

П Р А В И Л А
дистанционного банковского обслуживания клиентов «Нацинвестпромбанк» (АО)
с использованием системы «Клиент-Банк»

(редакция № 2)

г. Москва, 2024г.

ОГЛАВЛЕНИЕ

1.	Определения и термины	2
2.	Договор присоединения	5
3.	Общие положения	6
4.	Соглашение сторон	6
5.	Порядок подключения к личному кабинету Системы	8
6.	Порядок работы с электронными документами	10
7.	Порядок уведомления клиента в Системе	10
8.	Действия при компрометации средств идентификации, аутентификации и авторизации клиента в Системе	13
9.	Права и обязанности	14
10.	Стоимость услуг и порядок расчетов	19
11.	Ответственность сторон	19
12.	Срок действия Договора ДБО, порядок его изменения и расторжения	20
13.	Порядок разрешения споров сторон	21
14.	Приложение № 1 Рекомендации по обеспечению информационной безопасности при работе с Системой	24
15.	Приложение № 2 Заявление о присоединении к Правилам ДБО	26
16.	Приложение № 3 Перечень электронных документов, передаваемых по Системе	27
17.	Приложение № 4 Акт приема-передачи средств криптозащиты информации	28
18.	Приложение № 5 Сертификат ключа проверки электронной подписи	29
19.	Приложение № 6 Заявление на фильтрацию IP-адреса	30
20.	Приложение № 7 Заявление на отказ от фильтрации IP-адреса	31
21.	Приложение № 8 SMS-сервис с получением одноразовых паролей	32
22.	Приложение № 9 MAC-токен с получением одноразовых паролей	33
23.	Приложение №10 Заявление на установку, настройку Системы специалистом Банка	34
24.	Приложение №11 Заявление лимитов операций с использованием Системы	35
25.	Приложение №12 Информация для подключения к Информационной системе «Одно окно»	36

«Национальный инвестиционно-промышленный банк» (Акционерное Общество) (далее – Банк) предоставляет организациям, индивидуальным предпринимателям и физическим лицам, занимающимся в установленном законодательством Российской Федерации порядке частной практикой (далее – Клиент), услуги по дистанционному банковскому обслуживанию с использованием системы «Клиент-Банк» iBank (далее – Система).

1. ОПРЕДЕЛЕНИЯ И ТЕРМИНЫ

В настоящих Правилах дистанционного банковского обслуживания клиентов Банка с использованием Системы «Клиент-Банк» iBank (далее – Правила ДБО) применяются следующие термины:

Автоматизированное рабочее место Клиента (АРМ) – комплекс программных и аппаратных средств, установленных у Клиента, позволяющие Клиенту создавать и передавать в Банк, получать от Банка распоряжения, электронные документы, удовлетворяющие техническим требованиям Банка, указанных в пункте 5.1 Правил ДБО.

Владелец сертификата ключа проверки электронной подписи (Владелец ключа) – уполномоченное лицо Клиента, осуществляющее от имени Клиента работу в Системе, на имя которого в установленном настоящим Договором ДБО порядке оформлен Сертификат ключа проверки электронной подписи (ЭП), и которое владеет соответствующим ключом ЭП.

Заявление о присоединении – Заявление о присоединении к настоящим Правилам, составленное по форме Приложения № 2 к настоящим Правилам, поданное Клиентом в Банк с целью заключения Договора дистанционного банковского обслуживания клиентов «Нацинвестпромбанк» (АО) в соответствии с Правилами ДБО.

Информирование о событиях в системе – автоматическая отправка Системой сообщений о событии в Системе по каналам доставки, устанавливаемым Клиентом самостоятельно в разделе «Мониторинг» Системы.

Информирование об операциях, совершаемых с использованием Системы – информирование Банком Клиента о совершаемых с использованием Системы операциях по Счетам в соответствии с требованиями Федерального закона от 27.06.2011 № 161–ФЗ в порядке, установленных Правилами ДБО.

ИС «Одно окно» - информационная система «Одно окно» в сфере внешнеторговой деятельности - федеральная государственная автоматизированная информационная система, обеспечивающая взаимодействие в электронной форме участников внешнеторговой деятельности и иных лиц с органами государственной власти Российской Федерации, органами валютного контроля, уполномоченными Правительством Российской Федерации, и иными лицами в соответствии с их компетенцией в целях развития внешнеторговой деятельности и обеспечения возможности использования органами государственной власти Российской Федерации, органами валютного контроля, уполномоченными Правительством Российской Федерации, и иными лицами в соответствии с их компетенцией содержащихся в этой системе документов и информации в целях осуществления государственного контроля (надзора), предоставления государственных услуг, исполнения государственных функций, предоставления иных услуг в сфере внешнеторговой деятельности, формирования статистики в сфере внешнеторговой деятельности.

Оператором ИС «Одно окно» является акционерное общество "Российский экспортный центр"(официальный сайт в сети Интернет <https://www.exportcenter.ru>);

Карточка – карточка с образцами подписей и оттиска печати, оформленная по форме и в соответствии с требованиями, установленными Банком России.

Ключ электронной подписи (Ключ ЭП) – уникальная последовательность символов, предназначенная для создания электронной подписи, известная только Владельцу ключа. Система поддерживает хранение Ключей ЭП:

- на устройстве для защищенного хранения ключей MAC-токен BIFIT, USB-токен «MS_KEY К» – «АНГАРА» Исп.8.1.1, Рутокен ЭЦП 3.0, которое обеспечивает неизвлекаемость (невозможность считывания);
- на сервере Банка (облачная подпись, серверная подпись).

У Клиента может быть необходимое ему количество Ключей ЭП.

Ключ проверки электронной подписи (ЭП) – уникальная последовательность символов, однозначно связанная с Ключом ЭП и предназначенная для проверки подлинности электронной подписи (далее - проверка электронной подписи). Проверка ЭП Клиента выполняется банковским сервером в момент подписи Клиентом документов, а также шлюзом при выгрузке документов в АБС Банка. Ключи проверки ЭП клиентов хранятся на сервере Банка. Восстановить из Ключа проверки ЭП ключ ЭП клиента технически невозможно.

Кодовое слово – слово, указанное Клиентом при регистрации в Системе, которое будет использоваться для идентификации Клиента при обращении в Банк.

Компрометация ключа – событие, в результате которого возникает утрата доверия к тому, что Ключ ЭП, пароль от носителя информации с Ключом ЭП (USB-токен «MS_KEY К» - «АНГАРА», MAC-токен BIFIT, Рутокен), телефоны, номера телефонов и e-mail, используемые при работе в Системе и Мобильное устройство, содержащее приложение для работы в Системе, стали доступны неуполномоченному лицу (лицам).

К событиям, связанным с компрометацией ключей, относятся следующие события:

- утрата устройств защищенного хранения ключа ЭП (USB-токен «АНГАРА», MAC-токен BIFIT, Рутокен), в том числе с последующим их обнаружением;
- утрата контроля над Номером телефона или Устройством, содержащим Мобильное приложение;
- увольнение/прекращение полномочий сотрудников/представителей Клиентов, имевших доступ к ключам ЭП;
- временный доступ посторонних лиц к устройству защищенного хранения Ключа ЭП либо подозрение, что такой доступ имел место;
- обнаружение на компьютере или Мобильном устройстве, с использованием которых осуществляется доступ в Систему, постороннего программного обеспечения;
- искажение информации о Распоряжении в приложении «Весточка», на экране MAC-токена BIFIT или SMS-сообщении с кодом подтверждения (изменение получателя, суммы Распоряжения);
- иные события, в результате которых Ключи ЭП, Телефоны, Номера телефонов, устройства для хранения ключей, Мобильное приложение могут стать доступными неуполномоченным лицам и (или) несанкционированным процессам.

Мобильный Банк «Web-NIPBank» (мобильный банк) - мобильное приложение, предназначенное для доступа Клиента к Системе Интернет-Банк через телефон или планшет.

Мобильное приложение - мобильное приложение «Весточка», предназначенное для защищенного информирования Банком Клиента посредством push-сообщений, а также для подтверждения Платежных поручений и аутентификации Клиента при входе в Систему в случаях, установленных Правилами ДБО.

Многофакторная аутентификация – уполномоченному лицу Клиента при входе в Систему необходимо дополнительно вводить одноразовый пароль или подтверждать вход с помощью приложения «Весточка» или MAC-токена BIFIT.

Облачная подпись – электронная подпись, созданная посредством Ключа облачной подписи. Клиент дает согласие на хранение ключа ЭП в защищенном хранилище Сервера подписи и использование его для формирования ЭП под документами Системы через Мобильное приложение. При ее создании формируется Учетная запись для входа в Систему по логину и паролю. Использование облачной подписи позволяет не использовать устройство для защищенного хранения ключей, работать в системе с мобильных устройств.

Одноразовый пароль – комбинация цифр, формируемая программным (высылаются в виде SMS сообщений) или аппаратным (с помощью устройств генерации одноразовых паролей) способом, которая используется в механизме **Многофакторной аутентификации**. Источником одноразовых паролей и кодов подтверждений могут быть: MAC-токены или SMS-сообщения.

Пароль на доступ к ключу ЭП – пароль, устанавливается владельцем ключа с целью ограничения доступа к Ключу ЭП третьими лицами.

Персональный компьютер (ПК, рабочее место) – ноутбук или стационарный компьютер Клиента.

Представитель – лицо, действующее от имени и в интересах или за счет Клиента, полномочия которого основаны на доверенности, договоре, акте уполномоченного государственного органа или органа местного самоуправления, законе, в том числе лицо, наделенное полномочиями давать Банку распоряжения по осуществлению операций, используя Систему, а также единоличный исполнительный орган юридического лица.

Сайт Банка - официальный сайт Банка в сети Интернет по адресу <http://www.nipbank.ru/>.

Сертификат проверки Ключа ЭП (Сертификат) – документ на бумажном носителе, созданный Владелец ключа в Системе, который подтверждает принадлежность Ключа проверки ЭП Владельцу Сертификата. Срок действия Сертификата определяется сроком полномочий Владельца ключа, но не превышает 1 (Одного) года с даты начала действия Ключа ЭП. Срок действия ключа ЭП указывается в Сертификате.

Система «Клиент-Банк» iBank (Система) – автоматизированная система, представляющая собой совокупность программно-аппаратных средств, включающая подсистемы Интернет-банк и Мобильный банк, позволяющая осуществлять электронный документооборот (принимать и передавать расчетные документы и/или иные документы и сообщения) между Клиентом и Банком.

Доступ к Системе предоставляется Клиентам через личный кабинет Клиента Интернет-банка «Web-NIPBank» и Мобильного банка «Web-NIPBank».

В рамках настоящих Правил Система является в соответствии с Федеральным законом от 27.06.2011 № 161-ФЗ «О национальной платежной системе» электронным средством платежа (далее – ЭСП), разработчиком и владельцем всех исключительных прав на программное обеспечение является Акционерное общество «БИФИТ», ОГРН 1077746075461, ИНН 7719617469, адрес: 105203, г. Москва, ул. Нижняя Первомайская, д. 46.

Событие в Системе Интернет-Банк (Событие) – автоматическое обновление в Системе информации, доступной Клиенту.

Согласительная комиссия – комиссия, создаваемая Сторонами в случае возникновения спора по поводу авторства и неизменности содержания Электронных документов, переданных посредством Системы.

Сообщение (Письмо) – электронный документ, направляемый по Системе Интернет-Банк одной Стороной другой Стороне, подписываемый ЭП уполномоченного лица Клиента и не являющийся Распоряжением.

Средства идентификации, аутентификации и авторизации Клиента в Системе – средства, используемые уполномоченным лицом Клиента, подтверждающие полномочия на осуществление от имени Клиента работу в Системе. К таким средствам относятся:

- Ключ ЭП;
- носитель ключа ЭП (USB-токен «MS_KEY К» - «АНГАРА», Рутокен, MAC-токен BIFIT);
- MAC-токен;
- номер телефона и телефон;
- мобильное приложение «Весточка».

Средства криптографической защиты информации (СКЗИ) – шифровальные криптографические средства защиты информации конфиденциального характера – аппаратные и (или) программные средства, обеспечивающие создание и проверку электронной подписи, создание Ключей ЭП, а также реализующие алгоритмы криптографического преобразования информации и предназначенные для защиты информации при осуществлении электронного взаимодействия по каналам связи. Для криптографической защиты информации могут быть использованы:

- аппаратные криптопровайдеры: USB-токен «MS_KEY К» – «АНГАРА», Рутокен ЭЦП 3.0;

– программные СКЗИ: MAC-токен BIFIT.

Средства электронной подписи – шифровальные (криптографические) средства, используемые для реализации хотя бы одной из следующих функций – создание электронной подписи, проверка электронной подписи, создание Ключа электронной подписи и Ключа проверки электронной подписи.

Статус электронного документа – состояние электронного документа, соответствующее стадии обработки документа в АБС Банка.

Сторона – Банк или Клиент.

Стороны – Банк и Клиент.

Счет – счет, открытый Клиенту в Банке на основании Договора банковского счета.

Тарифы – тарифы расчетно-кассового обслуживания «Нацинвестпромбанк» (АО) для юридических лиц (кроме кредитных организаций), индивидуальных предпринимателей, физических лиц, занимающихся в установленном законодательством Российской Федерации порядке частной практикой, утвержденные Банком в установленном порядке, устанавливающие размер, срок и порядок уплаты комиссии при обслуживании Клиента. Тарифы являются неотъемлемой частью Договора банковского счета. Тарифы размещаются Банком на общедоступных ресурсах Банка (на информационных стендах в офисах Банка и на сайте Банка).

Уведомления о событиях в Системе (Уведомления) – услуга по предоставлению Клиенту информации о входе в систему, текущих остатках на счетах, изменении статусов документов, движении средств по счетам, выписки. Отправка уведомлений осуществляется по каналам: «Весточка», Мобильный Банк, SMS или E-mail.

Информация направляется Банком Клиенту в виде сообщения на адрес электронной почты со специального адреса Банка ibank@nipbank.ru и/или в виде SMS -сообщения со специального номера Банка «Нацинвестпромбанк» (АО) на номер телефона/адрес, указанный Клиентом в Системе.

Электронная подпись (ЭП) – информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию (электронный аналог собственноручной подписи уполномоченного лица).

Электронный документ – документ, в котором информация представлена в электронной форме, являющийся Распоряжением. Электронный документ подписывается ЭП уполномоченного лица Клиента, имеющего необходимые полномочия для подписания соответствующего Электронного документа от лица Клиента. Электронный документ с ЭП является основанием для совершения Банком финансовых операций.

2. ДОГОВОР ПРИСОЕДИНЕНИЯ

2.1. Настоящие Правила ДБО представляют собой условия договора дистанционного банковского обслуживания Клиента с использованием Системы в целях исполнения Договора банковского счета (далее – Договор ДБО) и регулируют отношения, возникающие при предоставлении Банком Клиенту услуг дистанционного банковского обслуживания с использованием Системы.

Система предназначена для проведения операций по счетам Клиента в рублях и иностранной валюте на основании Распоряжений, сформированных Клиентом посредством Системы, для передачи между Сторонами иной информации и документов, связанных с банковским обслуживанием Клиента в Банке, а также для совершения сделок между Банком и Клиентом.

2.2. Предоставление Клиенту услуги по дистанционному банковскому обслуживанию с использованием системы «Клиент-Банк» iBank осуществляется после заключения Договора ДБО. Договор ДБО публикуется на сайте Банка <http://www.nipbank.ru/> и размещается на информационных стендах в офисах Банка. Клиент имеет право получить текст Договора ДБО на бумажном носителе в офисе Банка.

Договор ДБО заключается в соответствии с условиями статьи 428 Гражданского кодекса Российской Федерации в результате присоединения Клиента к Правилам ДБО.

Для заключения Договора ДБО Клиент представляет в Банк Заявление о присоединении к Правилам ДБО на бумажном носителе (Приложение №2 к настоящим Правилам ДБО) в 2 (Двух) экземплярах.

Банк может отказать Клиенту в заключении Договора ДБО в случаях, предусмотренных Федеральным законом от 07.08.2001 № 115-ФЗ.

2.3. Договор ДБО считается заключенным в случае акцепта (принятия) Банком Заявления о присоединении к Правилам ДБО.

Акцепт Банком Заявления о присоединении к Правилам ДБО осуществляется после проведения Банком идентификации Клиента и его представителей, выгодоприобретателей и бенефициарных владельцев в соответствии с законодательством (если соответствующая идентификация не была осуществлена Банком ранее, в том числе при открытии счета).

2.4. Настоящий Договор ДБО может быть заключен только при наличии Договора банковского счета, заключенного между сторонами и является неотъемлемой его частью.

2.5. Настоящий Договор ДБО распространяется на все Счета Клиента в Банке, как открытые на дату заключения Договора ДБО, так и на счета, которые будут открыты Клиентом в последующем.

2.6. Обслуживание Клиента с использованием Системы осуществляется Банком в соответствии с законодательством Российской Федерации, настоящим Договором ДБО и Договором банковского счета.

3. ОБЩИЕ ПОЛОЖЕНИЯ

3.1. Правила ДБО регулируют вопросы предоставления Банком Клиенту возможности использования Системы в рамках Договора банковского счета.

3.2. Клиент, присоединяясь к Правилам ДБО, обязуется следовать их требованиям и условиям, оплачивать услуги Банка в соответствии с Тарифами.

3.3. Банк надлежащим образом исполняет свою обязанность по информированию Клиента путем размещения на сайте Банка Правил ДБО и в офисах Банка, руководств пользователя по использованию Системы, рекомендаций по информационной безопасности и иной информации.

3.4. До присоединения к Правилам Клиент обязан ознакомиться с информацией, размещенной на сайте Банка, с рекомендациями по информационной безопасности и неукоснительно соблюдать их требования.

4. СОГЛАШЕНИЯ СТОРОН

4.1. Стороны признают, что применяемая в Системе криптографическая защита информации, обеспечивающая шифрование, создание и проверку ЭП, соответствуют законодательству Российской Федерации и подзаконным актам уполномоченных органов, применяемым в области криптографической защиты информации, и достаточны для защиты информации от несанкционированного доступа со стороны третьих лиц, подтверждения принадлежности ЭП Владельцу ключа, подлинности и авторства ЭД, в том числе при рассмотрении спорных ситуаций.

Криптографическая защита информации, передаваемая посредством Системы, осуществляется Банком на основании бессрочной действующей лицензии, выданной Центром по лицензированию, сертификации и защите государственной тайны ФСБ России.

4.2. Стороны признают, что в соответствии с частью 2 статьи 6 Закона 63-ФЗ «Об электронной подписи», ЭД, подписанные ЭП Представителей Клиента, юридически равнозначны соответствующим документам на бумажном носителе, подписанным собственноручными подписями Представителями Клиента, наделенных соответствующими полномочиями подписывать соответствующие документы, заверенных оттиском печати Клиента и оформленных в соответствии с требованиями законодательства.

4.3. Стороны признают, что Сертификат ключа проверки ЭП, подписанное действующим Ключом ЭП Владельца сертификата ключа проверки ЭП признается равнозначным Сертификату ключа проверки ЭП на бумажном носителе подписанному стороной и заверенной печатью (при наличии).

4.4. Клиент предоставляет право распоряжения денежными средствами, находящимися на Счете, с использованием ЭП своим Представителям.

Электронные документы, передаваемые Клиентом в Банк по Системе, в том числе Распоряжения Клиента на списание денежных средств со Счета, иные документы, передаваемые Клиентом в Банк по Системе должны быть подписаны Представителями в соответствии с Карточкой и Соглашением об их сочетании.

Электронные документы, не относящиеся к распоряжению счетом, передаваемые Клиентом в Банк по Системе, должны быть подписаны ЭП лица, имеющего соответствующие полномочия.

4.5. Стороны признают, что получение Клиентом от Банка запросов и уведомлений по Системе юридически эквивалентно получению от Банка документов на бумажном носителе, подписанных уполномоченными представителями Банка и заверенных оттиском печати Банка.

4.6. Стороны договорились, что в целях исполнения Договора банковского счета, Клиент имеет право передавать в Банк электронные копии документов, подписанными уполномоченными лицами Клиента, которые приравниваются к документам, составленным на бумажных носителях.

Клиент вправе предоставить в Банк посредством Системы документы (копии документов), подписанные ЭП для целей идентификации и обновления сведений, проверки правоспособности Клиента и полномочий лиц, действующих от имени Клиента, в том числе при заключении/исполнении/прекращении Договора ДБО.

Электронные копии документов с использованием Системы передаются Клиентом в следующем порядке:

- передача электронных копий документов осуществляется с указанием Клиентом в тексте Письма перечня прикрепленных к Письму электронных копий документов с указанием точных данных в отношении каждого из прикрепленных документов, позволяющих идентифицировать соответствующий документ;
- подписанием Письма ЭП Клиент подтверждает, что прикрепленные к Письму электронные копии документов идентичны оригиналам соответствующих документов.

По первому требованию Банка Клиент обязуется предоставить в Банк соответствующие присланным электронным копиям оригиналы документов в указанный в требовании Банка срок.

Передача электронных копий документов, заверенных в указанном выше порядке, осуществляется Клиентом в случаях, не запрещенных требованиями действующего законодательства Российской Федерации, нормативных актов Банка России и других контролирующих органов, когда действующим законодательством Российской Федерации, нормативными актами Банка России и других контролирующих органов не установлено требований по предъявлению Клиентом в Банк и приему Банком только оригиналов документов, а также с соблюдением условий, предусмотренных настоящими Правилами, Договором банковского счета, иными договорами Сторон.

4.7. Стороны признают, что каждая Сторона обязана за собственный счет поддерживать в рабочем состоянии свои программно-технические средства, используемые для обмена документами по Системе в соответствии с Правилами ДБО и Приложениями к ним, в том числе Клиент обеспечивает наличие компьютера / Мобильного устройства для использования Системы, удовлетворяющего системным требованиям, указанным в пункте 5.1 настоящих Правил ДБО, устанавливает программное обеспечение для web-версии, используя ссылки на Сайте Банка / Мобильное приложение с web-сайтов авторизованных магазинов приложений на Мобильное устройство.

Клиент самостоятельно выбирает организацию провайдера, обеспечивающую доступ к сети Интернет. Все расходы, связанные с подключением к сети Интернет, эксплуатацией и обменом данными с Банком через сеть Интернет, осуществляются Клиентом за счет собственных средств и не входят в стоимость услуг Банка.

4.8. Отправка Банком SMS-сообщений Пользователю осуществляется только на номера мобильных телефонов российских операторов сотовой связи.

Отправка Банком push-сообщений Пользователю осуществляется только на зарегистрированные в Мобильном приложении Мобильные устройства.

В случае изменения Номера телефона Клиента (Владельца ключа) и/или при изменении Владельца ключа, Клиент должен предоставить в Банк информацию с актуализацией номеров телефонов для получения SMS-сообщений, оформленную Клиентом по форме Приложения № 8 к Правилам ДБО.

4.9. Банк не несет ответственность за качество услуг, предоставляемых операторами сотовой связи и провайдерами доступа в сеть Интернет.

4.10. Использование Клиентом Системы допускается из любых мест и любыми возможностями при условии обязательного выполнения Клиентом (Владельцем ключа) обязательств по безопасной работе с использованием Системы и рекомендациями по обеспечению информационной безопасности (Приложение № 1 к настоящим Правилам ДБО).

4.11. Стороны признают, что Кодовое слово, установленное Клиентом, используется в случае блокирования своей работы в Системе / блокирования Ключа ЭП (например, при компрометации Ключа ЭП).

Банк не несет ответственности за последствия сообщения Банком по телефону информации после сообщения Банку Кодового слова.

4.12. Стороны признают, что Клиент несет полную ответственность за действия, совершенные третьими лицами, в случае передачи им средств подтверждения («Весточка» или MAC-токена VIFIT) / Мобильного устройства, и/или в случае создания условий для несанкционированного использования ими Системы / Средств ЭП / Средств подтверждения / Мобильного устройства, и/или в случае разглашения Клиентом Кодового слова / пароля от носителя информации с Ключом ЭП. Клиент несет полную ответственность за ущерб, причиненный Банку указанными действиями и/или бездействием.

4.13. Клиент согласен, что в качестве доказательства при разбирательстве по факту нарушений Правил ДБО и требований по защите от вредоносных программ применяются логины (журналы) Системы ДБО и журналы модуля Системы детектирования вредоносных программ.

4.14. Стороны признают, что обязанность Банка, предусмотренная пунктом 4 статьи 9 Федерального закона от 27.06.2011 № 161-ФЗ «О национальной платежной системе», по информированию Клиента о совершении операций с использованием Системы, надлежащим образом выполняется Банком одним из способов:

- присвоением ЭД в Системе статуса, соответствующего текущей стадии обработки ЭД в АБС. Порядок уведомления Клиента установлен в разделе 7 Правил ДБО;

- отражением операции по Счету в выписке по Счету в Системе;

- направлением SMS-сообщения на номер мобильного телефона, указанный Клиентом в заявлении, принятом Банком к исполнению, в качестве номера телефона для направления Банком уведомлений о совершении операций по Счету;

- направлением push-сообщения на Мобильное устройство, зарегистрированное в Мобильном приложении;

– направлением сообщения на адрес электронной почты, указанный Клиентом в Системе, для направления Банком уведомлений о совершении операций по Счету.

Перечень и описание статусов ЭД приведен в разделе 7 Правил ДБО.

4.15. Стороны признают, что Ключ ЭП прекращает свое действие:

- в связи с истечением установленного срока его действия;
- в случае расторжения данного Договора ДБО;
- на основании заявления Владельца ключа и/или Уполномоченного представителя Клиента в случае компрометации ключа;
- в случае прекращения деятельности Банка по эксплуатации Системы ДБО без перехода его функций другим лицам;
- в иных случаях, установленных действующим законодательством Российской Федерации.

Действие Ключа ЭП прекращается в момент внесения записи об этом в Систему либо автоматически в момент окончания срока действия Ключа ЭП.

4.16. Стороны признают, что электронные документы, подписанные ЭП уполномоченным лицом Клиента и/или Банка, создаваемые в Системе, могут быть использованы в качестве доказательств при решении спорных вопросов в соответствии с разделом 13 настоящих Правил ДБО, в досудебном порядке, а также в качестве доказательств при разрешении споров в Арбитражном суде по месту заключения Договора банковского счета, в соответствии с требованиями действующего законодательства Российской Федерации.

4.17. Стороны признают в качестве единой шкалы времени при работе с Системой московское поясное время. Контрольным является время системных часов аппаратных средств Банка.

4.18. Стороны признают, что обработка Банком персональных данных, содержащихся в документах, переданных в Банк Клиентом, осуществляется в соответствии с условиями Договора банковского счета.

4.19. Прием, исполнение, отзыв и возврат Распоряжений Клиента на перевод денежных средств осуществляются в соответствии с Договором банковского счета.

4.20. Все платежные поручения, направляемые Клиентом в Банк на исполнение, должны быть подтверждены Клиентом SMS-сообщениями или получением одноразовых паролей на MAC-токен за исключением следующих случаев:

- при осуществлении переводов денежных средств в бюджет и внебюджетные фонды (налоги, сборы, пошлины и другие обязательные платежи в бюджеты всех уровней и внебюджетные фонды, установленные действующим законодательством Российской Федерации);
- при осуществлении переводов в пользу Доверенных получателей (контрагенты, в пользу которых регулярно совершаются платежи), за исключением переводов в пользу конкретного Доверенного получателя на суммы, превышающие заранее определенную сумму (в случае, если эта сумма определена Клиентом в Системе по конкретному Доверенному получателю).

4.21. Стороны признают, что выписки из Счета (Счетов) Клиента и документы к ней (ним), подтверждающие совершённые операции, предоставляются Банком в электронном виде без дублирования на бумажном носителе. Дубликаты на бумажном носителе предоставляются в установленном Банком порядке на основании письменного запроса Клиента с учётом Тарифов.

4.22. Стороны признают, что подписание Клиентом Заявления означает, что Клиент ознакомлен и полностью согласен с условиями Договора ДБО, Тарифами, а также готов своевременно и в полном объёме исполнять обязательства, из него вытекающие.

5. ПОРЯДОК ПОДКЛЮЧЕНИЯ К ЛИЧНОМУ КАБИНЕТУ СИСТЕМЫ

5.1. Клиент самостоятельно и за свой счет организует АРМ, оборудованное персональным компьютером и отвечающий следующим требованиям:

- компьютер со свободным USB разъемом, позволяющим использовать USB-токен;
- операционная система компьютера и мобильного телефона должна быть актуальной и обновляемой, поддерживаемая разработчиком;
- установленный и настроенный Интернет-браузер актуальной версии;
- настроенный канал доступа в Интернет;
- на компьютере установлена, используется и на постоянной основе обновляется современная система антивирусной защиты.

5.2. Для работы в Системе Банк предоставляет Клиенту средство криптографической защиты информации и/или устройство для генерации одноразовых паролей MAC-токен BIFIT, USB-токен «MS_KEY К» – «АНГАРА» Исп.8.1.1, Рутокен ЭЦП 3.0, MAC-токен, которое выдается Клиенту в офисах после заключения Договора ДБО и уплаты Клиентом комиссии в соответствии с Тарифами по Акту приема-передачи (Приложение № 4 к настоящим Правилам ДБО).

5.3. Для подключения к Системе Клиенту необходимо в адресной строке браузера ввести адрес <https://ibank.nipbank.ru/ibank2> или зайти на сайт Банка <https://nipbank.ru> и перейти на страницу входа, нажав

«Web-NIPBank для предприятий», выполнить процедуры входа и регистрации в личном кабинете Системы в соответствии с Документацией, размещенной на странице входа Системы.

Установку и настройку личного кабинета Системы можно осуществить при помощи специалиста Банка в Центральном офисе Банка или на территории Клиента в часы работы Банка в соответствии с тарифами Банка. Для этого Клиенту необходимо предоставить в Банк Заявление по форме Приложения № 10 к Правилам ДБО.

5.4. Каждый Владелец ключа самостоятельно осуществляют генерацию своего Ключа ЭП в Системе на устройстве для защищенного хранения ключей или на сервере Банка, по результатам которой распечатывает Сертификат на бумажном носителе в двух экземплярах по форме, установленной Приложением № 5 к Правилам ДБО. Сертификат заполняется Клиентом, собственноручно подписывается Владелцем ключа и лицом, уполномоченным Клиентом на заключение Договора ДБО, и заверяется печатью Клиента (при наличии).

Надлежащим образом оформленный Сертификат в двух экземплярах передается Клиентом в Банк. Допускается предоставление Сертификата Ключа посредством электронного документооборота, подписанного ЭП.

Владелец Ключа ЭП при генерации Ключа ЭП облачной подписи безусловно соглашается на хранение Ключа ЭП облачной подписи на Сервере Банка.

5.5. Банк сверяет информацию в полученных от Клиента экземплярах Сертификата с данными, представленными в Системе по результатам генерации Клиентом. При положительном результате сверки данных Банк принимает от Клиента Сертификат (один из экземпляров Сертификата), и возвращает Клиенту второй экземпляр Сертификата с соответствующими отметками Банка о приеме Сертификата.

5.6. Активация Ключа проверки ЭП в Системе (в Каталоге ключей проверки электронной подписи) осуществляется администратором Системы после приема Банком от Клиента и подтверждения корректности надлежащим образом оформленного Сертификата.

При этом Банк не имеет доступа к Ключу ЭП Клиента:

- в случае использования средств криптографической защиты в Банке хранятся только Ключи проверки ЭП Клиента, с помощью которых банковский сервер проводит аутентификацию Клиента в системе и проверяет подпись клиента под электронными документами;

- в случае использования облачной подписи Ключи ЭП Клиента находятся на специальном Сервере Банка в отдельных контейнерах, зашифрованных специальными ключами, созданными на основе пароля Клиента.

5.7. Банк подключает Клиента к Системе (начинает обслуживать Клиента в Системе) с момента регистрации необходимого количества Ключей проверки ЭП Владелец ключа в Системе.

5.8. Срок действия Ключа проверки ЭП, зарегистрированного в Системе, и, соответственно, Ключа ЭП определяется сроком полномочий Владельца ключа на основании документов, представленных Клиентом в Банк, но не может превышать 1 (Одного) года с даты начала действия Ключа проверки ЭП. Дата начала действия Ключа проверки ЭП и дата окончания действия Ключа проверки ЭП указываются Банком в Сертификате (далее – срок действия Сертификата).

Банк уведомляет Клиента (Владельца ключа) о предстоящем истечении срока действия Сертификата посредством Системы не менее чем за 30 (Тридцать) календарных дней до даты окончания срока действия Сертификата. Для продолжения работы в Системе Клиент должен сгенерировать (создать) новый Ключ ЭП и зарегистрировать в Банке соответствующий Ключ проверки ЭП согласно пунктам 5.4, 5.5 Правил ДБО.

В случае истечения срока действия полномочий Владельца ключа, Система уведомляет Владельца ключа об истечении срока действия полномочий. Клиент должен предоставить в Банк документы, подтверждающие полномочия Владельца ключа.

5.9. Клиент (Владелец ключа) может сгенерировать новый Ключ ЭП и зарегистрировать в Банке соответствующий Ключ проверки ЭП.

5.10. Ключ проверки ЭП считается недействительным со дня, следующим за днем окончания срока его действия.

5.11. Сертификаты хранятся Банком в Системе и на бумажных носителях не менее 5 (Пяти) лет с даты прекращения действия соответствующих Ключей проверки ЭП (Ключей ЭП).

5.12. Для получения одноразовых паролей Клиент обязан подключить любое дополнительное средство безопасности, а именно: SMS-сервис или MAC-токен по форме Приложений № 8 и 9 Правил ДБО.

5.13. Клиент может определить конечный перечень IP – адресов, с которых Клиент может осуществлять доступ к Системе, путем передачи Клиентом в Банк Заявления на IP-фильтрацию при использовании Системы по форме Приложения № 6 к Правилам ДБО, содержащего IP-адреса Клиента (далее – Заявление об IP – фильтрации) (в подтверждение принятия Банком заявления Клиенту передается его копия с отметками Банка о принятии документа).

Внесение изменений в перечень IP-адресов, с которых Клиент может осуществлять доступ к Системе, осуществляется путем передачи Клиентом в Банк нового Заявления об IP-фильтрации. При этом с даты

начала применения Банком последнего принятого от Клиента Заявления об IP – фильтрации предыдущее Заявление об IP – фильтрации утрачивает свою силу.

Отказ Клиента от ограничения перечня IP – адресов, с которых Клиент может осуществлять доступ к Системе, осуществляется путем передачи Клиентом в Банк Заявления на отказ от IP-фильтрации при использовании системы «Клиент-Банк» по форме Приложения № 7 к Правилам ДБО.

Заявления по формам Приложений № 6 и 7 применяются Банком с рабочего дня, следующего за днем их принятия.

6. ПОРЯДОК РАБОТЫ С ЭЛЕКТРОННЫМИ ДОКУМЕНТАМИ

6.1. Личный кабинет Системы позволяет Клиенту:

- формировать и направлять в Банк электронные документы в соответствии с Приложением № 3 к Правилам ДБО, а также иные электронные документы, предусмотренные Системой;
- получать и просматривать информацию об операциях по Счетам и об остатках на Счетах;
- просматривать информацию о распоряжениях, поступивших от Клиента в Банк, в том числе о статусах распоряжений и уведомлениях об исполнении распоряжений;
- доступ к регулярно обновляемым Банком справочникам, которые ведутся в Системе, в том числе к справочникам БИК, SWIFT, КБК;
- создавать и редактировать список «Доверенные получатели» в справочнике «Доверенные получатели». Использование справочника «Доверенные получатели» позволяет Клиенту создавать список контрагентов, в пользу которых регулярно совершаются платежи. По каждому Доверенному получателю Клиент может установить в Системе ограничение на возможную сумму Платежного поручения, исполняемого без дополнительного подтверждения SMS-сообщением;
- в разделе «Мониторинг» Системы дополнительно к уведомлениям об операциях, указанных в разделе 7 Правил ДБО, выбрать одно или несколько уведомлений (о входе в систему, о поступлении документа в Банк; об изменении статуса электронного документа, выписку по счету), а также указать способ доставки этих уведомлений – мобильное приложение «Весточка», SMS-сообщение на номер телефона, на адрес электронной почты;
- устанавливать Мобильное приложение на Телефон;
- организовывать обмен электронными документами с внешними бухгалтерскими программами;
- устанавливать лимиты на сумму одной операции, на общую сумму всех операций за период в целях противодействия осуществлению переводов денежных средств без согласия Клиента. Общая сумма совершенных переводов за период устанавливается в отношении совокупности операций по всем счетам Клиента, открытым в Банке в валюте Российской Федерации, осуществляемых с использованием Системы.

Клиент не сможет подписать Платежное поручение своим Ключом ЭП (и, соответственно, направить его в Банк на исполнение) в случае, если сумма Платежного поручения превышает Лимит одного платежа и/или если общая сумма всех Платежных поручений, направленных Клиентом в Банк на исполнение конкретным рабочим днем (с учетом суммы этого Платежного поручения) превышает Дневной лимит платежей и/или если общая сумма всех Платежных поручений, направленных Клиентом в Банк на исполнение в текущем календарном месяце (с учетом суммы этого Платежного поручения) превышает Месячный лимит платежей.

В случае использования Ключа ЭП облачной подписи Лимит одного платежа/ Дневной лимит платежей не устанавливается.

Для установления лимита Клиент направляет заявление в соответствии с Приложением № 11 Правил ДБО. Для изменения ранее установленных лимитов Клиент направляет новое заявление в порядке, изложенном в Приложении № 11 Правил ДБО. Для отмены действия всех установленных Клиентом ранее лимитов Клиент направляет через Систему в Банк письмо в произвольной форме об их отмене.

Действие Ограничений/отмены Ограничений начинается со следующего рабочего дня Банка после приема Банком письма Клиента в электронном виде через Систему;

- осуществлять иные действия, предусмотренные функционалом Системы;

6.2. Клиент самостоятельно устанавливает соединение с Интернет-сервером Системы и следит за поддержанием сеанса связи во время работы в Системе.

6.3. После осуществленной Системой аутентификации Клиента Клиент получает доступ к Системе и начинает работу в ней.

6.4. Клиент создает электронные документы в Системе, заверяет созданными ключами ЭП, дополнительно подтверждает платежные поручения SMS-сообщениями или MAC-токеном.

6.5. Банк предоставляет Клиенту возможность в рамках Системы использовать ИС «Одно окно». В Системе Клиент получает возможность оплаты счетов (начислений), выставленных через ИС «Одно окно». Для использования ИС «Одно окно» Клиент составляет письмо для подключения к ИС «Одно окно» в электронном виде с учетом требований и в порядке, изложенном в Приложении № 12 к Правилам ДБО.

7. ПОРЯДОК УВЕДОМЛЕНИЯ КЛИЕНТА ОБ ОПЕРАЦИЯХ В СИСТЕМЕ

7.1. В целях исполнения требований пункта 4 статьи 9 Федерального закона от 27.06.2011 № 161-ФЗ «О национальной платежной системе» Банк информирует Клиента о совершении каждой операции посредством направления уведомлений одним из способов:

- изменение статуса, соответствующего ЭД в Системе;
- предоставление выписки по счету через Систему.

7.2. Система присваивает платежным поручениям следующие статусы:

Статус	Основание для присвоения статуса
новый	статус присваивается по результатам создания Клиентом в Системе платежного поручения
подписан	присваивается в случае, если документ подписан, но число подписей под платежным поручением меньше необходимого. При внесении изменений в документ с таким статусом и его последующем сохранении статус документа меняется на «новый»
требует подтверждения	присваивается платежному поручению после получения необходимого количества подписей и в случае использования дополнительных мер защиты документа при отправке в Банк. Платежное поручение приобретает статус при определенных настройках системы – использование механизма одноразовых паролей для подтверждения документов, сумма которых превышает заданное пороговое значение. При данном механизме Клиент должен обладать источником получения одноразовых паролей – мобильным телефоном с зарегистрированным в Системе номером для получения SMS-сообщений или MAC-токеном;
доставлен	присваивается платежному поручению, когда число подписей под документом соответствует необходимому для рассмотрения документа Банком. Статус «доставлен» является для Банка указанием начать обработку документа (исполнить или отвергнуть)
на обработке	присваивается платежному поручению при его обработке в АБС
на исполнении	присваивается при принятии платежного поручения к исполнению
в картотеке	присваивается платежному поручению, принятому Банком к исполнению и помещенному в очередь неисполненных в срок распоряжений или в очередь распоряжений, ожидающих разрешения на проведение операций в связи с недостаточностью денежных средств на счете Клиента: <ul style="list-style-type: none"> – относящемуся к четвертой и предыдущей очередности списания денежных средств, установленной пунктом 2 статьи 855 Гражданского кодекса Российской Федерации; – распоряжений взыскателей средств пятой очередности списания денежных средств с банковского счета, установленной пунктом 2 статьи 855 Гражданского кодекса Российской Федерации; – принимаемому Банком к исполнению в соответствии с законодательством и договором
исполнен	присваивается платежному поручению при его исполнении Банком и проведении по счету
отвергнут	присваивается: <ul style="list-style-type: none"> – платежному поручению, не принятому Банком к исполнению по причине его несоответствия требованиям, установленным действующим законодательством Российской Федерации, Договором ДБО или иным договором, заключенным Сторонами. Банк дополнительно указывает в Системе причину, по которой документ не принят к исполнению; – в результате исполнения Банком сообщения на отзыв платежного поручения; – в иных случаях по усмотрению Банка
удален	присваивается платежному поручению, удаленному Клиентом. Удалению подлежат только документы в статусе «новый», «подписан» или «отвергнут». Документы в статусе «новый» и «подписан» удаляются из Системы безвозвратно

7.3. Результат проверки электронного документа считается положительным, если электронный документ оформлен в соответствии с действующим законодательством Российской Федерации и требованиями, установленными договорами между Банком и Клиентом, заверен надлежащей (надлежащими) ЭП и прошел в Банке проверку ЭП.

7.4. После проверки Банком электронного документа Система присваивает ему статус в соответствии с п. 7.2 Правил ДБО.

Статус каждого электронного документа отражает текущий этап его обработки и отслеживается Клиентом в процессе работы с Системой. В случае если Клиент своевременно не осуществил контроль за результатами обработки электронного документа, ответственность за возникающие в данном случае риски несет Клиент.

Обо всех операциях, произведенных по Счету в течение дня, в том числе с использованием Системы, Банк информирует Клиента путем предоставления ему возможности самостоятельно формировать выписку по Счету посредством Системы.

Выписку по Счету с отражением всех операций по Счету за текущий день Клиент имеет возможность сформировать посредством Системы на следующий за ним рабочий день.

7.5. Статус «исполнен» электронного документа подтверждает положительный результат контроля целостности Распоряжения, структурного контроля, контроля значений реквизитов Распоряжения и контроля достаточности денежных средств на счетах Клиента, а также иных видов контроля, предусмотренного законодательством, необходимых для исполнения Распоряжения Клиента.

Клиент признает надлежащим уведомлением об этапах и результатах обработки электронных документов, предусмотренные функционалом Системы. Клиент согласен с тем, что получение расчетным документом статуса «Исполнен» в Системе является надлежащим уведомлением Банком Клиента о совершении Банком соответствующей операции по Счету, определенном пунктом 4 статьи 9 Федерального закона 161-ФЗ.

7.6. Информация об электронных документах, не принятых Банком к исполнению по причине их оформления с нарушением требований Договора ДБО, требований, установленных законодательством и/или договорами, заключенными между Сторонами, доводится до Клиента путем присвоения электронному документу статуса «отвергнут» с указанием причины, по которой документ не принят к исполнению.

7.7. Банк имеет право посредством Системы направить Клиенту для акцепта платежное требование в валюте Российской Федерации, выставленное контрагентом Клиента к Счету (в случае отсутствия у Банка заранее данного акцепта Клиента).

Клиент обязан направить в Банк посредством Системы Заявление об акцепте (отказе от акцепта) платежного требования не позднее 5 (Пяти) рабочих дней со дня получения документа от Банка.

7.8. Клиент с использованием Системы заполняет и направляет в Банк Заявку на наличные, содержащую информацию о дате выдаче, сумме, номере банковского счета Клиента.

Если Клиент передумал получать денежные средства по направленной в Банк Заявке на наличные, либо принял решение изменить сумму, Клиент должен уведомить Банк любым удобным ему способом.

7.9. Клиент вправе отозвать электронные документы, указанные в Приложении № 3 к Правилам ДБО, направленные посредством Системы в Банк для исполнения, при этом Статус документа должен быть «доставлен», «на обработке», «на исполнении».

7.10. Клиент (Владелец ключа) имеет возможность самостоятельно осуществить соответствующие настройки в разделе «Мониторинг» Системы с целью автоматического получения информации о следующих событиях в Системе на указанный им адрес электронной почты и/или в виде SMS-сообщений на номер телефона и/или Push-сообщений в мобильном приложении «Весточка»:

- о входе в Систему;
- о поступлении в Банк документа;
- об отвержении документа;
- о входящих документах;
- о текущих остатках;
- выписка по счету.

7.11. При выявлении Банком операции, соответствующей признакам осуществления перевода денежных средств без добровольного согласия Клиента¹ Банк приостанавливает прием к исполнению Распоряжения Клиента на 2 (Два) календарных дня (следующих за датой приостановления)

Банк незамедлительно информирует Клиента о выполнении Банком действий, предусмотренных абзацем первым настоящего пункта Правил ДБО.

Уведомление должно содержать:

1) информацию о приостановлении исполнения Распоряжения Клиента на перевод денежных средств со Счета на срок не более 2 (Двух) календарных дней в связи с выявлением Банком операции, соответствующей признакам осуществления перевода денежных средств без добровольного согласия Клиента;

2) рекомендации по снижению рисков повторного осуществления перевода денежных средств без добровольного согласия Клиента;

3) требование подтверждения Клиентом Распоряжения. Подтверждение направляется Клиентом в Банк не позднее 1 (Одного) календарного дня, следующего за днем приостановления Банком приема к исполнению

¹ Признаки осуществления перевода денежных средств без согласия клиента устанавливаются Банком России и размещаются на его официальном сайте в информационно-телекоммуникационной сети "Интернет".

указанного Распоряжения с использованием Системы либо одним из способов, предусмотренных пунктом 8.1 Правил ДБО, если иной способ не указан в уведомлении Банка, или о возможности совершения Клиентом повторной операции, содержащей те же реквизиты получателя (плательщика) и ту же сумму перевода (далее - повторная операция). Способ направления подтверждения определяется Клиентом самостоятельно. При этом подтверждение Распоряжения с использованием Системы направляется Клиентом в Банк лицом, уполномоченным распоряжаться денежными средствами, находящимися на Счете.

В дополнение к указанной информации Банк вправе запросить у Клиента подтверждение о том, что перевод денежных средств не является переводом денежных средств без добровольного согласия Клиента.

7.12. Информирование Клиента, в соответствии с пунктами 7.11, 7.13 и 9.4.13 Правил ДБО, осуществляется путем направления уведомления по Системе или письма на адрес электронной почты и/или по телефону, заявленных Клиентом Банку в качестве средства связи. Способ направления, указанного в настоящем пункте Правил ДБО уведомления, определяется Банком самостоятельно.

Обязанность Банка по направлению Клиенту уведомлений с использованием Системы, предусмотренных Федеральным законом 161-ФЗ, считается исполненной в дату направления Банком соответствующего уведомления Клиенту.

7.13. Если иное не предусмотрено настоящим пунктом Правил ДБО, при получении от Клиента подтверждения Распоряжения или осуществление действий по совершению Клиентом повторной операции в соответствии с подпунктом 3 пункта 7.11 Правил ДБО, Банк незамедлительно принимает к исполнению подтвержденное Распоряжение Клиента или совершает повторную операцию, при условии отсутствия иных установленных законодательством Российской Федерации оснований не принимать Распоряжение Клиента к исполнению.

При неполучении от Клиента подтверждения Распоряжения и/или информации, запрошенной в соответствии с пунктом 7.11 Правил ДБО, указанное Распоряжение считается не принятым к исполнению и аннулируется, а при осуществлении действий по совершению Клиентом повторной операции и/или при неполучении информации, запрошенной в соответствии с пунктом 7.11 настоящих Правил, повторная операция считается несовершенной.

В случае, если, несмотря на направление Клиентом подтверждения Распоряжения или осуществление действий по совершению повторной операции Банк получил от Банка России информацию, содержащуюся в базе данных о случаях и попытках осуществления переводов денежных средств без добровольного согласия клиента, Банк приостанавливает прием к исполнению подтвержденного Распоряжения Клиента или отказывает в совершении Клиентом повторной операции на 2 (Два) календарных дня со дня направления Клиентом подтверждения Распоряжения.

Банк в порядке, установленном пунктом 7.12 Правил ДБО, незамедлительно уведомляет Клиента о приостановлении приема к исполнению подтвержденного Распоряжения Клиента или об отказе в совершении Клиентом повторной операции с указанием причины такого приостановления (отказа) и срока такого приостановления, а также о возможности совершения Клиентом последующей повторной операции.

В случае приостановления приема к исполнению подтвержденного Распоряжения Клиента в соответствии с абз. 3 настоящего пункта Правил ДБО, по истечении 2 (Двух) календарных дней со дня направления Клиентом подтверждения Распоряжения в соответствии с подпунктом 3 пункта 7.11 Правил ДБО Банк незамедлительно принимает к исполнению указанное Распоряжение при условии отсутствия иных установленных законодательством Российской Федерации оснований не принимать Распоряжение Клиента к исполнению. В случае отказа в совершении Клиентом повторной операции в соответствии с частью абз. 3 настоящего пункта по истечении 2 (Двух) календарных дней со дня осуществления действий по совершению Клиентом повторной операции Банк исполняет последующую повторную операцию Клиента при отсутствии иных установленных законодательством Российской Федерации оснований не совершать последующую повторную операцию Клиента.

7.14. Действие [пунктов 7.11 – 7.13](#) не распространяется на случаи осуществления переводов денежных средств, являющихся заработной платой и (или) иными доходами, в отношении которых [статьей 99](#) Федерального закона от 2 октября 2007 года № 229-ФЗ "Об исполнительном производстве" установлены ограничения размеров удержания, а также переводов денежных средств, являющихся доходами, на которые в соответствии со [статьей 101](#) Федерального закона от 2 октября 2007 года № 229-ФЗ "Об исполнительном производстве" не может быть обращено взыскание.

8. ДЕЙСТВИЯ ПРИ КОМПРОМЕТАЦИИ СРЕДСТВ ИДЕНТИФИКАЦИИ, АУТЕНТИФИКАЦИИ И АВТОРИЗАЦИИ КЛИЕНТА В СИСТЕМЕ

8.1. При компрометации средств идентификации, аутентификации и авторизации, т.е. при возникновении утраты доверия к тому, что Ключ ЭП, пароль от носителя информации с Ключом ЭП (МАС-токен BIFIT, USB-токен «АНГАРА», Рутокен), телефоны, номера телефонов и e-mail, используемые при

работе в Системе и Мобильное устройство, содержащее приложение для работы в Системе, стали доступны неуполномоченному лицу (лицам):

- утрата устройств защищенного хранения ключа ЭП (MAC-токен BIFIT, USB-токен «АНГАРА», Рутокен), в том числе с последующим их обнаружением;
- утрата Мобильного устройства с установленным Мобильным приложением и/или с номером мобильного телефона, на который поступают SMS/Push-сообщения;
- увольнение/прекращение полномочий сотрудников/представителей Клиентов, имевших доступ к ключам ЭП;
- временный доступ посторонних лиц к устройству защищенного хранения Ключа ЭП либо подозрение, что такой доступ имел место;
- обнаружение на компьютере или Мобильном устройстве, с использованием которых осуществляется доступ в Систему, постороннего программного обеспечения;
- искажение информации о Распоряжении в приложении «Весточка», на экране MAC-токена BIFIT или SMS-сообщении с кодом подтверждения (изменение получателя, суммы Распоряжения);
- иные события, в результате которых Ключи ЭП, телефоны, номера телефонов, устройства для хранения ключей, Мобильное приложение могут стать доступными неуполномоченным лицам и (или) несанкционированным процессам.

Клиент обязан незамедлительно прекратить работу в Системе, не предпринимать никаких действий для поиска и удаления компьютерных вирусов, восстановления работоспособности АРМ, сообщить о случившемся в Банк одним из следующих способов:

➤ по телефонам по рабочим дням (кроме пятницы) с 09:30 до 18:00, а в пятницу с 9:30 до 17:00 по московскому времени. Если компрометация произошла в нерабочий день, то Клиент представляет уведомление о компрометации на следующий за ним рабочий день:

Служба технической поддержки Банка: +7 (495) 276-22-82; +7 (495) 737-02-97;

Операционное управление Банка: +7 (495) 786-21-58.

При телефонном звонке в Банк с целью временно заблокировать работу необходимо сообщить Кодовое слово, которое зарегистрировано в Системе.

В случае блокировки Банком работы Клиента в Системе, которая осуществлена при обращении Клиента по телефонам, указанным выше, Клиент обязан не позднее следующего рабочего дня, предоставить в Банк уведомление на бумажном носителе о подтверждении блокировки, заверенное подписями уполномоченных лиц и оттиском печати (при наличии) в 2 (двух экземплярах).

➤ направить уведомление на электронную почту: **it@nipbank.ru** или **operzal@nipbank.ru**, с последующим представлением оригинала не позднее следующего рабочего дня;

➤ при личной явке Клиента / уполномоченного представителя Клиента в Банк с предоставлением письменного уведомления, заверенного подписями уполномоченных лиц и оттиском печати.

Несоблюдение Клиентом указанных требований является нарушением порядка использования Системы и не влечет возникновения ответственности Банка перед Клиентом за убытки, понесенные Клиентом, в том числе в результате действий третьих лиц, возникшие вследствие нарушения, установленного данным пунктом порядка направления уведомления о компрометации. В случае непредставления Клиентом в Банк уведомления о компрометации в соответствии с настоящим пунктом Банк не возобновляет прием ЭД.

8.2. Письменное уведомление, направляемое Клиентом в Банк по факту Компрометации ключа Клиента в Системе, должно содержать описание обстоятельств, послуживших причиной компрометации и/или использования Системы лицами, не имеющими соответствующих полномочий, а также описание предпринятых Клиентом или его представителями действий и их результатов.

Банк фиксирует обращение Клиента по факту Компрометации ключа в Журнале регистрации и временно блокирует работу Клиента в Системе. На уведомлении Клиента Банк проставляет дату и время его получения и передает Клиенту второй экземпляр уведомления.

О приостановлении использования Клиентом Системы Банк уведомляет Клиента, направив ему сообщение на электронную почту и/или в устной форме по телефону, заявленных Клиентом Банку в качестве средства связи.

8.3. При получении от Клиента информации о Компрометации ключа Банк незамедлительно приостанавливает операции по Счетам с использованием Системы, отменяет исполнение Распоряжений, принятых к исполнению, но не исполненных до момента поступления заявления о компрометации, если Банк имеет технологическую возможность такой отмены и блокирует Ключи ЭП.

Регенерация Ключей ЭП производится Клиентом в соответствии с пунктами 5.4, 5.5 Правил ДБО.

8.4. Банк вправе заблокировать работу Клиента в Системе при наличии подозрений в компрометации Ключа ЭП Клиента без предварительного уведомления Клиента. Возобновление работы Клиента происходит после регенерации Ключа ЭП Клиента в соответствии с пунктами 5.4, 5.5 Правил ДБО.

8.5. Банк не несет ответственность в случае несвоевременного уведомления Клиентом Банка о необходимости блокировки Ключей ЭП или об изменении Номера телефона.

9. ПРАВА И ОБЯЗАННОСТИ СТОРОН

9.1. Клиент имеет право:

9.1.1. Использовать Систему в соответствии с Правилами ДБО для создания и обмена с Банком Электронными документами.

9.1.2. Получать консультации специалистов Банка по вопросам использования Системы, а также по вопросам установки и настройки необходимого программного обеспечения на автоматизированном рабочем месте Клиента

9.1.3. Получать информацию о выполнении Банком электронного документа Клиента на проведение операций по Счету посредством Системы.

9.1.4. Перевыпускать свои Ключи ЭП в порядке, предусмотренном Правилами ДБО.

9.1.5. Отзывать Электронные документы, ранее переданные в Банк посредством Системы, в случае, если на момент поступления требования Клиента об отзыве Электронного документа Банком еще не были совершены действия по его исполнению, делающие отзыв документа невозможным.

9.1.6. Клиент имеет право подключить многофакторную аутентификацию с использованием одноразовых паролей при входе в Систему с использованием MAC-токена, SMS-информирования.

9.1.7. Клиент имеет право установить ограничения (лимиты) на осуществление переводов в валюте Российской Федерации в целях противодействия осуществлению переводов денежных средств без согласия Клиента (далее – Ограничение).

9.1.8. Оформлять и передавать в Банк распоряжения на бумажных носителях в период неработоспособности (неисправности) Системы, а также при приостановлении обслуживания Клиента с использованием Системы в соответствии с положениями настоящих Правил ДБО.

9.1.9. Клиент имеет право обратиться в Банк с требованием возобновить приостановленные ранее услуги с использованием Системы.

9.1.10. Представлять в Банк и получать от Банка документы на бумажных носителях в случае блокировки/ временной блокировки Ключа ЭП

9.1.11. Расторгнуть Договор ДБО, заключенный в соответствии с Правилами ДБО, подав в Банк соответствующее заявление в свободной форме.

9.1.12. Осуществлять иные права, предусмотренные Законодательством и Договором ДБО, заключенным в соответствии с Правилами ДБО.

9.2. Клиент обязан:

9.2.1. Соблюдать условия и требования Договора банковского счета, Правил ДБО, Рекомендаций по информационной безопасности, в том числе в отношении АРМ, используемого на стороне Клиента.

9.2.2. До присоединения к Правилам ДБО ознакомиться с документацией по работе с Системой ДБО на Сайте Банка, а также исполнять все указанные в ней требования и рекомендации.

9.2.3. Клиент обязуется в соответствии со статьей 10 Федерального Закона от 06 апреля 2011 года № 63-ФЗ «Об электронной подписи»:

3) обеспечивать конфиденциальность Ключей ЭП, в частности не допускать использование принадлежащих ему Ключей ЭП без его согласия третьими лицами;

4) не использовать Ключ ЭП при наличии оснований полагать, что конфиденциальность данного ключа нарушена;

5) уведомлять Банк о нарушении конфиденциальности Ключа ЭП Клиента в соответствии с разделом 8 настоящих Правил ДБО.

9.2.4. Незамедлительно уведомлять Банк о замене Номера телефона, об утере Телефона, Устройства для хранения ключей ЭП, MAC-токена.

9.2.5. Извлекать Устройство для хранения ключей ЭП из компьютера во всех случаях, когда Система не используется.

9.2.6. Хранить и использовать логин и пароль для входа в Мобильное приложение, а также в Мобильное устройство таким образом, чтобы исключить к ним доступ любых третьих лиц.

9.2.7. Проверять корректность данных в получаемых от Банка на Номер телефона SMS-сообщениях перед дополнительным подтверждением в Системе соответствующих Платежных поручений, проверять корректность данных в получаемых от Банка сообщениях в Мобильном приложении перед дополнительным подтверждением соответствующих Платежных поручений.

9.2.8. Контролировать срок действия Ключей ЭП и Сертификатов ключей проверки ЭП и заблаговременно инициировать их замену.

9.2.9. В случае прекращения действия Договора ДБО уничтожить ключи ЭП.

9.2.10. Клиент обязан предоставить сведения и документы, необходимые для идентификации уполномоченных Клиентом лиц (включая Владельцев сертификатов ключей проверки ЭП), в том числе при смене Владельцев сертификатов ключей проверки ЭП, в случае, если ранее такие сведения и документы в Банк не предоставлялись.

9.2.11. Предоставлять в Банк документы, информацию и сведения по запросу Банка в сроки, указанные в запросе, в целях исполнения требований законодательства Российской Федерации.

9.2.12. Своевременно оплачивать услуги Банка в соответствии Тарифами Банка.

9.2.13. Формировать ЭД в Системе ДБО в соответствии с законодательством Российской Федерации.

9.2.14. В течение дня регулярно заходить в Систему ДБО для оперативного реагирования на информационные сообщения, направляемые Банком, а также создаваемые Системой отчеты с целью незамедлительного принятия мер защиты от неправомерного (несанкционированного) доступа в Систему третьих лиц/ использования третьими лицами Ключа ЭП Уполномоченного представителя Клиента. При этом вышеуказанные сообщения, отчеты, иные сведения и информация считаются полученными Клиентом с даты формирования указанных сообщений в Системе.

9.2.15. В случае утраты Ключей ЭП, носителя ключа ЭП и (или) использования Системы без добровольного согласия Клиента, незамедлительно после обнаружения факта утраты и (или) использования Системы без добровольного согласия Клиента направить соответствующее письменное уведомление Банку в свободной форме способами, предусмотренными пунктом 8.1 Правил ДБО, но не позднее рабочего дня, следующего за днем получения от Банка уведомления о совершенной операции.

9.2.16. Незамедлительно информировать Банк в письменном виде об изменении сведений, предоставленных Клиентом в Банк ранее, в том числе об изменении его местонахождения, почтового адреса, номеров телефонов, электронных адресов и основного вида деятельности, в рамках которого Клиентом осуществляются операции по счету с использованием Системы.

9.3. Банк имеет право:

9.3.1. Ежемесячно взимать со счетов Клиента без его дополнительного распоряжения комиссионное вознаграждение за предоставление Услуги в соответствии с Тарифами, с которыми Клиент ознакомлен и согласен. Комиссионное вознаграждение взимается Банком в 1 (первый) рабочий день месяца с любого Счета Клиента, открытого в Банке.

9.3.2. Изменять, отменять, дополнять в одностороннем порядке Тарифы с предварительным уведомлением Клиента за 10 (Десять) календарных дней путем размещения соответствующей информации на Сайте Банка и в офисах Банка.

9.3.3. Приостановить обслуживание Клиента в Системе, о чем Банк направляет Клиенту соответствующее уведомление (с указанием причины) по Системе, и/или на адрес электронной почты, и/или по телефону на номер, заявленных Клиентом Банку в качестве средства связи:

- в случае неисполнения Клиентом обязательств по уплате Банку комиссионного вознаграждения за предоставление услуги Банк направляет уведомление на адрес электронной почты, указанный Клиентом в анкете, в течение 1 (Одного) рабочего дня до приостановления;

- при истечении срока полномочий лиц, указанных в карточке с образцами подписей и оттиска печати Клиента (в соответствии с пунктом 4.6 Правил ДБО);

- при истечении срока действия ключа ЭП (в соответствии с пунктом 5.8 Правил ДБО);

- до предоставления в Банк надлежаще оформленных документов, подтверждающих наличие полномочий у Владельцев сертификатов ключей проверки ЭП;

- до момента регистрации новых Владельцев сертификатов ключей проверки ЭП в случае смены уполномоченных лиц Клиента;

- в случае выявления признаков нарушения безопасности или подозрения на возможный несанкционированный доступ к Системе от имени Клиента приостановить прием, регистрацию и исполнение поступающих в Банк Распоряжений, передачу Клиенту Электронных документов посредством Системы, а также совершение сделок с Клиентом, а также в случаях, предусмотренных Федеральным законом 161-ФЗ;

- для выполнения работ, связанных с обслуживанием Системы, с указанием сроков проведения таких работ;

- в случае если в единый государственный реестр юридических лиц внесена запись о недостоверности сведений о Клиенте;

- при возникновении разногласий и конфликтных ситуаций, возникших в рамках настоящего Договора ДБО, заключенного в соответствии с Правилами ДБО;

- в случае, если Банку стало известно на основании сведений, полученных из ЕГРЮЛ, что уполномоченное лицо, ранее идентифицированное в качестве единоличного исполнительного органа юридического лица, на момент получения сведений не является лицом, имеющим право без доверенности действовать от имени Клиента.

- в случаях, указанных в подпункте 9.3.4, 9.3.7 Правил ДБО.

9.3.4. Приостановить использование Клиентом Системы в день получения от Клиента уведомления о Компрометации ключей Клиента, предусмотренного пунктом 9.2.3 Правил ДБО, о чем Банк направляет Клиенту соответствующее уведомление (с указанием причины), одним из способов, предусмотренных пунктом 7.12 настоящих Правил.

9.3.5. Возобновить доступ Клиента к Системе, приостановленный согласно подпункту 9.3.4 Правил ДБО, не позднее следующего рабочего дня после проведения Клиентом процедуры внеплановой смены Ключей ЭП.

9.3.6. Возобновить использование Системы / прием и отправку ЭД по Системе, приостановленных в соответствии с подпунктом 9.3.3 Правил ДБО, в случае получения Банком от Клиента документов, надлежащим образом подтверждающих полномочия Владельцев ключей проверки ЭП (уполномоченных лиц Клиента).

9.3.7. Приостановить обслуживание Клиента с использованием Системы ДБО и/или отказать в исполнении ЭД, с предварительным уведомлением Клиента по Системе ДБО в течение 1 (Одного) рабочего дня до приостановления:

- в случае непредоставления Клиентом по запросу Банка документов, необходимых Банку для исполнения требований Федерального закона от 07.08.2001 № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма»;

- в случае, если у Банка возникают подозрения, что операции осуществляются Клиентом с целью легализации (отмывания) доходов, полученных преступным путем, финансирования терроризма и финансирования распространения оружия массового уничтожения;

- если проведение операции нарушает положения Федерального закона от 10.12.2003 № 173-ФЗ «О валютном регулировании и валютном контроле»;

- в случае непредоставления документов, либо недостоверных документов, либо представления документов, не соответствующих требованиям Федерального закона от 10.12.2003 № 173-ФЗ «О валютном регулировании и валютном контроле»;

- по иным основаниям, предусмотренным законодательством Российской Федерации.

Банк сообщает Клиенту о возобновлении работы с использованием Системы, направив уведомление через Систему не позднее дня возобновления работы.

Приостановление в обслуживании Счетов Клиента по Системе не является отказом в совершении операции в соответствии с пунктом 11 статьи 7 Федеральный закон от 07.08.2001 N 115-ФЗ, а также отказом в предоставлении услуги по информационному обмену и взаимодействию, в том числе:

- предоставлению выписок о движении денежных средств по Счету Клиента;

- приему документов свободного формата (в том числе вложенный файл в документ свободного формата).

9.3.8. Банк имеет право без предварительного уведомления Клиента приостановить прием и исполнение поступающих в Банк Распоряжений в случае получения сведений о введении в отношении Клиента любой из процедур банкротства, предусмотренной Федеральным законом от 26.10.2002 № 127-ФЗ «О несостоятельности (банкротстве)».

9.3.9. Отказаться от заключения Договора ДБО либо расторгнуть Договор ДБО, заключенный в соответствии с Правилами ДБО, в одностороннем порядке по основаниям, предусмотренным пунктом 5.2 статьи 7 Федерального закона № 115-ФЗ. Банк в течение 5 (пяти) рабочих дней доводит до сведения Клиента уведомление о дате и причинах принятия такого решения на бумажном носителе путем вручения лично или заказным письмом через Почту России, в электронном виде в формате .pdf по Системе «Клиент-Банк» или на адрес электронной почты Клиента.

9.3.10. При открытии новых Счетов Клиенту подключать их к Системе в автоматическом режиме без предоставления Клиентом заявления на их подключение.

9.3.11. Установить лимит на проведение операций по переводу денежных средств в валюте Российской Федерации в Системе.

9.3.12. Проводить Аутентификацию Клиентов, их Представителей с использованием Кодового слова при обращении в Банк по телефону. Аутентификация считается пройденной, если Клиент/его Представитель верно сообщил сотруднику Банка Кодовое слово, указанное им при регистрации в Системе.

9.3.13. Запрашивать и получать от Клиента копии ЭД на бумажном носителе, оформленные надлежащим образом и удостоверенные уполномоченным лицом Клиента.

9.3.14. Определять перечень сервисов/услуг, доступных Клиенту для использования в Системе, а также условия их использования.

9.3.15. Проводить обновление Системы.

9.3.16. Не осуществлять техническую поддержку Мобильного приложения, версия которого ниже версии предыдущего Мобильного приложения, выпущенного Банком.

9.3.17. Отказывать в установке, обновлении и работоспособности Мобильного приложения на Мобильном устройстве, версия операционной системы которого устарела.

9.3.18. Отказать в приеме и отправке ЭД по Мобильному приложению в связи с прекращением доступа к Системе посредством Мобильного приложения по инициативе Банка, о чем Банк направляет Клиенту соответствующее уведомление (с указанием причины и даты прекращения доступа к Системе посредством Мобильного приложения).

Прекращение доступа к Системе посредством Мобильного приложения не прекращает доступ к Системе.

9.3.19. Приостановить использование Клиентом Системы, если получена от Банка России информация, содержащаяся в базе данных о случаях и попытках осуществления переводов денежных средств без добровольного согласия клиента, которая содержит сведения, относящиеся к Клиенту и (или) его Системе (в соответствии с пунктом 11.6 статьи 9 Федерального закона 161-ФЗ, на период нахождения сведений, относящихся к Клиенту и (или) его Системе, в базе данных о случаях и попытках осуществления переводов денежных средств без добровольного согласия клиента).

9.3.20. Приостановить использование Системы в случаях, предусмотренных законодательством Российской Федерации с последующим уведомлением Клиента одним из способов, предусмотренных пунктом 7.12 настоящих Правил.

9.3.21. Выполнять иные обязанности, предусмотренные законодательством Российской Федерации и настоящими Правилами.

9.4. Банк обязан:

9.4.1. Банк обязан принимать к исполнению ЭД, полученные по Системе от Клиента, подписанные необходимым количеством ЭП Клиента, соответствующие требованиям настоящих Правил ДБО и действующему законодательству Российской Федерации.

9.4.2. Банк обязан информировать Клиента о совершенных операциях с использованием Системы одним из способов, установленных в Порядке об уведомлении Клиента об операциях.

9.4.3. Банк осуществляет консультирование Клиента по вопросам эксплуатации Системы и предоставляет Клиенту необходимые рекомендации для работы с Системой.

9.4.4. Уведомлять Клиента в случае внесения Банком изменений (дополнений) в Правила ДБО и Приложения к ним.

9.4.5. Обеспечивать конфиденциальность созданных Банком Ключей ЭП / Облачной подписи.

9.4.6. Предварительно уведомлять Клиента об изменении Тарифов не позднее чем за 10 (Десять) календарных дней, а об изменении условий настоящего Договора ДБО не позднее чем за 5 (Пять) календарных дней до даты введения в действие соответствующих изменений.

Об изменении Тарифов и Правил ДБО Клиент информируется Банком путем размещения соответствующей информации на Сайте Банка и в офисах Банка.

9.4.7. В случае приостановки приема, исполнения Распоряжений посредством Системы, на время производства плановых технических работ принять разумные меры для уведомления об этом Клиента не позднее, чем за 1 (Один) рабочий день до начала работ, в том числе путем опубликования соответствующего сообщения в Системе;

9.4.8. В случае внеплановой приостановки приема, исполнения Электронных документов посредством Системы по техническим причинам и в случае наступления форс-мажорных обстоятельств принять разумные меры для незамедлительного уведомления об этом Клиента путем размещения соответствующей информации на Сайте Банка и в офисах Банка, в том числе путем опубликования соответствующего сообщения в Системе.

9.4.9. По требованию Клиента осуществлять обновление Ключей проверки ЭП Клиента в установленном порядке.

9.4.10. Незамедлительно приостановить операции по Счетам с использованием Системы и заблокировать Ключи ЭП при получении от Клиента информации о Компрометации ключа.

9.4.11. При получении от Клиента уведомления о списании денежных средств со Счета Клиента без его добровольного согласия, указанного в пункте 9.2.15 настоящих Правил, Банк незамедлительно направляет в адрес оператора по переводу денежных средств, обслуживающего получателя, уведомление о приостановлении зачисления денежных средств на банковский счет получателя (далее – уведомление о приостановлении) по форме и в порядке, установленном Банком России, с целью подтверждения легальности перевода и права получателя на переведенные средства.

В случае возврата денежных средств оператором по переводу денежных средств, обслуживающего получателя, Банк обязан осуществить зачисление денежных средств на банковский счет Клиента, не позднее 2 (Двух) рабочих дней со дня их получения.

9.4.12. Приостановить использование Клиентом Системы, если от Банка России получена информация, содержащаяся в базе данных о случаях и попытках осуществления переводов денежных средств без

добровольного согласия клиента, которая содержит сведения, относящиеся к Клиенту и (или) его Системе, в том числе сведения федерального органа исполнительной власти в сфере внутренних дел о совершенных противоправных действиях, получаемые в соответствии Федеральным законом 161-ФЗ, на период нахождения указанных сведений в базе данных о случаях и попытках осуществления переводов денежных средств без добровольного согласия Клиента на основании пункта 11.7 статьи 9 161-ФЗ.

9.4.13. Банк уведомляет Клиента о приостановлении использования Системы в случаях, предусмотренных пунктами 9.3.19 и 9.4.12 одним из способов, предусмотренных пунктом 7.12 настоящих Правил, а также подать Заявление в Банк России об исключении сведений, относящихся к Клиенту и (или) его Системе, в том числе сведений федерального органа исполнительной власти в сфере внутренних дел о совершенных противоправных действиях, из базы данных о случаях и попытках осуществления переводов денежных средств без добровольного согласия клиента.

9.4.14. Банк незамедлительно возобновляет использование Клиентом Системы и незамедлительно уведомляет Клиента о возможности использования Системы в порядке, установленном пунктом 7.12 Правил ДБО, в случае получения от Банка России информации об исключении сведений, относящихся к Клиенту и (или) его Системе из базы данных о случаях и попытках осуществления переводов денежных средств без добровольного согласия клиента, при отсутствии иных оснований для приостановления использования Системы в соответствии с законодательством Российской Федерации или настоящими Правилами ДБО.

9.4.15. Банк обязан возместить Клиенту сумму операции, совершенной без добровольного согласия Клиента, после получения от Клиента информации о Компрометации ключа, если Распоряжение, на основании которого были списаны денежные средства, было подписано скомпрометированной ЭП, в случае неисполнения Банком обязанности, предусмотренной пунктом 9.2.15 настоящих Правил.

9.4.16. Банк не обязан возместить Клиенту сумму операции, совершенной без добровольного согласия Клиента, в случае надлежащего исполнения Банком обязанности по информированию Клиента о совершении операции и не направлении Клиентом уведомления Банку в соответствии с настоящими Правилами ДБО.

9.4.17. Банк обязан хранить направленные Клиенту и полученные от Клиента уведомления о Компрометации ключа при работе с Системой не менее 3 (Трёх) лет.

10. СТОИМОСТЬ УСЛУГ И ПОРЯДОК РАСЧЕТОВ

10.1. За предоставление Клиенту услуг, связанных с использованием Системы, Банк взимает плату в соответствии с действующими Тарифами Банка, с которыми Клиент ознакомлен и согласен.

Тарифы размещаются в офисах Банка, осуществляющих обслуживание Клиентов и на официальном сайте Банка www.nipbank.ru.

10.2. Об изменении тарифов за услуги Банк извещает Клиента за 10 календарных дней до введения их в действие путем размещения в офисах Банка, осуществляющих обслуживание Клиентов, и/или на официальном сайте Банка www.nipbank.ru.

10.3. В случае несогласия с изменениями тарифов, Клиент имеет право досрочно расторгнуть Договор ДБО, заключенный в соответствии с Правилами ДБО, в порядке, предусмотренном пунктом 12.6 Правил ДБО.

10.4. Оплата услуг Банка, указанных в пункте 10.1 Правил ДБО, производится в 1 (Первый) рабочий день месяца, в котором будет осуществляться обслуживание Системы. Клиент дает согласие на списание комиссии с расчетного счёта Клиента без его дополнительного распоряжения (заранее данный акцепт). Частичная оплата не допускается.

Из-за неисполнения Клиентом обязательств по уплате Банку комиссионного вознаграждения за предоставление услуги, Банк имеет право приостановить обслуживание Клиента в Системе, о чем Банк направляет Клиенту соответствующее уведомление (с указанием причины) на адрес электронной почты, указанный Клиентом в анкете или по Системе.

При этом Клиент не освобождается от обязанности уплачивать Банку комиссионное вознаграждение за предоставление Услуги в соответствии с Тарифами, когда такое приостановление произошло в соответствии с условиями Правил ДБО.

Возобновить прием и отправку ЭД по Системе не позднее рабочего дня, следующего после дня уплаты Клиентом Банку комиссионного вознаграждения за предоставление Услуги.

10.5. Клиент в течение 3 (трех) рабочих дней после подписания Договора ДБО должен оплатить стоимость подключения Банком Клиента к Системе и обслуживание Системы. В случае, если срок с даты заключения Договора ДБО до конца текущего месяца составляет менее 15 дней, оплата за обслуживание Системы не производится, если - более 15 дней, оплата осуществляется как за полный месяц.

11. ОТВЕТСТВЕННОСТЬ СТОРОН

11.1. Банк не несет ответственности перед Клиентом за убытки, возникшие в результате надлежащего исполнения Банком требований, предусмотренных настоящим Договором, заключенным в соответствии с

Правилами ДБО, и Федеральным законом 161-ФЗ.

11.2. Банк не несет ответственность за последствия исполнения распоряжений, выданных неуполномоченными лицами, в тех случаях, когда с исполнением предусмотренных банковскими правилами и настоящими Правилами ДБО Банк не мог установить факт выдачи распоряжения неуполномоченными лицами, в том числе и в случае, когда Клиент не представил надлежащим образом оформленные изменения или дополнения в сведения, представленные в Банк ранее, о Клиенте и/или лицах, уполномоченных распоряжаться Счетом/денежными средствами на Счете.

11.3. Банк не несет ответственности:

1) в случаях финансовых потерь, понесенных Клиентом в связи с нарушением и (или) ненадлежащим исполнением им требований по организации и осуществлению защиты от вредоносных программ клиентских АРМ пользователя Системы;

2) за последствия исполнения ЭД, подписанных недействительной или скомпрометированной ЭП Клиента, поступивших в Банк до получения им информации о недействительности или нарушения конфиденциальности ключей ЭП Клиента;

3) в случае несоблюдения Клиентом положений Правил ДБО, в том числе Рекомендаций Банка по обеспечению информационной безопасности при работе с Системой (Приложение № 1);

4) за возможные опечатки и искажения в платежных документах, предоставленных Клиентом как на бумажном носителе, так и отправленных по Системе и заверенных его ЭП, возникшие по вине Клиента;

5) за неблагоприятные последствия для Клиента, наступившие в результате несанкционированного доступа к Системе неуполномоченных или третьих лиц, возникшего не по вине Банка;

6) за неблагоприятные последствия для Клиента, наступившие в результате утечки информации, являющейся банковской тайной, вызванные нарушением Клиентом условий настоящих Правил ДБО;

7) в случае несвоевременного уведомления Банка Клиентом о необходимости блокировки ключей;

8) в случае несоблюдения Клиентом требований, предусмотренных в Приложениях к настоящим Правилам ДБО.

11.4. Клиент несет ответственность:

9) за правильность и достоверность передаваемой в Банк, в т.ч. с помощью Системы информации;

10) за правильное использование СКЗИ;

11) за исполнение требований по организации и осуществлению защиты от вредоносных программ клиентских АРМ пользователя Системы;

12) за своевременное предоставление в Банк информации об изменении сведений, ранее предоставленных в Банк, о Клиенте и/или лицах, уполномоченных распоряжаться Счетом/денежными средствами на Счете.

11.5. Стороны освобождаются от ответственности за частичное или полное неисполнение обязательств по Договору, если такое неисполнение произошло в результате:

13) технических неисправностей, возникших по вине третьих лиц, и повлекших неполадки в работе Системы и препятствующих выполнению Клиентом и Банком своих обязательств согласно настоящим Правилам ДБО.

При этом срок исполнения обязательств переносится на срок соразмерно времени, в течение которого действовали такие обстоятельства.

11.6. Приостановление или прекращение использования Клиентом Системы не прекращает обязательств Клиента и Банка, возникших до момента приостановления или прекращения, указанного использования.

12. СРОК ДЕЙСТВИЯ ДОГОВОРА ДБО, ПОРЯДОК ЕГО ИЗМЕНЕНИЯ И РАСТОРЖЕНИЯ

12.1. Договор ДБО заключается на неопределенный срок и вступает в силу с даты, указанной Банком в Заявлении о заключении Договора ДБО.

12.2. Договор ДБО расторгается по инициативе одной из Сторон с предварительным уведомлением другой Стороны за 10 (десять) рабочих дней до предполагаемой даты расторжения.

12.3. Настоящий Договор может быть расторгнут в следующих случаях:

14) на основании информации, размещенной на официальном сайте Федеральной налоговой службы <https://www.nalog.gov.ru/o> внесении в ЕГРЮЛ записи об исключении из ЕГРЮЛ юридического лица или его ликвидации (письменное уведомление о закрытии Счета в этом случае Клиенту Банком не направляется) или о внесении в ЕГРИП записи о прекращении деятельности индивидуального предпринимателя (при отсутствии денежных средств на Счете);

15) в связи с закрытием всех банковских счетов Клиента, подключенных к Системе;

16) в случае принятия в течение календарного года двух и более решений об отказе в выполнении Распоряжения Клиента о совершении операций по основаниям, предусмотренным Федеральным законом № 115-ФЗ;

17) в иных случаях, предусмотренных действующим законодательством Российской Федерации.

12.4. Банк вправе в одностороннем порядке расторгнуть Договор ДБО в случаях:

- 18) не подключения Клиента к Системе в течение 30 (Тридцати) календарных дней с даты заключения настоящего Договора ДБО;
- 19) при задержке уплаты Клиентом в течение 3 (Трех) календарных месяцев вознаграждения за услуги Банка по Системе;
- 20) в иных случаях, предусмотренных законодательством.

12.5. Банк направляет Клиенту письменное уведомление о расторжении Договора ДБО на адрес электронной почты, указанный Клиентом в анкете, и Договор ДБО считается расторгнутым через 3 (Три) рабочих дня с даты направления Банком Клиенту такого уведомления.

12.6. Клиент вправе расторгнуть Договор ДБО, направив в Банк заявление о расторжении Договора ДБО в произвольной форме. Заявление должно быть подписано уполномоченным лицом и заверено печатью Клиента. Обслуживание в Системе прекращается со дня, следующего за днем получения Банком Заявления о расторжении Договора ДБО, если более поздняя дата расторжения Договора ДБО не указана в заявлении Клиента. Вознаграждение за последний месяц обслуживания Системы взимается с Клиента в соответствии с действующими Тарифами.

12.7. Банк вправе в одностороннем порядке вносить изменения в Правила ДБО, уведомив об этом Клиента, не позднее чем за 5 (Пять) календарных дней до вступления в силу указанных изменений. Указанный в настоящем пункте срок уведомления может быть уменьшен Банком в случае внесения изменений в Правила ДБО в связи с изменением законодательства Российской Федерации, а также в связи с введением дополнительных услуг для Клиента.

12.8. Банк уведомляет Клиента о внесении изменений в Правила ДБО путем размещения на информационных стендах во всех офисах Банка по обслуживанию Клиентов, а также на официальном сайте Банка www.nirbank.ru. Дополнительно к указанному способу уведомления Банк по своему усмотрению может использовать иные способы информирования Клиента.

Клиент самостоятельно осуществляет действия, необходимые для своевременного ознакомления с информацией, указанной в абзаце первом настоящего пункта, размещенной на официальном сайте Банка. Банк не несет ответственности за несвоевременное осуществление Клиентом указанных действий.

12.9. Новая редакция Правил ДБО с даты, начиная с которой применяется новая редакция, распространяется на отношения Сторон по настоящему Договору ДБО, в том числе на отношения Сторон, связанные с исполнением обязательств, возникших в соответствии с настоящим Договором ДБО до дня начала применения указанной новой редакции Правил ДБО.

12.10. В случае несогласия с изменениями, вносимыми в Правила ДБО, Клиент вправе расторгнуть Договор ДБО до вступления таких изменений в силу в порядке, установленном в пункте 12.6 Правил ДБО.

13. ПОРЯДОК РАЗРЕШЕНИЯ СПОРОВ СТОРОН

13.1. Все разногласия, споры и конфликтные ситуации, возникающие между Сторонами вследствие неисполнения или ненадлежащего исполнения Договора ДБО, заключенного в соответствии с Правилами ДБО, а также его заключения, изменения и расторжения разрешаются с учетом взаимных интересов Сторон путем переговоров. На время разрешения спорной ситуации Банк имеет право немедленно приостановить прием/отправку ЭД в одностороннем порядке, установленном пунктом 9.3.3 Правил ДБО.

13.2. Споры Сторон по поводу авторства и неизменности содержания Электронных документов рассматриваются согласительной комиссией, формируемой Сторонами. Процедура рассмотрения спора состоит из следующих этапов:

- предъявление претензии одной из Сторон другой Стороне;
- формирование согласительной комиссии для рассмотрения спора;
- разрешение Комиссией спора по существу.

13.3. Клиент представляет Банку заявление, содержащее существо претензии с указанием на ЭД, на основании которого Банк выполнил операции по счету Клиента не позднее дня, следующего за днем получения от Банка уведомления о совершенной операции. Претензия может быть направлена путем официального вручения уполномоченному представителю Банка либо заказным письмом с уведомлением о вручении, а также путем направления претензии посредством Системы.

13.4. Банк информирует Клиента о результатах рассмотрения заявления (претензии) в течение 30 (Десяти) рабочих дней (при трансграничном переводе денежных средств – в течение 60 (Шестидесяти) рабочих дней) с даты подачи заявления (претензии) Клиента.

Клиент в течение 5 (Пяти) рабочих дней после получения результатов рассмотрения претензии должен рассмотреть представленные объяснения и сообщить в письменной форме Банку о снятии претензии.

В случае несогласия Клиента с полученным результатом рассмотрения заявления (претензии), спорная ситуация передается для разрешения специально создаваемой согласительной комиссии.

Согласительная комиссия созывается Банком на основании письменного заявления Клиента.

В указанном заявлении Клиент сообщает о несогласии с позицией Банка и необходимости созыва согласительной комиссии. Также Клиент должен указать лицо (лиц), уполномоченное(-ых) представлять интересы Клиента в согласительной комиссии.

Не позднее 10 (Десяти) рабочих дней с даты получения заявления Банк по согласованию с Клиентом назначает дату, место и время начала работы согласительной комиссии. Банк письменно, не позднее, чем за 3 (Три) рабочих дня до начала работы согласительной комиссии, уведомляет Клиента о назначенной дате, времени и месте начала работы согласительной комиссии и необходимости представить в Банк копию оспариваемого документа на бумажном носителе, заверенную подписями и печатью Клиента (при наличии печати).

В случае если Клиент не известил в установленный настоящим пунктом срок в письменной форме Банк о согласии с представленными объяснениями и отказе от создания Комиссии или о своем согласии на формирование и участие в Комиссии и/или не обеспечил к назначенному времени участие в Комиссии своих представителей, то Клиент автоматически считается согласным с представленными объяснениями и отказавшимся от создания согласительной комиссии.

13.5. В состав Комиссии включается равное количество представителей Банка и Клиента и при необходимости – независимые эксперты – представители компании разработчика Системы. Выбор членов комиссии осуществляется по согласованию со всеми участниками. Максимальное количество членов Комиссии не должно превышать 6 (Шести) человек.

Полномочия представителей Сторон для участия в Комиссии должны подтверждаться оформленными надлежащим образом доверенностями.

13.6. Для работы комиссии Банк предоставляет помещение и оборудование, необходимое для работы комиссии.

13.7. При рассмотрении спора об авторстве и неизменности содержания Электронного документа Комиссия в течение 10 (Десяти) рабочих дней осуществляет следующие этапы:

- техническая экспертиза ЭД, заверенного необходимым количеством ЭП Клиента, на основании которого Банком выполнены оспариваемые Клиентом действия по его Счету;
- техническая экспертиза Ключей проверки ЭП Владельца ключа Клиента, период действия и статус Ключей проверки ЭП Владельцев ключа Клиента, и установление их принадлежности Клиенту;
- техническая экспертиза корректности ЭП Владельца ключа Клиента в ЭД;
- составление акта на основе полученных данных.

13.8. При рассмотрении спора Комиссия использует следующие данные в качестве эталонных:

- данные имеющегося в Банке архива отправленных/принятых Электронных документов;
- сертификаты, подписанные Клиентом и хранящиеся в Банке (далее – Эталонные сертификаты).

13.9. Разрешение споров осуществляется на основании результатов проверки ЭП Клиента в спорном Электронном документе.

13.10. Принимая во внимание математические свойства алгоритма ЭП, реализованные в соответствии с государственными стандартами Российской Федерации, гарантирующими невозможность подделки значения ЭП любым лицом, не обладающим ключом ЭП, Стороны признают, что рассмотрение спора в отношении авторства и неизменности содержания Электронного документа заключается в доказательстве принадлежности ЭП конкретного Электронного документа конкретной Стороне.

13.11. Рассмотрение согласительной комиссией спора об авторстве и неизменности содержания Электронного документа проводится с использованием АРМ «Операционист» Системы.

13.12. В целях формирования Протокола проверки ЭП администратор Системы со стороны Банка в присутствии Комиссии осуществляет следующие действия:

- выводит на печать Сертификат ключа проверки ЭП Клиента из Каталога ключей проверки ЭП, используя АРМ «Администратор» Системы;
- сравнивает распечатанный сертификат Ключа проверки ЭП Клиента из Каталога ключей проверки ЭП с Эталонным сертификатом, предоставленным Комиссии Администратором Системы, а также с аналогичным сертификатом, хранящимся у Клиента и представленным Комиссии Клиентом. Значения Ключа проверки ЭП Клиента, содержащиеся в Каталоге ключей проверки ЭП, в Эталонном сертификате и в хранящемся у Клиента сертификате, должны совпадать. В случае их несовпадения верным признается Эталонный сертификат;

– с помощью АРМ «Операционист» находит спорный документ и, используя меню «Проверить ЭП», формирует результат проверки ЭП, в котором указываются идентификаторы Ключей ЭП, участвовавшие в подписи Электронного документа, авторство которого оспаривается;

- выводит на печать Документ со списком идентификаторов подписавших его Ключей ЭП.

В случае если спорный Электронный документ был подписан несколькими ЭП, данная процедура повторяется применительно к каждой ЭП.

13.13. Принадлежность ЭП Клиенту и авторство Электронного документа считается установленным,

если идентификаторы Ключей проверки ЭП, содержащихся в списке идентификаторов, подписавших Документ, и Эталонном сертификате совпадают, в Документе сформирована запись «ЭП Корректна», и распечатанный сертификат Ключа проверки ЭП Клиента из Каталога ключей проверки совпадает с Эталонным сертификатом.

13.14. Заключение согласительной комиссии оформляется письменно в двух экземплярах – по одному для каждой из Сторон - и подписывается всеми членами согласительной комиссии.

13.15. Составленное Заключение может быть предъявлено в судебные и иные органы в случае необходимости такого разбирательства и будет являться доказательством признания подлинности ЭД/непризнания подлинности ЭД, в зависимости от того, что было зафиксировано в Заключении.

13.16. В случае возникновения спорных вопросов, связанных с заключением, толкованием, исполнением, изменением, расторжением и недействительностью Договора, заключенного в соответствии с правилами ДБО, за исключением споров, в соответствии с пунктом 13.2 настоящих Правил заинтересованная Сторона обязана направить другой Стороне претензию в письменной форме по адресу места нахождения Стороны. Претензии и ответы на них направляются почтовым отправлением (заказанным письмом) либо вручаются под расписку. Спор, связанный с каким-либо из вопросов, указанных в настоящем пункте Правил ДБО, может быть передан на рассмотрение суда по истечении 14 (Четырнадцати) календарных дней со дня направления претензии в соответствии с настоящим пунктом Правил.

Неурегулированные в предусмотренном настоящим разделом Правил ДБО порядке споры подлежат рассмотрению в Арбитражном суде по месту нахождения ответчика в соответствии с действующим законодательством Российской Федерации.

РЕКОМЕНДАЦИИ ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ РАБОТЕ С СИСТЕМОЙ «КЛИЕНТ-БАНК»

Во исполнение пункта 3 статьи 9 Федерального закона от 27.06.2011 № 161-ФЗ «О национальной платежной системе» Банк информирует Клиента о мерах безопасного использования Системы:

1. Назначать сотрудников, ответственных за использование Системы;
2. Обеспечить надежное хранение и защиту от компрометации носителя Ключа ЭП (MAC-токен BIFIT, USB-токен «MS_KEY K» – «АНГАРА» Исп.8.1.1, Рутокен ЭЦП 3.0). Размещение ключевой информации на жестком диске компьютера, на котором установлена Система запрещается;
3. Не передавать посторонним лицам данные об использовании Системы: адрес (IP-адрес) Web-сервера, особенности входа в Систему и использования ключа электронной подписи и т.п.;
4. Не оставлять без присмотра рабочие места с загруженной Системой. Ключевые носители информации, извлекать из USB разъема компьютера по завершении работы;
5. Заменять Ключи ЭП в случаях их компрометации или подозрения на компрометацию. Кроме того, рекомендуется заменять ключи электронной подписи при увольнении/прекращении полномочий сотрудников/представителей Клиентов, имевших доступ к ключам ЭП, а также руководителей, которые подписывали Сертификат ключа проверки электронной подписи;
6. Обратить внимание на увеличение риска хищения и дальнейшего неправомерного использования Ключа ЭП и другой аутентификационной информации при доступе к Системе с гостевых рабочих мест (интернет-кафе, гостиницы, офисные центры и т.д.);
7. Использовать на компьютерах, где установлена Система:
 - лицензионное антивирусное программное обеспечение с регулярным его обновлением (желательно в автоматическом режиме);
 - операционная система компьютера и мобильного телефона должна быть современной, лицензионной и обновляемой, поддерживаемая разработчиком;
 - установленный и настроенный Интернет-браузер актуальной версии;
8. Не вводить конфиденциальные данные, если окно для ввода отличается от стандартных окон Системы (логотип другого банка, другие надписи, шрифт и тому подобное), или отображается не так как всегда (нарушен порядок работы в системе), или получили SMS с паролем на вход в систему, в то время как такой доступ не осуществлялся, или нарушена нумерация платежных поручений и т.д. Необходимо обратиться в службу технической поддержки Банка при нетипичной работе Системы;
9. Периодически (не реже одного раза в год) менять пароль для входа в Систему и не создавать простых и легких паролей (например, 111111, 12345 и т.п.). Не указывать в качестве пароля дату рождения, номера телефонов и иные данные, которые легко можно узнать третьим лицам;
10. Не отвечать на подозрительные письма с просьбой выслать Ключ ЭП, пароль и иные конфиденциальные данные, либо с Вами связались по телефону от имени Банка, с просьбой установить какое-либо программное обеспечение, необходимо связаться со службой технической поддержки Банка и уточнить ситуацию. Банк никогда не осуществляет рассылку электронных писем с просьбой предоставить конфиденциальную информацию (ключи, пароли и т.п.);
11. Всегда используйте контактную информацию службы поддержки Банка, указанную в официальных источниках информации, и не используйте контактную информацию, указанную в письме или полученную в ходе телефонного разговора;
12. В случае, если не удается в штатном режиме войти в Систему или по невыясненным причинам компьютер, с которого осуществляется работа в Системе, перестал загружаться, некорректно реагирует на команды в обычном режиме (самопроизвольное перемещение курсора, открытие и закрытие окон, набор текста), внезапно прекратил работать – рекомендуется **немедленно** обратиться в Службу технической поддержки Банка, проинформировать Банк о сложившейся ситуации;
13. Ограничить доступ (физический и/или удаленный) к компьютеру третьих лиц, не имеющих полномочий для работы с Системой.
14. При работе с почтой не устанавливать и не сохранять подозрительные файлы, полученные из ненадежных источников, скачанные с неизвестных web-сайтов, присланные по электронной почте, полученные в телеконференциях. Такие файлы лучше немедленно удалять. В случае необходимости загрузки файла, убедиться, что он проверен антивирусом.

15. Рекомендуется использовать отдельный компьютер исключительно для работы с Системой. Другие действия (работа с другими программами, работа с электронной почтой, посещение сайтов в Интернете) с этого компьютера осуществляться не должны.

16. Контролировать адресную строку браузера, адрес должен начинаться с <https://ibank.nipbank.ru>. При появлении сообщения о несоответствии сертификата имени узла прекратить работу с Системой и сообщить в службу технической поддержки Банка;

17. Использовать дополнительные средства безопасности – SMS-сервис с получением разовых паролей (Приложение № 8 к Правилам ДБО), MAC-токены (Приложение № 9 к Правилам ДБО), проверку IP-адресов, с которых осуществляется работа с Системой (Приложение № 6 к Правилам ДБО).

18. В случае передачи (списания, утилизации и т.п.) сторонним лицам компьютера, на котором ранее была установлена Система, необходимо удалить с него всю информацию, использование которой третьими лицами может нанести вред Вашей организации.

ЗАЯВЛЕНИЕ
о присоединении к Правилам дистанционного банковского обслуживания клиентов «Нацинвестпромбанк»
(АО) с использованием системы «Клиент-Банк»

Дата заявления «___» _____ 202__ г.

Клиент	
полное или сокращенное официальное наименование организации / ФИО индивидуального предпринимателя / физического лица, занимающегося частной практикой	
В лице	
Действующий на основании	
ИНН/КИО	

Настоящим в соответствии со статьей 428 Гражданского кодекса Российской Федерации Клиент присоединяется к **Правилам дистанционного банковского обслуживания клиентов «Нацинвестпромбанк» (АО) с использованием системы «Клиент-Банк»** (далее – Правила ДБО) и подтверждает, что все положения (условия) Правил ДБО, включая взаимные права и обязанности сторон, а также порядок внесения изменений в Правила ДБО мне понятны.

Все положения Правил ДБО предоставления Банком «Нацинвестпромбанк» (АО) услуги дистанционного банковского обслуживания, включая требования к программно-техническим средствам, порядок подключения услуги и разрешения спорных ситуаций мне понятны.

С рекомендациями по обеспечению информационной безопасности в Системе «Клиент-Банк» ознакомлен.

Настоящим заявляю о своей согласии с тем, что электронный документ, сформированный и подписанный электронной подписью с соблюдением требований Правил ДБО, имеет силу документа, составленного на бумажном носителе и подписанного собственноручной подписью.

(должность руководителя)

(подпись)

(фамилия, инициалы)

М.П. (при наличии)

ОТМЕТКИ БАНКА

Заявление принято (акцептовано) Банком:

Дата принятия Заявления «___» _____ 202__ года.

Подпись уполномоченного сотрудника Банка _____ / _____
подпись Фамилия И.О.

Распоряжение на присоединение к Правилам ДБО:

Заместитель Председателя Правления

М.П. _____

ПЕРЕЧЕНЬ
электронных документов, передаваемых по Системе

	Наименование электронного документа
1	Платежное поручение
2	Заявление об акцепте
3	Платежное требование
4	Инкассовое поручение
5	Заявление на перевод иностранной валюты
6	Поручение на продажу иностранной валюты
7	Поручение на покупку иностранной валюты
8	Распоряжение на списание валюты с транзитного валютного счета
9	Распоряжение на обязательную продажу валюты
10	Поручение на конвертацию иностранной валюты
11	Сведения о валютных операциях
12	Справка о подтверждающих документах
13	Заявление о постановке на учет контракта (кредитного договора)
14	Заявление о снятии с учета контракта (кредитного договора)
15	Заявление о внесении изменений в раздел I ведомости банковского контроля
16	Запрос на отзыв ЭД
17	Письмо в произвольной форме
18	Документы для взаимодействия с системой «Одно окно»

АКТ

приема-передачи средств криптозащиты информации и/или устройств для генерации одноразовых паролей

«___» _____ г.

«Национальный инвестиционно-промышленный банк» (Акционерное Общество), именуемый в дальнейшем «Банк», в лице _____, действующего на основании _____, с одной стороны, и _____, именуемый в дальнейшем «Клиент», в лице _____, действующего на основании _____, с другой стороны, совместно именуемые «Стороны», в соответствии с Договором ДБО на основании Заявления о присоединении к Договору ДБО от «___» _____ 202__ г. составили настоящий Акт о нижеследующем:

Банк передал, а Клиент принял средства криптозащиты информации, устройство(-а) для генерации одноразовых паролей:

- Рутокен ЭЦП 3.0 _____ в количестве _____ штук № _____;
- USB-токен «MS_KEY К» – «АНГАРА» Исп.8.1.1 _____ в количестве _____ штук № _____;
- MAC-токен VIFIT _____ в количестве _____ штук;
- MAC-токен _____ в количестве _____ штук.

При передаче устройств(-а) Сторонами приняты меры по обеспечению его конфиденциальности.

Устройство передано представителю Клиента:

на основании _____

Ответственный за выдачу устройств(-а) ВЫДАЛ	Получатель устройств(-а) ПОЛУЧИЛ
--	---

(подпись) Ф.И.О.

Банк
119121, г. Москва, 2-й Неопалимовский пер., д.10
БИК 044525413
к/сч № 30101810745250000413 в ГУ Банка России по
Центральному федеральному округу
Заместитель Председателя правления
«Нацинвестпромбанк» (АО)

(подпись) Ф.И.О.

Клиент

(подпись) Ф.И.О.

М.П.

(подпись) Ф.И.О.

М.П.

**СЕРТИФИКАТ КЛЮЧА ПРОВЕРКИ ЭЛЕКТРОННОЙ ПОДПИСИ СОТРУДНИКА КЛИЕНТА
В СИСТЕМЕ "iBank"
"Нацинвестпромбанк" (АО)**

1. Наименование организации _____
2. Место нахождения юр. лица _____
3. ОГРН _____ дата внесения в ЕГРЮЛ (ЕГРИП) «___» _____ года
4. Тел. _____ 5. ИНН (КИО) _____ 6. КПП _____
7. Факс _____ 8. E-mail _____
9. Сведения о Владельце ключа
Фамилия, имя, отчество _____
Должность _____
Документ, удостоверяющий личность _____
серия _____ номер _____ дата выдачи «___» _____ года
кем выдан _____
10. Примечания* _____
*не обязательно для заполнения

Настоящим подтверждаю согласие на обработку банком моих персональных данных _____

Ключ проверки ЭП сотрудника клиента (создан _____) подпись

Идентификатор ключа проверки ЭП _____ Идентификатор устройства _____

Наименование криптосредств _____

Алгоритм _____ ID набора параметров алгоритма _____

Представление ключа проверки ЭП в шестнадцатеричном виде

XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX
XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX
XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX
XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX

Личная подпись владельца ключа проверки ЭП

Срок действия (заполняется банком)

с «___» _____ 20__ г.

по «___» _____ 20__ г.

Сертификат ключа проверки ЭП сотрудника клиента действует в рамках Договора дистанционного банковского обслуживания б/н от "___" _____ 20__ г.

Достоверность приведенных данных подтверждаю

Руководитель организации

(указать в соответствии с должностью сотрудника)

_____/_____
подпись / Ф.И.О.

М.П.

Заместитель Председателя правления

_____/_____
подпись / Ф.И.О.

М.П.

Дата приема сертификата

Ключа проверки ЭП

"___" _____ 20__ г.

Сотрудник Управления ИТ

_____/_____
подпись / Ф.И.О.

Дата регистрации сертификата

Ключа проверки ЭП

"___" _____ 20__ г.

в «Нацинвестпромбанк» (АО)

**Заявление
на фильтрацию IP-адреса, с которых осуществляется работа
с системой «Клиент-Банк»**

«___» _____ г.

Настоящим _____,
полное или сокращенное официальное наименование организации; Ф. И.О. индивидуального предпринимателя или

физического лица, занимающегося в установленном законодательством Российской Федерации порядке частной
практикой

ИНН _____ (далее – Клиент), заключивший с «Нацинвестпромбанк» (АО) (далее – Банк) с Договором
ДБО на основании Заявления о присоединении к Договору ДБО от «___» _____ 202_ г., просит Банк осуществлять
доступ Клиента (его Представителей) к Системе Клиент-Банк только со следующих IP – адресов:

--	--	--	--	--	--	--	--	--	--

--	--	--	--	--	--	--	--	--	--

--	--	--	--	--	--	--	--	--	--

Настоящее Заявление просим считать неотъемлемой частью Договора ДБО.

Подпись уполномоченного сотрудника Банка: _____
(подпись) Ф.И.О.

Банк

119121, г. Москва, 2-й Неопалимовский пер., д.10
БИК 044525413
к/сч № 30101810745250000413 в ГУ Банка России по Центральному
федеральному округу

Заместитель Председателя правления

«Нацинвестпромбанк» (АО)

Клиент

(подпись) Ф.И.О.

М.П.

(подпись) Ф.И.О.

М.П.

в «Нацинвестпромбанк» (АО)

**Заявление
на отказ от фильтрации IP-адреса, с которых осуществляется работа
с системой «Клиент-Банк»**

«___» _____ г.

Настоящим _____,
полное или сокращенное официальное наименование организации; Ф. И.О. индивидуального предпринимателя или

физического лица, занимающегося в установленном законодательством Российской Федерации порядке частной
практикой
ИНН _____ (далее – Клиент), заключивший с «Нацинвестпромбанк» (АО) (далее – Банк) с Договором
ДБО на основании Заявления о присоединении к Договору ДБО от «___» _____ 202__ г., просит Банк не
осуществлять контроль IP-адресов компьютеров, с которых от имени Клиента производится доступ к Системе «Клиент-
Банк».

Настоящее Заявление просим считать неотъемлемой частью Договора ДБО.

Подпись уполномоченного сотрудника Банка: _____
(подпись) Ф.И.О.

Банк
119121, г. Москва, 2-й Неопалимовский пер., д.10
БИК 044525413
к/сч № 30101810745250000413 в ГУ Банка России по Центральному
федеральному округу
Заместитель Председателя правления
«Нацинвестпромбанк» (АО)

Клиент

(подпись) Ф.И.О.

М.П.

(подпись) Ф.И.О.

М.П.

SMS-сервис с получением одноразовых паролей

«___» _____ г.

1. Банк обязуется передавать Клиенту одноразовые пароли (SMS-сообщения) для авторизации в Системе «Клиент-Банк», в следующих случаях:

регистрация Клиента в Системе «Клиент-Банк»:

передаче Клиентом платежного поручения на сумму свыше

(_____) рублей.

2. Банк обязуется подключить дополнительные функции SMS-сервиса:

не требовать подтверждения бюджетных платежей;

разрешить групповое подтверждение;

разрешить добавлять получателей в список доверенных получателей.

Данные функции доступны только при подключении п.1.

3. Клиент обеспечивает техническую возможность приема SMS-сообщений на следующие номера мобильных телефонов:

Номер телефона										Ф.И.О. владельца ключей ЭП Клиента

4. Оплата осуществляется в соответствии с действующими Тарифами.

5. Банк не несет ответственности за задержки и сбои, возникающие в сетях сотовых операторов и сервисах провайдеров, которые могут повлечь за собой задержки или недоставку SMS-сообщений Клиенту.

Банк

119121, г. Москва, 2-й Неопалимовский пер., д.10
БИК 044525413
к/сч № 30101810745250000413 в ГУ Банка России по
Центральному федеральному округу

Заместитель Председателя правления

«Нацинвестпромбанк» (АО)

Клиент

(подпись)

Ф.И.О.

М.П.

(подпись)

Ф.И.О.

М.П.

MAC-токен с получением одноразовых паролей

«___» _____ г.

1. Банк обязуется передавать Клиенту одноразовые пароли для авторизации в Системе «Клиент-Банк» с использованием MAC-токенов, в следующих случаях:

- регистрации Клиента в Системе «Клиент-Банк»;
- передаче Клиентом платежного поручения на сумму свыше _____ рублей.

2. Банк обязуется подключить дополнительные функции:

- не требовать подтверждения бюджетных платежей;
- разрешить добавлять получателей в список доверенных получателей.

2. Оплата осуществляется в соответствии с действующими Тарифами.

Банк

119121, г. Москва, 2-й Неопалимовский пер., д.10
БИК 044525413
к/сч № 30101810745250000413 в ГУ Банка России по
Центральному федеральному округу

Заместитель Председателя правления

«Нацинвестпромбанк» (АО)

Клиент

(подпись) Ф.И.О.
М.П.

(подпись) Ф.И.О.
М.П.

ЗАЯВЛЕНИЕ
на установку, настройку личного кабинета Системы «Клиент-Банк» специалистом Банка

Клиент _____
полное или сокращенное официальное наименование организации; Ф. И.О. индивидуального предпринимателя или
физического лица, занимающегося в установленном законодательством Российской Федерации порядке частной практикой
в лице _____,
действующего на основании _____ в соответствии с Договором ДБО на основании Заявления о
присоединении к ДБО от «___» _____ 202__ г. просит произвести установку и настройку Системы «Клиент-Банк» на
компьютере Клиента специалистом Банка:

на территории Центрального офиса Банка, по адресу: г. Москва, 2-ой Неопалимовский переулок, д. 10;

на территории Клиента по адресу: _____
(фактический адрес)

Контактное лицо _____
(должность, ФИО)

Контактный телефон _____

Предпочтительная дата и время выезда специалиста Банка _____

Комиссию за услуги списать с нашего расчетного счета в Банке в соответствии с действующими Тарифами.

КЛИЕНТ

_____/_____/

М.П.

«___» _____ 202__ г.

Заполняется сотрудником Банка

Принято:

«___» _____ 202__ г.

Подпись

Ф.И.О.

ЗАЯВЛЕНИЕ
на установление лимитов операций с использованием Системы «Клиент-Банк»

Клиент _____
полное или сокращенное официальное наименование организации; Ф. И.О. индивидуального предпринимателя или
физического лица, занимающегося в установленном законодательством Российской Федерации порядке частной практикой
в лице _____,

действующего на основании _____ в соответствии с Договором ДБО на основании Заявления о
присоединении к Договору ДБО от «___» _____ 202__ г. просит:

установить лимиты операций с использованием Системы

Лимит одного платежа, рублей	
Дневной лимит платежей, рублей	
Месячный лимит платежей, рублей	

(должность руководителя)

(подпись)

(фамилия, инициалы)

М.П.

Заполняется сотрудником Банка

Принято:

«___» _____ 202__ г.

Подпись

Ф.И.О.

Информация для подключения к Информационной системе «Одно окно»

В рамках Договора дистанционного банковского обслуживания с «Нацинвестпромбанком» (АО) от _____ прошу предоставить доступ к Информационной системе «Одно окно» для внешнеэкономической деятельности.

Номер телефона для получения уведомлений в рамках ИС «Одно окно»: +7 (XXX) XXX-XX-XX.