счете/Счетах, используя ЭП, согласно выбранным Клиентом сочетаниям подписей, а также всех необходимых для подключения Системы «iBank» документов.[[1]](#footnote-1)

* срок действия Сертификата составляет один календарный год с даты начала действия Сертификата. Сертификат действует в пределах срока должностных полномочий Владельца Сертификата ключа, а в случае их прекращения (без предоставления документов о продлении) автоматически отключается. Продление срока действия Сертификата на новый срок оформляется обязательной сменой Ключа электронной подписи не позднее 15 календарных дней до момента окончания срока действия Сертификата с обязательным предоставлением Клиентом в Банк подписанных актов приема-передачи и Сертификатов ключей.
  1. Настоящим, Клиент подтверждает, что до заключения настоящего Договора Клиент ознакомлен с порядком получения/продления Сертификатов ключей электронной подписи с условиями использования Системы «iBank», включая информацию о мерах безопасного использования Системы «iBank», о любых ограничениях способов и мест использования, случаях повышенного риска использования Системы «iBank» согласно Признакам осуществления перевода денежных средств без согласия клиента.
  2. Доступ Клиента в Систему «iBank» осуществляется через ссылку <https://dbo-zemcombank.ru>.
  3. Клиент должен предоставить в Банк на всех заявленных Владельцев Сертификатов (уполномоченных лиц) все необходимые документы, сведения позволяющие провести идентификацию и установить полномочия указанных лиц.
  4. Для целей обеспечения Сторонами электронного обмена документами в Системе «iBank» по Договору Клиент должен обеспечить создание Сертификатов на уполномоченных лиц Клиента, указанных в карточке с образцами подписей и оттиска печати, предоставленной Банку.
  5. Все заявленные Клиентом Владельцы Сертификатов должны предоставить в Банк в письменном виде оригиналы соответствующих актов приема-передачи и Сертификатов ключей, подписанные Владельцами Сертификатов.
  6. По завершении Клиентом и Владельцами Сертификатов всех необходимых действий, оформления должным образом и предоставления в Банк всех необходимых документов, оплаты услуг Банка (согласно Тарифам) Банк и Клиент при поддержке и консультационной помощи Банка производят подключение Клиента к Системе «iBank».

1. **Аутентификация Клиента при обмене ЭД**
   1. Определение лица, подписавшего ЭД ЭП, производится на основе сведений, указанных Клиентом, соответствия введенных Аутентификационных данных, а также с учетом примененного Клиентом СКЗИ, Ключа электронной подписи, Ключа проверки электронной подписи и ТОКЕНа. Стороны соглашаются, что указанный способ определения Клиента, создавшего и подписавшего ЭД, является достаточным для цели достоверной Аутентификации Клиента и исполнения Договора, а также придания ЭД юридической силы.
   2. Стороны признают и соглашаются, что для создания ЭП и проверки ЭП в Системе «iBank» Стороны используют СКЗИ. В качестве СКЗИ в системе будут использоваться СКЗИ, реализация которых имеет сертификат ФСБ и, в том числе, соответствует требованиям Федерального закона от 06.04.2011 г. № 63-ФЗ «Об электронной подписи». Данные СКЗИ являются достаточными для подтверждения подлинности ЭП в ЭД и защиты информации ЭД от искажений в Системе.
   3. Стороны признают и соглашаются, что, в соответствии с договором, заключенным между Банком и клиентом:
      1. Ключ электронной подписи Клиента уникален;
      2. Сертификат Клиента позволяет достоверно установить, что ЭД исходит от Клиента, ЭП Клиента (Владельца Сертификата) которого содержится в ЭД, и что ЭД является подлинным.
      3. Порядок формирования и возможности ЭП применяемых Сторонами в системе, дает Сторонам право причислять их к виду УНЭП.
   4. Проверка ЭП осуществляется с использованием программно-технических и иных средств автоматически Средствами ЭП в Системе. В случае положительного результата проверки ЭП – ЭД считается подписанным, а правовые последствия для соответствующего ЭД – наступившими. Осуществляется присоединение полученной ЭП к ЭД и его хранение в неизменном виде. В случае отрицательного результата проверки ЭП Банк отказывает Клиенту в приеме ЭД. ЭД без ЭП или имеющий формат, не отвечающий установленным правилам, в качестве ЭД в соответствии с настоящим Договором не рассматривается.
   5. Стороны признают и соглашаются, что при любом создании ЭП со стороны Клиента и Банка Средствами ЭП и программно-аппаратными средствами Системы «iBank», с которыми они непосредственно функционируют, выполняются все требования, предусмотренные законодательством к Средствам ЭП:
      1. представление лицу, подписывающему ЭД, содержания информации ЭД, которую оно подписывает;
      2. создание ЭП производится только после подтверждения уполномоченным лицом (Владельцем Сертификата), подписывающим ЭД, операции по созданию ЭП;
      3. представление Клиенту и/или уполномоченному лицу, подписавшему ЭД, информации, что ЭП создана, с указанием на лицо, с использованием ключа ЭП, которым подписаны ЭД;
      4. представление информации о внесении изменений в подписанный ЭП электронный документ;
      5. Проверка ЭП осуществляется автоматически Средствами ЭП в Системе с отображением статуса проверки ЭП.
2. **Порядок электронного документооборота**
   1. Банк обязан исполнять Распоряжения Клиента при условии соответствия этих документов требованиям законодательства РФ, договора банковского (расчетного) счета, форматам, установленным Системой «iBank», наличия корректной ЭП с положительным результатом Проверки ЭП, наличии денежных средств на счете.
   2. При приеме от Клиента Распоряжения Банк осуществляет следующие действия:

-удостоверение права использования Системы «iBank» посредством Проверки ЭП,

-контроль целостности Распоряжения посредством проверки неизменности реквизитов Распоряжения,

-структурный контроль посредством проверки установленных реквизитов и максимального количества символов в реквизитах Распоряжения,

-контроль значений реквизитов Распоряжения посредством проверки значений реквизитов Распоряжения, их допустимости и соответствия,

-контроль достаточности денежных средств.

* 1. При положительном результате процедур приема к исполнению Распоряжения в электронном виде Банк принимает Распоряжение к исполнению и направляет Клиенту уведомление в электронном виде о приеме Распоряжения к исполнению с указанием информации, позволяющей Клиенту идентифицировать Распоряжение и дату приема его к исполнению, и установлением статуса документа ЭД в Системе «iBank». При возникновении разногласий в правильности указания времени приема ЭД Клиента в Системе «iBank», Стороны признают, что временем приема ЭД Клиента является текущее время по системным часам аппаратных средств Банка.

В том случае, если в Системе «iBank» отсутствует техническая возможность установления соответствующего статуса ЭД, прием ЭД в Системе «iBank» подтверждается Банком в виде направления Клиенту в Системе «iBank» соответствующего дополнительного Электронного сообщения.

Исполнение Распоряжений Клиента осуществляется Банком не позднее рабочего дня, следующего за днем поступления в Банк данного Распоряжения.

* 1. При отрицательном результате процедур приема к исполнению Распоряжения в электронном виде Банк не принимает Распоряжение к исполнению и направляет Клиенту уведомление в электронном виде об аннулировании Распоряжения с указанием информации, позволяющей Клиенту идентифицировать аннулируемое Распоряжение, дату его аннулирования, а также причину аннулирования. Уведомление в электронном виде направляется в порядке, установленном Банком, не позднее рабочего дня, следующего за днем поступления в Банк Распоряжения.
  2. При выявлении Банком операции, соответствующей признакам осуществления перевода денежных средств без согласия Клиента, Банк до осуществления списания денежных средств со Счета Клиента приостанавливает на срок не более двух рабочих дней исполнение Распоряжения, соответствующей признакам осуществления перевода денежных средств без согласия Клиента. Банк вправе применять сервисы аналитики рисков, включая антифрод-решения, которые могут приводить к приостановке проведения операций Клиента до момента их подтверждения Клиентом / иными Уполномоченными лицами, при этом Клиент не имеет возражений против использования Банком. После приостановления исполнения Распоряжения Банк информирует Клиента о совершении приостановления исполнения Распоряжения, о рекомендациях по снижению рисков повторного осуществления перевода денежных средств без согласия Клиента и незамедлительно запрашивает у Клиента подтверждение возобновления исполнения Распоряжения.

При получении от Клиента подтверждения возобновления исполнения Распоряжения, Банк незамедлительно возобновляет исполнение Распоряжения. При уведомлении Клиента и неполучении от Клиента указанного подтверждения Банк возобновляет исполнение Распоряжения по истечении 2 (двух) рабочих дней после дня приостановления исполнения Распоряжения.

* 1. Клиент может направлять ЭД по Системе «iBank» круглосуточно.
  2. Прием и исполнение Банком ЭД осуществляется в течение установленного в Банке операционного дня, в соответствии с договором банковского (расчетного) счета. ЭД, направленный в Банк после завершения операционного дня, официально установленного Банком, считается принятым к исполнению Банком на следующий операционный день.
  3. Клиент обязуется предоставить Банку по первому обоснованному требованию документы на бумажном носителе, принятые от него по Системе «iBank» и подписанные его ЭП. При этом, указанные документы должны быть заверены печатью (при наличии) и подписями уполномоченных лиц Клиента, определенными в соответствии с карточкой с образцами подписей и оттиска печати.
  4. Банк уведомляет Клиента по факту совершения каждой операции с использованием Системы «iBank», по факту приема ЭД посредством данной Системы «iBank» путем изменения состояния обработки Распоряжения и иного ЭД, отражаемого в Системе «iBank» в разделе «Состояние».
  5. Обязанность Банка по уведомлению Клиента об операциях, совершенных с использованием Системы «iBank», считается исполненной, а уведомление считается полученным Клиентом в день направления Банком уведомления посредством Системы «iBank».
  6. Банк фиксирует направленные Клиенту и полученные от Клиента уведомления, а также хранит соответствующую информацию в электронном виде не менее пяти лет.

1. **Права и обязанности Сторон**
   1. **Клиент вправе:**
      1. Направлять в виде ЭД Распоряжения для осуществления расчетных операций по Счету.
      2. Осуществлять прием информации, данных и ЭД по Счету.
      3. Осуществлять прием/передачу иных ЭД и приложений к ним, определенных заключенными Сторонами любого вида/типа договорами и/или соглашениями.
      4. Получать информацию (в виде выписок) о движении денежных средств по его Счету, открытому в Банке, с помощью Системы «iBank».
      5. В течение всего срока действия Договора обращаться в Банк за получением бесплатных консультаций, связанных с эксплуатаций Системы «iBank».
      6. В течение срока действия Договора в любое время прекратить и/или временно приостановить передачу ЭД в Системе, направив соответствующее заявление. Такое заявление должно быть предоставлено Клиентом в Банк в письменной форме, подписано уполномоченными лицами Клиента и заверено печатью Клиента.
      7. Клиент и/или уполномоченное лицо Клиента, являющееся Владельцем Сертификата в течение срока действия Договора вправе инициировать замену Ключа электронной подписи в любой момент до истечения срока его действия. Соответствующее письменное уведомление должно быть направлено в Банк Владельцем Сертификата.
      8. Клиент имеет право устанавливать ограничения:

- на максимальную сумму одной операции;

- на максимальную сумму операции за определенный период времени *(Приложение № 3 к настоящему Договору)*.

В случае отказа Клиента на указанные ограничения Приложение № 3 к настоящему Договору не заполняется.

* 1. **Клиент обязан:**
     1. В случае компрометации/утраты Ключа электронной подписи, иных обстоятельств утраты возможности использования Системы «iBank», а также в случае проведения операции без согласия Клиента:
  + немедленно, но не позднее дня, следующего за днем получения от Банка уведомления о совершенной операции в порядке п.6.3 настоящего Договора, уведомить Банк о такой компрометации (инциденте), обратиться в Банк, но не позднее 2-х рабочих дней**,** с письменным заявлением на блокировку доступа к Системе «iBank», составленного по форме **Приложения №1** к настоящему Договору.
  + не использовать ключ электронной подписи при наличии оснований полагать, что конфиденциальность данного ключа нарушена;

Под компрометацией понимается:

* + утрата ключевых носителей Ключа электронной подписи (в том числе, с последующим их обнаружением);
  + обнаружение факта использования Системы «iBank» без согласия Клиента;
  + увольнение сотрудников – Владельцев Сертификата, имевших доступ к Ключам электронной подписи;
  + утрата ключей от сейфа, хранилища в момент нахождения в нем ключевых носителей Ключа электронной подписи;
  + нарушение конфиденциальности Ключа электронной подписи, констатация их Владельцем обстоятельств, или наступление обстоятельств, при которых возможно несанкционированное использование Ключа электронной подписи;
  + утеря/передача мобильного устройства с Зарегистрированным номером неуполномоченным лицам, замена/утеря SIM-карты Зарегистрированного номера;
  + иные обстоятельства, прямо или косвенно свидетельствующие о наличии возможности доступа к Ключу электронной подписи третьих неуполномоченных лиц.
    1. Соблюдать следующие требования по обеспечению информационной безопасности, в т.ч. в целях защиты от ВК клиентского АРМ**:**
* соблюдать правила обеспечения информационной безопасности при работе в Системе «iBank», указанные в разделе 12 настоящего Договора;
* при увольнении или смене лиц, обладающих ЭП, изменении данных, идентифицирующих Клиента, смене Ключей электронной подписи, в иных случаях, прекращающих действие Сертификата, Сертификат подлежит немедленной замене в порядке, предусмотренном Инструкцией по генерации и обновлению Сертификата клиентами ООО «ЗЕМКОМБАНК» размещенной на сайте <https://dbo-zemcombank.ru>. Смена ключей ЭП должна быть произведена немедленно в случае угрозы несанкционированного доступа к Счету/Счетам, программно-аппаратным средствам Клиента, копирования или подозрения в копировании ключей третьими лицами, изменений состава лиц, имеющих доступ к Системе «iBank» (обладающих правом использования Ключа электронной подписи);
* обеспечить хранение материального носителя, содержащего Ключ электронной подписи Клиента, в месте, исключающем доступ неуполномоченных лиц и/или возможность повреждения материального носителя;
* не использовать доступ к Системе «iBank» с гостевых рабочих мест (Интернет-кафе и т.п.), существенно увеличивающих риск хищения и дальнейшего неправомерного использования Ключа электронной подписи и другой аутентификационной информации;
* в целях исключения риска воздействия ВК на клиентский АРМ, действия которого в дальнейшем могут скомпрометировать его Ключи электронной подписи, использовать лицензионное, постоянно обновляемое антивирусное программное обеспечение, проводить регулярное антивирусное сканирование используемых устройств с использованием актуальных антивирусных баз и своевременно устанавливать обновления, выпускаемые разработчиками операционной системы и Интернет-браузера на компьютер, ноутбук или иное аналогичное устройство, которое относится к рабочему месту Клиента, на котором будет осуществляться работа с Системой «iBank»;
* контролировать соблюдение перечисленных выше требований по обеспечению информационной безопасности, а также требований, установленных разделом 12 настоящего Договора;
* Контролировать на регулярной основе (не реже одного раза в день) выписки по счету(ам) и статусы ЭД, направленных в Банк, посредством интерфейса Системы «iBank»;
* регулярно получать из Банка и принимать к обработке электронные служебно-информационные документы.
  1. **Банк вправе**:
     1. Приостановить или прекратить обслуживание Клиента в Системе «iBank» в случаях:

- компрометации Ключа электронной подписи и/или при изменении/прекращении полномочий Владельца Сертификата Ключа проверки электронной подписи,

- непредоставления Клиентом достоверной информации для связи с Клиентом, а в случае ее изменения, непредоставления обновленной информации,

- при обнаружении Банком признаков (фактов) нарушения требований информационной безопасности, установленных Системой «iBank» и Договором,

- по основаниям, предусмотренным Федеральным законом от 07.08.2001 №115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» и иными нормативными актами в области ПОД/ФТ, Правилами внутреннего контроля Банка в целях противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма.

- иных случаях, предусмотренных действующим законодательством РФ, настоящим Договором и договором банковского (расчетного) счета, а также внутренними требованиями Банка.

В таких случаях Клиент имеет право предоставить Распоряжения в рабочее время Банка в виде оригинала на бумажном носителе, подписанного подписями уполномоченных лиц с проставлением печати (при наличии) Клиента в соответствии с карточкой образцов подписей и оттиска печати и предоставления Банку документов, предусмотренных законодательством РФ.

Банк уведомляет Клиента о прекращении/приостановлении обслуживания Клиента по Системе «iBank» с указанием причины не позднее дня прекращения/приостановления одним из следующих способов по усмотрению Банка с фиксацией содержания и факта направления уведомления: указанные в реквизитах настоящего Договора телефон или электронная почта, врученное уполномоченному представителю Клиента при личной встрече письменное уведомление. В случае прекращения полномочий Владельца Сертификата в случае окончания срока действия Сертификата отключение доступа такого лица от Системы «iBank» осуществляется автоматически и не требует дополнительного уведомления со стороны Банка.

* + 1. Банк вправе в одностороннем внесудебном порядке изменять настоящий Договор и действующие Тарифы в соответствии с п. 8.1 настоящего Договора.
  1. **Банк обязан:**
     1. Обеспечить надлежащее функционирование программно-технических средств и иной инфраструктуры, используемой для обслуживания Системы «iBank». Банк не гарантирует, что данная инфраструктура всегда будет функционировать корректно и без остановок. Банк обязуется в разумный срок прилагать необходимые усилия по восстановлению работы инфраструктуры и устранению возникших поломок и аварий. Не являются ненадлежащим исполнением Банком своих обязанностей также кратковременные перерывы в работе программных и технических средств и иной инфраструктуры, необходимые для её обновления и выполнения регламентных работ по обслуживанию.
     2. Должным образом и своевременно предоставлять Клиенту услуги по ДБО с использованием Системы «iBank» по Договору.
     3. Предоставлять Клиенту необходимые рекомендации по работе в Системе «iBank».
     4. При наличии угрозы несанкционированного доступа к Системе «iBank» со стороны третьих лиц приостановить исполнение ЭД и проинформировать об этом Клиента через Систему «iBank» либо иным доступным способом в соответствии с п. 6.5 настоящего Договора.
     5. Информировать клиента о совершении каждой операции с использованием Системы «iBank» путем отображения клиенту соответствующего уведомления в интерфейсе Системы «iBank».
     6. В случае выявления Банком операции, соответствующей признакам осуществления перевода денежных средств без согласия Клиента осуществить действия, предусмотренные п. 6.5 настоящего Договора.
     7. По факту поступления соответствующего письменного уведомления-требования Клиента, приостанавливать (не принимать) в Системе «iBank» ЭД, подписанные ЭП уполномоченных лиц Клиента, а также временно приостанавливать работу с Клиентом в Системе «iBank».
     8. Рассматривать заявления Клиента, в том числе при возникновении споров, связанных с использованием Клиентом Системы «iBank», а также предоставить Клиенту возможность получать информацию о результатах рассмотрения заявлений в течение 30 дней со дня получения таких заявлений.

1. **Стоимость услуги и порядок расчетов**

8.1 Стоимость услуг по подключению к Системе «iBank» и ее использованию, предоставлению технической помощи, изготовлению/ выдаче/ замене Сертификатов, а также иных услуг, связанных с обслуживанием и использованием Системы «iBank», и порядок их оплаты определяются Тарифами Банка, действующими на момент оказания услуг.

В течение всего срока действия Договора Банк вправе в одностороннем порядке вносить изменения в Тарифы, которые вступают в действие с момента утверждения их Банком. Информирование Клиента об изменении Тарифов осуществляется по выбору Банка путем размещения соответствующей информации на сайте Банка и/или посредством направления соответствующей информации по Системе «iBank» за 10 (десять) рабочих дней до даты вступления в силу измененных Тарифов.

8.2. Оплата Клиентом стоимости услуг Банка по настоящему Договору осуществляется посредством списания Банком без дополнительного Распоряжения Клиента (на условиях заранее данного акцепта) в сумме не более стоимости услуг по настоящему Договору со Счета/Счетов Клиента, определенной тарифами Банка.

Для осуществления указанного списания, подписывая настоящий Договор, Клиент предоставляет согласие (заранее данный акцепт) Банку составлять и предъявлять к Счету/ Счетам платежные требования/ инкассовые поручения/ банковские ордера (далее – Расчетные документы) и списывать без дополнительного Распоряжения (согласия/акцепта) Клиента денежные средства c указанного Счета/ Счетов Клиента на их основании.

Заранее данный акцепт Клиента предоставлен по Договору без ограничения по количеству Расчетных документов, выставляемых Банком, в соответствии с условиями Договора. Возможно частичное списание.

8.3. В случае неоплаты Клиентом до 31 числа текущего месяца услуг Банка, Банк имеет право приостановить обслуживание Клиента по Системе «iBank» до урегулирования разногласий между Сторонами, либо расторгнуть настоящий Договор в одностороннем внесудебном порядке, направив Клиенту соответствующее уведомление.

8.4. Использование Системы «iBank» в течение неполного календарного месяца оплачивается Клиентом как за полный календарный месяц использования.

1. **Ответственность Сторон**

9.1. За невыполнение либо ненадлежащее выполнение своих обязательств по Договору Стороны несут ответственность, предусмотренную законодательством РФ.

9.2. Банк не несёт ответственности за ущерб, возникший вследствие неправильного оформления Клиентом ЭД, за срывы и помехи в работе используемой Клиентом линии связи, приводящих к невозможности направления в Банк документов, в случае воздействия на программно-аппаратные комплексы Клиента вредоносных программ, неправомерный доступ третьих лиц к программно-аппаратным комплексам/ мобильному устройству и/или Ключам электронной подписи Клиента, нарушения Клиентом принятых обязательств по настоящему Договору, сбоя в работе информационно-телекоммуникационной сети Интернет, электрических сетей связи, возникшие по независящим от Банка причинам и повлекшие за собой несвоевременное получение или исполнение Распоряжений и иных ЭД Клиента, некорректное формирование ЭД.

9.3. Банк не несет ответственности за исполнение Распоряжений Клиента в случае, если полномочия лиц, уполномоченных распоряжаться денежными средствами с использованием ЭП, были прекращены либо изменены по каким-либо основаниям, но Банк не был об этом своевременно извещен.

9.4. Банк не несёт ответственности в случаях финансовых потерь, понесенных Клиентом в связи с нарушением и (или) ненадлежащим исполнением им требований по защите от ВК клиентских АРМ Системы «iBank».

9.5. Банк не несет ответственности за несвоевременное получение или неполучение Клиентом уведомлений по факту совершения операций с использованием Системы «iBank» по причинам, находящимся вне сферы контроля Банка, в частности:

* + за отсутствие доступа к сети Интернет вследствие ненадлежащих действий Клиента (отключение связи Интернет, ненадлежащей связи Интернет и т.д.), сбои в работе сетей, обеспечивающих связь Интернет, мобильную/сотовую связь, и т.п.;
  + в случае непредставления Клиентом достоверной информации для связи с Клиентом, а в случае ее изменения, непредставления обновленной информации о Зарегистрированном номере, электронного почтового адреса Клиента.

9.6. Банк не несет ответственность за достоверность сведений (в т.ч. Зарегистрированного номера, электронного почтового адреса), представленных Клиентом.

9.7. Банк обязуется принимать меры для предотвращения несанкционированного доступа третьих лиц к информации, передаваемой в Системе, составляющей банковскую тайну, персональные данные представителей Клиента. Любая информация такого рода может быть предоставлена третьим лицам не иначе как в порядке, установленном законодательством РФ.

9.8. Клиент поставлен в известность и в полной мере осознает, что передача конфиденциальной информации в Системе «iBank» влечет риск несанкционированного доступа к такой информации третьих лиц.

1. **Форс-мажор**

10.1. Ни одна из Сторон не будет нести ответственность за полное или частичное неисполнение любого из своих обязательств по настоящему Договору, если неисполнение будет являться следствием таких обстоятельств, как: пожар, наводнение, землетрясение, любые другие стихийные бедствия, войны, военные операции любого характера, блокады, акты государственных органов, а также изменение действующего законодательства и иные ограничения экономического и политического характера.

10.2. Если любое из вышеуказанных обстоятельств непосредственно повлияло на исполнение обязательств в сроки, установленные настоящим Договором, то эти сроки соразмерно отодвигаются на время действия соответствующего форс-мажорного обстоятельства.

10.3. Сторона, для которой возникли условия, при которых исполнение ее обязательств стало невозможным, обязана не позднее 1 (Одного) дня направить другой Стороне уведомление посредством Системы «iBank» и/или в письменной форме о наступлении таких условий и о предполагаемых сроках прекращения форс-мажорных обстоятельств. Факты, изложенные в уведомлении, должны быть подтверждены компетентными органами Российской Федерации. Неуведомление или несвоевременное уведомление лишает Сторону права ссылаться на любое из перечисленных выше обстоятельств, как на основание, освобождающее от ответственности за неисполнение обязательств по настоящему Договору.

1. **Срок действия Договора**

11.1. Настоящий Договор считается заключенным с момента его подписания Сторонами и действует до «31» декабря следующего года включительно. В случае, если ни одна из Сторон не направит другой Стороне заявление (уведомление) о прекращении Договора в письменном виде не позднее, чем за 30 календарных дней до даты окончания срока действия Договора, Договор считается пролонгированным на каждый последующий календарный год. Указанный порядок пролонгации Договора применяется каждый раз перед окончанием срока его действия.

11.2. Банк имеет право в любое время расторгнуть в одностороннем внесудебном порядке Договор, предупредив об этом Клиента письменно за 10 календарных дней до предполагаемой даты расторжения. В случае принятия Банком в течение календарного года двух и более решений об отказе в выполнении распоряжения Клиента в связи с подозрениями, что операция совершается в целях легализации (отмывания) доходов, полученных преступным путем, или финансирования терроризма, а так в иных предусмотренных законом случаях в соответствии с действующим законодательством РФ.

11.3. Договор считается расторгнутым по истечении 30 календарных дней с даты окончания срока действия Сертификата Клиента, если Клиент не обратился в Банк за оформлением нового Сертификата.

11.4. Договор считается расторгнутым в случае закрытия всех Счетов Клиента в Банке с момента закрытия последнего из всех Счетов, при условии отсутствия у Клиента потребности в использовании Системы «iBank» для целей обмена ЭД с Банком в рамках иных договоров, заключенных с Банком, не связанных с открытием и управлением банковскими счетами.

11.5. Клиент имеет право при отсутствии задолженности перед Банком, расторгнуть Договор в одностороннем внесудебном порядке, предупредив об этом Банк письменно за 10 (Десять) календарных дней до предполагаемой даты расторжения.

11.6. Банк вправе в одностороннем порядке вносить изменения в условия настоящего Договора в случае внесения изменений в действующее законодательство РФ, путем подписания дополнительного соглашения к настоящему Договору сторонами.

11.7. С момента заключения Договора все предыдущие договоренности и соглашения между Сторонами, касающиеся предмета настоящего Договора, теряют силу.

1. **Правила обеспечения информационной безопасности при работе в Системе «iBank»**

12.1. Ответственность за безопасное хранение и использование Ключа электронной подписи лежит на Клиенте.

В целях минимизации рисков мошенничества и предотвращения атак ВК при работе с Системой «Банк-Клиент, Банк рекомендует Клиенту выполнять следующие действия и правила, включая требования ***Приложения № 4*** *к настоящему Договору:*

12.2.1. Для обеспечения информационной безопасности Ключа электронной подписи обязан:

12.2.1.1. по завершении работы с Системой «iBank» не оставлять ТОКЕН без присмотра;

12.2.1.2. обеспечить хранение ТОКЕНа в месте, исключающем доступ к носителю третьих лиц (в сейфе, личной запираемой ячейке и т. п.), не оставлять без присмотра и в легкодоступных местах;

12.2.1.3. исключить передачу Ключа электронной подписи или его копий третьим лицам, а также передачу по публичным сетям (например, в информационно-телекоммуникационную сеть «Интернет»);

12.2.1.4. исключить хранение Ключа электронной подписи на жестком диске, в сетевых каталогах и прочих общедоступных ресурсах;

12.2.1.5. при смене уполномоченного представителя Клиента, отвечающего за формирование и проведение Распоряжений с использованием Системы «iBank», сменить криптографические ключи;

12.2.2. Для обеспечения безопасности устройства, с которого осуществляется работа с Системой «iBank», Клиент обязан:

12.2.2.1. использовать только лицензионные общее и прикладное программное обеспечение, средства антивирусной защиты;

12.2.2.2. обеспечить на устройстве непрерывное функционирование средств антивирусной защиты и межсетевого экранирования (брандмауэр, firewall);

12.2.2.3. ограничить права пользователя на внесение изменений в настройку операционной системы и установку каких-либо программ на устройство. При использовании для работы в Системе «iBank» нескольких компьютеров, желательно поместить их в отдельный сегмент сети;

12.2.2.4. обеспечить своевременное обновление операционной системы, антивирусного программного обеспечения, а также антивирусных баз данных;

12.2.2.5. осуществлять автоматическую периодическую (не реже одного раза в неделю) проверку устройства на наличие вирусов, при обнаружении вирусов, шпионских программ и т. п. немедленно их удалять;

12.2.2.6. установить парольную политику на ТОКЕН, средствах доступа к Системе «iBank» в соответствии с требованиями Приложения №3 к настоящему Договору;

12.2.2.7. соблюдать правила информационной безопасности при работе в информационно- телекоммуникационной сети «Интернет» (не посещать подозрительные сайты, не устанавливать программы из «недоверенных» источников, не открывать письма и вложения от неизвестных отправителей и пр.).

12.2.3. Для обеспечения информационной безопасности при работе в Системе «iBank» Клиент обязан:

12.2.3.1. использовать вход в систему только с <https://dbo-zemcombank.ru>, обращать внимание на правильность адреса (ссылки). При выявленном несоответствии – немедленно прекратить проведение операций и проинформировать Банк;

12.2.3.2. ежедневно контролировать состояние Счета(ов) (путем просмотра выписки). При выявлении расхождений – немедленно прекратить проведение операций и проинформировать Банк;

12.2.3.3. обращать внимание на дату и время последних входов в Систему «iBank» (данные фиксируются на первой странице после входа в Систему «iBank», а также в специальном разделе «Безопасность» - «Журнал сеансов работы»);

12.2.4. Признаки нарушений режима безопасности:

12.2.4.1. хищение, утеря (безвозвратная или с последующим обнаружением), повреждение ТОКЕНа;

12.2.4.2. увольнение сотрудников, имевших доступ к Ключам электронной подписи, изменения функциональных обязанностей сотрудника Клиента, имевшего доступ к распоряжению Счетом;

12.2.4.3. возникновение подозрений на утечку информации или ее несанкционированное изменение в Системе «iBank»;

12.2.4.4. подозрение на несанкционированный доступ третьих лиц к Счетам, программно-аппаратным средствам Клиента, Ключу электронной подписи,

несанкционированные операции по банковскому Счету Клиента с использованием Системы «iBank»;

12.2.4.5. нарушение целостности замков, печатей (при наличии) на сейфе, где хранится ТОКЕН в момент нахождения в нем ТОКЕНа.

12.2.5. Обязательная замена Ключа электронной подписи:

12.2.5.1. истек срок действия Ключа электронной подписи;

12.2.5.2. произошла компрометация Ключа электронной подписи.

12.3. Настоящим Клиент подтверждает, что до присоединения к настоящим Условиям и заключения Договора Клиент ознакомлен и полностью согласен с тем, что до момента блокировки Ключа электронной подписи Банк не несет ответственности за платежи, совершенные с использованием этого Ключа электронной подписи, даже в случае его компрометации, в т.ч. при воздействии на клиентское АРМ вредоносных кодов.

12.4. В случае возникновения подозрения на компрометацию Ключа электронной подписи, Клиенту необходимо незамедлительно обратиться в Банк по телефону +7(863)280-00-64 и инициировать процедуру смены всех потенциально скомпрометированных Ключей электронной подписи или блокировку Системы «iBank».

1. **Дополнительные условия**

13.1. Во всем, что не урегулировано условиями настоящего Договора, Стороны руководствуются:

13.2. Инструкцией по генерации и обновлению Сертификата Клиентами Банка, размещенной на сайте <https://dbo-zemcombank.ru/>.

13.3. Банк вправе в одностороннем внесудебном порядке изменять условия настоящего Договора в случае внесения изменений в указанные в п.14.1 правила, предварительно письменно уведомив об этом Клиента за 10 (Десять) рабочих дней до даты вступления в силу таких изменений.

13.4. В случае замены Банком СКЗИ, привлекаемой для функционирования Системы «iBank» Банк обязуется уведомить Клиента, путем направления информации по системе «iBank».

13.5. Стороны признают, что настоящий Договор, иные относящиеся к нему документы, а также вся устная или письменная информация, предоставленная какой-либо Стороне другой Стороной, являются конфиденциальной информацией, и ни одна из Сторон не может устно или письменно разглашать такую конфиденциальную информацию какому-либо третьему лицу без письменного разрешения другой Стороны в течение всего срока действия Договора, а также в течение 5 (пяти) лет с даты истечения срока его действия. Положения п.13.4 не распространяются на случаи раскрытия информации предусмотренные в действующем законодательстве РФ.

13.6. Настоящий Договор составлен в 2 (Двух) экземплярах, по одному для каждой из Сторон, имеющих одинаковую юридическую силу.

**14. Адреса и реквизиты Сторон**

**Банк Клиент**

|  |  |
| --- | --- |
| **ОБЩЕСТВО С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ "ЗЕМЕЛЬНЫЙ КОММЕРЧЕСКИЙ БАНК"** 344010, г. Ростов-на-Дону, ул. Малюгиной,233б  тел./факс (863) 28 00 064  БИК 046015078, к/с 30101810760150000078 в Отделении Ростов-на-Дону  ИНН 6132001298  КПП 616301001  ОГРН 1026100001982 | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  р/счет \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  в \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  БИК \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  ИНН/КПП \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  ОГРН \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| **Уполномоченное лицо** (указатьдолжность)  **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ /\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/**  м.п. | **Уполномоченное лицо** (указатьдолжность)  **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/**  м.п. |

**Приложение № 1 к Договору**

**№\_\_\_ от «\_\_\_» \_\_\_\_\_\_\_\_\_\_\_2022 г**

**дистанционного банковского обслуживания**

**юридических лиц по Системе «iBank»**

**Заявление**

**на доступ/ блокировку доступа к системе «iBank»/уведомление**

Организация\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Наименование компании

в лице \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, действующего на основании\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ поручает Банку произвести нижеуказанные действия:

**Предоставление доступа:**

Предоставить доступ к Системе «iBank» нижеуказанным лицам:

|  |  |  |
| --- | --- | --- |
| **Владелец Сертификата ключа проверки электронной подписи** | ***ФИО*** | |
| **Документ, удостоверяющий личность:** | ***Вид, серия, номер*** | |
| **Выдан:** | ***Орган, выдавший документ, удостоверяющий личность, дата выдачи*** | |
| **Зарегистрированный номер мобильного телефона** | +7\_\_ \_\_ \_\_ \_\_ \_\_ \_\_ \_\_ \_\_ \_\_ \_\_ | |
| **Электронная почта (E-mail):** |  | |
| * + 1. **По счету:** | | |
| Номер счета Клиента: | С правом подписи |  |
| №\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |  |
| №\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |  |
| * + 1. **Перечень подключаемых модулей:**   Рублевые документы  Валютные документы  Постоянные поручения  Гарантии  Валютный контроль  Депозиты  Кредиты  Письма | | |

***При необходимости выдачи Ключей электронной подписи нескольким сотрудникам Клиента, дополнить следующим аналогичным разделом***

***Распоряжение Клиента по Системе «iBank» принимается Банком только, если оно подписано[[2]](#footnote-2)***

***(далее выбрать и заполнить нужное):***

|  |
| --- |
| ***Вариант 1 – «Одна любая подпись».*** Одной подписью любого из следующих Владельцев Сертификата ключа проверки электронной подписи / Владельцев Логина и Пароля с правом распоряжения денежными средствами на счете:  1.\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  2.\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  ***Вариант 2 – «Две подписи».*** Двумя различными подписями любых следующих Владельцев Сертификата ключа проверки электронной подписи / Владельцев Логина и Пароля с правом распоряжения денежными средствами на счете:  1.\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  2.\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
|  |

**Уведомление Банка об утрате электронного средства платежа и/или использовании Системы «iBank» без согласия Клиента**:

На основании п.11 ст.9 Федерального закона от 27.06.2011 г. №161-ФЗ «О национальной платежной системе» и п.7.2. Договора дистанционного банковского обслуживания юридических лиц и обмена электронными документами с юридическими лицами в Системе «iBank» №\_\_\_ от «\_\_» \_\_\_\_\_ \_\_\_ г. уведомляю об обнаружении факта использования Системы «iBank» без моего согласия.

**Блокировка доступа**: Заблокировать доступ к Системе «iBank» следующим Владельцам Сертификата ключа проверки электронной подписи / Владельцев Логина и Пароля.

Руководитель(указать должность)\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ /\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/

МП

**Приложение № 2 к Договору**

**№\_\_\_ от «\_\_\_» \_\_\_\_\_\_\_\_\_\_\_20\_\_г**

**дистанционного банковского обслуживания**

**юридических лиц по Системе «iBank»**

Типовая форма Акта приема-передачи ключевых носителей, программного обеспечения и средств криптографической защиты информации»

(подписывается в обязательном порядке при передаче Клиенту ключевых носителей, ПО и СКЗИ/ при изменении списка уполномоченных лиц Клиента в случае выдачи новых токенов)

**Акт приема-передачи**

**ключевых носителей, программного обеспечения и средств криптографической защиты информации**

г. Ростов-на-Дону «\_\_» \_\_\_\_\_\_\_\_\_\_\_ 20\_\_г.

В соответствии с Договором № \_\_\_\_\_\_\_\_\_\_\_\_\_\_ от \_\_ .\_\_.20\_\_г, ООО «ЗЕМКОМБАНК», Генеральная лицензия Банка России №574, именуемое в дальнейшем «БАНК», в лице \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, действующего на основании \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, и \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, именуемое в дальнейшем «КЛИЕНТ», в лице \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, действующего на основании \_\_\_\_\_\_\_\_\_\_\_, именуемые далее «**Стороны**», составили настоящий Акт о том, что Банк передал, а Клиент принял в рамках оказания услуг, связанных с эксплуатацией Системы «iBank»:

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | **Программное обеспечение Клиентской части Системы «iBank»:** | | | | | | | | | |
| **При подключении Системы «iBank»** | | | | | | | | | | |
| с интернет ресурса [https://dbo-zemcombank.ru](https://bifit.geprobank.ru/index.html) | | | | | | | | | | |
| **2** | **Средства криптографической защиты информации (СКЗИ) и носители:** | | | | | | | | | |
| № п/п | Наименование СКЗИ | | Идентификационный номер СКЗИ | | Наименование и учетный номер носителя | | | ФИО владельца (Уполномоченное /Визирующее лицо Клиента) | | ФИО и подпись получателя СКЗИ |
|  | MS\_KEY K - АНГАРА | |  | |  | | |  | |  |
| **3** | **Токены** | | | | | | | | | |
| * Электронный ключ USB-токен \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | | | | | | | | | | |
| № п/п | Наименование носителя | | Учетный номер носителя | | | ФИО владельца (Уполномоченное/ Визирующее лицо Клиента) | | | | ФИО и подпись получателя |
|  | MS\_KEY K - АНГАРА | |  | | |  | | | |  |
| * Генератор одноразовых кодов \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, в кол-ве \_\_\_\_\_\_ шт. | | | | | | | | | | |
| № п/п | | Наименование носителя | | Учетный номер носителя | | | ФИО владельца (Уполномоченное/ Визирующее лицо Клиента) | | ФИО и подпись получателя | |

Достоверность сведений подтверждаем.

Настоящий Акт составлен в 2-х экземплярах по одному для каждой из сторон и является неотъемлемой частью Договора.

**ПОДПИСИ СТОРОН**

|  |  |
| --- | --- |
| **БАНК** | **КЛИЕНТ** |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| М.П. | М.П. |

При получении программного обеспечения, СКЗИ и ключевых носителей не Уполномоченными лицами, дополнительно предоставляется Доверенность на получателя по форме, установленной ООО «ЗЕМКОМБАНК»

**Приложение № 3 к Договору**

**№\_\_\_ от «\_\_\_» \_\_\_\_\_\_\_\_\_\_\_20\_\_г**

**дистанционного банковского обслуживания**

**юридических лиц по Системе «iBank»**

|  |  |
| --- | --- |
| Председателю Правления | |
| ООО «ЗЕМКОМБАНК» | |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  . | |
| От \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | |
| «\_\_\_» \_\_\_\_\_\_\_\_\_\_\_ 20\_\_\_ г. | (Наименование клиента/ ФИО руководителя) |

Заявление

Прошу установить лимиты при проведении операций с использованием системы дистанционного банковского обслуживания по договору № \_\_\_ от «\_\_\_» \_\_\_\_\_\_\_20\_\_г. по счету №\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,

|  |  |  |
| --- | --- | --- |
| Лимит в рублях | 1 день | 30 дней |
| Максимальная сумма одной операции по счету |  |  |
| Максимальная общая сумма операций по счету |  |  |

|  |  |  |
| --- | --- | --- |
| Клиент: | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/  (ФИО)  М.П. | \_\_\_\_\_\_\_\_\_\_  (подпись) |

**Приложение № 4 к Договору**

**№\_\_\_ от «\_\_\_» \_\_\_\_\_\_\_\_\_\_\_20\_\_г**

**дистанционного банковского обслуживания**

**юридических лиц по Системе «iBank»**

**Требования к программному обеспечению и рекомендации для работы в Системе**

1. Для работы в Системе необходимо:
   1. Персональный компьютер или ноутбук с установленной операционной системой Microsoft Windows не ниже версии 10 с установленным антивирусным программным обеспечением и программным обеспечением, реализующим защиту от несанкционированного доступа (межсетевой экран). Всё программное обеспечение должно быть с установленными актуальными обновлениями.
   2. Подключение к сети Интернет.
   3. Установленный межсетевой экран не должен запрещать работу браузеров по порту 443.
   4. Поддерживаемые операционные системы: Microsoft Windows: 7 (x86/x64), 8 (x86/x64), 8.1 (x86/x64), 10 (x86/x64) и выше; Apple Mac OS X: 10.7 и выше; Ubuntu и прочие deb-дистрибутивы (последние версии x64). Web-браузер с поддержкой плагина BIFIT Signer для использования электронной подписи с применением аппаратных устройств. Поддержка плагина обеспечена в браузерах: Internet Explorer версия 11; Edge; Chrome (последняя версия); Яндекс-браузер (последняя версия); Firefox (последняя версия); Opera (последняя версия); Safari. Персональное аппаратное USB-устройство с возможностью использования цифровой ЭП или съемный USB-накопитель (при использовании файловых ключей). Аппаратное устройство предназначено для генерации ключей ЭП внутри самого устройства и обеспечения их защищенного неизвлекаемого хранения. Формирование ЭП под электронным документом происходит внутри самого устройства. Сервис поддерживает работу с аппаратными устройствами: MAC-токен BIFIT; Рутокен ЭЦП 2.0; MS\_KEY K – АНГАРА Исп.8.1.1.
   5. . Рекомендации Клиенту, Владельцам Сертификатов по обеспечению информационной безопасности при работе в Системе:
   6. . По завершении работы с Системой не оставлять Ключевой носитель подключенным к компьютеру.

. Обеспечить хранение Ключевого носителя в месте, исключающем доступ к нему третьих лиц (сейф, личная запираемая ячейка и т.п.) и не оставлять его в легко доступных местах.

* 1. . Обеспечить на персональном компьютере непрерывное функционирование актуального антивирусного программного обеспечения и программного обеспечения, реализующего защиту от несанкционированного доступа (межсетевой экран).
  2. . При выходе в Интернет использовать сетевой экран, разрешив доступ только к доверенным ресурсам сети.
  3. . Установить и своевременно обновлять на компьютере антивирусное ПО.
  4. . Обеспечить своевременное обновление операционной системы.
  5. . Антивирусное программное обеспечение должно быть запущено постоянно с момента загрузки персонального компьютера или ноутбука.
  6. . Рекомендуется полная еженедельная проверка персонального компьютера/ноутбука на наличие вирусов, удаление обнаруженного вредоносного программного обеспечения.
  7. . Осуществлять периодическую (не реже одного раза в неделю) проверку персонального компьютера/ноутбука на наличие вредоносных объектов (вирусов, шпионских программ и т.п.), при обнаружении таковых немедленно их удалять. Настроить антивирусное программное обеспечение на обновление баз сигнатур не реже 1 раза в час.
  8. . Соблюдать правила информационной безопасности при работе в Интернете- не посещать подозрительные сайты, не устанавливать программы из непроверенных источников, не открывать письма и вложения от неизвестных отправителей и пр.
  9. . Запретить на межсетевом экране соединение с Интернет по протоколам ftp, smtp. Разрешить соединения smtp только с конкретными почтовыми серверами, на которых зарегистрированы электронные почтовые ящики сотрудников Клиента.
  10. . Не давать разрешения неизвестным программам выходить в Интернет.
  11. . При работе в Интернет не соглашаться на установку каких-либо дополнительных программ, работу в Системе производить с правами локального пользователя компьютера (без локальных административных прав на компьютере).
  12. . Использовать вход в Систему только с сайтов <https://dbo-zemcombank.ru/> и ни при каких обстоятельствах не вводить логин и пароль доступа к Системе на других сайтах.
  13. . Периодически контролировать состояние счета (путем просмотра выписки).
  14. . Обращать внимание на дату и время последних входов в Систему (данные фиксируются на первой странице в Системе после входа в Систему, а также в специальном разделе Системы).
  15. . Установить пароль доступа к ключу ЭП таким образом, чтобы он соответствовал требованиям сложности, а именно, пароль должен состоять не менее чем из 8 символов, состоять из букв в верхнем и нижнем регистрах, цифр и символов. Требования к парольной политике пользователей Системы, а также учетным записям компьютера пользователя Системы:

- минимальная длина пароля: 8 символов,

- максимальный срок действия пароля: 365 дней,

- использование в пароле букв в верхнем и нижнем регистрах, а также цифр,

- максимальное количество последовательных неудачных попыток входа: 6;

- время блокировки учетной записи после превышения количества неудачных попыток входа: от 30 минут;

- автоматическое прерывание сессии пользователя после 15 минут бездействия (с последующим автоматическим запросом на повторную аутентификацию);

- автоматическое блокировка учетных записей, неактивных более 90 дней;

**Запрещено** использовать в качестве пароля или его части общеизвестные сочетания символов (например, «qwerty», «asdfg»), восходящие или нисходящие последовательности (например, «12345», «54321», «abcdef»), персональную информацию (название учетной записи, фамилию, имя, дату рождения и т.п.).

* 1. .Регулярно просматривать сообщения и рекомендации Оператора и Банка, размещаемые в Системе и на сайтах Банка и Оператора в соответствующих разделах, касающихся безопасности, рисков и работы в Системе и в сети Интернет.

1.23..Своевременно уведомлять Банк, Оператора об инцидентах информационной безопасности.

1. Возможные сочетания подписей лиц, наделенных правом подписи, правом распоряжения денежными средствами, находящимися на Счете/Счетах, используя ЭП, необходимых для подписания документов, содержащих Распоряжение Клиента, определяются в соответствии с отдельным заявлением о принятии карточки с образцами подписей и оттиска печати. [↑](#footnote-ref-1)
2. Заполняется при предоставлении доступа Владельцу Сертификата ключа проверки электронной подписи в случае распоряжения денежными средствами на счете с использованием Электронной подписи, более, чем одним уполномоченным лицом [↑](#footnote-ref-2)