

## 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 ДБО в КБ «Новый век» (ООО)

## 1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящие Правила дистанционного банковского обслуживания клиентов с использованием системы ДБО в КБ «Новый век» (ООО) определяют порядок заключения и расторжения Договора о дистанционном банковском обслуживании с использованием Системы ДБО, заключаемого в целях предоставления Банком услуг по дистанционному банковскому обслуживанию по Системе ДБО 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 работника 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 путем присоединения 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) (далее - Правила РКО).

1.5. Все термины и определения, прямо не описываемые в настоящих Правилах, применяются согласно тем определениям, которые даны в Правилах РКО и приложениях к Правилам РКО.

1.6. Используемые термины и определения.

Применительно к настоящим Правилам используется следующая терминология.

**Правила ДБО** - Правила дистанционного банковского обслуживания клиентов с использованием системы ДБО в КБ «Новый век» (ООО).

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

**Авторство ЭД** – свойство ЭД, определяющее принадлежность НЭП конкретному физическому лицу - участнику электронного документооборота в Системе ДБО.

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

**Блокировочное слово** – словесный пароль, конфиденциальный для всех кроме уполномоченных

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

**ДБО** – система дистанционного банковского обслуживания.

**Двухфакторная аутентификация** – аутентификация Клиента по постоянному паролю и одноразовому паролю, высылаемому Банком в виде SMS-сообщения.

**Договор** - объявленные Банком стандартные условия дистанционного банковского обслуживания Клиентов с использованием системы ДБО в КБ «Новый век» (ООО). Договор является договором присоединения и заключается с Клиентом путем направления Клиентом Банку заявления на подключение услуг в системе ДБО.

**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.

**Идентификация Клиента** – процесс подтверждения прав Клиента на выполнение определенных действий в Системе ДБО согласно перечню прав Клиента, установленных в системе, и предоставления прав на выполнение данных действий.

**Усиленная Квалифицированная электронная подпись - КЭП** - электронная подпись, соответствующая требованиям, предусмотренным частью 4 статьи 5 Федерального закона от 06.04.2011 №63-ФЗ «Об электронной подписи» (далее - Закон об электронной подписи). Информация в электронной форме, подписанная КЭП, признается электронным документом, равнозначным документу на бумажном носителе, подписанному собственноручной подписью. Проверка действительности подписи осуществляется сертифицированным программным обеспечением.

**Клиентский модуль (клиентская часть)** - on-line модуль — Java или HTML5-апплет, загружаемый в компьютер Клиента через глобальную сеть интернет в начале каждого сеанса связи Клиента с сервером Банка по Системе ДБО. При использовании онлайн модуля обмен информацией между клиентским модулем и сервером Системы возможен только путём соединения через глобальную сеть интернет. Вход в Систему осуществляется с помощью ключа НЭП с вводом пароля ключа НЭП.

**Ключ НЭП** – последовательность байтов, самостоятельно генерируемая Клиентом с использованием средств Системы и предназначенная для формирования НЭП электронного документа, т.е. секретная часть ключевой информации, представляющая собой уникальную последовательность двоичных данных и предназначенная для создания в электронном документе электронной подписи владельца НЭП, хранится владельцем ключевой информации в тайне. Клиент самостоятельно обеспечивает конфиденциальность ключа НЭП. Срок действия ключа НЭП считается с даты регистрации Сертификата ключа проверки НЭП Банком в системе ДБО по дате, определяемую в соответствии с п. 6.2. Правил ДБО и Регламентом (Приложение №5 к Договору). Носителями ключа НЭП или Ключевым носителем являются: USB-токен или его аналоги. В случае использования облачной подписи, ключ хранится в защищённой зоне на оборудовании Банка.

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

**Облачная подпись** – сочетание Ключа НЭП и Ключа проверки НЭП, самостоятельно генерируемые Клиентом с использованием средств Системы, хранящиеся в защищённой зоне на оборудовании Банка.

**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.

**Компрометация ключа НЭП** — утрата доверия к тому, что используемые ключи НЭП 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 работников, 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 ДБО) 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.

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

**Код подтверждения** – уникальный набор символов, состоящий из 6 или 8 цифр, направляемый Клиенту Системой ДБО посредством SMS -сообщения и служащий для подтверждения произведенной операции или действия в системе ДБО.

**Корректная НЭП** — электронная подпись электронного документа, дающая положительный результат её проверки средствами Системы ДБО с помощью ключа проверки НЭП.

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

**Носители ключевой информации (ключевые носители)** – физический носитель, на котором записан и хранится ключ НЭП. 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 ДБО Клиент самостоятельно определяет тип носителя ключевой информации. Для повышения безопасности пользования Системой ДБО Банк рекомендует Клиенту пользоваться персональным аппаратным криптопровайдером.

**Операционное обслуживание клиентов** - время, установленное для приема и обработки поступивших платежных документов приказом по КБ «Новый век» (ООО). Изменения в операционном обслуживании доводятся до Клиента в ЭСИД с использованием Системы ДБО.

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

**Подлинность ЭД** – свойство ЭД, означающее, что данный ЭД создан в Системе ДБО Клиентом без отступлений от принятой технологии. Электронный документ считается подлинным, если он был, с одной стороны, должным образом оформлен, заверен (подписан) НЭП 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 ДБО.

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

**Представление 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 ДБО, а также при помощи другого программного обеспечения, входящего в состав Системы ДБО.

**Система ДБО (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.

**Сертификат ключа проверки НЭП сотрудника Клиента (Сертификат ключа проверки НЭП)** – документ на бумажном носителе или документ, в электронном виде, поступивший по телекоммуникационным каналам связи, 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 НЭП; содержит информацию о его назначении и области применения. Сертификат, поступивший на бумажном носителе, удостоверяется подписями уполномоченных лиц Сторон и заверяется оттиском печати Клиента и Банка. Сертификат, поступивший в электронном виде, заверяется КЭП или действующей НЭП Клиента. Форма Сертификата (Приложение №2 к Правилам ДБО) формируется автоматически программными средствами Системы ДБО в процессе генерации Клиентом ключей НЭП.

**СКЗИ (средство криптографической защиты информации)** — это программа или устройство, которое шифрует документы и генерирует электронную подпись (НЭП). Все операции производятся с помощью ключа электронной подписи, который невозможно подобрать вручную, так как он представляет собой сложный набор символов.

**Телекоммуникационный канал связи** — это спутниковый, наземный радио-коммуникационный канал передачи информации, или канал связи в компьютерных сетях для подключения двух или более точек.

**Усиленная Неквалифицированная Электронная подпись (НЭП)** — последовательность байтов, являющаяся результатом работы, входящей в Систему ДБО программы генерации электронной подписи. НЭП 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. НЭП позволяет удостовериться в подлинности, целостности этого ЭД, установить его авторство. НЭП жестко увязывает в одно целое содержимое ЭД и секретный ключ подписывающего лица и делает невозможным изменение этого документа без нарушения корректности (подлинности) данной НЭП. Средства НЭП, входящие в состав Системы, реализуют алгоритмы формирования НЭП и её проверки в соответствии со стандартом ГОСТ Р 34.10-94. НЭП соответствует требованиям к неквалифицированной электронной подписи, предусмотренным частью 3 статьи 5 Закона об электронной подписи.

**Уполномоченные службы Банка** – подразделения Банка, осуществляющие техническое и организационное взаимодействие с Клиентом в рамках его обслуживания по Системе ДБО.

**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.

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

**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, в том числе средствами Системы ДБО, 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 НЭП 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 являющейся основанием для совершения операции по счету Клиента, открытому в Банке.

**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.

**Интернет-Банк для корпоративных клиентов** (далее по тексту приложения **Интернет-Банк**) - приложение, в котором Клиент может с любого мобильного устройства на платформах iOS и Android, веб браузера на платформах Windows или MAC OS 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 Интернет-Банк позволяет корпоративным клиентам осуществлять доступ к Системе ДБО и ограниченный функционал через мобильные устройства.

**USB-токен (токен)**- разновидность персональных аппаратных криптопровайдеров. Это аппаратное USB-устройство, которое объединяет в компактном корпусе USB-картридер и карточный криптографический микроконтроллер (криптопровайдер). В Системе ДБО используются несколько разновидностей USB-токенов различных производителей.

**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.

## **2. ПРЕДМЕТ ДОГОВОРА**

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

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

2.3. Клиент и Банк признают, что используемые во взаимоотношениях Сторон документы, подписанные электронной подписью (НЭП), в том числе с использованием механизма облачной подписи), подготовленные и переданные одной Стороной другой Стороне с помощью программного обеспечения Системы ДБО, а также прикрепленные к созданным в Системе письмам изображения документов в виде файлов (в форматах jpeg, pdf, tiff, rtf, документы MS Office)<sup>1</sup>, 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.

2.4. Электронные документы подготавливаются и обрабатываются с помощью программного обеспечения Системы ДБО, в том числе приложений Интернет-Банк, в течение рабочего времени Банка. На время перерывов в функционировании Системы ДБО 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.

2.5. Стороны доверяют используемому программному обеспечению Системы ДБО. Стороны признают, что используемое в Системе ДБО программное СКЗИ, сертифицировано 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.

2.6. Система ДБО 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.

2.7. Сертификат ключа НЭП сотрудника Клиента в Системе ДБО автоматически формируется из клиентской части Системы ДБО в момент осуществления Клиентом генерации ключей НЭП.

### **3. ПРАВА И ОБЯЗАННОСТИ СТОРОН**

#### **3.1. Банк обязуется:**

3.1.1. После получения оплаты комиссии за предоставление USB-токена провести регистрацию ключей НЭП Клиента в порядке, установленном настоящими Правилами, не позднее 3 (трех) месяцев с момента заключения настоящего Договора. Если Банк получил комиссию за предоставление USB-токена по истечении 3 (трех) месяцев с момента заключения настоящего Договора, регистрация ключей НЭП Клиента проводится не позднее рабочего дня, следующего за днем поступления комиссии на соответствующий счет Банка.

Принимать к исполнению полученные по Системе ДБО 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.

3.1.2. Осуществлять операции по счету Клиента в пределах остатка денежных средств, за исключением случаев предоставления Банком овердрафта по счету Клиента или осуществления встречных платежей, условия которых оговариваются отдельными соглашениями Сторон.

3.1.3. Предоставлять Клиенту информацию по видам сообщений, которые Клиент передает в Банк и получает из Банка по Системе ДБО в соответствии с Приложением №3 к настоящему Договору.

3.1.4. Информировать Клиента о совершении каждой операции с использованием ключа (ей) электронной подписи Клиента, а также о приостановлении или прекращении использования Клиентом Системы ДБО в случаях, предусмотренных Федеральным законом №161-ФЗ и/или настоящим Договором, путем направления Клиенту соответствующего уведомления тем способом, который указан Клиентом в Приложении № 8 к настоящему Договору.

3.1.5. Консультировать персонал Клиента по вопросам обслуживания Системы ДБО на стороне Клиента.

3.1.6. Обеспечивать защиту от несанкционированного доступа в Систему ДБО в пределах своей компетенции, установленной Правилами ДБО, и сохранять конфиденциальность информации по счетам Клиента.

---

<sup>1</sup> Положения о приравнивании, прикрепленных к созданным в Системе письмам, изображений документов в виде файлов (в форматах jpeg, pdf, tiff, rtf, документы MS Office), к документам на бумажном носителе, подписанным должностными лицами Сторон и скрепленными печатью (в случае наличия таковой) – не подлежат применению к заявлению об открытии счета, заявлению о закрытии счета, Приложениям № 1-№ 10 к Правилам дистанционного банковского обслуживания клиентов с использованием системы «ДБО» в КБ «Новый век» (ООО), Приложениям № 1-№ 4 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).

3.1.7. Сообщать Клиенту о ставших известными Банку попытках несанкционированного доступа к Системе ДБО, если это затрагивало операции Клиента, в срок не позднее 1 (одного) рабочего дня с момента обнаружения таких фактов.

3.1.8. Предоставлять Клиенту возможность использования дополнительных услуг (по мере их введения в Банке) в рамках Системы ДБО.

3.1.9. 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 ДБО.

3.1.10. 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 НЭП по форме Приложения № 4.

3.1.11. Без предварительного уведомления Клиента приостановить или прекратить использование НЭП Клиента на основании полученного от Клиента извещения и/или уведомления, направленного в соответствии с подпунктами 3.3.8. и 3.3.9. настоящего Договора.

### **3.2. Банк имеет право:**

3.2.1. Взимать с Клиента за обслуживание в Системе ДБО 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.

3.2.2. В одностороннем порядке вносить изменения в Правила ДБО, изменять Тарифы на обслуживание в Системе ДБО с предварительным уведомлением Клиента за 3 (три) рабочих дня путем размещения информации в порядке, предусмотренном разделом 9 Правил ДБО. 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.

3.2.3. 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.

3.2.4. В случае наличия подозрений в компрометации ключа НЭП Клиента, в одностороннем порядке блокировать действие ключа НЭП с уведомлением об этом Клиента в течение 1 (одного) рабочего дня со дня принятия такого решения с использованием средств связи, обеспечивающих фиксирование отправления. При этом обслуживание Клиента через Систему ДБО приостанавливается. Снятие блокировки либо исключение ключа НЭП Клиента в случае подтверждения факта компрометации ключа осуществляется в порядке, установленном Регламентом.

3.2.5. Без предварительного уведомления Клиента приостановить или прекратить использование НЭП Клиента в случае нарушения Клиентом порядка использования ключа НЭП Клиента, а также не исполнения Клиентом своих обязательств по представлению достоверной информации для связи с ним, предусмотренные пунктом 3.3.12. Правил ДБО. Приостановление или прекращение использования Клиентом НЭП Клиента не прекращает обязательств Клиента и Банка, возникших до момента приостановления или прекращения указанного использования.

3.2.6. Запретить анонимную регистрацию в Системе ДБО.

3.2.7. Осуществлять иные права, установленные Правилами ДБО и приложениями к ним.

### **3.3. Клиент обязан:**

3.3.1. Соблюдать требования Регламента и Руководства пользователя Системы ДБО (далее – Описание), размещенных на официальном сайте Банка в Информационно-телекоммуникационной сети «Интернет» по адресу: <https://newbank.ru/>.

3.3.2. Представить в Банк Сертификат ключа проверки НЭП сотрудника Клиента в Системе ДБО, оформленный в порядке, установленном Регламентом и Правилами ДБО.

3.3.3. Оплачивать обслуживание и иные услуги Банка, связанные с использованием Системы ДБО в порядке и на условиях, установленных действующими Тарифами Банка. Клиент обязуется обеспечить наличие средств на своем счете для своевременной оплаты услуг Банка.

3.3.4. Обеспечить конфиденциальность в отношении использования и хранения ключей НЭП/ паролей/носителей ключевой информации/персональных аппаратных криптопровайдеров/ мобильных устройств, на которых установлено приложение Интернет-Банк.

3.3.5. Обеспечивать предоставление права на работу в Системе ДБО 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.

3.3.6. Самостоятельно и за свой счет обеспечивать безопасность и целостность среды исполнения на

компьютерах и мобильных устройствах, с которых осуществляется работа в Системе ДБО, в том числе обеспечивать защиту от несанкционированного доступа неуполномоченных лиц в Систему ДБО в пределах своей компетенции, обеспечить защиту применяемых аппаратных средств для работы в Системе ДБО от компьютерных вирусов, вредоносного программного обеспечения, в том числе вредоносного кода, несанкционированного удаленного администрирования. Эффективные способы защиты изложены в Памятке клиенту (Приложение № 9 к настоящему Договору). О применении таких способов защиты Клиент обязан сообщать Банку по запросу последнего.

3.3.7. Своевременно обращаться в Банк для блокировки утраченного/украденного токена в случае пользования соответствующей услугой.

В случае компрометации ключа НЭП Клиент обязан прекратить использование ключа НЭП и немедленно известить в простой письменной форме Банк в порядке, указанном в пункте 5.4. Приложения № 5 и Приложения № 8 к настоящему Договору. Такое извещение по телефону не влечет никаких правовых последствий, кроме обязанности Банка приостановить использование в Системе ДБО того ключа НЭП 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 к настоящему Договору на бумажном носителе в предусмотренный Правилами ДБО срок.

3.3.8. В случае утраты ключа НЭП 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 к настоящему Договору 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 к настоящему Договору. В случае если Клиент направил уведомление Банку указанным в настоящем Договоре способом, в тот период времени, который является нерабочим временем Банка, то поступившее уведомление считается полученным Банком в первый рабочий день Банка, следующий за датой отправки уведомления.

3.3.9. Контролировать соответствие суммы платежа и остатка 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.

3.3.10. 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.

3.3.11. 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.

3.3.12. Своевременно уведомлять Банк об изменении номера мобильного телефона и/или адреса электронной почты, используемых для двухфакторной идентификации (Приложение №2 к настоящему Договору). В случае неисполнения/несвоевременного исполнения Клиентом данной обязанности, Банк не несет ответственности за исполнение распоряжения Клиента, подтвержденного с использованием имеющейся у Банка информации о номере мобильного телефона и адреса электронной почты. До момента получения Банком от Клиента сведений о новом (-ых) номере мобильного телефона и/или адреса электронной почты, ранее предоставленные Клиентом номер мобильного телефона и адрес электронной почты Стороны, признают действительными.

3.3.13. Сообщать в течение 3 (трех) банковских дней после получения выписки об ошибочно зачисленных на счет суммах.

#### **3.4. Клиент имеет право:**

3.4.1. Получать от Банка организационно-техническую информацию в рамках обслуживания по Системе ДБО, в том числе информацию в виде электронных документов в соответствии с Приложением №3 к настоящему Договору.

3.4.2. Отзывать платежные поручения по перечислению средств, переданных ранее Банку по Системе ДБО, в форме письма свободного формата, содержащего реквизиты отзываемого платежного поручения, с соблюдением порядка, установленного настоящим пунктом.

3.4.3. Клиент имеет право передавать в Банк все документы, указанные в приложениях к данным Правилам: на бумажном носителе с собственной подписью и печатью (при наличии), либо в виде электронного документа подписанное КЭП (исключая расчётные документы), переданного по телекоммуникационным каналам связи. Банк со своей стороны аналогично подписывает и передает экземпляр клиенту.

#### **4. ПОРЯДОК РАСЧЕТОВ**

4.1. За обслуживание Клиента по Системе ДБО, 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 10 Правил ДБО.

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

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

#### **5. КОНФИДЕНЦИАЛЬНОСТЬ ИНФОРМАЦИИ**

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

5.2. Клиент обязан соблюдать конфиденциальность информации, касающейся Системы ДБО.

5.3. Клиент согласен на передачу ему Банком конфиденциальной информации о его счетах и совершаемых им операций по счетам через сеть интернет с использованием защищенного SSL-соединения, а также применения дополнительного шифрования передаваемого трафика с использованием российских криптографических алгоритмов.

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

5.5. Сведения, содержащиеся в документах, переданных Сторонами друг другу по Системе ДБО, 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.

5.6. Все конфиденциальные сведения хранятся и уничтожаются Сторонами в соответствии с порядком и сроками хранения и уничтожения этих сведений.

#### **6. ОТВЕТСТВЕННОСТЬ СТОРОН И РАСПРЕДЕЛЕНИЕ УБЫТКОВ**

6.1. Стороны несут ответственность за достоверность информации, предоставляемой друг другу в рамках использования Системы ДБО.

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

6.3. За не уведомление Банка в соответствии с пунктом 3.3.13. настоящего Договора об ошибочно зачисленных на счет Клиента суммах Клиент уплачивает Банку за каждый день просрочки пени в размере 0.05% от ошибочно зачисленной на счет Клиента суммы.

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

6.5. Банк не несет ответственности за исполнение ЭД Клиента, подготовленного и переданного без участия уполномоченных лиц Клиента, указанных в Сертификате ключа проверки НЭП, в том числе при смене указанных лиц и непредставлении 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 НЭП Клиента и целостности информации.

6.6. Банк не несет ответственности за ущерб, причиненный Клиенту в результате использования ключа НЭП Клиента и его носителя, а также средств многофакторной аутентификации Клиента третьими лицами, не имеющими права работать с Системой ДБО 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.

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

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

6.9. Стороны не несут ответственности за работу глобальной сети интернет, 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 интернет, ее программ и протоколов, иных телекоммуникационных каналов и систем связи Сторонами не принимаются и не рассматриваются.

6.10. Клиент согласен с тем, что Банк не несёт никакой ответственности за ошибки или сбои в работе Системы ДБО, 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.

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

6.12. 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 интернет, 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 настоящему 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.

6.13. В случае возникновения обстоятельств, указанных в п. 6.12. настоящего Договора Сторона, подвергаясь их воздействию, уведомляет об этом другую Сторону в письменной форме в течение 2 (двух) рабочих 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 настоящему Договору.

6.14. Если обстоятельства, указанные в п. 6.12 настоящего Договора., и их последствия будут существовать больше 6 (шести) 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.

6.15. 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 ДБО, в том числе при её неработоспособности или приостановлении обслуживания Клиента через Систему ДБО Банком в одностороннем порядке.

6.16. 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.

## **7. ОСОБЫЕ УСЛОВИЯ**

7.1. 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.

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

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

Ключи (подписи и соответствующий ему ключ проверки) НЭП Клиента считаются зарегистрированными в Системе ДБО с момента регистрации Банком надлежащим образом оформленного Сертификата ключа проверки НЭП.

Сертификат ключа проверки НЭП может поступать в Банк, как на бумажном носителе, так и в электронном виде по телекоммуникационным каналам связи, подписанным КЭП или действующей НЭП Клиента.

Исчисление срока действия ключа НЭП осуществляется с даты регистрации Сертификата ключа проверки НЭП в системе ДБО и составляет 1 (Один) год.

Срок действия ключа проверки НЭП равен сроку действия ключа НЭП.

Выпуск нового ключа проверки НЭП можно провести в Системе ДБО до окончания срока действия действующего сертификата. Клиент самостоятельно генерирует новую НЭП, путем подачи Заявления по форме Приложения № 11 к настоящему Договору в системе ДБО. Для выпуска сертификата, подписанного действующим ключом, не требуются скан-копии документов и посещение Банка. Инструкция по обновлению сертификата в Приложении №12к настоящему Договору.

Процедуры генерации (создания), регистрации, смены, блокировки и исключения ключей НЭП производятся в соответствии с Регламентом.

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

7.4. Обязательства Сторон по НЭП, вытекающие из настоящего Договора, возникают после регистрации НЭП Клиента в Системе ДБО.

ЭД имеет силу только в случае, если по результатам его проверки Системой ДБО будет установлена корректность НЭП Клиента, подлинность и целостность ЭД.

7.5. На основании требований Федерального Закона от 08.07.2006 №152 ФЗ «О персональных данных» владелец ключа НЭП для возможности обработки Банком его персональных данных, содержащихся в Сертификате ключа проверки НЭП, 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 НЭП, а, следовательно, не имеет возможности зарегистрировать ключи НЭП Клиента в Системе ДБО и надлежащим образом исполнять обязанности по настоящему Договору.

## **8. РАЗРЕШЕНИЕ СПОРОВ**

8.1. 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 к настоящему Договору).

8.2. Банк обязан рассматривать заявления Клиента, в том числе при возникновении Споров, связанных с использованием Клиентом его ключа НЭП, 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 НЭП 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.

8.3. 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.

8.4. В ходе рассмотрения комиссией Спора о подлинности и/или целостности ЭД, обрабатываемого/обработанного с помощью Системы ДБО, подписанного НЭП, 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.

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

8.6. 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 не достижения соглашения Сторон, отсутствия согласия по Спорам и добровольного исполнения решения комиссии, Споры по настоящему Договору передаются на рассмотрение Арбитражного суда г. Москвы.

## **9. СРОК ДЕЙСТВИЯ ДОГОВОРА И ПОРЯДОК ЕГО ИЗМЕНЕНИЯ И РАСТОРЖЕНИЯ**

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

9.2. 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.3.2.2. Договора, и при расторжении Договора банковского счета.

9.3. Дата акцепта Банком предложения (оферты) Клиента о заключении Договора о дистанционном банковском обслуживании по системе ДБО определяется Банком в Заявлении о присоединении согласно Приложению №1 к настоящему Договору.

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

9.5. В соответствии с п.1 статьи 450 Гражданского кодекса Российской Федерации Стороны договорились, что Банк имеет право в одностороннем внесудебном порядке вносить изменения и/или дополнения в Правила ДБО (включая все приложения к ним) и Тарифы, в том числе путем утверждения новой редакции Правил ДБО и Тарифов.

При этом изменения и/или дополнения, внесенные Банком в Правила ДБО и/или Тарифы, становятся обязательными для Сторон в дату введения редакции Правил ДБО и/или Тарифов в действие, установленную Банком.

9.6. Банк также вправе в одностороннем порядке утверждать формы документов (заявлений, уведомлений, сообщений, актов и других), применяемых при исполнении Договора, и вносить в них изменения, в том числе путем утверждения новых редакций форм документов.

9.7. Изменения и/или дополнения в Правила ДБО (включая приложения к ним) и/или Тарифы, внесенные Банком, доводятся до Клиента Банком не менее чем за 3 (три) рабочих дня до вступления изменений/дополнений в силу путем размещения соответствующей информации в порядке, предусмотренном разделом 10 Правил ДБО.

9.8. Клиент обязан самостоятельно или через своего представителя ежедневно знакомиться с информацией, в том числе новой редакцией Правил ДБО, Тарифов и прочей информацией, размещаемой Банком в соответствии с разделом 10 Правил ДБО. В случае несогласия Клиента с изменениями и/или дополнениями Правил и/или Тарифов Клиент вправе расторгнуть настоящий Договор в порядке, установленном пунктом 9.2. Правил ДБО.

9.9. Банк не несет ответственности, если информация об изменении и/или дополнении Правил ДБО и/или Тарифов, размещенная в порядке и сроки, установленные Правилами ДБО, не была получена и/или изучена и/или правильно истолкована Клиентом.

9.10. Любые изменения и/или дополнения в Правила ДБО (включая все приложения к ним) и/или Тарифы с момента их вступления в силу равно распространяются на всех Клиентов, заключивших Договоры, том числе заключивших настоящий Договор ранее даты вступления изменений и/или дополнений в силу.

## **10. РАЗМЕЩЕНИЕ ИНФОРМАЦИИ**

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

- размещение информации, в том числе Правил ДБО, приложений к ним, Тарифов, форм документов на официальном сайте Банка в информационно-телекоммуникационной сети «Интернет» <https://newbank.ru/>;

- размещение информации на информационных стендах в местах обслуживания клиентов Банка;

- иными способами, позволяющими Клиенту получить информацию.

10.2. Моментом размещения (публикации) Правил ДБО, приложений к ним, форм документов и информации считается момент их первого размещения на официальном сайте Банка в информационно-телекоммуникационной сети «Интернет» <https://newbank.ru/>.

## 11. ПРИЛОЖЕНИЯ

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

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

**Приложение №2** - Заявление на изменение данных для двухфакторной аутентификации в системе ДБО.

**Приложение №3** - Перечень электронных документов, пересылаемых по Системе ДБО.

**Приложение №4** - Заявление о блокировке/исключении ключа НЭП Клиента из Системы ДБО.

**Приложение №5** - Регламент банковского обслуживания с применением Системы ДБО.

**Приложение №6** - Порядок разрешения споров.

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

**Приложение №8** - Соглашение о порядке информирования при работе по Системе ДБО.

**Приложение №9** - Памятка Клиента о возможных угрозах хищения денежных средств с использованием системы ДБО и способах защиты.

**Приложение №10** - Рекомендации по обеспечению безопасности при работе с Интернет-Банк для корпоративных клиентов и индивидуальных предпринимателей.

**Приложение №11** - Заявление на выпуск сертификата ключа проверки НЭП.

**Приложение №12** - Инструкции по выпуску сертификата юридического лица на токене/в облаке.

**Заявление о присоединении № \_\_\_\_\_**  
**к Правилам дистанционного банковского обслуживания клиентов с использованием**  
**системы ДБО 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	адрес электронной почты
<b>Данные для двухфакторной аутентификации:</b>	
Номер мобильного телефона для направления SMS-сообщений	адрес электронной почты

Оферта на заключение Договора о дистанционном банковском обслуживании по системе ДБО:

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

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

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

В случае акцепта Банком в порядке, предусмотренном Правилами ДБО, настоящей оферты считать Договор о дистанционном банковском обслуживании по Системе ДБО 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 ДБО, 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 ДБО, настоящей оферты, Клиент:

- полностью и, безусловно, принимает все условия Правил ДБО;
- ознакомлен и согласен с Правилами ДБО и Тарифами Банка, в том числе с правом Банка на внесение изменений в Правила ДБО 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.

III. Настоящим Клиент проинформирован, что в случае взлома его НЭП Клиент обязан немедленно уведомить об этом Банк любым способом.

В случае акцепта Банком настоящей оферты прошу предоставить на указанный адрес электронной почты, сертифицированные криптобиблиотеки для работы в Системе ДБО.

**ПЕРЕЧЕНЬ ДОПОЛНИТЕЛЬНЫХ УСЛУГ, ОКАЗЫВАЕМЫХ БАНКОМ ПРИ ОБСЛУЖИВАНИИ  
КЛИЕНТОВ В СИСТЕМЕ ДБО**

Произвести настройку ПЭВМ Клиента для работы в Системе ДБО специалистами Банка, на территории Банка. Количество ПЭВМ, на которых необходимо провести настройку \_\_\_\_\_ шт.

Подключить сервис работы в Системе ДБО по определенным IP-адресам  
(услуга предоставляется в соответствии с Тарифами Банка):

Да     Нет    Системой ДБО будут приниматься только те ЭД Клиента, которые были направлены с указанного клиентом IP адреса (диапазона IP адресов). Иные ЭД Клиента, приниматься Системой ДБО не будут.

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

IP-адреса	Диапазоны IP-адресов

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

тип криптопровайдера	кол-во, шт.
USB-токен	

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

с нашего счета № \_\_\_\_\_ Договор банковского счета № \_\_\_\_\_ от «\_\_» \_\_\_\_\_ 20 \_\_ г.

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.

Руководитель/представитель Клиента, \_\_\_\_\_, действующий на основании \_\_\_\_\_

\_\_\_\_\_ /  
подпись

\_\_\_\_\_ /  
ФИО

Главный бухгалтер \_\_\_\_\_

\_\_\_\_\_ /  
подпись

\_\_\_\_\_ /  
ФИО

М.П.

**Отметка Банка:**

Заявление-оферта принято « \_\_\_\_\_ » \_\_\_\_\_ 20 \_\_ г.

Ответственный исполнитель, осуществляющий настройку в Системе ДБО:

\_\_\_\_\_  
подпись с расшифровкой

Настройка доступа осуществлена « \_\_-\_\_ » \_\_\_\_\_ 20 \_\_ г.

**Отметка Банка об акцепте оферты Клиента:**

Оферта Клиента об открытии Договора о дистанционном банковском обслуживании по системе ДБО акцептована, Договор о дистанционном банковском обслуживании по системе ДБО заключен на условиях, изложенных в Правилах.

Дата акцепта « \_\_\_\_\_ » \_\_\_\_\_ 20 \_\_ г.

\*В акцепте отказано « \_\_\_\_\_ » \_\_\_\_\_ 20 \_\_ г.

Представитель Банка \_\_\_\_\_

\_\_\_\_\_ /  
подпись

\_\_\_\_\_ /  
ФИО

М.П.

\*Заполняется в случае отказа Банка в акцепте заявления-оферты

**ЗАЯВЛЕНИЕ**  
**НА ИЗМЕНЕНИЕ ДАННЫХ ДЛЯ ДВУХФАКТОРНОЙ АУТЕНТИФИКАЦИИ В**  
**СИСТЕМЕ ДБО**

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

Просим использовать для двухфакторной аутентификации в системе ДБО КБ «Новый век» (ООО) следующие данные:

Е-mail		Номер моб. телефона	+7
Подпись	Должность	Дата	
М.П.			

-----  
*Отметки Банка:*

Заявление получено Банком, предоставленные Клиентом сведения проверил:

Должность	Подпись	Инициалы, фамилия	Дата
-----------	---------	-------------------	------

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

**ПЕРЕЧЕНЬ ЭЛЕКТРОННЫХ ДОКУМЕНТОВ, ПЕРЕСЫЛАЕМЫХ ПО СИСТЕМЕ ДБО**

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

<i>№ п.п.</i>	<i>Наименование ЭД</i>	<i>Вид сообщения</i>
<i>1</i>	<i>2</i>	<i>3</i>
1	Платежное поручение по перечислению рублевых средств;	Формализованное
2	Платёжная ссылка СБП одnorазовая/многоразовая	Формализованное
3	Заявление об отказе от акцепта по перечислению рублевых средств;	Формализованное
4	Заявление на перевод средств в иностранной валюте;	Формализованное
5	Поручение на продажу иностранной валюты за рубли;	Формализованное
6	Поручение на покупку иностранной валюты за рубли;	Формализованное
7	Поручение на конвертацию иностранной валюты (покупка одной валюты за другую);	Формализованное
8	Поручение на обратную продажу иностранной валюты;	Формализованное
9	Заявление на перевод иностранной валюты с транзитного счета на текущий;	Формализованное
10	Запрос на получение выписки по рублевым счетам клиента, включая остатки по счетам и приложения к выписке;	Формализованное
114	Запрос на получение выписки по валютным счетам клиента, включая остатки по счетам и приложения к выписке;	Формализованное
12	Документы валютного контроля (контракты, кредитные договоры, справки о валютных операциях, справки о подтверждающих документах, корректирующие справки о валютных операциях и подтверждающих документах)	Формализованное
13	Информационные и сопроводительные письма (к информации для осуществления валютных операций)	Формализованное
14	Заявление на выпуск сертификата ключа проверки ЭП	Формализованное
15	Информация для осуществления валютных операций в виде прикрепленных файлов (договоры, 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 №138-И);	Свободный формат
16	Запрос по вопросам расчетов и другим видам услуг, предоставляемых Банком (в соответствии с адресной книгой).	Свободный формат

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

<i>№ п.п.</i>	<i>Наименование ЭД</i>	<i>Вид сообщения</i>
<i>1</i>	<i>2</i>	<i>3</i>
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 прикрепленными 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:

Представитель Банка

\_\_\_\_\_ / \_\_\_\_\_ /

\_\_\_\_\_ / \_\_\_\_\_ /

М.П.

От Клиента:

\_\_\_\_\_ / \_\_\_\_\_ /

\_\_\_\_\_ / \_\_\_\_\_ /

М.П.

**ПРИЛОЖЕНИЕ № 4**  
**к Правилам дистанционного банковского**  
**обслуживания клиентов с использованием системы**  
**ДБО в КБ «Новый век» (ООО)**

**ЗАЯВЛЕНИЕ О БЛОКИРОВКЕ / ИСКЛЮЧЕНИИ/ ВНЕПЛАНОВОЙ СМЕНЫ КЛЮЧА НЭП КЛИЕНТА ИЗ СИСТЕМЫ ДБО**

\_\_\_\_\_  
(наименование предприятия, организации)

именуемое по договору «Клиент», в лице \_\_\_\_\_  
(должность, фамилия, имя, отчество)

- просит Банк с «\_\_\_» \_\_\_\_\_ 20\_\_ г. исключить ключ НЭП Клиента, со следующим идентификатором ключа проверки НЭП Клиента: \_\_\_\_\_, и исключить указанный ключ проверки НЭП из базы данных Системы ДБО. Соответствующий ему ключ НЭП Клиента утрачивает силу для дальнейшего применения в Системе ДБО с вышеуказанной даты.
- просит Банк с «\_\_\_» \_\_\_\_\_ 20\_\_ г. на период по \_\_\_\_\_ блокировать ключ НЭП Клиента, со следующим идентификатором ключа проверки НЭП Клиента: \_\_\_\_\_, в связи с \_\_\_\_\_.

Соответствующий ему ключ НЭП Клиента временно утрачивает силу для дальнейшего применения в Системе ДБО с вышеуказанной даты на указанный период.

- Просит Банк произвести внеплановую смену ключей НЭП (дополнительная генерация ключей НЭП 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 ДБО:

\_\_\_\_\_  
подпись с расшифровкой

**От Банка:**

**От Клиента:**

**Представитель Банка**

\_\_\_\_\_  
/\_\_\_\_\_/

\_\_\_\_\_

\_\_\_\_\_  
/\_\_\_\_\_/

\_\_\_\_\_  
/\_\_\_\_\_/

М.П.

\_\_\_\_\_  
/\_\_\_\_\_/

М.П.

## **РЕГЛАМЕНТ БАНКОВСКОГО ОБСЛУЖИВАНИЯ С ПРИМЕНЕНИЕМ СИСТЕМЫ ДБО**

### **1. ВВЕДЕНИЕ**

1.1. Система ДБО предназначена для подготовки, приема-передачи по линиям связи, учета и предварительной обработки Банком платежных документов Клиентов.

Система ДБО построена на основе технологии обмена информацией по телекоммуникационной сети, обеспечивающей конфиденциальность, надежность и достоверность передачи информации, установление подлинности отправителя, проверку целостности и авторства платежного документа.

1.2. Настоящий Регламент устанавливает порядок подключения Клиента к Системе ДБО и регламентирует передачу и обработку видов сообщений, указанных в Приложении №3 к настоящему Договору.

1.3. Для работы с Системой ДБО пользователю необходимы:

• Современный компьютер с операционной системой. Работа с сервисом возможна на следующих ОС:

— Microsoft Windows: 7 (x86/x64), 8 (x86/x64), 8.1 (x86/x64), 10 (x86/x64) и выше;

— Apple Mac OS X: 10.7 и выше;

• Монитор с разрешением не менее 1280x1024;

• Для обеспечения защиты конфиденциальной информации необходимо наличие СКЗИ на компьютере пользователя. СКЗИ используется для реализации функций формирования ключей шифрования и электронной подписи, выработки и проверки электронной подписи, шифрования и имитозащиты информации.

• Web-браузер с поддержкой BIFIT Signer для использования электронной подписи. Поддержка BIFIT Signer обеспечена в следующих браузерах:

• Microsoft Edge;

• Google Chrome;

• Яндекс.Браузер;

• Firefox;

• Opera;

• Atom;

• Safari (при условии, что браузер используется совместно с Mac OS X).

Рекомендуется использовать последние версии браузеров.

• Необходимо наличие в компьютере пользователя USB-порта для подключения аппаратных устройств.

• Доступ в Интернет. Рекомендуемая скорость соединения — 33,6 Кбит/сек и выше.

• Рекомендуется наличие принтера.

Требования к операционным системам на мобильных устройствах:

• iOS - новее 14 версии

• Android - новее 7.1 версии

1.4. При работе в Системе ДБО Клиент обязан руководствоваться Правилами дистанционного банковского обслуживания с использованием Системы ДБО в КБ «Новый век» (ООО), данным Регламентом и Руководством пользователя Системы ДБО для клиентов – юридических лиц (именуемым далее – Описание), а также Обзором приложения для мобильных устройств, размещенными в сети интернет адресу <https://newbank.ru>. Описание является составной частью настоящего Договора. В случае противоречий между Описанием и Договором применяются нормы последнего.

### **2. ОБЩИЕ ПОЛОЖЕНИЯ**

2.1. Система ДБО 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 Интернет-Банк может быть ограничен только разработчиком Системы ДБО АО «БИФИТ».

2.2. Электронные платежные документы, применяемые в Системе ДБО, 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 ДБО 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 ДБО, 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 ДБО 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 НЭП становится некорректной, то есть её проверка даёт отрицательный результат;

- подделка НЭП, то есть создание корректной НЭП ЭД, направленного Клиентом, невозможна без знания ключа НЭП и пароля;

- Клиент уведомлен, что Система не предусматривает подписание Банком исходящих от Клиента 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 иницирующей Стороной должным образом оформлен (документ содержит все реквизиты платежного (расчетного) документа, установленные банковскими правилами), НЭП 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 ДБО.

2.5. Готовность Сторон к работе по Системе ДБО оформляется заполнением Сторонами Акта приема материалов и/или выполненных работ, а также подписанием Сторонами необходимого количества Сертификатов ключей НЭП.

2.6. Банк оставляет за собой право использовать записи и данные журналов событий и аудита средств защиты, установленных, как в контуре Системы ДБО, так и вне её предела, а также документов, направленных Клиентом по Системе ДБО для доказательного разрешения споров, возникших в рамках данного Договора.

2.7. Ключ НЭП записывается Системой в зашифрованном виде на персональный аппаратный криптопровайдер или в защищенное облачное хранилище Банка. В первом случае, ключ НЭП хранится на персональном аппаратном криптопровайдере, именуемым - «ключевой носитель», во втором случае – в защищенном облачном хранилище Банка. Ключ НЭП используется уполномоченными лицами Клиента в целях подписи ЭД/ЭПД, подготовленных с помощью Системы ДБО.

2.8. Ключ проверки НЭП после регистрации Клиента, хранится Банком в базе данных Системы ДБО.

2.9. Архив входящих и исходящих ЭД хранится Банком в базе данных Системы ДБО.

2.10. Проверка подлинности НЭП под ЭД осуществляется в автоматическом режиме программными средствами Системы ДБО.

### **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 НЭП лиц, идентификатор ключа проверки НЭП которых соответствует данным, указанным в Сертификате ключа проверки НЭП.

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 ДБО. Оказывать консультационные услуги Клиенту по вопросам технической и организационной поддержки в рамках оказания услуг с использованием Системы ДБО, а также информировать и оказывать консультационные услуги Клиенту по вопросам информационной безопасности при работе в Системе ДБО.

3.1.7. Осуществлять необходимую модернизацию программного обеспечения Системы ДБО.

3.1.8. Сообщать Клиенту о плановых работах или непредвиденных сбоях в работе Системы ДБО 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 ДБО для получения/передачи ЭД в Банк/из Банка.

3.2.2. Ознакомиться с инструкциями по работе в Системе ДБО, размещенными на сайте Банка <https://newbank.ru/> и руководствоваться их требованиями и положениями при работе в Системе ДБО.

Ознакомиться с Обзором приложения для Интернет-Банк, размещенным на сайте Банка <https://newbank.ru/> и руководствоваться им при работе в Системе ДБО.

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 НЭП, носителей ключевой информации, паролей и кодов доступа и другой информации, передаваемой и получаемой по Системе ДБО.

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 ДБО 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 ДБО.

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 ДБО.

3.3.2. Не осуществлять операцию по ЭД, заверенному НЭП, если программа проверки, используя действующий ключ проверки подписывающей Стороны, не подтвердила подлинность НЭП 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 ДБО.

3.3.5. Вести архивы передаваемых и получаемых по системе ДБО 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 ДБО и предполагает использование Клиентом этой же Системы.

4.1.2. Банк и Клиент взаимно признают достаточную криптографическую устойчивость используемых в Системе ДБО алгоритмов, используемых для создания ключа ЭП.

4.1.3. Стороны взаимно признают достоверность и достаточную защищенность от подделок НЭП, созданной посредством Системы ДБО, на ЭД, передаваемых согласно условиям настоящего Договора.

4.1.4. После заполнения Клиентом Заявления (Приложение №4 к настоящему Договору) и оплаты вознаграждения Банка за выбранные в рамках Договора услуги Стороны проводят техническую и организационную подготовку по подключению Клиента к Системе ДБО и регистрации ключей НЭП 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 настоящему Договору) и Сертификат ключа проверки НЭП.

4.1.5. Подготавливаемые в Системе ДБО 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 ДБО.

4.1.6. После заполнения электронной формы платежного или иного документа Клиента осуществляется его подписание. Клиент подписывает ЭД своей НЭП, 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 НЭП, 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 НЭП 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, ФНС 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 ДБО 24/7. Прием и обработка платежных ЭД, поступивших по системе ДБО, осуществляется в течение времени, установленного для обработки поступивших платежных документов, приказом по Банку.

4.2.2. Гарантированная работа Системы ДБО 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 ДБО 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 ДБО, Клиент до 17:30 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 ДБО 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 ДБО.

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

- создание (генерация) ключей/ключей проверки шифрования и НЭП;
- НЭП под ЭД;
- шифрование передаваемой информации;
- аутентификацию Клиентов и разграничение их прав;
- достоверность факта получения документа получателем;
- проверка корректности НЭП;
- 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 НЭП, а также архивы ключей проверки НЭП. 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 НЭП Клиента, подписавшего ЭД.

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

## 5.2. ПОРЯДОК ГЕНЕРАЦИИ И РЕГИСТРАЦИИ КЛЮЧЕЙ НЭП

5.2.1. В процессе предварительной регистрации Клиент самостоятельно создает ключ НЭП и парный ему ключ проверки НЭП. Ключ НЭП Клиента сохраняется в файле на ключевом носителе Клиента (персональном аппаратном криптопровайдере)<sup>2</sup> или в облачном хранилище Банка. Ключ проверки НЭП по защищенному соединению передается в Банк и предварительно регистрируется в Системе ДБО.

Ключ проверки НЭП может быть распечатан Клиентом на бумажном носителе в форме Сертификата ключа проверки НЭП в двух экземплярах. Оба экземпляра Сертификата должны быть подписаны руководителем и главным бухгалтером Клиента (при наличии в штате) с проставлением оттиска печати Клиента и представлены в Банк для регистрации согласно п.5.2.5 настоящего Регламента.

Также ключ проверки может быть сформирован в электронном виде в форме Сертификата ключа проверки НЭП, подписан КЭП или действующей НЭП Клиента. Сертификат ключа проверки НЭП, подписанный действующей НЭП Клиента и направляется в Банк посредством Системы ДБО. Сертификата ключа проверки НЭП, подписанный КЭП направляется в Банк по телекоммуникационным каналам связи.

Форма Сертификата приведена в Приложении №2 к Договору.

5.2.2. Все ключи НЭП 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 НЭП, созданных в Системе ДБО, несут персональную ответственность за обеспечение сохранности ключевой информации, защиты ключевых файлов (элементов) и ключевых носителей от несанкционированного доступа.

5.2.4. Процедуры регистрации и проверки ключей проверки НЭП, производятся в помещениях Банка на программном обеспечении и оборудовании Банка.

5.2.5. При регистрации ключа проверки НЭП Клиента в Банке производится сверка ключа проверки НЭП Клиента с ключом проверки НЭП, указанным в Сертификате ключа проверки НЭП, и проверка лиц, на имя которых сформированы ключи, на соответствие именам, фамилиям, отчествам (при наличии) образцам подписей и оттиску печати, указанным в банковской карточке Клиента и Соглашении о праве подписи, хранящимся в Банке – в случае предоставления Клиентом Сертификата ключа проверки НЭП на бумажном носителе.

В случае поступления Сертификата ключа проверки НЭП в банк в электронном виде, производится проверка лица, которому принадлежит КЭП и действующая НЭП, которыми был скреплен Сертификат ключа проверки НЭП Клиента. Данные лица, которому принадлежит действующая НЭП/КЭП, сверяются с данными уполномоченного представителя Клиента, указанного в банковской карточке Клиента и Соглашении о праве подписи, хранящимся в Банке.

---

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

5.2.6. Ключ НЭП Клиента регистрируется после получения Банком надлежаще оформленного и заверенного Клиентом Сертификата ключа проверки НЭП, а также успешной верификации данных, указанных в п.п.5.2.5 настоящего Регламента. Сертификат проверки ключа НЭП регистрируется в системе ДБО. Исчисление срока действия ключа НЭП осуществляется с даты регистрации Сертификата ключа проверки НЭП в системе ДБО и составляет 1 (Один) год. При регистрации ключа НЭП Клиента в Системе ДБО уполномоченные на совершение соответствующих действий сотрудники Банка проставляют в Сертификате ключа проверки НЭП на бумажном носителе отметки о дате регистрации и сроке его действия в Системе ДБО и заверяют печатью Банка.

В случае если Сертификат ключа проверки НЭП поступил в Банк в электронном виде, срок действия ключа НЭП не проставляется и отсчитывается с даты регистрации Сертификата проверки ключа НЭП в Системе ДБО.

После регистрации ключа НЭП Клиента в Системе ДБО, один экземпляр Сертификата ключа проверки НЭП на бумажном носителе передается Клиенту, второй - остается на хранении в Банке, а его электронный аналог находится в каталоге ключей Банка и Клиента.

Срок действия ключа проверки НЭП равен сроку действия ключа НЭП.

Сертификат проверки ключа НЭП, поступивший в Банк в электронном виде, хранится в Системе ДБО, а также распечатывается и помещается в юридическое дело Клиента.

### 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 НЭП, а также исключения несанкционированного доступа посторонних лиц к Интернет-Банку. К событиям, связанным с компрометацией или подозрением на компрометацию ключа, относятся, включая, но, не ограничиваясь, следующие события:

- утеря носителя ключевой информации, в том числе с последующим обнаружением, а также утрата контроля за доступом к мобильному устройству/компьютеру, на которых осуществляется работа Системы ДБО;

- 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);

- обнаружение факта или угрозы использования (копирования) паролей доступа и/или доступа к Системе ДБО неуполномоченных лиц (несанкционированная отправка электронных документов);

- обнаружение ошибок в работе Системы ДБО, 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 ДБО.

5.3.1.2. Клиент берет на себя полную ответственность и обязуется самостоятельно обеспечить условия хранения своих ключей НЭП, а также пароля и мобильного устройства/компьютера, зарегистрированного в Системе ДБО, исключая возможность их компрометации. В случае потери, кражи, несанкционированного копирования или любого подозрения в компрометации ключей НЭП/паролей Клиент обязан немедленно в письменном виде оповестить Банк о необходимости блокировки ключей НЭП Клиента или необходимости удалить скомпрометированное мобильное устройство Клиента из списка устройств, зарегистрированных в Системе ДБО. Допускается возможность дистанционного оповещения уполномоченного сотрудника Банка о необходимости блокировки ключей НЭП Клиента/удаления мобильного устройства из списка зарегистрированных с последующим обязательным предоставлением в Банк письменного заявления о блокировке ключей НЭП.

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

5.3.2.1. Смена ключей производится при:

- замене банковской карточки Клиента;
- истечении срока действия ключей;

- компрометации ключей;
- предоставлении Клиентом соответствующего заявления в письменной форме.

5.3.2.2. Срок действия ключей НЭП устанавливается (срок действия ключа НЭП исчисляется с даты регистрации Сертификата ключа проверки НЭП в системе ДБО уполномоченным сотрудником Банка) 12 месяцев;

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

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

#### 5.4. ПОРЯДОК БЛОКИРОВКИ КЛЮЧЕЙ НЭП

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 НЭП, составленного по форме Приложения №4 к настоящему Договору, подписанного руководителем и главным бухгалтером Клиента, а также заверенного печатью организации, либо подписано КЭП и передано по телекоммуникационным каналам связи.

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

- по телефону;
- по электронной почте с почтового адреса, 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 НЭП 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 НЭП, а также в случаях, предусмотренных действующим законодательством Российской Федерации. 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 НЭП

5.5.1. Банк блокирует ключ Клиента с момента получения уполномоченными службами Банка письменного заявления Клиента, составленного по форме Приложения №4 к настоящему Договору и подписанного руководителем и главным бухгалтером Клиента (при его наличии). Вход в Систему ДБО, прием и обработка ЭД, подписанных заблокированным Ключом НЭП невозможны.

5.5.2. Ключи НЭП Клиента, срок действия которых истек, признаются недействующими автоматически и блокируются в Системе ДБО. Вход в Систему, так же как и другие операции с использованием просроченного ключа НЭП становятся невозможными. Банк не несет ответственность за несвоевременную смену Клиентом ключей НЭП и возникшие в связи с этим последствия для Клиента.

5.5.3. Банк и Клиент обеспечивают сохранность исключенных ключей НЭП Клиента согласно п.п. 5.3.1. настоящего 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. настоящего Регламента.

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

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

5.6.4. ЭД, подписанные скомпрометированным ключом, и соответствующий ему ключ проверки НЭП 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 НЭП. Использование ПАК делает принципиально невозможным несанкционированное копирование ключей НЭП, используемых при работе в Системе ДБО.

#### 5.7.1.2. В ПАК реализованы следующие криптографические функции:

- аппаратный криптографически стойкий генератор случайных чисел;
- генерация пары ключей НЭП;
- формирование и проверка НЭП 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 НЭП в соответствии с ГОСТ Р34.10-2001 происходит непосредственно внутри ПАК: на вход ПАК принимает электронный документ, на выходе выдает НЭП под данным документом. При этом время формирования НЭП приблизительно равно 0,5 сек.

5.7.1.4. Ключ НЭП 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 НЭП ответственных сотрудников одного клиента.

5.7.1.5. Срок действия ключа НЭП, генерируемого внутри ПАК составляет 12 месяцев.

5.7.2. Банк предоставляет ПАК в виде USB токена с не извлекаемыми ключами.

5.7.3. USB-токены предназначены для работы на следующих платформах: Windows XP, Server 2000/2003/2000/2008/2012 Windows Vista/7/10/11, 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 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 НЭП Клиента с использованием ПАК и порядок расчетов.

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

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

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

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

5.7.6.3. Для активации и начала использования ПАК в Системе ДБО Клиент обязан осуществить смену ключей НЭП в порядке, указанном в разделе 5.2. настоящего Регламента, с использованием в качестве ключевого носителя ПАК.

За внеплановую смену ключей НЭП взимается комиссия в соответствии с действующими Тарифами Банка, за исключением случая, указанного в п. 5.7.6.4 настоящего Регламента.

5.7.6.4. 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 С ИСПОЛЬЗОВАНИЕМ СИСТЕМЫ ДБО ДЛЯ КОРПОРАТИВНЫХ КЛИЕНТОВ.

5.8.1. Интернет-Банк для корпоративных клиентов – приложение, с помощью которого Клиент может с любого мобильного устройства/компьютера осуществлять доступ к Системе ДБО, а также формировать, подписывать подписью НЭП 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.

5.8.2. ЭД, полученные с использованием Интернет-Банк и подписанные корректными НЭП уполномоченных лиц, влекут такие же правовые последствия, как и аналогичные документы на бумажном носителе, содержащем собственноручные подписи уполномоченных лиц.

5.8.3. Процедура генерации и порядок хранения ключей подписи и ключей проверки подписи осуществляется в порядке, указанном в Обзоре приложения Интернет-Банк, размещенном на сайте Банка <https://newbank.ru/>.

5.8.4. Запрещается анонимная регистрация в приложении Интернет-Банк.

5.8.5. Банк предоставляет доступ к приложению не позднее дня, следующего за днем даты регистрации в Банке Сертификата ключа проверки ЭП.

5.8.6. Клиент подтверждает, что мобильное устройство/компьютер, зарегистрированные в системе ДБО, с приложением Интернет-Банк, используются исключительно уполномоченными лицами.

5.8.7. В случае угрозы несанкционированного доступа к счетам посредством приложения Интернет-Банк, в том числе утраты мобильного устройства/компьютера, Клиент обязан незамедлительно заблокировать (прекратить) доступ к счетам в порядке, предусмотренном пунктом 5.6. настоящего Регламента.

5.8.8. Банк не несет ответственности за последствия доступа к счетам неуполномоченными лицами в случае нарушения Клиентом обязанности, предусмотренной пунктом 5.8.7. настоящего Регламента.

5.8.9. Банк не несет ответственности за ущерб, возникший вследствие передачи Клиентом/уполномоченным лицом Клиента третьим лицам логина, пароля к приложению Интернет-Банк, вне зависимости от причин.

5.8.10. Банк не несет ответственности за сбои и помехи в работе линий и средств связи, приводящие к невозможности доступа и использования приложения Интернет-Банк.

5.8.11. Банк не несет ответственности за сбои в работе приложения Интернет-Банк, обусловленные неисправностью мобильного устройства/компьютера, нарушением работоспособности установленного на мобильном устройстве/компьютере программного обеспечения, производителем которого Банк не является, или иными внешними факторами, в том числе повреждением приложения Интернет-Банк, установленного на мобильном устройстве/компьютере.

## 6. ПОРЯДОК ПРЕДОСТАВЛЕНИЯ УСЛУГИ КЛИЕНТУ ДЛЯ ОСУЩЕСТВЛЕНИЯ ПЕРЕВОДОВ (ПЕРИОДИЧЕСКИХ ПЕРЕВОДОВ) ДЕНЕЖНЫХ СРЕДСТВ С ИСПОЛЬЗОВАНИЕМ СИСТЕМЫ ДБО.

Порядок предоставления услуги Клиенту для осуществления переводов денежных средств с использованием Системы ДБО регламентируется ПАМЯТКОЙ Клиенту, являющейся пошаговой инструкцией для создания платежного поручения.

### ПАМЯТКА КЛИЕНТУ:

6.1. Заполните в Системе ДБО платежное поручение с указанием информации о получателе платежа.

6.2. Укажите сумму и назначение платежа.

6.3. При необходимости укажите признак условий перевода денежных средств (Срок исполнения платежа) в виде даты в формате ДД.ММ.ГГГГ в поле «Рез. поле» платежного поручения (поле 23 платёжного поручения по Положению Банка России от 29.06.2021 №762-П «О правилах осуществления перевода денежных средств»). Если такого условия нет, оставьте поле пустым.

6.4. Подпишите платёж и отправьте его в Банк для исполнения.

*Примечание:* Такие платежи, исполняются Банком в указанный Клиентом срок исполнения. При недостаточности денежных средств для исполнения распоряжения Клиента в указанную Клиентом дату применяется общий порядок исполнения платежного поручения.

## **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 ДБО.

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

1.3. При наличии сомнений в подлинности ЭД или его содержания Сторона - инициатор спора обязана направить другой Стороне письмо с подробным изложением нарушения, обстоятельств произошедшего 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 НЭП или несанкционированный доступ к ресурсам либо приложению Интернет-Банк.

### **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 обеспечения 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 ДБО, в том числе приложения Интернет-Банк. 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 ДБО и подписанного НЭП, 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 ДБО 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 иницирующая Сторона-отправитель должным образом оформила, заверила (подписала) НЭП и передала на обработку документ, а Сторона-отправитель отрицает факт подготовки, заверения (подписания) НЭП 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 ДБО, *sign.bin* - файл с НЭП Клиента под электронным документом, выгруженным из Сервера базы данных Системы ДБО, *certificate.xml* - файл с ключом проверки НЭП Клиента, с помощью которого осуществляется проверка подлинности НЭП под электронным документом.

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

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

### 4. ПОРЯДОК ФОРМИРОВАНИЯ И ПРОВЕРКИ НЭП 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 НЭП для указанного в п.4.1.2 байтового массива представляются Банком в шестнадцатиричном виде по запросу согласительной экспертной комиссии.

4.2. Контрольная проверка НЭП Клиента под электронным документом, пришедшим в Банк, осуществляется в АРМе "Операционист", входящим в комплекс Системы ДБО.

При проверке НЭП Клиента в АРМе "Операционист", отображается:

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

4.3. Результат проверок НЭП Клиента под ЭД в АРМе "Операционист" является подтверждением верности/неверности НЭП Клиента под ЭД.

**ПРИЛОЖЕНИЕ № 7**  
**к Правилам дистанционного банковского**  
**обслуживания клиентов с использованием системы**  
**ДБО 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 \_\_\_\_\_ действующего на основании \_\_\_\_\_, 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 ДБО № \_\_\_\_\_ от «\_\_» \_\_\_\_\_ 20\_\_ г. по заявке Клиента Банком выполнен следующий перечень услуг, переданы следующие материалы:

- Настройка системы ДБО на технических средствах Клиента в офисе Банка.  
Стоимость выполненных услуг составила \_\_\_\_\_ руб. \_\_\_\_ коп. без НДС.
- Внеплановая смена ключей НЭП (дополнительная генерация ключей НЭП Клиента). Количество сертификатов ключей ЭП \_\_\_\_ шт.  
Стоимость выполненных услуг составила \_\_\_\_\_ руб. \_\_\_\_ коп. без НДС.
- Регистрация сертификата ключа ЭП Клиента. Количество сертификатов ключей ЭП \_\_\_\_ шт.  
Стоимость выполненных услуг составила \_\_\_\_\_ руб. \_\_\_\_ коп. без НДС.
- Материалы для пользования услугой защиты секретного ключа НЭП.  
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. без НДС.

**От Банка**  
**Представитель Банка**

\_\_\_\_\_/ /

\_\_\_\_\_/ /

М.П.

**От Клиента**

\_\_\_\_\_

\_\_\_\_\_/ /

\_\_\_\_\_

\_\_\_\_\_/ /

М.П.

**СОГЛАШЕНИЕ**  
**о порядке информирования при работе**  
**по Системе ДБО**

« \_\_\_\_\_ » \_\_\_\_\_ 20\_\_ г.

**Коммерческий Банк «Новый век» (Общество с Ограниченной Ответственностью)**, именуемый в дальнейшем «Банк», в лице \_\_\_\_\_, действующего(ей) на основании \_\_\_\_\_ 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 НЭП Клиента, а также направлять уведомления об утрате ключа НЭП 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) 223-00-70**

При этом Клиент обязан сообщить полное наименование Клиента, ФИО владельца ключа ЭП.

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 НЭП Клиента), то Банк не считается извещенным о компрометации (или подозрении на компрометацию) ключа НЭП Клиента/уведомленным об утрате ключа НЭП и (или) его использования без согласия Клиента и не обязан приостанавливать использование в Системе ДБО ключа НЭП Клиента.

2. способ направления извещения/уведомления.

Клиент обязан известить/уведомить Банк путем направления с адреса электронной почты, указанного Клиентом в Сертификате ключа проверки НЭП, на адрес электронной почты Банка [block@newbank.ru](mailto: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 НЭП Клиента/уведомленным об утрате ключа НЭП и (или) его использования без согласия Клиента и не обязан приостанавливать использование в Системе ДБО ключа НЭП Клиента.

**2. Банк обязан информировать Клиента о совершении каждой операции с использованием ключа(ей) НЭП 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 ДБО (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 ДБО 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 ДБО и за ознакомление со статусом своего распорядительного документа)	
--	--

Уведомление посредством направления SMS-сообщения или устного 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 или звонка 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 ответа на звонок уполномоченного лица Банка;
- 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 ДБО 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**

**Представитель Банка**

\_\_\_\_\_/\_\_\_\_\_/\_\_\_\_\_/

\_\_\_\_\_/\_\_\_\_\_/\_\_\_\_\_/

\_\_\_\_\_/\_\_\_\_\_/\_\_\_\_\_/

\_\_\_\_\_/\_\_\_\_\_/\_\_\_\_\_/

М.П.

М.П.

## **ПАМЯТКА ДЛЯ КЛИЕНТА**

### **о возможных угрозах хищения денежных средств с использованием системы ДБО и способах защиты**

Атаки злоумышленников на банковские счета юридических лиц, физических лиц, индивидуальных предпринимателей, 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 работников самих компаний.

Хищение средств с банковских счетов клиентов возможно при получении злоумышленниками доступа к ключам НЭП 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 Вас ознакомиться с «Памяткой о возможных угрозах хищения денежных средств с использованием системы ДБО 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 НЭП используйте **USB-токены - 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, 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 НЭП невозможно.

- Никогда не передавайте третьим лицам одноразовые пароли для подтверждения платежей, приходящие Вам из Банка в виде SMS-сообщений.

- Используйте **IP-фильтрацию** - дополнительный сервис, запрещающий пользование ключами НЭП 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 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 НЭП ИТ-сотрудникам для проверки работы** Системы и настроек взаимодействия с Банком. Если такая проверка необходима, владелец ключа НЭП должен лично подключить носитель к компьютеру, убедиться, что пароль доступа к ключу вводится в интерфейс клиентского АРМа ДБО, и вводит пароль, исключая умышленное наблюдение посторонними лицами.

- **Не передавайте ключи НЭП замещающим сотрудникам** (заместителям, временно исполняющим обязанности). Для них необходимо получить персональные НЭП и внести их в банковскую карточку.

- **При увольнении сотрудника**, имевшего доступ к ключу НЭП, **обязательно заблокируйте его ключ НЭП**;

- **При увольнении ИТ-специалиста**, обслуживавшего компьютеры, подключенные к Системе ДБО, **обязательно проверьте их на отсутствие вредоносных программ**.

- **При продолжительной работе в Клиент-Банке**, отключите и **извлеките из компьютера носители с ключами НЭП**, 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 ДБО** и не выполняйте на нем никакие другие задачи (по возможности).

- **Ограничьте доступ к компьютерам**, используемым для работы с Системой ДБО 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 ИТ-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 НЭП или наличие в компьютере вредоносных программ – **обязательно заблокируйте ключи НЭП.**

- **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 НЭП.

#### **Предполагаемая аудитория мошенников**

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

- Ответственные работники Вашей компании, ранее имевшие доступ к ключам НЭП, например, уволенные директора, бухгалтеры и их заместители, бывшие совладельцы Компании.

- Штатные ИТ-сотрудники Вашей компании, имеющие или имевшие технический доступ к носителям (дискеты, флеш-носители) с ключами НЭП 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 НЭП 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 НЭП и не может от Вашего имени сформировать НЭП под электронным платежным документом.

- Банк никогда не осуществляет рассылку электронных писем с просьбой прислать Ваш ключ НЭП 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 НЭП/паролей, срочно сообщите об этом в Службу технической поддержки клиентов Банка.

- Вы являетесь единственным владельцем ключей НЭП и ответственность за их конфиденциальность лежит на Вас.

- Если Вы сомневаетесь в конфиденциальности ключей НЭП или подозреваете компрометацию (копирование) данных, срочно заблокируйте ваши ключи НЭП.

- Изменение пароля доступа к ключу НЭП 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.**

**Рекомендации по обеспечению безопасности при работе с приложением Интернет-Банк для корпоративных клиентов и индивидуальных предпринимателей**

Несмотря на то, что операционные системы мобильных устройств/компьютеров 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.

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

- Скачивать и устанавливать приложение Интернет-Банк для корпоративных клиентов на мобильные устройства следует только из официальных магазинов приложений RuStore, Google Play, AppStore. Разработчиком приложения должна быть указана компания "New Century Bank LTD".

- 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.

**ПРИЛОЖЕНИЕ № 11**  
**к Правилам дистанционного банковского**  
**обслуживания клиентов с использованием системы**  
**ДБО в КБ «Новый век» (ООО)**

Заявление на выпуск сертификата ключа проверки НЭП и облачной НЭП №  
Банку **КБ "Новый век" (ООО)** г. Москва

от клиента

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

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

Дата создания ключа НЭП:

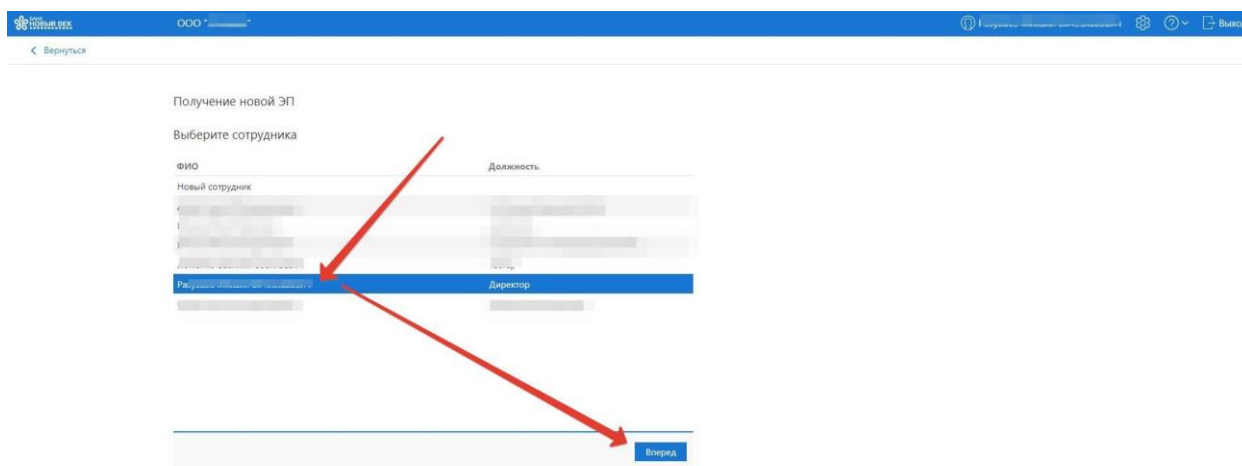
\_\_\_\_\_

## **I. Инструкция по выпуску нового сертификата на токене юридического лица при наличии действующего сертификата (НЭП)**

1. Заходим в Клиент-Банк по своему текущему сертификату (текущая НЭП) (флешка-токен вставлена в USB порт компьютера). Далее выбираем слева меню «Электронные подписи» и нажимаем кнопку «Новая ЭП».



2. Выбираем в списке ФИО на кого делается новая НЭП и нажимаем кнопку «Вперед».



3. Проверяем сведения владельца новой НЭП или вносим изменения (в случае смены паспорта или должности). Нажимаем кнопку «Вперед».

Получение новой ЭП

Укажите сведения о себе

Фамилия:

Имя:

Отчество:

Должность:

Документ, удостоверяющий личность:

Тип:

Серия:  Номер:

Дата выдачи:  Код подразделения:

Кем выдан:

Назад **Вперед**

**Необходимо заполнить данные**

4. Выбираем Аппаратное устройство (новая НЭП формируется на текущей флешке-токене). Нажимаем далее кнопку «Вперед».

Получение новой ЭП

Выберите место хранения ключа электронной подписи

**Электронная подпись должна быть добавлена в хранилище.**  
В одном хранилище может содержаться несколько ключей ЭП.

Укажите полный путь к файлу или серийный номер аппаратного устройства, которое будет использоваться для генерации ключей ЭП.

Если хранилище не существует, будет создано новое.

аппаратное устройство:  **Выбрать...**

Назад **Вперед**

5. Вводим вручную в поле «Наименование ключа» название новой НЭП. Обычно рекомендуется название организации или ИП и год. Пример: «ООО Ромашка 2024» или «ИП Иванов 2023». Далее нажимаем кнопку «Вперед».

Получение новой ЭП

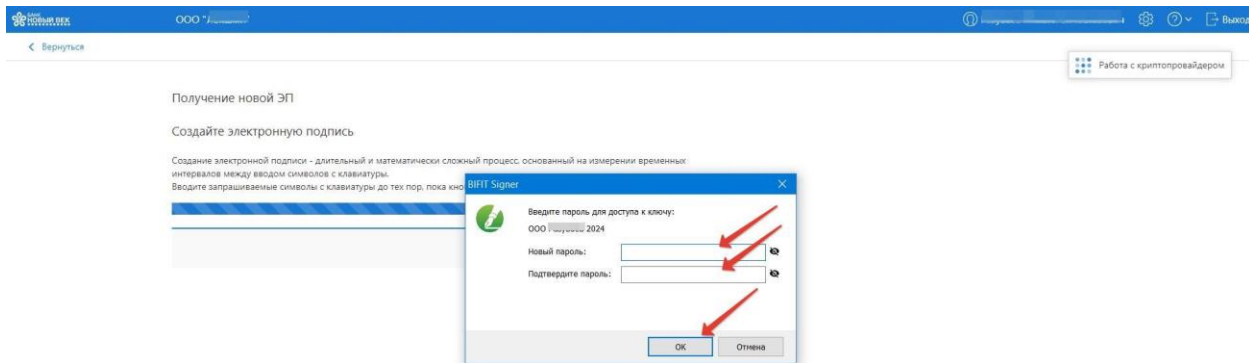
Задайте название ключа электронной подписи

Все ключи ЭП клиентов хранятся в хранилище в зашифрованном на пароле виде. Для добавления ключа ЭП в хранилище введите произвольное наименование ключа.

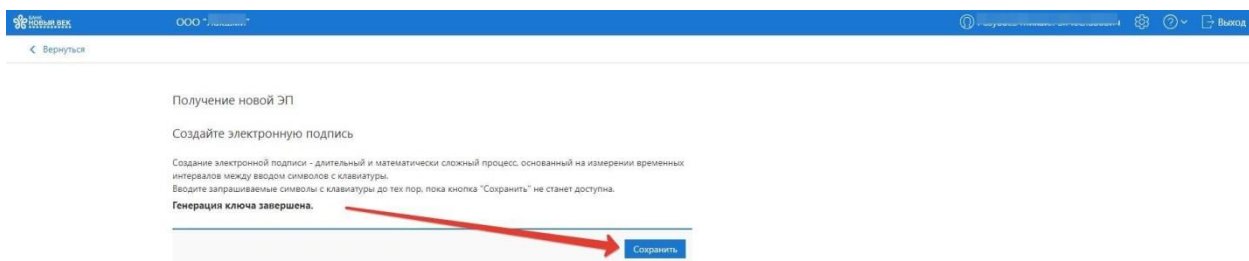
Наименование ключа:  **Выбрать...**

Назад **Вперед**

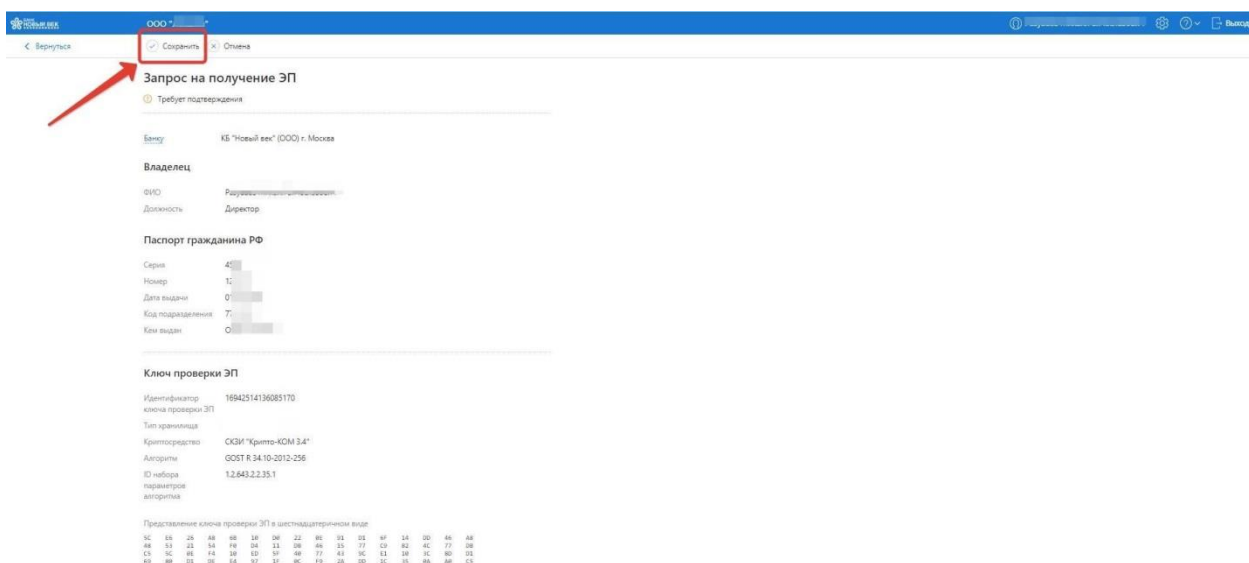
6. Вводим придуманный Вами сложный пароль в поле «Новый пароль», в поле «Подтвердите пароль» вводим такой же еще раз. Нажимаем кнопку «ОК».



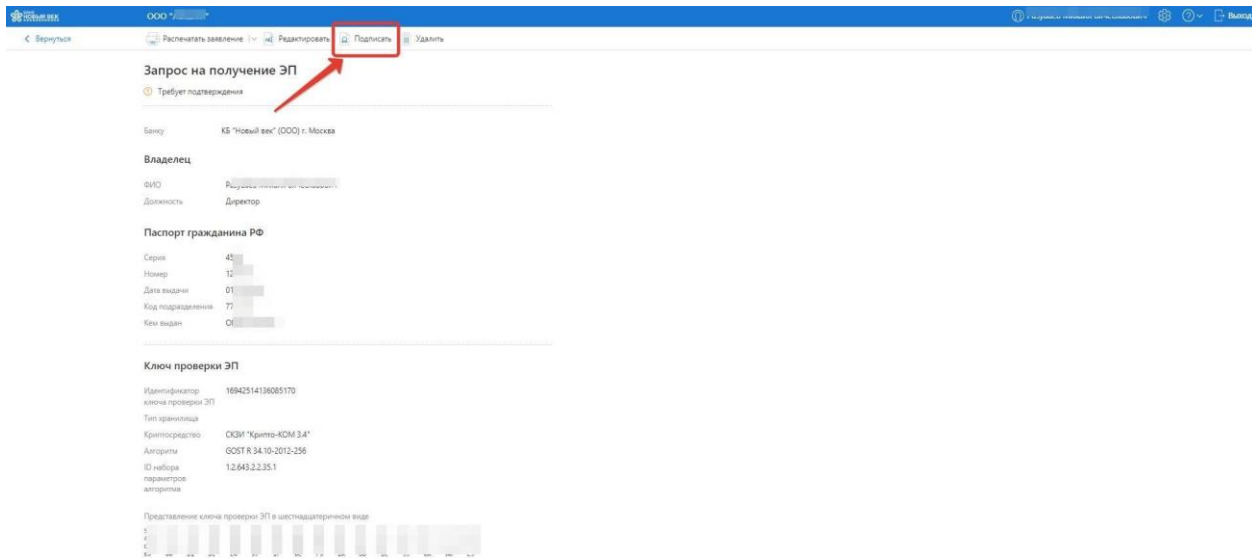
7. Если все делалось правильно, на экране будет сообщение: Генерация ключа завершена. Нажимаем кнопку «Сохранить».



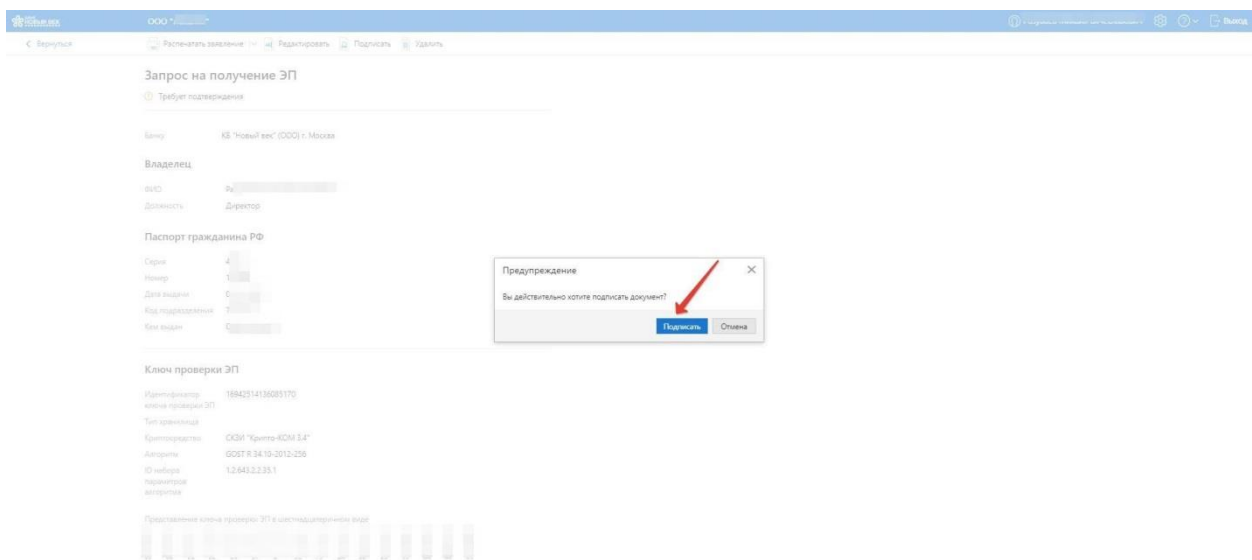
8. На экране отобразиться Запрос на получение НЭП со статусом: требует подтверждения. Нажимаем кнопку «Сохранить».



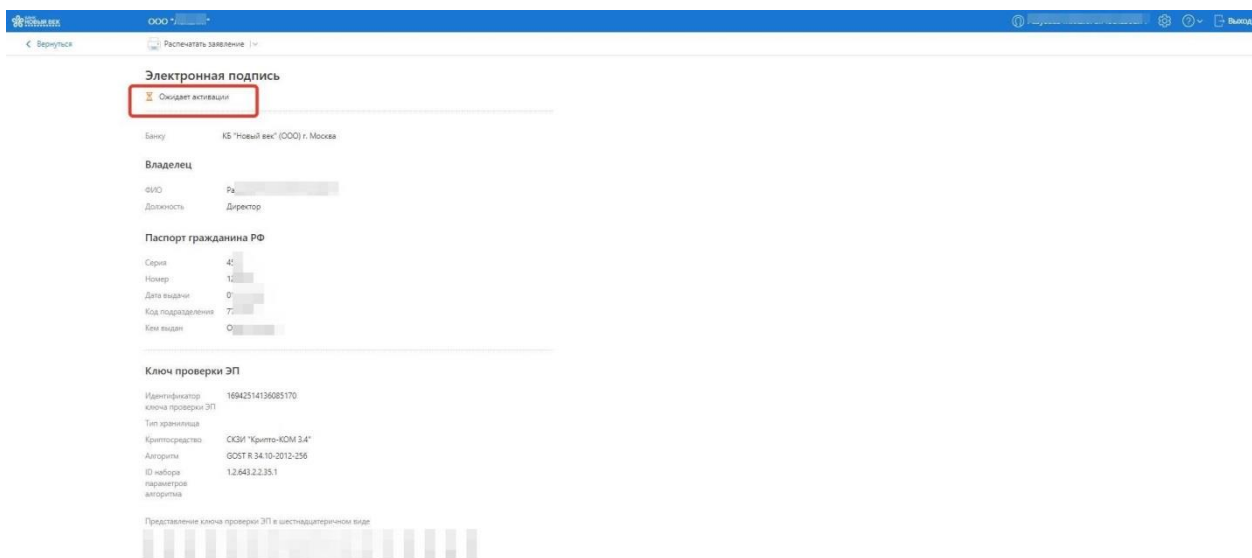
9. Далее нажимаем кнопку «Подписать». Подписываем запрос для новой НЭП своей текущей НЭП.



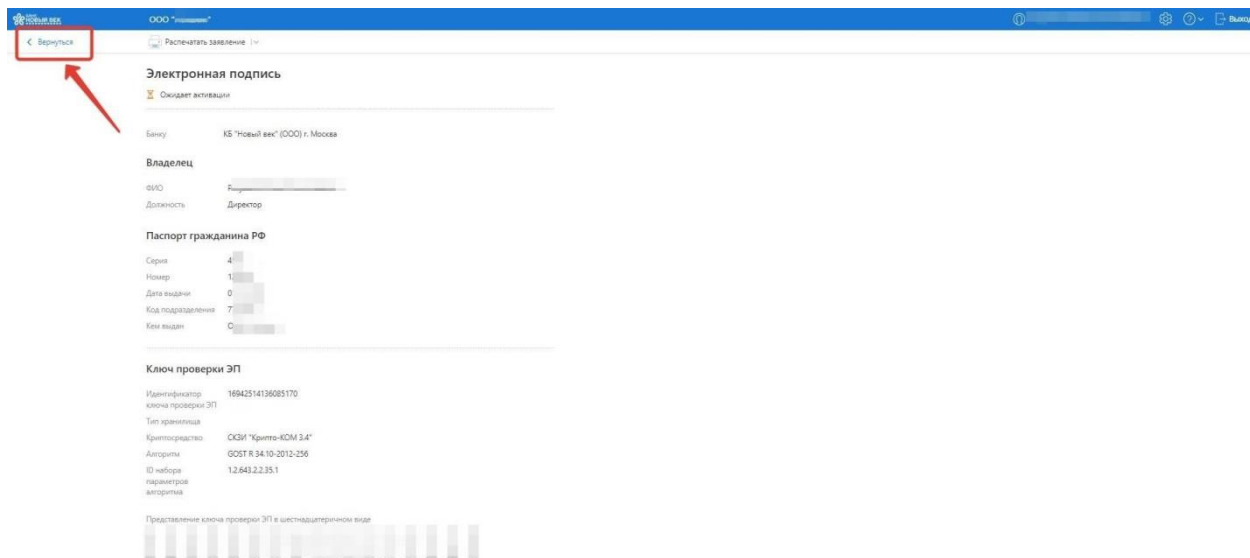
10. Нажимаем «Подписать» для подтверждения.



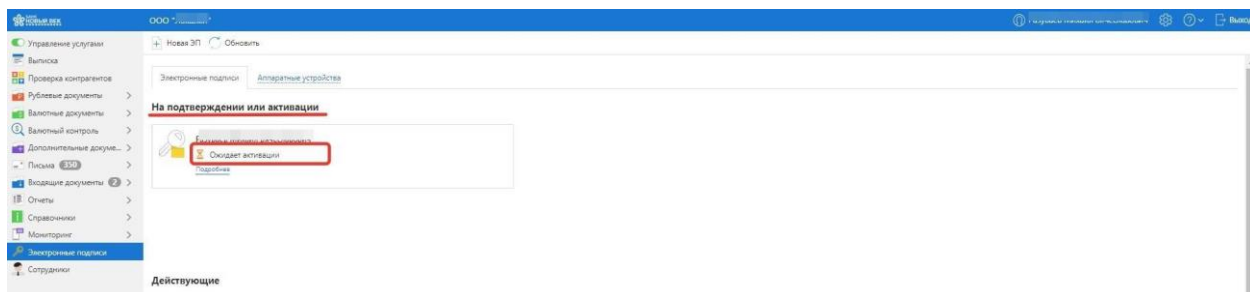
11. Далее у запроса на новую НЭП появится статус: ожидает активации.



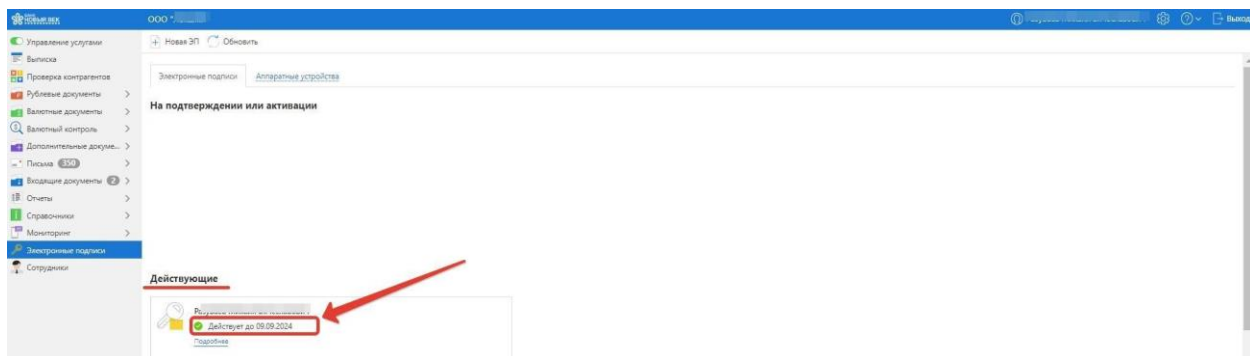
12. Нажимаем «Вернуться».



13. Новая НЭП переходит в статус: ожидает активации (раздел: на подтверждении или активации). Необходимо теперь подождать, когда Банк активируют Вашу подпись.



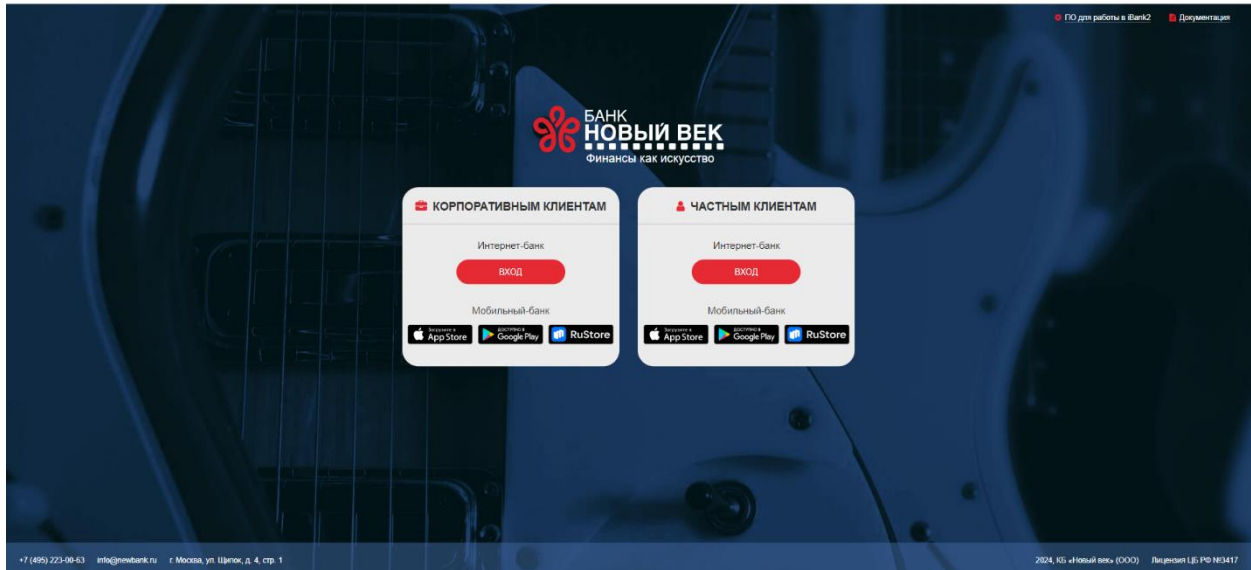
14. После активации Вашей подписи она переходит в раздел: «действующие». Там же указан срок действия подписи.



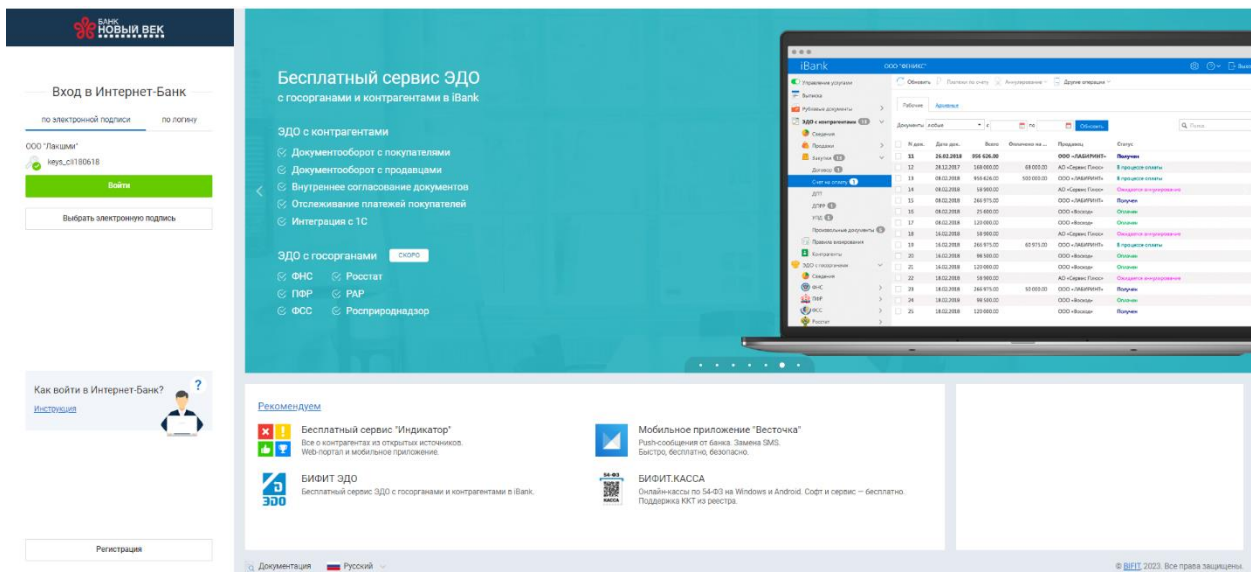
По техническим вопросам формирования новой НЭП просьба обращаться в Банк по телефону: +7(495) 223-0063

## II. Инструкция по созданию облачной подписи НЭП (все подписи просрочены)

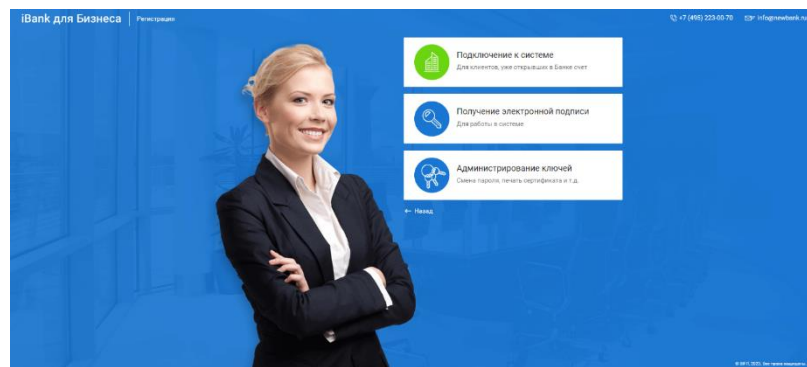
1. Открываем сайт <https://ibank2.newbank.ru>, выбираем пункт «Корпоративным клиентам» Интернет- банк, нажимаем кнопку «Вход».



2. Находим внизу слева кнопку «Регистрация» и нажимаем ее.



3. Выбираем пункт «Получение электронной подписи» (если все подписи просрочены и клиент зарегистрирован в ДБО).



Выберите тип электронной подписи, которую планируете создать.

ЭП в файловом хранилище или на аппаратном устройстве

Облачная ЭП

ЭП создается, хранится и используется для подписи документов на сервере банка, что позволяет работать с любыми устройствами без дополнительного ПО.

Вперед

#### 4. Выбираем «Облачная ЭП». Нажимаем кнопку «Вперед».

Выберите тип электронной подписи, которую планируете создать.

ЭП в файловом хранилище или на аппаратном устройстве

Облачная ЭП

ЭП создается, хранится и используется для подписи документов на сервере банка, что позволяет работать с любыми устройствами без дополнительного ПО.

Вперед

#### 5. Заполняем все поля и нажимаем кнопку «Вперед».

Регистрация новых ключей ЭП

Шаг 1 из 6

Введите информацию о владельце ключа ЭП.

Тип: Организация

Фамилия: \_\_\_\_\_

Имя: \_\_\_\_\_

Отчество: \_\_\_\_\_

Должность: \_\_\_\_\_

Документ, удостоверяющий личность:

Тип: Паспорт гражданина РФ

Серия: \_\_\_\_\_ Номер: \_\_\_\_\_

Дата выдачи: [25] Код подразделения: \_\_\_\_\_

Ключ выдан: \_\_\_\_\_

Назад Вперед

Регистрация новых ключей ЭП

Шаг 1 из 6

Введите информацию о владельце ключа ЭП.

Тип:

Фамилия:

Имя:

Отчество:

Должность:

Документ, удостоверяющий личность:

Тип:

Серия:  Номер:

Дата выдачи:  Код подразделения:

Кем выдан:

- Вводим e-mail для логина и номер телефона для двухфакторной идентификации (обратить внимание на формат номера на скрине). Нажимаем кнопку «Вперед».

Регистрация новых ключей ЭП

Шаг 2 из 6

Укажите свой номер телефона и адрес электронной почты.

Эта информация будет использоваться для входа в Интернет-банк.

E-mail:

Телефон:

Номер указывается в международном формате.  
Помощь для России: +79161234567

- Ставим галку на пункт «Я согласен с условиями доверенности» и нажимаем кнопку «Вперед».

Регистрация новых ключей ЭП

Шаг 3 из 6

Настоящим доверяю банку хранить ключ ЭП в защищенном хранилище и использовать его для формирования ЭП под документами системы "Bank".

Я согласен с условиями доверенности

8. Вводим наименование ЭП (например: ООО «Ромашка 2024»). Вводим придуманный Вами сложный пароль и повторяем его в поле «Пароль еще раз». Далее вводим проверочный код и нажимаем кнопку «Вперед».

Регистрация новых ключей ЭП  
Шаг 4 из 6

Задайте название электронной подписи и пароль  
Все ЭП хранятся в защищенном виде. Для добавления ключа ЭП в кранализе введите произвольное наименование ЭП и пароль для доступа к ней.

Наименование ЭП

Пароль

Надежность пароля:

Пароль еще раз

Проверочный код

9. Нажимаем на ссылку «Сохранить сертификат», чтобы сохранить его на устройстве, далее нажимаем на кнопку «Вперед». Эта процедура необходима для дальнейшего подписания сертификата подписью УКЭП и отправки его в Банк по ссылке: <https://app.newbank.ru/sign/start>, либо для распечатки его бумажной копии.

Регистрация новых ключей ЭП  
Шаг 5 из 6

Для выпуска сертификата предоставьте в Банк:

- распечатанное Заявление на выпуск сертификата;
- оригинал удостоверения личности или нотариально заверенную копию;
- оригинал документа, подтверждающего право пребывания в РФ (только для нерезидентов).

Идентификатор ключа проверки ЭП

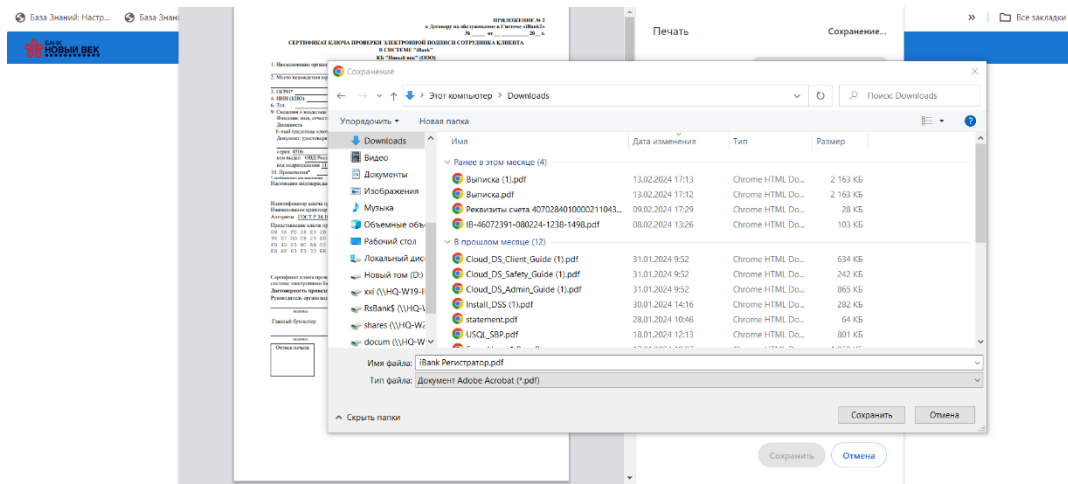
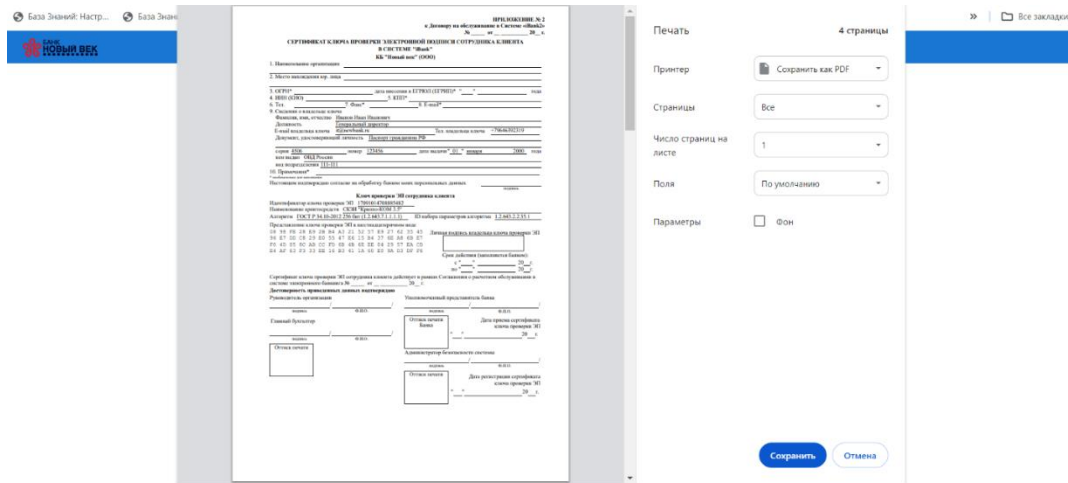
Распечатать сертификат

Заполнить сертификат ключа проверки ЭП реквизитами организации из другого ключа

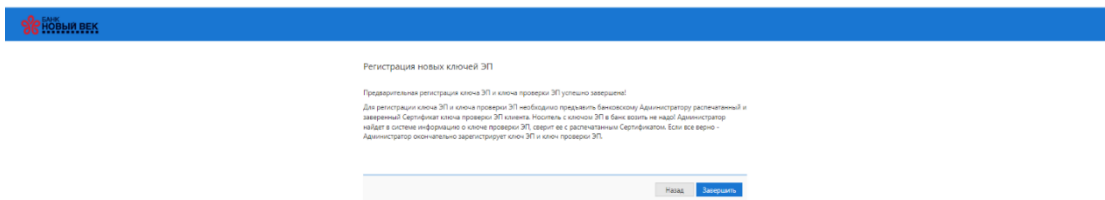
Создать еще ключи ЭП и ключ проверки ЭП

[Сохранить сертификат](#)

10. Можно сразу распечатать сертификат или сохранить его на устройстве в формате PDF и распечатать, когда будет удобно. Это процедура необходима для собственноручного подписания сертификата и дальнейшего предоставления его в Банк.



11. Нажимаем кнопку Завершить.



После регистрации Сертификата в Банке Вы сможете подписывать документы в системе ДБО. По техническим вопросам формирования новой НЭП просьба обращаться в Банк по телефону: +7(495) 223-0063