

УТВЕРЖДЕН

Приказом № 3 от 15.01.2020 г.

**Договор
дистанционного банковского
обслуживания клиентов – физических лиц
с использованием системы «iBank для жизни»
АО «Тольяттихимбанк»
(в редакции приказа № 108 а от 04.09.2020 г.)**

Тольятти

2020

1. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Авторизация – разрешение Банка на вход в Систему ДБО или проведение Операций после удостоверения права осуществления Клиентом действий в Системе ДБО, в том числе распоряжения денежными средствами.

Автоматизированное рабочее место (АРМ) – совокупность программных и аппаратных средств (компьютер или Мобильное устройство), с которого осуществляется работа Клиента с Системой ДБО.

Аутентификация – выполняемая средствами Системы ДБО процедура установления принадлежности Клиенту указываемого им Логина посредством сопоставления с Долговременным паролем.

Банк – Акционерное общество «Тольяттихимбанк». Место нахождения: 445009, Самарская область, г. Тольятти, улица Горького, дом 96.

Безотзывность – характеристика перевода денежных средств, обозначающая отсутствие или прекращение возможности отзыва распоряжения об осуществлении перевода денежных средств в определенный момент времени. Безотзывность перевода денежных средств наступает с момента списания денежных средств с банковского счета плательщика.

Безусловность – характеристика перевода денежных средств, обозначающая отсутствие условий или выполнение всех условий для осуществления перевода денежных средств в определенный момент времени. Безусловность перевода денежных средств наступает в момент выполнения определенных плательщиком и (или) получателем средств либо иными лицами условий осуществления перевода денежных средств, в том числе осуществления встречного перевода денежных средств в иной валюте, встречной передачи ценных бумаг, представления документов, либо при отсутствии указанных условий.

Браузер – используемое Клиентом для работы с Системой ДБО прикладное программное обеспечение предназначенное для: просмотра веб-сайтов, содержания веб-документов, компьютерных файлов и их каталогов; управления веб-приложениями; запроса веб-страниц, их обработки, вывода и перехода от одной страницы к другой; а также для решения других задач. Разрешенные для использования Клиентом при работе с Системой ДБО наименования браузеров, а также их версии приведены в документации к соответствующим каналам обслуживания (интерфейсам, модулям) Системы ДБО, размещенной на сайте Банка в Сети Интернет по адресу https://ibank.thbank.ru/web_banking.

Вредоносный код (ВК) – компьютерная программа, предназначенная для внедрения в автоматизированные системы, ПО, средства вычислительной техники, телекоммуникационное оборудование приводящего к уничтожению, созданию, копированию, блокированию, модификации и (или) передаче информации (в том числе защищаемой в соответствии с пунктом 2.1 «Положения о требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств» Банка России № 382-П от 09.06.2012.), а также к созданию условий для такого уничтожения, создания, копирования, блокирования, модификации и (или) передачи.

Договор дистанционного банковского обслуживания клиентов – физических лиц с использованием Системы «iBank для жизни» (далее - Договор) – настоящий документ, являющийся одновременно публичным договором и договором присоединения, а также Заявление о присоединении, надлежащим образом заполненное и подписанное Клиентом и Банком и Тарифы и комиссии АО «Тольяттихимбанк» (далее – Тарифы).

Договор банковского карточного счета – совокупность документов: Правила заключения договора банковского карточного счета, предоставления и использования банковской карты АО «Тольяттихимбанк», Тариф, каждое Заявление, надлежащим образом заполненное и подписанное Клиентом и Банком, на основании которого Клиенту выдана Платежная карта.

Защита информации – комплекс организационно-технических мероприятий, проводимых Банком с целью предотвращения утечки, хищения, утраты, несанкционированного уничтожения, изменения, модификации (подделки), несанкционированного копирования, блокирования информации.

Защита от ВК – организованная деятельность по защите автоматизированных систем, ПО, средств вычислительной техники, телекоммуникационного оборудования от атак ВК и устранению их последствий.

Защитное ПО – специализированное программное обеспечение, используемое для осуществления защиты от ВК.

Заявление о присоединении к Договору дистанционного банковского обслуживания клиентов – физических лиц с использованием Системы «iBank для жизни» АО «Тольяттихимбанк» (далее – Заявление о присоединении) – согласие (акцепт) Клиента на предложение (оферту) Банка заключить Договор на изложенных ниже условиях. Заявление о присоединении оформляется на бумажном носителе по установленной Банком форме (Приложение № 1 к настоящему Договору).

Интернет-Банк – канал обслуживания (интерфейс, модуль) Системы ДБО предназначенный для использования Клиентом посредством персональных компьютеров. Особенности использования данного интерфейса

описаны в Руководстве пользователя «Интернет-Банк для частных клиентов», размещенном на сайте Банка в Сети Интернет по адресу https://ibank.thbank.ru/web_banking.

Информационная безопасность – состояние сохранности информации, информационных ресурсов и информационных систем, при котором с требуемой вероятностью обеспечивается защита информации (данных) от утечки, хищения, утраты, несанкционированного уничтожения, искажения, модификации (подделки), копирования, блокирования и т.п., состояние защищенности информации, обрабатываемой средствами вычислительной техники или автоматизированной системы, от внутренних или внешних угроз.

Клиент – физическое лицо, находящееся на обслуживании в Банке, на имя которого на момент заключения настоящего Договора открыт Счет и выпущена основная Платежная карта.

Код доступа – уникальный цифровой код, заданный Клиентом, который известен только Клиенту. Код доступа хранится в зашифрованном виде в секретном хранилище операционной системы Мобильного устройства. Код доступа невозможно восстановить. При утрате или утере Кода доступа необходимо задать его заново.

На устройствах, оснащенных соответствующими датчиками, в качестве Кода доступа может использоваться отпечаток пальца. При этом для обработки информации содержащей сведения об отпечатке пальца используются средства операционной системы Мобильного устройства, а информация об отпечатке пальца не покидает пределов Мобильного устройства. Банком при этом не осуществляется обработка биометрических персональных данных. Поддерживаются технологии идентификации пользователя по отпечатку пальца операционных систем Android и iOS.

Код подтверждения – генерируемая Системой ДБО одноразовая динамическая последовательность цифровых символов (от 4 до 6), которая направляется Клиенту посредством SMS-сообщения на номер мобильного телефона или в сообщении на адрес электронной почты Клиента, указанные в Заявлении на присоединение. Срок действия Кода подтверждения составляет 5 (пять) минут, по истечении указанного срока Код подтверждения становится недействительным. Код подтверждения используется для дополнительной Аутентификации Клиента и для подтверждения Клиентом права доступа в Систему ДБО. Код подтверждения является элементом Многофакторной аутентификации.

Компрометация – факт доступа постороннего лица к защищаемой информации, а также подозрение на него.

Компрометация Средств доступа – событие, в результате которого Средства доступа становятся или могут стать известными или доступными постороннему лицу.

Лимит – максимальная сумма операций, осуществляемых в течение одних суток в Системе ДБО, за исключением переводов между Счетами / Платежными картами Клиента и оплаты услуг торгово-сервисных предприятий через платежную систему «КиберПлат».

Логин – уникальный идентификатор Клиента в Системе ДБО, обеспечивающей в сочетании с Долговременным паролем однозначную Аутентификацию Клиента при каждом его обращении к Системе ДБО.

Многофакторная аутентификация – аутентификация, для осуществления которой используются два и более различных факторов аутентификации (обязательные: Логин, Долговременный пароль; дополнительные: Код подтверждения).

Мобильный телефон – переносное устройство Клиента, предназначенное для оперативной мобильной связи с Клиентом, отправки Банком Клиенту Кодов подтверждения, SMS-уведомлений и иных SMS-сообщений от Системы ДБО.

Мобильное устройство – переносное устройство Клиента, такое как смартфон или планшетный компьютер, используемое для оказания услуг дистанционного банковского обслуживания посредством канала обслуживания «Мобильный Банк».

Мобильное приложение – специализированное программное обеспечение, устанавливаемое Клиентом на его Мобильное устройство с официального ресурса распространения программного обеспечения. Официальными ресурсами являются: для операционной системы Android – магазин приложений Google Play, для операционной системы iOS – магазин приложений App Store. В перечисленных выше магазинах приложений мобильное приложение размещено под названием «ТХБ Online». Разработчиком мобильного приложения является АО «БИФИТ».

Мобильный Банк – канал обслуживания (интерфейс, модуль) Системы ДБО, предназначенный для использования Клиентом посредством Мобильных устройств. Для использования данного модуля требуется установка Мобильного приложения на Мобильное(-ые) устройство(-а) Клиента. Особенности использования данного интерфейса описаны в Руководстве пользователя мобильного приложения «Мобильный Банк для частных клиентов», размещенном на сайте Банка в Сети Интернет по адресу https://ibank.thbank.ru/web_banking.

Окончателность – характеристика перевода денежных средств, обозначающая предоставление денежных средств получателю средств в определенный момент времени. В случае, если плательщик средств и получатель средств

обслуживаются в Банке, Окончательность перевода денежных средств наступает в момент зачисления денежных средств на банковский счет получателя средств или обеспечения получателю средств возможности получения наличных денежных средств. В случае, если плательщика средств и получателя средств обслуживают разные операторы по переводу денежных средств, Окончательность перевода денежных средств наступает в момент зачисления денежных средств на банковский счет оператора по переводу денежных средств, обслуживающего получателя средств.

Операционное время – время, в течение которого поступившие от Клиента по Системе ДБО платежные документы принимаются Банком в обработку, исполняются и отражаются по счетам бухгалтерского учета. Для различных операций, осуществляемых с использованием Системы ДБО, Операционное время может отличаться. Информацию об установленном Операционном времени Банк размещает в настоящем Договоре и (или) Тарифах.

Операция – действия, осуществляемые Банком на основании электронного документа, переданного Клиентом в Банк с использованием Системы ДБО в порядке, установленном настоящим Договором.

Долговременный пароль – секретная, известная только Клиенту последовательность алфавитно-цифровых символов, соответствующая Логину Клиента многократно используемая в совокупности с Логинем для Аутентификации Клиента при Авторизации в Системе ДБО. При регистрации в Системе ДБО Клиент самостоятельно создает и с необходимой регулярностью, а также по мере необходимости в любой момент времени самостоятельно изменяет Долговременный пароль посредством Системы ДБО.

Платежная карта – выпущенная Банком Клиенту основная платежная карта международной платежной системы VISA International или платежной системы «МИР», являющаяся электронным средством для осуществления безналичных расчетов, предназначенным для оплаты товаров, работ и услуг, а также получения денежных средств и выполнения других операций на территории Российской Федерации и за ее пределами.

ПО – программное обеспечение.

Послеоперационное время – время, в течение которого поступившие от Клиента по Системе ДБО платежные документы по определенным типам операций принимаются Банком в обработку, но не исполняются.

Простая электронная подпись (ПЭП) – электронная подпись, факт формирования которой определенным лицом подтверждается посредством использования кодов, паролей или иных средств. Для каждого Клиента при его регистрации в Системе ДБО формируется уникальный идентификатор (далее - УИ). При авторизации Клиента в Системе ДБО определяется этот УИ, который в дальнейшем используется Системой ДБО при подписи сформированного Клиентом ЭД. Наличие УИ Клиента в поле CLIENT_ID записи базы данных содержащей этот ЭД, а также наличие любого из последующих статусов начиная со статуса «Доставлен» у этого ЭД является однозначным безоговорочным подтверждением создания этого ЭД Клиентом и его подписи простой электронной подписью Клиента.

Рабочий день – день, который в соответствии с законодательством Российской Федерации не является выходным и (или) нерабочим праздничным днем.

Регламентные работы – комплекс технических мероприятий, проводимых Банком периодически или регулярно при эксплуатации программно-аппаратного комплекса Системы ДБО.

Система дистанционного банковского обслуживания «iBank для жизни» (далее - Система ДБО) – корпоративная информационная система дистанционного банковского обслуживания, совокупность программно-аппаратных средств, согласованно эксплуатируемых Клиентом и Банком, а также организационных мероприятий, проводимых Клиентом и Банком, позволяющая осуществлять обмен электронными документами и информацией в электронном виде между ее участниками, и предназначенная для предоставления Клиентам – физическим лицам возможности получать информационные услуги и совершать банковские операции посредством сети Интернет.

В Системе ДБО Клиентом может использоваться только встроенный в Систему ДБО механизм простой электронной подписи (ПЭП). Не поддерживается использование генерируемых Клиентом ключей электронной подписи, плагина для web-браузера и USB-токенов.

Программное обеспечение Системы ДБО разработано АО «БИФИТ». Товарный знак № 182 «iBank» принадлежит АО «БИФИТ» на основании Свидетельства на общеизвестный товарный знак № 182 от 11 мая 2017 года.

Помимо наименования «Система «iBank для жизни», в тексте документации разработчика может также использоваться тождественное наименование – Система «iBank 2».

Система «iBank для жизни» состоит из:

- программных и аппаратных средств Банка, эксплуатируемых Банком за свой счет;
- АРМ, комплектуемых и эксплуатируемых Клиентом за свой счет;
- программных и аппаратных средств связи, обеспечивающих обмен ЭД между Сторонами;
- программных средств Системы «iBank для жизни», устанавливаемых на АРМ и самостоятельно эксплуатируемых Клиентом;
- Мобильного приложения, устанавливаемого Клиентом на его Мобильных устройствах, и самостоятельно им эксплуатируемого.

Перечень разрешенных для использования Клиентом поддерживаемых Банком каналов обслуживания (интерфейсов, модулей) Системы «iBank для жизни» определяется Банком и указывается в настоящем Договоре. Если

Банк разрешает Клиенту одновременно использовать несколько каналов обслуживания (интерфейсов, модулей) Системы «iBank для жизни», то Клиент вправе по своему усмотрению использовать любой(-ые) из них с учетом всех возможностей, особенностей и рисков, указанных в настоящем Договоре и в соответствующих руководствах пользователя по использованию каждого из каналов обслуживания (интерфейсов, модулей) Системы «iBank для жизни». Разрешенными для использования Клиентами Банка каналами обслуживания (интерфейсами, модулями) Системы «iBank для жизни», являются: «Интернет-Банк» и «Мобильный Банк».

Средства доступа – Логин, Долговременный пароль.

Статус ЭД – реквизит электронного документа, характеризующий стадию его обработки Банком и отображающийся в Системе ДБО. Возможны следующие статусы электронных документов: «Принят», «На обработке», «На исполнении», «Исполнен», «Отвергнут».

Стороны – Банк и Клиент при совместном упоминании.

Счет – текущий счет / счет по вкладу, открытый на имя Клиента в Банке, по которому Клиент совершает Операции и получает информацию в рамках настоящего Договора.

Электронный документ (далее - ЭД) – документ, в том числе платежный, в котором информация представлена в электронной форме в виде файла или записи в базе данных, созданный посредством программного обеспечения Системы ДБО с использованием носителей и способов записи, обеспечивающих его обработку техническими и программными средствами Системы ДБО. ЭД считается подписанным ЭП при наличии любого из последующих статусов начиная со статуса «Доставлен» у этого ЭД.

Электронная подпись (далее - 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. Обслуживание Клиентов с использованием Системы ДБО осуществляется с применением Простой электронной подписи.

SMS-уведомление – сообщение, содержащее информацию об Операции, совершенной по Счету / Платежной карте с использованием Системы ДБО, направляемое Банком Клиенту в электронном виде на номер мобильного телефона, указанный в Заявлении на присоединение.

2. ОБЩИЕ ПОЛОЖЕНИЯ

2.1. Настоящий Договор определяет условия, на которых может он может быть заключен между Банком и Клиентом, и устанавливает порядок взаимоотношений между Сторонами при осуществлении операций с использованием Системы ДБО.

2.2. Все Приложения к настоящему Договору являются их неотъемлемой частью.

2.3. Текст настоящего Договора публикуется на официальном сайте Банка по адресу www.thbank.ru (далее – официальный сайт Банка) и размещается на информационных стендах в офисах Банка. Текст настоящего Договора может быть выдан Клиенту на бумажном носителе при личном обращении Клиента в Банк.

2.4. Заключение Договора производится в форме присоединения Клиента к нему в соответствии со ст. 428 Гражданского кодекса Российской Федерации путем личного обращения в Банк и вручения уполномоченному работнику Банка Заявления о присоединении к Договору дистанционного банковского обслуживания клиентов – физических лиц с использованием Системы «iBank для жизни», оформленного Клиентом на бумажном носителе (Приложение № 1).

2.5. Подписывая Заявление о присоединении, Клиент подтверждает свое ознакомление с настоящим Договором, согласие с его условиями и принятие на себя обязательства неукоснительно их выполнять. Регистрация Банком Заявления о присоединении в реестре заключенных Банком договоров влечет возникновение у Сторон прав и обязанностей, предусмотренных настоящим Договором.

2.6. Доступ Клиента в Систему ДБО осуществляется через официальный сайт Банка.

2.7. Для подключения к Системе ДБО Клиент, после обработки Банком Заявления о присоединении, проходит самостоятельную регистрацию в соответствии с Руководством пользователя «Интернет-Банк для частных клиентов». По желанию Клиента регистрация может быть выполнена в Банке уполномоченным работником Банка.

2.8. Код подтверждения, необходимый как для завершения процедуры регистрации в Системе ДБО, так и для подтверждения каждого входа Клиента в Систему ДБО, направляется Банком Клиенту на номер мобильного телефона, указанный в Заявлении о присоединении (Приложение № 1).

Код подтверждения прав доступа Клиента в Систему ДБО с незарегистрированного в Системе ДБО устройства направляется на адрес электронной почты Клиента, указанный в Заявлении о присоединении (Приложение № 1).

При этом номер мобильного телефона и адрес электронной почты должны совпадать со сведениями, указанными Клиентом при заключении Договора банковского карточного счета. В случае, если номер мобильного телефона и (или) адрес электронной почты Клиента, указанные в Заявлении о присоединении, не совпадают со сведениями, указанными при заключении Договора банковского карточного счета, Клиент обязан оформить соответствующее заявление по установленной Банком форме на внесение изменений в Договор банковского карточного счета.

Номер мобильного телефона и адрес электронной почты, на которые направляется Коды подтверждения, могут быть изменены Клиентом при этом он обязан уведомить об этом Банк обратившись в Банк лично и вручив при этом уполномоченному работнику Банка заявление по установленной Банком форме и в соответствии с условиями, определенными Договором банковского карточного счета.

2.9. В случае не предоставления Клиентом в Банк Заявления о присоединении на бумажном носителе доступ к Системе ДБО Клиенту не предоставляется.

2.10. Обслуживание Клиента посредством Системы ДБО осуществляется в соответствии с настоящим Договором, требованиям законодательства Российской Федерации, нормативными актами Банка России.

2.11. Клиент предупрежден о следующих случаях повышенного риска, связанных с использованием Системы ДБО:

2.11.1. Кража или потеря Мобильного телефона, номер которого используется для доступа в Систему ДБО. В случае подозрения на кражу или потерю мобильного телефона Клиент обязан незамедлительно обратиться в Банк для временной блокировки доступа в Систему ДБО (до восстановления SIM-карты) или изменения номера мобильного телефона;

2.11.2. Невыполнение «Требований к обеспечению информационной безопасности при использовании Системы «iBank для жизни» АО «Тольяттихимбанк»» (Приложение № 2).

2.11.3. Получение доступа в Систему ДБО посредством браузера с устройства, содержащего вредоносный или модифицированный код.

2.12. Клиент проинформирован о недопустимости, ввиду повышенного риска, использования для доступа в Систему ДБО Мобильного устройства, которое:

2.12.1. Может содержать вредоносный или модифицированный код;

2.12.2. Может содержать не предусмотренное разработчиками и/или не сертифицированное производителем мобильного устройства ПО;

2.12.3. Прошло модификацию операционной системы, Мобильного приложения или иного программного обеспечения, не предусмотренную разработчиками программного обеспечения и/или не сертифицированную производителем Мобильного устройства.

2.13. Клиент проинформирован, что использование Системы ДБО с персонального компьютера, размещенного в общественном или ином общедоступном месте имеет повышенный риск несанкционированного доступа в Систему ДБО.

2.14. Клиент подтверждает, что до заключения настоящего Договора Банк проинформировал его об условиях использования Системы ДБО, об ограничениях способов, мест использования и случаях повышенного риска использования Системы ДБО. Соблюдение Клиентом условий Договора, «Требований к обеспечению информационной безопасности при использовании Системы «iBank для жизни» (Приложение № 2) и соответствующих Руководств пользователя для каждого из каналов обслуживания (интерфейсов, модулей) Системы ДБО снижает возможные риски при совершении операций с использованием Системы ДБО. Клиент подтверждает, что согласен нести все риски, связанные с доступом в Систему ДБО через сеть Интернет с использованием его устройств .

2.15. Клиент соглашается на подключение к Системе ДБО, осознавая, что сеть Интернет не является безопасным каналом связи и передачи информации, и осознает риски, связанные с возможным нарушением конфиденциальности и целостности информации при работе через Сеть Интернет, и иные риски, возникающие вследствие использования такого канала доступа.

2.16. Получая информацию о Кодах подтверждения в виде сообщений направляемых на номер мобильного телефона и адрес электронной почты, Клиент полностью осознает и соглашается с тем, что передача информации посредством SMS-сообщений и сообщений электронной почты осуществляется в открытом виде без применения средств шифрования. Банк не гарантирует полную конфиденциальность информации, передаваемой Клиенту по открытым каналам связи.

2.17. Обеспечение Информационной безопасности достигается реализацией комплекса необходимых мер, изложенных в настоящем Договоре.

2.18. Стороны признают, что используемые ими по настоящему Договору Система ДБО и каналы связи являются достаточными для обеспечения надежной и эффективной работы при приеме, передаче, обработке и хранении информации, для Защиты информации от несанкционированного доступа, однозначного подтверждения подлинности и авторства ЭД Клиента, при условии соблюдения Клиентом мер Информационной безопасности в соответствии с Требованиями к обеспечению информационной безопасности при использовании Системы «iBank для жизни» АО «Тольяттихимбанк» (Приложение № 2).

2.19. Стороны дают согласие на использование в рамках настоящего Договора Простой электронной подписи в соответствии с Федеральным законом от 06.04.2011 N 63-ФЗ «Об электронной подписи».

2.20. В соответствии с требованиями законодательства Российской Федерации Банк осуществляет информирование Клиента о совершении каждой Операции с использованием Системы ДБО по Счету / Платежной карте в порядке, установленном разделом 5 настоящего Договора.

2.21. Стороны гарантируют сохранение конфиденциальности, а также достоверность информации, содержащейся в формируемых и передаваемых ЭД в соответствии с настоящим Договором.

2.22. Стороны признают, что использующиеся для шифрования данных при передаче по Сети Интернет следующие криптографические алгоритмы шифрования/хеширования достаточны для обеспечения конфиденциальности информации при её передаче по сетям передачи данных, в т.ч. по Сети Интернет, защиты передаваемой информации от несанкционированного доступа для канала (интерфейса, модуля) «Мобильный Банк» в зависимости от используемой Клиентом операционной системы Мобильного устройства, а также для канала обслуживания (интерфейса, модуля) «Интернет-Банк» в зависимости от используемого Клиентом Браузера и операционной системы АРМ:

TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA,
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,
RSA_WITH_AES_128_CBC_SHA256.

2.23. Стороны признают, что выход из строя АРМ Клиента в результате вмешательства третьих лиц через Сеть Интернет рассматривается как выход из строя по вине Клиента.

2.24. Для получения услуги Клиент может использовать только АРМ, технические характеристики и операционные системы которых, соответствуют техническим требованиям, указанным в руководствах пользователя к соответствующим каналам обслуживания (интерфейсам, модулям), размещенным на сайте Банка в Сети Интернет по адресу https://ibank.thbank.ru/web_banking.

2.25. Стороны признают, что датой и временем отправки Клиенту SMS–уведомления, являются дата и время, определенные по системным часам аппаратных средств Банка в момент записи информации об отправке сообщения в протокол работы Системы ДБО.

2.26. Стороны признают, что ЭД, подписанные ЭП Клиента, а также журналы учета ЭД, ведущиеся в Системе ДБО, журналы учета действий Клиента в Системе ДБО могут быть представлены Банком в качестве доказательств в случае рассмотрения спора, возникшего в результате применения Системы ДБО.

2.27. Стороны признают, что сканированные копии документов, переданные вложенными файлами по Каналам связи с использованием Системы ДБО, вместе с сопроводительным письмом, подписанным ЭП, юридически эквивалентны получению копий документов, заверенных в соответствии с требованиями действующего законодательства Российской Федерации.

2.28. Клиент признает все ЭД, направленные им или полученные посредством Системы ДБО, равнозначными документам на бумажном носителе, подписанным собственноручной подписью Клиента.

3. ПРЕДМЕТ ДОГОВОРА

3.1. Посредством Системы ДБО Клиент получает возможность удаленно распоряжаться денежными средствами, размещенными на Счетах / Платежных картах, и доступ к информации о наличии и (или) состоянии Счетов / Платежных карт, о движении денежных средств на Счетах, об операциях, совершенных с использованием Платежных карт.

3.2. В рамках Договора Банком могут предоставляться Клиенту следующие услуги и сервисы:

3.2.1. переводы денежных средств между Счетами и (или) Платежными картами, открытыми в одной валюте;

3.2.2. конверсионные операции между Счетами и (или) Платежными картами, открытыми в разных валютах;

3.2.3. переводы денежных средств в валюте Российской Федерации на платежные карты третьих лиц, открытые в Банке;

3.2.4. переводы денежных средств в валюте Российской Федерации и иностранной валюте в соответствии с законодательством Российской Федерации на счета третьих лиц, открытые в Банке;

3.2.5. переводы денежных средств в валюте Российской Федерации и иностранной валюте в соответствии с законодательством Российской Федерации на счета, открытые в других кредитных организациях;

3.2.6. переводы денежных средств в валюте Российской Федерации через платежную систему «КиберПлат» в пользу отдельных поставщиков услуг;

3.2.7. переводы денежных средств в валюте Российской Федерации через Систему Быстрых Платежей Банка России в соответствии с Регламентом денежных переводов СПБ (Приложение № 6);

3.2.8. открытие текущих счетов;

3.2.9. размещение денежных средств во вклады, в том числе пополнение и (или) частичное изъятие, если такая возможность предусмотрена условиями вклада (досрочное истребование Клиентом всей суммы вклада осуществляется только при личном обращении Клиента в Банк);

3.2.10. приостановление действия Платежной карты;

3.2.11. восстановление Средств доступа;

3.2.12. самостоятельное изменение Средств доступа;

3.2.13. обмен информационными сообщениями с Банком;

3.2.14. просмотр ЭД, созданных в Системе ДБО;

3.2.15. получение информации о движении средств по Счетам / Платежным картам;

3.2.16. получение информации о реквизитах Счетов / Платежных карт.

3.3. Информацию о валютах, в которых возможно проведение Клиентом Операций в Системе ДБО, Банк размещает в Системе ДБО.

3.4. Операции, указанные в п.3.2. настоящего Договора, совершаются при условии их соответствия требованиям законодательства Российской Федерации, нормативным актам Банка России, соблюдении установленного Банком Лимита и наличия на Счете / Платежной карте доступного остатка собственных денежных средств Клиента (с учетом всех возможных ограничений: ареста денежных средств, заблокированных сумм и т.п.) в объеме, достаточном для совершения Операции и взимания Банком комиссионного вознаграждения за её совершение в соответствии с Тарифами, действующими на момент совершения Операции.

3.5. Отдельные виды услуг и сервисов, указанные в п. 3.2. настоящего Договора, предоставляются Клиенту по мере технической готовности Системы ДБО. Банк информирует Клиента о внедрении новых услуг и сервисов в рамках Системы ДБО, размещая информационные сообщения в Системе ДБО и (или) на официальном сайте Банка.

3.6. Оплата услуг, оказанных Банком Клиенту с использованием Системы ДБО, осуществляется в соответствии с Тарифами Банка. Настоящим Клиент поручает Банку без какого-либо дополнительного распоряжения (заранее данный акцепт) списывать денежные средства со Счетов / Платежных карт Клиента за предоставляемые услуги в сумме комиссий согласно Тарифам Банка, действующим на момент оказания услуги и (или) совершения Операции.

4. ПОРЯДОК ОСУЩЕСТВЛЕНИЯ ОПЕРАЦИЙ

4.1. При успешной Авторизации Операции по Счету / Платежной карте осуществляются Банком на основании полученного от Клиента ЭД, подтвержденного ЭП. ЭД передаются и принимаются с использованием Системы ДБО без их последующего предоставления на бумажном носителе.

4.2. Стороны признают, что полученные Банком ЭД, переданные посредством Системы ДБО в соответствии с настоящим Договором, равнозначны по своей юридической силе распоряжениям, подписанным Клиентом на бумажном носителе, и считаются оформленными в соответствии с требованиями законодательства Российской Федерации и нормативных актов Банка России, существующими в отношении таких документов.

4.3. Для Операций по переводу денежных средств, осуществляемых Клиентом с использованием Системы ДБО, применимы понятия Безотзывность, Безусловность и Окончателность.

4.4. ЭД порождает обязательства Сторон в случае, если он надлежащим образом оформлен, подтверждена ЭП Клиента, ЭД передан в Банк и принят Банком в обработку.

4.5. Стадию обработки Банком ЭД характеризует Статус ЭД. Стороны признают Статус ЭД способом уведомления Клиента об исполнении / аннулировании Банком ЭД. Информация об этапе обработки ЭД признается переданной Клиенту с момента изменения Статуса ЭД в Системе ДБО независимо от факта ознакомления с ней Клиента.

4.6. Банк вправе отказать Клиенту в исполнении ЭД в случае, если Операция противоречит законодательству Российской Федерации, нормативным актам Банка России, настоящему Договору.

4.7. При составлении Клиентом ЭД контроль полноты и правильности заполнения реквизитов ЭД осуществляется автоматически.

4.8. Банк принимает к исполнению ЭД Клиента при обязательном выполнении следующих проверочных процедур:

4.8.1. удостоверение права распоряжения денежными средствами (удостоверение права использования электронного средства платежа);

4.8.2. структурный контроль ЭД;

4.8.3. контроль значений реквизитов ЭД;

4.8.4. контроль достаточности денежных средств;

4.8.5. проверка документов, предоставляемых для обоснования перевода в случаях, установленных законодательством Российской Федерации, нормативными актами Банка России.

4.9. Удостоверение права распоряжения денежными средствами осуществляется Банком в момент авторизации Клиента.

4.10. Структурный контроль ЭД осуществляется Банком посредством автоматической проверки установленных реквизитов и максимального количества символов в реквизитах ЭД.

4.11. Контроль значений реквизитов ЭД осуществляется посредством проверки Банком значений реквизитов ЭД, их допустимости и соответствия требованиям законодательства Российской Федерации, нормативных актов Банка России.

4.12. При приеме к исполнению ЭД Банком осуществляется контроль достаточности денежных средств. Банк исполняет ЭД в пределах доступных собственных денежных средств Клиента на Счете / Платежной карте, с учетом всех ограничений (ареста на денежные средства, заблокированных сумм и т.п.). Исполнение ЭД на часть суммы не допускается.

4.13. Сформированный Клиентом ЭД после прохождения первичных автоматических проверок сохраняется в Системе ДБО и ему присваивается Статус ЭД «Принят». Статус ЭД «Принят» является промежуточным.

4.14. При положительном результате выполнения всех автоматических проверочных процедур Банк принимает ЭД в обработку, в процессе которой (в том числе по Операциям, требующим сопровождения сотрудниками Банка), возможны следующие промежуточные Статусы ЭД: «На обработке», «На исполнении».

4.15. В соответствии с законодательством Российской Федерации Банк может приостановить исполнение ЭД и запросить у Клиента подтверждающие Операцию документы. В случае не предоставления Клиентом запрошенных документов ЭД Банком не исполняется.

4.16. В случае, если ЭД не принят Банком к исполнению, ему присваивается Статус «Отвергнут», по которому Клиент определяет, что ЭД не будет исполнен Банком. Статус ЭД «Отвергнут» является окончательным. Информация о причине, по которой ЭД не принят Банком к исполнению, отражается в Системе ДБО.

4.17. Статус ЭД меняется на «Исполнен» после исполнения Банком ЭД Клиента. Статус ЭД «Исполнен» является окончательным, с момента его присвоения наступает Безотзывность перевода денежных средств.

4.18. Стороны признают в качестве единой шкалы времени при работе в Системе ДБО самарское время (UTC/GMT+4).

4.19. Прием ЭД в обработку осуществляется Банком круглосуточно без выходных дней. Временем принятия ЭД Клиента в обработку является текущее системное время Банка в момент сохранения ЭД в Системе ДБО.

4.20. Исполнение ЭД Клиента осуществляется Банком в Операционное время, определенное для данного типа Операций, в автоматическом режиме или в полуавтоматическом режиме с сопровождением сотрудниками Банка.

4.21. В автоматическом режиме с контролем программными средствами осуществляется проведение Клиентом в Системе ДБО следующих Операций:

4.21.1. переводы денежных средств между Счетами и (или) Платежными картами, открытыми в одной валюте;

4.21.2. переводы денежных средств в валюте Российской Федерации на платежные карты и банковские счета третьих лиц, открытые в Банке;

4.21.3. переводы денежных средств в валюте Российской Федерации через платежную систему «КиберПлат» в пользу отдельных поставщиков услуг;

4.21.4. пополнение имеющегося вклада и (или) частичное изъятие вклада, если такая возможность предусмотрена условиями вклада;

4.21.5. переводы денежных средств в валюте Российской Федерации через Систему Быстрых Платежей Банка России.

4.22. Для Операций, проводимых в автоматическом режиме, Банком устанавливается Операционное время: ежедневно и круглосуточно.

4.23. При осуществлении переводов денежных средств в валюте Российской Федерации через платежную систему «КиберПлат» в пользу отдельных поставщиков услуг устанавливаются следующие ограничения: максимальная сумма одной операции составляет 15 000-00 (Пятнадцать тысяч) рублей, максимальная сумма операций в пользу одного поставщика услуг, содержащих одинаковые реквизиты, в течение 1 (одного) календарного дня составляет 15 000-00 (Пятнадцать тысяч) рублей.

4.24. В полуавтоматическом режиме с выполнением дополнительных процедур контроля сотрудниками Банка осуществляется проведение Клиентом в Системе ДБО следующих Операций:

4.24.1. переводы денежных средств в валюте Российской Федерации в соответствии с законодательством Российской Федерации на счета, открытые в других кредитных организациях;

4.24.2. открытие текущих счетов;

4.24.3. размещение денежных средств во вклады.

4.25. Банк размещает информацию об Операционном времени, установленном для Операций, проводимых в полуавтоматическом режиме с сопровождением сотрудниками Банка, в Тарифах.

4.26. ЭД Клиента по Операциям, проводимым в полуавтоматическом режиме с сопровождением сотрудниками Банка, сформированные с использованием Системы ДБО в Послеоперационное время, исполняются Банком в Операционное время на следующий Рабочий день.

4.27. Операции, проводимые Клиентом с использованием Системы ДБО, отображаются в выписке по Счету / Платежной карте не позднее Рабочего дня, следующего за днем исполнения ЭД Клиента.

4.28. Банк устанавливает следующие лимиты на Операции по переводу денежных средств на счета, открытые в других кредитных организациях, на счета / платежные карты третьих лиц, открытые в Банке:

- ежемесячный - в размере 600 000-00 (Шестьсот тысяч) рублей – для всех видов переводов;

- ежедневный – в размере 100 000 -00 (сто тысяч рублей) – для переводов через Систему Быстрых Платежей.

4.29. Клиент может предоставить заявление об отмене установленного Лимита, оформленное на бумажном носителе, обратившись в Банк лично. Возможность отмены установленного Лимита определяется Банком.

5. ПОРЯДОК ИНФОРМИРОВАНИЯ КЛИЕНТА О СОВЕРШЕНИИ ОПЕРАЦИЙ

5.1. Банк информирует Клиента о совершении каждой Операций, проведенной по Счету / Платежной карте с использованием Системы ДБО в соответствии с условиями Договора банковского карточного счета, а также посредством отражения информации о совершенной Операции в выписке, формируемой в Системе ДБО.

5.2. Клиент имеет возможность в любое время сформировать в Системе ДБО выписку по каждому своему Счету / Платежной карте, обслуживание которых ведется с использованием Системы ДБО. Обновление данных об Операциях, остатках денежных средств на Счетах / Платежных картах Клиента в течение дня происходит непрерывно и носит предварительный характер. Окончательная выписка по Счету / Платежной карте в базе данных Системы ДБО может быть сформирована не позднее 12:00 часов Рабочего дня, следующего за днем исполнения ЭД.

5.3. Стороны признают, что Клиент не может считаться уведомленным или уведомленным ненадлежащим образом, если он отказывается или уклоняется от получения направленных в его адрес уведомлений, или не обеспечивает постоянную работоспособность и круглосуточную готовность Мобильного телефона к приему уведомлений от Банка.

5.4. Стороны пришли к соглашению, что обязанность Банка по уведомлению Клиента об Операциях по Счету / Платежной карте, совершенных с использованием Системы ДБО, считается исполненной с момента направления Банком SMS-уведомления на номер мобильного телефона, предоставленный Клиентом при заключении настоящего Договора или измененный на основании заявления предоставленного Клиентом Банку по установленной Банком форме и в соответствии с условиями, определенными Договором банковского карточного счета.

6. ПРАВА И ОБЯЗАННОСТИ СТОРОН

6.1. Клиент имеет право:

6.1.1. Совершать посредством Системы ДБО Операции, предусмотренные настоящим Договором, по всем Счетам / Платежным картам, открытым на его имя в Банке.

6.1.2. В случае несогласия со списанием денежных средств по Операции, проведенной с использованием Системы ДБО, или в случае возникновения претензий, связанных с принятием к обработке / исполнением ЭД, предоставлять в Банк мотивированное заявление о разногласиях, оформленное в свободной форме на бумажном носителе, обратившись в Банк лично.

6.1.3. В любой момент отказаться от использования Системы ДБО, письменно уведомив Банк о намерении расторгнуть Договор и предоставив Заявление о расторжении договора дистанционного банковского обслуживания с использованием Системы «iBank для жизни» АО «Тольяттихимбанк» (Приложение № 3), оформленное на бумажном

носителе, обратившись в Банк лично. На основании указанного заявления Банк прекращает обслуживание Клиента с использованием Системы ДБО не позднее Рабочего дня, следующего за днем его поступления от Клиента.

6.1.4. Временно приостановить использование Системы ДБО, обратившись в Банк лично и представив Заявление о приостановлении обслуживания с использованием Системы «iBank для жизни» АО «Тольяттихимбанк» (Приложение № 4), оформленное на бумажном носителе.

6.1.5. Возобновить доступ к Системе ДБО, приостановленный Банком, в том числе после Компрометации Средств доступа, только при личном обращении в Банк, подав на бумажном носителе Заявление на возобновление обслуживания с использованием Системы «iBank для жизни» АО «Тольяттихимбанк» (Приложение № 5).

6.1.6. В случае приостановления обслуживания по Системе ДБО предоставлять в Банк распоряжения на проведение Операций, оформленные на бумажном носителе в соответствии с требованиями законодательства Российской Федерации, нормативных актов Банка России.

6.1.7. Подать в Банк по установленной Банком форме и в соответствии с условиями, определенными Договором банковского карточного счета Заявление об изменении номера Мобильного телефона и адреса электронной почты.

6.2. Клиент обязан:

6.2.1. Использовать ПО и аппаратные средства, соответствующие требованиям, изложенным в соответствующих руководствах пользователя по использованию каждого из каналов обслуживания (интерфейсов, модулей) Системы ДБО, размещенных на сайте Банка в Сети Интернет по адресу https://ibank.thbank.ru/web_banking.

6.2.2. При подключении новых каналов обслуживания (интерфейсов, модулей) и (или) услуг Системы ДБО самостоятельно осуществлять настройки своего АРМ в соответствии с руководством пользователя по использованию соответствующего канала обслуживания (интерфейса, модуля) Системы ДБО, размещенном на сайте Банка в Сети Интернет по адресу https://ibank.thbank.ru/web_banking.

6.2.3. Хранить в секрете и не передавать третьим лицам Долговременный пароль.

6.2.4. Во избежание рисков, связанных с осуществлением несанкционированных операций с использованием дистанционного банковского обслуживания посредством Системы ДБО и для обеспечения безопасного использования Системы ДБО - выполнять Требования к обеспечению информационной безопасности при использовании Системы «iBank для жизни» АО «Тольяттихимбанк» (Приложение № 2).

Неисполнение Клиентом Требований к обеспечению информационной безопасности при использовании Системы «iBank для жизни» АО «Тольяттихимбанк» (Приложение № 2) является основанием для отказа в возмещении Клиенту суммы операции, совершенной без согласия клиента в соответствии с частью 12 статьи 9 Федерального закона от 27.06.2011 N 161-ФЗ «О национальной платежной системе».

6.2.5. Использовать Систему ДБО в соответствии с настоящим Договором.

6.2.6. Предоставить Банку достоверные данные о номере Мобильного телефона и адресе электронной почты используемых для получения Кодов подтверждения и иных предупреждений и сообщений Системы ДБО.

6.2.7. Использовать для получения SMS-уведомлений и иных SMS-сообщений от Системы ДБО номер мобильного телефона, зарегистрированный за Клиентом у оператора, оказывающего услуги мобильной связи.

6.2.8. В случае указания неверного номера Мобильного телефона для получения SMS-сообщений - компенсировать Банку выплаты по претензии владельца неверно указанного номера Мобильного телефона, если таковые выплаты имелись и подтверждены Банком документально.

6.2.9. Не допускать нарушений условий тарифного плана оператора связи, в результате которых происходит блокировка приема входящих SMS-сообщений на Мобильный телефон.

6.2.10. Не допускать переполнение памяти Мобильных телефонов предназначенной для приема и хранения SMS-сообщений, что может являться препятствием для приема SMS – подтверждений и SMS, e-mail – уведомлений.

6.2.11. В случае утраты или компрометации пароля для доступа к электронному почтовому ящику незамедлительно изменить адрес электронной почты или заблокировать до завершения восстановления пароля доступа к электронному почтовому ящику доступ в Систему ДБО обратившись в Банк лично и представив уполномоченному работнику Банка оформленное на бумажном носителе Заявление о приостановлении обслуживания с использованием Системы «iBank для жизни» АО «Тольяттихимбанк» (Приложение № 4).

6.2.12. Незамедлительно уведомить Банк, обратившись в Банк лично и представив уполномоченному работнику Банка оформленное на бумажном носителе по установленной Банком форме и в соответствии с условиями, определенными Договором банковского карточного счета заявление об изменении следующих сведений при обнаружении факта возникновения следующих нижеперечисленных событий:

6.2.12.1. Номера Мобильного телефона, указанного для получения SMS-сообщений в случае утраты по каким-либо причинам (кража, утеря и т.п.) Мобильного телефона или при изменении номера Мобильного телефона.

6.2.12.2. Адреса электронной почты в случае компрометации пароля для доступа к электронному почтовому ящику или при изменении адреса электронной почты.

6.2.13. Информировать Банк об изменениях иных, не указанных в пп. 6.2.12 Договора сведений о Клиенте, содержащихся в Заявлении о присоединении к Договору дистанционного банковского обслуживания клиентов – физических лиц с использованием Системы «iBank для жизни» (Приложение № 1 к Договору) в срок не позднее 10 (Десяти) календарных дней со дня их изменения обратившись в Банк лично и представив уполномоченному работнику Банка заявление, оформленное на бумажном носителе по установленной Банком форме и в соответствии с условиями, определенными Договором банковского карточного счета.

6.2.14. Не раскрывать третьим лицам информацию, которая может быть использована для доступа к Системе ДБО, в том числе информацию о Средствах доступа и Кодах подтверждения.

6.2.15. Не хранить на АРМ, используемом для работы в Системе ДБО, информацию о Средствах доступа.

6.2.16. Обеспечить сохранность Мобильных устройств с установленным Мобильным приложением.

6.2.17. Незамедлительно, после обнаружения факта утраты Средств доступа и (или) доступа / предполагаемой возможности доступа третьих лиц в Систему ДБО, использования Системы ДБО без согласия Клиента установить новый Долговременный пароль используя соответствующие возможности Системы ДБО.

6.2.18. В момент обнаружения несанкционированного доступа или попытки несанкционированного доступа к Системе ДБО незамедлительно письменно сообщить об этом Банку.

6.2.19. При обнаружении факта несанкционированного Клиентом списания со счета(-ов) денежных средств, Клиент обязан действовать в соответствии с «Планом действий при обнаружении факта несанкционированного Клиентом списания со счета(-ов) денежных средств», изложенным в п. 9 Приложения № 2 «Требования к обеспечению информационной безопасности при использовании Системы «iBank для жизни» к настоящему Договору.

6.2.20. Обеспечить отсутствие на АРМ ВК, безопасность и целостность среды исполнения АРМ.

6.2.21. При поступлении от Банка по электронной почте или посредством интерфейса Системы ДБО соответствующего запроса, подтвердить оговоренным в запросе способом выполнение требований по защите от ВК АРМ.

6.2.22. Не передавать по Системе ДБО ПО, содержащее ВК и нелегальное программное обеспечение.

6.2.23. В случае обнаружения какого-либо ВК в АРМ незамедлительно предпринять меры по удалению ВК и после этого незамедлительно установить новый Долговременный пароль используя соответствующие возможности Системы ДБО.

6.2.24. Составлять ЭД с использованием имеющихся в Системе ДБО шаблонов (форм) документов, с учетом требований нормативных актов Банка России и действующего законодательства Российской Федерации, а при отсутствии таких шаблонов – в соответствии с требованиями нормативных актов Банка России и действующего законодательства Российской Федерации.

6.2.25. Получать выписки по Счету Клиента и не позднее 10 (Десяти) календарных дней со дня совершения операции по Счету Клиента с использованием Системы ДБО письменно уведомить Банк о выявленных расхождениях (о не признании (не подтверждении) остатка), а также ошибочно зачисленных на Счет Клиента денежных средствах и возвратить Банку указанные средства. В случае отсутствия претензий со стороны Клиента остатки и операции по Счету Клиента считаются подтвержденными.

6.2.26. По требованию Банка представлять ему документы, информацию и сведения, необходимые для исполнения Банком требований Федерального закона от 07.08.2001 № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма», иных действующих нормативных актов Российской Федерации, в том числе раскрывающие экономический смысл Операций, проводимых посредством Системы ДБО. Предоставление документов осуществляется в сроки и в порядке, установленные запросом Банка. Выполнение данного требования является условием исполнения Банком ЭД Клиента.

6.2.27. Не осуществлять с использованием Системы ДБО Операции, связанные с проведением предпринимательской деятельности.

6.2.28. При возникновении спорной ситуации, связанной с отказом Клиента от авторства или содержания ЭД, оказывать содействие Банку при выяснении соответствующих обстоятельств.

6.2.29. Не использовать Систему ДБО на мобильном устройстве, которое используется для получения Кодов подтверждения.

6.2.30. Выполнять иные обязанности, предусмотренные действующим законодательством Российской Федерации, документами (в том числе методическими рекомендациями) Банка России и настоящим Договором.

6.3. Банк имеет право:

6.3.1. Отказать в заключении Договора.

6.3.2. Вносить изменения в настоящий Договор в порядке, установленном разделом 10 Договора.

6.3.3. Отказать в исполнении ЭД Клиента на проведение Операции посредством Системы ДБО по Счетам / Платежным картам в случаях, предусмотренных законодательством Российской Федерации, в том числе, но не ограничиваясь, Федеральным законом от 10.12.2003 № 173-ФЗ «О валютном регулировании и валютном контроле» и Федеральным законом от 07.08.2001 № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма».

6.3.4. В целях обеспечения безопасности работы Клиента в Системе ДБО устанавливать и изменять размер Лимита по Операциям.

6.3.5. Отказать в исполнении ЭД Клиента на проведение Операции посредством Системы ДБО в случае превышения установленного Лимита по Операциям.

6.3.6. Без предварительного уведомления Клиента приостановить использование Системы ДБО в следующих случаях:

- при возникновении у Банка технических неисправностей или других обстоятельств, препятствующих использованию Системы ДБО, обеспечению требуемого уровня безопасности проведения Операций посредством Системы ДБО;

- при неоднократном некорректном вводе Пароля, Кода подтверждения;

- при нарушении Клиентом своих обязательств, принятых в соответствии с настоящим Договором;

- в случае поступления в Банк информации о Компрометации Средств доступа или в случае обоснованных подозрений Банка в Компрометации Средств доступа ввиду имеющейся у него информации;

- в иных случаях, предусмотренных настоящим Договором.

6.3.7. Приостановить использование Клиентом Системы ДБО в случае возникновения подозрения о том, что проводимые Операции осуществляются с целью легализации (отмывания) доходов, полученных преступным путем, и финансирования терроризма, предварительно уведомив Клиента посредством Системы ДБО за 2 (два) Рабочих дня до момента приостановления.

6.3.8. На основании п. 3.6. настоящего Договора списывать со Счетов / Платежных карт без дополнительного распоряжения Клиента комиссионное вознаграждение за использование Системы ДБО в соответствии с Тарифами.

6.3.9. Без предварительного уведомления Клиента отключить доступ к Системе ДБО в случае, если Клиент не осуществлял Операции в Системе ДБО в течение 6 (шести) месяцев с момента осуществления первого доступа Клиента к Системе ДБО / последней совершенной Клиентом Операции.

6.3.10. Приостанавливать использование Клиентом Системы ДБО на время проведения обязательных регламентных работ, предварительно уведомив Клиента об этом за 2 рабочих дня до проведения регламентных работ.

6.3.11. По своему усмотрению ограничивать набор функций, выполняемых Системой ДБО. Наличие той или иной функции, отображаемой в интерфейсе Системы ДБО, не является подтверждением её функционирования и не дает Клиенту права требовать обеспечить работоспособность этой функции.

6.4. Банк обязан:

6.4.1. Обеспечить Клиенту доступ к Системе ДБО в порядке, определенном настоящим Договором.

6.4.2. Приостановить использование Системы ДБО, в том числе исполнение ЭД, после получения соответствующего уведомления Клиента.

6.4.3. Принять все разумные меры для предотвращения несанкционированного доступа третьих лиц к конфиденциальной информации, связанной с использованием Клиентом Системы ДБО.

6.4.4. Информировать Клиента о проведении Регламентных работ путем размещения информации на официальном сайте Банка и (или) путем направления Клиенту уведомления по Системе ДБО.

6.4.5. Не разглашать и не передавать третьим лицам информацию, переданную (полученную) Клиентом с использованием Системы ДБО, за исключением случаев, предусмотренных законодательством Российской Федерации.

6.4.6. Информировать Клиента о каждой Операции, совершенной по Счету / Платежной карте посредством Системы ДБО.

6.4.7. Рассматривать заявления Клиента, связанные с использованием Системы ДБО, и сообщать о результатах рассмотрения в письменной форме в срок не более 30 (тридцати) календарных дней со дня получения таких заявлений, а в случае осуществления трансграничного перевода денежных средств – в срок не более 60 (шестидесяти) календарных дней со дня получения заявления.

7. ОТВЕТСТВЕННОСТЬ СТОРОН

7.1. Стороны несут ответственность за неисполнение и/или ненадлежащее исполнение своих обязательств, предусмотренных настоящим Договором, в соответствии с законодательством Российской Федерации и условиями настоящего Договора.

7.2. Стороны несут ответственность за достоверность предоставляемой друг другу информации, в том числе по Системе ДБО.

7.3. Стороны обязуются при разрешении экономических и иных споров, которые могут возникнуть в связи с использованием Системы ДБО, представлять в письменном виде свои оценки, доказательства и выводы по запросу заинтересованной Стороны.

7.4. Банк и Клиент не несут ответственности за убытки, понесенные одной Стороной не по вине другой Стороны в результате использования Системы ДБО, в том числе при исполнении ошибочных ЭД, если эти документы надлежащим образом Клиентом оформлены и переданы, а Банком получены, проверены и признаны верными.

7.5. При несогласии со списанием денежных средств по Операции, проведенной с использованием Системы ДБО, Клиент обязан направить соответствующее уведомление Банку в форме и в порядке, предусмотренных настоящим Договором, незамедлительно после обнаружения факта проведения Операции с использованием Системы ДБО без согласия Клиента, но не позднее дня, следующего за днем получения от Банка уведомления о совершенной Операции.

7.6. Банк обязан возместить Клиенту сумму Операции:

7.6.1. совершенной без согласия Клиента после получения Банком уведомления, указанного в п. 7.5. настоящего Договора;

7.6.2. совершенной без согласия Клиента до момента направления Клиентом уведомления, указанного в п. 7.3. настоящего Договора, если Банк не докажет, что Клиент нарушил порядок использования Системы ДБО, указанный в настоящем Договоре, что повлекло совершение Операции без согласия Клиента;

7.6.3. совершенной без согласия Клиента, о которой Клиент не был проинформирован Банком в порядке, предусмотренном разделом 5 настоящего Договора.

7.7. Банк не обязан возместить Клиенту сумму Операции, совершенной без согласия Клиента, в случае если Банк проинформировал Клиента о совершенной Операции в порядке, предусмотренном разделом 5 настоящего Договора, и Клиент не направил Банку уведомление, указанное в п. 7.5. настоящего Договора.

7.8. Банк не несет ответственности:

7.8.1. За последствия компрометации Средств доступа Клиента, Кодов подтверждения.

7.8.2. За ущерб, вне зависимости от причин, возникший вследствие разглашения Клиентом неуполномоченным лицам собственных Средств доступа и Кодов подтверждения.

7.8.3. За ущерб, причиненный Клиенту, из-за несанкционированного доступа к Системе ДБО, в результате использования третьими лицами Средств доступа и/или нарушения Клиентом Требований к обеспечению информационной безопасности при использовании Системы «iBank для жизни» установленных Приложением № 2 к настоящему Договору.

7.8.4. За убытки, понесенные Клиентом в связи с неправомерными действиями третьих лиц.

7.8.5. В случае реализации угроз несанкционированного доступа неуполномоченных лиц к АРМ (в том числе удаленный сетевой доступ), включая угрозы со стороны внутренних (локальных) и внешних (глобальных) сетей связи, а также в результате воздействия ВК.

7.8.6. За возможные искажения, ошибки и опечатки в ЭД, отправленных Клиентом по Системе ДБО и подписанных ЭП Клиента.

7.8.7. За повторное исполнение ЭД Клиента, направленного в Банк повторно/ошибочно.

7.8.8. За неработоспособность оборудования, программных средств и каналов связи Клиента и третьих лиц, повлекшую за собой невозможность доступа Клиента к банковской части Системы ДБО, и возникшие в результате этого задержки в осуществлении операций Клиента, а также за возможное уничтожение (в полном или частичном объеме) информации, содержащейся на АРМ Клиента, подключенных к Сети Интернет для обеспечения предоставления услуг по настоящему Договору.

7.8.9. За скорость и факт доставки Клиенту информации, переданной через каналы передачи данных, находящиеся вне ведения Банка.

7.8.10. За обеспечение конфиденциальности информации, содержащей персональные данные Клиента и сведений, являющиеся банковской тайной, при их передаче по телекоммуникационным сетям и каналам связи за пределами Банка в виде SMS-сообщений и писем, направленных по электронной почте.

7.8.11. За убытки, расходы, а также иные негативные последствия, которые могут возникнуть в случае, если передаваемые при передаче SMS сообщений сведения станут известны третьим лицам, в том числе за последствия передачи оператором мобильной связи номера Мобильного телефона Клиента, предоставленного Банку для отправки SMS сообщений, другому абоненту.

7.8.12. За последствия исполнения ЭД подписанного ЭП Клиента, в том числе в случае использования АРМ неуполномоченным лицом.

7.8.13. За неисполнение или ненадлежащее исполнение ЭД, произошедшее из-за нарушения Клиентом настоящего Договора и условий иных договоров, заключенных между Клиентом и Банком, регулирующих правоотношения по порядку исполнения Банком ЭД Клиента.

7.8.14. За неисполнение или просрочку исполнения ЭД Клиента, если таковые произошли из-за неисполнения Клиентом обязанностей по настоящему Договору, в том числе обязанности по установлению сеанса связи с Банком.

7.8.15. За задержки в расчетах, возникающие в результате действий других кредитных организаций, расчетных центров и других организаций, участвующих в расчетах.

7.8.16. В случае утери Мобильного устройства Клиента.

7.9. Банк не несет ответственности, если информация об изменении и/или дополнении настоящего Договора и/или Тарифов Банка, опубликованная в порядке и в сроки, установленные настоящим Договором, не была получена и/или изучена и/или правильно истолкована Клиентом.

7.10. Банк не несет ответственности, в том числе, в виде возмещения ущерба Клиента, в случае невозможности осуществления обмена ЭД с Клиентом, если это вызвано ненадлежащим функционированием технических и программных средств, Каналов связи, принадлежащих Клиенту или третьим лицам, и используемых в работе с (в) Системой(-е) ДБО.

7.11. Клиент несет полную ответственность:

7.11.1. За сохранение в тайне информации о Средствах доступа, Кодах подтверждения и обязуется исключить доступ к ним третьих лиц.

7.11.2. За действия лиц, получивших по любым основаниям (в том числе противоправным) доступ к Системе ДБО.

7.11.3. За правильность заполнения и корректное содержание ЭД, переданных в Банк посредством Системы ДБО.

7.11.4. За полноту, достоверность и своевременность предоставления сведений о номере Мобильного телефона и адресе электронной почты.

7.11.5. За правильность и актуальность всех документов (иной информации), предоставляемых им в Банк при заключении и исполнении настоящего Договора.

7.12. Клиент полностью принимает на себя все риски, связанные с подключением его оборудования (в том числе компьютерного) к сети Интернет. Клиент самостоятельно обеспечивает защиту данного оборудования от несанкционированного доступа и от воздействия ВК из сети Интернет.

7.13. Поскольку для сообщения Банку своего адреса электронной почты, Клиент самостоятельно выбирает провайдера, предоставляющего услуги обработки и хранения сообщений электронной почты, то Клиент несет ответственность за обеспечение конфиденциальности данных вследствие такого выбора.

7.14. Учитывая особенности передачи данных через открытые средства коммуникаций, Банк не несет ответственность за убытки, причиненные неполучением Клиентом и (или) получением неуполномоченным на то лицом информации, передаваемой посредством SMS-сообщений.

7.15. Направление Банком информации об Операции, совершенной посредством Системы ДБО, по известному Банку номеру мобильного телефона Клиента признается надлежащим информированием об Операции, если на дату отправки таких сообщений Банк не был извещен Клиентом об изменении номера мобильного телефона. В этом случае Банк не несет ответственности за ущерб, причиненный Клиенту вследствие направления информации на номер мобильного телефона, более не используемый Клиентом.

7.16. Стороны освобождаются от ответственности за частичное или полное неисполнение обязательств по настоящему Договору, если это неисполнение явилось следствием обстоятельств непреодолимой силы, возникшей при конкретных условиях, конкретного периода времени в результате событий чрезвычайного характера, которые имели непредвиденный и (или) непредотвратимый при данных условиях характер, наступили после даты подписания Договора, непосредственно повлияли на его исполнение и которые Стороны не могли ни предвидеть, ни предотвратить разумными мерами. К обстоятельствам непреодолимой силы относятся стихийные бедствия, аварии, пожары, наводнение, землетрясение, военные действия, массовые беспорядки, массовые заболевания (эпидемии), военные перевороты, террористические акты, национальные забастовки, противоправные действия третьих лиц, действия либо

решения органов государственной власти и правоохранительных органов, а также принятие (издание) нормативно-правовых актов, прямо или косвенно запрещающих или препятствующих полному или частичному выполнению Сторонами своих функций и иных обязательств по настоящему Договору. Факт наступления обстоятельств непреодолимой силы подтверждается Сторонами путем предоставления соответствующих документов.

7.17. Сторона по Договору, ссылающаяся на обстоятельства непреодолимой силы, обязана в течение 3 (трех) Рабочих дней информировать другую Сторону о наступлении подобных обстоятельств, а также об оценке их влияния на исполнение своих обязательств по Договору и на срок исполнения этих обязательств.

7.18. При расторжении настоящего Договора Стороны несут ответственность по всем ЭД с ЭП Клиента, сформированным в Системе ДБО, в соответствии с действующим законодательством Российской Федерации.

7.19. В случае нарушения Клиентом срока уведомления, предусмотренного п. 5.3.7. настоящего Договора, а также в случае не возврата Клиентом сумм, ошибочно зачисленных на Счет Клиента, в срок, установленный п. 5.3.7. настоящего Договора, и если Банк не имеет возможности взыскать эти суммы без дополнительного распоряжения Клиента, Клиент уплачивает Банку пеню в размере 0,3 (ноль целых три десятых) процентов от ошибочно зачисленной суммы в рублях или 0,15 (ноль целых пятнадцать сотых) процентов от суммы в иностранной валюте за каждый день нарушения срока уведомления и/или просрочки возврата сумм.

7.20. Банк несет ответственность за несвоевременное информирование (уведомление) Клиента о совершенных операциях по Счету Клиента в размере реального ущерба Клиента, вызванного таким несвоевременным информированием, но не более 1 000 (Одной тысячи) рублей.

7.21. Возмещение Банком убытков, возникших у Клиента в результате необоснованного неисполнения или ненадлежащего исполнения ЭД Клиента, в том числе, несвоевременного перечисления денежных средств, ограничивается уплатой Банком суммы в размере 0,3 (ноль целых три десятых) процентов годовых при осуществлении операций в валюте Российской Федерации и 0,15 (ноль целых пятнадцать сотых) процентов годовых при осуществлении операций в иностранной валюте от суммы, указанной в неисполненном или ненадлежащим образом исполненном ЭД Клиента, но не более чем за 30 (тридцать) календарных дней неисполнения или ненадлежащего исполнения ЭД Клиента.

8. РАЗРЕШЕНИЕ СПОРОВ

8.1. Споры и разногласия, связанные с выполнением настоящего Договора, разрешаются Сторонами путем переговоров. Обязательным для Сторон является соблюдение досудебного претензионного порядка урегулирования спора: претензия (и ответ на нее) должны направляться Сторонами друг другу в письменной форме, заказным письмом и уведомлением о вручении. Срок ответа на претензию – 30 (тридцать) календарных дней с момента ее получения, если иной срок не установлен настоящим Договором.

8.2. Разногласия, по которым Сторонами не достигнуты договоренности, подлежат рассмотрению судом в соответствии с законодательством Российской Федерации.

8.3. Приостановление использования Системы ДБО, а также временное прекращение осуществления Операций в Системе ДБО по инициативе одной из Сторон не влечет прекращения обязательств по взаиморасчетам и возмещению убытков, возникших до момента приостановления использования Системы ДБО или прекращения осуществления Операций.

8.4. Клиент, желающий опротестовать проведение спорной Операции, обязан в срок, не позднее Рабочего дня, следующего за днем исполнения спорной Операции, предоставить заявление об отказе от Операции, оформленное в свободной форме на бумажном носителе (с обязательным указанием информации, позволяющей идентифицировать спорную Операцию), обратившись в Банк лично.

8.5. Банк рассматривает заявление Клиента об отказе от операции и удовлетворяет претензию Клиента, либо направляет ему письменное заключение о необоснованности претензии в срок, указанный в п. 6.4.7. настоящего Договора. В случае несогласия Клиента с заключением Банка, Клиент может обратиться в суд в соответствии с законодательством Российской Федерации.

9. СРОК ДЕЙСТВИЯ ДОГОВОРА

9.1. Договор заключен на неопределенный срок, вступает в силу с даты заключения Договора и действует до момента его расторжения в порядке, предусмотренном настоящим Договором.

9.2. Датой заключения Договора является дата регистрация Банком Заявления о присоединении в реестре заключенных Банком договоров.

9.3. Договор может быть расторгнут по инициативе Клиента в любое время в одностороннем порядке путем представления в Банк соответствующего заявления, оформленного на бумажном носителе при личном обращении в Банк.

9.4. Банк вправе в одностороннем порядке расторгнуть Договор в случае невыполнения Клиентом обязательств, установленных настоящим Договором, а также если Банку стало известно о представлении Клиентом в Банк заведомо ложных или искаженных документов / сведений и в иных случаях, предусмотренных законодательством Российской Федерации, письменно уведомив Клиента за 5 (пять) Рабочих дней до расторжения Договора, если иное не предусмотрено настоящим Договором или законом.

9.5. Договор прекращает свое действие при закрытии Клиентом всех Счетов / Платежных карт в Банке, при отсутствии входов Клиента в Систему ДБО в течение 6 (шести) месяцев с момента осуществления первого доступа Клиента к Системе ДБО или последней совершенной Клиентом Операции.

9.6. Прекращение действия Договора не влияет на действие других договоров, заключенных между Банком и Клиентом, а также на юридическую силу и действительность ЭД, которыми Банк и Клиент обменивались до прекращения действия Договора.

10. ПОРЯДОК ВНЕСЕНИЯ ИЗМЕНЕНИЙ И ДОПОЛНЕНИЙ В ДОГОВОР

10.1. При необходимости внесения изменений в Договор Банк не менее, чем за 10 (десять) Рабочих дней до даты вступления в силу таких изменений, доводит их до сведения Клиента путем размещения соответствующей информации на официальном сайте Банка и в офисах Банка, за исключением изменений, обусловленных требованиями законодательства Российской Федерации, более ранний срок вступления которых в силу определяется нормативными и правовыми актами Российской Федерации.

10.2. В случае неполучения Банком возражений Клиента относительно вносимых изменений в течение 10 (десяти) Рабочих дней с даты уведомления Клиента в соответствии с п.10.1. настоящего Договора, согласие Клиента на внесение изменений считается полученным, а изменения безоговорочно принятыми и обязательными для исполнения. Любые изменения и дополнения к настоящему Договору с момента вступления их в действие распространяются на всех лиц, присоединившихся к нему, в том числе присоединившихся к настоящему Договору ранее даты вступления изменений в силу.

10.3. В случае несогласия с изменениями Клиент имеет право представить свои мотивированные возражения в письменной форме в срок, указанный в п.10.2. настоящего Договора. В случае отклонения Банком возражений Клиента последний имеет право расторгнуть Договор.

11. ПРОЧИЕ УСЛОВИЯ

11.1. Во всем, что не урегулировано настоящим Договором, Стороны руководствуются законодательством Российской Федерации.

11.2. Вся переписка между Сторонами по настоящему Договору об использовании Системы ДБО ведется на русском языке.

12. ПРИЛОЖЕНИЯ

12.1. Неотъемлемой частью настоящего Договора являются:

12.1.1. Приложение № 1 Заявление о присоединении к Договору дистанционного банковского обслуживания клиентов – физических лиц с использованием Системы «iBank для жизни» АО «Тольяттихимбанк».

12.1.2. Приложение № 2 Требования к обеспечению информационной безопасности при использовании Системы «iBank для жизни» АО «Тольяттихимбанк».

12.1.3. Приложение № 3 Заявление о расторжении договора дистанционного банковского обслуживания с использованием системы Системы «iBank для жизни» АО «Тольяттихимбанк».

12.1.4. Приложение № 4 Заявление о приостановлении обслуживания с использованием Системы «iBank для жизни» АО «Тольяттихимбанк».

12.1.5. Приложение № 5 Заявление о возобновлении обслуживания с использованием Системы «iBank для жизни» АО «Тольяттихимбанк».

12.1.6. Приложение № 6 Регламент денежных переводов СПб.

ЗАЯВЛЕНИЕ № _____
о присоединении к договору дистанционного банковского обслуживания клиентов – физических лиц с использованием Системы «iBank для жизни» АО «Тольяттихимбанк»

Гор. Тольятти

« _____ » _____ 20__ г.

Настоящим Заявлением

(Фамилия Имя Отчество полностью)

Документ, удостоверяющий личность:

Серия

Номер

Дата выдачи

Кем выдан

Дата рождения

Настоящим вышеуказанный Клиент заявляет о присоединении к действующей в АО «Тольяттихимбанк» редакции Договора дистанционного банковского обслуживания клиентов – физических лиц с использованием Системы «iBank для жизни» (далее – Договор) в порядке, предусмотренном статьей 428 Гражданского кодекса Российской Федерации, подтверждает, что все положения (условия) действующей в АО «Тольяттихимбанк» редакции Договора ему известны и разъяснены в полном объеме (включая все приложения и дополнения к нему, порядок внесения изменений и дополнений, порядок опубликования информации, ответственность и Тарифы Банка). Клиент подтверждает свое ознакомление и согласие с условиями Договора, а также получение от Банка исчерпывающей информации о предоставляемых услугах, позволившее осуществить самостоятельный выбор и принять осознанное решение о заключении Договора.

Прошу направлять коды подтверждения входа в Систему «iBank для жизни» и информировать о совершении операций с использованием Системы «iBank для жизни» в соответствии со ст. 9 Федерального Закона «О национальной платежной системе» от 27.06.2011 № 161-ФЗ путем направления SMS-сообщений на номер мобильного телефона:

+7																			
----	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--

Коды подтверждения входа в Систему «iBank для жизни», направляемые в виде сообщений по электронной почте, прошу направлять на следующий адрес электронной почты:

(подпись)

(Фамилия Имя Отчество полностью)

Заполняется Банком:

Отметка сотрудника Банка о принятии Заявления Клиента, его регистрации и присвоении номера договора:

№ договора _____

« _____ » _____ 20__ г.

(подпись)

(расшифровка)

Требования к обеспечению информационной безопасности при использовании Системы «iBank для жизни»

1. Вниманию Клиента.

1.1. Согласно статистике, наиболее часто попытки хищения денежных средств осуществляются:

1.1.1. ИТ-специалистами, оказывающими (или оказывавшими ранее, в т.ч. однократно) для АРМ различные ИТ-услуги по поддержке, подключению к сети Интернет, установке, настройке, обновлению и поддержке различных программ (бухгалтерских, правовых, информационных), компьютерных игр и т.д.;

1.1.2. мошенниками, использующими методы социальной инженерии для заражения АРМ ВК через сеть Интернет, используя уязвимости в безопасности АРМ или вынуждающие Клиента скомпрометировать Логин, Долговременный пароль и Код подтверждения.

1.2. Во всех перечисленных в пп. 1.1.1 - 1.1.2 случаях, злоумышленники, завладев Средствами доступа Клиента или путем перехвата управления АРМ Клиента, направляют от имени Клиента в Банк электронные документы для перевода денежных средств со счетов Клиента различным физическим и юридическим лицам.

1.3. Банк не осуществляет рассылку электронных писем с просьбой прислать Логин, Долговременный пароль, Код подтверждения и никогда не запрашивает у Клиентов эту информацию.

1.3.1. Запрещается выполнять указания, в случае получения Клиентом такого письма от имени Банка, содержащего ссылку на установку программы, программу для установки или запрос на предоставление Логина, Долговременного пароля, Кода подтверждения, используемых Клиентом в Системе «iBank для жизни». О произошедшем необходимо незамедлительно сообщить в службу технической поддержки Клиентов Системы «iBank для жизни» Банка.

2. Обеспечить безопасность Долговременного пароля, используемого в Системе «iBank для жизни»:

2.1. Требования к паролю:

2.1.1. Длина пароля должна быть не менее восьми символов.

2.1.2. Пароль должен состоять из комбинации следующих символов: прописные и строчные латинские буквы, цифры.

2.1.3. Необходимо выбирать трудно подбираемые пароли.

2.1.4. При выборе паролей не должна использоваться какая-либо «система»: новый пароль не должен быть прогнозируемым на основе знаний о предыдущих паролях, датах их смены и т.д.

2.1.5. При выборе пароля запрещается:

2.1.5.1. Использовать пустые пароли.

2.1.5.2. Совпадение пароля с Логинем;

2.1.5.3. Повторно использовать старые пароли. Новый пароль не должен совпадать ни с одним из предыдущих паролей. Новый пароль должен отличаться от предыдущего не менее чем в четырех символах.

2.1.5.4. Использовать в качестве пароля последовательность символов, состоящих из одних цифр. Например, «12349876», «03826495».

2.1.5.5. Использовать в качестве пароля идущие подряд (расположенные рядом) в раскладке клавиатуры символы. Например, «QWERTYUI», «qazxswEDC», «qazwsxedc».

2.1.5.6. Использовать в качестве пароля буквы, расположенные в прямом и в обратном алфавитном порядке, в том числе набранные на регистре другого языка. Например: «CDEFGHIJ» (идущие подряд буквы латинского алфавита), «zyxwVUTS» (буквы латинского алфавита в обратном порядке), «f,dult'»;», (абвгдеёж – идущие подряд буквы русского алфавита, набранные на латинской раскладке клавиатуры).

2.1.5.7. Использовать в качестве пароля осмысленные слова любого языка, сленговые выражения или общеупотребительные сокращения, имена собственные (названия, имена и фамилии), адреса, в том числе набранные на регистре другого языка или преобразованные транслитерацией. Например, «grapefruit» (грейпфрут (англ.)), «Churchill» (Черчилль (англ.)), «Zelenograd» (Зеленоград), «admin» (сленговое выражение, сокращенное от «administrator»), «bcntvtf» (система), «svetofor» (светофор).

2.1.5.8. Включать в пароль последовательности из четырех и более повторяющихся символов. Например, «qqqqqqqq», «ad111111» или «ZZZZaaaa».

2.1.5.9. Включать в пароль ассоциируемую с Клиентом или АРМ информацию, которую легко узнать: Ф.И.О. Клиента или его ближайших родственников, марку автомобиля, кличку домашнего животного, название АРМ в локальной сети, полное или сокращенное наименование Банка, название сервера и т.д.. Например, «dmitry666» (если имя Клиента - Дмитрий), «ТНВPass».

2.1.5.10. Наличие очевидных закономерностей между символами пароля. Например, пароли a1a2a3a4, 12367890, имеют очевидные закономерности.

2.2. Не назначать Долговременный пароль, используемый в Системе «iBank для жизни», в любых других системах и сервисах.

2.3. Не сообщать Долговременный пароль, используемый в Системе «iBank для жизни», кому-либо, в том числе ИТ-специалистам для проверки работы системы, настроек взаимодействия с Банком и т.п. При необходимости таких проверок Клиент обязан лично вводить Долговременный пароль в Систему «iBank для жизни».

3. Для АРМ, необходимо:

3.1. Применять для работы лицензионное программное обеспечение.

- 3.2. **Использовать операционную систему, поддерживаемую производителем.**
- 3.3. **Рекомендуется использовать только последние версии браузера. Регулярно (не реже чем ежедневно) в автоматическом режиме производить обновление браузера.**
- 3.4. **Применять лицензионное средство защиты от ВК или защитное ПО.**
 - 3.4.1. **Применять последние версии лицензионного средства защиты от ВК или защитного ПО.**
 - 3.4.2. **Обеспечивать регулярное обновление в автоматическом режиме баз данных ВК, по мере их размещения (обновления) разработчиками средств защиты от ВК, но не реже чем ежедневно.**
 - 3.4.3. **Обеспечивать регулярный в автоматическом режиме ежедневный полный Контроль АРМ на наличие ВК.**
 - 3.4.4. **Рекомендуется использовать средства защиты от ВК или защитное программное обеспечение следующих производителей: Kaspersky, Dr.Web, Eset Nod32.**
- 3.5. **Обеспечить регулярную (не реже чем ежедневно) в автоматическом режиме загрузку и установку обновлений безопасности операционной системы.**
- 3.6. **Исключить загрузку и установку нелегального программного обеспечения. В особенности ПО, загруженного с неизвестных сайтов сети Интернет.**
- 3.7. **Осуществлять проверку на наличие ВК посредством средств защиты от ВК любых файлов и программ, загружаемых из сети Интернет, полученных по электронной почте, посредством мессенджеров, из социальных сетей или на внешних носителях (дискеты, Flash-накопители (флэшки), CD/DVD и т.п.).**
- 3.8. **Принимать повышенные меры по обеспечению отсутствия ВК (как минимум, проверять работоспособность средств защиты от ВК и актуальность баз данных ВК, а также осуществлять полный Контроль АРМ на наличие ВК) после любых действий ИТ-специалистов или любых других лиц, выполнявших любые операции на АРМ (например, решение каких-либо проблем, подключение к сети Интернет, настройка, установка, обновление и поддержке различных бухгалтерских, правовых, информационных и др. программ и т.п.).**
- 3.9. **Исключить доступ к АРМ лиц, не имеющих отношения к работе с Системой «iBank для жизни».**
- 3.10. **Не допускать работу с Системой «iBank для жизни» под учётной записью пользователей операционной системы, имеющих права администратора. Использовать учётную запись с ограниченными правами. Работа с правами администратора повышает вероятность проникновения ВК.**
- 3.11. **Ограничить локальными или доменными (при наличии) политиками на АРМ список пользователей, имеющих право входа в операционную систему.**
- 3.12. **Все учетные записи пользователей АРМ должны быть защищены паролем.**
 - 3.12.1. **Следует осуществлять периодическую смену паролей (не реже 1 раза в месяц).**
 - 3.12.2. **Ограничить количество неудачных попыток входа в систему. Рекомендуется блокировать вход после трех неудачных попыток.**
 - 3.12.3. **Устанавливать пароли в соответствии с требованиями, установленными п. 2.1.**
- 3.13. **Блокировать сетевой доступ к АРМ (в том числе запретить Дистанционное управление рабочим столом, Удаленный помощник) с других рабочих станций локальной сети и из внешних сетей, включая сеть Интернет.**
- 3.14. **Запрещается использовать любые средства удалённого (дистанционного) управления АРМ, используемые ИТ-специалистами для удалённой (дистанционной) поддержки. Например, «TeamViewer», «Admin» и т.п.**
- 3.15. **Запрещается переходить по ссылкам на неизвестные сайты, полученным от известных и тем более от неизвестных отправителей.**
- 3.16. **Разрешить сетевое взаимодействие АРМ только с необходимым доверенным перечнем IP-адресов в локальной сети Клиента (при наличии таковой).**
- 3.17. **Для выполнения требований пп 3.12 – 3.15 рекомендуется применение лицензионного персонального межсетевое экрана (программного и/или аппаратного).**
- 3.18. **На АРМ должна быть установлена только одна операционная система.**
- 3.19. **Рекомендуется не использовать АРМ в публичных (проводных/беспроводных) сетях, предоставляющих доступ к сети Интернет, для исключения значительного повышения риска компрометации Логина и Долговременного пароля, используемых в Системе «iBank для жизни».**
- 3.20. **Запрещается устанавливать на АРМ средства разработки программного обеспечения и отладчики программного обеспечения.**
- 3.21. **Запрещается оставлять без контроля АРМ. При кратковременном отсутствии следует блокировать рабочее место средствами операционной системы.**
- 3.22. **Разрешить для АРМ загрузку только с носителя, на котором установлена операционная система. Отключить загрузку с других носителей (приводов оптических дисков, съёмных носителей, загрузку по сети и т.д.).**
- 3.23. **Отключить учётную запись для гостевого входа (Гость, Guest).**
- 3.24. **Запретить режим автоматического входа пользователя без ввода пароля в операционную систему при ее загрузке.**
- 3.25. **Запретить режим отображения окна всех зарегистрированных на АРМ пользователей и быстрое переключение пользователей.**
- 3.26. **Использовать штатные возможности операционной системы для защиты от ВК и несанкционированного доступа. В зависимости от используемой операционной системы, задействовать следующие встроенные механизмы защиты (при наличии):**
 - 3.26.1. **Контроль учетных записей – механизм, упрощающий использование учетных записей, не обладающих административными привилегиями;**
 - 3.26.2. **Брандмауэр – встроенный межсетевой экран;**
 - 3.26.3. **Использование технологии AppLocker;**

3.26.4. Защитник Windows – служба защиты от шпионского ПО;

3.26.5. Средство удаления вредоносных программ.

3.27. В случае передачи (списания, утилизации и т.п.) сторонним лицам стационарного АРМ, ноутбука или мобильного устройства, на котором ранее была установлена Система «iBank для жизни», необходимо гарантированно удалить с него всю информацию, использование которой третьими лицами может потенциально нанести вред финансовой деятельности Клиента.

3.28. Не рекомендуется посещайте сайты, предлагающие быстро и бесплатно скачать различные файлы или программы, поскольку даже вход на такой сайт может угрожать безопасности АРМ.

4. Дополнительные меры по обеспечению безопасности при использовании для работы в Системе «iBank для жизни» в качестве АРМ мобильных устройств:

4.1. Разрешается использовать Мобильное приложение, полученное только через официальный ресурс распространения программного обеспечения для Мобильных устройств. Официальными ресурсами являются: для операционной системы Android – магазин приложений Google Play, для операционной системы iOS – магазин приложений App Store.

4.2. Запрещается использовать на мобильных устройствах модифицированные или измененные операционные системы.

5. После входа на стартовую страницу Системы «iBank для жизни» следует удостовериться, что установлено защищенное соединение по протоколу HTTPS (в адресной строке указана аббревиатура https://). В противном случае следует прекратить использование Системы «iBank для жизни» и принять меры по обеспечению работы только с использованием защищенного соединения.

6. При подключении к сайту Системы «iBank для жизни» проверить подлинность сертификата сайта (наличие значка защищенного соединения - «замочек» в правом нижнем углу или в адресной строке браузера).

7. Запрещается использовать Систему ДБО с персонального компьютера, размещенного в общественном или ином общедоступном месте в связи с наличием повышенного риска несанкционированного доступа в Систему ДБО.

8. Требования по защите информации от несанкционированного доступа путем использования ложных (фальсифицированных) ресурсов сети Интернет.

8.1. Для входа в Систему «iBank для жизни» следует набрать в адресной строке браузера: адрес официального сайта банка в сети Интернет <https://www.thbank.ru> и по ссылке перейти к сайту Системы ДБО.

8.2. Прежде чем ввести Логин и Долговременный пароль, используемые в Системе «iBank для жизни», еще раз внимательно проверить в адресной строке браузера адрес сайта - https://ibank.thbank.ru/web_banking.

9. Использовать следующие меры обеспечения безопасности при работе с сообщениями, полученными посредством мессенджеров, из социальных сетей или по электронной почте:

9.1. Запрещено открывать сообщения, письма и прикрепленные к ним файлы, полученные от неизвестных отправителей, переходить по содержащимся в таких письмах ссылкам.

9.2. Используя средства защиты от ВК или защитное программное обеспечение, осуществлять исключение из информационного потока сообщений, которые имеют признаки наличия ВК, или приостанавливать их обработку (помещать таких сообщения в карантин) с выдачей соответствующего уведомления.

10. План действий в случае обнаружении факта несанкционированного Клиентом списания со счета(-ов) денежных средств.

10.1. При обнаружении факта несанкционированного Клиентом списания со счета(-ов) денежных средств, Клиент обязан немедленно:

10.1.1. не выключать АРМ(-ы) с которого(-ых) выполняется работа в Системе «iBank для жизни»;

10.1.2. физически отключить АРМ(-ы) от сети Интернет (отключить соединительный провод к устройству посредством которого осуществляется доступ в сеть Интернет или в случае, если доступ осуществляется посредством оборудования, расположенного в локальной сети, от локальной сети или отключить беспроводной маршрутизатор, если используется беспроводное подключение к сети Интернет);

10.1.3. сообщить о произошедшем в Банк;

10.1.4. сообщить о произошедшем в правоохранительные органы;

11. Рекомендации по защите АРМ от несанкционированного доступа.

11.1. Для защиты АРМ от несанкционированного доступа на АРМ установить программно-аппаратный комплекс защиты от несанкционированного доступа.

11.2. Сформировать с помощью комплекса защиты от несанкционированного доступа функционально замкнутую среду, обеспечивающую контроль целостности программного обеспечения и допускающую работу пользователей строго в рамках, предоставляемых им возможностей и полномочий.

ЗАЯВЛЕНИЕ № _____
о расторжении договора дистанционного банковского обслуживания клиентов – физических лиц с использованием Системы «iBank для жизни» АО «Тольяттихимбанк»

Гор. Тольятти

« ____ » _____ 20__ г.

Настоящим Заявлением

(Фамилия Имя Отчество полностью)

Документ, удостоверяющий личность:

Серия

Номер

Дата выдачи

Кем выдан

Дата рождения

Прошу отключить доступ к Системе «iBank для жизни» и расторгнуть Договор дистанционного банковского обслуживания клиентов – физических лиц с использованием системы «iBank для жизни».

Подтверждаю, что на момент предоставления настоящего заявления мной выполнены все обязательства в соответствии с действующими условиями Договора дистанционного банковского обслуживания клиентов – физических лиц с использованием системы «iBank для жизни» и Тарифов АО «Тольяттихимбанк».

(подпись)

(Фамилия Имя Отчество полностью)

Заполняется Банком:

Отметка сотрудника Банка о принятии Заявления Клиента:

« ____ » _____ 20__ г.

(подпись)

(расшифровка)

ЗАЯВЛЕНИЕ № _____
о приостановлении обслуживания с использованием
Системы «iBank для жизни» АО «Тольяттихимбанк»

Гор. Тольятти

« _____ » _____ 20__ г.

Настоящим Заявлением

(Фамилия Имя Отчество полностью)

Документ, удостоверяющий личность:

Серия

Номер

Дата выдачи

Кем выдан

Дата рождения

Прошу приостановить доступ к Системе «iBank для жизни» с

(подпись)

(Фамилия Имя Отчество полностью)

Заполняется Банком:

Отметка сотрудника Банка о принятии Заявления Клиента:

« _____ » _____

20__ г.

(подпись)

(расшифровка)

ЗАЯВЛЕНИЕ № _____
о возобновлении обслуживания с использованием
Системы «iBank для жизни» АО «Тольяттихимбанк»

Гор. Тольятти

« _____ » _____ **20** ____ г.

Настоящим Заявлением

(Фамилия Имя Отчество полностью)

Документ, удостоверяющий личность:

Серия

Номер

Дата выдачи

Кем выдан

Дата рождения

Прошу возобновить обслуживание с использованием Системы «iBank для жизни» с

(подпись)

(Фамилия Имя Отчество полностью)

Заполняется Банком:

Отметка сотрудника Банка о принятии Заявления Клиента:

« _____ » _____ **20** ____ г.

(подпись)

(расшифровка)

РЕГЛАМЕНТ

осуществления Переводов СБП

1. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Перевод СБП – перевод денежных средств в российских рублях, совершенный с использованием СБП. Для переводов СБП используются Счета Клиента, открытые в российских рублях, исключая счета, открытые по договору банковского вклада.

Система быстрых платежей (СБП) – сервис платежной системы Банка России, позволяющий Клиенту круглосуточно в режиме реального времени осуществлять Перевод СБП и получать денежные средства, перевод которых был осуществлен плательщиком с использованием СБП по номеру мобильного телефона. Оператором Системы быстрых платежей и ее расчетным центром является Банк России.

Операционным и платежным клиринговым центром, обеспечивающим Участникам СБП доступ к обмену электронными сообщениями, осуществляющим прием и подтверждение распоряжений на перевод денежных средств и другие операции является Акционерное общество «Национальная система платежных карт» (АО «НСПК»).

Участник СБП – кредитная организация, являющаяся одновременно прямым участником платежной системы Банка России и участником платежной системы «Мир».

2. ОБЩИЕ ПОЛОЖЕНИЯ

2.1. С использованием Системы ДБО Клиент может отправлять и получать денежные средства через СБП.

2.2. Для получения денежных средств через СБП Клиент с использованием интерфейса Системы ДБО должен самостоятельно активировать соответствующую функцию Системы ДБО.

2.3. Отправка Переводов СБП доступна Клиентам без выполнения дополнительных действий с использованием интерфейса Системы ДБО, при этом использование СБП для осуществления Переводов СБП явно обозначено в интерфейсе Системы ДБО.

2.4. Выполнение Клиентом действий по подготовке и отправке Перевода СБП или активация функции получения денежных средств через СБП, указанная в п. 2.2, является подтверждением Клиентом своего согласия с настоящим Регламентом.

2.5 Переводы СБП осуществляются только в рублях Российской Федерации на счета клиентов-физических лиц Участников СБП, открытые в рублях Российской Федерации (в том числе на счета Клиента Банка, открытые в банках - Участниках СБП).

2.6. Лимиты на совершение операций в СБП предусмотрены действующим законодательством Российской Федерации. Банк вправе устанавливать дополнительные лимиты на совершение операций в СБП (разовый/суточный/месячный).

2.7. Банк вправе без объяснения причин отказать Клиенту в возможности использования СБП (отключить СБП) в следующих случаях:

2.7.1. при наличии у Банка подозрений и/или информации о незаконном характере операций;

2.7.2. при выявлении подозрительных и/или мошеннических операций;

2.7.3. при обнаружении Банком фактов в результате анализа которых выявлен риск нарушения Клиентом действующего законодательства РФ;

2.7.4. в иных, установленных настоящим Регламентом и/или действующим законодательством РФ, случаях.

3. ПОРЯДОК ОСУЩЕСТВЛЕНИЯ ПЕРЕВОДОВ СБП

3.1. Для осуществления Перевода СБП по номеру мобильного телефона Клиент должен указать следующие реквизиты перевода:

- счет, с которого будет произведен перевод;
- номер мобильного телефона получателя перевода;
- один из доступных банков - Участников СБП получателя платежа из списка;
- сумма перевода;

3.2. После ввода Клиентом всех реквизитов перевода Банк через интерфейс Системы ДБО отображает Клиенту информацию о получателе, хранимую в СБП. Клиент обязан осуществить проверку сведений о получателе и убедиться, что сведения о получателе соответствуют намерениям Клиента осуществить Перевод СБП данному получателю, в противном случае Клиент должен отказаться от совершения перевода. Если сведения о получателе соответствуют намерениям, Клиент подтверждает операцию.

3.3. На основании полученных от Клиента реквизитов перевода Банк:

- осуществляет проверку достаточности денежных средств на указанном Клиентом Счете;
- резервирует денежные средства на указанном Счете в соответствии с указанной Клиентом суммой перевода с учетом комиссии, установленной Тарифами;
- формирует от имени Клиента платежный документ и на его основании осуществляет перевод денежных средств через СБП в соответствии с реквизитами, указанными Клиентом.

3.4. Ответственность за корректность/достаточность ввода Клиентом Номера мобильного телефона получателя перевода и всех иных реквизитов для совершения операции возлагается на Клиента.

3.5. Исполнение платежного документа Клиента при Переводe СБП в пользу физического лица осуществляется Банком в порядке поступления, но не позднее следующего рабочего дня с даты подтверждения Банком приема платежного документа к исполнению. Перевод считается отправленным в момент подтверждения Банком факта наличия денежных средств на счете Клиента, достаточных для осуществления перевода по СБП и отражения соответствующей информации в СБП. Безотзывность Перевода СБП наступает после подтверждения перевода клиентом.

3.6. В целях приема поступающих денежных средств через СБП, Клиент должен самостоятельно выбрать в Системе ДБО номер счета, открытый Клиенту в Банке, на который Банк будет осуществлять зачисление денежных средств. Счетом для зачисления денежных средств, поступивших Клиенту через СБП может быть текущий счет/карточный счет, при этом в качестве идентификатора Счета, Банком используется зарегистрированный Номер мобильного телефона.

3.7. При зачислении средств Клиенту – получателю перевода посредством СБП в случае, если Клиент не установил счет в Банке для зачисления денежных средств в рамках СБП, либо счет, установленный ранее закрыт/платежная карта заблокирована или закрыта, Банк руководствуется следующим: при наличии у Клиента нескольких Счетов, зачисление будет произведено на счет действующей основной Платежной карты, открытый в рублях, если таких карт несколько, зачисления будет произведено на Счет Платежной карты с более ранней датой открытия.

3.8. Банк вправе отказать Клиенту в осуществлении Перевода СБП в следующих случаях:

- при отсутствии у Банка технической возможности для работы в СБП;
- при наличии запретов или ограничений на осуществление операций в рамках СБП установленных Банком России и/или действующим законодательством РФ;
- при неоплате Клиентом комиссий, предусмотренных Тарифами Банка;
- в иных случаях, установленных действующим законодательством РФ.

3.9. За осуществление Перевода СБП Банком может взиматься комиссионное вознаграждение согласно Тарифам Банка, действующим на момент перевода.

3.10. Сумма комиссии (в случае ее наличия) отображается Банком Клиенту после ввода последним реквизитов перевода или перед подтверждением операции Клиентом.

3.11. Комиссия в рамках Системы быстрых платежей взимается с отправителя перевода.

4. СОГЛАСИЕ НА ОБРАБОТКУ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИСПОЛЬЗОВАНИИ СБП

4.1. Выполнив действия, указанные в п. 2.4 настоящего Регламента, Клиент даёт АО «Голыяттихимбанк», расположенному по адресу 445009, г. Тольятти ул. Горького, д. 96 согласие с целью обеспечения возможности осуществления операций в СБП и осуществления таких операций:

4.1.2. на использование номера мобильного телефона Клиента в качестве идентификатора, позволяющего установить принадлежность Клиенту номера банковского счета, открытого в Банке, при совершении в пользу Клиента Переводов СБП, зачисление денежных средств по Переводам СБП на банковский Счет Клиента;

4.1.3. на передачу персональных данных Клиента (фамилия, имя отчество, номер мобильного телефона, адрес регистрации, ИНН, номер счета зачисления/списания денежных средств, данные документа, удостоверяющего личность), необходимых для осуществления операции в СБП, Банком в Банк России (адрес местонахождения: РФ, 107016, г. Москва, ул. Неглинная, д. 12), в операционный и платежный клиринговый центр АО «НСПК» (адрес местонахождения: РФ, 115184, г. Москва, ул. Большая Татарская, д.11А), Участнику СБП (банку, участвующему в переводе через СБП), для:

- регистрации персональных данных Клиента в СБП;
- обеспечения возможности отправителями переводов денежных средств выполнять проверку сведений о Клиенте как получателе платежа;
- получения через СБП входящих переводов от клиентов Банка или клиентов других банков по Номеру мобильного телефона;
- назначения счета для зачисления получаемых через СБП переводов по Номеру мобильного телефона;
- совершения перевода денежных средств отправителем Клиенту;
- осуществления Клиентом перевода денежных средств зарегистрированному в СБП получателю.

4.2. Согласие на обработку персональных данных указанное в п. 4.1. действует в течение срока действия Договора ДБО, может быть отозвано путем направления Банку письменного уведомления, и считается отозванным по истечении 30 дней с момента получения Банком соответствующего уведомления, при условии, что на момент отзыва согласия между Клиентом и Банком не будет действующих договорных отношений, если иное не установлено законодательством Российской Федерации.

4.3. Банк вправе продолжить обработку персональных данных Клиента в иных целях, не связанных с платежами в СБП, в объеме и в течение периода времени, предусмотренных законодательством РФ и необходимых для выполнения взаимных обязательств Банка и Клиента в соответствии с заключенными между ними договорами.