

Утверждено Правлением ПАО КБ «РусЮгбанк»  
Протокол № 11-04/63в от «21» апреля 2017 г.

Действует с 02.05.2017 г.

в редакции с учетом изменений: от 12.07.2017 г. протокол Правления ПАО КБ «РусЮгбанк» № 11-04/115 от 12.07.2017 г.

в редакции с учетом изменений: от 29.05.2018 г. протокол Правления ПАО КБ «РусЮгбанк» № 11-04/85 от 29.05.2018 г.

в редакции с учетом изменений: от 13.06.2018 г. протокол Правления АО Банка «Национальный стандарт» № 205 от 22.05.2018 г.

**Регламент системы дистанционного банковского обслуживания  
«Банк-клиент»**

г. Москва, 2018 г.

## Оглавление

1. Определения.....	3
2. Общие положения. ....	6
3. Порядок вступления в действие и внесения изменений в Регламент.....	6
4. Порядок и особенности организации технического доступа к Системе. Обеспечение информационной безопасности работы в Системе. ....	7
5. Порядок осуществления обмена электронными документами. ....	9
6. Порядок взаимодействия сторон в случае компрометации закрытого ключа и (или) использования электронного средства платежа без согласия клиента.....	16
7. Прочие условия.....	18
8. Права и обязанности сторон.....	19
9. Порядок расчетов.....	22
10. Ответственность.....	22
11. Порядок разрешения конфликтных ситуаций и споров.....	23
12. Срок действия договора и порядок его расторжения.....	26

## 1. Определения.

**АБС** — автоматизированная система Банка, используемая для обработки ЭД Клиента.

**Автоматизированная система подтверждения платежей Банка** - автоматизированная система, часть системы Fraud-мониторинга, предназначенная для связи с уполномоченными лицами Клиента и проверки легитимности принятых по системе «Банк-Клиент» платежей, определенных системой Fraud-мониторинга к группе подозрительных платежей.

**Банк** — Акционерное общество Банк «Национальный стандарт» (сокращенное наименование — АО Банк «Национальный стандарт»).

**Безотзывность Платежного ЭД** — характеристика Платежного ЭД, обозначающая отсутствие или прекращение возможности отзыва Клиентом Платежного ЭД в определенный момент времени. Безотзывность Платежного ЭД наступает в момент списания денежных средств со Счета Клиента в соответствии с условиями, изложенными в заключенных с Клиентом договорах банковского счета, банковского вклада (депозита), в том числе заключаемых в рамках Соглашений/Генеральных соглашений об общих условиях привлечения денежных средств (далее по тексту по отдельности - Договор Счета или Договор Депозита, а в совокупности – Договор Счета/Депозита).

**Гибернация** — энергосберегающий режим операционной системы компьютера, позволяющий сохранять содержимое оперативной памяти на энергонезависимое устройство хранения данных (жёсткий диск или твердотельный накопитель) перед выключением питания.

**Закрытый ключ** — совмещенный ключ электронной подписи и шифрования, состоящий из последовательности символов, известной Уполномоченному лицу Стороны, Стороне и предназначенной для создания ЭП ЭД с использованием Средств ЭП и расшифровывания ЭД.

**Защищенный носитель** — Ключевой носитель «Рутокен ЭЦП» или «Рутокен ЭЦП 2.0», являющийся одновременно и Ключевым носителем, и аппаратным СКЗИ.

**Карточка с образцами подписей** — банковская карточка с образцами подписей и оттиска печати Клиента.

**Клиент** — юридическое лицо, индивидуальный предприниматель или физическое лицо, занимающееся в установленном законодательством Российской Федерации порядке частной практикой, присоединившееся к Регламенту.

**Клиентская часть системы** — часть Системы, используемая Клиентом для обмена ЭД с Банком.

**Ключевой носитель** — информационный (материальный) носитель, на который могут быть записаны Криптографические ключи. В Системе допускается использование только Ключевых носителей, совместимых со СКЗИ, разрешенных к использованию в Системе.

**Компрометация Закрытого ключа** — нарушение конфиденциальности Закрытого ключа, констатация Уполномоченным лицом Стороны, Стороной обстоятельств или наступление обстоятельств, при которых возможно несанкционированное использование Закрытого ключа неуполномоченными лицами. Утрата ЭСП, использование ЭСП без согласия Клиента являются частными случаями Компрометации Закрытого ключа.

**Криптографические ключи** — общее название Открытых и Закрытых ключей.

**Неплатежный ЭД** — любой ЭД, не представляющий собой распоряжение Клиента на совершение операции по Счету, содержащий все реквизиты, предусмотренные действующим законодательством Российской Федерации, нормативными актами Банка России и установленными Банком правилами. Неплатежный документ может содержать как документы, сформированные в электронном виде, так и полученные с использованием сканирующих устройств изображения документов, оформленных первоначально на бумажном носителе.

**Ограниченный доступ в Систему** — доступ к Счету на просмотр получаемой из Банка информации, запрос выписки, создание электронного сообщения, прием электронного документа.

**Открытый ключ** — совмещенный ключ проверки электронной подписи и открытый ключ шифрования, состоящий из последовательности символов, соответствующей совмещенному ключу электронной подписи и шифрования и предназначенной для Проверки ЭП ЭД и зашифровывания ЭД.

**Офис банка** — подразделение Банка, в котором осуществляется обслуживание Счета Клиента.

**Платежный ЭД** — ЭД, представляющий собой распоряжение Клиента на совершение операций по Счету, содержащий все предусмотренные законодательством Российской Федерации реквизиты.

**Подозрительная операция** — сомнительная операция, по которой, в результате реализации мер внутреннего контроля, у Банка возникает подозрение в том, что такая операция осуществляется в целях легализации (отмывания) доходов, полученных преступным путём, или финансирования терроризма.

**Подтверждение подлинности Электронной подписи в Электронном документе (Проверка ЭП в ЭД)** — положительный результат проверки принадлежности ЭП в ЭД Уполномоченному лицу Стороны, Стороне и отсутствия искажений в данном ЭД. Проверка ЭП в ЭД должна осуществляться соответствующим Средством ЭП с использованием Открытого ключа.

**Рабочее время Службы информационной поддержки клиентов** — рабочие будние дни (с понедельника по пятницу) с 8:30 до 19:00 по Московскому времени, суббота — с 8:30 до 16:00 по Московскому времени.

**Рабочее время Службы технической поддержки клиентов** — рабочие будние дни (с понедельника по четверг) с 8:30 до 17:30 по Московскому времени, пятница и предпраздничные дни — с 8:30 до 16:30 по Московскому времени.

**Регистрация открытого ключа** — внесение в Часть системы на стороне банка Открытого ключа Уполномоченного лица Клиента, используемого для подтверждения подлинности ЭП, идентификации Уполномоченного лица Клиента и зашифрования ЭД.

**Регламент** — настоящий регламент системы дистанционного банковского обслуживания «Банк-клиент», утвержденный Правлением Банка и содержащий условия оказания услуг по дистанционному банковскому обслуживанию «Банк-клиент», требования к техническому и информационному обеспечению процессов формирования, обработки и хранения ЭД. Регламент в соответствии со статьей 428 Гражданского кодекса Российской Федерации является договором присоединения (далее по тексту также — *Договор*).

**Сайт Банка** — официальный сайт Банка в сети Интернет по адресу [www.ns-bank.ru](http://www.ns-bank.ru).

**Система дистанционного банковского обслуживания «Банк-клиент» Банка (Система)** — система, представляющая собой совокупность программного, информационного и аппаратного обеспечения, включая программный комплекс, состоящий из средств формирования, обработки, хранения, передачи ЭД, реализующая обмен ЭД между Клиентом и Банком в соответствии с Регламентом. Система состоит из Клиентской части системы и Части системы на стороне банка.

**Система Fraud-мониторинга** – автоматизированная система контроля и выявления подозрительных и/или мошеннических платежей в системе «Банк-клиент».

**Служба информационной поддержки клиентов** — подразделение Банка, позволяющее Клиенту обратиться по Телефону Службы информационной поддержки клиентов в Рабочее время Службы информационной поддержки клиентов в случае Компрометации закрытого ключа и (или) использования Электронного средства платежа без согласия Клиента.

**Служба технической поддержки клиентов** — подразделение Банка, позволяющее Клиенту обратиться по Телефонам Службы технической поддержки клиентов в Рабочее время Службы технической поддержки клиентов за получением консультаций и иной помощи при возникновении вопросов при использовании Системы.

**Соглашение** — Соглашение о присоединении к системе дистанционного банковского обслуживания «Банк-клиент».

**Сомнительная операция** — это операция, осуществляемая Клиентом, имеющая необычный характер и признаки отсутствия явного экономического смысла и очевидных законных целей, которая может проводиться для вывода капитала из страны, финансирования "серого" импорта, перевода денежных средств из безналичной в наличную форму и последующего ухода от налогообложения, а также для финансовой поддержки коррупции и других противозаконных целей; операция, относящаяся к отдельным видам операций, в отношении которых Банком России даны рекомендации о повышении к ним внимания кредитными организациями, а также любая иная операция, которая, по мнению Банка, может осуществляться с целью отмывания доходов, полученных преступным путем, и/или финансирования терроризма.

**Средства криптографической защиты информации (СКЗИ)** — аппаратные и (или) программные средства, обеспечивающие применение ЭП и шифрования при организации обмена ЭД. В Системе

допускается использование только средств криптографической защиты информации, разрешённых к использованию Банком и приведенных в Приложении № 3 к Регламенту.

**Средства электронной подписи (Средства ЭП)** — аппаратные и (или) программные средства, являющиеся частью средств криптографической защиты информации и реализующие хотя бы одну из следующих функций при организации обмена ЭД: создание ЭП в ЭД с использованием Закрытого ключа; Подтверждение подлинности ЭП, содержащейся в ЭД, с использованием Открытого ключа; создание Закрытого и Открытого ключа.

**Сторона** — Клиент или Банк.

**Счет** — банковский счет, открытый Клиенту Банком в соответствии с Договором Счета/Депозита, распоряжение которым Клиент осуществляет, в том числе, посредством Системы. В рамках Системы Клиент может распоряжаться несколькими Счетами, подключенными к Системе.

**Тарифы** — Сборник тарифов на услуги Банка для юридических лиц, индивидуальных предпринимателей и физических лиц, занимающихся в установленном законодательством Российской Федерации порядке частной практикой, утверждаемый Правлением Банка и размещаемый в помещениях Банка в общедоступном месте и на Сайте Банка. Тарифы являются неотъемлемой частью Регламента.

**Телефон Службы информационной поддержки клиентов** — 8-800-250-33-00.

**Телефоны Службы технической поддержки клиентов** — 8 (495) 725-59-53, 8 (8442) 99-50-32, 8 (8443) 24-10-52, 8 (84457) 2-33-15, 8-800-250-33-00.

**Уполномоченное лицо Банка** — работник Банка, уполномоченный от имени Банка взаимодействовать с Клиентом в рамках Системы, в том числе вести переписку, отправлять документы, а также осуществлять иные полномочия.

**Уполномоченное лицо Клиента** — лицо, наделенное правом подписания расчетных документов по распоряжению денежными средствами на Счете (-ах) (правом подписания распоряжений об осуществлении перевода денежных средств) и создания Неплатежных ЭД, либо обладающее только Ограниченными правами доступа в Систему, действующее в соответствии с учредительными документами Клиента или на основании доверенности и имеющее доступ к Счету (-ам) согласно Заявления на распоряжение по счету/изменение прав доступа уполномоченного лица клиента в системе дистанционного банковского обслуживания «Банк-клиент» (Приложение № 2 к Регламенту) или Заявления на предоставление/изменение прав ограниченного доступа уполномоченного лица клиента в систему дистанционного банковского обслуживания «Банк-клиент» (Приложение № 2а к Регламенту).

**Уполномоченное лицо Клиента на подтверждение платежей** — лицо, наделенное правом подтверждать платежи, принятые по системе «Банк-Клиент» и определенные системой Fraud-мониторинга к группе подозрительных платежей, посредством автоматизированной системы подтверждения платежей Банка.

**Усиленная неквалифицированная электронная подпись (Электронная подпись, ЭП)** — реквизит ЭД, предназначенный для защиты ЭД от подделки, полученный в результате криптографического преобразования информации с использованием Закрытого ключа и позволяющий идентифицировать Уполномоченное лицо Стороны, Сторону, а также установить отсутствие утраты, добавления, перестановки или искажения содержащейся в ЭД информации.

**Часть системы на стороне банка** — часть Системы, используемая Банком для обмена ЭД с Клиентом.

**Шифрование** — криптографическое преобразование данных, позволяющее предотвратить доступ неуполномоченных лиц к содержимому зашифрованного ЭД.

**Электронное сообщение (ЭС)** — логически целостная совокупность структурированных данных, имеющих смысл для Сторон. Информация в ЭС представлена в электронно-цифровой форме, позволяющей обеспечить ее обработку средствами вычислительной техники, передачу по каналам связи и хранение на машиночитаемых носителях информации.

**Электронное средство платежа (ЭСП)** — Электронное устройство, Ключевой носитель, Криптографические ключи Уполномоченного лица Клиента в совокупности, позволяющие Уполномоченному лицу Клиента в рамках Системы составлять, удостоверять и передавать распоряжения в целях осуществления перевода денежных средств в соответствии с Договором Счета/Депозита.

**Электронное устройство (ЭУ)** — персональный компьютер, ноутбук и иное рабочее место, используемое Уполномоченным лицом Клиента для дистанционного управления Счетом в рамках Системы.

**Электронный документ (ЭД)** — ЭС, заверенное ЭП. ЭД может быть преобразован в форму, пригодную для однозначного восприятия его содержания.

## **2. Общие положения.**

- 2.1. Регламент устанавливает порядок организации обмена ЭД между Клиентом и Банком в рамках Системы. Присоединение к Регламенту и подключение Клиента к Системе осуществляется путем подписания между Клиентом и Банком Соглашения по форме Приложения № 9 к Регламенту.
- 2.2. Присоединение Клиента к Регламенту означает безусловное и добровольное принятие Клиентом Регламента в целом.
- 2.3. Положения настоящего Регламента применяются, если иное не предусмотрено законодательными или иными правовыми актами Российской Федерации, включая нормативные акты Банка России. При исполнении Договора Счета/Депозита положения настоящего Регламента применяются в той мере, в которой они не противоречат условиям данных договоров.
- 2.4. Стороны признают, что:
  - 2.4.1. получение ЭД, подписанного ЭП другой Стороны, Уполномоченного лица другой Стороны юридически эквивалентно получению Стороной документа на бумажном носителе, заверенного собственноручными подписями Уполномоченных лиц другой Стороны и оттиском печати другой Стороны; ЭД, подписанный ЭП другой Стороны, Уполномоченного лица другой Стороны юридически эквивалентен документу на бумажном носителе, заверенному собственноручными подписями Уполномоченных лиц другой Стороны и оттиском печати Стороны. Обязательства, предусмотренные настоящим пунктом, действительны при условии создания Закрытого ключа, ЭП и Открытого ключа в соответствии с настоящим Регламентом;
  - 2.4.2. используемые в Системе способы защиты информации, которые обеспечивают формирование и проверку ЭП, достаточны для подтверждения авторства и подлинности ЭД;
  - 2.4.3. подделка ЭП, то есть создание корректной ЭП ЭД, невозможна без знания Закрытого ключа Стороны (доступа к Закрытому ключу Стороны);
  - 2.4.4. ЭП ЭД является аналогом собственноручной подписи Уполномоченного лица Стороны.
  - 2.4.5. Заявления, оформленные Клиентом в рамках действия настоящего Регламента до 30 мая 2016 года, распространяются на взаимоотношения Сторон в Системе в целом, вне зависимости от реквизитов Договора Счета/Депозита, указанных в соответствующих заявлениях.
  - 2.4.6. ЭД являются легитимными и подлежат исполнению Банком при выполнении одновременно следующих условий:
    - полученные ЭД оформлены надлежащим образом и подписаны необходимыми ЭП уполномоченных лиц Клиента,
    - подтверждены уполномоченным лицом Клиента по автоматизированной системе подтверждения платежей Банка в случае, если ЭД определены системой Fraud-мониторинга как подозрительные.

## **3. Порядок вступления в действие и внесения изменений в Регламент.**

- 3.1. Регламент может быть изменен по инициативе Банка в одностороннем порядке путем утверждения новой редакции Регламента в порядке, установленном настоящим разделом Регламента.

- 3.2. В случае изменения законодательства Российской Федерации Регламент до момента его изменения Банком применяется в части, не противоречащей требованиям законодательства Российской Федерации.
- 3.3. Новая редакция Регламента утверждается Правлением Банка и вступает в силу в сроки, определяемые Правлением Банка.
- 3.4. Действующая редакция Регламента размещается на Сайте Банка.
- 3.5. Новая редакция Регламента, а также информация о сроках вступления его в силу доводится Банком до сведения Клиентов посредством уведомления. Уведомление осуществляется путем размещения новой редакции Регламента на Сайте Банка либо иным способом извещения в соответствии с п.7.5 Регламента, обеспечивающим возможность получения Клиентом указанных изменений.
- 3.6. В случае несогласия Клиента с условиями новой редакции Регламента Клиент вправе расторгнуть Договор в порядке, предусмотренном разделом 12 Регламента.
- 3.7. С момента вступления в силу новой редакции Регламента Стороны при работе в Системе руководствуются новой редакцией Регламента. Начало работы Клиента на условиях, предусмотренных новой редакцией Регламента со дня вступления их в силу автоматически означает полное согласие с условиями, а также принятие всех обязательств, предусмотренных Регламентом.
- 3.8. Банк не несет ответственности, если информация об утверждении новой редакции Регламента, опубликованная в порядке и в сроки, установленные Регламентом, не была получена и/или изучена, и/или правильно истолкована Клиентом.

#### **4. Порядок и особенности организации технического доступа к Системе. Обеспечение информационной безопасности работы в Системе.**

- 4.1. Банк до заключения Договора информирует Клиента об условиях использования ЭСП путем размещения соответствующей информации на Сайте Банка.
- 4.2. Клиент до подключения к Системе обязан оценить риски, связанные с использованием Системы, в соответствии с п.7.1 и других положений настоящего Регламента, размещаемого на Сайте Банка, и, основываясь на проведенной оценке рисков, принять решение об использовании Системы или отказе от работы с ней.
- 4.3. Клиент до подключения к Системе, а затем на постоянной основе обязан обеспечить выполнение следующих требований информационной безопасности при использовании Системы:
  - 4.3.1. Ключевой носитель использовать только Уполномоченным лицом Клиента, которому принадлежит Закрытый ключ, содержащийся на данном Ключевом носителе;
  - 4.3.2. не передавать Ключевой носитель одного Уполномоченного лица другому Уполномоченному лицу Клиента и иным лицам;
  - 4.3.3. хранить Ключевые носители отдельно, в защищенном от несанкционированного доступа месте;
  - 4.3.4. не устанавливать Ключевые носители в компьютеры, ноутбуки и иные устройства, не используемые для работы в Системе;
  - 4.3.5. не оставлять Ключевые носители установленными в ЭУ после завершения сеанса работы в Системе;
  - 4.3.6. не размещать Закрытый ключ на жестком диске, в сетевом каталоге и прочих совместно используемых ресурсах;
  - 4.3.7. использовать ЭУ в помещениях с малой проходимостью или ограниченным доступом во избежание хищения Ключевых носителей, используемых для работы с Системой;

- 4.3.8. размещать ЭУ способом, не позволяющим производить визуальное наблюдение за экраном ЭУ и его клавиатурой, в том числе посредством системы видеонаблюдения и через оконные проемы;
- 4.3.9. использовать ЭУ с установленной лицензионной операционной системой;
- 4.3.10. незамедлительно после публикации обновлений — обновлять операционную систему (устанавливать критичные обновления и обновления безопасности) и иное программное обеспечение, установленное на ЭУ;
- 4.3.11. не использовать установленные на ЭУ операционную систему и иное программное обеспечение, для которых прекращен предусмотренный разработчиком выпуск обновлений безопасности;
- 4.3.12. использовать ЭУ с установленным лицензионным антивирусным программным обеспечением;
- 4.3.13. производить проверку наличия обновлений антивирусных баз у разработчика антивирусного программного обеспечения не реже раза в сутки и в случае наличия обновлений производить их своевременное обновление;
- 4.3.14. не использовать установленное на ЭУ антивирусное программное обеспечение, для которого прекращен выпуск обновлений антивирусных баз;
- 4.3.15. производить не реже раза в неделю полное антивирусное сканирование машинных носителей информации ЭУ;
- 4.3.16. осуществлять работу на ЭУ с использованием учетной записи с ограниченными правами, доступ к учетной записи с полными правами (администратора) защищать надежным паролем;
- 4.3.17. устанавливать длинные и сложные пароли для доступа к Клиентской части системы, а при необходимости и пароли для доступа к Закрытому ключу, содержащие не менее 8 символов, в числе которых обязательны буквы в верхнем и нижнем регистре (например, «Q» и «q»), цифры и спецсимволы (например, !;%:\*?\*)\_+ и т.п.);
- 4.3.18. производить регулярную смену паролей не реже одного раза в месяц;
- 4.3.19. максимально ограничить работу с отчуждаемыми носителями информации (флэш-накопители, дискеты, диски и т.п.) за исключением Ключевых носителей, перед использованием первых осуществлять их полное сканирование антивирусным программным обеспечением на наличие вредоносного кода.
- 4.3.20. Обязательным условием допуска для работы в Системе Уполномоченного лица Клиента, наделенного правом подписания расчетных документов по распоряжению денежными средствами на Счете(-ах) (правом подписания распоряжений об осуществлении перевода денежных средств) и создания Платежных ЭД, является предоставление Банку его номера(-ов) телефона(-ов), а также номера(-ов) телефона(-ов) и ФИО лица(лиц) Клиента уполномоченного(-ых) на подтверждение платежей для направления и запроса информации по вопросам использования Системы и обработки ЭД, в том числе посредством автоматизированной системы подтверждения платежей Банка. Указанные сведения предоставляются в форме Неплатежного ЭД или Приложения № 2 к настоящему Регламенту.

Уполномоченное лицо Клиента, наделенное правом подписания расчетных документов по распоряжению денежными средствами на Счете(-ах) (правом подписания распоряжений об осуществлении перевода денежных средств) и создания Платежных ЭД обязано незамедлительно направлять в Банк новые номера телефонов и ФИО лица(лиц) Клиента уполномоченного(-ых) на подтверждение платежей в случае их изменения.

- 4.4. Для существенного повышения безопасности работы в Системе Клиенту предлагается обеспечить выполнение следующих рекомендаций информационной безопасности при использовании Системы на постоянной основе:
  - 4.4.1. настроить сетевое оборудование, обеспечивающее доступ Клиента в сеть, или специализированное программное обеспечение (брандмауэр, прокси-сервер и т.п.) на блокировку сетевых пакетов, передаваемых с ЭУ, применяемого для работы в



Системе, на любые адреса, не относящиеся к Системе, системе доменных имён (Domain Name System), DHCP-серверу, службе каталогов (Active Directory и т.п.) и службам синхронизации времени, обновления установленного программного обеспечения, операционной системы и антивирусных баз;

- 4.4.2. настроить аудит событий, регистрирующий возникающие ошибки работы операционной системы и приложений, вход пользователей и запуск программ, периодически просматривать журналы аудита, реагировать на ошибки и попытки несанкционированного доступа;
  - 4.4.3. ЭУ, применяемые для работы в Системе, не использовать в других целях, в том числе рабочих;
  - 4.4.4. использовать возможности информирования по электронной почте о расходных операциях по Счету;
  - 4.4.5. использовать возможности дополнительной услуги SMS-информирования;
  - 4.4.6. следовать иным рекомендациям информационной безопасности, размещенным на Сайте Банка.
- 4.5. Об ошибках в работе Системы Клиенту необходимо уведомлять Службу технической поддержки клиентов.
- 4.6. Клиент для работы с Системой обязан использовать только технически исправное ЭУ.
- 4.7. Требования и рекомендации по настройке ЭУ Клиента для работы в Системе приведены в Приложении №3 к Регламенту. Клиенту запрещается использовать для работы с Системой ЭУ, не настроенное в соответствии с настоящим Регламентом.

## **5. Порядок осуществления обмена электронными документами.**

- 5.1. Условия допуска к осуществлению обмена электронными документами в системе.
- 5.1.1. Клиенту – юридическому лицу для дистанционного управления в Системе может быть подключен Счет Клиента, открытый на счетах первого порядка: 405-407, 414-422; счетах второго порядка 40807, 40821.
  - 5.1.2. Клиенту – юридическому лицу дополнительно для дистанционного просмотра движения и остатков на Счете, запроса выписки по Счету в Системе могут быть подключены Счета Клиента, открытые на счетах второго порядка 45201-45208, и иных счетах по усмотрению Сторон.
  - 5.1.3. Клиенту – индивидуальному предпринимателю или физическому лицу, занимающемуся в установленном законодательством Российской Федерации порядке частной практикой, для дистанционного управления в Системе может быть подключен Счет Клиента, открытый на счете первого порядка 421; на счетах второго порядка: 40802, 40807, 40821, 42309.
  - 5.1.4. Клиенту – индивидуальному предпринимателю или физическому лицу, занимающемуся в установленном законодательством Российской Федерации порядке частной практикой, дополнительно для дистанционного просмотра движения и остатков на Счете, запроса выписки по Счету в Системе могут быть подключены Счета Клиента, открытые на счетах первого порядка: 423, 426, счетах второго порядка: 40817, 40820, 45401-45408, и иных счетах по усмотрению Сторон.
  - 5.1.5. Регистрация открытого ключа может быть произведена на имя Уполномоченного лица Клиента, непосредственно использующего Закрытый ключ.
  - 5.1.6. Право подписи ЭС может принадлежать:
    - клиенту – индивидуальному предпринимателю, физическому лицу, занимающемуся в установленном законодательством Российской Федерации порядке частной практикой;
    - физическим лицам на основании соответствующей доверенности, выданной в случаях и в порядке, установленных законодательством Российской Федерации, индивидуальным предпринимателем, физическим лицом, занимающимся в

установленном законодательством Российской Федерации порядке частной практикой;

- единоличному исполнительному органу клиента-юридического лица;
- иным сотрудникам (работникам), наделенным правом подписи клиентом – юридическим лицом, в том числе на основании доверенности. **Право подписи может принадлежать только сотрудникам (работникам) клиента - юридического лица.**

5.1.6.1. Единоличный исполнительный орган Клиента-юридического лица, индивидуальный предприниматель, могут не указываться в карточке в качестве лиц, наделенных правом подписи, при условии наделения правом подписи иных лиц.

5.1.6.2. Уставом корпорации<sup>1</sup> может быть предусмотрено предоставление полномочий единоличного исполнительного органа нескольким лицам, действующим совместно, или образование нескольких единоличных исполнительных органов, действующих независимо друг от друга. В указанных случаях должен быть установлен единоличный исполнительный орган корпорации, уполномоченный открывать/закрывать в кредитных организациях банковские счета, распоряжаться денежными средствами организации, выдавать доверенности на распоряжение денежными средствами сотрудникам юридического лица.

5.1.6.3. Доверенность от имени Клиента - юридического лица выдается в порядке, установленном законодательством Российской Федерации. Доверенности Клиентов - индивидуальных предпринимателей и лиц, занимающихся в установленном законодательством Российской Федерации порядке частной практикой, должны быть удостоверены нотариально.

5.1.6.4. Предоставляемые Банку доверенности должны содержать полномочия лиц на распоряжение денежными средствами и подписание Неплатежных ЭД с использованием ЭП.

5.1.7. Уполномоченному лицу Клиента, не наделенному правом подписи, может быть предоставлен только Ограниченный доступ в Систему, согласно Заявления на предоставление/изменение прав ограниченного доступа уполномоченного лица клиента в системе дистанционного банковского обслуживания «Банк-клиент» (Приложение №2а к Регламенту) на основании доверенности. При этом указанному лицу не может быть предоставлено право доступа на подписание ЭС и отправку ЭД. Для хранения Криптографических ключей в этом случае может использоваться Ключевой носитель, не являющийся Защищенным носителем.

5.1.8. Права доступа Уполномоченного лица Клиента могут быть дополнительно сокращены при наличии технической возможности по заявлению Клиента, оформленному в свободной форме.

5.1.9. К исполнению принимаются Платежные и Неплатежные ЭД при наличии одной ЭП любого Уполномоченного лица Клиента, обладающего правом подписи, действующего в соответствии с учредительными документами Клиента или на основании доверенности и имеющего доступ к Счету (-ам) согласно Заявления на распоряжение по счету/изменение прав доступа уполномоченного лица клиента в системе дистанционного банковского обслуживания «Банк-клиент» (Приложение №2 к Регламенту).

---

<sup>1</sup> Юридические лица, учредители (участники) которых обладают правом участия (членства) в них и формируют их высший орган в соответствии с пунктом 1 статьи 65.3 Гражданского Кодекса Российской Федерации, являются корпоративными юридическими лицами (корпорациями). К ним относятся хозяйственные товарищества и общества, крестьянские (фермерские) хозяйства, хозяйственные партнерства, производственные и потребительские кооперативы, общественные организации, ассоциации (союзы), товарищества собственников недвижимости, казачьи общества, внесенные в государственный реестр казачьих обществ в Российской Федерации, а также общины коренных малочисленных народов Российской Федерации.

- 5.1.10. Закрытый ключ Уполномоченного лица Клиента, по усмотрению Сторон, может использоваться для доступа к Счетам разных Клиентов в случае, если данное лицо является Уполномоченным лицом Клиента для каждого из этих Клиентов. В таком случае в каждом заявлении по форме Приложения №2 или №2а к Регламенту Уполномоченным лицом Клиента должны быть идентично заполнены поля «Ф.И.О. уполномоченного лица Клиента».
- 5.1.11. Если Карточка с образцами подписей оформлена до вступления в силу Инструкции Банка России от 30.05.2014 № 153-И «Об открытии и закрытии банковских счетов, счетов по вкладам (депозитам), депозитных счетов», то:
- Если у Клиента согласно Карточке с образцами подписей не предусмотрены лица, наделенные правом второй подписи, к исполнению принимаются Платежные ЭД при наличии ЭП Уполномоченного лица Клиента с правом первой подписи.
  - Если у Клиента согласно Карточке с образцами подписей предусмотрены лица, наделенные правом первой и второй подписи, к исполнению принимаются Платежные ЭД, подписанные ЭП Уполномоченного лица Клиента с правом первой подписи и ЭП Уполномоченного лица Клиента с правом второй подписи.
  - К исполнению принимаются Неплатежные ЭД, подписанные единственной ЭП Уполномоченного лица Клиента с правом первой или второй подписи.
- 5.1.12. Обязательным условием допуска для работы в Системе Уполномоченного лица Клиента, наделенного правом подписи, является использование им Защищенного носителя.
- 5.1.13. С «01» июля 2018 года все новые Криптографические ключи Системы будут выпускаться по новому криптоалгоритму ГОСТ Р 34.10-2012. Выпуск Криптографических ключей Уполномоченного лица Клиента, наделенного правом подписи, будет осуществляться на следующих защищенных носителях:
- 5.1.13.1. «Рутокен ЭЦП 2.0»;
- 5.1.13.2. «Рутокен ЭЦП», при условии передачи в банк Неплатежного ЭД в соответствии с «Инструкцией по отправке заявления на разрешение выпуска криптографических ключей на Рутокен ЭЦП», размещенной на Сайте Банка. Банк вправе отказать Уполномоченному лицу Клиента в выпуске Криптографических ключей на защищенном носителе «Рутокен ЭЦП» без объяснения причин. В данном случае выпуск Криптографических ключей осуществляется на защищенном носителе «Рутокен ЭЦП 2.0».
- 5.1.14. 01.01.2019 года Криптографические ключи выпущенные по старому криптоалгоритму ГОСТ Р 34.10.2001 будут заблокированы.
- 5.2. Порядок допуска к осуществлению обмена электронными документами в системе.
- 5.2.1. В случае необходимости Клиентом подается «Заявление о направлении дополнительной информации для обеспечения информационной безопасности работы в системе дистанционного банковского обслуживания «Банк-клиент» по форме Приложения №1 к Регламенту, если данные, предоставляемые по указанному заявлению, не предоставлялись ранее или требуют актуализации.
- 5.2.2. Для работы с Системой Клиентом на каждое Уполномоченное лицо Клиента для работы с Системой подается «Заявление на распоряжение по счету/изменение прав доступа уполномоченного лица клиента в системе дистанционного банковского обслуживания «Банк-клиент» по форме Приложения №2 к Регламенту или «Заявление на предоставление/изменение прав ограниченного доступа уполномоченного лица клиента в систему дистанционного банковского обслуживания «Банк-клиент» по форме Приложения №2а к Регламенту, если данные, предоставляемые по указанному заявлению, не предоставлялись ранее или требуют актуализации. При этом для каждого Уполномоченного лица необходимо указать перечень Счетов и прав доступа к ним посредством Системы (указание хотя бы одного Счета обязательно).

- 5.2.3. При подаче заявления в соответствии с п.5.2.2 по Уполномоченному лицу Клиента, не наделенному правом подписи, но обладающему ограниченными правами доступа к Счету в рамках Системы, Клиент должен предоставить доверенность, оформленную в соответствии с требованиями раздела 1 Регламента, о наделении Уполномоченного лица Клиента такими правами, если она не была предоставлена ранее.
- 5.2.4. В случае если Открытый ключ Уполномоченного лица Клиента уже зарегистрирован в Системе, Закрытый ключ, соответствующий данному Открытому ключу, может использоваться Уполномоченным лицом Клиента, на имя которого выпущены Криптографические ключи, при исполнении условий п.5.2.2 Регламента.
- 5.2.5. В случае необходимости для работы в Системе Уполномоченного лица Клиента Клиентом у Банка приобретаются Защищенные носители по цене согласно Тарифам, действующим на день приобретения.
- 5.2.6. Клиентом производится подготовка безопасной работы в Системе в соответствии с требованиями раздела 4 настоящего Регламента, настройка необходимого количества ЭУ в соответствии с «Требованиями и рекомендациями по настройке электронного устройства Клиента для работы в Системе», приведенными в Приложении №3 к Регламенту.
- 5.2.7. Для каждого Уполномоченного лица Клиента Банком организуется процедура установки Клиентской части системы на ЭУ, запись Криптографических ключей на Ключевой носитель, Регистрация открытого ключа в Части системы на стороне банка. Установка Клиентской части системы осуществляется в соответствии с Тарифами Службой технической поддержки либо непосредственно на ЭУ Уполномоченного лица Клиента, либо путем удаленного подключения для управления ЭУ Уполномоченного лица Клиента с использованием технических средств (программного обеспечения), определенных Банком, до начала обмена ЭД.
- 5.2.8. Акт признания ключа проверки электронной подписи и открытого ключа шифрования по форме Приложения №4 к Регламенту на каждого Уполномоченного лица Клиента Клиент заверяет подписью Уполномоченного лица Клиента и печатью Клиента, после чего указанные акты предоставляет в Банк.
- 5.2.9. Не позднее пяти рабочих дней до дня окончания срока действия Открытого ключа Уполномоченного лица Клиента, указанное лицо осуществляет создание на Ключевом носителе Криптографических ключей и направляет запрос на получение Открытого ключа в соответствии с «Инструкцией по перевыпуску криптографических ключей», размещенной на Сайте Банка. Направляемый в электронном виде запрос на получение Открытого ключа подписывается ЭП, сформированной действующим Закрытым ключом Уполномоченного лица Клиента.
- В срок не позднее трех рабочих дней с даты подтверждения запроса, Банк выпускает Открытый ключ, соответствующий Закрытому ключу Уполномоченного лица Клиента, и направляет его в Клиентскую часть Системы. Открытый ключ устанавливается на Ключевой носитель в соответствии с «Инструкцией по перевыпуску криптографических ключей», размещенной на Сайте Банка.
- 5.2.10. Возможность работы Уполномоченного лица Клиента в Системе предоставляется не позднее двух рабочих дней после получения Банком оформленных должным образом актов признания ключа проверки электронной подписи и открытого ключа шифрования при положительной сверке информации, содержащейся в них, с информацией, зарегистрированной в Части системы на стороне банка.
- 5.2.11. Подписанные Сторонами акты признания ключа проверки электронной подписи и открытого ключа шифрования по форме Приложения №4 к Регламенту на каждого Уполномоченного лица Клиента являются неотъемлемыми частями Договора.
- 5.3. Условия отказа в заключении Договора.
- 5.3.1. Отказ Клиенту в заключении Договора возможен по причине:
- 5.3.1.1. отказа в передаче Банку персональных данных Уполномоченного лица Клиента;

- 5.3.1.2. имевшимся ранее фактам отключения Клиента от Системы по инициативе Банка по основаниям негативного характера: нарушение условий оплаты Услуг Банка за использование Системы, нарушению Регламента и прочим;
- 5.3.1.3. наличия повышенных рисков Банка, связанных с использованием Системы Клиентом.

#### 5.4. Регламент обмена электронными документами.

- 5.4.1. Клиент допускается к использованию Системы круглосуточно. Возможно временное прекращение работы Системы для проведения регламентных, профилактических, иных работ суммарно не более чем на 3 (три) часа в сутки в рабочие дни и не более чем на 12 (двенадцать) часов — в выходные и праздничные дни. В отдельных случаях в выходные и праздничные дни работа Системы может быть приостановлена на срок более 12 (двенадцати) часов с предварительным уведомлением Клиента не позднее 1 (одного) рабочего дня путем размещения информации на Сайте Банка либо иным способом извещения в соответствии с п.7.5 Регламента, обеспечивающим возможность получения Клиентом указанной информации.
- 5.4.2. Проведение всех операций и получение всей информации в Системе осуществляется Клиентом в режиме offline с последующим обменом ЭД посредством сети Интернет во время сеансов связи с Частью системы на стороне банка.
- 5.4.3. Инициатором сеансов связи с Банком всегда является Клиент. Любая просрочка в выполнении Банком своих обязательств, которая произошла из-за отсутствия инициативы Клиента в установлении сеанса связи с Банком, не влечет за собой ответственности Банка.
- 5.4.4. Все действия в Системе Клиент осуществляет в соответствии с документацией, входящей в состав программного обеспечения Клиентской части системы.
- 5.4.5. Система может использоваться для обмена ЭД, в том числе Платежными ЭД, Неплатежными ЭД.
- 5.4.6. Оформление и содержание ЭД в Системе должно соответствовать эксплуатационной документации, входящей в состав программного обеспечения Клиентской части системы.
- 5.4.7. ЭД в Системе хранятся в том же формате, в котором они были сформированы, отправлены или получены. Срок хранения ЭД в Клиентской части системы должен составлять не менее 3 (трех) лет.
- 5.4.8. Клиент обязан проверять все ЭД, получаемые по Системе, на предмет корректности ЭП Банка в порядке, предусмотренном документацией, входящей в состав программного обеспечения Клиентской части системы.
- 5.4.9. ЭД в Системе может принимать следующие статусы:
  - 5.4.9.1. «Новый» — ЭД создан или импортирован без серьезных ошибок в реквизитах;
  - 5.4.9.2. «Подписан I (Ждет II)» / «Подписан II (Ждет I)» — ЭД подписан одной ЭП из двух необходимых; ЭД с этим статусом может подписываться дополнительными ЭП до тех пор, пока под ним не будет проставлен предусмотренный для этого ЭД полный комплект ЭП; ЭД не может быть изменен или удален, пока под ним есть хотя бы одна ЭП; с ЭД с этим статусом могут быть поочередно сняты имеющиеся под ним ЭП; ЭД, с которого сняты все ЭП, возвращается к статусу «Новый» и может быть удален или изменен;
  - 5.4.9.3. «Подписан» — ЭД подписан предусмотренным для него комплектом ЭП;
  - 5.4.9.4. «Ждет отправки» — ЭД подготовлен для отправки на исполнение в Часть системы на стороне банка, но еще не обработан транспортной подсистемой Клиентской части системы. Если настроены и включены автопроцедуры, отвечающие за отправку ЭД в Часть системы на стороне банка, происходит автоматическая смена статусов: «Ждет отправки» → «Отправляется»;

- 5.4.9.5. «Отправляется» — Клиентская часть системы передает ЭД в транспортную подсистему Клиентской части системы;
  - 5.4.9.6. «Не отправлен» — произошла ошибка при передаче ЭД в транспортную подсистему Клиентской части системы;
  - 5.4.9.7. «Отправлен» — транспортная подсистема Клиентской части системы передает ЭД в транспортный шлюз Части системы на стороне банка;
  - 5.4.9.8. «Ошибка вставки» — произошла ошибка при добавлении ЭД в АБС Части системы на стороне банка;
  - 5.4.9.9. «Не расшифрован» — произошла ошибка при расшифровке ЭД в Части системы на стороне банка;
  - 5.4.9.10. «Ошибка структуры» — проверка структуры ЭД в Части системы на стороне банка дала отрицательный результат;
  - 5.4.9.11. «Истек таймаут» — истекло максимальное время пребывания ЭД в статусе «Отправлен» в Клиентской части системы;
  - 5.4.9.12. «Доставлен» — получен документарный квиток с информацией о доставке ЭД в Часть системы на стороне банка;
  - 5.4.9.13. «Расшифрован» — ЭД расшифрован транспортной подсистемой Части системы на стороне банка;
  - 5.4.9.14. «Не распознан» — произошла ошибка при установлении реквизитов ЭД (тип ЭД, наименование Клиента и иные данные) в Части системы на стороне банка;
  - 5.4.9.15. «Распознан» — в Части системы на стороне банка установлены реквизиты ЭД (тип ЭД, наименование Клиента и иные данные);
  - 5.4.9.16. «ЭЦП не верна» — проверка ЭП в ЭД в Части системы на стороне банка дала отрицательный результат;
  - 5.4.9.17. «Не принят» — ЭД не прошел контроль Части системы на стороне банка, в частности, контроль системы Fraud-мониторинга;
  - 5.4.9.18. «Принят» — ЭД прошел контроль Части системы на стороне банка и готов к дальнейшей обработке;
  - 5.4.9.19. «Принят АБС» — ЭД прошел контроль системы Fraud-мониторинга и экспортирован в АБС;
  - 5.4.9.20. «Не принят АБС» — экспорт ЭД в АБС завершился с ошибками, из АБС получена информация о том, что ЭД не будет проведен в АБС;
  - 5.4.9.21. «Отложен» — исполнение ЭД в АБС отложено;
  - 5.4.9.22. «Отказан АБС» — из АБС получена информация о том, что ЭД не будет проведен в АБС;
  - 5.4.9.23. «Исполнен» — получено подтверждение из АБС об исполнении ЭД.
- 5.4.10. Клиент самостоятельно получает информацию о статусе ЭД с использованием Клиентской части системы. Статусы ЭД, отражающие их текущее состояние, автоматически обновляются во время сеансов связи с Частью системы на стороне банка, проводимых Уполномоченным лицом Клиента.
- 5.4.11. При получении от Клиента ЭД Банк осуществляет проверку соответствия ЭП Клиента содержимому ЭД и в случае ее успешного завершения принимает ЭД к обработке.
- 5.4.12. ЭД обрабатывается Банком в операционное время, а в случаях предоставления дополнительной услуги о продлении операционного дня (проведении платежей по окончании операционного времени) — в предусмотренное Договором Счета время.
- 5.4.13. При обработке Банком ЭД осуществляется контроль правильности заполнения реквизитов в соответствии с законодательством Российской Федерации и нормативно-правовыми актами Банка России.

- 5.4.14. В случае выявления несоответствий в ходе проверки, в том числе с использованием автоматизированной системы подтверждения платежей Банка и (или) наличия иных оснований, препятствующих совершению операции по Счету, исполнение Платежного ЭД не проводится. При этом не позднее следующего рабочего дня Платежному ЭД устанавливается статус «Не принят» с указанием причины отказа в исполнении Платежного ЭД.
- 5.4.15. В случае выявления несоответствий в ходе проверки и (или) наличия иных оснований, препятствующих его исполнению, исполнение Неплатежного ЭД не проводится. При этом не позднее следующего рабочего дня Неплатежному ЭД устанавливается статус «Не принят».
- 5.4.16. Отзыв Платежного ЭД осуществляется в соответствии с порядком отзыва распоряжений на списание денежных средств со Счета предусмотренным Договором Счета/Депозита.
- 5.4.17. Отзыв Неплатежного ЭД осуществляется в соответствии с документацией Системы.
- 5.4.18. Датой и временем исполнения Платежного ЭД в Системе считается дата и время наступления Безотзывности Платежного ЭД.
- 5.4.19. Датой и временем исполнения Неплатежного ЭД в Системе считается дата и время присвоения ему статуса «Обработан».
- 5.4.20. Не позднее рабочего дня, следующего за днем совершения операций по Счету, Банк посредством Системы выдает Клиенту выписку по Счету в ответ на запрос об ее предоставлении, направленный Уполномоченным лицом Клиента посредством Системы.
- 5.4.21. Банк направляет Клиенту уведомление о совершении каждой операции по Счету с использованием Системы путем уведомления об изменении состояния Платежного ЭД, доступного для просмотра в Клиентской части системы, или путем выдачи выписки по Счету на бумажном носителе при обращении Клиента или его уполномоченного представителя в Офис банка не позднее рабочего дня, следующего за днем совершения операции по Счету. В случае если в течение рабочего дня, следующего за днем совершения операции, Клиент не осуществляет сеанса связи с Частью системы на стороне банка для просмотра посредством Клиентской части системы состояния соответствующего Платежного ЭД или если Клиент или его уполномоченный представитель не обратились в Офис банка за выпиской по Счету на бумажном носителе, уведомление, направленное Банком, считается полученным Клиентом в рабочий день, следующий за днем совершения операции.
- 5.4.22. В дополнение к информированию Клиента о совершении каждой операции с использованием Системы способом, предусмотренным п.5.4.21 Регламента, Клиент вправе подать «Заявление о направлении дополнительной информации для обеспечения информационной безопасности работы в системе дистанционного банковского обслуживания «Банк-клиент» по форме Приложения №1 к Регламенту, выбрав предусмотренный(-ые) Банком способ(-ы) дополнительного уведомления о совершении каждой операции с использованием Системы, или воспользоваться дополнительной услугой SMS-информирования.
- 5.5. Порядок приостановки обслуживания Клиента в системе.
- 5.5.1. Банк приостанавливает обслуживание Клиента в Системе в случаях:
- 5.5.1.1. получения от Клиента уведомления о компрометации Закрытого ключа в порядке, предусмотренном разделом 6 Регламента;
  - 5.5.1.2. прекращения для Уполномоченного лица Клиента действия прав подписи или Ограниченного доступа в Систему — в части доступа в Систему данного Уполномоченного лица Клиента;
  - 5.5.1.3. возникновения технических неисправностей при работе с Системой — до их устранения;
  - 5.5.1.4. не осуществления планового перевыпуска Криптографических ключей Уполномоченного лица Клиента — в части доступа в Систему данного Уполномоченного лица Клиента;

- 5.5.1.5. предусмотренных Договором Счета/Депозита.
- 5.5.2. Банк имеет право приостановить обслуживание Клиента в Системе в случаях:
  - 5.5.2.1. возникновения спорной ситуации, связанной с исполнением Договора — до разрешения спора;
  - 5.5.2.2. нарушения действующих законодательных или иных правовых актов Российской Федерации и нормативных актов Банка России;
  - 5.5.2.3. неисполнения Клиентом условий настоящего Регламента;
  - 5.5.2.4. невозможности взимания платы в соответствии с Тарифами за обслуживание в Системе и совершение операций по Счету с использованием Системы ввиду недостаточности денежных средств на Счете Клиента по истечении 30 (тридцати) календарных дней с даты направления требования Клиенту о погашении задолженности;
  - 5.5.2.5. непредставления Клиентом документов по запросу Банка в случаях, предусмотренных Договором Счета/Депозита;
  - 5.5.2.6. признания операции Клиента сомнительной/подозрительной, согласно п.8.4.9 настоящего Регламента;
  - 5.5.2.7. иных случаях, предусмотренных действующим законодательством Российской Федерации.
- 5.5.3. Приостановка обслуживания Клиента в Системе не прекращает обязательств Сторон, возникших до момента приостановки обслуживания Клиента в Системе.
- 5.5.4. В случае приостановки обслуживания Клиента в Системе, а также в иных случаях невозможности предоставления услуг по Договору, обслуживание Клиента производится в порядке, установленном Договором Счета/Депозита

## **6. Порядок взаимодействия сторон в случае компрометации закрытого ключа и (или) использования электронного средства платежа без согласия клиента.**

- 6.1. В случае Компрометации Закрытого ключа Клиент обязан направить в Банк соответствующее уведомление. Уведомление может быть направлено путем:
  - 6.1.1. устного обращения Клиента в Службу информационной поддержки клиентов с последующей обязательной подачей в Офис банка соответствующего письменного заявления в следующем порядке:
    - 6.1.1.1. Незамедлительно после обнаружения факта Компрометации Закрытого ключа Клиент обращается в Службу информационной поддержки клиентов с соответствующим сообщением. При приеме сообщения Клиента по телефону Банк:
      - 6.1.1.1.1. ведет аудиозапись разговора с Клиентом;
      - 6.1.1.1.2. производит блокировку ЭСП, препятствующую совершению операций по Счету с использованием Системы при условии, что Банк имеет возможность установить, что сообщение исходит от Клиента, в том числе по кодовому слову, указанному Клиентом в «Заявлении о направлении дополнительной информации для обеспечения информационной безопасности работы в системе дистанционного банковского обслуживания «Банк-клиент» по форме Приложения №1 к Регламенту;
      - 6.1.1.1.3. фиксирует в аудиозаписи разговора дату и время получения сообщения Клиента о Компрометации Закрытого ключа путем озвучивания Клиенту текущей даты и времени по часам Системы, синхронизированным с серверами точного времени.
    - 6.1.1.2. После обращения в Службу информационной поддержки клиентов с сообщением о Компрометации Закрытого ключа Клиент не позднее следующего рабочего дня должен подать в Офис банка «Заявление о



блокировке закрытого ключа» по форме Приложения №5 к Регламенту, подписанное лицом, наделенным правом подписи, и заверенное печатью в соответствии с Карточкой с образцами подписей;

- 6.1.1.3. После получения от Клиента «Заявления о блокировке закрытого ключа» в соответствии с требованиями п.6.1.1.2 Регламента Банк считается должным образом уведомленным Клиентом о Компрометации Закрытого ключа. В этом случае датой и временем получения Банком уведомления Клиента о Компрометации Закрытого ключа считается дата и время получения сообщения от Клиента по телефону в порядке, предусмотренном п.6.1.1.1 Регламента.
- 6.1.1.4. В случае, если Банк не получает от Клиента «Заявление о блокировке закрытого ключа» в соответствии с требованиями п.6.1.1.2 Регламента, Банк не считается должным образом уведомленным Клиентом о Компрометации Закрытого ключа, а обязанность Клиента направить указанное уведомление считается неисполненной. При этом Банк вправе произвести разблокировку ЭСП;
- 6.1.2. подачи Клиентом в Офис банка соответствующего письменного заявления в следующем порядке:
  - 6.1.2.1. Незамедлительно после обнаружения факта Компрометации Закрытого ключа Клиент подает в Офис банка менеджеру, осуществляющему обслуживание Счета, «Заявление о блокировке закрытого ключа» по форме Приложения №5 к Регламенту, подписанное лицом, наделенным правом подписи, и заверенное печатью в соответствии с Карточкой с образцами подписей. При приеме заявления Клиента Банк:
    - 6.1.2.1.1. производит блокировку ЭСП, препятствующую совершению операций по Счету с использованием Системы;
    - 6.1.2.1.2. фиксирует в заявлении в качестве даты и времени его приема текущую дату и время по часам Системы, синхронизированным с серверами точного времени.
  - 6.1.2.2. После получения от Клиента «Заявления о блокировке закрытого ключа» в соответствии с требованиями п.6.1.2.1 Регламента, Банк считается должным образом уведомленным Клиентом о Компрометации Закрытого ключа. В этом случае датой и временем получения Банком уведомления Клиента о Компрометации Закрытого ключа считается дата и время приема указанного заявления.
- 6.2. В случае неожиданного выхода из строя ЭУ или обнаружения вирусного заражения ЭУ Закрытый ключ Клиента считается скомпрометированным и Клиент обязан руководствоваться в своих дальнейших действиях главой 6 настоящего Регламента, включая незамедлительное уведомление Банка о Компрометации в соответствии с п.6.1.1.
- 6.3. Дальнейшее использование Клиентом скомпрометированного Закрытого ключа Уполномоченного лица Клиента не допускается.
- 6.4. Банк проверяет наличие ЭД, поступивших в Банк на обработку с использованием Системы и не исполненных на момент поступления от Клиента уведомления о Компрометации Закрытого ключа, в порядке, предусмотренном п.6.1 Регламента. В случае наличия указанных ЭД, Банк прекращает их обработку с установкой для каждого из них статуса «Не принят» или «Не принят АБС».
- 6.5. В случае обнаружения факта использования ЭСП (операций, совершенных с использованием ЭСП) Клиента без согласия Клиента, в дополнение к действиям, предписанным п.6.1:
  - 6.5.1. Клиент обязан направить соответствующее уведомление путем подачи в Офис банка «Заявления об операции, совершенной без согласия клиента» по форме Приложения №6 к Регламенту незамедлительно после обнаружения факта использования ЭСП без согласия Клиента, но не позднее рабочего дня, следующего за днем получения от Банка уведомления о совершенной операции способом, предусмотренным п.5.4.21 Регламента.

- 6.5.2. Для сохранения доказательств использования ЭСП без согласия Клиента Клиенту необходимо строго соблюдать последовательность нижеизложенных действий, которые рекомендуется производить коллегиально и протоколировать:
- 6.5.2.1. Незамедлительно прекратить любые действия с ЭУ, используемыми для работы с Системой.
  - 6.5.2.2. ЭУ перевести в режим «Гибернация» и отключить от информационных сетей (если было подключение, например, по Ethernet, USB, Wi-Fi и др.). В случае затруднения перевода ЭУ в режим гибернации — обесточить ЭУ (принудительно отключить электропитание в обход штатной процедуры завершения работы, извлечь аккумуляторную батарею из ноутбука и т.п.).
  - 6.5.2.3. Не предпринимать каких-либо действий для самостоятельного или с привлечением сторонних специалистов поиска и удаления компьютерных вирусов, восстановления работоспособности ЭУ.
  - 6.5.2.4. Не отправлять ЭУ в сервисные службы для восстановления работоспособности.
- 6.5.3. Банк настоятельно рекомендует Клиенту:
- 6.5.3.1. незамедлительно обратиться с заявлением в правоохранительные органы о возбуждении уголовного дела по факту хищения денежных средств;
  - 6.5.3.2. незамедлительно обратиться в суд с исковым заявлением в отношении получателя денежных средств о взыскании неосновательно полученного обогащения и процентов за пользование денежными средствами (глава 60 Гражданского Кодекса Российской Федерации), а также с ходатайством о принятии судом мер по обеспечению иска в виде ареста денежных средств на счете получателя в сумме неосновательно полученного обогащения.
- 6.5.4. Клиент не позднее следующего рабочего дня должен направить в Офис банка «Справку по факту инцидента информационной безопасности в системе дистанционного банковского обслуживания «Банк-клиент» по форме Приложения №7 Регламента с приложением документов, указанных в Приложении №8 к Регламенту.
- 6.5.5. Для возобновления работы в Системе Клиент должен произвести настройку не используемого ранее ЭУ согласно требованиям Регламента.
- 6.6. Возобновление работы в Системе Уполномоченного лица Клиента, Закрытый ключ которого был скомпрометирован, производится после повторной подачи заявления по форме Приложения №2 или №2а к Регламенту, замены Закрытого ключа и прохождения указанным Уполномоченным лицом Клиента процедуры Регистрации открытого ключа.
- 6.7. Продолжение работы в Системе Уполномоченного лица Клиента, Закрытый ключ которого не был скомпрометирован, допускается при отсутствии у Сторон оснований, допускающих использование ЭСП без согласия Клиента.

## **7. Прочие условия.**

- 7.1. Стороны осознают риски, возникающие при использовании Системы:
- 7.1.1. риск изготовления Криптографических ключей на неуполномоченное лицо;
  - 7.1.2. риск Компрометации Закрытого ключа, в том числе копирования Закрытого ключа;
  - 7.1.3. риск атаки на ЭУ, в том числе с использованием вредоносного кода, с целью совершения операции без согласия Клиента;
  - 7.1.4. риск утраты доказательств совершения мошенничества в случае обнаружения факта использования ЭСП без согласия Клиента.
- 7.2. Стороны минимизируют риски, связанные с использованием Системы, исполнением обязательных требований и следованием рекомендациям положений настоящего Регламента, а также Договоров Счета/Депозита.

- 7.3. Сторона, передающая персональные данные Уполномоченных лиц Стороны другой Стороне во исполнение Договора, гарантирует получение согласия Уполномоченных лиц Стороны на обработку и передачу их персональных данных другой Стороне. Сторона, получающая по Договору персональные данные Уполномоченных лиц другой Стороны, должна использовать их только в целях исполнения Договора, а также хранить конфиденциальность данной информации.
- 7.4. Стороны признают, что взаимодействие в рамках Системы не нарушает прав собственности Сторон в отношении информации, передаваемой с использованием Системы, а также не нарушает обязательств Сторон по неразглашению информации.
- 7.5. Сторона считается извещенной надлежащим образом любым из следующих способов:
- 7.5.1. со дня размещения информации на Сайте Банка;
  - 7.5.2. со дня направления извещения с использованием Системы;
  - 7.5.3. со дня получения извещения одной Стороной от другой Стороны;
  - 7.5.4. по истечении 6 рабочих дней со дня направления извещения заказным письмом по почте;
  - 7.5.5. со дня размещения для Клиента информации на стендах в помещениях Банка.

7.6. Стороны осознают, что ключевой носитель "Рутокен ЭЦП" с применением Криптографических ключей с криптоалгоритмом ГОСТ Р 34.10-2012 используется исключительно как средство хранения ключевой информации, тем самым увеличивает риски перечисленные в п. 7.1 настоящего Регламента.

## **8. Права и обязанности сторон.**

### **8.1. Взаимные права и обязанности Сторон.**

- 8.1.1. Стороны принимают на себя обязательства рассматривать всю информацию, полученную в ходе работы с Системой, как конфиденциальную, не подлежащую разглашению, и каждая Сторона отвечает за соблюдение данного требования с учетом пп.7.3 и 8.1.2 Регламента. Обязательства соблюдения конфиденциальности указанной информации остаются в силе неограниченное время.
- 8.1.2. Банк освобождается от обязательств по сохранению конфиденциальности информации, передаваемой в сообщениях электронной почты, направляемых Клиенту в порядке, предусмотренном Регламентом.
- 8.1.3. При обмене ЭД с использованием Системы Стороны обязуются руководствоваться правилами и требованиями, установленными Банком России, действующим законодательством Российской Федерации, Регламентом, Договором Счета/Депозита.
- 8.1.4. Стороны обязаны за собственный счет поддерживать в рабочем состоянии свои программно-технические средства, используемые для проведения электронных расчетов в Системе и получения уведомлений, оплачивать услуги предоставления доступа в Интернет, электронной почты.

### **8.2. Клиент имеет право:**

- 8.2.1. Использовать Клиентскую часть системы для осуществления обмена ЭД с Банком.
- 8.2.2. Получать по телефону техническую поддержку и консультации по вопросам использования Системы, обращаясь в Службу технической поддержки клиентов.
- 8.2.3. Для первичной установки и настройки Клиентской части системы до начала обмена ЭД санкционировать удаленное подключение сотрудника Службы технической поддержки клиентов для управления ЭУ Уполномоченного лица Клиента с использованием технических средств (программного обеспечения), определенных Банком.
- 8.2.4. В целях разрешения проблемных ситуаций, связанных с использованием Системы, санкционировать удаленное подключение на просмотр сотрудником Службы технической поддержки клиентов к ЭУ Уполномоченного лица Клиента с

использованием для этого технических средств (программного обеспечения), определенных Банком.

8.2.5. Изменить состав Уполномоченных лиц Клиента в порядке, предусмотренном разделом 5.2 Регламента, подав в Офис банка «Заявление на распоряжение по счету/изменение прав доступа уполномоченного лица клиента в системе дистанционного банковского обслуживания «Банк-клиент» по форме Приложения №2 к Регламенту или «Заявление на предоставление/изменение прав ограниченного доступа уполномоченного лица клиента в системе дистанционного банковского обслуживания «Банк-клиент» по форме Приложения №2а к Регламенту.

8.3. Клиент обязуется:

8.3.1. Немедленно информировать Банк о прекращении полномочий Уполномоченного лица Клиента для своевременного блокирования Банком доступа в Систему и прекращения обработки ЭД (при их наличии), подписанных ЭП с использованием Закрытых ключей лиц, утративших на то полномочия. В случае отзыва доверенности на Уполномоченное лицо, временной невозможности исполнять полномочия, указанные в доверенности (по причине командировки, отпуска, болезни и т.д.) Клиент обязан информировать Банк незамедлительно с момента наступления указанного события путем направления Неплатежного ЭД с последующей обязательной подачей в Офис Банка соответствующего письменного извещения. Банк приостанавливает доступ Уполномоченного лица Клиента в Систему со дня получения указанного извещения. Все риски, связанные с невыполнением указанного требования и совершения действий в Системе неуполномоченными лицами несет Клиент.

8.3.2. При создании Платежного ЭД проверять корректность указания реквизитов распоряжения на списание денежных средств. Положительный результат проверки корректности реквизитов подтверждать созданием ЭП на ЭС.

8.3.3. Контролировать соответствие суммы платежа и остатка средств на Счете на начало операционного дня и осуществлять платежи только в пределах этого остатка за исключением случаев предоставления Банком овердрафта по Счету Клиента, условия которого согласовываются Сторонами отдельно.

8.3.4. Предоставлять в Банк достоверные и актуальные сведения, необходимые для работы в Системе.

8.3.5. Самостоятельно обеспечить доступность и работоспособность канала доступа к сети Интернет, каналов получения уведомлений, направляемых Клиенту при использовании Системы.

8.3.6. Осуществлять проверку исполнения Уполномоченными лицами Клиента требований Регламента и надежности хранения ими Ключевых носителей.

8.3.7. Не передавать третьим лицам права или обязанности, предусмотренные Договором, за исключением случаев, предусмотренных Регламентом.

8.3.8. Инициировать замену Закрытого ключа и повторно проходить процедуру Регистрации открытого ключа в Системе Уполномоченного лица Клиента в случае изменения его персональных данных.

8.3.9. На основании уведомления Системы о приближении срока окончания действия Открытого ключа самостоятельно инициировать процедуру плановой замены Криптографических ключей каждым Уполномоченным лицом Клиента.

8.3.10. Регулярно знакомиться с информацией и уведомлениями Банка, размещаемыми на Сайте Банка.

8.3.11. Регулярно проверять наличие и знакомиться с новой редакцией Регламента, размещаемой на Сайте Банка.

8.3.12. После расторжения Договора уничтожить все Закрытые ключи, не передавать третьим лицам конфиденциальные данные, относящиеся к Договору, и уничтожить все имеющиеся копии программного обеспечения, необходимые для работы в Системе.

8.3.13. Если при получении уведомления или запроса Банка, указанного в п.8.4.10 настоящего Регламента, Клиентом будет установлено, что Платежный ЭД сформирован от его имени без согласия Клиента, последний обязан незамедлительно уведомить Банк о Компрометации Закрытого ключа в порядке, установленном разделом 6 настоящего Регламента.

8.4. Банк имеет право:

8.4.1. Приостанавливать обработку ЭД, поступающих через Систему, для проведения регламентных, профилактических, иных работ суммарно не более чем на 3 (три) часа в сутки в рабочие дни и не более чем на 12 (двенадцать) часов — в выходные и праздничные дни.

8.4.2. В отдельных случаях в выходные и праздничные дни приостанавливать работу Системы на срок более 12 (двенадцати) часов с предварительным уведомлением Клиента не позднее 1 (одного) рабочего дня путем размещения информации на Сайте Банка.

8.4.3. В одностороннем порядке вносить изменения в Регламент.

8.4.4. Самостоятельно определять порядок и условия обмена ЭД с Клиентом с использованием Системы.

8.4.5. Самостоятельно принимать решение о приостановке доступа Клиента в Систему в случаях выявления признаков нарушения безопасности, наличия информации о компрометации Закрытого ключа и подозрения на использование ЭСП без согласия Клиента.

8.4.6. Для первичной установки и настройки Клиентской части системы до начала обмена ЭД осуществлять санкционированное Клиентом удаленное подключение сотрудника Службы технической поддержки клиентов для управления ЭУ Уполномоченного лица Клиента с использованием технических средств (программного обеспечения).

8.4.7. В целях разрешения проблемных ситуаций, связанных с использованием Системы, осуществлять санкционированное Клиентом удаленное подключение на просмотр сотрудником Службы технической поддержки клиентов Банка к ЭУ Уполномоченного лица Клиента с использованием для этого технических средств (программного обеспечения).

8.4.8. Определять технические средства (программное обеспечение) пригодные и безопасные для использования в соответствии с п.8.4.6 и 8.4.7 Регламента.

8.4.9. Отказать в проведении операции по Счету и/или приостановить исполнение распоряжения Клиента, а также приостановить проведение всех расчетов с использованием Системы:

а) в случаях выявления Банком сомнительной/подозрительной операции Клиента, при условии незамедлительного уведомления об этом Клиента посредством направления ему соответствующего ЭД;

б) в иных случаях, установленных Регламентом, Договором Счета/Депозита, и действующим законодательством Российской Федерации, уведомив об этом Клиента (посредством направления ему ЭД) не позднее следующего рабочего дня с момента наступления соответствующего события.

8.4.10. В случае возникновения подозрений об использовании ЭСП без согласия Клиента и в целях повышения безопасности работы в Системе, Банк вправе по своему усмотрению дополнительно выполнять следующие действия:

- Уведомлять Клиента о поступивших в Банк Платежных ЭД посредством SMS-информирования.
- Запрашивать у Клиента подтверждение направления Клиентом поступившего в Банк Платежного ЭД, в том числе с использованием автоматизированной системы подтверждения платежей Банка.

Вышеуказанные уведомления и запросы осуществляются по телефону, указанному Клиентом Банку в рамках настоящего Регламента.

## 8.5. Банк обязуется:

- 8.5.1. Осуществить Регистрацию открытого ключа Уполномоченного лица Клиента в Системе в случае корректного заполнения заявлений и исполнения всех условий и требований, предусмотренных Регламентом.
- 8.5.2. Обеспечивать бесперебойную обработку ЭД, полученных в Системе.
- 8.5.3. Фиксировать направленные Клиенту уведомления о совершении каждой операции с использованием ЭСП в порядке, предусмотренном п.5.4.21 Регламента, а также хранить соответствующую информацию не менее 3 (трех) лет.
- 8.5.4. Обеспечить возможность направления Клиентом Банку уведомления о Компрометации Закрытого ключа в порядке, предусмотренном п.6.1 Регламента.
- 8.5.5. Фиксировать полученные от Клиента уведомления о Компрометации Закрытого ключа в порядке, предусмотренном п.6.1 Регламента, а также хранить соответствующую информацию не менее 3 (трех) лет.
- 8.5.6. Приостановить использование Клиентом ЭСП в порядке, предусмотренном разделом 6 Регламента, в случае получения от Клиента уведомления о компрометации Закрытого ключа, в том числе с использованием автоматизированной системы подтверждения платежей Банка, в порядке, предусмотренном п.6.1 Регламента.
- 8.5.7. Заявления, полученные от Клиента в порядке, предусмотренном в п.6.5.1 Регламента хранить не менее трех лет.
- 8.5.8. Возместить Клиенту не позднее одного рабочего дня с момента его обращения в Банк сумму операции, совершенной без согласия Клиента с использованием Закрытого ключа Клиента после получения Банком уведомления о Компрометации данного Закрытого ключа в порядке, предусмотренном п. 6.1 Регламента. Возмещение суммы такой операции производится в безналичном порядке на Счет либо согласно реквизитам, указанным в обращении Клиента. Срок рассмотрения Банком Заявления о совершении операции без согласия Клиента (Приложение №6 к Регламенту) составляет 30 дней со дня его получения Банком. Письменный ответ на Заявление Клиента отправляется Банком на указанный Клиентом адрес заказным письмом с уведомлением. Срок возмещения денежных средств по результатам рассмотрения Заявления Клиента по операциям, совершенным без согласия Клиента, составляет 7 (Семь) рабочих дней с момента отправки Клиенту ответа на Заявление.
- 8.5.9. Осуществлять по телефону техническую поддержку и консультирование Клиента по вопросам использования Системы по Телефонам Службы технической поддержки клиентов в Рабочее время Службы технической поддержки клиентов.
- 8.5.10. При расторжении с Клиентом Договора блокировать возможность использования в Системе Криптографических ключей Уполномоченных лиц Клиента.

## 9. Порядок расчетов.

- 9.1. За обслуживание в Системе и совершение операций по Счету с использованием Системы Клиент уплачивает Банку комиссии в соответствии с Тарифами, действующими в Банке на дату совершения операции, а также условиями Договора Счета/Депозита.
- 9.2. Настоящим Клиент поручает Банку списывать со Счета Клиента плату за услуги, предоставляемые Банком по Договору с применением банковских ордеров или иных расчетных документов, предусмотренных нормативными документами Банка России.
- 9.3. Клиент должен ежемесячно обеспечивать наличие на Счете денежных средств, достаточных для оплаты Банку комиссии за услуги, предоставляемые Банком по Договору в соответствии с Тарифами.

## 10. Ответственность.

- 10.1. Каждая из Сторон несет ответственность за необеспечение сохранности, разглашение и распространение Закрытых ключей, кодовых слов, паролей и другой конфиденциальной

информации, а также за их несанкционированное использование, и принимает на себя все риски, связанные с данными нарушениями.

- 10.2. Стороны несут ответственность за недостоверность информации, предоставляемой друг другу.
- 10.3. Банк не несет ответственности за задержку в формировании выписки по Счету Клиента, если она связана с задержкой получения Банком информации об исполнении перевода денежных средств оператором платежной системы или банком-корреспондентом по причинам, от Банка не зависящим.
- 10.4. Банк несет ответственность за несоблюдение сроков проведения расчетных операций по Счету Клиента на основании надлежащим образом оформленных и своевременно доставленных платежных ЭД в соответствии с Договором Счета/Депозита.
- 10.5. Банк не несет ответственности за неисполнение или ненадлежащее исполнение распоряжений Клиента, произошедшее из-за нарушения Клиентом порядка пользования Системой, условий Договора и иных обязательств, принятых им на себя в связи с подключением и использованием Системы, а также пользование Системой неуполномоченными лицами.
- 10.6. Банк возмещает Клиенту все убытки, произошедшие из-за нарушения системы защиты информации по вине Банка, в соответствии с действующим законодательством РФ.
- 10.7. Каждая из Сторон несет ответственность по всем документам, подписанным электронной цифровой подписью уполномоченных ею лиц, как в период действия Договора, так и после прекращения его действия в соответствии с действующим законодательством Российской Федерации.
- 10.8. Ни одна из Сторон не несет ответственности за ущерб, возникший вследствие некачественного функционирования каналов связи, вне зависимости от причин.

## **11. Порядок разрешения конфликтных ситуаций и споров.**

11.1. Возникновение конфликтных ситуаций в связи с осуществлением обмена ЭД в Системе.

11.1.1. В связи с осуществлением обмена ЭД возможно возникновение конфликтных ситуаций, связанных с формированием, доставкой, получением, подтверждением получения ЭД, а также использованием в данных ЭД ЭП. Данные конфликтные ситуации могут возникать, в частности, в следующих случаях:

- 11.1.1.1. неподтверждение подлинности ЭД средствами проверки ЭП принимающей Стороны;
- 11.1.1.2. оспаривание факта формирования ЭД;
- 11.1.1.3. оспаривание факта идентификации Уполномоченного лица Клиента, подписавшего ЭД;
- 11.1.1.4. заявление Стороны об искажении ЭД;
- 11.1.1.5. оспаривание факта отправления и/или доставки ЭД;
- 11.1.1.6. оспаривание времени отправления и/или доставки ЭД;
- 11.1.1.7. иные случаи возникновения конфликтных ситуаций, связанных с функционированием Системы.

11.1.2. Конфликтная ситуация возникает также в случае, если Сторона:

- 11.1.2.1. высказывает недоверие к составу и формату ЭД, хранящихся в локальном архиве Клиентской части системы или Части системы на стороне банка;
- 11.1.2.2. высказывает недоверие к программному обеспечению, функционирующему на Клиентской части системы или Части системы на стороне банка.

11.2. Уведомление о конфликтной ситуации:

11.2.1. В случае возникновения конфликтной ситуации Банк или Клиент, считающий, что его права были нарушены действиями противоположной Стороны, должен не

позднее следующего рабочего дня, когда соответственно Банку или Клиенту стало известно о нарушении его права, направить уведомление о конфликтной ситуации противоположной Стороне.

- 11.2.2. Уведомление о предполагаемом наличии конфликтной ситуации должно содержать информацию о существовании конфликтной ситуации и обстоятельствах, которые, по мнению уведомителя, свидетельствуют о наличии конфликтной ситуации. Независимо от формы, в которой составлено уведомление (письменная форма или ЭД), оно должно содержать реквизиты спорного(-ых) ЭД в случае его (их) наличия, а также фамилию, имя, отчество, должность, контактные телефоны, факс, адрес электронной почты лица или лиц, уполномоченных вести переговоры по урегулированию конфликтной ситуации.
  - 11.2.3. Уведомление о наличии конфликтной ситуации оформляется и отправляется в виде ЭД, а в случае, если это невозможно, составляется в письменной форме и направляется способом, обеспечивающим подтверждение вручения корреспонденции адресату.
  - 11.2.4. Уведомления о конфликтной ситуации, направленные Банком Клиенту, рассматриваются Клиентом с направлением Банку письменного ответа в срок не более 14 (четырнадцать) календарных дней со дня получения таких уведомлений.
  - 11.2.5. Уведомления о конфликтной ситуации, направленные Клиентом в Банк, рассматриваются Банком с направлением Клиенту письменного ответа в срок не более 30 (тридцати) календарных дней со дня получения таких заявлений, а также не более 60 (шестидесяти) календарных дней со дня получения заявлений в случае использования ЭСП для осуществления трансграничного перевода денежных средств.
- 11.3. Разрешение конфликтной ситуации в рабочем порядке.
- 11.3.1. Конфликтная ситуация признается разрешенной в рабочем порядке в случае если уведомитель удовлетворен информацией, полученной от Стороны, которой было направлено уведомление.
  - 11.3.2. Для разрешения конфликтной ситуации могут использоваться автоматически формируемые журналы Системы, фиксирующие обмен ЭС и ЭД с Клиентом, а также их обработку Системой и прочие события. Целью ведения указанных журналов являются выявление ситуаций, связанных с несанкционированными действиями, мониторинг событий для осуществления контроля, разрешение спорных и конфликтных ситуаций, связанных с работой в Системе. Заверенная выписка из указанных журналов, содержащая регистрацию событий в Системе, имеющих отношение к предмету спора, предоставляется Банком по письменному запросу Клиента.
  - 11.3.3. В случае если уведомитель не удовлетворен информацией, полученной от Стороны, которой направлялось уведомление, для рассмотрения конфликтной ситуации формируется техническая комиссия.
- 11.4. Формирование технической комиссии, ее состав.
- 11.4.1. В случае, если конфликтная ситуация не была урегулирована в рабочем порядке, Банк формирует техническую комиссию в течение двух рабочих дней с даты принятия решения об этом.
  - 11.4.2. Если Стороны, являющиеся сторонами в конфликтной ситуации, не договорятся об ином, в состав технической комиссии входит равное количество, но не менее чем по одному уполномоченному представителю каждой из конфликтующих Сторон и по согласованию Сторон представитель разработчика программного обеспечения Системы.
  - 11.4.3. В состав технической комиссии, как правило, назначаются специалисты из числа сотрудников технических служб, служб информационной безопасности Сторон.



- 11.4.4. Право представлять в комиссии соответствующую Сторону, а также разработчика программного обеспечения Системы, должно подтверждаться доверенностью, выданной каждому представителю на срок работы комиссии.
- 11.4.5. По инициативе любой из Сторон к работе комиссии для проведения технической экспертизы могут привлекаться независимые эксперты без права голоса, обладающие необходимыми знаниями в области защиты информации, работы компьютерных информационных систем. Сторона, привлекающая независимых экспертов, самостоятельно решает вопрос об оплате экспертных услуг.
- 11.4.6. Работа технической комиссии осуществляется по месту нахождения Банка или, по согласованию Сторон, разработчика программного обеспечения Системы.
- 11.5. Компетенция и полномочия технической комиссии.
- 11.5.1. Сформированная техническая комиссия при рассмотрении конфликтной ситуации устанавливает на технологическом уровне наличие или отсутствие фактических обстоятельств, свидетельствующих о факте и времени составления и/или отправки ЭД, его подлинности, а также о подписании ЭД конкретной ЭП, идентичности отправленного и полученного ЭД.
- 11.5.2. Комиссия вправе рассматривать любые иные технические вопросы, необходимые, по мнению комиссии, для выяснения причин и последствий возникновения конфликтной ситуации.
- 11.5.3. Комиссия не вправе давать правовую или какую-либо иную оценку установленных ею фактов.
- 11.5.4. Для проведения необходимых проверок и документирования данных, используемых при указанных проверках, может применяться специальное программное обеспечение.
- 11.6. Акт по итогам работы технической комиссии.
- 11.6.1. По итогам работы технической комиссии составляется акт, который должен содержать следующие данные:
- 11.6.1.1. состав комиссии с указанием сведений о квалификации каждого из членов комиссии;
  - 11.6.1.2. дату и место составления акта;
  - 11.6.1.3. даты и время начала и окончания работы комиссии;
  - 11.6.1.4. краткое изложение обстоятельств возникшей конфликтной ситуации;
  - 11.6.1.5. мероприятия, проводимые комиссией для установления причин и последствий возникшей конфликтной ситуации, с указанием даты времени и места их проведения;
  - 11.6.1.6. выводы, к которым пришла комиссия в результате проведенных мероприятий;
  - 11.6.1.7. подписи членов комиссии;
  - 11.6.1.8. указание на особое мнение члена (или членов комиссии), в случае наличия такового.
- 11.6.2. В случае если мнение члена (или членов) комиссии относительно порядка, методики, целей проводимых мероприятий не совпадает с мнением большинства членов комиссии, об этом составляется соответствующая запись, которая подписывается членом (или членами комиссии), чье особое мнение отражает соответствующая запись. Такая запись может быть составлена как в самом акте, так и в виде приложения к нему в произвольной форме и в таком же количестве подлинных экземпляров, что и акт.
- 11.6.3. Акт составляется в таком количестве экземпляров, чтобы каждая из сторон в конфликтной ситуации имела по одному подлинному экземпляру составленного акта. По требованию члена комиссии ему может быть выдана заверенная Банком копия акта.

- 11.6.4. Акт по итогам работы технической комиссии направляется Банком сторонам в конфликтной ситуации с нарочным либо иным способом, обеспечивающим подтверждение вручения корреспонденции адресату.
- 11.7. Претензионный порядок урегулирования конфликтной ситуации.
- 11.7.1. В случае, если конфликтная ситуация не урегулирована в результате работы технической комиссии либо в иной ситуации, если Сторона считает, что ее права при осуществлении обмена ЭД в рамках Системы были нарушены, она обязана направить Стороне, которая по ее мнению нарушила ее права, претензию.
- 11.7.2. Претензия должна содержать:
- 11.7.2.1. изложение существа требований Стороны;
  - 11.7.2.2. указание суммы претензии и ее расчет (если претензия подлежит денежной оценке);
  - 11.7.2.3. изложение обстоятельств, на которых основываются требования, и доказательства, подтверждающие их, со ссылкой на нормы законодательства и/или внутренние нормативные документы;
  - 11.7.2.4. сведения о работе технической комиссии и, в случае, если техническая комиссия работала в связи с возникшей конфликтной ситуацией, копии материалов работы технической комиссии, независимо от выводов технической комиссии, согласия или несогласия с этими выводами заявителя претензии;
  - 11.7.2.5. иные документы, имеющие значение, по мнению заявителя претензии;
  - 11.7.2.6. перечень прилагаемых к претензии документов и других доказательств, а также иные сведения, необходимые для урегулирования разногласий по претензии.
- 11.7.3. Претензия и все прилагаемые к ней документы направляются с нарочным либо иным способом, обеспечивающим подтверждение вручения корреспонденции адресату.
- 11.7.4. Сторона, в адрес которой направлена претензия, обязана не позднее чем в течение 14 (четырнадцати) рабочих дней удовлетворить претензию или представить мотивированный отказ в удовлетворении заявленной претензии. Непредставление ответа на претензию в течение установленного срока является нарушением установленного настоящим Регламентом претензионного порядка и может рассматриваться лицом, направившим претензию, в качестве отказа в удовлетворении претензии.
- 11.8. Разрешение споров в судебном порядке.
- 11.8.1. Все споры и разногласия между Сторонами, возникающие в связи с осуществлением обмена ЭД в соответствии с Договором, а также в связи с применением, нарушением, толкованием Договора, признанием недействительным Договора или его части, в случае если претензия истца не была удовлетворена в сроки, установленные настоящим Договором, передаются на рассмотрение в судебные органы в соответствии с действующим законодательством Российской Федерации.

## **12. Срок действия договора и порядок его расторжения.**

- 12.1. Договор вступает в силу с момента его подписания и действует в течение календарного года. Если ни одна из Сторон не заявит о своем желании расторгнуть Договор не позднее, чем за один месяц до окончания срока его действия, Договор автоматически продлевается на каждый последующий календарный год.
- 12.2. Клиент вправе в любое время расторгнуть Договор в одностороннем порядке, подав в Банк соответствующее письменное заявление. При этом Договор считается расторгнутым:
- 12.2.1. со следующего рабочего дня после получения Банком соответствующего заявления Клиента, в случаях, если в заявлении не указана дата его расторжения;

- 12.2.2. с даты, указанной в соответствующем заявлении Клиента, если она наступает позднее даты его получения Банком.
- 12.3. В случае, если у Клиента к Системе подключено несколько Счетов, закрытие Клиентом одного из указанных Счетов, влечет прекращение Банком дистанционного банковского обслуживания Клиента по данному Счету. Закрытие Клиентом последнего либо единственного Счета, подключенного к Системе, влечет автоматическое расторжение Договора.
- 12.4. Банк вправе в одностороннем порядке расторгнуть Договор в случае отсутствия у Банка технической возможности осуществления дистанционного банковского обслуживания Клиента, направив Клиенту соответствующее уведомление с указанием причин за 10 (десять) календарных дней до даты расторжения Договора.
- 12.5. В иных случаях допускается расторжение Договора в порядке, предусмотренном действующим законодательством Российской Федерации.
- 12.6. Расторжение Договора не прекращает обязательств Сторон, возникших до момента расторжения Договора.
- 12.7. При расторжении Договора уплаченные Клиентом комиссии возврату не подлежат.



**Заявление на распоряжение по счету/изменение прав доступа уполномоченного лица клиента в системе дистанционного банковского обслуживания «Банк-клиент»**

\_\_\_\_\_  
\_\_\_\_\_  
именуемый в дальнейшем Клиент, в лице \_\_\_\_\_

\_\_\_\_\_  
просит АО Банк «Национальный стандарт» зарегистрировать совмещенный ключ проверки электронной подписи и открытый ключ шифрования в системе «Банк-клиент» для уполномоченного лица с указанными правами.

Ф. И. О. уполномоченного лица Клиента: \* \_\_\_\_\_

Тел. номер(-а): \* \_\_\_\_\_ <sup>1</sup>

Доверенные IP-адреса: \_\_\_\_\_ <sup>2</sup>

Использовать действующий открытый ключ с правом доступа к счету № \_\_\_\_\_ <sup>3</sup>,

принадлежащим Клиенту: \_\_\_\_\_

защищенный носитель получен

Номера счетов *	Распоряжение по счету, в том числе с правом создания и подписи Платежных и Неплатежных ЭД <sup>4</sup>	Аннулирование прав
_____	<input type="checkbox"/>	<input type="checkbox"/>
_____	<input type="checkbox"/>	<input type="checkbox"/>
_____	<input type="checkbox"/>	<input type="checkbox"/>
_____	<input type="checkbox"/>	<input type="checkbox"/>
_____	<input type="checkbox"/>	<input type="checkbox"/>

Уполномоченное лицо Клиента\* \_\_\_\_\_ (Подпись) (\_\_\_\_\_) (Ф.И.О.)

\_\_\_\_\_ \* \_\_\_\_\_ (Подпись) (\_\_\_\_\_) (Ф.И.О.)  
(Должность руководителя)

М.П.

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

**Заполняется МЕНЕДЖЕРОМ БАНКА:**

Данная заявка получена и проверена:

\_\_\_\_\_ (Должность) \_\_\_\_\_ (Подпись) (\_\_\_\_\_) (Ф.И.О.)

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

\* Обязательно к заполнению.

<sup>1</sup> Используется для направления и запроса информации по вопросам использования Системы и обработки ЭД.

<sup>2</sup> ЭД с прочих IP-адресов не будут приняты Банком.

<sup>3</sup> Указать любой счет с правом доступа из Системы.

<sup>4</sup> Распоряжение по счету включает в себя право Ограниченного доступа в Систему без подписания дополнительного заявления.

**Заявление на предоставление/изменение прав ограниченного доступа уполномоченного лица клиента в системе дистанционного банковского обслуживания «Банк-клиент»**

\_\_\_\_\_  
\_\_\_\_\_  
именуемый в дальнейшем Клиент, в лице \_\_\_\_\_

просит АО Банк «Национальный стандарт» зарегистрировать совмещенный ключ проверки электронной подписи и открытый ключ шифрования в системе «Банк-клиент» для уполномоченного лица с указанными правами.

Ф. И. О. уполномоченного лица Клиента: \*

Использовать действующий открытый ключ с правом доступа к счету № \_\_\_\_\_<sup>1</sup>,  
принадлежащим организации: \_\_\_\_\_

защищенный носитель получен

Номера счетов *	Ограниченный доступ в Систему <sup>2</sup>	Аннулирование прав
_____	<input type="checkbox"/>	<input type="checkbox"/>
_____	<input type="checkbox"/>	<input type="checkbox"/>
_____	<input type="checkbox"/>	<input type="checkbox"/>
_____	<input type="checkbox"/>	<input type="checkbox"/>
_____	<input type="checkbox"/>	<input type="checkbox"/>

Уполномоченное лицо Клиента\* \_\_\_\_\_ (\_\_\_\_\_) (Ф.И.О.)  
(Подпись)

\_\_\_\_\_ \* \_\_\_\_\_ (\_\_\_\_\_) (Ф.И.О.)  
(Должность руководителя) (Подпись)

М.П.

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

**Заполняется МЕНЕДЖЕРОМ БАНКА:**

Данная заявка получена и проверена:

\_\_\_\_\_ (\_\_\_\_\_) (Ф.И.О.)  
(Должность) (Подпись)

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

\* Обязательно к заполнению.

<sup>1</sup> Указать любой счет с правом доступа из Системы.

<sup>2</sup> Заявление на предоставление прав ограниченного доступа в Систему (просмотр получаемой из Банка информации, запрос выписки, создание электронного сообщения, прием электронного документа) заполняется при наличии только таких прав (без прав распоряжения денежными средствами).

## **Требования и рекомендации по настройке электронного устройства Клиента для работы в Системе**

### **1. Требования к операционной системе:**

Windows 2008 Server x86 (Standard, Datacenter, Web Editions), Windows 2012 Server x64 (Foundation, Essentials, Standard, Datacenter Editions), Windows 7 x64/x86 (Ultimate, Professional, Enterprise, Home Premium, Home Basic Editions), Windows 8.1 x64/x86 (Core, Pro, Enterprise Editions), Windows 10 x64/x86 (Home, Professional, Enterprise).

### **2. Требования к наличию ODBC-драйвера:**

Microsoft Access Driver 4.00.4200.00 и выше (odbcjt32.dll).

### **3. Требования к СКЗИ:**

Используется интегрированная в Клиентскую часть системы СКЗИ — Крипто-Ком версии 3.3.  
Допустимо использовать Рутокен ЭЦП с соответствующими ему драйверами.

### **4. Требования к XML-парсеру:**

Необходимо наличие парсера Microsoft XML Core Services (MSXML) версии 6.0, который входит в состав ОС Windows 7, Windows 8.1, 10.

### **5. Требования к текстовому процессору:**

Microsoft Word 2010 или OpenOffice 2.3.0, 3.x.

### **6. Требования к редактору электронных таблиц (необходим в случае использования функциональности выгрузки данных в Excel):**

Microsoft Excel 2010.

### **7. Требования к программному обеспечению для работы с документацией:**

Adobe Reader 5.0 и выше или Adobe Acrobat Standard 5.0 и выше или Adobe Acrobat Professional 5.0 и выше.

### **8. Рекомендации к настройке брандмауэра (прокси-сервера):**

Разрешить исходящие соединения на mx1.rsbank.ru, TCP порты: 110, 25.  
Запретить иные исходящие и входящие подключения.

### **9. Поддерживаемые средства виртуализации:**

VmWare vSphere Hypervisor ESXi 4.1, 5.1

Microsoft Hyper-V R2

Oracle VM Virtual Box 4.0

Parallels Desktop 6 для Mac

Citrix XenServer 5.6

### **10. Порядок использования программного обеспечения.**

Использование иного программного обеспечения или специфическая настройка ЭУ могут негативно сказываться на работоспособности Системы.

## Акт признания ключа проверки электронной подписи и открытого ключа шифрования

“ \_\_\_\_ “ \_\_\_\_\_ 20\_\_ г.

г. \_\_\_\_\_

Настоящим актом признаётся ключ проверки электронной подписи и открытый ключ шифрования, принадлежащий уполномоченному лицу Клиента: \_\_\_\_\_  
(\_\_\_\_\_).

### Параметры ключа:

Алгоритм:

### Текст открытого ключа:

### Дополнительные поля открытого ключа (сертификата):

Имя владельца ключей:

UID:

**Ключ зарегистрирован и может использоваться для обмена сообщениями.**

**Банк**

\_\_\_\_\_  
\_\_\_\_\_

М.П.

**Уполномоченное лицо клиента**

\_\_\_\_\_  
\_\_\_\_\_

М.П.



**Заявление о блокировке закрытого ключа  
в системе дистанционного банковского обслуживания «Банк-Клиент»**

\_\_\_\_\_  
(Наименование Клиента)

именуем \_\_\_\_\_ в дальнейшем Клиент, в лице \_\_\_\_\_

настоящим уведомляет о компрометации закрытого ключа, используемого в системе дистанционного банковского обслуживания «Банк-клиент», в связи с обнаружением:

- утраты закрытых ключей
- доступа к защищенному носителю или в систему неуполномоченных лиц
- наличия операции, совершенной без согласия Клиента

Прошу Вас считать скомпрометированными и заблокировать Закрытые ключи, используемые в системе дистанционного банковского обслуживания «Банк-клиент» Уполномоченным(-ми) лицом(-ами):

\_\_\_\_\_  
(Должность руководителя)

М.П.

\_\_\_\_\_  
(Подпись)

(\_\_\_\_\_  
(Ф.И.О.)

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

Заявление от Клиента получил

\_\_\_\_\_  
(Должность)

\_\_\_\_\_  
(Подпись)

\_\_\_\_\_  
(Ф.И.О.)

\_\_\_\_\_  
(Дата)

\_\_\_\_\_  
(Время)

**Заявление об операции, совершенной без согласия клиента  
в системе дистанционного банковского обслуживания «Банк-клиент»**

\_\_\_\_\_  
(Наименование Клиента)

именуем \_\_\_\_\_ в дальнейшем Клиент, в лице \_\_\_\_\_

настоящим уведомляет об обнаружении в выписке по счету \_\_\_\_\_ операции, совершенной без согласия Клиента.

Реквизиты операции по переводу денежных средств:

Дата документа: \_\_\_\_\_

Номер документа: \_\_\_\_\_

Наименование плательщика: \_\_\_\_\_

ИНН плательщика: \_\_\_\_\_

Номер счета плательщика: \_\_\_\_\_

БИК банка плательщика: \_\_\_\_\_

Наименование банка плательщика: \_\_\_\_\_

Наименование получателя: \_\_\_\_\_

ИНН получателя: \_\_\_\_\_

Номер счета получателя: \_\_\_\_\_

БИК банка получателя: \_\_\_\_\_

Наименование банка получателя: \_\_\_\_\_

Сумма документа: \_\_\_\_\_

Назначение: \_\_\_\_\_

\_\_\_\_\_  
(Должность руководителя)

М.П.

\_\_\_\_\_  
(Подпись)

( \_\_\_\_\_ )  
(Ф.И.О.)

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

Заявление от Клиента получил

\_\_\_\_\_  
(Должность)

\_\_\_\_\_  
(Подпись)

\_\_\_\_\_  
(Ф.И.О.)

\_\_\_\_\_  
(Дата)

\_\_\_\_\_  
(Время)

**Справка по факту инцидента информационной безопасности в системе дистанционного  
банковского обслуживания «Банк-клиент»**

(Наименование Клиента)

именуем \_\_\_\_\_ в дальнейшем Клиент, в лице \_\_\_\_\_

настоящим доводит дополнительную информацию по факту обнаружения операции, совершенной без согласия клиента «\_\_» \_\_\_\_\_ 20\_\_ г.

Количество электронных устройств (ЭУ), настроенных для доступа в Систему: \_\_\_\_\_.

- Для доступа в Систему используются:
  - корпоративные ЭУ
  - личные ЭУ
  - ЭУ, находящиеся в общественном пользовании
- Периодичность смены пароля системы ДБО: \_\_\_\_\_
- соблюден порядок подготовки ЭУ к установке Системы в соответствии с Регламентом
- ЭУ расположен и используется в помещении с доступом:  свободным /  ограниченным
- ЭУ размещен способом, не позволяющим производить визуальное наблюдение за экраном ЭУ и его клавиатурой
- используется программное обеспечение для работы в Системе: \_\_\_\_\_
- используется только лицензионное программное обеспечение
- операционная система и приложения обновляются \_\_\_\_\_  
(Периодичность)
- используется антивирусное программное обеспечение: \_\_\_\_\_
- антивирусное программное обеспечение обновляется \_\_\_\_\_  
(Периодичность)
- производится обмен сообщениями электронной почты на ЭУ
- используются средства сетевой защиты: \_\_\_\_\_
- на ЭУ запрещены входящие соединения из сети Интернет
- с ЭУ разрешены исходящие соединения с Банком и ограниченным числом сайтов сети Интернет для проведения обновлений операционной системы, программного обеспечения, в том числе антивирусного, число разрешенных сайтов составляет \_\_\_\_\_
- обеспечивается возможность доступа к ЭУ только уполномоченных лиц
- Ключевые носители хранятся \_\_\_\_\_  
(Место хранения)
- Уполномоченные лица в операционной системе наделены правами
  - пользователей
  - администраторов

- пароль на доступ в Клиентскую часть системы, Закрытый ключ состоит из \_\_\_\_ символов и содержит:
  - буквы в нижнем регистре
  - буквы в верхнем регистре
  - цифры
  - спецсимволы (например, !»№;%;:?\*()\_+ / и т.п.)
- обеспечивается возможность доступа к Ключевым носителям только уполномоченных лиц
- ведется аудит событий, регистрирующий возникающие ошибки работы операционной системы и приложений, вход пользователей и запуск программ
- отчуждаемые носители информации (флеш-накопители, дискеты, диски и т.п.) используются в среднем \_\_\_\_\_ для целей \_\_\_\_\_  
(Периодичность)
- Интернет на ЭУ используется для целей \_\_\_\_\_
- Иная информация, имеющая отношение к инциденту: \_\_\_\_\_
- По факту хищения денежных средств:
  - Клиент не намерен обращаться в правоохранительные органы.
  - Клиент намерен обратиться в правоохранительные органы.
  - Клиент обратился в правоохранительные органы. Заявление принято в \_\_\_\_\_

(Район, округ, город, субъект федерации и иные идентифицирующие ОВД данные)

\_\_\_\_\_ и зарегистрировано за № \_\_\_\_\_ в КУСП.
- О необходимости предоставления доступа сотрудников правоохранительных органов к электронному устройству, об ответственности за использование нелегализованного и контрафактного программного обеспечения в соответствии со статьей 146 УК Российской Федерации предупрежден.

\_\_\_\_\_  
(Должность руководителя)

М.П.

\_\_\_\_\_  
(Подпись) (\_\_\_\_\_  
(Ф.И.О.)

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

**Перечень документов, которые Клиент предоставляет в Банк в случае выявления операции, совершенной без согласия Клиента**

1. Копия лицензии на операционную систему ЭУ.
2. Копия счета или чека на приобретение операционной системы ЭУ.
3. Описание используемого программного обеспечения (перечень использованного лицензионного и нелицензионного программного обеспечения на рабочем месте, информация о версии операционной системы и наличии критических обновлений, рекомендуемых разработчиком операционной системы).
4. Копия договора на оказание услуг доступа в Интернет.
5. Описание организации доступа в сеть Интернет на рабочем месте.
6. Копия счета или чека на оказание доступа в сеть Интернет на повременной основе (при наличии).
7. Копия заявления в правоохранительные органы (при наличии).
8. Копия лицензии на антивирусное программное обеспечение.
9. Копия счета или чека на антивирусное программное обеспечение.
10. Описание антивирусной защиты рабочего места (наличие установленного на жестком диске ЭУ антивирусного программного обеспечения и актуальность его баз, частота обновления, сканирования, наличие сведений о проявлении на ЭУ вредоносных программ).

АО Банк «Национальный стандарт»

**СОГЛАШЕНИЕ**  
**о присоединении к системе дистанционного банковского обслуживания**  
**«БАНК-КЛИЕНТ»**

\_\_\_\_\_  
(Место заключения соглашения)

« \_\_\_\_ » \_\_\_\_\_ 20 \_\_\_\_ г.

**Акционерное общество Банк «Национальный стандарт»**, именуемый в дальнейшем «Банк», в лице \_\_\_\_\_, действующего на основании доверенности от \_\_\_\_\_ № \_\_\_\_\_, с одной стороны, и \_\_\_\_\_

\_\_\_\_\_  
(Наименование Клиента)

именуемый в дальнейшем «Клиент», в лице \_\_\_\_\_ (Должность, ФИО руководителя)

\_\_\_\_\_ действующего на основании \_\_\_\_\_, с другой стороны, в дальнейшем совместно именуемые «Стороны», заключили настоящее Соглашение (далее — «Соглашение») о нижеследующем:

1. Стороны договариваются о дистанционном банковском обслуживании Клиента путем обмена документами в электронной форме, подписанными Электронной подписью, в соответствии с «Регламентом системы дистанционного банковского обслуживания «Банк-Клиент», далее — «Регламент».
2. Регламентом определены условия оказания услуг по дистанционному банковскому обслуживанию «Банк-клиент», требования к техническому и информационному обеспечению процессов формирования, обработки и хранения ЭД.
3. Подписанием Соглашения Клиент подтверждает, что полностью и безусловно присоединяется к Регламенту, до подписания Соглашения ознакомлен с содержанием Регламента, а также со Сборником тарифов на услуги Банка для юридических лиц, индивидуальных предпринимателей и физических лиц, занимающихся в установленном законодательством Российской Федерации порядке частной практикой и Инструкцией по перевыпуску криптографических ключей.\*
4. Стороны определяют, что дистанционное банковское обслуживание Клиента осуществляется по всем счетам, открытым Клиентом в Банке.
5. По взаимному согласию Стороны определили, что право Электронной подписи ЭД имеют Уполномоченные лица, указанные в карточке с образцами подписей и оттиска печати, доверенности.
6. Соглашение составлено в двух идентичных экземплярах равной юридической силы — по одному для каждой Стороны.

**БАНК:**

АО Банк «Национальный стандарт»  
Место нахождения: 115093, г. Москва, Партийный пер., д.1,  
корп. 57, стр. 2,3

\_\_\_\_\_  
(Наименование уполномоченного подразделения)

\_\_\_\_\_  
(Адрес уполномоченного подразделения)

БИК 044525498, ИНН 7750056688,  
к/с 30101810045250000498 в ГУ Банка России по  
Центральному федеральному округу

\_\_\_\_\_  
(Должность руководителя подразделения)

\_\_\_\_\_  
(Подпись)

\_\_\_\_\_  
(Ф.И.О.)

М. П.

**КЛИЕНТ:**

\_\_\_\_\_  
(Сокращенное наименование, место нахождения,

\_\_\_\_\_  
(ОГРН/ОГРНИП, ИНН, контактные телефоны)\*\*

\_\_\_\_\_  
(Должность руководителя)

\_\_\_\_\_  
(Подпись)

\_\_\_\_\_  
(Ф.И.О.)

М. П.

\* Регламент системы дистанционного банковского обслуживания «Банк-клиент», Сборник тарифов на услуги Банка для юридических лиц, индивидуальных предпринимателей и физических лиц, занимающихся в установленном законодательством Российской Федерации порядке частной практикой и Инструкция по перевыпуску криптографических ключей размещены на сайте [www.ns-bank.ru](http://www.ns-bank.ru).

\*\* При заключении соглашения с индивидуальным предпринимателем дополнительно указывать следующие сведения:

- реквизиты документа, удостоверяющего личность;
- дата и место рождения;
- адрес регистрации (в случае, если адрес регистрации индивидуального предпринимателя не совпадает с адресом его фактического места жительства, необходимо указывать адрес регистрации и адрес фактического места жительства).