Приложение №2 к Правилам расчетно-кассового обслуживания юридических лиц, индивидуальных предпринимателей и лиц, занимающихся в установленном законодательством Российской Федерации порядке частной практикой в КБ «Новый век» (ООО)

Правила дистанционного банковского обслуживания клиентов с использованием системы «iBank 2» в КБ «Новый век» (ООО)

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящие Правила определяют порядок заключения и расторжения Договора о дистанционном банковском обслуживании с использованием Системы «iBank 2», заключаемого в целях предоставления Банком услуг по дистанционному банковского обслуживанию по Системе «iBank 2» юридических лиц, индивидуальных предпринимателей и лиц, занимающихся в установленном законодательством РФ порядке частной практикой, а также права, обязанности и ответственность Клиента и Банка (вместе по тексту Стороны) по указанному Договору. Настоящие Правила не регулируют отношения Банка и клиентов по иным системам дистанционного банковского обслуживания.

1.2. Договор заключается путем присоединения Клиента к настоящим Правилам (включая Приложения к ним, определяющие условия заключаемого Клиентом Договора) на основании ст. 428 Гражданского кодекса Российской Федерации путем принятия (акцепта) Банком предложения (оферты) Клиента о заключении Договора, изложенной в Заявлении о присоединении. Опубликование Банком настоящих Правил в порядке, установленном разделом 9 Правил, не является публичной офертой. Договор считается заключенным со дня принятия (акцепта) Банком предложения (оферты) Клиента о заключении Договора, изложенной в Заявлении о присоединении. Принятие (акцепт) Банком предложения (оферты) Клиента подтверждается специальной отметкой об акцепте на Заявлении о присоединении, совершенной сотрудником Банка, уполномоченным на заключение Договора. Договор включает в себя в качестве составных и неотъемлемых частей Заявление о присоединении, настоящие Правила и Тарифы, а в случаях, предусмотренных Правилами – также иные документы, оформляющие соглашения Банка и Клиента по условиям дистанционного банковского обслуживания.

1.3. Заявление о присоединении по форме Приложения № 1 оформляется в двух экземплярах. Второй экземпляр Заявления о присоединении с отметкой о принятии (акцепте) Банком, заверенный подписью уполномоченного сотрудника Банка и печатью подразделения Банка, после заключения Договора передается Клиенту и является единственным документом, подтверждающим факт заключения Договора.

1.4. Настоящий Договор является неотъемлемой частью Договора (-ов) банковского счета (-ов), заключенного (-ых) между Сторонами.

ИСПОЛЬЗУЕМЫЕ ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Применительно к настоящим Правилам используется следующая терминология.

Система «iBank 2» (или **Система**) - автоматизированная организационно-техническая система, составляющая совокупность программно-аппаратных средств, включающая в себя серверную часть (сервер), установленную на территории Банка, и клиентскую часть (клиентский модуль), загружаемую на компьютер Клиента, обеспечивающая организацию электронного документооборота и безбумажных расчетов между Банком и его Клиентами, обеспечивающая подготовку, защиту и обработку документов в электронном виде с использованием электронно-вычислительных средств обработки информации, а также разбор конфликтных ситуаций. Система не предусматривает осуществление связи клиентами Банка между собой.

Разработчиком и владельцем исключительных прав на Систему «iBank 2» является АО «БИФИТ» (ИНН 7719617469). Адреса и контакты компаний разработчика и правообладателя: www.bifit.com.

Система «iBank 2» является разновидностью систем Клиент-Банк.

Клиентский модуль (клиентская часть) - on-line модуль — Java или HTML5-апплет, загружаемый в компьютер Клиента через Глобальную сеть Internet в начале каждого сеанса связи Клиента с сервером Банка по Системе «iBank 2». При использовании on-line модуля обмен информацией между клиентским модулем и сервером Системы возможен только путём соединения через Глобальную сеть Internet. Вход в Систему осуществляется с помощью ключа ЭП, пароля ключа ЭП.

Договор - объявленные Банком стандартные условия дистанционного банковского обслуживания Клиентов с использованием системы «iBank 2» в КБ «Новый век» (ООО). Договор является договором

присоединения и заключается с Клиентом путем направления Клиентом Банку заявления на подключение услуг в системе «iBank 2».

Электронный документ (ЭД) — определённая последовательность байтов, зафиксированная на магнитных или иных устройствах хранения данных, содержащая информацию о платежах Клиента и другую информацию, подписанная электронной подписью уполномоченного лица Клиента и переданная Клиентом в Банк по телекоммуникационным каналам связи средствами Системы «iBank 2», с реквизитами, позволяющими идентифицировать эти данные и их автора.

Электронный платежный документ (ЭПД) – это разновидность электронного документа, представляющего собой поручение Клиента на совершение операции по счету Клиента, открытому в Банке, содержащее все предусмотренные банковскими правилами реквизиты, подписанное необходимым количеством групп подписей ЭП Клиента, имеющий равную юридическую силу с платежным документом, составленным на бумажном носителе, подписанным собственноручными подписями уполномоченных лиц (лица) Клиента и заверенными оттиском печати в соответствии с предоставленной Банку Карточкой с образцами подписей и оттиска печати, и являющийся основанием для совершения операции по счету Клиента, открытому в Банке.

Предоставление ЭД в электронном виде/форме – демонстрация наличия записи о существовании ЭД и непосредственно самого ЭД на компьютере Клиента и/или Сотрудника Банка при помощи Клиентского модуля и/или Модуля операциониста Системы «iBank 2», а также при помощи другого программного обеспечения, входящего в состав Системы «iBank 2».

Электронная подпись (ЭП) — последовательность байтов, являющаяся результатом работы, входящей в Систему «iBank 2» программы генерации электронной подписи. ЭП является аналогом физической (собственноручной) подписи и обладает двумя основными свойствами: воспроизводима только одним лицом, а подлинность её может быть удостоверена многими; неразрывно связана с конкретным ЭД и только с ним. ЭП позволяет удостовериться в подлинности, целостности этого ЭД, установить его авторство. ЭП жестко увязывает в одно целое содержимое ЭД и секретный ключ подписывающего лица и делает невозможным изменение этого документа без нарушения корректности (подлинности) данной ЭП. Средства ЭП, входящие в состав Системы, реализуют алгоритмы формирования ЭП и её проверки в соответствии со стандартом ГОСТ Р 34.10-94.

Электронный служебно-информационный документ (ЭСИД) – электронный документ, обеспечивающий обмен информацией между Клиентом и Банком при совершении операций по счетам Клиента, открытым в Банке, и не являющийся основанием для совершения бухгалтерских проводок. К ЭСИД относятся: выписки, запросы, отчеты, информационные сообщения, уведомления и т.п.

Операционное время – период времени, в течение рабочего дня, устанавливаемый Банком для приема поручений Клиента, на выполнение различных видов операций, подлежащих исполнению в тот же день. Изменение операционного времени доводится до Клиента в ЭСИД с использованием Системы.

Владелец ЭП – уполномоченное должностное лицо Клиента, указанное в Карточке с образцами подписей и оттиска печати, электронная подпись которого зарегистрирована в Банке.

Криптографическая защита – защита электронного документа от несанкционированного изменения и доступа к его содержимому посторонних лиц при помощи алгоритмов криптографического преобразования. В рамках Системы под криптографической защитой понимается шифрование, электронная подпись и вычисление хеш-функций программного обеспечения.

Ключ ЭП – последовательность байтов, самостоятельно генерируемая Клиентом с использованием средств Системы и предназначенная для формирования ЭП электронного документа, т.е. секретная часть ключевой информации, представляющая собой уникальную последовательность двоичных данных и предназначенная для создания в электронном документе электронной подписи владельца ЭП. Хранится владельцем ключевой информации в тайне. Клиент самостоятельно обеспечивает конфиденциальность ключа ЭП. Срок действия ключа ЭП считается с даты подписания Сертификата ключа ЭП Банком по дату, определяемую в соответствии с Регламентом (Приложение №5 к Договору). Носителями ключа ЭП или Ключевым носителем являются: USB-токен или его аналоги (рекомендуется), магнитные или иные съемные носители. При использовании Клиентом приложения Mobile-Банкинг для корпоративных клиентов ключ ЭП хранится на Сервере Подписи.

Ключ проверки ЭП – последовательность байтов, однозначно связанная с ключом ЭП, самостоятельно генерируемая Клиентом с использованием средств Системы и предназначенная для проверки корректности ЭП электронного документа, сформированного Клиентом, т.е. несекретная часть ключевой информации, связанная с ключом ЭП с помощью особого математического соотношения и предназначенная для подтверждения подлинности электронной подписи в электронном документе. Ключ проверки ЭП считается принадлежащим владельцу ключевой информации, если он был зарегистрирован установленным порядком.

Mobile-Банкинг для корпоративных клиентов (далее по тексту приложения **Mobile-Банкинг**) – приложение, в котором Клиент может с любого мобильного устройства на платформах iOS и Android формировать, подписывать и отправлять в банк платежные поручения, работать со справочниками корреспондентов и бенефициаров, отслеживать статусы документов, получать выписки по своим счетам за произвольный период, обмениваться с банком письмами. Приложение Mobile-Банкинг позволяет корпоративным клиентам осуществлять доступ к системе «iBank 2» и ограниченный функционал через мобильные устройства.

Серверная подпись - механизм подписи документов из мобильного приложения Mobile-Банкинг усиленной неквалифицированной электронной подписью, ключ которой хранится в Банке на Сервере Подписи.

Ключ серверной подписи- это ключ электронной подписи Клиента, используемый для подписи документов исключительно из мобильного приложения Mobile-Банкинг.

Код подтверждения – уникальный набор символов, состоящий из 6 или 8 цифр, направляемый Клиенту Системой «iBank 2» посредством sms или email сообщения и служащий для подтверждения произведенной операции или действия в системе «iBank 2».

Сертификат ключа проверки ЭП сотрудника Клиента (Сертификат ключа проверки ЭП) – документ на бумажном носителе, содержащий данные Клиента, сведения о владельце ключа - сотруднике Клиента, идентификатор ключа проверки ЭП, сведения о наименовании криптосредств и алгоритмов шифрования, содержащий представленный в шестнадцатеричном виде ключ проверки ЭП; содержит информацию о его назначении и области применения. Сертификат удостоверяется подписями уполномоченных лиц Сторон и заверяется оттиском печати Клиента и Банка. Форма Сертификата (Приложение № 2 к настоящим Правилам) формируется автоматически программными средствами Системы «iBank 2» в процессе генерации Клиентом ключей ЭП.

Носители ключевой информации (ключевые носители) – физический носитель, на котором записан и хранится ключ ЭП. В качестве ключевых носителей могут выступать:

– персональный аппаратный криптопровайдер (рекомендуется);

– магнитные или иные съемные носители, содержащие ключевую информацию.

Клиенту не предоставляется возможность одновременного использования персонального аппаратного криптопровайдера и магнитного или иного съемного носителя. При регистрации в Системе «iBank 2» Клиент самостоятельно определяет тип носителя ключевой информации. Для повышения безопасности пользования Системой «iBank 2» Банк рекомендует Клиенту пользоваться персональным аппаратным криптопровайдером.

Персональные аппаратные криптопровайдеры (криптопровайдеры) – носители ключевой информации для защищенного хранения ключей ЭП, использование которых делает принципиально невозможным хищение ключей ЭП, используемых при работе в Системе «iBank 2». К таким носителям относится USB-токен или его аналог.

USB-токен - разновидность персональных аппаратных криптопровайдеров. Это аппаратное USB-устройство, которое объединяет в компактном пластиковом корпусе USB-картридер и карточный криптографический микроконтроллер (криптопровайдер). В системе «iBank 2» используются несколько разновидностей USB-токенов различных производителей:

USB-токен «iBank 2 Key» — это аппаратное USB-устройство в компактном пластиковом корпусе, состоящее из USB-картридера и защищенного карточного микроконтроллера ST19NR66 или ST23YL18 производства компании STMicroelectronics.

Микроконтроллеры сертифицированы на соответствие стандарту ISO/IEC 15408 (common criteria) с уровнем доверия EAL5+.

Тип микроконтроллера зависит от модели исполнения корпуса «iBank 2 Key»:

• исполнение корпуса «A», «M», «B2» — микроконтроллер ST19NR66

• исполнение корпуса «M2», «B» — микроконтроллер ST23YL18

В микроконтроллере при производстве масочным методом «прошита» карточная операционная система «Магистра» (разработчик ООО «Смарт-Парк»). В составе операционной системы содержится СКЗИ, сертифицированное ФСБ РФ по классу КС2.

В составе микроконтроллера ST19NR66 содержится СКЗИ «ФОРОС. Исполнение №1» (разработчик ООО «СмартПарк»), сертифицированное ФСБ РФ по классу КС2. Сертификат ФСБ РФ рег. № СФ/124-2151 от 03.06.2013 г.

В составе микроконтроллера ST23YL18 содержится СКЗИ «Криптомодуль С23» (разработчик ООО «СмартПарк»), сертифицированное ФСБ РФ по классу КС2. Сертификат ФСБ РФ рег. № СФ/114-2312 от 31.12.2013 г.

USB-токен «Рутокен ЭЦП 2.0» - основу составляет современный защищенный микроконтроллер и встроенная защищенная память, в которой безопасно хранятся данные пользователя: пароли, ключи шифрования и подписи, сертификаты и т.д.

В составе микроконтроллера содержится СКЗИ, сертифицированное ФСТЭК и ФСБ РФ:

• Сертификат ФСТЭК № 2592 от 19.03.2012 г. – действителен до 19.03.2018г.

• Сертификат ФСБ РФ рег. № СФ/124-2771 от 25.12.15 г. – действителен до 25.12.2018г.

В системе «iBank 2» поддерживается работа USB-токенов «Рутокен ЭЦП 2.0» в специальной конфигурации, предназначенной для использования исключительно в системе «iBank 2».

USB-токен «MS_KEY K» — это аппаратное USB-устройство в компактном пластиковом корпусе, состоящее из USB-картридера и защищенного карточного микроконтроллера NXP P5CC081. Разработчиком устройства является компании «Multisoft». «MS_KEY K» строится на базе карточного микроконтроллера NXP P5CC081 с операционной системой «Вигрид» (VIGRID – Verification Interoperability GRID) версии 1.0. Устройство «MS_KEY K» сертифицировано как СКЗИ по классам КС1 и КС2 и имеет сертификат соответствия ФСБ РФ № СФ/124-2211.

OTP-токен (устройство для генерации одноразовых паролей, с использованием алгоритмов: алгоритм с синхронизацией по событию и использованием DES/3DES для вычисления одноразового пароля; собственный патентованный алгоритм ActivIdentity с синхронизацией по времени и событию).

Хеш-функция — определенный математический способ проверки целостности электронных документов, результат которого изображается в виде последовательности шестнадцатеричных цифр. Реализованный в Системе алгоритм вычисления хеш-функции соответствует стандарту ГОСТ Р 34.11-94.

Корректная ЭП — электронная подпись электронного документа, дающая положительный результат её проверки средствами Системы «iBank 2» с помощью ключа проверки ЭП.

Проверка ЭП ЭД – проверка соотношения, связывающей электронной подписи под этим электронным документом и ключом проверки ЭП Клиента. Если рассматриваемое соотношение оказывается выполненным, то ЭП признается корректной, а сам электронный документ – подлинным. В противном случае, электронный документ считается измененным, а ЭП под ним - недействительной (некорректной).

Подлинность ЭД – свойство ЭД, означающее, что данный ЭД создан в Системе «iBank 2» Клиентом без отступлений от принятой технологии. Электронный документ считается подлинным, если он был, с одной стороны, должным образом оформлен, заверен (подписан) ЭП Клиента и передан на обработку, а с другой, был принят к исполнению. Свидетельством того, что ЭД принят Банком к исполнению, является значение «доставлен» в строке статуса соответствующего документа в Клиентском модуле Системы «iBank 2».

Целостность ЭД - свойство ЭД, характеризующее отсутствие каких-либо изменений в ЭД после его создания Клиентом и заверения принадлежащей ему ЭП.

Авторство ЭД – свойство ЭД, определяющее принадлежность ЭП конкретному физическому лицу - участнику электронного документооборота в Системе «iBank 2».

Компрометация ключа ЭП — утрата доверия к тому, что используемые ключи ЭП недоступны посторонним лицам и их использование обеспечивает конфиденциальность информации. К событиям, связанным с компрометацией ключей относятся, включая, но не ограничиваясь, следующие события:

- утрата Носителей ключевой информации или иных носителей ключа, в том числе с последующим их обнаружением, а также утрата контроля за доступом к мобильному устройству;
- увольнение сотрудников, имевших доступ к Носителям ключевой информации;
- утрата ключей от сейфа (нарушение целостности печатей на сейфах, если используется процедура опечатывания сейфов) в момент нахождения в нем Носителей ключевой информации;
- временный доступ посторонних лиц к Носителям ключевой информации;
- несанкционированный удаленный доступ к ключевой информации, хранящейся на носителе, копирование, либо модификация криптографических ключей посредством линий связи (телекоммуникаций), электронных вычислительных сетей или возникновение подозрений на утечку информации или ее искажение в системе конфиденциальной связи;
- обнаружение на персональном компьютере (с использованием которого осуществляется доступ в систему «iBank 2») или на носителе ключевой информации постороннего (вредоносного) кода;
- иные обстоятельства, когда нельзя достоверно установить, что произошло с Носителями ключевой информации, и прямо или косвенно свидетельствующие о наличии возможности несанкционированного доступа к Системе неуполномоченными лицами.

АБС Банка – Автоматизированная банковская система Банка (далее - **АБС Банка**).

Криптографическая устойчивость - устойчивость криптографического алгоритма к его криптоанализу, в том числе проводимому злоумышленником с целью получения доступа к ключу ЭП, созданному с использованием данного алгоритма.

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

Конфиденциальность информации - обязательное для выполнения лицом, получившим доступ к определённой информации, требование не передавать такую информацию третьим лицам без согласия её обладателя.

Идентификация Клиента – процесс подтверждения прав Клиента на выполнение определенных действий в Системе «iBank 2» согласно перечню прав Клиента, установленных в системе, и предоставления прав на выполнение данных действий.

Аутентификация Клиента – процесс проверки принадлежности Клиенту предъявленных им идентификаторов (пароли, ключи проверки ЭП); подтверждение подлинности Клиента.

Блокировочное слово – словесный пароль, конфиденциальный для всех кроме уполномоченных лиц Банка и Клиента, вводимый Клиентом в Систему «iBank 2» при регистрации в Системе и хранящейся в ней. Блокировочное слово используется в целях мгновенного дистанционного оповещения Клиентом уполномоченного сотрудника Банка о необходимости блокировки ключей ЭП Клиента.

Уполномоченные службы Банка – подразделения Банка, осуществляющие техническое и организационное взаимодействие с Клиентом в рамках его обслуживания по Системе «iBank 2».

SSL-соединение – соединение с применением криптографического протокола, который обеспечивает установление безопасного соединения между Клиентом и сервером.

IP-адрес - уникальный сетевой адрес узла в компьютерной сети Интернет, построенной по протоколу IP. В рамках настоящего Договора под IP-адресом понимаются только IP-адреса, обладающие глобальной уникальностью адреса (так называемые «реальные», прямые, публичные, общественные IP-адреса), предоставленные (назначенные) Клиенту его провайдером услуг Интернет в рамках заключенных между ними договорных отношений.

1.5. ПРЕДМЕТ ДОГОВОРА

1.5.1. Клиент и Банк (по тексту возможно – Стороны) договариваются об обмене документами в электронной форме, подписанными электронной подписью (ЭП), осуществляемом в соответствии с «Регламентом банковского обслуживания с применением Системы «iBank 2»» (далее – Регламент) (Приложение №5 к настоящим Правилам) в порядке и на условиях, установленных настоящим Договором.

1.5.2. Стоимость услуг, оказываемых Банком в рамках настоящего Договора, определяется в соответствии с Тарифами Банка, действующими на момент оказания услуги.

1.5.3. Клиент и Банк признают, что используемые во взаимоотношениях Сторон документы, подписанные электронной подписью (ЭП) (в том числе с использованием механизма серверной подписи), подготовленные и переданные одной Стороной другой Стороне с помощью программного обеспечения Системы «iBank 2», а также прикреплённые к созданным в Системе письмам изображения документов в виде файлов (в форматах jpeg, pdf, tiff, rtf, документы MS Office), эквивалентны документам на бумажном носителе и имеют юридическую силу наравне с документами, подписанными должностными лицами Сторон и скрепленными печатью (в случае наличия таковой). Использование документов в электронной форме не исключает возможность использования документов на бумажном носителе.

1.5.4. Электронные документы подготавливаются и обрабатываются с помощью программного обеспечения Системы «iBank 2», в том числе приложения Mobile-Банкинг, в течение рабочего времени Банка. На время перерывов в функционировании Системы «iBank 2» обслуживание Клиента посредством Системы прекращается. При неработоспособности Системы, а также при приостановлении передачи электронных документов посредством Системы все документы представляются Клиентом в Банк на бумажном носителе.

1.5.5. Стороны доверяют используемому программному обеспечению Системы «iBank 2». Стороны признают, что используемое в Системе «iBank 2» программное средство криптографической защиты информации (далее – **СКЗИ**), сертифицированное ФСБ РФ на соответствие российским стандартам по защите информации, не составляющей государственной тайну, достаточно для подтверждения подлинности и целостности ЭД, а также для обеспечения защиты ЭД от несанкционированного доступа.

1.5.6. Система «iBank 2» не предусматривает создание организационно выделенного удостоверяющего центра. Выполнение функций по генерации ключей и изготовлению сертификатов ключей, приостановлению и аннулированию сертификатов ключей распределяется в соответствии с условиями настоящего Договора.

2. ПРАВА И ОБЯЗАННОСТИ СТОРОН

2.1. Банк обязуется:

2.1.1. После получения оплаты комиссии за подключение к Системе «iBank 2» провести совместно с Клиентом регистрацию ключей ЭП в порядке, установленном настоящими Правилами.

2.1.2. Принимать к исполнению полученные по Системе «iBank 2» электронные документы, перечисленные в Приложении №3 к настоящему Договору, оформленные и подписанные в соответствии с требованиями настоящего Договора и Регламента. Банк не принимает к исполнению электронные документы, оформленные с нарушением требований Регламента.

2.1.3. Осуществлять операции по счету Клиента в пределах остатка денежных средств на его счете на начало операционного дня, за исключением случаев предоставления Банком овердрафта по счету Клиента или осуществления встречных платежей, условия которых оговариваются отдельными соглашениями Сторон.

2.1.4. Предоставлять Клиенту информацию по видам сообщений, которые Клиент передает в Банк и получает из Банка по Системе «iBank 2» в соответствии с Приложением №3 к Договору.

2.1.5. Информировать Клиента о совершении каждой операции с использованием ключа(ей) электронной подписи Клиента путем направления Клиенту соответствующего уведомления тем способом, который указан Клиентом в Приложении № 8 к настоящему Договору.

2.1.6. Консультировать персонал Клиента по вопросам обслуживания Системы «iBank 2» на стороне Клиента.

2.1.7. Обеспечивать защиту от несанкционированного доступа в Систему «iBank 2» в пределах своей компетенции, установленной настоящими Правилами, и сохранять конфиденциальность информации по счетам Клиента.

2.1.8. Сообщать Клиенту о ставших известными Банку попытках несанкционированного доступа к Системе «iBank 2», если это затрагивало операции Клиента, в срок не позднее 1 одного рабочего дня с момента обнаружения таких фактов.

2.1.9. Предоставлять Клиенту возможность использования дополнительных услуг (по мере их введения в Банке) в рамках Системы «iBank 2».

2.1.10. В случае расторжения Договора обеспечить своевременную блокировку и исключение учетной записи Клиента и его ключей ЭП, в том числе ключа серверной подписи из хранилища, в Системе «iBank 2».

2.1.11. Обеспечить возможность направления Клиентом в порядке, предусмотренном настоящим договором, уведомления об утрате или использовании без согласия Клиента носителя ключевой информации путем блокирования/ исключения/ внеплановой замены ключа ЭП по форме Приложения № 4.

2.1.12. Без предварительного уведомления Клиента приостановить или прекратить использование ЭП Клиента на основании полученного от Клиента извещения и/или уведомления, направленного в соответствии с подпунктами 2.3.8.и 2.3.9.

2.1.13. Запросить у Клиента подтверждение платежа, созданного и подписанного с использованием приложения Mobile-Банкинг, посредством направления SMS-сообщений с кодом подтверждения.

2.2. Банк имеет право:

2.2.1. Взимать с Клиента за обслуживание в Системе «iBank 2» и оказание иных услуг в рамках настоящего Договора комиссию в соответствии с действующими на момент оказания услуг Тарифами Банка в порядке предварительно данного согласия на списания денежных средств с имеющихся счетов Клиента в Банке.

2.2.2. В одностороннем порядке вносить изменения в настоящие Правила, изменять Тарифы на обслуживание в Системе «iBank 2» с предварительным уведомлением Клиента за 10 (Десять) календарных дней путем размещения информации в порядке, предусмотренном разделом 9 настоящих Правил. В случае неполучения в течение указанного срока письменного возражения со стороны Клиента относительно изменения Тарифов, новые Тарифы считаются согласованными с Клиентом. Несогласие Клиента с изменениями Правил и/или Тарифов, оформленное письменно и направленное в Банк в сроки, определенные настоящим пунктом, является основанием для расторжения Договора в день получения такого уведомления.

2.2.3. Отказывать Клиенту в приеме электронных документов после предварительного уведомления Клиента, в том числе с использованием Системы, в случае непредставления запрашиваемых документов и/или признания Банком сделок Клиента подозрительными.

В таком случае Банк принимает от Клиента только надлежащим образом оформленные расчетные документы на бумажном носителе.

2.2.4. В случае наличия подозрений в компрометации ключа ЭП Клиента, в одностороннем порядке блокировать действие ключа ЭП с уведомлением об этом Клиента в течение 1 рабочего дня со дня принятия такого решения с использованием средств связи, обеспечивающих фиксирование отправления. При этом обслуживание Клиента через Систему «iBank 2» приостанавливается. Снятие блокировки либо исключение ключа ЭП Клиента в случае подтверждения факта компрометации ключа осуществляется в порядке, установленном Регламентом.

2.2.5. Банк вправе без предварительного уведомления Клиента приостановить или прекратить использование ЭП Клиента в случае нарушения Клиентом порядка использования ключа ЭП Клиента, а также не исполнения Клиентом своих обязательств по представлению достоверной информации для связи с ним, предусмотренные пунктом 2.3.12. настоящих Правил. Приостановление или прекращение использования Клиентом ЭП Клиента не прекращает обязательств Клиента и Банка, возникших до момента приостановления или прекращения указанного использования.

2.2.6. Банк имеет право запретить анонимную регистрацию в мобильном приложении Mobile-Банкинг.

2.2.7. Осуществлять иные права, установленные настоящими Правилами и приложениями к ним.

2.3. Клиент обязан:

2.3.1. Соблюдать требования Регламента и Руководства пользователя Системы «iBank 2» (далее – Описание), размещенного по адресу: https://ibank2.newbank.ru/docs/Corporate_Internet-Banking_Guide.pdf, в редакциях, действующих на дату осуществления операции в Системе «iBank 2».

2.3.2. Представить в Банк Сертификат ключа проверки ЭП сотрудника Клиента в Системе «iBank 2», оформленный в порядке, установленном Регламентом, с указанием даты его составления, сведений о владельце ключа, подписи владельца ключа, заверенный подписями лиц, указанных в карточке с образцами подписей и оттиска печати Клиента и скрепленный печатью Клиента.

2.3.3. Оплачивать подключение к Системе «iBank 2», обслуживание и иные услуги Банка, связанные с использованием Системы «iBank 2» в порядке и на условиях, установленных действующими Тарифами Банка. Клиент обязуется обеспечить наличие средств на своем счете для своевременной оплаты услуг Банка.

2.3.4. Обеспечить конфиденциальность в отношении использования и хранения ключей ЭП/паролей/блокировочного слова/носителей ключевой информации/персональных аппаратных криптопровайдеров/ мобильных устройств, на которых установлено приложение Mobile-Банкинг.

2.3.5. Обеспечивать предоставление права на работу в Системе «iBank 2» только лицам, указанным в предоставленной в Банк карточке образцов подписей и оттиска печати Клиента. Клиент обязан поддерживать соответствие между лицами, уполномоченными распоряжаться средствами на счете Клиента, указанными в карточке с образцами подписей и оттиска печати, и лицами, фактически использующими носители ключевой информации и средства многофакторной аутентификации.

2.3.6. Самостоятельно и за свой счет обеспечивать безопасность и целостность среды исполнения на компьютерах и мобильных устройствах, с которых осуществляется работа в Системе «iBank 2», в том числе обеспечивать защиту от несанкционированного доступа неуполномоченных лиц в Систему «iBank 2» в пределах своей компетенции, обеспечить защиту применяемых аппаратных средств для работы в Системе «iBank 2» от компьютерных вирусов, вредоносного программного обеспечения, в том числе вредоносного кода, несанкционированного удаленного администрирования. Эффективные способы защиты изложены в Памятке клиенту (Приложение № 9). О применении таких способов защиты Клиент обязан сообщать Банку по запросу последнего.

2.3.7. Своевременно обращаться в Банк для блокировки утраченного/украденного OTP-токена в случае пользования соответствующей услугой.

2.3.8. В случае компрометации ключа ЭП Клиент обязан прекратить использование ключа ЭП и немедленно известить в простой письменной форме Банк в порядке, указанном в пункте 5.4. Приложения № 5 и Приложении № 8 к настоящему Договору. Такое извещение по телефону/факсу не влечет никаких правовых последствий, кроме обязанности Банка приостановить использование в Системе «iBank 2» того ключа ЭП Клиента, о компрометации (или подозрении на компрометацию) которого извещен Банк. Извещение дистанционным способом не освобождает Клиента от обязанности представить в Банк заявление по форме приложения № 4 на бумажном носителе в предусмотренный Правилами срок.

2.3.9. В случае утраты ключа ЭП Клиента и(или) его использования без согласия последнего Клиент обязан незамедлительно направить Банку уведомление:

- путем направления в адрес Банка уведомления одним из дистанционных способов, указанных в Приложении № 8 к настоящему Договору. При этом Клиент обязуется в срок не более трех рабочих дней со дня направления уведомления одним из указанных выше способов, представить в Банк заявление по форме Приложения № 4 на бумажном носителе; или

- путем предоставления, непосредственно в Банк уведомления, составленного на бумажном носителе, которое в обязательном порядке должно содержать собственноручные подписи уполномоченных лиц Клиента, указанных в Карточке, и печать Клиента, оттиск которой заявлен в Карточке, а также заявления по форме Приложения № 4. В случае, если Клиент направил уведомление Банку указанным в Договоре способом, в тот период времени, который является нерабочим временем Банка, то поступившее уведомление считается полученным Банком в первый рабочий день Банка, следующий за временем отправки уведомления.

2.3.10. Контролировать соответствие суммы платежа и остатка на начало операционного дня на своем счете в Банке и осуществлять платежи только в пределах этого остатка за исключением случаев предоставления Банком овердрафта по счету клиента или осуществления встречных платежей, условия которых оговариваются отдельными соглашениями сторон.

2.3.11. При уведомлении Банком о смене (обновлении) программного обеспечения осуществлять все необходимые действия для своевременного получения и установки новой версии программы клиентского модуля или обновления имеющейся.

2.3.12. Предоставить Банку достоверную информацию для связи с ним, а в случае ее изменения своевременно предоставить обновленную информацию. Обязанность Банка по направлению Клиенту уведомлений считается исполненной при направлении уведомления в соответствии с имеющейся у Банка информацией для связи с Клиентом.

2.3.13. Сообщать в течение трех банковских дней после получения выписки об ошибочно зачисленных на счет суммах.

2.4. Клиент имеет право:

2.4.1. Получать от Банка организационно-техническую информацию в рамках обслуживания по Системе «iBank 2», в том числе информацию в виде электронных документов в соответствии с Приложением №3 к Договору.

2.4.2. Отзывать платежные поручения по перечислению средств, переданных ранее Банку по Системе «iBank 2», в форме письма свободного формата, содержащего реквизиты отзываемого платежного поручения, с соблюдением порядка, установленного настоящим пунктом.

Отзыв может быть осуществлен не позднее 15 часов московского времени даты, в течение которой было отправлено отзываемое платежное поручение, если документ был отправлен до 15 часов московского времени, и не позднее 15 часов московского времени даты, следующей за датой отправки, в случае, если платежное поручение было передано в Банк после 15 часов московского времени, при условии, что Банк не отправил вышеуказанное поручение в систему расчетов Банка России.

2.4.3. Оформить наряду с ключом ЭП, позволяющим распоряжаться денежными средствами на счете Клиента, ключ ЭП, позволяющий осуществлять только получение информации по счету, но не распоряжаться им (далее – просмотровый ключ). Владельцем просмотрового ключа может быть не только лицо, указанное в карточке образцов подписей и оттиска печати. Клиент несет все риски и убытки, связанные с передачей просмотрового ключа третьим лицам, не указанным в Карточке образцов подписей и оттиска печати.

2.4.4. Клиент имеет право, позвонив в уполномоченную службу Банка, и произнеся блокировочное слово, впредь до иных письменных указаний Клиента, блокировать действующие ключи ЭП Клиента.

3. ПОРЯДОК РАСЧЁТОВ

3.1. За подключение и обслуживание Клиента по Системе «iBank 2», а также оказание иных услуг по настоящему Договору, с Клиента взимается комиссионное вознаграждение (комиссия) в размерах и на условиях, установленных действующими Тарифами Банка, которые доводятся до сведения Клиента в порядке, предусмотренном разделом 9 настоящих правил.

Клиент заранее предоставляет Банку согласие на списание Банком за обслуживание в Системе «iBank 2» и оказание иных услуг в рамках настоящего Договора комиссий и иных платежей в соответствии с действующими на момент оказания услуг Тарифами Банка.

3.2. Факт подключения Клиента к Системе «iBank 2», а также оказания дополнительных услуг в рамках настоящего Договора подтверждается подписанием Сторонами Акта приема-передачи материалов и/или выполненных услуг (Приложение №7 к Договору).

4. КОНФИДЕНЦИАЛЬНОСТЬ ИНФОРМАЦИИ

4.1. Клиенту в рамках настоящего Договора гарантируется конфиденциальность информации о его счетах и совершаемых им операциях в рамках, установленных требованиями действующего законодательства РФ.

4.2. Клиент обязан соблюдать конфиденциальность информации, касающейся Системы «iBank 2».

4.3. Клиент согласен на передачу ему Банком конфиденциальной информации о его счетах и совершаемых им операций по счетам через сеть Интернет или телефонную сеть общего пользования с использованием защищенного SSL-соединения (в случае использования сети Интернет), а также применения дополнительного шифрования передаваемого трафика с использованием российских криптографических алгоритмов.

4.4. Клиент признает используемую в Системе «iBank 2» систему обеспечения целостности передаваемой информации и аутентификации Клиента, достаточной для авторизации зарегистрированного пользователя Системы «iBank 2» и защиты от несанкционированного доступа третьих лиц к банковским счетам Клиента.

4.5. Сведения, содержащиеся в документах, переданных Сторонами друг другу по Системе «iBank 2», персональные электронные адреса, идентификационные параметры, пароли и ключи обеих Сторон, используемые для разграничения доступа, передачи и защиты передаваемой информации, а также материалы работы согласительной экспертной комиссии по разбору споров являются конфиденциальными сведениями. Конфиденциальные сведения не подлежат разглашению третьим лицам, кроме установленного законом порядка.

4.6. Все конфиденциальные сведения хранятся и уничтожаются Сторонами в соответствии с порядком и сроками хранения и уничтожения финансовых документов.

5. ОТВЕТСТВЕННОСТЬ СТОРОН И РАСПРЕДЕЛЕНИЕ УБЫТКОВ

5.1. Стороны несут ответственность за достоверность информации, предоставляемой друг другу в рамках использования Системы «iBank 2».

5.2. Банк не несет ответственности перед Клиентом за фактическое соответствие средств СКЗИ требованиям по их сертификации.

5.3. За неуведомление Банка в соответствии с пунктом 2.3.13. об ошибочно зачисленных на счет Клиента суммах Клиент уплачивает Банку за каждый день просрочки пеню в размере 0.05% от ошибочно зачисленной на счет Клиента суммы.

5.4. В случае несвоевременного извещения или неизвещения Клиентом Банка о компрометации или любом подозрении на компрометацию ключей ЭП Клиента Банк не несет ответственности за исполнение электронного документа, подписанного действующей корректной ЭП. Все связанные в данном случае риски убытков несет Клиент.

5.5. Банк не несет ответственности за исполнение ЭД Клиента, подготовленного и переданного без участия уполномоченных лиц Клиента, указанных в Сертификате ключа проверки ЭП, в том числе при смене указанных лиц и непредоставлении данных изменений в Банк, а также в тех случаях, когда ЭД подготовлен лицом либо лицами, подписи которых имеются в карточках образцов подписей и оттиска печати Клиента, а действительные полномочия указанных лиц сфальсифицированы, если эти ЭД имеют все необходимые для установления их подлинности реквизиты и прошли соответствующий контроль при проверке ЭП Клиента и целостности информации.

5.6. Банк не несет ответственности за ущерб, причиненный Клиенту в результате использования ключа ЭП Клиента и его носителя, а также средств многофакторной аутентификации Клиента третьими лицами, не имеющими права работать с Системой «iBank 2» и давать распоряжения по счету Клиента, а также за последствия воздействия вредоносных программ, в том числе вредоносного кода. Клиент несет полную ответственность за обеспечение сохранности и конфиденциальности ключевой информации, носителей ключевой информации и средств многофакторной аутентификации Клиента, а также за соблюдение мер защиты своего АРМ от вредоносных программ.

5.7. Банк возмещает Клиенту все убытки, связанные с некорректными и неправомочными операциями по счету Клиента, имевшими место в рамках действия данного Договора, произошедшие исключительно по вине Банка, в соответствии с действующим законодательством РФ.

5.8. В случае несвоевременного приостановления Банком операций по счету с использованием Системы «iBank 2», после получения письменного сообщения Клиента о компрометации его ключей, Банк возмещает Клиенту причинённые этим бездействием убытки.

5.9. Стороны не несут ответственности за работу глобальной сети Internet, ее программ и протоколов, а также иных телекоммуникационных каналов и систем связи, включая проводную и мобильную телефонную связь. Убытки, возникшие у одной из Сторон при их полной или частичной

неработоспособности, другой Стороной не возмещаются. Никакие претензии по работоспособности глобальной сети Internet, ее программ и протоколов, иных телекоммуникационных каналов и систем связи Сторонами не принимаются и не рассматриваются.

5.10. Клиент согласен с тем, что Банк не несёт никакой ответственности за ошибки или сбои в работе Системы «iBank 2», если они произошли не по вине Банка (в том числе по вине разработчика или правообладателя Системы), даже если они повлекли убытки Клиента. Указанные убытки Банком не возмещаются.

5.11. Стороны освобождаются от ответственности в том случае, если используемые в Системе алгоритмы не соответствуют техническому описанию Системы «iBank 2», а также при нарушении разработчиком установленных правил изготовления (разработки) Системы. Возникшие в связи с этим убытки Сторонами не возмещаются.

5.12. Стороны освобождаются от ответственности за неисполнение или ненадлежащее исполнение взятых по настоящему Договору обязательств в случае возникновения обстоятельств непреодолимой силы, к которым относятся: массовые беспорядки, забастовки, военные действия, стихийные бедствия, пожары, аварии, повреждение линий связи (в том числе помехи в телефонных сетях связи), действие вирусов в глобальной сети Internet, отключения электроэнергии и компьютерного оборудования, приводящие к невозможности передачи электронных документов, финансовый и (или) экономический кризисы, кризисные явления в банковской системе РФ, вступление в силу законодательных актов, актов федеральных, государственных или муниципальных органов, в том числе судебных, правоохранительных и налоговых органов, судебных приставов-исполнителей и обязательных для исполнения одной из сторон, прямо или косвенно запрещающих указанные в договоре виды деятельности или препятствующие выполнению Сторонами своих обязательств по Договору, а также любые другие обстоятельства, находящиеся за пределами разумного контроля и влекущие за собой невозможность исполнения настоящего Договора.

Сторона, не исполнившая свои обязательства вследствие непреодолимой силы, должна в разумно короткий срок представить другой стороне письменные доказательства, подтверждающие причинную связь данных обстоятельств с негативными результатами (нарушением обязательств), а также письменные доказательства, подтверждающие наличие последствий, их продолжительность и непреодолимость указанных обстоятельств.

5.13. В случае возникновения обстоятельств, указанных в п. 5.12. сторона, подвергшаяся их воздействию, уведомляет об этом другую сторону в письменной форме в течение 2-х дней с использованием средств связи, обеспечивающих фиксирование отправления.

Уведомление должно содержать информацию о характере обстоятельств, оценку их воздействия на выполнение стороной своих обязательств по настоящему договору и предполагаемом сроке возобновления выполнения стороной обязательств по договору.

5.14. Если обстоятельства, указанные в п.5.12 и их последствия будут существовать больше 6 месяцев или если очевидно в момент их возникновения, что они будут существовать более указанного срока, Стороны в кратчайшее время проведут переговоры по выявлению приемлемых альтернативных путей выполнения настоящего договора.

5.15. В связи с тем, что Клиент в любом случае имеет возможность представлять в Банк расчётные документы на бумажном носителе, Банк не несёт ответственность перед Клиентом за несвоевременное представление Клиентом документов в Банк при невозможности передачи документов по Системе «iBank 2», в том числе при её неработоспособности или приостановлении обслуживания Клиента через Систему «iBank 2» Банком в одностороннем порядке.

5.16. Все риски и убытки, связанные с повторным предоставлением электронного документа, переданного ранее Банку в иной форме (электронной или бумажной), полностью несет Клиент. Банк не осуществляет контроль за повторным предоставлением одного и того же расчетного документа Клиентом и не несет ответственности за его повторное исполнение.

6. ОСОБЫЕ УСЛОВИЯ

6.1. Инициатором сеансов связи с Банком всегда является Клиент. Любая просрочка в выполнении Банком своих обязательств, которая произошла из-за отсутствия инициативы Клиента в установлении сеанса связи с Банком, в том числе при выборе Клиентом дополнительных услуг по многофакторной аутентификации и подтверждении направления платежных документов, не влечет за собой ответственности Банка.

6.2. Клиент при подписании ЭД ЭП применяет свои электронные ключи подписи, а Банк при проверке ЭП ЭД - ключи проверки электронной подписи Клиента, являющиеся действующими на момент подписания и передачи ЭД на обработку соответственно.

Ключи (подписи и соответствующий ему ключ проверки) ЭП Клиента являются действующими на момент подписания ЭД, если они зарегистрированы в соответствие с Регламентом, не блокированы и не исключены, а срок их действия не окончен.

Ключи (подписи и соответствующий ему ключ проверки) ЭП Клиента считаются зарегистрированными в Системе «iBank 2» с момента регистрации Банком надлежащим образом оформленного Сертификата ключа проверки ЭП, о чем на бумажном носителе Сертификата уполномоченным сотрудником Банка ставится соответствующая отметка. Сведения о сроке действия ключа ЭП указываются в Сертификате ключа проверки ЭП уполномоченным сотрудником Банка в соответствии с Регламентом и вносятся в данные Системы «iBank 2». Исчисление сроков действия ключа ЭП осуществляется с даты регистрации Сертификата ключа проверки ЭП.

Все процедуры генерации (создания), регистрации, смены, блокировки и исключения ключей ЭП производятся в соответствии с Регламентом.

6.3. Клиент обязан производить смену ключей ЭП Клиента в случаях, установленных Регламентом. Смена/блокировка/исключение ключей ЭП может быть произведена в любой момент по желанию Клиента, в соответствии с действующими Тарифами Банка.

6.4.Обязательства Сторон по ЭД, вытекающие из настоящего Договора, возникают после регистрации ЭП Клиента в Системе «iBank 2».

ЭД имеет силу только в случае если по результатам его проверки Системой «iBank 2» будет установлена корректность ЭП Клиента, подлинность и целостность ЭД.

6.6. На основании требований Федерального Закона от 08.07.2006 №152 ФЗ “О персональных данных” владелец ключа ЭП для возможности обработки Банком его персональных данных, содержащихся в Сертификате ключа проверки ЭП, должен передать Банку письменное согласие на обработку персональных данных. Стороны признают, что без получения такого Согласия Банк не имеет права осуществлять верификацию данных, представленных в Сертификате ключа проверки ЭП, а, следовательно, не имеет возможности зарегистрировать ключи ЭП Клиента в Системе «iBank 2» и надлежащим образом исполнять обязанности по Договору.

7. РАЗРЕШЕНИЕ СПОРОВ

7.1. Все разногласия, споры и конфликтные ситуации (далее – “Споры”), возникающие между Сторонами в рамках выполнения настоящего Договора, разрешаются с учетом взаимных интересов Сторон путем переговоров в порядке, установленном настоящим Договором и «Порядком разрешения споров» (Приложение № 6).

7.2. Банк обязан рассматривать заявления Клиента, в том числе при возникновении Споров, связанных с использованием Клиентом его ключа ЭП, а также предоставить Клиенту возможность получать информацию о результатах рассмотрения заявлений, в том числе в письменной форме по требованию Клиента:

- в случае использования Клиентом ключа ЭП Клиента для осуществления трансграничного перевода денежных средств – в срок не более 60 дней со дня получения заявлений Клиента;
- в остальных случаях – в срок не более 30 дней со дня получения заявлений Клиента.

7.3. В случае возникновения Споров между Клиентом и Банком в рамках настоящего Договора совместным решением обеих Сторон создается согласительная экспертная комиссия из равного количества представителей от каждой Стороны.

7.4. В ходе рассмотрения комиссией Спора о подлинности и/или целостности ЭД, обрабатываемого/обработанного с помощью Системы «iBank 2», подписанного ЭП, каждая Сторона обязана доказать лишь то, что она своевременно и надлежащим образом выполнила обязанности, взятые на себя по Договору. Своевременным и надлежащим выполнением Стороной обязанностей признается соблюдение порядка и условий выполнения действий при обмене документами в электронном виде, закрепленных в Договоре и приложениях к нему.

7.5. Сторона, признанная виновной, возмещает убытки другой Стороне в срок, не превышающий 15 рабочих дней.

7.6. Уклонение какой-либо Стороны настоящего Договора от участия в создании или работе согласительной экспертной комиссии может привести к невозможности ее создания и работы, но не может привести к невозможности урегулирования Спора в судебном порядке. В случае недостижения соглашения Сторон, отсутствия согласия по Спорам и добровольного исполнения решения комиссии, Споры по настоящему Договору передаются на рассмотрение Арбитражного суда г. Москвы.

8. СРОК ДЕЙСТВИЯ ДОГОВОРА И ПОРЯДОК ЕГО ИЗМЕНЕНИЯ И РАСТОРЖЕНИЯ

8.1.Договор вступает в силу со дня принятия (акцепта) Банком предложения (оферты) Клиента о заключении Договора, изложенной в Заявлении о присоединении (Приложение № 1) и действует до конца текущего года. Если ни одна из Сторон не заявит о своем желании расторгнуть Договор не позднее, чем за 10 дней до окончания срока его действия, Договор автоматически продлевается на каждый последующий календарный год.

8.2. Стороны вправе расторгнуть настоящий Договор в одностороннем порядке. Сторона, прекращающая в одностороннем порядке договорные отношения, обязана письменно уведомить об этом другую Сторону не менее, чем за один месяц до его расторжения, с обязательным исполнением всех обязательств, предусмотренных настоящим Договором. Кроме того, Договор расторгается также в случае, указанном в п.2.2.2., Договора, и при расторжении Договора банковского счета.

8.3. Договор в части конфиденциальности информации действителен в течение одного календарного года после расторжения Договора.

8.4. Договор может быть изменен или дополнен письменным соглашением Сторон, за исключением случая, указанного в п.2.2.2. Договора, предоставляющего Банку право вносить изменения в настоящий Договор в одностороннем порядке.

9. РАЗМЕЩЕНИЕ ИНФОРМАЦИИ

9.1. Под размещением информации в настоящих Правилах понимается доведение Банком до Клиентов и других заинтересованных лиц информации, в том числе самих Правил и приложений к ним, Тарифов, форм заявлений, уведомлений и других документов, подлежащих обязательному использованию Банком и Клиентом при исполнении Договора, в местах и способами, установленными настоящими Правилами, обеспечивающими возможность ознакомления с этой информацией Клиентов, в том числе:

- размещение информации, в том числе Правил, приложений к ним, Тарифов, форм документов на Сайте Банка;
- размещение информации на информационных стендах в местах обслуживания клиентов Банка;
- иными способами, позволяющими Клиенту получить информацию.

9.2. Моментом размещения (публикации) Правил, приложений к ним, форм документов и информации считается момент их первого размещения на Сайте Банка.

10. Приложения

10.1. В Договор включены следующие приложения, являющиеся его неотъемлемой частью:

Приложение №1 - Заявление о присоединении к Правилам дистанционного банковского обслуживания клиентов с использованием системы «iBank 2» в КБ «Новый век» (ООО).

Приложение №2 - Сертификат ключа проверки ЭП сотрудника Клиента в Системе «iBank 2».

Приложение №3 - Перечень электронных документов, пересылаемых по Системе «iBank 2».

Приложение №4 - Заявление о блокировке/исключении ключа ЭП Клиента из Системы «iBank 2».

Приложение №5 - Регламент банковского обслуживания с применением Системы «iBank 2»

Приложение №6 - Порядок разрешения споров.

Приложение №7 - Акт приемки материалов и/или выполненных услуг.

Приложение №8 - Соглашением о порядке информирования при работе по Системе «iBank 2».

Приложение №9- Памятка Клиента о возможных угрозах хищения денежных средств с использованием системы «iBank 2» и способах защиты.

Приложение № 10 - Рекомендации по обеспечению безопасности при работе с мобильным приложением "Mobile-Банкинг для корпоративных клиентов"

ОБРАЗЕЦ

ПРИЛОЖЕНИЕ № 1
к Правилам дистанционного банковского обслуживания клиентов с использованием системы «iBank 2» в КБ «Новый век» (ООО)

Заявление о присоединении № _____
к Правилам дистанционного банковского обслуживания клиентов с использованием системы «iBank 2» в КБ «Новый век» (ООО)

(далее - Заявление)

Информация о Клиенте: □ **резидент** □**нерезидент**

Наименование Клиента		
	Полное наименование организации, предприятия (в соответствии с Уставом, Положением)/ФИО индивидуального предпринимателя/физического лица, занимающегося в установленном законодательством РФ порядке частной практикой.	
Адрес местонахождения		
ОГРН/ОГРНИП		
ИНН		
Телефон	**Факс**	**Адрес электронной почты**

Оферта на заключение Договора о дистанционном банковском обслуживании по системе «iBank 2»:

I. Настоящим заявляем/заявляю о присоединении к действующей редакции «Правил дистанционного банковского обслуживания клиентов с использованием системы «iBank 2» в КБ «Новый век» (ООО)» (далее-Правила) в порядке, предусмотренном ст. 428 Гражданского кодекса Российской Федерации, и подтверждаем/подтверждаю, что положения Правил нам/мне известны и разъяснены в полном объеме, включая права, обязанности и ответственность сторон, порядок внесения в Правила изменений и дополнений.

Настоящим Банк заключает с Клиентом в порядке и на условиях, установленных Правилами Договор о дистанционном банковском обслуживании по Системе «iBank 2».

Дата и номер Договора соответствуют дате принятия Банком Заявления о присоединении и номеру Заявления о присоединении.

В случае акцепта Банком в порядке, предусмотренном Правилами, настоящей оферты считать Договор о дистанционном банковском обслуживании по Системе «iBank 2» заключенным с Банком. Клиент согласен с тем, что день направления Банком уведомления об акцепте настоящей оферты является днем заключения Договора о дистанционном банковском обслуживании по Системе «iBank 2», при этом акцепт считается полученным Клиентом в день направления Банком Клиенту сообщения об акцепте.

Настоящим Клиент подтверждает право Банка отказать в акцепте настоящей оферты, при этом Банк не обязан уведомлять Клиента об отказе от акцепта настоящей оферты.

Клиент уведомлен и согласен, что в случае отказа в акцепте настоящей оферты либо отзыва Клиентом настоящей оферты документы, предоставленные Клиентом в Банк, могут быть получены Клиентом в течение 60 (Шестидесяти) календарных дней с момента передачи настоящего Заявления в Банк. По истечении указанного срока документы уничтожаются без уведомления Клиента.

II. Настоящим Клиент подтверждает, что в случае акцепта Банком в порядке, предусмотренном Правилами, настоящей оферты, Клиент:

- полностью и безусловно принимает все условия Правил;
- ознакомлен и согласен с Правилами и Тарифами Банка, в том числе с правом Банка на внесение изменений в Правила и Тарифы и порядком внесения изменений, не имеет возражений против реализации Банком указанного права.

Настоящим Клиент подтверждает право Банка отказать в акцепте настоящей оферты без объяснения причин, при этом Банк не обязан уведомлять Клиента об отказе от акцепта настоящей оферты.

☐ В случае акцепта Банком настоящей оферты прошу предоставить на указанный адрес электронной почты сертифицированные криптобиблиотеки для работы в Системе «iBank 2».

ПЕРЕЧЕНЬ ДОПОЛНИТЕЛЬНЫХ УСЛУГ, ОКАЗЫВАЕМЫХ БАНКОМ ПРИ ОБСЛУЖИВАНИИ КЛИЕНТОВ В СИСТЕМЕ «IBANK 2»

☐ Произвести настройку ПЭВМ Клиента для работы в Системе «iBank 2» специалистами Банка, на территории Банка. Количество ПЭВМ, на которых необходимо провести настройку _____ шт.

☐ Произвести регистрацию Просмотрового ключа ЭП (без права подписи ЭД) в количестве _____ шт.

☐ Подключить сервис работы в Системе «iBank 2» по определенным IP-адресам
(услуга предоставляется в соответствии с Тарифами Банка):

☐ **Да**
☐ **Нет**

Системой «iBank 2» будут приниматься только те ЭД Клиента, которые были направлены с указанного клиентом IP адреса (диапазона IP адресов). Иные ЭД Клиента, приниматься Системой «iBank 2» не будут.

В случае положительного ответа, указать необходимые IP-адреса/диапазон IP-адресов, с которых будет осуществляться взаимодействие с Системой «iBank 2»:

IP-адреса	Диапазоны IP-адресов

☐ Предоставить мне услуги по защите ключа ЭП Клиента (стоимость услуги в соответствие с действующими Тарифами Банка):

☐ **Да**
☐ **Нет**

В случае положительного ответа - указать необходимое Вам количество персональных аппаратных криптопровайдеров:

Тип криптопровайдера	Кол-во, шт.
USB-токен	

☐ Предоставить мне услуги по многофакторной аутентификации с использованием OTP – токена (Стоимость услуги в соответствие с действующими Тарифами Банка):

☐ **Да**
☐ **Нет**

В случае положительного ответа - указать необходимое Вам количество OTP-токенов:

Тип устройства многофакторной аутентификации	Кол-во, шт.
OTP-токен	

Укажите какие функции OTP-токена необходимы Вам для активации в Системе «iBank 2»:

☐ Двухуровневая аутентификация при входе в Систему «iBank 2» (вход в систему будет возможен только при вводе пароля, указанного при регистрации Клиента и одноразового пароля, сгенерированного OTP-токеном).

☐ Подтверждение направляемого платежного документа в Банк (после подписи документа для подтверждения отправки платежного документа в Банк необходимо будет ввести одноразовый пароль, сгенерированный OTP-токеном). Необходимо установление лимита операции, свыше которой потребуется подтверждение платежа.

Сумма лимита (прописью):

руб. 00 коп.

Прошу списать комиссию за выбранные услуги в соответствии с действующими Тарифами Банка:

☐ **с нашего счета № _____;**
☐ **принять наличными в кассу Банка.**

Настоящее Заявление составлено в двух экземплярах. В случае акцепта Банком в порядке, предусмотренном Правилами, настоящей оферты, Клиент обязуется получить самостоятельно или через своего надлежащим образом уполномоченного представителя один экземпляр Заявления с отметкой Банка об акцепте.

1. РЕКВИЗИТЫ БАНКА:

Полное фирменное наименование на русском языке: **Коммерческий Банк «Новый век» (Общество с Ограниченной Ответственностью)**
Сокращенное фирменное наименование на русском языке: **КБ «Новый век» (ООО)**
Полное фирменное наименование на английском языке: **«New Century Bank» Limited**
Сокращённое фирменное наименование на английском языке: **«NC Bank» Ltd**.
Лицензия на осуществление банковских операций **№ 3417**, выдана **29 августа 2002** года Банком России
Адрес места нахождения: **115093, г. Москва, ул. Щипок, д.4, стр.1** БИК: **044525517**
Корр. счет: **30101810845250000517 в Главном управления Центрального банка Российской Федерации по Центральному федеральному округу**
ОГРН: 1027700047715 ИНН: 7744002652 ОКВЭД: **64.19 ОКПО:** 59055502 **ОКАТО:** 45286560000 **ОКОГУ:** 15001 **КПП:** 775001001

Руководитель/представитель Клиента,_____

действующий на основании _____

_____ _____
(подпись) *ФИО*

Главный бухгалтер _____ _____
(подпись) *ФИО*

МП.

Отметки Банка:
Заявление-оферта принято « _____ »_____20 _____г.

Должность сотрудника Банка _____ _____
(подпись) *ФИО*

Договор банковского счета №_____от «____» _____20 ____ г.
Руководитель Подразделения

_____ / _____ / _____/ _____
(подпись) (ФИО) (должность) (дата)

ОТМЕТКА БАНКА ОБ АКЦЕПТЕ ОФЕРТЫ КЛИЕНТА:
Оферта Клиента об открытии Договора о дистанционном банковском обслуживании по системе «iBank 2» акцептована, Договор о дистанционном банковском обслуживании по системе «iBank 2» заключен на условиях, изложенных в Правилах.
Дата акцепта « _____ »_____20 __ г.
*В акцепте отказано « _____» _____ 20 __г.

Представитель Банка _____

_____ /_____ МП.
Подпись *ФИО*

*Заполняется в случае отказа Банка в акцепте заявления-оферты

ОТМЕТКА КЛИЕНТА/ПРЕДСТАВИТЕЛЯ КЛИЕНТА О ПОЛУЧЕНИИ 2-ГО ЭКЗЭМПЛЯРА ЗАЯВЛЕНИЯ

Второй экземпляр получил
_____ _____

(Фамилия, имя, отчество уполномоченного лиц Клиента) (Подпись)

Дата « _____» _____201_ г.

От Клиента:
Генеральный директор Главный бухгалтер

_____/_____/ _____/_____/
м.п.

ОТМЕТКИ БАНКА

Дата принятия заявления "___" _ _ _ _ _ 20 __г. Структурное подразделение:	Настройка доступа осуществлена "___"_____20__г. Ответственный исполнитель, осуществляющий настройку в Системе «iBank 2»:
Уполномоченный сотрудник Банка: _____/_____/ подпись с расшифровкой	_____/_____/ подпись с расшифровкой

От Банка:

Зам. Председателя Правления

_____/Е.Н. Пономарева/
Главный бухгалтер

_____/Л.М. Клементьева/
м.п.

От Клиента:

Генеральный директор

_____/_____/
Главный бухгалтер

_____/_____/
м.п.

ПРИЛОЖЕНИЕ №2
к Правилам дистанционного банковского обслуживания клиентов с использованием системы «iBank 2» в КБ «Новый век» (ООО)

ОБРАЗЕЦ

СЕРТИФИКАТ КЛЮЧА ПРОВЕРКИ ЭП
СОТРУДНИКА КЛИЕНТА В СИСТЕМЕ «IBANK 2»

Сертификат ключа ЭП сотрудника Клиента в Системе «iBank 2» автоматически формируется из клиентской части Системы «iBank 2» в момент осуществления Клиентом генерации ключей ЭП.

От Банка:

Зам. Председателя Правления

_____/Е.Н. Пономарева/

Главный бухгалтер

_____/Л.М. Клементьева/
м.п.

От Клиента:

Генеральный директор

_____/_____/

Главный бухгалтер

_____/_____/
м.п.

ПРИЛОЖЕНИЕ №3
к Правилам дистанционного банковского обслуживания клиентов с использованием системы «iBank 2» в КБ «Новый век» (ООО)

ОБРАЗЕЦ

ПЕРЕЧЕНЬ ЭЛЕКТРОННЫХ ДОКУМЕНТОВ, ПЕРЕСЫЛАЕМЫХ ПО СИСТЕМЕ «IBANK 2»

Виды сообщений, которые Клиент передает в Банк по Системе «iBank 2»:

№пп	*Наименование ЭД*	*Вид сообщения*
1	*2*	*3*
1	**Платежное поручение** по перечислению рублевых средств;	Формализованное
2	**Заявление об отказе от акцепта** по перечислению рублевых средств;	Формализованное
4	**Заявление** на перевод средств в иностранной валюте;	Формализованное
6	**Поручение** на продажу иностранной валюты за рубли;	Формализованное
7	**Поручение** на покупку иностранной валюты за рубли;	Формализованное
8	**Поручение** на конвертацию иностранной валюты (покупка одной валюты за другую);	Формализованное
9	**Поручение** на обратную продажу иностранной валюты;	Формализованное
10	**Заявление** на перевод иностранной валюты с транзитного счета на текущий;	Формализованное
12	**Запрос** на получение выписки по рублевым счетам клиента, включая остатки по счетам и приложения к выписке;	Формализованное
13	**Запрос** на получение выписки по валютным счетам клиента, включая остатки по счетам и приложения к выписке;	Формализованное
14	**Документы валютного контроля** (паспорт сделки (контракты, кредитные договора), справка о валютных операциях, справка о подтверждающих документах, корректирующие справки о валютных операциях и подтверждающих документах)	Формализованное
15	**Информационные и сопроводительные письма (к информации для осуществления валютных операций)**	Формализованное
16	**Информация для осуществления валютных операций в виде прикреплённых файлов (**договора, контракты, соглашения, грузовые таможенные декларации (ГТД), товарно-транспортные накладные (ТТН), акты приёма-сдачи работ (услуг), счета, инвойсы, иные документы, являющиеся основанием для проведения валютных операций, указанные в части 4 статьи 23 Федерального закона № 173-ФЗ и пунктах 5.1 – 5.1.5, 9.1.1 – 9.1.4 Инструкции Банка России от 04.06.2012 г. № 138-И);	Свободный формат
17	**Запрос** по вопросам расчетов и другим видам услуг, предоставляемых Банком (в соответствии с адресной книгой).	Свободный формат

Виды сообщений, которые Клиент получает по Системе «iBank 2» из Банка:

№пп	*Наименование ЭД*	*Вид сообщения*
1	*2*	*3*
1	**Выписка** по рублевым счетам Клиента, включая остатки по счетам и приложения к выписке;	Формализованное
2	**Выписка** по валютным счетам Клиента, включая остатки по счетам и приложения к выписке;	Формализованное
3	**Прочие сообщения (в т.ч. с прикреплёнными файлами).**	Свободный формат

Остальные документы изготавливаются и представляются в Банк только на бумажном носителе.
Перечень принимаемых и передаваемых документов в электронной форме может быть изменен Банком в одностороннем порядке.

От Банка:
Зам. Председателя Правления

_____/Е.Н. Пономарева/
Главный бухгалтер

От Клиента:
Генеральный директор

_____/_____/
Главный бухгалтер

_____/Л.М. Клементьева/
м.п.

_____/_____/
м.п.

Приложение № 4
к Правилам дистанционного банковского обслуживания клиентов с использованием системы «iBank 2» в КБ «Новый век» (ООО)

ОБРАЗЕЦ

ЗАЯВЛЕНИЕ О БЛОКИРОВКЕ / ИСКЛЮЧЕНИИ/ ВНЕПЛАНОВОЙ СМЕНЫ КЛЮЧА ЭП КЛИЕНТА ИЗ СИСТЕМЫ «IBANK 2».

_____,
(*наименование предприятия, организации*)

именуемое по договору «Клиент», в лице _____
(*должность, фамилия, имя, отчество*)

- просит Банк с «____» _____ 20___ г. исключить ключ ЭП Клиента, со следующим идентификатором ключа проверки ЭП Клиента: _____, и исключить указанный ключ проверки ЭП из базы данных Системы «iBank 2». Соответствующий ему ключ ЭП Клиента утрачивает силу для дальнейшего применения в Системе «iBank 2» с вышеуказанной даты.

- просит Банк с «____» _____ 20___ г. на период по _____ блокировать ключ ЭП Клиента, со следующим идентификатором ключа проверки ЭП Клиента: _____, в связи с _____.

  Соответствующий ему ключ ЭП Клиента временно утрачивает силу для дальнейшего применения в Системе «iBank 2» с вышеуказанной даты на указанный период.

- Просит Банк произвести внеплановую смену ключей ЭП (дополнительная генерация ключей ЭП Клиента).

_____
(*ФИО, подпись руководителя организации*)

_____
(*ФИО, подпись главного бухгалтера*)

м.п.

Отметки банка:

Дата принятия уведомления: «____» _____ 20 __г.

Время принятия уведомления: ____:____ по московскому времени.

Ответственный исполнитель, осуществляющий настройку в Системе «iBank 2»:

_____/_____/
подпись с расшифровкой

От Банка:

Зам. Председателя Правления

_____/Е.Н. Пономарева/

Главный бухгалтер

_____/Л.М. Клементьева/
м.п.

От Клиента:

Генеральный директор

_____/_____/

Главный бухгалтер

_____/_____/
м.п.

Приложение №5
к Правилам дистанционного банковского обслуживания клиентов с использованием системы «iBank 2» в КБ «Новый век» (ООО)

РЕГЛАМЕНТ БАНКОВСКОГО ОБСЛУЖИВАНИЯ С ПРИМЕНЕНИЕМ СИСТЕМЫ «iBank 2»

1. ВВЕДЕНИЕ

1.1. Система «iBank 2» предназначена для подготовки, приема-передачи по линиям связи, учета и предварительной обработки платежных документов Клиентов Банком. Она построена на основе технологии обмена информацией по телекоммуникационной сети, обеспечивающей конфиденциальность, надежность и достоверность передачи информации, установление подлинности отправителя, проверку целостности и авторства документа.
1.2. Настоящий документ устанавливает порядок подключения Клиента к Системе «iBank 2» и регламентирует передачу и обработку видов сообщений, указанных в Приложении №3.
1.3. Для пользования Системой Клиент должен иметь ПЭВМ (минимальные требования к компьютеру: процессор 900 МГц, 512 Мбайт оперативной памяти, операционная система Microsoft Windows XP и выше), подключённый к Глобальной сети Internet, и использовать только Web-браузер с поддержкой JRE 1.8.0 и выше. В качестве Web-браузера должен использоваться Microsoft Internet Explorer версии 8 и выше, Firefox 50 и выше, Chrome 44 и выше. Надлежащая работа Системы при использовании иных Web-браузеров не гарантируется разработчиком.
1.4. При работе в Системе Клиент обязан руководствоваться Правилами дистанционного банковского обслуживания с использованием системы «iBank 2» в КБ «Новый век» (ООО), данным Регламентом и Руководством пользователя Системы «iBank 2» для клиентов – юридических лиц (именуемым далее – Описание), размещенном в сети Интернет адресу https://ibank2.newbank.ru/docs/Corporate_Internet-Banking_Guide.pdf, а также Обзором приложения для мобильных устройств, размещенным по адресу https://ibank2.newbank.ru/docs/Corporate_Mobile_Banking_Guide_Review.pdf. Описание является составной частью Договора. В случае противоречий между Описанием и Договором применяются нормы последнего.

2. ОБЩИЕ ПОЛОЖЕНИЯ

2.1. Система позволяет Клиенту вводить, редактировать, удалять, подписывать и отправлять в Банк ЭД, перечисленные в Приложении №3 к настоящему Договору, а также Сторон просматривать информацию о состоянии своих счетов в Банке и получать выписки по счетам в электронном виде. Функционал приложения Mobile-Банкинг может быть ограничен только разработчиком Системы «iBank 2» АО «БИФИТ».
2.2. Электронные платежные документы, применяемые в Системе «iBank 2», эквивалентны бумажным платежным документам, используемым в соответствии с нормативными актами Центрального банка Российской Федерации, и являются основанием для осуществления операции по счету Клиента.
2.3. Стороны признают, что:
- используемые в Системе «iBank 2» системы защиты информации (системы разграничения доступа, средства контроля целостности передаваемой информации, средства криптографической защиты и т.д.), механизмы доставки/приема, обработки и хранения электронных сообщений являются достаточными для обеспечения надежной и эффективной работы Системы «iBank 2», подтверждения авторства и подлинности информации, содержащейся в получаемых электронных документах, а также для защиты информации, циркулирующей внутри Системы, от несанкционированного доступа. Для расшифровки электронного документа и экспертной проверки электронной подписи под ним в Системе «iBank 2» используется программное обеспечение, реализующее и использующее сертифицированные средства криптографической защиты информации (СКЗИ).
- Банк не гарантирует невозможность несанкционированного доступа к Системе третьими лицами, а Клиент принимает на себя соответствующие риски;
- если после заверения ЭД электронной подписью этот ЭД был изменён, то эта ЭП становится некорректной, то есть её проверка даёт отрицательный результат;
- подделка ЭП, то есть создание корректной ЭП ЭД, направленного Клиентом, невозможна без знания ключа ЭП и пароля;
- Клиент уведомлен, что Система не предусматривает подписание Банком исходящих от него документов, и несет связанные с этим риски. При обмене информацией для ее шифрования используется SSL-протокол.
2.4. ЭД/ЭПД порождает обязательства Сторон по настоящему Договору, если он инициирующей Стороной должным образом оформлен (документ содержит все реквизиты платежного (расчетного) документа, установленные банковскими правилами), ЭП под документом является подлинной и действующей и содержит необходимой количество групп подписей, передан на обработку, а принимающей Стороной принят к исполнению. Свидетельством того, что ЭД/ЭПД принят Банком к исполнению, является значение “доставлен” в строке статуса соответствующего документа в клиентской части Системы «iBank 2».
2.5. Готовность Сторон к работе по Системе «iBank 2» оформляется заполнением Сторонами Акта приемки материалов и/или выполненных работ, а также подписанием Сторонами Сертификата ключа ЭП.
2.6. Банк оставляет за собой право использовать записи и данные журналов событий и аудита средств защиты, установленных, как в контуре Системы «iBank 2», так и вне её предела, а также документов, направленных Клиентом по Системе «iBank 2» для доказательного разрешения споров, возникших в рамках данного Договора.

2.7. Ключ ЭП записывается Системой в зашифрованном виде на персональный аппаратный криптопровайдер или в файл KEYS.DAT. Ключ ЭП должен храниться на персональном аппаратном криптопровайдере или на съёмном носителе (дискета, флеш-накопитель и т.п.) в виде файла KEYS.DAT, именуемым - «ключевой носитель», и используется уполномоченными лицами Клиента в целях подписи ЭД/ЭПД, подготовленных с помощью Системы «iBank 2».
Ключ ЭП, сгенерированной Клиентом в приложении Mobile-Банкинг, хранится в зашифрованном виде на Сервере Подписи Банка.
2.8. Ключ проверки ЭП после регистрации Клиента, хранится Банком в базе данных Системы «iBank 2».
2.9. Архив входящих и исходящих ЭД хранится Банком в базе данных Системы «iBank 2».
2.10. Проверка подлинности ЭП под ЭД осуществляется в автоматическом режиме программными средствами Системы «iBank 2».

3. ОБЯЗАННОСТИ СТОРОН

3.1. В рамках настоящего Регламента Банк обязуется:
3.1.1. Принимать от Клиента на условиях настоящего Договора по электронным каналам связи должным образом оформленные электронные документы с контролем их целостности и авторства.
3.1.2. Осуществлять обработку ЭД только с подлинной ЭП лиц, идентификатор ключа проверки ЭП которых соответствует данным, указанным в Сертификате ключа проверки ЭП.
3.1.3. Осуществлять обработку и исполнение полученных ЭД Клиента в строгом соответствии с установленными законодательством РФ и нормативными актами Банка России нормами, техническими требованиями и инструкциями.
3.1.4. Предоставлять Клиенту информацию о результатах проверки и обработки принятого ЭД Клиента или отказе в приеме на обработку с указанием причин.
3.1.5. По результатам обработки и исполнения ЭД Клиента, а также по мере совершения иных операций по счету, в течение следующего банковского дня после совершения операции, подготавливать и предоставлять Клиенту в ответ на его запрос выписки по счету (счетам) с указанием основных реквизитов платежного документа, на основании которого совершена операция по счету.
3.1.6. Своевременно информировать Клиента об изменениях порядка осуществления обработки ЭД и другой информации посредством направления ЭСИД по Системе «iBank 2». Оказывать консультационные услуги Клиенту по вопросам технической и организационной поддержки в рамках оказания услуг с использованием Системы «iBank 2», а также информировать и оказывать консультационные услуги Клиенту по вопросам информационной безопасности при работе в Системе «iBank 2».
3.1.7. Осуществлять необходимую модернизацию программного обеспечения Системы «iBank 2».
3.1.8. Сообщать Клиенту о непредвиденных сбоях в работе Системы «iBank 2» для принятия им мер по своевременной доставке бумажного документа в Банк.
3.2. В рамках данного Регламента Клиент обязуется:
3.2.1. Инициировать соединение с Банком по Системе «iBank 2» для получения/передачи ЭД в Банк/из Банка.
3.2.2. Ознакомиться с инструкциями по работе в Системе «iBank 2», размещенными на сайте Банка (https://ibank2.newbank.ru/docs/Corporate_Internet-Banking_Guide.pdf) и руководствоваться их требованиями и положениями при работе в Системе «iBank 2».
Ознакомиться с Обзором приложения для мобильных устройств Mobile-Банкинг, размещенным на сайте Банка (https://ibank2.newbank.ru/docs/Corporate_Mobile_Banking_Guide_Review.pdf) и руководствоваться им при работе в Системе «iBank 2».
3.2.3. Осуществлять ввод документов (и осуществлять контроль введенной информации) в электронном виде, соблюдая порядок подготовки документов, обеспечивая заполнение форм в соответствии с банковскими требованиями и законодательством.
3.2.4. Осуществлять в течение любого рабочего дня не менее одного сеанса связи с Банком для получения выписок по счету(ам), контролю проводимых операций, а также возможных экстренных (технических) или информационных сообщений Банка, либо другой актуальной информации.
3.2.5. Выполнять требования по оформлению и защите передаваемой информации в виде ЭД, защите ключей ЭП, носителей ключевой информации, паролей и кодов доступа и другой информации, передаваемой и получаемой по Системе «iBank 2».
3.2.6. Соблюдать порядок осуществления приема и передачи ЭД и обеспечивать передачу только надлежащим образом оформленных документов.
3.2.7. Самостоятельно и за свой счет обеспечивать режим информационной безопасности при работе в Системе «iBank 2» путем принятия соответствующих организационно-технических мер, в том числе описанных в настоящем Договоре, на сайте Банка и/или в сообщениях, рассылаемых Клиенту по каналам Системы «iBank 2».
3.2.8. По запросу Банка подтвердить выполнение мероприятий по защите от воздействия вредоносных программ, в том числе вредоносного кода, либо сообщить о невыполнении таких мероприятий или выполнении их не в полном объеме. Подтверждение Клиент направляет в той же форме, что и полученный от Банка запрос.
3.3. В рамках данного Регламента стороны взаимно обязуются:
3.3.1. Не осуществлять действий, наносящих ущерб другой Стороне вследствие использования Системы «iBank 2».
3.3.2. Не осуществлять операцию по ЭД, заверенному ЭП, если программа проверки, используя действующий ключ проверки подписывающей Стороны, не подтвердила подлинность ЭП подписывающей Стороны под ЭД.

3.3.3. При осуществлении операций на основании полученных по Системе ЭД руководствоваться требованиями законодательства РФ, нормативных актов Банка России, и соглашений (договоров), заключенных между Банком и Клиентом.
3.3.4. Обеспечивать целостность и сохранность программных средств, ЭД, ключевой информации, ключевых носителей, паролей и кодов доступа, а также иной информации, передаваемой и получаемой по Системе «iBank 2».
3.3.5. Вести архивы передаваемых и получаемых по системе «iBank 2» документов на магнитных и бумажных носителях, хранить их в соответствии с порядком и сроками, установленными для хранения данного вида документов.

4. УСЛОВИЯ И ПОРЯДОК ОСУЩЕСТВЛЕНИЯ ЭЛЕКТРОННОГО ВЗАИМОДЕЙСТВИЯ

4.1. Общие положения

4.1.1. Программное обеспечение Банка настроено на взаимодействие с Системой «iBank 2», права на которую принадлежат АО «БИФИТ», и предполагает использование Клиентом этой же Системы.
4.1.2. Банк и Клиент взаимно признают достаточную криптографическую устойчивость используемых в Системе «iBank 2» алгоритмов, используемых для создания ключа ЭП.
4.1.3. Стороны взаимно признают достоверность и достаточную защищенность от подделок ЭП, созданной посредством Системы «iBank 2», на ЭД, передаваемых согласно условиям настоящего Договора.
4.1.4. После заполнения Клиентом Заявления (Приложение №4 к Договору) и оплаты вознаграждения Банка за выбранные в рамках Договора услуги Стороны проводят техническую и организационную подготовку по подключению Клиента к Системе «iBank 2» и регистрации ключей ЭП Клиента в порядке, определенном настоящим Регламентом. По результатам успешного исполнения указанных процедур Сторонами должны быть подписаны Акт приемки материалов и/или выполненных услуг (Приложение №7 к Договору) и Сертификат ключа проверки ЭП.
4.1.5. Подготавливаемые в Системе «iBank 2» ЭД проходят автоматическую проверку на датировку, присутствие обязательной информации в полях документа, на соответствие вводимых данных - реквизитам, записанным во встроенных справочниках и иное в соответствии с принятой технологией Системы «iBank 2».
4.1.6. После заполнения электронной формы платежного или иного документа Клиента осуществляется его подписание. Клиент подписывает ЭД своей ЭП, на основании которой однозначно устанавливается авторство документа. Количество групп подписей под ЭД должно соответствовать количеству групп подписей, указанных в Соглашении о праве подписи Клиента, хранящемся в Банке.
4.1.7. На этапе обработки ЭД в Банке осуществляется автоматический контроль (на соответствие электронной подписи содержимому документа, на соответствие количества групп подписей, на целостность и достоверность ЭП, на правильность указанного номера счета Клиента, на соответствие реквизитов Банка и РКЦ получателя, установленных Банком России, и иное в соответствии с принятой технологией). В случае выявления несоответствий в ходе проверки документа, операции по документу не проводятся, а Клиент получает информацию с указанием причин отказа в приеме на обработку ЭД, а в строке статуса ЭД в соответствующем модуле устанавливается значение “Отвергнут”.
4.1.8. Основанием для отказа Банка от приема и/или исполнения электронного платежного документа служат:

- отрицательный результат автоматической проверки ЭП на ЭД;
- недостаток денежных средств для проведения операций на счете Клиента (за исключением случаев предоставления овердрафта, оговоренных соответствующими договорами);
- несоответствие количества групп подписей, которыми подписан ЭД, количеству, указанному в соглашении о праве подписи Клиента;
- несоответствие даты документа требованиям действующего законодательства РФ;
- несоответствие указанных реквизитов отправителя или получателя платежа информации, приведенной в справочниках Банка России;
- несоответствие ЭД требованиям Банка России, МНС и Банка.

4.1.9. Активной стороной при установлении связи является Клиент.

4.2. Сроки обработки документов

4.2.1. Время передачи Клиентом платежных ЭД по Системе «iBank 2» для обработки их в текущем банковском дне – до 14:00. Платежные ЭД, направленные в Банк после 14:00 по московскому времени, проходят обработку в следующем банковском дне. ЭД, переданные по Системе «iBank 2» после 14:00, могут быть направлены в том же банковском дне после согласования данного вопроса с Банком и в соответствии с установленными Тарифами Банка.
4.2.2.Гарантированная работа Системы «iBank 2» обеспечивается Банком непрерывно, за исключением перерывов для профилактических работ**.**
Примечание: Обработка ЭД Банком в другое время возможна, но не гарантируется.
4.2.3. Стороны признают в качестве единой шкалы времени при направлении ЭД по Системе «iBank 2» московское поясное время. Контрольным является время системных часов аппаратных средств Банка.

4.3. Аварийный режим работы

4.3.1. При возникновении неисправности технических или программных средств Клиента, или других нештатных ситуаций, возникающих не со стороны и не по вине Банка, делающих невозможным передачу ЭД Клиента Банку по Системе «iBank 2», Клиент до 14:00 часов московского времени того же дня должен предупредить уполномоченных сотрудников Банка, и осуществить действия для доставки в Банк уполномоченным лицом надлежащим образом оформленных документов на бумажных носителях.

5. ОБЕСПЕЧЕНИЕ ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

5.1. ОБЩИЕ ПОЛОЖЕНИЯ

5.1.1. Защита информации в Системе «iBank 2» является многоуровневой и задействует возможности операционной системы, прикладного программного обеспечения, специализированных программных и технических средств и организационных мер (наличие соответствующих администраторов), организации хранения ПО, используемого в Системе «iBank 2».

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

- создание (генерация) ключей/ключей проверки шифрования и ЭП;
- ЭП под ЭД;
- шифрование передаваемой информации;
- аутентификацию Клиентов и разграничение их прав;
- достоверность факта получения документа получателем;
- проверка корректности ЭП;
- подтверждение авторства и целостности электронных документов;
- выявление ошибок, сбоев и несанкционированных действий обслуживающего персонала;
- доказательную базу, применяемую при разборе конфликтных ситуаций.

5.1.3. Для разрешения возможных споров в Банке ведутся контрольные архивы ЭД подписанных ЭП, а также архивы ключей проверки ЭП. Хранение контрольных архивов осуществляется в течение трех лет с момента проведения операций.

5.1.4. При проверке подписи под документом используется соответствующий действующий ключ проверки ЭП Клиента, подписавшего ЭД.

5.1.5. Обработка принятых Банком от Клиента ЭД производится только при условии корректности ЭП на ЭД.

5.2. ПОРЯДОК ГЕНЕРАЦИИ И РЕГИСТРАЦИИ КЛЮЧЕЙ ЭП

5.2.1. В процессе предварительной регистрации Клиент самостоятельно создает ключ ЭП и парный ему ключ проверки ЭП. Ключ ЭП Клиента сохраняется в файле на ключевом носителе Клиента (дискете/USB-флеш-накопителе или персональном аппаратном криптопровайдере)[1] либо в хранилище формата PKCS#8 в зашифрованном на пароле Клиента виде. Ключ проверки ЭП по защищенному соединению передается в Банк и предварительно регистрируется в Системе «iBank 2». Также ключ проверки ЭП должен быть распечатан Клиентом на бумажном носителе в виде Сертификата ключа проверки ЭП в двух экземплярах. Форма Сертификата приведена в Приложении №2 к Договору. Оба экземпляра Сертификата должны быть подписаны руководителем и главным бухгалтером Клиента (при наличие в штате) с проставлением оттиска печати Клиента и представлены в Банк для регистрации согласно п.5.2.5 настоящего Регламента.

5.2.2. Все ключи ЭП в процессе генерации защищаются паролями. Указанный пароль является конфиденциальной информацией владельца ключа. Владелец ключа несет ответственность за обеспечение сохранности такой конфиденциальной информации.

5.2.3. Владельцы ключей ЭП, созданных в Системе «iBank 2», несут персональную ответственность за обеспечение сохранности ключевой информации, защиты ключевых файлов (элементов) и ключевых носителей от несанкционированного доступа.

5.2.4. Все процедуры окончательной регистрации и проверки ключей проверки ЭП, происходят только в помещениях Банка и только на программном обеспечении и оборудовании Банка.

5.2.5. При регистрации ключа проверки ЭП Клиента в Банке производится сверка ключа проверки ЭП Клиента с ключом проверки ЭП, напечатанным в Сертификате ключа проверки ЭП, и проверка лиц, на имя которых сформированы ключи, на соответствие их с именами, фамилиями, отчествами (при наличии) образцами подписей и оттиском печати, указанными в банковской карточке Клиента и Соглашении о праве подписи, хранящимися в Банке.

5.2.6. Ключ ЭП Клиента регистрируется только после получения Банком надлежаще оформленного и заверенного Клиентом Сертификата ключа проверки ЭП, а также успешной верификации данных, указанных в п.п.5.2.5 настоящего Регламента. При регистрации ключа Клиента в Системе «iBank 2» уполномоченные на совершение соответствующих действий сотрудники Банка проставляют в Сертификате ключа проверки ЭП отметки о дате регистрации и сроке его действия в Системе «iBank 2» и заверяют печатью Банка. После регистрации ключа ЭП Клиента в Системе, один экземпляр Сертификата ключа проверки ЭП на бумажном носителе передается Клиенту, второй - остается на хранении в Банке, а его электронный аналог находится в каталоге ключей Банка и Клиента.

5.2.7. Факт передачи представителю Клиента оформленных со стороны Банка Сертификатов ключей проверки ЭП фиксируются уполномоченным сотрудником Банка и представителем Клиента в письменном виде.

5.3. ПОРЯДОК ХРАНЕНИЯ И СМЕНЫ КЛЮЧЕЙ ЭП

5.3.1. ПОРЯДОК ХРАНЕНИЯ КЛЮЧЕЙ

5.3.1.1. Надежность средств криптозащиты и подлинность передаваемой по каналам связи информации обеспечивается только при условии сохранности от компрометации действующих ключей ЭП, а также исключения несанкционированного доступа посторонних лиц к Mobile-Банкингу. К событиям, связанным с компрометацией или подозрением на компрометацию ключа относятся, включая, но не ограничиваясь, следующие события:

---

[1] Регистрация Банком ключей ЭП Клиента, сгенерированных с использованием персональных аппаратных криптопровайдеров, производится только в том случае, когда Клиент использовал для генерации ключей ЭП аппаратные криптопровайдеры, полученные в результате использования услуги по защите ключей ЭП Клиента с использованием аппаратных криптопровайдеров, предоставляемой Банком. В случаях, когда используемый в процессе генерации ключа ЭП аппаратный криптопровайдер не передавался Клиенту Банком в рамках оказания услуги по защите ключей ЭП Клиента, Банк оставляет за собой право отказать Клиенту в регистрации ключа ЭП Клиента в Системе «iBank 2».

• утеря носителя ключевой информации, в том числе с последующим обнаружением, а также утрата контроля за доступом к мобильному устройству;

• выход из строя носителя ключевой информации, когда невозможно достоверно определить причину этого события (доказательно не опровергнута возможность того, что данный факт произошел в результате несанкционированных действий злоумышленника);

• доступ, передача, ознакомление неуполномоченных сотрудников Клиента и третьих лиц с серийными номерами (идентификаторами) ***OTP-токенов***;

• обнаружение факта или угрозы использования (копирования) паролей доступа и/или доступа к Системе «iBank 2» неуполномоченных лиц (несанкционированная отправка электронных документов);

• обнаружение ошибок в работе Системы «iBank 2», в том числе возникающих в связи с попытками нарушения информационной безопасности;

• обнаружение вредоносных программ, в том числе вредоносного кода, в компьютере, используемом для работы в Системе «iBank 2».

5.3.1.2. Клиент берет на себя полную ответственность и обязуется самостоятельно обеспечить условия хранения своих ключей ЭП, а также пароля и мобильного устройства, зарегистрированного в Системе «iBank 2», исключающие возможность их компрометации. В случае потери, кражи, несанкционированного копирования или любого подозрения в компрометации ключей ЭП Клиент/паролей мобильного приложения обязан немедленно в письменном виде оповестить Банк о необходимости блокировки ключей ЭП Клиента или необходимости удалить скомпрометированное мобильное устройство Клиента из списка устройств, зарегистрированных в Системе «iBank 2». Допускается возможность дистанционного оповещения уполномоченного сотрудника Банка о необходимости блокировки ключей ЭП Клиента/ удаления мобильного устройства из списка зарегистрированных с указанием блокировочного слова, вводимого Клиентом при регистрации в Системе «iBank 2», с последующим обязательным предоставлением в Банк письменного заявления о блокировке ключей ЭП.

5.3.1.3. Банк не несет ответственности в случаях компрометации действующих ключей ЭП Клиента за последствия, которые могут возникнуть в результате данной компрометации. При рассмотрении Банком ЭД считается действительным и подлинным, если он подписан подлинной ЭП Клиента, сформированной при использовании действующего ключа ЭП, сгенерированного Клиентом в процессе создания ключей ЭП, и зарегистрированного в Системе «iBank 2» на основании Сертификата ключа проверки ЭП, предоставляемого Клиентом в Банк.

5.3.1.4. Выведенные из употребления ключи хранятся в Банке те же сроки, что и документы, подписанные и зашифрованные этими ключами, т.е. в соответствии с правилами организации государственного архивного дела, но не менее пяти лет.

5.3.2. ПОРЯДОК СМЕНЫ КЛЮЧЕЙ ЭП

5.3.2.1. Смена ключей производится при:

- замене банковской карточки Клиента;
- истечении срока действия ключей;
- компрометации ключей;
- переходе от обычных ключевых носителей к персональным аппаратным криптопровайдерам.
- предоставлении Клиентом соответствующего заявления в письменной форме.

5.3.2.2. Срок действия ключей ЭП устанавливается (срок действия ключа ЭП исчисляется с даты регистрации Сертификата ключа проверки ЭП в Банке уполномоченным сотрудника Банка) следующим:

- 12 месяцев для ключей, сгенерированных без использования персональных аппаратных криптопровайдеров;
- 24 месяца для ключей, сгенерированных с использованием персональных аппаратных криптопровайдеров.

5.3.2.3. Смена ключей уполномоченных лиц Клиента производится в соответствии с п.5.2. данного Регламента.

5.3.2.4 ЭД, подписанный ЭП Клиента, сформированной с использованием новых ключей, принимается Банком только после регистрации новых ключей ЭП Клиента в соответствии с порядком, изложенным в п.5.2 данного Регламента.

5.4. ПОРЯДОК БЛОКИРОВКИ КЛЮЧЕЙ ЭП

5.4.1. Банк блокирует (приостанавливает) действие ключа с момента получения уполномоченными службами Банка письменного заявления Клиента о блокировке ключа, содержащего причину блокировки, ФИО владельца и/или ID ключа, указанного в Сертификате ключа проверки ЭП, составленного по форме Приложения №4 к Договору, подписанного руководителем и главным бухгалтером Клиента, а также заверенного печатью организации.

5.4.2. В экстренных случаях блокировка может быть произведена при уведомлении Банка иным способом:

- по телефону на основании блокировочного слова, указанного Клиентом при регистрации в Системе «iBank 2»;
- по электронной почте с почтового адреса, указанного Клиентом в Сертификате ключа проверки ЭП;
- по факсу с зарегистрированного номера, указанного Клиентом в Сертификате ключа проверки ЭП.

При использовании средств коммуникации, указанных в настоящем пункте, Клиент обязуется не позднее трех рабочих дней со дня блокировки ЭП Клиента, представить в Банк подтверждающее письменное заявление. После блокирования ключа, прием и обработка документов, подписанных данным ключом, прекращаются.

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

5.4.4. Снятие блокировки производится на основании письменного заявления Клиента об устранении причин, приведших к блокированию ключа, подписанного руководителем и главным бухгалтером Клиента и заверенного

печатью организации. В случае блокировки ключа по инициативе Банка снятие блокировки с ключа Клиента производится Банком самостоятельно по согласованию с Клиентом.

5.5. ПОРЯДОК ИСКЛЮЧЕНИЯ ЭП

5.5.1. Банк исключает ключ из каталога (базы) действующих ключей, с момента получения уполномоченными службами Банка письменного заявления Клиента, составленного по форме Приложения № 4к Договору и подписанного руководителем и главным бухгалтером Клиента (при его наличии). Ключ ЭП Клиента исключается из каталога действующих ключей, прием и обработка ЭД, подписанных таким ключом, прекращается.

5.5.2. Ключи ЭП Клиента, срок действия которых истек, признаются недействующими автоматически и исключаются из каталога действующих ключей в Системе «iBank 2». Вход в Систему, также как и другие операции с использованием просроченного ключа ЭП становятся невозможными. Банк не несет ответственность за несвоевременную смену Клиентом ключей ЭП и возникшие в связи с этим последствия для Клиента.

5.5.3. Банк и Клиент обеспечивают сохранность исключенных ключей ЭП Клиента согласно п.п. 5.3.1. данного Регламента, при этом исключенные ключи хранятся те же сроки, что и документы, подписанные и зашифрованные этими ключами.

5.6. ПОРЯДОК ДЕЙСТВИЙ В СЛУЧАЕ КОМПРОМЕТАЦИИ СЕКРЕТНЫХ КЛЮЧЕЙ

5.6.1. В случае компрометации или подозрения на компрометацию ключа Клиент должен незамедлительно известить уполномоченных сотрудников Банка для блокировки соответствующего ключа, в соответствии с порядком, установленным п.5.4. данного Регламента.

5.6.2. В случае не подтверждения компрометации ключа, Банк производит снятие блокировки ключа в соответствии с п.5.4.4 данного Регламента.

5.6.3. В случае подтверждения компрометации ключа Банк исключает скомпрометированный ключ в соответствии с п.5.5 данного Регламента.

5.6.4. ЭД, подписанные скомпрометированным ключом, и соответствующий ему ключ проверки ЭП Клиента, хранятся в соответствии с правилами организации государственного архивного дела, но не менее пяти лет.

5.7. ПОРЯДОК ПРЕДОСТАВЛЕНИЯ УСЛУГ ПО ИСПОЛЬЗОВАНИЮ ПЕРСОНАЛЬНЫХ АППАРАТНЫХ КРИПТОПРОВАЙДЕРОВ (USB-ТОКЕНОВ).

5.7.1. Общие сведения о персональных аппаратных криптопровайдерах

5.7.1.1. Персональные аппаратные криптопровайдеры (далее - ПАК) представляют собой устройства для защищенного хранения ключей ЭП. Использование ПАК делает принципиально невозможным несанкционированное копирование ключей ЭП, используемых при работе в Системе «iBank 2».

5.7.1.2. В ПАК реализованы следующие криптографические функции:

- аппаратный криптографически стойкий генератор случайных чисел;
- генерация пары ключей ЭП;
- формирование и проверка ЭП по ГОСТ Р34.10-2001;
- генерация ключей шифрования;
- шифрование и расшифровка в соответствии с ГОСТ 28147-89;
- формирование и проверка имитовставки (последовательности данных фиксированной длины, получаемой по определенному правилу из открытых данных и ключа и добавляемой к данным для обеспечения имитозащиты) в соответствии с ГОСТ 28147-89;
- вычисление хеш-функции в соответствии с ГОСТ Р34.11-94.

5.7.1.3. Формирование ЭП в соответствии с ГОСТ Р34.10-2001 происходит непосредственно внутри ПАК: на вход ПАК принимает электронный документ, на выходе выдает ЭП под данным документом. При этом время формирования ЭП приблизительно равно 0,5 сек.

5.7.1.4. Ключ ЭП генерируется самим ПАК, хранится в защищенной памяти ПАК и никогда, никем и ни при каких условиях не может быть считан из ПАК. В ПАК имеется защищенная область памяти, позволяющая хранить до 64-х секретных ключей ЭП ответственных сотрудников одного клиента.

5.7.1.5. Срок действия ключа ЭП, генерируемого внутри ПАК составляет 24 месяца.

5.7.2. Варианты ПАК, предоставляемых Банком:

USB-токен «iBank 2 Key» — это аппаратное USB-устройство в компактном пластиковом корпусе, состоящее из USB-картридера и защищенного карточного микроконтроллера ST19NR66 или ST23YL18 производства компании STMicroelectronics.

Микроконтроллеры сертифицированы на соответствие стандарту ISO/IEC 15408 (common criteria) с уровнем доверия EAL5+.

Тип микроконтроллера зависит от модели исполнения корпуса «iBank 2 Key»:

• исполнение корпуса «A», «M», «B2» — микроконтроллер ST19NR66

• исполнение корпуса «M2», «B» — микроконтроллер ST23YL18

В микроконтроллере при производстве масочным методом «прошита» карточная операционная система «Магистра» (разработчик ООО «Смарт-Парк»). В составе операционной системы содержится СКЗИ, сертифицированное ФСБ РФ по классу КС2.

В составе микроконтроллера ST19NR66 содержится СКЗИ «ФОРОС. Исполнение №1» (разработчик ООО «СмартПарк»), сертифицированное ФСБ РФ по классу КС2. Сертификат ФСБ РФ рег. № СФ/124-2151 от 03.06.2013 г.

В составе микроконтроллера ST23YL18 содержится СКЗИ «Криптомодуль С23» (разработчик ООО «СмартПарк»), сертифицированное ФСБ РФ по классу КС2. Сертификат ФСБ РФ рег. № СФ/114-2312 от 31.12.2013 г.

USB-токен «Рутокен ЭЦП 2.0» - основу составляет современный защищенный микроконтроллер и встроенная защищенная память, в которой безопасно хранятся данные пользователя: пароли, ключи шифрования и подписи, сертификаты и т.д.

В составе микроконтроллера содержится СКЗИ, сертифицированное ФСТЭК и ФСБ РФ:

• Сертификат ФСТЭК № 2592 от 19.03.2012 г. – действителен до 19.03.2018г.

• Сертификат ФСБ РФ рег. № СФ/124-2771 от 25.12.15 г. – действителен до 25.12.2018г.

В системе «iBank 2» поддерживается работа USB-токенов «Рутокен ЭЦП 2.0» в специальной конфигурации, предназначенной для использования исключительно в системе «iBank 2».

USB-токен «MS_KEY K» — это аппаратное USB-устройство в компактном пластиковом корпусе, состоящее из USB-картридера и защищенного карточного микроконтроллера NXP P5CC081.

Разработчиком устройства является компании «Multisoft».

«MS_KEY K» строится на базе карточного микроконтроллера NXP P5CC081 с операционной системой «Вигрид» (VIGRID – Verification Interoperability GRID) версии 1.0. Устройство «MS_KEY K» сертифицировано как СКЗИ по классам КС1 и КС2 и имеет сертификат соответствия ФСБ РФ № СФ/124-2211.

5.7.3. USB-токены предназначены для работы на следующих платформах: Windows XP Professional/XP Home/Server 2000/Server 2003/2000 Professional/Vista/7, Linux x86_64 с использованием Java, Mac OS X с использованием Java.

5.7.4. Порядок эксплуатации и хранение USB-токенов:

USB-токены являются чувствительными электронными устройствами. При их хранении и эксплуатации пользователю необходимо соблюдать ряд правил и требований, при нарушении которых указанные устройства могут выйти из строя.

Следующие правила эксплуатации и хранения обеспечат длительный срок службы USB-токенов, а также сохранность конфиденциальной информации пользователя:

- Необходимо оберегать USB-токены от сильных механических воздействий (падения с высоты, сотрясения, вибрации, ударов и т.п.).
- USB-токены необходимо оберегать от воздействия высоких и низких температур. При резкой смене температур (вносе охлажденного устройства с мороза в теплое помещение) не рекомендуется использовать USB-токен в течение 3 часов во избежание повреждений из-за сконденсированной на электронной схеме влаги. Необходимо оберегать USB-токены от попадания на них прямых солнечных лучей.
- Необходимо оберегать USB-токены от воздействия влаги и агрессивных сред.
- Недопустимо воздействие на USB-токены сильных магнитных, электрических или радиационных полей, высокого напряжения и статического электричества.
- При подключении USB-токена к компьютеру не прилагайте излишних усилий.
- USB-токен в нерабочее время необходимо всегда держать закрытым во избежание попадания на разъем USB-токена пыли, грязи, влаги и т.п. При засорении разъема USB-токена нужно принять меры для его очистки. Для очистки корпуса и разъема используйте сухую ткань. Использование воды, растворителей и прочих жидкостей недопустимо.
- Не разбирать USB-токены.
- Необходимо избегать скачков напряжения питания компьютера и USB-шины при подключенном USB-порте, а также не извлекать USB-токен или картридер из USB-порта во время записи и считывания.
- В случае неисправности или неправильного функционирования USB-токенов следует обращаться в Банк.

5.7.5. Стоимость услуг по защите ключей ЭП Клиента с использованием ПАК и порядок расчетов.

За оказанные Банком услуги и предоставленные материалы по защите ключей ЭП Клиента с использованием ПАК Клиент осуществляет оплату в соответствии с действующими Тарифами комиссионного вознаграждения Банка.

5.7.6. Порядок подключения услуги по защите ключей ЭП Клиента с использованием ПАК:

5.7.6.1. Услуга предоставляется на основании письменного заявления Клиента (Приложение №1). При оформлении заявления на подключение услуги Клиент указывает количество USB-токенов необходимых Клиенту. Банк рекомендует Клиентам для каждого лица, наделенного ЭП, использовать отдельный ПАК.

5.7.6.2. При выборе указанной услуги не допускается одновременное использование в качестве носителя ключевой информации иных носителей кроме ПАК.

5.7.6.3. Прием услуги осуществляется путем подписания Сторонами Акта приема-передачи материалов и/или выполненных услуг (Приложение №7), которым подтверждается передача Клиенту заявленного количества USB-токенов, пользовательской документации и драйверов для работы ПАК.

5.7.6.4. Для активации и начала использования ПАК в Системе «iBank 2» Клиент обязан осуществить смену ключей ЭП в порядке, указанном в разделе 5.2. Регламента, с использованием в качестве ключевого носителя ПАК.

За первичную генерацию ключей ЭП с использованием USB-токена при подключении Клиентом услуги по защите ключей ЭП комиссия Банком не взимается. В дальнейшем, за внеплановую смену ключей ЭП взимается комиссия в соответствии с действующими Тарифами Банка, за исключением случая, указанного в п. 5.7.6.5 Регламента.

5.7.6.5. Клиент вправе в период гарантийного срока заменить неисправный USB-токен без внесения дополнительной платы. Срок замены неисправного USB-токена составляет не более трех рабочих дней. Гарантийный срок составляет 12 месяцев со дня передачи USB-токена Клиенту, и не распространяется на USB-токены с видимыми повреждениями, произошедшими в результате внешних воздействий на устройство.

5.8. ПОРЯДОК ПРЕДОСТАВЛЕНИЯ УСЛУГ

ПО МНОГОФАКТОРНОЙ АУТЕНТИФИКАЦИИ КЛИЕНТА.

5.8.1. Общие сведения.

Для предотвращения хищения средств с расчетного счета Клиента, которое может быть осуществлено злоумышленником методом направления в банк по Системе «iBank 2» ЭД с корректной ЭП Клиента, сформированной с использованием ранее похищенного ключа ЭП Клиента и пароля для доступа к этому ключу, используется одна из мер пресечения подобных хищений — многофакторная аутентификация.

Многофакторная аутентификация реализована в Системе «iBank 2» с использованием Клиентами одноразовых паролей, генерируемых OTP-токенами. Клиентам, пользующимся услугой «расширенная многофакторная аутентификация», для входа в Систему необходимо дополнительно вводить одноразовый пароль, сгенерированный OTP-токеном. Злоумышленники, похитившие ключи ЭП клиента, не смогут без OTP-токена Клиента подключиться и направить в банк по Системе «iBank 2» ЭД с корректными ЭП клиента. Генерируемый OTP-токеном одноразовый пароль используется в процедуре аутентификации клиента при входе в Систему «iBank 2», а также в процедуре подтверждения электронных документов клиента, в случае установки Клиентом ограничительного лимита платежа, проведение которого без ввода, сгенерированного OTP-токеном одноразового пароля, будет невозможно. Не пройдя процедуру многофакторной аутентификации Клиента с использованием одноразового пароля, сгенерированного OTP-токеном, злоумышленник не сможет передать в Банк платежное поручение с корректной ЭП.

Одноразовый пароль не защищает ключи ЭП клиента, но может участвовать в процедуре подтверждения ЭД Клиента (в случае установки лимита) и не позволяет злоумышленнику воспользоваться ранее похищенным у клиента ключом ЭП для отправки в Банк по Системе «iBank 2» платежных поручений от имени Клиента.

OTP–токен (One time password) – устройство, предназначенное для генерации одноразовых паролей для дополнительной авторизации при входе в Систему «iBank 2», а также для подтверждения платежных документов, направляемых в Банк.

Генерация одноразового пароля происходит при однократном нажатии кнопки, расположенной на лицевой панели устройства OTP–токен рядом с дисплеем. После нажатия кнопки на дисплее будет отображен одноразовый пароль, который необходимо ввести в окно дополнительной авторизации и/или подтверждения платежного документа в системе «iBank 2».

Срок полезной эксплуатации OTP-токенов составляет 5 лет.

5.8.2. OTP-токены могут выполнять следующие функции в Системе «iBank 2»:

- Двухуровневая аутентификация при входе в Систему «iBank 2» (вход будет возможен только после ввода пароля, указанного при регистрации Клиента и одноразового пароля, сгенерированного OTP-токеном);
- Подтверждение направляемого платежного документа в Банк, сумма которого превышает установленный Клиентом лимит операции (после подписания ЭД для подтверждения отправки платежного документа в Банк Клиент обязан будет ввести одноразовый пароль, сгенерированный OTP-токеном).

Клиент самостоятельно определяет перечень функций OTP-токена в Системе «iBank 2» при подключении услуги, указывая в соответствующем заявлении.

5.8.3. Правила эксплуатации и хранения OTP-токенов:

- оберегать OTP-токены от сильных механических воздействий (падения с высоты, сотрясения, вибрации, ударов и т.п.);
- оберегать от воздействия высоких и низких температур. При резкой смене температур (вносе охлажденного устройства с мороза в теплое помещение) не рекомендуется использовать OTP-токены в течение 3 часов во избежание повреждений из-за сконденсированной на электронной схеме влаги. Необходимо оберегать OTP-токены от попадания на них прямых солнечных лучей.
- оберегать OTP-токены от воздействия влаги и агрессивных сред.
- Недопустимо воздействие на OTP-токены сильных магнитных, электрических или радиационных полей, высокого напряжения и статического электричества.
- При нажатии кнопки OTP-токена не прилагать излишних усилий.
- Не разбирать OTP-токены.

5.8.4. В случае утраты OTP-токена, Клиент обязан незамедлительно обратиться в Банк для блокировки утраченного OTP-токена и приобретения нового.

5.8.5. Порядок подключения услуги многофакторной аутентификации Клиента:

5.8.6. Услуга предоставляется на основании письменного заявления Клиента (Приложение № 1).

5.8.7. При оформлении заявления на подключение услуги Клиент указывает перечень необходимых функций OTP-токена в Системе «iBank 2», сумму операций в рублях РФ, свыше которой потребуется введение одноразового пароля, генерируемого OTP-токеном, и указывает количество OTP-токенов необходимых Клиенту.

5.8.8. Прием Клиентом услуги Банка по многофакторной аутентификации Клиента в рамках настоящего Договора осуществляется путем подписания Сторонами Акта приема-передачи материалов и/или выполненных услуг (Приложение №7), которым подтверждается передача Клиенту заявленного количества OTP-токенов и пользовательской документации. OTP-токен считается активным, а услуга доступной Клиенту с момента подписания Сторонами Акта приема-передачи материалов и/или выполненных услуг.

5.8.9. Стоимость услуг и материалов по многофакторной аутентификации Клиента определяется Тарифами комиссионного вознаграждения Банка, действующими на момент оказания услуги. При отказе от дальнейшего использования данной услуги, деньги, внесенные Клиентом за ее приобретение, не возвращаются.

5.8.10.Данная услуга не исключает обязательности использования ключей ЭП, как традиционного средства аутентификации и подтверждения платежных документов, направляемых в Банк.

5.8.11. Клиент может приобрести данную услугу в том количестве, в котором это диктуется удобством и порядком работы его организации.
5.8.12. При использовании Клиентом нескольких OTP-токенов, каждый из них при первом использовании “привязывается” к используемому с данным OTP-токеном ключу ЭП. Перепривязка OTP-токенов к другим ключам ЭП Клиента производится специалистами Банка на основании Заявления Клиента в произвольном форме с указанием серийного номера OTP-токена и ID ключа соответствующего ключа ЭП Клиента.
5.8.13. Клиент вправе в период гарантийного срока заменить неисправный OTP-токен без внесения дополнительной платы. Срок замены неисправного OTP-токена составляет не более трех рабочих дней. Гарантийный срок составляет 12 месяцев со дня выдачи OTP-токена, и не распространяется на OTP-токены с видимыми повреждениями, произошедшими в результате внешних воздействий на устройство.
5.8.14. Использование данной услуги не предполагает приобретения и установки дополнительного оборудования и программного обеспечения кроме самого OTP-токена.

5.9. ПОРЯДОК ПРЕДОСТАВЛЕНИЯ УСЛУГ С ИСПОЛЬЗОВАНИЕМ ПРИЛОЖЕНИЯ ДЛЯ МОБИЛЬНЫХ УСТРОЙСТВ MOBILE-БАНКИНГ ДЛЯ КОРПОРАТИВНЫХ КЛИЕНТОВ.

5.9.1. Mobile-Банкинг для корпоративных клиентов –приложение, с помощью которого Клиент может с любого мобильного устройства осуществлять доступ к системе" iBank 2", а также формировать, подписывать серверной подписью ЭП и отправлять в банк платежные поручения, работать со справочниками корреспондентов и бенефициаров, отслеживать статусы документов, получать выписки по своим счетам за произвольный период, обмениваться с банком письмами.
5.9.2. ЭД, полученные с использованием Mobile-Банкинг и подписанные корректными ЭП уполномоченных лиц, влекут такие же правовые последствия, как и аналогичные документы на бумажном носителе, содержащем собственноручные подписи уполномоченных лиц.
5.9.3. Процедура генерации и порядок хранение ключей серверной подписи и ключей проверки серверной подписи осуществляется на Сервере Подписи системы iBank2 в порядке, указанном в Обзоре приложения для мобильных устройств Mobile-Банкинг, размещенным на сайте Банка (https://ibank2.newbank.ru/docs/Corporate_Mobile_Banking_Guide_Review.pdf).
5.9.4. Запрещается анонимная регистрация в приложении Mobile-Банкинг.
5.9.5. Банк предоставляет доступ к мобильному приложению не позднее дня, следующего за днем даты регистрации в Банке Сертификата ключа проверки ЭП.
5.9.6. Клиент подтверждает, что мобильное устройство, зарегистрированное в системе «iBank 2», подключенные к мобильному приложению Mobile-Банкинг, используются исключительно уполномоченными лицами.
5.9.7. В случае угрозы несанкционированного доступа к счетам посредством приложения Mobile-Банкинг, в том числе утраты мобильного устройства Клиент обязан незамедлительно блокировать (прекратить) доступ к счетам в порядке, предусмотренном пунктом 5.6. настоящего Регламента.
5.9.8. Банк не несет ответственности за последствия доступа к счетам неуполномоченными лицами в случае нарушения Клиентом обязанности, предусмотренной пунктом 5.9.7. настоящего Регламента.
5.9.9. Банк не несет ответственности за ущерб, возникший вследствие передачи Клиентом/уполномоченным лицом Клиента третьим лицам логина, пароля к приложению Mobile-Банкинг, вне зависимости от причин.
5.9.10. Банк не несет ответственности за сбои и помехи в работе линий и средств связи, приводящие к невозможности доступа и использования приложения Mobile-Банкинг.
5.9.11. Банк не несет ответственности за сбои в работе приложения Mobile-Банкинг, обусловленные неисправностью мобильного устройства, нарушением работоспособности установленного на мобильном устройстве программного обеспечения, производителем которого Банк не является, или иными внешними факторами, в том числе повреждением приложения Mobile-Банкинг, установленного на мобильном устройстве.

ПРИЛОЖЕНИЕ №6
к Правилам дистанционного банковского обслуживания клиентов с использованием системы «iBank 2» в КБ «Новый век» (ООО)

ПОРЯДОК РАЗРЕШЕНИЯ СПОРОВ

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. В данном Порядке описана процедура разрешения споров между Банком и Клиентом, связанных с подлинностью электронных документов, исполненных в Системе «iBank 2».

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

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

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

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

2. РАБОТА СОГЛАСИТЕЛЬНОЙ ЭКСПЕРТНОЙ КОМИССИИ

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

2.2. Экспертная комиссия осуществляет свою работу на территории Банка, с использованием ПЭВМ Банка, программного обеспечении и ключевых элементов.

Клиент обязуется в случае необходимости предоставлять членам Комиссии доступ в помещения, где установлены компьютеры, с которых могла производиться передача спорного документа, а также к самим компьютерам, для проведения проверок соблюдения Клиентом условий Договора, в том числе для копирования информации.

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

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

2.5. Стороны обязаны предоставить комиссии возможность ознакомиться с условиями и порядком работы Системы «iBank 2», в том числе приложения Mobile-Банкинг. Стороны способствуют работе комиссии и не допускают отказа от представления необходимых документов и материалов, имеющих отношение к рассматриваемому Спору.

2.6. В ходе рассмотрения комиссией Спора о подлинности (наличии или отсутствии) документа, исполненного с помощью Системы «iBank 2» и подписанного ЭП, каждая Сторона обязана доказать лишь то, что она своевременно и надлежащим образом выполнила обязательства, взятые на себя по Договору и Приложениям к нему, в том числе настоящим Регламентом.

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

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

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

2.8. В случае, если предложение о создании комиссии оставлено другой стороной без ответа (по истечении 15 дней согласно п.2.1. данного Порядка), либо Сторона отказывается от участия в комиссии, либо работе комиссии были учинены препятствия, которые не позволили комиссии оформить надлежащий Акт, заинтересованная Сторона составляет Акт в одностороннем порядке с указанием причины составления его в одностороннем порядке. В указанном Акте фиксируются обстоятельства, позволяющие сделать вывод о том, что оспариваемый электронный

документ, произведенный в Системе «iBank 2» в соответствии с Договором, является подлинным, либо формулируется вывод об обратном. Указанный Акт направляется другой Стороне для сведения.

3. РАССМАТРИВАЕМЫЕ СПОРЫ

3.1. Согласительная экспертная комиссия рассматривает споры следующих основных типов, (данный список не является исчерпывающим):

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

  В этом случае Сторона-отправитель предоставляет комиссии письменное разрешение на передачу для независимой экспертизы в АО ”БИФИТ” следующие файлы, полученные с помощью эталонного программного обеспечения, предоставляемого АО “БИФИТ”: *file.bin* - файл с электронным документом, выгруженным из Сервера базы данных Системы «iBank 2», *sign.bin* - файл с ЭП Клиента под электронным документом, выгруженным из Сервера базы данных Системы «iBank 2», *certificate.xml* - файл с ключом проверки ЭП Клиента, с помощью которого осуществляется проверка подлинности ЭП под электронным документом.

  После передачи комиссией перечисленных файлов АО «БИФИТ» проводит на собственном оборудовании проверку подлинности ЭП Клиента с использованием указанных файлов и эталонной утилиты для проверки подлинности ЭП, содержащей встроенные сертифицированные ФСБ РФ криптографические библиотеки.

  В результате проверки ЭП проверяется корректность ЭП файла, содержащего оспариваемый ЭД. В том случае, если корректность ЭП подтверждается, виновной признается Сторона-отправитель ЭД, в противном случае виновной признается Сторона-получатель ЭД.

4. ПОРЯДОК ФОРМИРОВАНИЯ И ПРОВЕРКИ ЭП под ЭД

4.1. Последовательность формирования электронной цифровой подписи под электронным документом следующая:

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

<Наименование поля 1>=<Значение поля 1> <символ перевода строки>
<Наименование поля 2>=<Значение поля 2> <символ перевода строки>
……...

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

4.1.3. Электронная подпись формируется от указанного в п.4.1.2 байтового массива в соответствии с ГОСТ.

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

4.2. Контрольная проверка ЭП Клиента под электронным документом, пришедшим в Банк, осуществляется в АРМе “Операционист”, входящим в комплекс Системы “IBank 2”.

При проверке ЭП Клиента в АРМе “Операционист”, отображается:

- Содержание электронного документа
- Идентификаторы ключей ЭП Клиента, которыми подписан ЭД
- Время формирования ЭП (если документ подписан несколькими ЭП – время формирования каждой ЭП)
- Результаты проверки каждой из ЭП под ЭД

4.3. Результат проверок ЭП Клиента под ЭД в АРМе “Операционист” является подтверждением верности/неверности ЭП Клиента под ЭД.

ОБРАЗЕЦ

Приложение №7
к Правилам дистанционного банковского обслуживания клиентов с использованием системы «iBank 2» в КБ «Новый век» (ООО)

АКТ
ПРИЕМА-ПЕРЕДАЧИ МАТЕРИАЛОВ И/ИЛИ ВЫПОЛНЕННЫХ УСЛУГ

Коммерческий Банк «Новый век» (Общество с Ограниченной Ответственностью), именуемый в дальнейшем «Банк», в лице заместителя Председателя Правления Пономаревой Екатерины Николаевны, действующего на основании Доверенности №298 от 23.03.2012г, с одной стороны, и _____,
именуемое в дальнейшем «Клиент», в лице _____, действующего на основании _____, с другой стороны, совместно именуемые «Стороны», подписали настоящий Акт приема-передачи материалов и/или выполненных услуг (далее – «Акт») о том, что в рамках Договора на обслуживание в Системе «iBank 2» № _____ от «___» _____ 20__ г. по заявке Клиента Банком выполнен следующий перечень услуг, переданы следующие материалы:

☐ подключение Клиента к Системе «iBank 2».
Стоимость выполненных услуг составила _____ руб. ____ коп. без НДС.

☐ настройка ПЭВМ Клиента для работы в Системе «iBank 2» специалистами Банка.
Стоимость выполненных услуг составила _____ руб. ____ коп. без НДС.

☐ Внеплановая смена ключей ЭП (дополнительная генерация ключей ЭП Клиента).
Стоимость выполненных услуг составила _____ руб. ____ коп. без НДС.

☐ Регистрация Просмотрового ключа ЭП (без права подписи). Количество просмотровых ключей ___ шт.
Стоимость выполненных услуг составила _____ руб. ____ коп. без НДС.

☐ материалы для пользования услугой защиты секретного ключа ЭП.
Банком переданы, а Клиентом получены USB-токен(ы) с инструкцией пользователя и драйверами для работы, в количестве____ шт.:

№ п/п	Наименование криптопровайдера	Серийный номер (идентификатор, ID) криптопровайдера (заполняется Банком)
1	USB-токен	

Стоимость переданных/принятых материалов составляет _____ руб. ____ коп.
НДС _____ руб. ____ коп.

☐ материалы для пользования услугой многофакторной аутентификации Клиента.
Банком переданы, а Клиентом получены OTP-токен(ы) с инструкцией пользователя, в количестве____ шт.:

№ п/п	Наименование	Серийный номер (идентификатор, ID) OTP-токена (заполняется Банком)
1	OTP-токен	

Стоимость переданных/принятых материалов составляет _____ руб. ____ коп.
НДС _____ руб. ____ коп.

Услуги выполнены Банком в полном объеме и нареканий со стороны Клиента не вызывают.

От Банка	**От Клиента**
Зам. Председателя Правления	**Генеральный директор**
_____/Е.Н. Пономарева/	_____/_____/
Главный бухгалтер	**Главный бухгалтер**
_____/Л.М. Клементьева/	_____/_____/
м.п.	м.п.

ОБРАЗЕЦ

Приложение № 8
к Правилам дистанционного банковского обслуживания клиентов с использованием системы «iBank 2» в КБ «Новый век» (ООО)

СОГЛАШЕНИЕ
о порядке информирования при работе по Системе «iBank 2»

«_____»_____ 201___ г.

Коммерческий Банк «Новый век» (Общество с Ограниченной Ответственностью), именуемый в дальнейшем «Банк», в лице Заместителя Председателя Правления Пономаревой Екатерины Николаевны, действующего(ей) на основании Доверенности № 742 от 26.05.2017, с одной стороны, и _____, именуемое в дальнейшем «Клиент», в лице _____, действующего(ей) на основании _____, с другой стороны, вместе именуемые «Стороны», заключили настоящее Соглашение о нижеследующем:

1. Клиент обязан незамедлительно извещать Банк о компрометации (или подозрении на компрометацию) ключа ЭП Клиента, а также направлять уведомления об утрате ключа ЭП Клиента и(или) его использовании без согласия Клиента любым из перечисленных способов исключительно в следующем порядке:

1 способ направления извещения/уведомления.

Клиент обязан известить/уведомить Банк, позвонив по следующему телефону Банка:**8 (495) 223-00-72**

При этом Клиент обязан сообщить полное наименование Клиента, ФИО владельца ключа ЭП, а также блокировочное слово.

Стороны настоящим пришли к соглашению, что если хотя бы одно из вышеуказанных требований к извещению/уведомлению по телефону не будет выполнено (в частности, извещение/уведомление будет сделано не на вышеуказанный телефонный номер, и/или не будет названо полное наименование Клиента и/или ФИО владельца ключа ЭП Клиента и/или не названо либо неправильно названо блокировочное слово), то Банк не считается извещенным о компрометации (или подозрении на компрометацию) ключа ЭП Клиента/уведомленным об утрате ключа ЭП и (или) его использования без согласия Клиента и не обязан приостанавливать использование в Системе «iBank 2» ключа ЭП Клиента.

2 способ направления извещения/уведомления.

Клиент обязан известить/уведомить Банк путем направления с адреса электронной почты, указанного Клиентом в Сертификате ключа проверки ЭП, на адрес электронной почты Банка block@newbank.ru сканированной копии уведомления/извещения на бумажном носителе, которое в обязательном порядке должно содержать собственноручные подписи уполномоченных лиц Клиента, указанных в Карточке образцов подписей и печать Клиента, оттиск которой заявлен в Карточке.

Стороны настоящим пришли к соглашению, что в случаях, если уведомление/извещение отправлено с любого другого адреса электронной почты Клиента и/или поступило на любой другой адрес электронной почты Банка; и/или хотя бы один образец подписи уполномоченных лиц Клиента и/или оттиск печати Клиента не соответствуют образцам, заявленным в Карточке, то Банк не считается извещенным о компрометации (или подозрении на компрометацию) ключа ЭП Клиента/уведомленным об утрате ключа ЭП и (или) его использования без согласия Клиента и не обязан приостанавливать использование в Системе «iBank 2» ключа ЭП Клиента.

3 способ направления извещения/уведомления.

Клиент обязан известить/уведомить Банк путем направления по факсу с зарегистрированного номера, указанного Клиентом в Сертификате ключа проверки ЭП, на номер факса Банка (495) 223-00-72 сканированной копии уведомления/извещения на бумажном носителе, которое в обязательном порядке должно содержать собственноручные подписи уполномоченных лиц Клиента, указанных в Карточке образцов подписей, и печать Клиента, оттиск которой заявлен в Карточке.

Стороны настоящим пришли к соглашению, что в случаях, если уведомление/извещение отправлено с любого другого номера Клиента и/или поступило на любой другой номер Банка; и/или хотя бы один образец подписи уполномоченных лиц Клиента и/или оттиск печати Клиента не соответствуют образцам, заявленным в Карточке, то Банк не считается извещенным о компрометации (или подозрении на компрометацию) ключа ЭП Клиента/ уведомленным об утрате ключа ЭП и (или) его использования без согласия Клиента и не обязан приостанавливать использование в Системе «iBank 2» ключа ЭП Клиента.

2. Банк обязан информировать Клиента о совершении каждой операции с использованием ключа(ей) ЭП Клиента путем направления Клиенту соответствующего уведомления следующим(и) способом(ами) (в подтверждение выбора способа информирования уполномоченное лицо Клиента проставляет свою собственноручную подпись в соответствующей строке нижеприведенной таблицы):

Уведомление средствами Системы «iBank 2» (Стороны настоящим пришли к соглашению, что при данном способе информирования уведомление о совершении операции считается полученным Клиентом с момента присвоения распорядительному документу Клиента о совершении операции (в частности, платежному документу – платежному поручению Клиента) в Системе «iBank 2» статуса «ОБРАБОТАН», при этом с данного момента обязанность Банка по информированию Клиента является полностью и надлежаще исполненной, Клиент самостоятельно несет ответственность за своевременность вхождения в систему «iBank 2» и за ознакомление со статусом своего распорядительного документа)	
Уведомление посредством направления SMS-сообщения на следующий телефонный номер, указанный Клиентом: (____) _____ - ___ - ___ (Стороны настоящим пришли к соглашению, что при данном способе информирования уведомление о совершении операции считается полученным Клиентом с момента отправки Банком SMS-сообщения на указанный Клиентом телефонный номер, при этом с данного момента обязанность Банка по информированию Клиента является полностью и надлежаще исполненной, Клиент самостоятельно несет ответственность за: - своевременность проверки входящих SMS-сообщений; - своевременность оплаты за использование телефонного номера, за исправность мобильных телефонов, нахождение в зоне покрытия оператора связи, за недопущение ситуаций переполнения памяти мобильных телефонов, что может являться препятствием для приема SMS-сообщений)	

В случае уведомления Клиента посредством направления SMS-сообщений Банк предупреждает Клиента о том, что доставка SMS-сообщений может быть приостановлена на время не более 12 (Двенадцати) часов. Такая приостановка возможна лишь в случаях проведения профилактических работ поставщиком телематических услуг связи. Банк обязан уведомить Клиента по системе «iBank 2» о планируемом приостановлении доставки SMS-сообщений не менее, чем за 2(Два) календарных дня до такого приостановления. По окончании профилактических работ доставка возобновляется.

От Банка	**От Клиента**
Зам. Председателя Правления	**Генеральный директор**
_____/Е.Н. Пономарева/	_____/_____/
Главный бухгалтер	**Главный бухгалтер**
_____/Л.М. Клементьева/	_____/_____/
м.п.	м.п.

Приложение № 9
к Правилам дистанционного банковского обслуживания клиентов с использованием системы «iBank 2» в КБ «Новый век» (ООО)

ПАМЯТКА КЛИЕНТА
о возможных угрозах хищения денежных средств с использованием системы «iBank 2» и способах защиты

Сегодня атаки злоумышленников на банковские счета предприятий и частных лиц, мошенничество с использованием вирусных программ – это не миф, а реальная угроза для бизнеса. При этом кража средств зачастую происходит из-за недостаточного внимания и компетентности пользователей, а также конфиденциальности при обращении с данными со стороны сотрудников самих компаний.

Хищение средств с расчетных счетов возможно при получении злоумышленниками доступа к ключам ЭП и паролям. Для исключения несанкционированного доступа в систему электронного банкинга КБ «Новый век» (ООО) проводит комплекс мероприятий для повышения Вашей информационной и финансовой безопасности. Убедительно просим Вам ознакомиться с «Памяткой о возможных угрозах хищения денежных средств с использованием системы «iBank 2» и способах защиты» и настоятельно рекомендуем придерживаться правил, указанных в ней. Они позволят защитить ваши счета и информацию от взлома.

- Для хранения файлов с ключами ЭП используйте внешние носители: дискеты, флеш-карты. Наилучшим средством защиты являются **USB-токены «iBank 2 Key» - специализированные хранилища, выполненные в виде USB-накопителя**, данные с которых нельзя скопировать на любой другой носитель**.**
- По завершении работы всегда вынимайте внешние носители из компьютера. Никогда не передавайте их третьим лицам и храните отдельно, например, в личном сейфе.
- Работая с USB-токеном «iBank 2 Key», обязательно задавайте пароль **(PIN-код)** доступа достаточной сложности (Достаточной считается длина не менее 10 символов, среди которых обязательно присутствуют строчные и прописные буквы, цифры, спецсимволы). Без его корректного ввода получить доступ к ключам ЭП невозможно.
- Никогда не передавайте третьим лицам одноразовые пароли для подтверждения платежей, приходящие Вам из Банка в виде SMS-сообщений или генерируемые OTP-токеном (устройство генерации одноразовых паролей).
- Используйте **IP-фильтрацию -** дополнительный сервис, запрещающий пользование ключами ЭП на компьютерах вне вашего офиса. В этом случае информация от Вас будет обработана, только если IP-адрес передающего компьютера совпадет с адресом, указанным в базе данных Банка.
- **Не храните** на носителях с ключами ЭП какую-либо **другую информацию**.
- **Не ставьте на компьютеры «пустые» или простые пароли**, например, 123456, qwerty – и периодически меняйте их. Требования к сложности паролей для компьютера – аналогичны требованиям к паролям на USB – токены. Рекомендуемая частота смены паролей -1 раз в месяц;
- **Не передавайте ключи ЭП ИТ-сотрудникам для проверки работы** Системы и настроек взаимодействия с Банком. Если такая проверка необходима, владелец ключа ЭП должен лично подключить носитель к компьютеру, убедиться, что пароль доступа к ключу вводится в интерфейс клиентского АРМа «iBank 2», и вводит пароль, исключая умышленное наблюдение посторонними лицами.
- **Не передавайте ключи ЭП замещающим сотрудникам** (заместителям, временно исполняющим обязанности). Для них необходимо получить персональные ЭП и внести их в банковскую карточку.
- **При увольнении сотрудника**, имевшего доступ к ключу ЭП, **обязательно заблокируйте его ключ** ЭП;
- **При увольнении ИТ-специалиста**, обслуживавшего компьютеры, подключенные к Системе «iBank 2», обязательно **проверьте их на отсутствие вредоносных программ**.
- **При продолжительной работе в Клиент-Банке**, отключите и **извлеките из компьютера носители с ключами** ЭП, если они не используются. Носители с ключами должны находиться в компьютере только в момент подписания документов и извлекаться сразу после подписания документов.
- **Выделите отдельный компьютер для работы с Системой** «iBank 2» и не выполняйте на нем никакие другие задачи (по возможности).
- **Ограничьте доступ к компьютерам**, используемым для работы с Системой «iBank 2» и исключите к ним доступ персонала, не работающего с Системой.
- **Исключите обслуживание компьютеров**, используемых для работы в Клиент-Банке, **нелояльными ИТ-сотрудниками**.
- При обслуживании компьютера ИТ-сотрудниками, **обязательно контролируйте ход выполняемых ими действий**.
- **На компьютерах**, подключенных к Системе, никогда **не посещайте Интернет-сайты сомнительного содержания, не устанавливайте нелицензионное программное обеспечение** и т. п. Наиболее безопасным будет полный запрет на все соединения (входящие и исходящие) с сетью Интернет, оставив доступ к необходимым ресурсам.

- **Используйте только лицензионное программное обеспечение** и обеспечьте его автоматическое обновление.
- **Применяйте только лицензионные средства антивирусной защиты**, обеспечив ежедневное автоматическое обновление антивирусных баз, резидентную защиту в реальном времени и еженедельную полную антивирусную проверку.
- **Используйте специализированные средства безопасности**: персональные межсетевые экраны (файрволлы, МСЭ), антишпионское программное обеспечение.
- **Проверяйте на наличие вирусов все файлы** и программы, загружаемые из Интернета, полученные по электронной почте и на внешних носителях (дискеты, флеш-накопители, CD/DVD).
- **Осуществляйте полную антивирусную проверку после вспомогательных операций** на компьютере, подключенном к системе Электронного банкинга. Например, после решения технических проблем, подключения к сети Интернет, установки или обновления бухгалтерских и информационно-правовых программ.
- **Не допускайте работу под учётной записью Windows, имеющей права администратора**. Необходимо использовать учётную запись с ограниченными правами в операционной системе Windows, установленной на компьютере.
- **С особым вниманием используйте средства удалённого (дистанционного) доступа**, которые часто применяют IT-специалисты для удалённой поддержки. Заблокируйте возможность использования данных систем без непосредственного подтверждения со стороны пользователя АРМ, в остальное время отключите средства удаленного доступа с помощью файрвола (программного и/или аппаратного).
- **При возникновении подозрений** на копирование ключей ЭП или наличие в компьютере вредоносных программ – **обязательно заблокируйте ключи ЭП**.
- **Если Вы заметили проявление необычного поведения Системы** или изменения в интерфейсе программы – срочно **позвоните в Банк** и уточните причину. Если изменения не связаны с обновлением версии программного обеспечения, заблокируйте ключи ЭП.

Предполагаемая аудитория мошенников

Хищение средств с расчетных счетов при получении доступа к ключам ЭП и паролям с целью направления в Банк платежных поручений, заверенных от Вашего лица предположительно могут осуществить:

- Ответственные сотрудники Вашей компании, ранее имевшие доступ к ключам ЭП, например, уволенные директоры, бухгалтеры и их заместители, бывшие совладельцы Компании.
- Штатные ИТ-сотрудники Вашей компании, имеющие или имевшие технический доступ к носителям (дискеты, флеш-носители) с ключами ЭП и к компьютерам компании, подключенным к Клиент-Банку.
- Внештатные, приходящие по вызову ИТ-специалисты, обслуживающие компьютеры Вашей компании, осуществляющие профилактику и подключение к Интернету, установку и обновление бухгалтерских, информационно-правовых и других программ на компьютеры, подключенные к Клиент-Банку.
- Другие злоумышленники путем заражения через Интернет Ваших компьютеров вредоносными программами и хищения ключей ЭП и паролей.

Таким образом, в Банк могут поступать не вызывающие подозрений платежи, направленные злоумышленниками с использованием действующих ключей ЭП, имеющие обычные реквизиты получателей и типовые назначения платежа.

КБ «Новый век» (ООО) напоминает Вам о том, что:

- Банк не имеет доступа к Вашим ключам ЭП и не может от Вашего имени сформировать корректную ЭП под электронным платежным документом.
- Банк никогда не осуществляет рассылку электронных писем с просьбой прислать Ваш ключ ЭП или пароль;
- Банк не рассылает по электронной почте программы для установки на Ваши компьютеры. Если Вы получили подобное письмо от имени Банка, содержащее программу для установки или запрос на предоставление ключей ЭП/паролей, срочно сообщите об этом в Службу технической поддержки клиентов Банка.
- Вы являетесь единственным владельцем ключей ЭП и ответственность за их конфиденциальность лежит на Вас.
- Если Вы сомневаетесь в конфиденциальности ключей ЭП или подозреваете компрометацию (копирование) данных, срочно заблокируйте ваши ключи ЭП.
- Изменение пароля доступа к ключу ЭП не защищает Вас от использования злоумышленниками ранее похищенного ключа. В этом случае необходимо заблокировать старый ключ и получить новый.

Для получения дополнительной информации по техническим вопросам Вы можете обратиться к нашим специалистам. Мы всегда рады Вам помочь.

Приложение № 10
к Правилам дистанционного банковского
обслуживания клиентов с использованием системы
«iBank 2» в КБ «Новый век» (ООО)

Рекомендации по обеспечению безопасности при работе с мобильным приложением "Mobile-Банкинг для корпоративных клиентов"

Несмотря на то, что операционные системы мобильных устройств и приложения имеют различные инструменты для защиты персональных данных и денежных средств, ключевая роль в обеспечении безопасной работы принадлежит пользователю. Следуя приведенным ниже рекомендациям, Клиент максимально обезопасит себя от действий злоумышленников и вредоносного ПО:

• Следует установить и регулярно обновлять специальное антивирусное ПО для мобильных устройств.

•Клиенту надлежит скачивать и устанавливать программное обеспечение из проверенных источников (рекомендованных производителями мобильных устройств).

• На устройствах, используемых для работы с приложением, не рекомендуется выполнять процедуры получения доступа к файловой системе устройства (Jailbreak, Rooting). Такие операции наносят существенный ущерб системе безопасности, предоставленной производителем устройства.

• Скачивать и устанавливать приложение "Mobile-Банкинг для корпоративных клиентов" следует только из официальных магазинов приложений Google Play, AppStore. Разработчиком приложения должна быть указана компания "БИФИТ".

• Не следует записывать и не сохранять свой код доступа к приложению на устройстве, с которого осуществляется работа в приложении.

• Не следует сообщать код доступа третьим лицам, в том числе сотрудникам Банка.

• При получении любых сообщений или писем, связанных с работой приложения, следует обращать внимание на отправителя. Подобные сообщения должны поступать только с официального сервисного номера или адреса электронной почты Банка.

• Не следует переходить по ссылкам и не открывать вложения из писем от подозрительных или неизвестных отправителей.

• После завершения работы с документами и банковскими счетами каждый раз следует выполнять выход из приложения (Меню → Выход).

• При подозрении, что код доступа Клиента к приложению стал известен посторонним лицам или при получении уведомлений об операциях по счету, которых Клиент не совершал, немедленно обратиться в Банк и заблокировать свою учетную запись.