Приложение № 2
к Условиям расчетно-кассового обслуживания юридических лиц,
индивидуальных предпринимателей и физических лиц, занимающихся в
установленном законодательством Российской Федерации порядке
частной практикой, в АО «Банк Русский Стандарт»

Условия дистанционного банковского обслуживания корпоративных клиентов

1. Настоящие Условия дистанционного банковского обслуживания корпоративных клиентов (далее – **Условия ДБО**) являются составной и неотъемлемой частью Условий расчетно-кассового обслуживания юридических лиц, индивидуальных предпринимателей и физических лиц, занимающихся в установленном законодательством Российской Федерации порядке частной практикой, в АО «Банк Русский Стандарт» (далее – **Условия**) и определяют отношения между Банком и Клиентом в рамках Договора, возникающие в связи с предоставлением Клиенту удаленного доступа к Системе «Интернет-Банк» и дистанционным обслуживанием Клиента.

2. ИСПОЛЬЗУЕМЫЕ ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

В настоящем документе указанные ниже термины и определения, написанные с заглавной буквы, будут иметь следующие значения:

2.1. **Аутентификационные данные** – Пароль/ TouchID/ FaceID, используемые для целей установления личности уполномоченного лица Клиента при доступе к Мобильному устройству и/или Ключу ЭП PayControl;

2.2. **Владелец ЭП** – уполномоченное лицо Клиента, которому в установленном действующим законодательством Российской Федерации и Договором порядке выдан Сертификат ключа проверки ЭП или Ключ eToken PASS, или которым самостоятельно выпущен (сгенерирован) Ключ ЭП PayControl, или которому сформирован Сертификат ЦР и выпущены (сгенерированы) соответствующие ключи усиленной неквалифицированной электронной подписи в порядке, установленном Условиями по операциям с ЦР;

2.3. **Дистанционное банковское обслуживание (ДБО)** – предоставление Банком Клиенту предусмотренных Условиями ДБО банковских и информационных услуг с использованием Системы «Интернет-Банк»;

2.4. **Документы валютного контроля –** справки о подтверждающих документах, ведомости банковского контроля, документы, связанные с проведением валютной операции, предусмотренные Инструкцией Банка России от 16.08.2017 № 181-И «О порядке представления резидентами и нерезидентами уполномоченным банкам подтверждающих документов и информации при осуществлении валютных операций, о единых формах учета и отчетности по валютным операциям, порядке и сроках их представления» (далее – **Инструкция № 181-И**), в том числе, документы, связанные с проведением валютных операций, открытием и ведением счетов, представляемые Клиентом в соответствии с п.4 ст.23 Федерального закона от 12.10.2003 № 173-ФЗ «О валютном регулировании и валютном контроле»;

2.5. **Зарегистрированный номер** – телефонный номер, обслуживаемый оператором подвижной радиотелефонной связи, указанный в Заявлении или в Заявлении на открытие счета в качестве контактного, или в Заявлении на смену или предоставление нового QR-кода (по форме Приложения № 11 к Условиям ДБО), Заявлении о регистрации уполномоченного лица Клиента (по форме Приложения № 12 к Условиям ДБО) или ином принятом Банком от Клиента письменном заявлении и зарегистрированный в Системе;

2.6. **Ключ проверки ЭП** – уникальная последовательность символов, однозначно связанная с Ключом ЭП и предназначенная для проверки подлинности ЭП;

2.7. **Ключ проверки ЭП PayControl –** уникальный ключ, самостоятельно выпускаемый Клиентом одновременно с Ключом ЭП PayControl с использованием средства ЭП PayControl при выполнении процедуры первичного выпуска Ключа ЭП PayControl, а также при проведении плановой/внеочередной/экстренной смены Ключей ЭП PayControl, однозначно связанный с Ключом ЭП PayControl и предназначенный для проверки подлинности ЭП, созданной с использованием Ключа ЭП PayControl;

2.8. **Ключ ЭП** – уникальная последовательность символов, предназначенная для создания ЭП;

2.9. **Ключ ЭП PayControl –** уникальный ключ, самостоятельно выпускаемый Клиентом одновременно с Ключом проверки ЭП PayControl с использованием средства ЭП PayControl при выполнении процедуры первичного выпуска Ключа ЭП PayControl, а также при плановой/внеочередной/экстренной смене Ключей ЭП PayControl, предназначенный для создания ЭП;

2.10. **Ключ eToken PASS** – автономное устройство, предназначенное для генерации Одноразовых паролей, используемых для дополнительной авторизации в Системе, а также подтверждения и отправки ЭД;

2.11. **Ключевая информация** – обобщенное понятие информации, содержащей Логин, Пароль, Одноразовый пароль, Одноразовый код, Ключи, Ключ eToken PASS, Ключи PayControl, QR-код, используемые для аутентификации ЭД;

2.12. **Ключи** – совокупность Ключа ЭП и соответствующего ему Ключа проверки ЭП;

2.13. **Ключи PayControl –** совокупность Ключа ЭП PayControl и соответствующего ему Ключа проверки ЭП PayControl;

2.14. **Компрометация ключевой информации** – ситуация, при которой Логин, Пароль, Ключи, Ключ eToken PASS, Одноразовый пароль, Одноразовый код, Ключи PayControl, QR-код стали доступны постороннему лицу независимо от того, нанесен или нет ущерб Банку и/или Клиенту. Под Компрометацией ключевой информации подразумеваются произошедшие события: утрата, утрата с последующим обнаружением, несанкционированное копирование или подозрение на копирование, любые другие ситуации, при которых достоверно неизвестно, что произошло с носителем Ключевой информации;

2.15. **Корпоративный удостоверяющий центр Банка (**далее **– Удостоверяющий центр)** – уполномоченное подразделение Банка, осуществляющее функции по созданию и выдаче Сертификатов ключей проверки ЭП, Сертификатов ЦР, а также иные функции, предусмотренные действующим законодательством Российской Федерации;
2.16. **Логин** – уникальная последовательность алфавитно-цифровых символов, присваиваемая каждому уполномоченному лицу Клиента при регистрации в Системе;
2.17. **Мобильное приложение PayControl –** мобильное приложение для операционных систем iOS и Android, разработанное ООО «СэйфТек» (SafeTech LTD), выполняющее функции управления ключевой информацией, а именно: Ключами PayControl и QR-кодом, (считывание, хранение, использование, обновление, удаление), получения информации для подтверждения от серверной части, отображения подтвержденной информации на экране Мобильного устройства, выработки кода подтверждения на основе данных операции, ключа пользователя, времени обработки, отправки кода подтверждения в серверную часть;
2.18. **Мобильное устройство –** смартфоны, мобильные телефоны, планшеты и прочие устройства, на которых есть доступ в Интернет и установлено Мобильное приложение PayControl. Используется как носитель Ключевой информации для средства ЭП PayControl;
2.19. **Неквалифицированная электронная подпись –** усиленная неквалифицированная электронная подпись, которая:

- сформирована в соответствии с Условиями ДБО (включая приложения к ним);
- получена в результате криптографического преобразования информации с использованием Ключа ЭП;
- позволяет определить лицо, подписавшее ЭД;
- позволяет обнаружить факт внесения изменений в ЭД после момента его подписания;
- создается с использованием Средств электронной подписи;

2.20. **Одноразовый пароль** – пароль, генерируемый Ключом eToken PASS для дополнительной авторизации в Системе и подписи ЭД, не является статичным и действует только на единоразовое подтверждение действий в Системе;
2.21. **Одноразовый код** – персональный одноразовый цифровой код, генерируемый программным модулем Системы и направляемый Банком уполномоченному лицу Клиента в виде СМС-сообщения (короткого текстового сообщения) на Зарегистрированный номер при входе уполномоченного лица Клиента в Систему для генерации (самостоятельного выпуска) Ключей PayControl, а также при оформлении Акта признания ключа подписи для обмена сообщениями (Приложение № 9 к Условиям ДБО) в электронной форме;
2.22. **Ответственный сотрудник Банка** – уполномоченный сотрудник Банка, который на основании распорядительного акта Банка уполномочен осуществлять от имени Банка предусмотренные Инструкцией №181-И действия по валютному контролю, в том числе подписывать ЭП Документы валютного контроля/уполномоченный сотрудник Банка, который уполномочен на основании распорядительного акта Банка на подписание ЭП иных ЭД (кроме Документов валютного контроля), в рамках настоящих Условий ДБО;
2.23. **Пароль** – последовательность алфавитно-цифровых символов, связанная в Системе с соответствующим Логином;
2.24. **Простая электронная подпись (**далее **– Простая ЭП) –** электронная подпись, которая посредством использования Одноразового пароля, Одноразового кода, Ключей PayControl подтверждает подпись уполномоченного лица Клиента;
2.25. **Сертификат ключа проверки ЭП/Сертификат** – документ на бумажном носителе или ЭД, выданные Удостоверяющим центром в соответствии с Условиями ДБО (включая приложения к ним) и подтверждающие принадлежность Ключа проверки ЭП Владельцу ЭП;
2.26. **Сертификат ЦР** – сертификат ключа проверки электронной подписи, выданный Клиенту в соответствии с Условиями по операциям с ЦР;
2.27. **Средства Удостоверяющего центра** – программные и (или) аппаратные средства, используемые для реализации функций Удостоверяющего центра;
2.28. **Средства электронной подписи** – шифровальные (криптографические) средства, используемые для реализации хотя бы одной из следующих функций – создание ЭП, проверка ЭП, создание Ключа ЭП и Ключа проверки ЭП, создание Ключа ЭП PayControl и Ключа проверки ЭП PayControl;
2.29. **Статус документа** – информация о текущем состоянии ЭД в Системе;
2.30. **Удаленное рабочее место Системы (**далее **– Рабочее место)** – составная часть Системы, используемая Клиентом для направления Банку и получения от Банка ЭД;
2.31. **Условия по операциям с ЦР** – Условия по осуществлению юридическими лицами операций с цифровыми рублями, являющиеся составной и неотъемлемой частью Условий (Приложение № 13 к Условиям);
2.32. **Участники Системы** – Банк и Клиент, осуществляющие электронный документооборот посредством Системы в рамках заключенных между ними договоров;
2.33. **Электронная подпись (**ранее и далее **– ЭП)** – реквизит ЭД, информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию. Под ЭП в рамках настоящих Условий ДБО понимается Неквалифицированная электронная подпись, Простая ЭП или усиленная неквалифицированная электронная подпись, созданная Клиентом в порядке, установленном Условиями по операциям с ЦР;
2.34. **Электронный документ (**ранее и далее **– ЭД)** – документированная информация, представленная в электронной форме, то есть в виде, пригодном для восприятия человеком с использованием электронных вычислительных машин, а также для передачи по информационно-телекоммуникационным сетям или обработки в информационных системах;

2.35. **QR-код -** оптическая метка, содержащая компонент Ключа проверки ЭП PayControl.

В настоящих Условиях ДБО термины и определения, обозначающие единственное число, включают в себя, как единственное, так множественное число.

Иные термины и определения (не перечисленные в настоящем разделе Условий ДБО), используемые в настоящем документе и написанные с заглавной буквы, имеют то же значение, что и в Условиях.

3. ОБЩИЕ УСЛОВИЯ

3.1. Настоящие Условия ДБО регулируют отношения между Банком и Клиентом (далее при совместном упоминании **Стороны**, а по отдельности – **Сторона**) по предоставлению Банком услуг по Дистанционному банковскому обслуживанию Клиента с использованием Системы, в том числе порядок обмена ЭД, права, обязанности и ответственность Сторон.

3.2. Для целей обмена ЭД с использованием Системы Банк передает Клиенту на срок действия Договора право доступа к Системе и право использования Рабочего места для получения услуг по Дистанционному банковскому обслуживанию, а Клиент оплачивает Банку такие услуги в соответствии с Тарифами. При этом Банк не предоставляет Клиенту Мобильное устройство и право использования Мобильного приложения PayControl. Стоимость услуг третьих лиц, обеспечивающих подключение Клиента к сети Интернет и обслуживание его в сети Интернет, а также Мобильное устройство и право использования Мобильного приложения PayControl, оплачиваются Клиентом самостоятельно и не входит в стоимость услуг Банка. Клиент самостоятельно урегулирует вопросы использования Мобильного приложения PayControl с правообладателем указанного приложения.

3.3. Настоящим Банк и Клиент пришли к соглашению об использовании Системы для защищенного обмена между Сторонами следующими ЭД:

3.3.1. документами для осуществления расчетных и иных Операций по Счету Клиента, открытому в Банке, получения Клиентом информации в электронной форме о состоянии Счета, а также реестрами перечислений согласно договору об обслуживании организации по выплате заработной платы с использованием банковских карт, заключенному между Сторонами;

3.3.2. документами в целях совершения операций с цифровыми рублями, или документами, связанными с операциями с цифровыми рублями, или документами, обмен которыми осуществляется между Клиентом и платформой цифрового рубля в порядке, установленном Условиями по операциям с ЦР;

3.3.3. Документами валютного контроля (в случае если оригинал документов оформлен на бумажном носителе и содержит все необходимые для данного вида документа отметки, включая подписи уполномоченных лиц и печать Клиента (при наличии)). Для представления Документа валютного контроля в Банк с использованием Системы, оригинал документа должен быть преобразован в электронную копию посредством электронного сканирования. Электронные копии Документов валютного контроля представляются в Банк в виде вложенного файла в составе сообщения свободного формата;

3.3.4. иными документами, сообщениями и информацией, обмен которыми предусмотрен Договором, а также иными договорами и соглашениями, заключенными между Банком и Клиентом.

Банк вправе принять от Клиента ЭД, не предусмотренные в п.п. 3.3.1 - 3.3.4 Условий ДБО, подписанные ЭП Владельца ЭП. При этом принятие Банком от Клиента ЭД, не предусмотренных в п.п. 3.3.1 - 3.3.4 Условий ДБО, является правом, а не обязанностью Банка, и ничто из Договора не говорит и не может говорить об обратном.

3.4. Каждый ЭД, направляемый с использованием Системы одной Стороной другой Стороне, должен быть подписан ЭП Владельца ЭП или ЭП Ответственного сотрудника Банка соответственно.

3.5. Стороны признают, что получение Банком ЭД с использованием Системы, подписанного ЭП Владельца ЭП, (в том числе в порядке, установленном Условиями по операциям с ЦР), направленного от Клиента, юридически эквивалентно (равнозначно) получению соответствующего документа на бумажном носителе, подписанного от имени Клиента уполномоченным лицом Клиента и заверенного оттиском печати Клиента (при наличии) с учетом требований действующего законодательства Российской Федерации. При этом документы, указанные в п.п. 3.3.1, 3.3.3, 3.3.3 Условий ДБО, должны быть подписаны ЭП Владельцев ЭП, имеющих право подписи расчетных документов Клиента, каждому из которых выдан Сертификат, Сертификат ЦР или Ключ eToken PASS, или каждым из которых самостоятельно выпущен (сгенерирован) Ключ ЭП PayControl в соответствии с Условиями ДБО и Договором в целом.

3.6. Стороны признают, что получение Клиентом ЭД с использованием Системы, подписанного ЭП Ответственного сотрудника Банка, направленного от Банка, юридически эквивалентно (равнозначно) получению соответствующего документа на бумажном носителе, подписанного от имени Банка уполномоченным лицом Банка, и заверенного оттиском печати Банка с учетом требований действующего законодательства Российской Федерации.

3.7. Настоящим Стороны подтверждают и соглашаются с тем, что:

3.7.1. Сторона, получившая ЭД с использованием Системы, не несет ответственности за правильность содержания и/или оформления такого ЭД Стороной, его направившей (в том числе при направлении ЭД в рамках Условий по операциям с ЦР);

3.7.2. используемые Сторонами ЭП реализуют подлинность и авторство ЭД и являются достаточными для обеспечения безопасности, конфиденциальности, а также авторства и подлинности направляемых/ принимаемых с использованием Системы ЭД. Проверка ЭП осуществляется в соответствии с порядком, изложенным в Приложении № 3 к Условиям ДБО, или в соответствии с порядком, изложенным в Условиях по операциям с ЦР и приложениях к Условиям по операциям с ЦР.

3.8. В качестве уполномоченных лиц Сторон имеют право выступать лица, имеющие полномочия на осуществление соответствующих действий от имени соответствующей Стороны.

3.9. В части электронного документооборота между Клиентом и платформой цифрового рубля в соответствии с Условиями по операциям с ЦР, в том числе при совершении операций с цифровыми рублями или в связи с операциями с цифровыми рублями, положения Условий по операциям с ЦР имеют преимущественную силу перед Условиями ДБО, и в случае расхождений положений Условий ДБО с положениями Условий по операциям с ЦР, применяются положения Условий по операциям с ЦР.
3.10. Исключительные права на программное обеспечение «Correqts», используемое Сторонами при эксплуатации Системы, принадлежат ООО «БСС» (ОГРН 1087746170181).

4. ОБЩИЕ УСЛОВИЯ И ПОРЯДОК ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА

4.1. ЭД передаются Клиентом в Банк с использованием Системы. При невозможности поступления в Банк ЭД с использованием Системы Клиент передает (при наличии у Банка возможности) документы на бумажных носителях.
4.2. Банк осуществляет переводы на основании распоряжений в электронной форме при условии соответствия таких документов требованиям законодательства Российской Федерации, требованиям нормативных актов Банка России, требованиям Договора (в том числе Условий и приложений к ним), форматам, установленным Системой, с учетом ограничений на совершение Клиентом Операций по Счету (-ам) с использованием Системы, установленных Банком на основании письменного заявления Клиента, оформленного на бумажном носителе и подписанного уполномоченным лицом Клиента, а также при условии положительного результата проверки подлинности ЭП в ЭД.
4.3. В случае несоответствия ЭД требованиям законодательства Российской Федерации, требованиям нормативных актов государственных органов Российской Федерации, в том числе Банка России, требованиям Договора (в том числе Условий и приложений к ним), положениям заключенных между Сторонами договоров, соглашений, и/или в случае выявления угрозы несанкционированного доступа к программно-аппаратным средствам Клиента или его Счету, а также в случае наличия ограничений на совершение Клиентом Операций по Счету (-ам) с использованием Системы, установленных Банком на основании письменного заявления Клиента, оформленного на бумажном носителе и подписанного уполномоченным лицом Клиента, Банк отказывает в исполнении ЭД Клиента, уведомив Клиента посредством Системы о причинах отказа.
4.4. Порядок электронного документооборота установлен в Приложении №3 к настоящим Условиям ДБО, а также в Условиях по операциям с ЦР.
4.5. Стороны признают, что способы защиты и обеспечения целостности информации, средства аутентификации и авторизации, применяемые Системой при передаче ЭД, достаточны для подтверждения авторства, целостности и подлинности документов, и обязуются выполнять режим обеспечения безопасности, установленный «Инструкцией по обеспечению безопасности» (Приложение № 4 к Условиям ДБО), а также режим обеспечения безопасности, установленный Условиями по операциям с ЦР.
4.6. Стороны также признают, что:
- 4.6.1. при любом изменении ЭД, совершенном после его подписания ЭП одной из Сторон, ЭП становится некорректной;
- 4.6.2. знание информации, которая передается между Сторонами по каналу связи Системы, не приводит к компрометации Ключевой информации;
- 4.6.3. подделка ЭП Участника Системы, т.е. создание корректной ЭП, невозможна без знания Ключа ЭП, или Одноразового пароля, или Одноразового кода или Ключа ЭП PayControl;
- 4.6.4. созданный в единственном экземпляре в рамках Условий ДБО Ключ ЭП Клиента уникален, создание дубликата Ключа ЭП возможно только Клиентом или иными лицами при нарушении Клиентом условий хранения и/или использования Ключа ЭП, предусмотренных Условиями ДБО;
- 4.6.5. каждый переданный Клиенту в соответствии с Условиями ДБО Ключ eToken PASS уникален;
- 4.6.6. каждый созданный Клиентом в единственном экземпляре в рамках Условий ДБО Ключ ЭП PayControl уникален;
- 4.6.7. каждый созданный в единственном экземпляре в рамках Условий ДБО QR-код Клиента уникален, создание дубликата QR-кода возможно только Клиентом или иными лицами при нарушении Клиентом условий хранения и/или использования QR-кода, предусмотренных Условиями ДБО;
- 4.6.8. каждый Участник Системы несет ответственность за сохранение в тайне своих Логина, Пароля, Ключей, Ключа eToken PASS, Одноразовых паролей, Одноразовых кодов, Ключей PayControl, QR-кода, Аутентификационных данных, за правильность заполнения и оформления ЭД и за действия своего персонала при работе с Системой и Мобильным устройством,
- 4.6.9. Правильность оформления и заполнения полей ЭД Клиента проверяется ответственным должностным лицом Клиента. Ответственность за передачу ошибочного ЭД Клиента несет Клиент.

4.7. Если иное в отношении документов на бумажном носителе, выдаваемых Банком Клиенту, не предусмотрено действующим законодательством Российской Федерации и нормативными актами Банка России, ЭД, переданные Клиенту в соответствии с Условиями ДБО, Условиями по операциям с ЦР, не представляются впоследствии Банком Клиенту на бумажном носителе.
4.8. По заявлению Клиента Банк предоставляет дубликат выписки по Счету на бумажном носителе. Данная услуга оплачивается Клиентом в соответствии с Тарифами, действующими на момент оказания соответствующей услуги.

5. ПРАВА И ОБЯЗАННОСТИ СТОРОН

5.1. При эксплуатации Системы Стороны обязаны:
- руководствоваться Положением Банка России от 29.06.2021 № 762-П «О правилах осуществления перевода денежных средств», Положением Банка России от 03.08.2023 № 820-П «О платформе цифрового рубля», Федеральным законом от 27.06.2011 №161-ФЗ «О национальной платежной системе», Федеральным законом

от 06.04.2011 № 63-ФЗ «Об электронной подписи», Инструкцией № 181-И, Договором, иными договорами и соглашениями, заключенными между Банком и Клиентом, а также иными нормативно-правовыми и нормативными актами, действующими в Российской Федерации;

- за свой счет поддерживать в рабочем состоянии свои технические средства и оборудование, используемые для функционирования Системы, требования к которым указаны в Приложении № 1 к Условиям ДБО;
- сохранять конфиденциальность информации относительно применяемых в Системе систем ограничения доступа к коммуникационному оборудованию Банка, обеспечения конфиденциальности, подлинности и авторства информации;
- своевременно и добросовестно выполнять условия Договора.

5.2. Права и обязанности Клиента.

5.2.1. Клиент вправе:

5.2.1.1. осуществлять с использованием Системы:

- Операции по Счету;
- операции с цифровыми рублями в порядке, установленном Условиями по операциям с ЦР;
- прием/передачу ЭД, указанных в п. 3.3 Условий ДБО;

5.2.1.2. получать с помощью Системы выписки о движении денежных средств по Счету и/или информацию, связанную с операциями с цифровыми рублями (в порядке, установленном Условиями по операциям с ЦР);

5.2.1.3. обращаться к сотрудникам технической поддержки Банка за получением консультаций, связанных с эксплуатацией Системы, в течение срока действия Договора;

5.2.1.4. в течение срока действия Договора в любое время прекратить передачу ЭД путем направления в Банк соответствующего уведомления. Уведомление должно быть предоставлено в письменной форме, подписано уполномоченным лицом Клиента и заверено печатью Клиента (при наличии);

5.2.1.5. самостоятельно осуществлять выпуск (генерацию) первых, вторых и последующих Ключей PayControl;

5.2.1.6. инициировать замену Ключей, Ключей PayControl в любой момент до истечения срока их действия;

5.2.1.7. хранить на одном Мобильном устройстве Ключи ЭП PayControl, самостоятельно выпущенные (сгенерированные) только одним уполномоченным лицом Клиента;

5.2.1.8. подать в Банк письменное заявление, оформленное на бумажном носителе и подписанное уполномоченным лицом Клиента (по форме Приложения № 13 к Условиям ДБО), с целью установления ограничений на совершение Клиентом Операций по Счету (-ам) с использованием Системы;

5.2.1.9. подать в Банк письменное заявление, оформленное на бумажном носителе и подписанное уполномоченным лицом Клиента (по форме Приложения № 14 к Условиям ДБО), с целью отмены установленных ограничений на совершение Клиентом Операций по Счету (-ам) с использованием Системы.

5.2.2. Клиент обязан:

5.2.2.1. самостоятельно контролировать исполнение расчетных ЭД, отправленных в Банк с использованием Системы, посредством контроля изменений Статуса документа;

5.2.2.2. за свой счет поддерживать в рабочем состоянии принадлежащие Клиенту аппаратные и программные средства, в том числе средства антивирусной защиты, используемые для функционирования Системы, Мобильное устройство, Мобильное приложение PayControl, а также обеспечить своевременное их обновление;

5.2.2.3. соблюдать инструкцию по обеспечению безопасности при использовании Системы (Приложение № 4 к Условиям ДБО);

5.2.2.4. обеспечить хранение материального носителя, содержащего Ключ ЭП или Ключ eToken PASS, или Мобильного устройства, содержащего Ключ ЭП PayControl, в месте, исключающем доступ неуполномоченных лиц и/или повреждение материального носителя/Мобильного устройства;

5.2.2.5. при хранении Ключа ЭП на сменном носителе (flash-карта, диск), исключить несанкционированный доступ к данному носителю;

5.2.2.6. исключить хранение Ключа ЭП на жёстком диске, в сетевых каталогах и прочих общедоступных ресурсах, за исключением Ключа ЭП, выпущенного в соответствии с Условиями по операциям с ЦР, подлежащего хранению на устройствах (хранилищах), прошедших аппаратную проверку при выпуске такого Ключа ЭП;

5.2.2.7. исключить передачу Логина, Пароля, Ключа eToken PASS, Одноразовых паролей, Одноразовых кодов, Ключей, Ключей PayControl, QR-кода, Аутентификационных данных (если это применимо) и их копий третьим лицам, а также их передачу по телефону, электронной почте или иным способом;

5.2.2.8. хранить Ключи ЭП PayControl на Мобильных устройствах (Мобильном устройстве), исключая несанкционированный доступ к Мобильному устройству (Мобильным устройствам);

5.2.2.9. инициировать получение нового QR-кода для формирования Ключа ЭП PayControl при смене Мобильного устройства, удалении Мобильного приложения PayControl, утрате Аутентификационных данных, для каждого самостоятельного выпуска (генерации) вторых и последующих Ключей PayControl, а также для выпуска (генерации) Ключей PayControl при смене Ключей PayControl, в том числе по требованию Банка;

5.2.2.10. при подозрении несанкционированного доступа третьих лиц к Счету, программно-аппаратным средствам Клиента, Ключу eToken PASS, Мобильному устройству, а также копирования или

подозрения в копировании Ключей, Ключей PayControl, третьими лицами или иной ситуации, которая приводит к Компрометации ключевой информации, с целью предотвращения финансовых потерь, незамедлительно любым доступным способом проинформировать об этом Банк (продублировав сообщение по электронной почте) и инициировать процедуру смены потенциально скомпрометированной Ключевой информации. По требованию Банка в случае подозрения у Банка в Компрометации ключевой информации осуществить смену Ключей, Ключей PayControl в срок 14 (четырнадцать) календарных дней с момента получения соответствующего уведомления от Банка;

5.2.2.11. по требованию Банка в течение 2 (двух) рабочих дней представить оригиналы документов, являющихся основанием для проведения валютной операции, либо копии указанных документов, заверенные лицом, имеющим право подписи расчетных документов, и печатью Клиента (при ее наличии);

5.2.2.12. соблюдать требования, установленные Условиями по операциям с ЦР, и правила платформы цифрового рубля, в том числе при направлении в Банк ЭД в целях совершения операций с цифровыми рублями, а также действий, связанных с использованием платформы цифрового рубля;

5.2.2.13. исполнять требования Банка, предусмотренные п. 5.3.1 Условий ДБО;

5.2.2.14. в случае прекращения действия Договора произвести удаление с аппаратных средств программного обеспечения и пользовательской документации, используемых при эксплуатации Системы.

5.2.3. Клиент гарантирует Банку, что все проводимые им с использованием Системы Операции по Счету, а также операции и действия, связанные со счетом цифрового рубля, в том числе открытие счета цифрового рубля, получение доступа к платформе цифрового рубля, совершение операций с цифровыми рублями носят легитимный характер, не нарушают законодательство Российской Федерации, нормативные акты государственных органов, в том числе Банка России, правила платформы цифрового рубля и не связаны с легализацией (отмыванием) доходов, полученных преступным путем, и финансированием терроризма.

5.3. Права и обязанности Банка.

5.3.1. Банк вправе:

5.3.1.1. приостановить совершение Клиентом Операций по Счету с использованием Системы в случаях и в порядке, установленных законодательством Российской Федерации (в том числе Федеральным законом от 07.08.2001 № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма», Федеральным законом от 27.06.2011 № 161-ФЗ «О национальной платежной системе»);

5.3.1.2. отказать в принятии или приостановить принятие ЭД Клиента в целях совершения операций с цифровыми рублями и/или в связи с использованием Клиентом платформы цифрового рубля, в порядке, установленном Условиями по операциям с ЦР, правилами платформы цифрового рубля;

5.3.1.3. приостановить использование Системы (приостановить доступ к Системе, и/или приостановить прием ЭД Клиента, и/или приостановить совершение Клиентом Операций по Счету с использованием Системы, и/или приостановить доступ Клиента к платформе цифрового рубля с использованием Системы, и/или приостановить совершение Клиентом операций с цифровыми рублями с использованием Системы) при наличии в базе данных Банка России о случаях и попытках осуществления переводов денежных средств без добровольного согласия клиента (далее – **База данных Банка России**) сведений, относящихся к Клиенту и/или Системе, на период нахождения таких сведений в Базе данных Банка России. При этом в случае получения Банком от Банка России информации об исключении сведений, относящихся к Клиенту и/или Системе, из Базы данных Банка России, Банк возобновляет использование Клиентом Системы при отсутствии иных оснований для приостановления использования Системы в соответствии с законодательством Российской Федерации, нормативными актами Банка России, в том числе правилами платформы цифрового рубля, Условиями ДБО, Условиями по операциям с ЦР, Условиями и/или Договором в целом. Банк направляет Клиенту уведомления, сообщения, решения, связанные с включением в Базу данных Банка России и исключением из неё сведений, относящихся к Клиенту и/или Системе, а также связанные с указанными в настоящем пункте (п. 5.3.1.3) Условий ДБО приостановлениями и возобновлениями использования Системы, любым из способов, указанных в п. 11.4 Условий, в случаях, когда обязанность по направлению Банком Клиенту таких уведомлений, сообщений, решений установлена законодательством Российской Федерации;

5.3.1.4. в случаях, предусмотренных действующим законодательством Российской Федерации, запрашивать у Клиента документы и сведения о проводимых/проведенных Операциях по Счету Клиента, и/или операциях с цифровыми рублями, осуществленных с использованием Системы. При этом обязательный срок для представления документов по запросам Банка составляет 3 (три) рабочих дня со дня получения Клиентом запроса Банка;

5.3.1.5. использовать инструменты контроля переводов Клиента на предмет компрометации Ключей, Ключа eToken PASS, Ключей PayControl Клиента по своему усмотрению;

5.3.1.6. при обнаружении Банком признаков (фактов) нарушения требований безопасности, установленных Условиями ДБО и/или Условиями по операциям с ЦР, немедленно приостановить прием ЭД Клиента, после чего любым доступным способом известить об этом Клиента;

5.3.1.7. в случае подозрения Компрометации ключевой информации по своему усмотрению блокировать Ключи ЭП, Ключ eToken PASS, Ключи PayControl Клиента и требовать от Клиента смены Ключей, Пароля, Ключа eToken PASS, Ключей PayControl или смену средства доступа к Системе (в том числе смену средств подписи для работы в Системе);

5.3.1.8. при необходимости, в том числе в случае изменения параметров ключевой информации, а также в целях реализации установленных законодательством Российской Федерации и/или нормативными актами Банка России требований к обеспечению защиты информации, в том числе при осуществлении переводов денежных средств, по своему усмотрению блокировать Ключи ЭП, Ключ eToken PASS, Ключи PayControl Клиента и требовать от Клиента смены Ключей, Пароля, Ключа eToken PASS, Ключей PayControl или смену средства доступа к Системе (в том числе смену средств подписи для работы в Системе);

5.3.1.9. требовать от Клиента использовать в рамках Договора определенный вид ЭП, предусмотренный Договором (Ключ ЭП, или Ключ eToken PASS, или Ключ ЭП PayControl, или иной криптографический ключ, предусмотренный Условиями по операциям с ЦР).

5.3.1.10. направлять Клиенту с использованием Системы рекламные материалы и информационные сообщения об услугах и продуктах Банка;

5.3.1.11. изменить в Системе Зарегистрированный номер на основании письменного заявления Клиента, оформленного на бумажном носителе и подписанного уполномоченным лицом Клиента.

5.3.2. Банк обязан (при наличии технической возможности у Клиента, Банка, платформы цифрового рубля, АО «НСПК»):

5.3.2.1. предоставлять Клиенту услуги с использованием Системы согласно Условиям ДБО, а также Условиям по операциям с ЦР;

5.3.2.2. произвести подключение и предоставление права доступа Клиента к Системе для совершения Операций и обмена документами в рамках Договора и иных договоров, заключенных между Банком и Клиентом, в соответствии с порядком, установленным в Приложении №3 к Условиям ДБО. Факт предоставления права доступа Клиента к Системе оформляется Актом о предоставлении права доступа и введении в действие Системы «Интернет-Банк» (Приложение №6 к Условиям ДБО), с момента подписания которого Клиент вправе осуществлять Операции и обмен документами с использованием Системы, за исключением случаев, когда иной порядок предоставления права доступа Клиента к Системе прямо предусмотрен настоящими Условиями ДБО и/или приложениями к ним;

5.3.2.3. предоставлять Клиенту необходимые рекомендации и методическую помощь в работе с Системой;

5.3.2.4. по требованию Клиента блокировать в Системе Пароль, активные Ключи проверки ЭП Клиента, активные Ключи eToken PASS, активные Ключи проверки ЭП PayControl, регистрировать новые Ключи, Ключи PayControl, временно блокировать работу Клиента в Системе.

6. ОТВЕТСТВЕННОСТЬ СТОРОН, РИСКИ

6.1. Стороны обязуются обеспечивать конфиденциальность сведений о технологии Системы и программного обеспечения Системы.

6.2. Клиент несет ответственность за все Операции, операции с цифровыми рублями и все действия, проводимые Клиентом при использовании Системы, а также за все действия, осуществляемые уполномоченными лицами Клиента в рамках Условий ДБО, Условий по операциям с ЦР и Договора в целом.

6.3. Банк не несёт ответственности за ущерб, возникший вследствие:

6.3.1. некорректного оформления Клиентом ЭД;

6.3.2. ошибочно переданных ЭД Клиентом в Банк;

6.3.3. несанкционированного доступа посторонних лиц к программно-аппаратным средствам, Паролю, Одноразовому паролю, Одноразовому коду, Ключу ЭП, Ключу eToken PASS, Ключу ЭП PayControl, Мобильному устройству и другой Ключевой информации и Аутентификационным данным, используемых Клиентом для осуществления обмена ЭД;

6.3.4. несанкционированного доступа посторонних лиц к Логину и/или Паролю при их предоставлении Банком в соответствии с Условиями ДБО (включая приложения к ним) на адрес электронной почты, указанный Клиентом (уполномоченным лицом Клиента), в том числе по причине несанкционированного доступа таких посторонних лиц к такому адресу электронной почты;

6.3.5. действия или бездействия оператора сотовой связи и/или интернет провайдера, либо иного третьего лица, при осуществлении Клиентом доступа к Системе при помощи Мобильного устройства и Мобильного приложения PayControl;

6.3.6. воздействия вредоносного программного обеспечения на программно-аппаратные средства, Мобильное устройство, используемые Клиентом для осуществления обмена ЭД, а также внесение любых изменений в Мобильное устройство, не предусмотренных производителем;

6.3.7. срывов и помех на линии связи, используемой Клиентом при работе с Системой;

6.3.8. невыполнения Клиентом предусмотренных Условиями ДБО требований Банка по смене Ключей, Пароля, Ключа eToken PASS, Ключей PayControl или по смене средства доступа к Системе.

6.4. В случае несоблюдения требований Договора, ответственность за негативные последствия несет Сторона, допустившая эти нарушения, в размере прямого ущерба, за исключением случаев, прямо предусмотренных Условиями ДБО.

6.5. Банк не несет ответственности за убытки, возникшие в результате неознакомления или несовременного ознакомления Клиентом со Статусами документа в Системе в порядке и сроки, установленные настоящими Условиями ДБО, а также за несоблюдение Клиентом мер по обеспечению защиты от несанкционированного доступа к информации.

6.6. Банк не контролирует, не проверяет, не дает одобрения и не несет какой-либо ответственности за дополнительные приложения, добавляемые Клиентом на свое Мобильное устройство, на котором установлено Мобильное приложение PayControl.

6.7. Урегулирование споров и конфликтов между Сторонами, возникших в отношении получения/обмена/исполнения ЭД осуществляется в порядке, предусмотренном Приложением № 8 к Условиям ДБО, за исключением ЭД, обмен которыми осуществляется в соответствии с Условиями по операциям с ЦР.

6.8. По всем вопросам, не урегулированным Условиями ДБО, Условиями по операциям с ЦР, Стороны руководствуются законодательством Российской Федерации, нормативными актами государственных органов, в том числе Банка России и Договором.

6.9. Составной и неотъемлемой частью Условий ДБО являются:

6.9.1. Приложение №1 – Требования к техническим средствам и оборудованию Клиента;

6.9.2. Приложение №2 – Порядок работы с Ключами, Сертификатом ключа проверки ЭП, Ключом eToken PASS, Ключами PayControl;

6.9.3. Приложение №3 – Порядок подключения и использования Системы «Интернет-банк»;

6.9.4. Приложение №4 – Инструкция по обеспечению безопасности;

6.9.5. Приложение №5 – Образец Сертификата ключа проверки ЭП;

6.9.6. Приложение №6 – Акт о предоставлениии права доступа и введении в действие Системы «Интернет-Банк» (форма);

6.9.7. Приложение № 7 – Письмо о смене Логина и Пароля (форма);

6.9.8. Приложение № 8 – Порядок урегулирования споров;

6.9.9. Приложение № 9 – Акт признания ключа подписи для обмена сообщениями (форма);

6.9.10. Приложение № 10 – Заявление на смену средства доступа к Системе (форма);

6.9.11. Приложение № 11 – Заявление на смену или предоставление нового QR-кода (форма);

6.9.12. Приложение № 12 – Заявление о регистрации уполномоченного лица Клиента (форма);

6.9.13. Приложение № 13 - Заявление об установлении ограничений на совершение Клиентом Операций по Счету (-ам) с использованием Системы (форма);

6.9.14. Приложение № 14 – Заявление об отмене установленных ограничений на совершение Клиентом Операций по Счету (-ам) с использованием Системы (форма);

6.9.15. Приложение № 15 – Условия предоставления информационного сервиса «Автоматизированная упрощенная система налогообложения.

Приложение №1
к Условиям дистанционного банковского обслуживания корпоративных клиентов

ТРЕБОВАНИЯ К ТЕХНИЧЕСКИМ СРЕДСТВАМ И ОБОРУДОВАНИЮ КЛИЕНТА

1. Для установки Системы необходимо обеспечить минимальные требования, предъявляемые к программно-аппаратному обеспечению, техническим средствам и оборудованию Клиента для установки и работы Системы (клиентская часть):

Локальный персональный компьютер следующей конфигурации:

- цветной дисплей и видео-адаптер с минимальной разрешающей способностью 1024x600 точек на дюйм;
- 32-разрядный (x86) или 64-разрядный (x64) процессор с тактовой частотой 1 ГГц или выше;
- оперативная память 1 ГБ (для 32-разрядного процессора) или 2 ГБ (для 64-разрядного процессора);
- 16 ГБ (для 32-разрядной системы) или 20 ГБ (для 64-разрядной системы) свободного места на жестком диске;
- графическое устройство DirectX 9 с драйвером WDDM 1.0 или более поздней версии;
- операционная система не позднее, чем Windows 7 x86/x64;
- наличие браузера Internet Explorer версии 11 и выше, или Mozila FireFox, Google Chrome, Opera;
- доступ к сети Интернет;
- средства антивирусной защиты.

Мобильное устройство (при использовании Клиентом для входа в Систему и обмена документами в Системе Ключа ЭП PayControl) в следующем режиме:

- на Мобильном устройстве установлены лицензионные, регулярно обновляемые (устанавливаются обновления безопасности) операционная система, антивирусное программное обеспечение.
- Мобильное устройство не подвергнуто операциям повышения привилегий/взлома операционной системы устройства (jail-break, rooting).
- Клиент использует Аутентификационные данные при доступе к Мобильному устройству.
- Версия Android – 5.0 и выше.
- Версия IOS – 11.0 и выше.
- Версия iPhone – iPhone 5S и выше.
- Версия iPad – iPad Air и выше, iPad Mini 2 и выше, iPad Pro и выше.

Оснащение Клиента вышеуказанными и иными, требующимися программами и техническими средствами осуществляется силами Клиента и за счет его средств.

2. Все перечисленное в п. 1. настоящего Приложения к Условиям ДБО оборудование Клиента должно иметь соответствующую техническую документацию.

Приложение №2
к Условиям дистанционного банковского обслуживания корпоративных клиентов

ПОРЯДОК РАБОТЫ С КЛЮЧАМИ, СЕРТИФИКАТОМ КЛЮЧА ПРОВЕРКИ ЭП, КЛЮЧОМ eToken PASS, КЛЮЧАМИ PayControl

1. Порядок работы с Ключами и Сертификатом ключа проверки ЭП

1.1. Банк предоставляет уполномоченному лицу Клиента доступ в Систему исключительно для генерации Ключа ЭП, а также документацию на Средства электронной подписи. Все работы со Средствами электронной подписи Стороны проводят в соответствии с документацией, содержащей описание процедур генерации Ключей, создания и контроля правильности Ключей и других предусмотренных Системой операций.
1.2. Клиент самостоятельно производит генерацию своей пары Ключей: Ключа ЭП и Ключа проверки ЭП. Запрос на Сертификат ключа проверки ЭП в электронном виде передается в Банк посредством Системы.
1.3. Банк, получив запрос на Сертификат ключа проверки ЭП от Клиента (в электронном виде), проводит сертификацию (регистрацию) Ключа проверки ЭП Клиента в Удостоверяющем центре.
1.4. После проведения сертификации (регистрации) Ключа проверки ЭП Клиенту направляется Сертификат ключа проверки ЭП в двух экземплярах на бумажном носителе, оформленный в соответствии с Приложением №5 к Условиям ДБО.
1.5. Клиент, получив от Банка свой Сертификат ключа проверки ЭП, должен убедиться, что Ключ проверки ЭП в Сертификате ключа проверки ЭП и в запросе на Сертификат ключа проверки ЭП совпадают.
1.6. Подписанные уполномоченным лицом и заверенные оттиском печати Клиента (при наличии) оригиналы Сертификата ключа проверки ЭП на бумажном носителе передаются в Банк (по почте либо курьером).
1.7. Экземпляр Сертификата ключа проверки ЭП, подписанный уполномоченным лицом и заверенный оттиском печати Удостоверяющего центра Банка, передается Клиенту (по почте либо курьером).
1.8. При первичном предоставлении Клиенту Ключей ввод в действие Ключей производится с даты подписания Банком и Клиентом Акта о предоставлении права доступа и введении в действие Системы «Интернет-Банк» в соответствии с Приложением №6 к Условиям ДБО.
1.9. В случае экстренной, плановой или внеочередной смены Сертификата ключа проверки ЭП для доступа в Систему «Интернет-Банк», ввод в действие Ключей производится после проведения Банком и Клиентом процедуры, описанной в п.п. 1.3 – 1.7 настоящего Приложения.
1.10. При смене по инициативе Клиента средства доступа к Системе, ввод в действие Ключей производится после предоставления в Банк заявления по форме Приложения № 10 к Условиям ДБО и проведения Банком и Клиентом процедуры, описанной в п.п. 1.3 – 1.7 настоящего Приложения.

2. Порядок работы с Ключами PayControl и QR-кодом

2.1. Банк предоставляет уполномоченному лицу Клиента доступ в Систему исключительно для генерации Ключей PayControl и подписания Акта признания ключа подписи для обмена сообщениями (Приложение № 9 к Условиям ДБО) в электронной форме, а также документацию на Средства электронной подписи. Все работы со Средствами электронной подписи Стороны проводят в соответствии с документацией, содержащей описание процедур генерации Ключей PayControl, создания и контроля правильности Ключей PayControl и других предусмотренных Системой операций.
2.2. Стороны пришли к соглашению, что в целях подписания электронной формы Акта признания ключа подписи для обмена сообщениями (Приложение № 9 к Условиям ДБО) в качестве ЭП Клиента используется Одноразовый код.
2.3. Клиент самостоятельно производит выпуск (генерацию) своей пары Ключей PayControl: Ключа ЭП PayControl и Ключа проверки ЭП PayControl. С использованием QR-кода из Системы, путем его сканирования с использованием функционала Мобильного приложения PayControl, Клиент записывает Ключ ЭП PayControl на Мобильное устройство. В случае выпуска (генерации) Клиентом второй и каждой последующей пары Ключей PayControl: Ключа ЭП PayControl и Ключа проверки ЭП PayControl, действия в соответствии с настоящим пунктом Клиент выполняет в отношении каждой такой пары Ключей PayControl.
2.4. После проведения Клиентом в соответствии с п. 2.3 настоящего Приложения записи Ключа ЭП PayControl на Мобильное устройство Банк направляет Клиенту в электронной форме Акт признания ключа подписи для обмена сообщениями, оформленный в соответствии с Приложением № 9 к Условиям ДБО, подписанный ЭП Ответственного сотрудника Банка, и Одноразовый код. В случае выполнения Клиентом в соответствии с п. 2.3 настоящего Приложения действий в отношении нескольких Ключей ЭП PayControl, Банк направляет Клиенту в электронной форме отдельные Акты признания ключа подписи для обмена сообщениями (Приложение № 9 к Условиям ДБО) и отдельные Одноразовые коды в отношении каждого такого Ключа ЭП PayControl.
2.5. Клиент подписывает (подтверждает) полученный(-ые) от Банка в соответствии с п. 2.4 настоящего Приложения Акт(-ы) признания ключа подписи для обмена сообщениями (Приложение № 9 к Условиям ДБО) ЭП Клиента (Одноразовым(-и) кодом(-ами)).
2.6. Каждый подписанный (подтвержденный) в соответствии с п. 2.5 настоящего Приложения с использованием ЭП Клиента (Одноразовым кодом) Акт признания ключа подписи для обмена сообщениями (Приложение № 9 к Условиям ДБО) передается в Банк посредством Системы.
2.7. При каждом первичном выпуске (генерации) Клиентом Ключей PayControl ввод в действие таких Ключей PayControl производится с даты получения Банком Акта признания ключа подписи для обмена сообщениями

(Приложение № 9 к Условиям ДБО), подписанного ЭП Клиента (Одноразовым кодом), при условии положительного результата проверки подлинности ЭП Клиента (Одноразового кода). В данном случае Банк предоставляет Клиенту право доступа к Системе для совершения Операций и обмена документами в рамках Договора и иных договоров, заключенных между Банком и Клиентом, без оформления и подписания Акта о предоставлении права доступа и введении в действие Системы «Интернет-Банк» (Приложением №6 к Условиям ДБО).

2.8. В случае экстренной, плановой или внеочередной смены Ключей PayControl для доступа в Систему «Интернет-Банк», ввод в действие таких Ключей PayControl производится после проведения Банком и Клиентом процедуры, описанной в п.п. 2.3 – 2.6 настоящего Приложения.

2.9. При смене средства доступа к Системе «Интернет-Банк», ввод в действие Ключей PayControl производится после предоставления в Банк заявления по форме Приложения № 10 к Условиям ДБО и проведения Банком и Клиентом процедуры, описанной в п.п. 2.3 – 2.6 настоящего Приложения.

2.10. Стороны пришли к соглашению, что Акт признания ключа подписи для обмена сообщениями (Приложение № 9 к Условиям ДБО) в электронной форме считается подписанным (подтвержденным) ЭП Ответственного сотрудника Банка/ЭП Клиента (Одноразовым кодом) и в том случае, когда такой Акт признания ключа подписи для обмена сообщениями подписан (подтвержден) соответственно одной ЭП Ответственного сотрудника Банка/ЭП Клиента (Одноразовым кодом), одновременно с другим связанным с ним ЭД, направленным с использованием Системы (включен с таким ЭД в один пакет Электронных документов).

2.11. В случае самостоятельного выпуска (генерации) первых, вторых и последующих Ключей PayControl, в том числе в случае выпуска (генерации) Ключей PayControl при смене средства доступа к Системе по требованию Банка в соответствии с Условиями ДБО, Клиент обязуется оплатить за свой счет услуги Банка по предоставлению Дистанционного банковского обслуживания с использованием первого, второго и каждого последующего Ключа ЭП PayControl в соответствии с Тарифами.

3. Порядок хранения, использования Ключевой информации, смена Ключей, Ключей PayControl, получение нового QR-кода

3.1. Режим хранения и использования Ключевой информации должен исключать возможность доступа к ней кого-либо, кроме уполномоченных лиц Сторон.

3.2. Сторона, допустившая возможность Компрометации ключевой информации, обязана немедленно сообщить об этом другой Стороне в порядке и в сроки, указанные в Условиях ДБО. Скомпрометированные Ключи, Ключи PayControl, QR-код не подлежат дальнейшему использованию и Стороны производят экстренную смену Ключей, Ключей PayControl, QR-кода.

3.3. Экстренная, внеочередная и плановая смена Ключей, Ключей PayControl производится Сторонами со следующей периодичностью:

- 3.3.1. плановая смена Ключей производится через 2 (два) года с даты их формирования;
- 3.3.2. плановая смена Ключей PayControl производится через 1 (один) год с даты их формирования;
- 3.3.3. экстренная смена Ключей Банка – при Компрометации ключевой информации Банка по решению Банка;
- 3.3.4. экстренная смена Ключей Клиента, Ключей PayControl – при Компрометации ключевой информации Клиента;
- 3.3.5. внеочередная смена Ключей Банка – по желанию Банка;
- 3.3.6. внеочередная смена Ключей Клиента, Ключей PayControl – по желанию Клиента или по требованию Банка в соответствии с Условиями ДБО.

3.4. В случае смены уполномоченных лиц Клиента Клиенту необходимо произвести смену Паролей, Ключей, Ключей PayControl, к которым такие уполномоченные лица имели доступ.

3.5. В случае смены Мобильного устройства, удалении Мобильного приложения PayControl, утрате Аутентификационных данных, необходимо произвести смену Ключей PayControl, получение нового QR-кода. При плановой/экстренной/внеочередной смене Ключей PayControl Клиенту необходимо получение нового QR-кода. При самостоятельном выпуске (генерации) вторых и последующих Ключей PayControl Клиенту также необходимо получение нового QR-кода (отдельно для каждых последующих Ключей PayControl).

3.6. В случае экстренной смены Ключей, Ключей PayControl/ внеочередной смены Ключей, Ключей PayControl, в том числе по требованию Банка в соответствии с Условиями ДБО, Клиент обязуется оплатить за свой счет услуги Банка по возобновлению предоставления Дистанционного банковского обслуживания в связи со сменой Ключей, Ключей PayControl, QR-кода в соответствии с Тарифами.

4. Порядок работы с Ключами eToken PASS

4.1. Использование Клиентом Ключа eToken PASS в Системе осуществляется на основании Заявления на регистрацию Ключа eToken PASS для использования в Системе, составленного по форме Банка, оформленного на каждое уполномоченное лицо Клиента.

4.2. Авторизация Клиента в Системе происходит по Логину и Паролю, дополнительная авторизация осуществляется путем ввода Одноразового пароля, сформированного Ключом eToken PASS.

4.3. Подпись ЭД в Системе осуществляется путем ввода Одноразового пароля, сформированного Ключом eToken PASS.

4.4. Отправка ЭД в Банк осуществляется путем ввода Одноразового пароля, сформированного Ключом eToken PASS.

5. Порядок хранения и использования Ключей eToken PASS

5.1. Режим хранения и использования Ключа eToken PASS должен исключать возможность доступа к Ключу eToken PASS кого-либо, кроме уполномоченного лица Клиента, на которого зарегистрирован такой Ключ eToken PASS.
5.2. В случае Компрометации ключевой информации Клиент обязан немедленно сообщить об этом в Банк в порядке и в сроки, указанные в Условиях ДБО.

ПОРЯДОК ПОДКЛЮЧЕНИЯ И ИСПОЛЬЗОВАНИЯ СИСТЕМЫ «ИНТЕРНЕТ-БАНК»

1. Подключение к Системе

1.1. Клиент обеспечивает наличие Рабочего места, отвечающего требованиям, изложенным в Приложении №1 к Условиям ДБО.

1.2. Банк производит необходимые настройки Системы. Действие указанных настроек будет распространяться на все операции Клиента в Системе, если Клиент дополнительно не представит в Банк заявление на ограничение указанных настроек в Системе.

1.3. Подключение к Системе производится Клиентом самостоятельно, с использованием инструкций по установке и настройке Системы, предоставленных ему Банком.

1.4. Банк:

1.4.1. в течение 3 (трех) рабочих дней с даты заключения Договора и/или на основании Заявления о регистрации уполномоченного лица Клиента, составленного Клиентом по форме Приложения №12 к Условиям ДБО и переданного в Банк, формирует для Клиента сочетание Логина и Пароля, зарегистрированное в Системе на имя каждого уполномоченного лица Клиента, являющееся для каждого такого уполномоченного лица Клиента уникальным и:

- обеспечивающее доступ каждого такого лица в Систему с режимом работы, предусмотренным в п. 1.5.7 настоящего Приложения; или
- обеспечивающее доступ каждого такого лица в Систему в сочетании с Ключом ЭП, либо Ключом eToken PASS, либо Ключом ЭП PayControl, либо Одноразовым кодом, сформированным для такого уполномоченного лица, либо с обязательной авторизацией иным согласованным Банком способом, - с соответствующим выбранным режимом работы, указанным в п. 1.5.1 - п. 1.5.6 настоящего Приложения (в зависимости от полномочий уполномоченного лица Клиента);

1.4.2. в течение 3 (трех) рабочих дней с даты заключения Договора передает документацию, содержащую описание процедур формирования Ключа ЭП, либо передает документацию, содержащую процедуру формирования Ключей ЭП PayControl, в зависимости от выбранного режима работы в соответствии с п. 1.5 настоящего Приложения.

1.5. В Системе возможны следующие режимы работы:

1.5.1. вход в Систему осуществляется по Логину и Паролю и с обязательной авторизацией с помощью Ключа ЭП, подпись и отправка ЭД осуществляется с помощью Ключа ЭП;

1.5.2. вход в Систему осуществляется по Логину и Паролю и с обязательной авторизацией путем ввода Одноразового пароля, сформированного Ключом eToken PASS, подпись и отправка ЭД осуществляется путем ввода Одноразового пароля, сформированного Ключом eToken PASS;

1.5.3. вход в Систему осуществляется по Логину и Паролю и с обязательной авторизацией с помощью Ключа ЭП PayControl, подпись и отправка ЭД осуществляется с помощью Ключа ЭП PayControl;

1.5.4. вход в Систему осуществляется по Логину и Паролю и с обязательной авторизацией с помощью Ключа ЭП без права подписи ЭД;

1.5.5. вход в Систему осуществляется по Логину и Паролю и с обязательной авторизацией путем ввода Одноразового кода для самостоятельного выпуска (генерации) Ключей PayControl и подписания Акта признания ключа подписи для обмена сообщениями (Приложение № 9 к Условиям ДБО) в электронной форме;

1.5.6. вход в Систему осуществляется по Логину и Паролю с обязательной авторизацией иным согласованным Банком способом;

1.5.7. вход в Систему осуществляется по Логину и Паролю без права подписи ЭД.

1.6. В случае намерения ограничить режим работы отдельных уполномоченных лиц Клиента возможностью подписания ЭД Клиент письменно информирует об этом Банк.

1.7. При необходимости Клиент вправе направить в Банк уведомление в произвольной форме с указанием списка IP-адресов, с которых Клиенту будет разрешен доступ в Систему, тем самым ограничивая доступ в Систему с других IP-адресов.

1.8. После подключения к Системе уполномоченные лица Клиента в течение срока действия Договора вправе получать/ самостоятельно выпускать (генерировать) первые, вторые и последующие Ключи PayControl в соответствии с Условиями ДБО и приложениями к ним.

1.9. В рамках Условий ДБО и Договора в целом Клиент (уполномоченные лица Клиента) вправе одновременно использовать несколько средств доступа к Системе для получения услуг по Дистанционному банковскому обслуживанию.

1.10. В случае прекращения действия Договора доступ Клиента к Системе аннулируется.

2. Электронный документооборот

2.1. Все документы в Системе «Интернет-Банк» представлены в электронном виде.

2.2. Ввод, обработка, прием и передача ЭД по Системе производится на специально оборудованных Рабочих местах Клиента и Банка.

2.3. Электронный документооборот между Клиентом и Банком осуществляется по открытым каналам передачи данных, в том числе с использованием сети Интернет.
2.4. Электронный документооборот осуществляется ежедневно 24 часа в сутки. Банк обязуется обеспечить функционирование своих технических средств и оборудования Системы в режиме ожидания взаимодействия с Клиентом.
2.5. Любые ЭД Клиента должны быть подписаны от имени Клиента Владельцем ЭП. Для ЭД Клиента в Системе предусмотрены следующие операции:

а) формирование и подписание;
б) отправка Банку с подтверждением получения;
в) возможность отзыва;
г) учет и хранение.

2.6. Исполнение расчетных ЭД при осуществлении переводов в рублях, поступивших и принятых к исполнению Банком, осуществляется:

- в тот же день, если ЭД поступил и принят Банком до 19-00 часов МСК;
- не позднее следующего рабочего дня, если ЭД поступил и принят Банком после 19-00 часов МСК.

Расчетные ЭД при осуществлении переводов в иностранной валюте, поступившие и принятые Банком текущим рабочим днём, исполняются Банком не позднее 3-го рабочего дня от даты поступления[1]».

При этом, для отдельных видов переводов, осуществляемых на основании соглашения, заключенного между Банком и Клиентом, могут быть предусмотрены иные порядок и сроки исполнения расчетных ЭД.
2.7. Датой получения Банком Документа валютного контроля считается:

- при поступлении Документа валютного контроля в Банк до 18-00 МСК - текущий рабочий день;
- при поступлении Документа валютного контроля в Банк после 18-00 МСК - следующий рабочий день;
- при поступлении Документа валютного контроля в Банк в выходной день/нерабочий праздничный день - следующий рабочий день.

2.8. Датой принятия Документов валютного контроля Банком в целях исполнения валютного законодательства РФ является дата присвоения в Системе Статуса документа «Принят ВК».
2.9. Датой отказа в приеме Документов валютного контроля Банком является дата присвоения в Системе Статуса документа «Отказан ВК».
2.10. Информация о факте постановки на учет/ принятия на обслуживание контрактов (кредитных договоров), изменения и/или дополнения сведений о контрактах (кредитных договорах), принятых на учет и иной учетной информации, снятие с учета контрактов (кредитных договоров) при переводе в другой уполномоченный банк, отказа постановки на учет/ принятия на обслуживание контрактов (кредитных договоров), принятия/возврата справки о подтверждающих документах доводится до Клиента путем изменения Статуса документа соответствующего ЭД в Системе. Порядок заполнения Документов валютного контроля уставлен Инструкцией 181-И.
2.11. Прием ЭД подтверждается электронным извещением Банка с указанием времени приема ЭД. При возникновении разногласий в правильности указания времени приема ЭД, Стороны признают, что временем приема является время приема ЭД по системным часам аппаратных средств Банка.
2.12. Клиент обязан удостовериться в получении Банком отправленных Клиентом ЭД:

- ЭД считается принятым Банком в случае изменения Статуса документа на «Принят», «Принят в обработку» по результатам автоматизированной проверки полученных Банком от Клиента ЭД;
- ЭД считается не принятым Банком в случае изменения Статуса документа на «Ошибка реквизитов», «Отвергнут банком», «Отказан АБС», «ЭП/АСП не верна» по результатам автоматизированной проверки полученных Банком от Клиента ЭД.

2.13. Банк не несет ответственность за неисправность каналов связи, используемых для взаимодействия Банка с Клиентом по Системе. Тем не менее, Банк обязуется принимать все возможные меры для устранения неисправности линий связи в кратчайшие сроки с момента их возникновения.
2.14. Все ЭД, подлежащие отправке от одной Стороны другой Стороне, перед установлением очередного сеанса связи между Клиентом и Банком подписываются ЭП Стороны, направляющей ЭД. Во время сеанса связи, подготовленные ЭД, по Системе передаются другой Стороне.
2.15. Все ЭД Банка формируются в соответствующем формате и подписываются ЭП Ответственного сотрудника Банка.
2.16. ЭД Банка загружаются Банком в Систему и могут быть получены Клиентом только в процессе соединения Клиента с Банком с использованием Системы. Надлежащей отправкой Клиенту ЭД Банка считается загрузка ЭД Банка в Систему, а датой отправки – дата загрузки.
2.17. В Системе предусмотрена операция присвоения Банком ЭД Клиента статуса приема/исполнения/отказа в исполнении, при этом при присвоении или изменении Статуса документа Система извещает Клиента о новом Статусе документа, информируя таким образом о состоянии ЭД.
2.18. Стороны признают, что срок действия Сертификата составляет 2 (два) года с даты его выдачи. Продление срока действия Сертификата осуществляется путем выдачи нового Сертификата с обязательной сменой Ключей. Выдача нового Сертификата производится по инициативе Клиента.
2.19. Стороны признают, что срок действия Ключа eToken PASS ограничен сроком работы элемента питания такого Ключа eToken PASS.

[1] Возможность осуществления перевода в иностранной валюте необходимо уточнять в Банке.

2.20. Стороны признают, что срок действия Ключа ЭП PayControl составляет 1 (один) год с даты его формирования. Продление предоставления Дистанционного обслуживания с использованием Ключа ЭП PayControl осуществляется путем самостоятельного выпуска (генерации) Клиентом нового Ключа ЭП PayControl с обязательной сменой Ключей PayControl. Выпуск (генерация) Клиентом нового Ключа ЭП PayControl производится по инициативе Клиента.
2.21. Доступ уполномоченного лица Клиента к Системе приостанавливается с момента окончания срока действия Сертификата/ Ключа eToken PASS/ Ключа ЭП PayControl такого уполномоченного лица Клиента и до момента оформления такому уполномоченному лицу Клиенту нового Сертификата/ нового Ключа ЭП PayControl. При этом доступ к Системе приостанавливается только для уполномоченных лиц Клиента, у которых закончился срок действия Сертификата/ Ключа eToken PASS/ Ключа ЭП PayControl. В течение этого срока такие уполномоченные лица Клиента не вправе проводить в Системе какие-либо операции, а Банк прекращает прием ЭД от таких уполномоченных лиц Клиента.
2.22. Стороны определили, что в течение срока действия Договора допускается временное приостановление Банком работы Системы по техническим причинам, но не более чем на 3 (три) часа в сутки.

3. Формирование, подписание, отправка и отзыв ЭД

3.1. Порядок формирования, заполнения, подписания и представления в Банк ЭД Клиента должен, помимо требований, установленных в Условиях ДБО, отвечать требованиям и условиям Договора (в том числе Условий и приложений к ним), а также того договора, во исполнение которого ЭД Клиента представляется в Банк.
3.2. Переданные в Банк ЭД Клиента, в том числе составленные в свободном формате, не требуют представления Клиентом в Банк их версий на бумажном носителе.
3.3. Порядок заполнения встроенных бланков при формировании ЭД Клиента предусматривает контроль Системы за наличием и корректностью информации в полях соответствующей формы, при этом обязательному контролю подлежат те реквизиты, при отсутствии которых исполнение Банком ЭД Клиента является невозможным. При наличии в Системе встроенного бланка для определенного вида ЭД формирование этого вида ЭД в свободном формате не допускается. Встроенный бланк может не содержать визуального отображения всех реквизитов, заявлений, инструкций и информации, предусмотренных стандартным бланком, использование которого предписано соответствующим договором для оформления аналогичного документа на бумажном носителе. При этом, передача в Банк ЭД Клиента, оформленного путем заполнения встроенного бланка, безусловно означает, что все дополнительные реквизиты, заявления, инструкции и информация, содержащиеся в тексте документа, выданы Клиентом Банку надлежащим образом.
3.4. Отзыв ЭД Клиента производится с использованием ЭД «Запрос на отзыв документа», специально предусмотренного в Системе для этих целей. Отправка в Банк отзыва ЭД Клиента, оформленного в свободном формате, не гарантирует своевременного прекращения Банком процедуры исполнения соответствующего ЭД Клиента. Если отзыв ЭД от Клиента получен Банком после того, как Банк исполнил содержащееся в нем поручение по распоряжению денежными средствами, Банк не несет ответственности за своевременно исполненное поручение Клиента, которое содержалось в полученном Банком ЭД.
3.5. При отсутствии в Системе встроенного бланка для ЭД какого-либо вида, ЭД формируется в свободном формате, а именно: а) в виде письма; б) в виде письма с прикрепленным файлом.
3.6. В случае если договором с Банком предусмотрено использование бланка, Клиент в обязательном порядке формирует ЭД в виде письма с прикрепленным файлом, при этом содержанием файла должен являться бланк, заполненный Клиентом в соответствии с требованиями соответствующего договора. Во всех остальных случаях вид ЭД свободного формата – просто письмо или просто с прикрепленным файлом – выбирается Клиентом по собственному усмотрению, если иное не предусмотрено соответствующим договором.
3.7. Сформированные ЭД Клиента подписываются уполномоченными лицами Клиента с использованием Ключей ЭП или Одноразового кода, Одноразового пароля Ключа eToken PASS или Ключей PayControl.
3.8. Факт доставки в Банк ЭД Клиента подтверждается статусом «Доставлен», который присваивается ЭД Системой при одновременном соблюдении следующих условий:

- ЭД подписан действующими ЭП уполномоченных лиц Клиента;
- ЭД передан Банку с использованием Системы.

3.9. Факт приема Банком ЭД Клиента подтверждается статусом «Принят», «Принят в обработку», который присваивается ему Системой, если перечисленные ниже проверки дают положительный результат:

- проверка ЭП Клиента;
- проверка наличия информации и корректности ее значений в полях ЭД, обязательных к заполнению.

В случае если хотя бы одно из перечисленных в предыдущем пункте условий не выполнено, присвоение Системой ЭД статуса «Принят» не производится, о чем Клиент автоматически извещается Системой.

4. Проверка ЭП

4.1. Проверка ЭП в ЭД, передаваемых Сторонами друг другу в Системе, осуществляется в соответствии с процедурой, описанной в документации на Систему.
4.2. Исходными данными для процедуры проверки ЭП являются:

- ЭД, переданный одной из Сторон в формате Системы и подписанный ее ЭП;
- Сертификат ключа проверки ЭП, или Сертификат ЦР, или Ключ eToken PASS, или Ключи PayControl Стороны, подписавшей ЭД, или Одноразовый код.

4.3. Электронная подпись в ЭД, передаваемых Сторонами в Системе, признается действительной при одновременном соблюдении следующих условий:

- Сертификат ключа проверки ЭП/Сертификат ЦР выпущен Удостоверяющим центром;
- Сертификат ключа проверки ЭП/Сертификат ЦР действителен на момент подписания ЭД;
- положительный результат проверки принадлежности Сертификата ЭП/Сертификата ЦР Участнику Системы;
- положительный результат проверки Одноразового кода, сформированного Ключа eToken PASS Уполномоченного лица Клиента;
- положительный результат проверки Одноразового кода;
- подтверждено отсутствие изменений, внесенных в ЭД после его подписания;
- при прохождении всех уровней крипто контроля PayControl (на основании 4-х составляющих, привязка к реквизитам платежа, времени его создания, Ключа ЭП PayControl и расчету хэш-функций Мобильного устройства и уникального IMEI номера).

4.4. Проверка ЭП, созданной посредством использования Ключа ЭП, осуществляется Средством электронной подписи «Крипто-Ком», используемым в соответствии с Условиями ДБО, или Средством электронной подписи, предусмотренным Условиями по операциям с ЦР.

4.5. Сертификат ключа проверки ЭП, используемый при проверке ЭП, должен соответствовать форме Сертификата по форме, установленной Приложением №5 Условий ДБО.

4.6. Ключ ЭП PayControl, используемый при проверке ЭП, должен соответствовать идентификатору ключа в форме Акта признания ключа подписи для обмена сообщениями, установленной Приложением № 9 Условий ДБО.

5. Смена или предоставление нового Пароля и Логина, QR-кода

5.1. Смена Пароля и/или Логина уполномоченного лица Клиента в случаях, установленных Условиями ДБО, осуществляется:

5.1.1. на основании письма о смене Логина и Пароля, составленного Клиентом по форме Приложения № 7 к Условиям ДБО и/или по иной согласованной Банком форме и переданного в Банк;

5.1.2. в случае если уполномоченное лицо Клиента является также Держателем[2] – при обращении такого Держателя в Call-Центр Русский Стандарт (при условии правильного сообщения Держателем Кодов доступа и наличия у Банка технической возможности) с просьбой смены Пароля и/или Логина, зарегистрированного(-ых) в Системе на имя такого Держателя. В указанном случае предоставление Логина и/или Пароля, соответственно, осуществляется Банком на адрес электронной почты, указанный Держателем при обращении за сменой Логина и/или Пароля по телефону в Call-Центра Русский Стандарт, при условии успешной верификации такого адреса электронной почты в соответствии с внутренними процедурами, установленными Банком.

5.2. Предоставление нового Пароля и/или Логина уполномоченного лица Клиента в случаях, установленных Условиями ДБО, осуществляется на основании Заявления о регистрации уполномоченного лица Клиента, составленного Клиентом по форме Приложения № 12 к Условиям ДБО и переданного в Банк.

5.3. Смена или предоставление нового QR-кода в случаях, установленных Условиями ДБО, осуществляется на основании Заявления на смену или предоставление нового QR-кода, составленного Клиентом по форме Приложения № 11 к Условиям ДБО, или Заявления о регистрации уполномоченного лица Клиента, составленного Клиентом по форме Приложения № 12 к Условиям ДБО, и переданного в Банк.

6. Хранение ЭД

6.1. Стороны осуществляют хранение всех входящих и исходящих ЭД в Системе.

6.2. Клиент обязуется хранить не менее 5 (пяти) лет Ключи, Ключ eToken PASS, Ключи PayControl, используемые в рамках Условий ДБО. Сроки хранения ЭД должны соответствовать срокам хранения, установленным для документов на бумажных носителях. Архивы подлежат защите от несанкционированного доступа, непреднамеренного или преднамеренного уничтожения и/или искажения.

6.3. Банк формирует и хранит не менее 5 (пяти) лет (а в случае возникновения споров – до их разрешения) архивы:

6.3.1. всех входящих ЭД в принятом виде с ЭП;

6.3.2. всех исходящих ЭД в исходном виде с ЭП;

6.3.3. извещений (в электронном виде с ЭП) о приеме ЭД;

6.3.4. сообщений свободного формата, подписанных ЭП;

6.3.5. электронных протоколов сеансов обмена информацией.

6.4. Банк обязуется хранить не менее 5 (пяти) лет Ключи, используемые в рамках Условий ДБО. Сроки хранения ЭД должны соответствовать срокам хранения, установленным для документов на бумажных носителях. Архивы подлежат защите от несанкционированного доступа, непреднамеренного или преднамеренного уничтожения и/или искажения.

[2] Термины «Держатель», «Коды Доступа» имеют в настоящем пункте 5.1.2 настоящего Приложения те же значения, что и в Условиях предоставления и обслуживания корпоративной карты и в Условиях предоставления и обслуживания корпоративной кредитной карты, являющихся неотъемлемой частью Условий.

Приложение № 4
к Условиям дистанционного банковского обслуживания корпоративных клиентов

ИНСТРУКЦИЯ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ

1. Системы ограничения доступа и защиты информации

1.1. Для обеспечения безопасности использования Системы каждой из Сторон должен быть определен и утвержден:
- 1.1.1. порядок учета, хранения и использования носителей Ключевой информации, который должен полностью исключать возможность несанкционированного доступа к ним;
- 1.1.2. порядок доступа и работы на персональном компьютере с Системой, который должен полностью исключать возможность несанкционированного доступа к Системе и носителю Ключевой информации; список лиц, имеющих доступ к Системе с разграничением прав доступа.

1.2. Ключи хранятся на сменных носителях у каждой из Сторон. Каждая из Сторон несет полную ответственность за сохранность, конфиденциальность и подлинность своего комплекта Ключей.
1.3. Ключ eToken PASS является автономным устройством и хранится в соответствии с п. 5.2.2.4 Условий ДБО. Клиент несет полную ответственность за сохранность, конфиденциальность каждого Ключа eToken PASS.
1.4. Ключи PayControl хранятся на Мобильном устройстве Клиента.
1.5. Все работы по выработке и смене Ключей производятся в соответствии с порядком работы с Ключами и Сертификатом ключа проверки ЭП, указанным в Приложении №2 к Условиям ДБО.
1.6. Все работы по выработке и смене Ключей PayControl производятся в соответствии с порядком работы с Ключами PayControl и QR-кодом, указанным в Приложении №2 к Условиям ДБО.
1.7. Доступ неуполномоченных лиц к носителям Ключевой информации должен быть исключен.
1.8. По окончании рабочего дня, а также вне времени составления и обмена ЭД, носители секретных Ключей, Ключ eToken PASS, должны храниться в, недоступном для неуполномоченных лиц, месте.
1.9. Не допускается:
- 1.9.1. снимать несанкционированные копии с ключевых носителей;
- 1.9.2. знакомить с содержанием ключевых носителей или передавать ключевые носители лицам, к ним не допущенным;
- 1.9.3. выводить секретные Ключи на дисплей (монитор) персонального компьютера или принтер;
- 1.9.4. устанавливать носитель Ключевой информации в считывающее устройство (дисковод) локального персонального компьютера в режимах, не предусмотренных функционированием Системы, а также в другие персональные компьютеры;
- 1.9.5. записывать на носитель Ключевой информации постороннюю информацию;
- 1.9.6. передавать Одноразовый код и/или Одноразовый пароль Ключа eToken PASS неуполномоченным лицам;
- 1.9.7. сообщать кому-либо Аутентификацонные данные;
- 1.9.8. использование с Ключами PayControl Мобильного устройства, приобретенного не у официального продавца и не сертифицированного по требованиям ГОСТ в соответствии с действующим законодательством для использования на территории Российской Федерации;
- 1.9.9. использование на Мобильном устройстве, применяемом для подключения к Системе, нелицензионного программного обеспечения;
- 1.9.10. устанавливать Мобильное приложение PayControl не из официальных репозитариев AppStore и Google Play.

1.10. Банк имеет право производить замену средств защиты информации и других программных или аппаратных средств, используемых при обмене ЭД, о чем уведомляет Клиента не менее чем за 30 (тридцать) дней. Клиент обязан в соответствующий срок приобрести за свой счет необходимые программно-технические средства и подготовить их ввод в действие в соответствии с рекомендациями Банка.

2. Процедура обмена информацией между Банком и Клиентом

2.1. Для обеспечения безопасности и конфиденциальности обмена ЭД в Системе используются специальные процедуры, включающие:
- 2.1.1. формирование ЭП, предназначенной для обеспечения подтверждения подлинности ЭП в ЭД. ЭП жестко увязывает в одно целое содержание документа и Ключ ЭП, или Ключ eToken PASS, или Ключ ЭП PayControl уполномоченных лиц Сторон и делает невозможным изменение ЭД без нарушения подлинности данной ЭП;
- 2.1.2. использование Паролей/ Одноразовых паролей/ Одноразовых кодов/ Аутентификационных данных для ограничения доступа к Системе.

2.2. Процесс обмена ЭД происходит в следующем порядке:
- 2.2.1. Сторона-отправитель формирует документы и ставит под ними ЭП Владельца ЭП/Ответственного сотрудника Банка;
- 2.2.2. документы передаются по защищенному каналу связи Стороне-получателю;
- 2.2.3. Сторона-получатель проверяет в принятых ЭД их ЭП. Если проверка ЭП под ЭД с применением Ключей проверки ЭП другой Стороны подтверждает их авторство и подлинность, то такие ЭД принимаются Стороной-получателем в качестве документов, поступивших от противоположной Стороны. В противном случае ЭД не принимаются Стороной-получателем в качестве документов, поступивших от противоположной

Стороны, о чем Сторона-отправитель уведомляется посредством формирования соответствующего статуса о неприеме ЭД после автоматизированной обработки ЭД в Системе;

2.2.4. Банк проверяет в принятых ЭД их ЭП, сформированную с использованием Ключа eToken PASS Клиента. Если проверка ЭП, сформированной с использованием Одноразового пароля Ключа eToken PASS, введенного Клиентом подтверждает авторство и подлинность, то такие ЭД принимаются Банком в качестве документов, поступивших от Клиента. В противном случае ЭД не принимаются Банком в качестве документов, поступивших от Клиента, о чем Банк уведомляется Клиента посредством формирования соответствующего статуса о неприеме ЭД после автоматизированной обработки ЭД в Системе;

2.2.5. Банк проверяет в принятых ЭД их ЭП, сформированную с использованием Одноразового кода. Если проверка ЭП, сформированной с использованием Одноразового кода, введенного Клиентом, подтверждает авторство и подлинность, то такие ЭД принимаются Банком в качестве документов, поступивших от Клиента. В противном случае ЭД не принимаются Банком в качестве документов, поступивших от Клиента, о чем Банк уведомляется Клиента посредством формирования соответствующего статуса о неприеме ЭД после автоматизированной обработки ЭД в Системе;

2.2.6. Банк проверяет в принятых ЭД их ЭП, сформированную с использованием Ключей PayControl Клиента. Если проверка ЭП, сформированной с использованием Ключей PayControl Клиента подтверждает авторство и подлинность, то такие ЭД принимаются Банком в качестве документов, поступивших от Клиента. В противном случае ЭД не принимаются Банком в качестве документов, поступивших от Клиента, о чем Банк уведомляет Клиента посредством формирования соответствующего статуса о неприеме ЭД после автоматизированной обработки ЭД в Системе.

2.3. Подлинность и авторство информации обеспечивается применением ЭП.

2.3.1. Для формирования Неквалифицированной электронной подписи используется сертифицированное ФСБ РФ Средство электронной подписи «Крипто-Ком». Ключи ЭП Клиента генерируются в соответствии с порядком работы с Ключами и Сертификатом ключа проверки ЭП, указанным в Приложение № 2 к Условиям ДБО.

2.3.2. Для формирования Простой электронной подписи используются уникальные Одноразовые пароли, формируемые с помощью Ключа eToken PASS для подписи документов, генерируются в соответствии с индивидуальным алгоритмом каждого Ключа eToken PASS, или Одноразовые коды;

2.3.3. Коды подтверждения транзакции, вырабатываемые PayControl, формируются на основании 4-х составляющих, привязка к реквизитам платежа, времени его создания, Ключа ЭП PayControl и расчету хэш-функций Мобильного устройства и уникального IMEI номера.

Приложение № 5

к Условиям дистанционного банковского обслуживания корпоративных клиентов

Образец Сертификата ключа проверки ЭП

```
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number:
      :xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:
    Signature Algorithm: :xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:
    Issuer: C=xx, L=xxxxxxxxx, O=xxxxxxxxxxxxxxxxxxxxxx, T=xxxxxxxxxxxxxxxxxxxx, CN=xxxxxxxxxxxxxxxxxxxxxxxxxxxx,
Email=xxxxxx@xxxxxx.xx
    Validity
      Not Before: Month  Date Time Year GMT
      Not After : Month  Date Time Year GMT
    Subject: C=xx, SP=xxxxxxxxx, L=xxxxxxxxx, O=xxxxxxxxxxxxxxxxxxxxxx, T= xxxxxxxxxxxxxxxxxxxxxx,
CN= xxxxxxxxxxxxxxxxxxxxxx, Email= xxxxxx@xxxxxx.xx
    Subject Public Key Info:
      Public Key Algorithm: xxxxxxxxxxxxxxxxxxxxxx
      Public Key:
        pub:
          xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:
          xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:
          xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:
          xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:
          xx:xx:xx:xx
        Parameters OID: xxxxxxxxxxxxxxxxxxxxxx
    X509v3 extensions:
      Subject Key Identifier:
        xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx
      Authority Key Identifier:
        DirName:C=xx, L=xxxxxxxxx, O=xxxxxxxxxxxxxxxxxxxxxx, OU=xxxxxxxxxxxxxxxxxxxxxx,
T=xxxxxxxxxxxxxxxxxxxxxx, CN=xxxxxxxxxxxxxxxxxxxxxx, Email=xxxxxx@xxxxxx.xx
        serial:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx

      Key Usage:
        Digital Signature, Non Repudiation, Key Encipherment, Data Encipherment, Key Agreement, Certificate Sign, CRL Sign
  Signature Algorithm: xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
    xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:
    xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:
    xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:
    xx:xx:xx:xx:xx:xx:xx:xx:xx:xx

-----BEGIN CERTIFICATE-----
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxx
-----END CERTIFICATE-----
```


Начальник Корпоративного
удостоверяющего центра ___________________ ( )
подпись Ф.И.О.

Владелец сертификата (уполномоченное лицо) ___________________ ( )
подпись Ф.И.О.

Подпись владельца сертификата (уполномоченного лица) заверяю:

КЛИЕНТ

_____________________________/____________________/

подпись *Ф.И.О.*

М.П. (при наличии)

Приложение № 6
к Условиям дистанционного банковского обслуживания корпоративных клиентов

ФОРМА

АКТ
о предоставлении права доступа и введении в действие Системы «Интернет-Банк»

г._____ «__» _____20_ _г.

АО «Банк Русский Стандарт», именуемое в дальнейшем «**Банк**», в лице_____, действующего на основании_____, с одной стороны, и _____, именуемое в дальнейшем «**Клиент**», в лице_____, действующего на основании_____, с другой стороны, именуемые вместе в дальнейшем «**Стороны**», составили настоящий Акт о предоставлении права доступа и введении в действие Системы «Интернет-Банк» (далее – **Акт**) о нижеследующем:

1. Банком произведена регистрация Клиента в Системе.

2. Банк предоставил Клиенту Логин и Пароль для доступа к Системе «Интернет-Банк».

3. Банк передал, а Клиент принял Сертификат(-ы) ключа проверки ЭП.

Клиент подтверждает, что ознакомлен с порядком работы в Системе «Интернет-Банк» с использованием выбранного(-ых) им из вышеперечисленных средств доступа к Системе «Интернет-Банк».

4. Программное обеспечение Рабочего места признано Сторонами работоспособным и принято Клиентом в эксплуатацию с «___» __20__г. С указанной даты Стороны обязуются выполнять обязательства, предусмотренные Условиями ДБО.

5. Программное обеспечение Рабочего места Клиента считается принятым в эксплуатацию с момента подписания настоящего Акта Сторонами. Все корректно оформленные документы, переданные с использованием Системы «Интернет-Банк», начиная с даты подписания настоящего Акта, будут иметь юридическую силу.

6. Стороны претензий к друг другу не имеют.

7. Настоящий Акт составлен в 2 (Двух) экземплярах, имеющих одинаковую юридическую силу, по одному экземпляру для каждой из Сторон и является неотъемлемой частью Условий.

ПОДПИСИ СТОРОН

БАНК	**КЛИЕНТ**
_____/_____/	_____/_____/
подпись *Ф.И.О.*	*подпись* *Ф.И.О.*
М.П. (при наличии)	М.П. (при наличии)

Приложение № 7
к Условиям дистанционного банковского обслуживания корпоративных клиентов

ФОРМА

В АО «Банк Русский Стандарт»

от _____
(наименование Клиента)

Дата: _____
(формат ДД.ММ.ГГГГ)

Письмо о смене Логина и Пароля

Просим прислать на электронную почту *@*.* новые учетные данные уполномоченному лицу Клиента _____ (*Ф.И.О.*) для входа в Систему «Интернет-Банк» в связи с _____ (*указывается причина смены Логина и/или Пароля*).

- ☐ Логин
- ☐ Пароль

Должность руководителя _____ / _____/
подпись *Ф.И.О.*

М.П. (при наличии)

Приложение № 8

к Условиям дистанционного банковского обслуживания корпоративных клиентов

ПОРЯДОК УРЕГУЛИРОВАНИЯ СПОРОВ

1.1. Все споры и разногласия, возникающие при исполнении Условий ДБО, Стороны будут стремиться разрешать путем переговоров. На время разрешения спорной ситуации Стороны имеют право приостановить доступ в Систему, уведомив об этом другую Сторону в день приостановки доступа в Систему посредством отправки соответствующего ЭД с использованием Системы с обязательным его дублированием на бумажном носителе в срок не позднее следующего рабочего дня со дня отправки такого ЭД. Соответствующее уведомление на бумажном носителе должно быть подписано уполномоченным лицом и заверено оттиском печати (при наличии) соответствующей Стороны.

При возникновении спора между Клиентом и Банком о факте получения одной Стороной ЭД, направленного другой Стороной, доказательством получения ЭД является изменение в Системе Статуса документа такого ЭД.

1.2. Разбор конфликтных ситуаций о подлинности ЭП под ЭД заключается в доказательстве принадлежности ЭП конкретного ЭД, соответствующему уполномоченному лицу Клиента или Банка. Разбор основывается на математических свойствах алгоритмов, гарантирующих невозможность подделки значения ЭП любым лицом, не обладающим Ключом ЭП или Ключом eToken PASS или Ключом ЭП PayControl.

1.3. При не урегулировании между Сторонами возникшего спора, до обращения одной из Сторон в суд, Сторона – инициатор спора в течение 3 (трех) рабочих дней с момента направления спорного ЭД осуществляет подготовку и направляет другой Стороне заявление с использованием Системы с подробным изложением обстоятельств происшедшего и предложением создать комиссию. В случае приостановления доступа к Системе такое заявление направляется на бумажном носителе, подписывается уполномоченным лицом и заверяется оттиском печати (при наличии) соответствующей Стороны. Создание Сторонами указанной комиссии является досудебным претензионным порядком урегулирования спора.

1.4. В предложении о создании комиссии указывается предлагаемые место сбора комиссии, дата и время. Окончательные место, дата и время сбора комиссии определяется по согласованию Сторон не позднее 7 (семи) календарных дней с момента получения предложения о создании комиссии Стороной, в адрес которой такое предложение было направлено.

1.5. В случае если другая Сторона не согласна с существом претензий и не намерена участвовать в работе комиссии, то эта Сторона должна ответить в письменной форме Стороне – инициатору спора не позднее 3 (трех) рабочих дней с момента получения предложения о создании комиссии об отказе в ее участии.

1.6. В состав комиссии должно входить равное количество представителей от каждой Стороны (не менее 2 (двух) представителей от каждой Стороны). В случае рассмотрения спора в отношении ЭД, подписанного Ключом ЭП, при необходимости, с письменного согласия обеих Сторон, в состав комиссии могут быть дополнительно включены специалисты организации-разработчика программного обеспечения Message Pro (разработчик АО «СИГНАЛ-КОМ»). В случае рассмотрения спора в отношении ЭД, подписанного Ключом ЭП PayControl, при необходимости, с письменного согласия обеих Сторон, в состав комиссии могут быть дополнительно включены специалисты организации-разработчика программного обеспечения АРМ РКС PayControl. В случае привлечения независимых специалистов их услуги оплачивает Сторона, признанная виновной.

1.7. Стороны предоставляют комиссии следующие документы и материалы:

1.7.1. затребованные Сертификаты на магнитном и бумажном носителях;

1.7.2. подписанный ЭП ЭД, по которому предъявляются претензии;

1.7.3. Мобильное устройство.

1.8. Комиссия в двухнедельный срок проводит разбор конфликтной ситуации и по итогам работы составляет акт в двух экземплярах для каждой Стороны (в случае рассмотрения комиссией спора в отношении ЭД, подписанного Ключом ЭП и привлечения в состав комиссии специалистов организации-разработчика программного обеспечения Message Pro (разработчик АО «СИГНАЛ-КОМ»), а также в случае рассмотрения комиссией спора в отношении ЭД, подписанного Ключом ЭП PayControl и привлечения в состав комиссии специалистов организации-разработчика программного обеспечения АРМ РКС PayControl – составляется третий экземпляр акта) с указанием существа конфликта, виновной Стороны и сроков устранения конфликтной ситуации.

Для разрешения спора в отношении ЭД, подписанного Ключом ЭП, с целью подтверждения подлинности ЭП в ЭД, используется программное обеспечение Arbiter-PKI (разработчик АО «СИГНАЛ-КОМ»), соответствующее требованиям Федерального закона от 06.04.2011 №63-ФЗ «Об электронной подписи». Процедура проверки ЭП в ЭД производится в соответствии с документацией на указанное программное обеспечение.

Для разрешения спора в отношении ЭД, подписанного с использованием Ключа eToken PASS, с целью подтверждения подлинности ЭП в ЭД, используются внутренние средства Системы.

Для разрешения спора в отношении ЭД, подписанного Ключом ЭП PayControl, с целью подтверждения подлинности ЭП в ЭД, используется программное обеспечение АРМ РКС PayControl. Процедура проверки ЭП в ЭД производится в соответствии с документацией на указанное программное обеспечение.

1.9. Порядок разрешения конфликта, если одна Сторона отрицает, что передавала второй Стороне спорный ЭД:

1.9.1. если вторая Сторона не может предъявить копию спорного ЭД – конфликт решается в пользу первой Стороны;

1.9.2. если вторая Сторона предъявляет копию спорного ЭД, подписанного первой Стороной:

1.9.2.1. подпись первой Стороны подтверждается в соответствии с п. 1.8 настоящего Приложения – конфликт решается в пользу второй Стороны;

1.9.2.2. подпись первой Стороны не подтверждается в соответствии с п. 1.8 настоящего Приложения – конфликт решается в пользу первой Стороны.

1.10. Порядок разрешения конфликта, если одна Сторона утверждает, что исполненный второй Стороной спорный ЭД не соответствует переданному ЭД:

1.10.1. если вторая Сторона не может предъявить копию спорного ЭД – конфликт решается в пользу первой Стороны;

1.10.2. если вторая Сторона предъявляет копию спорного ЭД, спорный ЭД проверяется в соответствии с п. 1.8 настоящего Приложения:

1.10.2.1. подпись первой Стороны подтверждается – конфликт решается в пользу второй Стороны;

1.10.2.2. подпись первой Стороны не подтверждается – конфликт решается в пользу первой Стороны.

Если все предпринятые меры по добровольному урегулированию спора не принесут удовлетворяющего обе Стороны результата, либо одна из Сторон откажется от участия в комиссии, либо Стороны не смогут в течение 7 (семи) рабочих дней с даты получения одной из Сторон предложения о создании комиссии другой Стороне определить дату сбора комиссии, либо в даты сбора комиссии комиссия не будет собрана, либо лица, прибывшие для участия в ней, не будут наделены полномочиями от Стороны, их направившей на участие, в работе комиссии, принятие решений, подписание актов, указанных в п. 1.8 настоящего Приложения, то обязательный досудебный претензионный порядок считается соблюденным Сторонами и спор подлежит разрешению в Арбитражном суде г. Москвы (Российская Федерация) в порядке, предусмотренном Арбитражно-процессуальным кодексом Российской Федерации.

Приложение № 9
к Условиям дистанционного банковского обслуживания корпоративных клиентов

ФОРМА

Документ из банка № X от «ДД» мммм ГГГГ г.

«АКТ ПРИЗНАНИЯ КЛЮЧА ПОДПИСИ ДЛЯ ОБМЕНА СООБЩЕНИЯМИ»
для

XXXXXXXXXXXXXXX
(наименование организации)

Текст заявления клиента:

Акт признания ключа подписи для обмена сообщениями. Я, нижеподписавшийся, уполномоченный представитель Клиента XXXXXXXXXXXXXXX, 77XXXXXXX7 ФИО составил настоящий акт о том, что мною самостоятельно выпущен и получен ключ PayControl XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXX, открытый ключ XX XX XX XX XX X XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX со сроком действия с ДД.ММ.ГГГГ по ДД.ММ.ГГГГ. Личная подпись владельца ключа PayControl: ФИО

Дополнительная информация:

Наименование организации	XXXXXXXXXXXXXXX
ИНН организации	XXXXXXX
ФИО владельца ключа	ФИО
Дата начала срока действия ключа	ДД.ММ.ГГГГ
Дата окончания срока действия ключа	ДД.ММ.ГГГГ
Идентификатор ключа:	XXXXXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX
Публичный ключ	XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX
Уполномоченное лицо	XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX

Заполняется сотрудником Банка

Документ получен Банком, предоставленные Клиентом сведения проверил:

(фамилия и инициалы) (подпись)

Дата обработки: ДД.ММ.ГГГГ

От клиента:

ФИО подписанта	Тип криптографии	Тип подписи	Дата и время подписи	Серийный номер сертификата
ФИО, должность	OneTimePassword	Единственная	xxxx-xx-xx xx:xx:xx	

От банка:

ФИО подписанта	Тип криптографии	Тип подписи	Дата и время подписи	Серийный номер сертификата
Акционерное общество "Банк Русский Стандарт"	Message-PRO	Технологическая	xxxx-xx-xx xx:xx:xx	xxxxxxxxxxxxxxxxxx

Приложение № 10
к Условиям дистанционного банковского обслуживания корпоративных клиентов

ФОРМА

В АО «Банк Русский Стандарт»

от _____
(наименование Клиента)

Дата: _____
(формат ДД.ММ.ГГГГ)

Заявление на смену средства доступа к Системе

Прошу провести соответствующие настройки по смене средства доступа к Системе для уполномоченного лица Клиента: _____
ФИО

Использовать следующее средство подписи для работы в Системе:

- ☐ Ключ ЭП
- ☐ Ключ ЭП PayControl

Должность руководителя _____ / _____/
подпись *Ф.И.О.*

М.П. (при наличии)

Приложение № 11
к Условиям дистанционного банковского обслуживания корпоративных клиентов

ФОРМА

В АО «Банк Русский Стандарт»

от _____
(наименование Клиента)

Дата: _____
(формат ДД.ММ.ГГГГ)

Заявление на смену или предоставление нового QR-кода

Просим предоставить посредством Системы «Интернет-Банк» новый QR-код для формирования Ключей ЭП PayControl для уполномоченного лица Клиента _____ (Ф.И.О.), Зарегистрированный номер _____ в связи:

□ *со сменой Мобильного устройства/*

□ *с удалением Мобильного приложения PayControl/*

□ *с утратой Аутентификационных данных*

□ *с необходимостью генерации очередной пары Ключей PayControl для указанного уполномоченного лица Клиента*

(указать причину смены или получения нового QR-кода)

□ *с экстренной/внеплановой сменой Ключей PayControl*

□ *с плановой сменой Ключей PayControl*

□ Просим изменить в Системе Зарегистрированный номер уполномоченного лица Клиента _____ (Ф.И.О.) и в качестве Зарегистрированного номера уполномоченного лица Клиента _____ (Ф.И.О.) считать следующий телефонный номер: _____ _____.

Должность руководителя _____ / _____/
подпись *Ф.И.О.*

М.П. (при наличии)

Приложение № 12
к Условиям дистанционного банковского обслуживания корпоративных клиентов

ФОРМА

В АО «Банк Русский Стандарт»

от _____
(наименование Клиента)

Дата: _____
(формат ДД.ММ.ГГГГ)

Заявление о регистрации уполномоченного лица Клиента

Просим:

1. Зарегистрировать в Системе уполномоченное лицо Клиента _____ (*Ф.И.О.*) _____ (*должность*), данные документа, удостоверяющего личность: _____ (*наименование, серия, номер, дата выдачи, кем и когда выдан*) (далее – **УЛК**).

2. В качестве Зарегистрированного номера для УЛК зарегистрировать в Системе телефонный номер: _____.

3. Использовать следующее средство подписи УЛК для работы в Системе:
- ☐ Ключ ЭП
- ☐ Ключ ЭП PayControl

4. Сформировать и прислать на электронную почту *@*.* учетные данные УЛК (Логин и Пароль) для входа в Систему «Интернет-Банк».

5. Предоставить посредством Системы «Интернет-Банк» новый QR-код на Зарегистрированный номер _____ для генерации очередной пары Ключей ЭП PayControl для УЛК.

Должность руководителя _____ / _____/
подпись *Ф.И.О.*

М.П. (при наличии)

Приложение № 13
к Условиям дистанционного банковского обслуживания корпоративных клиентов

ФОРМА

В АО «Банк Русский Стандарт»
от _____
(наименование клиента, ИНН)

Дата: __.____.____
(формат ДД.ММ.ГГГГ)

Заявление об установлении ограничений на совершение Клиентом Операций по Счету (-ам) с использованием Системы[1]

1. Прошу установить следующие ограничения на совершение Клиентом Операций по Счету (-ам) с использованием Системы:

№	Ф.И.О. уполномоченного лица Клиента	Вид и № Счета	Вид Операции	Максимальная сумма Операции	Максимальная совокупная сумма Операций в течение одного календарного дня
1		расчетный счет № _____	□ перевод денежных средств в рублях РФ[2] □ перевод денежных средств в иностранной валюте □ конверсионная операция		
2		расчетный счет № _____	□ перевод денежных средств в рублях РФ[2] □ перевод денежных средств в иностранной валюте □ конверсионная операция		
3		расчетный счет № _____	□ перевод денежных средств в рублях РФ[2] □ перевод денежных средств в иностранной валюте □ конверсионная операция		

[1] Термины, используемые в настоящем Заявлении об установлении ограничений на совершение Клиентом Операций по Счету (-ам) с использованием Системы и написанные с заглавной буквы, имеют то же значение, что и в Условиях расчетно-кассового обслуживания юридических лиц, индивидуальных предпринимателей и физических лиц, занимающихся в установленном законодательством Российской Федерации порядке частной практикой, в АО «Банк Русский Стандарт».

[2] Ограничения на совершение уполномоченным лицом Клиента Операций по Счету (расчетному счету) не распространяются на операции по переводу денежных средств, осуществляемые с использованием системы быстрых платежей (сервиса быстрых платежей платежной системы Банка России).

2. Клиент понимает и соглашается с тем, что в случае если Клиентом в п. 1 настоящего заявления в отношении конкретного Счета и в отношении конкретного уполномоченного лица Клиента установлено одно или несколько ограничений на совершение Клиентом Операций по Счету (-ам) с использованием Системы, то ранее установленные Банком на основании ранее поданного (-ых) письменного (-ых) заявления (-й) Клиента ограничения на совершение Клиентом Операций по Счету (-ам) с использованием Системы в отношении такого Счета и в отношении такого уполномоченного лица Клиента отменяются с момента осуществления Банком соответствующих настроек в информационных системах Банка на основании настоящего заявления.

3. Клиент подтверждает, что данные указанные в настоящем заявлении являются корректными.

Должность руководителя _____/_____

подпись Ф.И.О.

М.П. (при наличии)

Приложение № 14
к Условиям дистанционного банковского обслуживания корпоративных клиентов

ФОРМА

В АО «Банк Русский Стандарт»

от _____
(наименование Клиента и ИНН)

Дата: _____
(формат ДД.ММ.ГГГГ)

Заявление об отмене установленных ограничений на совершение Клиентом Операций по Счету (-ам) с использованием Системы

1. Прошу отменить все ограничения на совершение Клиентом Операций с использованием Системы, установленные ранее в отношении следующего (-их) Счета (-ов) и уполномоченного (-ых) лица / лиц Клиента:

№	Ф.И.О. уполномоченного лица Клиента	Вид и № Счета
1		расчетный счет №_____
2		расчетный счет №_____
3		расчетный счет №_____

2. Клиент понимает и соглашается с тем, что все ограничения, установленные ранее в отношении конкретного Счета и в отношении конкретного уполномоченного лица Клиента, указанных в п. 1 настоящего заявления, отменяются с момента осуществления Банком соответствующих настроек в информационных системах Банка на основании настоящего заявления.

Должность руководителя _____ / _____/
подпись *Ф.И.О.*

М.П. (при наличии)