Приложение

Договор[1]

№ _____

г. _____ «___» _____ 20__ г.

Центральный банк Российской Федерации (Банк России), являющийся оператором платформы цифрового рубля в соответствии со статьей 82.10 Федерального закона от 10 июля 2002 года № 86-ФЗ «О Центральном Банке Российской Федерации (Банке России)» (далее – Федеральный закон № 86-ФЗ), именуемый в дальнейшем «Банк», в лице _____,

(должность, фамилия, имя, отчество (при его наличии) представителя Банка)

действующего(ей) на основании _____,

(наименование и реквизиты документа (если присвоены),

с одной стороны, и _____

_____,

(полное (сокращенное) фирменное наименование и БИК кредитной организации)

именуемый(ое) в дальнейшем «Клиент», в лице _____

_____,

(должность, фамилия, имя, отчество (при его наличии) представителя кредитной организации)

действующего(ей) на основании _____,

(наименование и реквизиты документа (если присвоены)

с другой стороны (далее при совместном упоминании – Стороны), заключили настоящий договор (далее – Договор) о нижеследующем.

1. Предмет Договора

1.1. Банк обязуется на условиях, согласованных Сторонами, открыть Клиенту счет цифрового рубля (далее – Счет) и зачислять цифровые рубли, поступающие на открытый на платформе цифрового рубля Счет, списывать цифровые рубли, учитываемые на Счете, а также выполнять распоряжения Клиента о совершении операций с цифровыми рублями.

[1] По тексту Договора применяются термины и определения в значениях, установленных законодательством Российской Федерации, правилами платформы цифрового рубля.

1.2. Клиент оказывает Банку услуги, указанные в пункте 1.2 Положения Банка России от 03.08.2023 № 820-П «О платформе цифрового рубля», в том числе обеспечивает информационное и технологическое взаимодействие между Банком и пользователями платформы цифрового рубля (далее – Услуги). Банк за оказанные ему Услуги выплачивает Клиенту вознаграждение.

2. Порядок открытия Счета

2.1. После выполнения Клиентом мероприятий, предусмотренных Стандартом платформы цифрового рубля «Порядок подключения участника платформы к платформе цифрового рубля» (далее – Порядок подключения)[2], Условиями по защите информации для участников платформы цифрового рубля[3] (далее – Условия по защите информации), а также процедуры выпуска сертификатов ключей проверки электронной подписи и получения Клиентом ключевой информации в соответствии с Регламентом взаимодействия Финансового посредника и Банка России при управлении криптографическими ключами Платформы Цифрового рубля (далее – Порядок управления ключами)[4], Банк открывает Клиенту Счет.

2.2. Не позднее рабочего дня, следующего за днем открытия Счета, Банк посредством личного кабинета[5] направляет Клиенту уведомление об открытии ему Счета с указанием номера Счета.

3. Права и обязанности Сторон

3.1. Банк обязан:

3.1.1. Обеспечить подключение Клиента к платформе цифрового рубля в соответствии с Порядком подключения и предоставить Клиенту программный модуль Банка России[6] в соответствии с Условиями передачи

---

[2] Размещен на сайте Банка России по адресу https://www.cbr.ru/fintech/dr/doc_dr/standarts/.

[3] Размещен на сайте Банка России по адресу https://www.cbr.ru/fintech/dr/doc_dr/forms/.

[4] Размещен на сайте Банка России по адресу https://www.cbr.ru/fintech/dr/doc_dr/reglaments/.

[5] Порядок взаимодействия в электронном виде посредством личного кабинета, ссылка на который размещена на сайте Банка России (далее – личный кабинет), устанавливается Банком России на основании частей 1 и 4 статьи 73.1 Федерального закона № 86-ФЗ, частей 1 и 4 статьи 35.1 Федерального закона 27 июня 2011 года № 161-ФЗ «О национальной платежной системе» (далее – Федеральный закон № 161-ФЗ).

[6] Программный модуль Банка России, предназначенный для встраивания Клиентом в мобильное приложение клиента для проведения операций с цифровым рублем, содержащий в своем составе сертифицированное программное обеспечение средств криптографической защиты информации для осуществления криптографических преобразований.

программного обеспечения Клиенту Банка России (далее – Условия передачи ПО)[7].

3.1.2. Осуществлять перевод цифровых рублей в рамках платформы цифрового рубля путем одновременного уменьшения остатка цифровых рублей на счете цифрового рубля Клиента и увеличения остатка цифровых рублей на счете цифрового рубля пользователя платформы – получателя средств на сумму перевода цифровых рублей.

3.1.3. Осуществлять увеличение остатка цифровых рублей на счете цифрового рубля Клиента путем перевода денежных средств, списанных с его корреспондентского счета.

3.1.4. Осуществлять уменьшение остатка цифровых рублей на счете цифрового рубля Клиента путем перевода денежных средств на его корреспондентский счет.

3.1.5. Обеспечивать взаимодействие платформы цифрового рубля с платежной системой Банка России в течение стандартного периода графика функционирования платежной системы Банка России, предусмотренного приложением 17 к Положению Банка России от 24 сентября 2020 года № 732-П «О платежной системе Банка России» (далее – Положение № 732-П), при совершении операций с использованием Счета.

3.1.6. Перечислить остаток цифровых рублей со Счета на корреспондентский счет Клиента не позднее дня приостановления Клиенту доступа к платформе цифрового рубля в связи с поступлением на платформу цифрового рубля от платежной системы Банка России информации об отзыве (аннулировании) у Клиента лицензии на осуществление банковских операций и установлении в отношении Клиента ограничений в платежной системе Банка России.

3.1.7. Направлять Клиенту по электронной почте уведомление о возникновении чрезвычайных ситуаций и операционных сбоев, приведших к нарушению функционирования платформы цифрового рубля, в срок не позднее одного часа с момента установления факта нарушения функционирования платформы цифрового рубля.

3.1.8. Направлять Клиенту информацию о результатах рассмотрения запросов или претензий пользователя платформы, по которым Клиентом было

[7] Размещен на сайте Банка России по адресу https://www.cbr.ru/development/mcirabis/Involve_EM/.

принято решение об их направлении в Банк, в порядке и сроки, предусмотренные Стандартом ОТВ[8].

3.2. Банк вправе:

3.2.1. При выявлении признаков нарушения пользователем платформы правил платформы цифрового рубля запрашивать у Клиента информацию о действиях, выполненных Клиентом при взаимодействии с пользователем платформы.

3.3. Клиент обязан:

3.3.1. Направить документы, необходимые для регистрации Клиента на платформе цифрового рубля и открытия Счета, оформленные в соответствии с Порядком подключения.

3.3.2. Соблюдать Условия обеспечения обслуживания Клиентом пользователей платформы цифрового рубля на платформе цифрового рубля (далее – Условия обслуживания на платформе), Условия по защите информации и требования стандартов платформы цифрового рубля (далее – Стандарты)[9].

3.3.3. Использовать альбом распоряжений и альбом электронных сообщений[10], предусмотренные частью 6 статьи 30.7 Федерального закона № 161-ФЗ для взаимодействия с Банком на платформе цифрового рубля.

3.3.4. Выполнять процедуры тестовых испытаний взаимодействия с платформой цифрового рубля и пользовательского тестирования при изменении существующих или появлении новых типов электронных сообщений в альбоме электронных сообщений, в соответствии с требованиями Процедуры проведения тестовых испытаний взаимодействия участника платформы цифрового рубля и Порядка проведения пользовательского тестирования, размещенных на портале поддержки участников платформы цифрового рубля[11] (далее – портал поддержки).

3.3.5. Информировать Банк путем направления сообщения через портал поддержки о проведении плановых технических (регламентных) работ, при которых возможность открытия и (или) закрытия Счета и (или) доступ пользователей платформы к платформе цифрового рубля в целях совершения операций с цифровыми рублями будут временно недоступны, не позднее, чем

---

[8]Стандарт платформы цифрового рубля «Требования операционно-технологического взаимодействия на платформе цифрового рубля», размещен на сайте Банка России по адресу https://www.cbr.ru/fintech/dr/doc_dr/standarts/.

[9] Стандарты – документы Банка России, содержащие условия, необходимые для взаимодействия между Банком и Клиентом посредством платформы цифрового рубля, размещенные на сайте Банка России по адресу https://www.cbr.ru/fintech/dr/doc_dr/standarts/.

[10] Размещены на сайте Банка России по адресу https://www.cbr.ru/fintech/dr/doc_dr/albums_r/.

[11] Размещен на сайте Банка России по адресу www.support-dr.cbr.ru.

за три рабочих дня до проведения указанных работ, незамедлительно по факту начала и окончания таких работ.

3.3.6. Информировать Банк путем направления сообщения через портал поддержки о возникновении у Клиента чрезвычайных ситуаций, операционных сбоев, при которых пользователям платформы недоступна возможность открытия и (или) закрытия Счета и (или) пользователям платформы не предоставляется доступ к платформе цифрового рубля в целях совершения операций с цифровыми рублями (далее – инцидент), незамедлительно по факту возникновения инцидента (в том числе об ориентировочных сроках восстановления штатного режима предоставления услуг пользователям платформы) и по факту устранения инцидента.

3.3.7. Предоставлять по запросу Банка информацию и документы, необходимые для реализации Банком прав и обязанностей, установленных Договором.

3.3.8. Присоединиться к Правилам оказания услуг по предоставлению универсального платежного кода «Правила Сервиса универсального платежного кода» АО «Национальная система платежных карт» и обеспечивать пользователям платформы возможность осуществления переводов цифровых рублей с использованием универсального платежного кода.

4. Ответственность Сторон

4.1. Банк не несет ответственности за любые понесенные Клиентом убытки, вызванные перечислением цифровых рублей по распоряжениям Клиента с ошибочно указанными реквизитами получателя.

4.2. Банк не несет ответственности за сбои в работе оборудования, программных и технических средств, используемых для передачи информации, возникшие по независящим от Банка причинам, за технические сбои (отключение/повреждение электропитания и сетей связи, сбой программного обеспечения, технические сбои в сети технических устройств, за сбои, возникающие на стороне операторов связи и (или) в информационных системах Клиента, а также в иных ситуациях, находящихся вне сферы контроля Банка), повлекшие за собой невыполнение условий Договора.

4.3. Банк не несет ответственности за последствия исполнения распоряжений, выданных неуполномоченными лицами, наступившие в результате непредставления или несвоевременного представления Клиентом в

Банк информации и документов, необходимых для совершения операций на платформе цифрового рубля в соответствии с законодательством Российской Федерации, и в тех случаях, когда с использованием предусмотренных Договором процедур Банк не мог установить факта выдачи распоряжения неуполномоченными лицами.

4.4. Клиент несет ответственность за убытки, возникшие у Банка по вине Клиента, в том числе вследствие нарушения Клиентом условий Договора и (или) действующего законодательства Российской Федерации, предоставления Клиентом некорректных и (или) неполных и (или) недостоверных сведений и информации о пользователе платформы, его представителе, выгодоприобретателе, бенефициарном владельце. Клиент обязан возместить Банку все убытки в течении пяти рабочих дней с момента получения соответствующей претензии Банка, в размере, указанном Банком в претензии.

5. Порядок взаимодействия Сторон

Взаимодействие Сторон при обмене информацией и официальной корреспонденцией осуществляется в электронном виде посредством личного кабинета, путем направления документов на бумажном носителе, подписанных руководителем Клиента (лицом, его замещающим) или иным уполномоченным им лицом и заверенных печатью, через подразделение Банка, обслуживающее корреспондентский счет Клиента, если иное не предусмотрено Договором, Стандартами.

6. Порядок изменения условий Договора

6.1. Банк вправе в одностороннем порядке вносить изменения в Договор.

Информирование Клиента о внесении изменений в Договор осуществляется Банком не менее чем за один месяц до даты вступления в силу новой редакции Договора путем размещения новой редакции Договора на сайте Банка России по адресу https://www.cbr.ru/fintech/dr/doc_dr/forms/ с указанием даты вступления его в силу, а также посредством уведомления Клиента на портале поддержки о размещении на сайте Банка России новой редакции Договора.

6.2. Новая редакция Договора распространяется на отношения Сторон по Договору со дня вступления в силу новой редакции Договора, в том числе на отношения Сторон, связанные с исполнением обязательств, возникших в соответствии с Договором до вступления в силу новой редакции Договора.

6.3. При внесении изменений в названия документов, упомянутых в Договоре в соответствующих пунктах, и (или) изменении адресов их размещения на сайте Банка России, пункты Договора, содержащие неактуальные названия документов и (или) адреса их размещения на сайте Банка России, продолжают действовать, указанные в них документы применяются в последней актуальной редакции, размещенной на сайте Банка России.

6.4. При внесении изменений в Стандарты Банк не менее чем за один месяц до даты вступления в силу новых редакций Стандартов размещает новые редакции Стандартов на сайте Банка России по адресу https://www.cbr.ru/fintech/dr/doc_dr/standarts/ и информирует Клиента о дате вступления в силу новых редакций Стандартов путем размещения соответствующей информации на сайте Банка России.

7. Урегулирование споров и разногласий

Споры и разногласия, возникающие вследствие неисполнения или ненадлежащего исполнения Сторонами обязательств по Договору, разрешаются путем переговоров или в порядке, предусмотренном в приложении 1 к Положению Банка России от 3 августа 2023 года № 820-П «О платформе цифрового рубля», а в случае невозможности разрешения существующих разногласий подлежат рассмотрению в судебном порядке в соответствии с законодательством Российской Федерации.

8. Порядок расторжения Договора

8.1. Обращение Клиента о расторжении Договора направляется Клиентом в подразделение Банка, обслуживающее корреспондентский счет Клиента, посредством личного кабинета не позднее, чем за семь рабочих дней до предполагаемой даты закрытия счета цифрового рубля Клиента.

8.2. При направлении в Банк обращения об установлении временного сохранения корреспондентского счета Клиента с его функционированием в ограниченном режиме Клиент включает в данное обращение просьбу о

закрытии Счета и указывает дату закрытия Счета не позднее даты установления ограниченного режима функционирования корреспондентского счета при временном его сохранении.

Перед направлением обращения о расторжении Договора в Банк Клиент обеспечивает перечисление остатка цифровых рублей со Счета на корреспондентский счет Клиента.

8.3. Счет закрывается при отсутствии остатка цифровых рублей не позднее семи рабочих дней со дня получения Банком обращения Клиента о расторжении Договора или в день, указанный Клиентом в обращении о расторжении Договора.

При закрытии Счета Банком в случаях, предусмотренных законодательством Российской Федерации, Счет закрывается не позднее рабочего дня, следующего за днем перечисления остатка цифровых рублей Клиента со Счета на его корреспондентский счет.

8.4. Не позднее рабочего дня, следующего за днем закрытия Счета, Банк посредством личного кабинета направляет Клиенту уведомление о закрытии Счета с указанием даты его закрытия.

9. Заключительные положения

9.1. Настоящий Договор вступает в силу со дня подписания его Сторонами и действует до его прекращения (расторжения) в соответствии с законодательством Российской Федерации и условиями настоящего Договора.

9.2. Настоящий Договор составлен на бумажном носителе в двух экземплярах, каждый из которых имеет одинаковую юридическую силу, один экземпляр передается Клиенту, другой хранится в Банке.

9.3. Условия обслуживания на платформе (приложение 1 к Договору) и Условия по защите информации (приложение 2 к Договору) являются неотъемлемой частью Договора.

10. Адреса и подписи Сторон

Приложение 1 к Договору
_____ от «____» _____20__г.

Условия обслуживания на платформе[12]

1. Порядок действий Клиента при предоставлении пользователю платформы доступа к платформе цифрового рубля и обслуживании пользователя платформы на платформе цифрового рубля

1.1. Клиент обеспечивает предоставление пользователю платформы доступа к платформе цифрового рубля с соблюдением требований Стандарта по пользовательским интерфейсам[13], Стандарта ОТВ и настоящих Условий обслуживания на платформе.

1.2. При открытии Банком счета цифрового рубля пользователю платформы Клиент для обслуживания пользователя платформы с использованием приложения клиента обеспечивает присвоение пользователю платформы уникальных признаков (идентификаторов пользователя платформы), полученных от Банка, а также идентификацию и аутентификацию пользователя платформы[14] с использованием приложения клиента, в том числе при изменении сведений и информации о пользователе платформы, предоставленных пользователем платформы при открытии счета цифрового рубля и (или) получении доступа к платформе цифрового рубля.

1.3. Клиент с использованием предоставляемого им приложения клиента обеспечивает направление пользователю платформы поступившей от Банка информации о статусе счета цифрового рубля пользователя платформы, об остатке цифровых рублей, об операциях по его счету цифрового рубля, сведений о приостановлении доступа пользователя платформы к платформе цифрового рубля путем приостановления совершения операций с использованием приложения клиента или путем прекращения исполнения распоряжений пользователя платформы, и иных сведений и документов в виде информационных сообщений, извещений и уведомлений.

---

[12] По тексту Условий обслуживания на платформе применяются сокращения, определенные Договором, и/или термины и определения в значениях, установленных законодательством Российской Федерации, включая правила платформы цифрового рубля.

[13] Стандарт платформы цифрового рубля «Требования и рекомендации к пользовательским интерфейсам при совершении операций с цифровыми рублями», размещен на сайте Банка России по адресу https://www.cbr.ru/fintech/dr/doc_dr/standarts/.

[14] Значение терминов «идентификация и аутентификация» в настоящих Условиях обслуживания на платформе применяется в соответствии с ГОСТ Р 57580.1-2017 «Национальный стандарт Российской Федерации. Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер».

1.4. Клиент ежедневно обеспечивает и контролирует наличие на Счете остатка цифровых рублей в размере, достаточном для выполнения операций пополнения счетов цифрового рубля пользователей платформы и операций вывода средств со счетов цифрового рубля пользователей платформы в течение периода после окончания стандартного периода регулярного сеанса текущего операционного дня платежной системы Банка России до начала стандартного периода регулярного сеанса следующего операционного дня платежной системы Банка России в соответствии с графиком функционирования платежной системы Банка России, предусмотренным приложением 17 к Положению № 732-П.

1.5. При получении Клиентом от пользователя платформы, представителя пользователя платформы, наследников пользователя платформы или лиц, указанных в постановлении нотариуса о возмещении расходов на достойные похороны, заявления о переводе[15] или обращения о расторжении договора счета цифрового рубля на бумажном носителе, и документов, в том числе подтверждающих полномочия указанных лиц, Клиент обеспечивает проверку и направление принятых документов в Банк в порядке и в сроки, предусмотренные Стандартом ОТВ.

1.6. Клиент обеспечивает прием от пользователей платформы запросов на бумажном носителе на предоставление сведений и документов, составленных по форме, предусмотренной в Сборнике типовых форм документов, применяемых в рамках условий договоров счета цифрового рубля с пользователями платформы цифрового рубля, участниками платформы цифрового рубля на платформе цифрового рубля[16], а также иных документов (в том числе дополнительных соглашений), предоставление которых пользователем платформы в Банк на бумажном носителе предусмотрено условиями договора цифрового рубля, заключенного между оператором платформы и пользователем платформы, и их направление в Банк в порядке и в сроки, предусмотренные Стандартом ОТВ.

1.7. При закрытии Счета Клиент обеспечивает уведомление своих клиентов – пользователей платформы о закрытии Счета и невозможности дальнейшего предоставления им доступа к платформе цифрового рубля:

---

[15] Заявление о переводе денежных средств пользователя платформы, представителя пользователя платформы, наследника, лица, указанного в постановлении нотариуса о возмещении расходов на достойные похороны, или иных лиц в соответствии с законодательством Российской Федерации, составленное на бумажном носителе (далее – заявление о переводе).

[16] Размещен на сайте Банка России по адресу https://www.cbr.ru/fintech/dr/doc_dr/standard_forms/.

при закрытии Счета на основании обращения Клиента о расторжении Договора, в том числе в случае установления временного сохранения корреспондентского счета Клиента с его функционированием в ограниченном режиме, с доведением до пользователей платформы планируемой даты закрытия Счета – не менее чем за три рабочих дня до направления в Банк обращения Клиента о расторжении Договора;

при закрытии счета Банком в случаях, предусмотренных законодательством Российской Федерации, – не позднее рабочего дня, следующего за днем закрытия Счета.

2. Права и обязанности Клиента

2.1. Клиент обязан:

2.1.1. Обеспечивать проверку наличия подтвержденной учетной записи пользователя платформы в ЕСИА[17] путем формирования запроса на аутентификацию пользователя платформы в ЕСИА с целью проверки принадлежности и подтверждения подлинности идентификатора, присвоенного пользователю платформы в ЕСИА.

2.1.2. Обеспечивать идентификацию пользователя платформы, а также проверку полномочий представителя пользователя платформы при получении сертификата ключа проверки электронной подписи.

2.1.3. Направлять пользователю платформы посредством размещения в приложении клиента извещение об исполнении распоряжения или уведомление о неуспешном завершении процедур приема к исполнению распоряжения, в том числе поступившие от Банка.

2.1.4. В рамках исполнения Клиентом функций участника платформы цифрового рубля обеспечивать пользователям платформы, реализующим товары, работы, услуги за цифровые рубли, заключившим с Клиентом договоры о приеме электронных средств платежа, взаимодействие с АО «Национальная система платежных карт» (далее – АО «НСПК») в части

[17] Физические лица и индивидуальные предприниматели для открытия счета цифрового рубля на платформе цифрового рубля должны быть зарегистрированы в федеральной государственной информационной системе «Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме» (далее – ЕСИА) и получить ключ простой электронной подписи при личной явке в соответствии с правилами использования простой электронной подписи при обращении за получением государственных и муниципальных услуг в электронной форме, установленными Правительством Российской Федерации в соответствии с пунктом 1 части 1 статьи 13 Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи».

использования ими сервиса управления ссылками АО «НСПК» (далее – СУС) в соответствии с требованиями Стандарта ОТВ и предоставления пользователям платформы, приобретающим товары, работы, услуги, возможности их оплаты цифровыми рублями (или возврата цифровых рублей по ранее совершенному переводу цифровых рублей) по платежной ссылке[18], переданной СУС.

В случае предоставления Клиентом доступа к платформе цифрового рубля пользователю платформы, осуществляющему прием оплаты за реализованные товары, работы, услуги цифровыми рублями, обеспечить информирование такого пользователя платформы о порядке действий, необходимых для выполнения данным пользователем платформы, при приеме оплаты за товары, работы, услуги цифровыми рублями или оформлении возврата цифровых рублей по ранее совершенному переводу цифровых рублей с использованием универсального платежного кода АО «НСПК».

2.1.5. Обеспечить доведение до пользователей платформы, реализующих товары, работы, услуги, информации о результате совершения операции оплаты товаров, работ, услуг цифровыми рублями путем отображения результата совершения операции оплаты в программных средствах и (или) технических устройствах, используемых такими пользователями платформы для приема оплаты за товары, работы, услуги с использованием универсального платежного кода АО «НСПК».

2.1.6. Направлять своим клиентам – пользователям платформы уведомление о приостановлении (возобновлении) Банком доступа к платформе цифрового рубля Клиенту и невозможности (возобновлении возможности) дальнейшего предоставления Банком доступа к платформе цифрового рубля его клиентам не позднее одного рабочего дня, следующего за днем приостановления (возобновления) доступа Клиента к платформе цифрового рубля.

2.1.7. Направлять запросы и претензии, по которым Клиентом принято решение об их направлении в Банк, а также заявления о переводе, обращения пользователя платформы, представителя пользователя платформы о расторжении договора счета цифрового рубля, поступившие Клиенту на бумажном носителе, иные документы (в том числе дополнительные соглашения), предоставление которых пользователем платформы в Банк на

[18] Платежная ссылка – представление реквизитов перевода в электронной форме в виде кода, имеющего вид графического символа, NFC-метки или текстовой строки в целях использования для оплаты, товаров, работ, услуг.

бумажном носителе предусмотрено условиями договора цифрового рубля, заключенного между оператором платформы и пользователем платформы, и документы, в том числе подтверждающие полномочия указанных лиц, и иные сведения в Банк на рассмотрение в порядке и в сроки, предусмотренные Стандартом ОТВ.

2.1.8. Направлять своим клиентам – пользователям платформы с использованием приложения клиента уведомление о возникновении чрезвычайных ситуаций и операционных сбоев, приведших к нарушению функционирования платформы цифрового рубля, в срок не позднее одного часа с момента получения такого уведомления от Банка.

2.1.9. Выделить канал поддержки для обращения своих клиентов – пользователей платформы по вопросам, связанным с доступом к платформе цифрового рубля и обслуживанием на платформе цифрового рубля, и обеспечить функционирование и доступность выделенного канала поддержки в круглосуточном режиме.

2.2. Клиент вправе направлять в Банк электронные сообщения пользователя платформы, содержащие запросы на:

осуществление Банком возврата цифровых рублей со счета цифрового рубля пользователя платформы по операциям оплаты товаров, работ, услуг цифровыми рублями, ранее совершенным на его счет цифрового рубля;

совершение Банком переводов цифровых рублей на счет пользователя платформы в оплату реализованных им товаров, работ, услуг цифровыми рублями;

предоставление Банком пользователю платформы информации о результатах совершения операций оплаты товаров, работ, услуг цифровыми рублями на его счет цифрового рубля;

предоставление Банком пользователю платформы информации об остатке цифровых рублей, учитываемых на счете цифрового рубля, и об операциях по счету цифрового рубля пользователя платформы.

Приложение 2 к Договору
_____ от «____» _____20__г.

Условия по защите информации[19]

1. Открытие Счета и предоставление Клиенту доступа к платформе цифрового рубля осуществляются при условии готовности выполнения Клиентом требований к обеспечению защиты информации для участников платформы цифрового рубля, установленных нормативным актом Банка на основании статьи 82.10 Федерального закона № 86-ФЗ, пункта 7 части 1, части 3 статьи 30.7 Федерального закона № 161-ФЗ, а также требований по созданию отдельной службы безопасности и контроля, осуществляющей функции контроля эксплуатации мобильного приложения и программного модуля Банка России в составе мобильного приложения, установленных стандартом платформы цифрового рубля «Порядок проведения работ по оценке влияния аппаратных, программно-аппаратных и программных средств сети (системы) конфиденциальной связи, совместно с которыми предполагается штатное функционирование программного модуля Банка России, на выполнение предъявленных к входящему в его состав средству криптографической защиты информации требований»[20] в разделе «Обязанности участника ПлЦР при использовании настоящего Порядка».

2. Банк проверяет готовность выполнения Клиентом требований, указанных в пункте 1 настоящих условий, на основании полученного от Клиента акта о готовности выполнения требований к обеспечению защиты информации для участников платформы цифрового рубля, форма которого приведена в приложении к настоящим условиям (далее – акт), и документов, указанных в пункте 4 настоящих условий.

В ходе проверки Банк вправе запросить у Клиента пояснения относительно содержания полученных от Клиента документов,

[19] По тексту Условий по защите информации применяются сокращения, определенные Договором и Условиями обслуживания на платформе, и/или термины и определения в значениях, установленных законодательством Российской Федерации, включая правила платформы цифрового рубля.

[20] Размещен на сайте Банка Росси по адресу http://cbr.ru/Content/Document/File/161203/standard_drp.pdf.

дополнительные сведения и документы, связанные с обеспечением защиты информации, а также провести проверку готовности выполнения указанных требований по месту осуществления деятельности Клиента.

3. Акт предоставляется Клиентом в подразделение Банка, обслуживающее корреспондентский счет Клиента, в электронном виде посредством личного кабинета.

4. К акту прилагаются документы, подтверждающие полномочия заместителя руководителя Клиента на утверждение акта, распорядительный документ о создании комиссии для проверки готовности выполнения требований, указанных в пункте 1 настоящих условий, и документы, подтверждающие готовность выполнения Клиентом указанных требований.

5. При изменении сведений о выполнении требований к обеспечению защиты информации, отраженных в акте, предоставленном Клиентом в Банк в рамках открытия Счета, Клиент посредством личного кабинета направляет в Банк актуализированные сведения и подтверждающие их документы в течение семи календарных дней с момента наступления такого изменения.

Приложение
к Условиям по защите информации
для участников платформы
цифрового рубля

УТВЕРЖДАЮ

_____
(личная подпись, Ф.И.О. заместителя руководителя Клиента[21])

_____
(полное фирменное наименование кредитной организации)
«___» _____ г.

АКТ

о готовности выполнения Клиентом

_____
(указывается полное фирменное наименование кредитной организации)

требований к обеспечению защиты информации для участников платформы цифрового рубля от «____» _____ г.

Настоящий акт составлен по результатам проверки готовности выполнения _____
(указывается полное фирменное наименование кредитной организации)
требований к обеспечению защиты информации для участников платформы цифрового рубля.

Комиссия[22] _____, созданная
(указывается полное фирменное наименование кредитной организации)
на основании _____
(указывается наименование, дата и номер распорядительного документа кредитной организации)
в составе:

Руководитель Комиссии _____
(наименование должности, инициалы, фамилия)

Члены Комиссии: _____
(наименование должности, инициалы, фамилия)

_____
(наименование должности, инициалы, фамилия)

_____
(наименование должности, инициалы, фамилия)

_____
(наименование должности, инициалы, фамилия)

установила готовность выполнения _____
(указывается полное фирменное наименование кредитной организации)

[21] Заместитель руководителя Клиента, на которого в соответствии с Указом Президента Российской Федерации от 1 мая 2022 года № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации» возложены полномочия по обеспечению информационной безопасности.

[22] Комиссия назначается распорядительным документом кредитной организации, подписанным заместителем руководителя Клиента.

(далее – Клиент) следующих требований к обеспечению защиты информации для участников платформы цифрового рубля (далее – требования к обеспечению защиты информации).

№ п/п	Требования к обеспечению защиты информации	Сведения и/или документы, подтверждающие готовность выполнения Клиентом требований к обеспечению защиты информации
1	Объекты информационной инфраструктуры, используемые при обеспечении возможности совершения операций с цифровыми рублями, размещены Клиентом в выделенных сегментах (группах сегментов) вычислительных сетей.	
2	Для объектов информационной инфраструктуры в пределах выделенного сегмента (группы сегментов) вычислительных сетей Клиентом, являющимся кредитной организацией, которая определена как системно значимая в соответствии с частью шестой статьи 57 Федерального закона от 10 июля 2002 года № 86-ФЗ «О Центральном банке Российской Федерации (Банке России)» и (или) значимая на рынке платежных услуг в соответствии с частью второй статьи 30.5 Федерального закона от 27 июня 2011 года № 161-ФЗ «О национальной платежной системе» (далее – Федеральный закон № 161-ФЗ), обеспечено применение организационных и технических мер, реализующих усиленный уровень защиты информации, предусмотренный пунктом 6.7 раздела 6 национального стандарта Российской Федерации ГОСТ Р 57580.1-2017 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер» (далее – ГОСТ Р 57580.1-2017). Для объектов информационной инфраструктуры в пределах выделенного сегмента (группы сегментов) вычислительных сетей Клиентом, не являющимся системно значимой кредитной организацией и (или) кредитной организацией, значимой на рынке платежных услуг, в целях обеспечения защиты информации обеспечено применение мер защиты информации, реализующих стандартный уровень защиты информации,	

№ п/п	Требования к обеспечению защиты информации	Сведения и/или документы, подтверждающие готовность выполнения Клиентом требований к обеспечению защиты информации
	предусмотренный пунктом 6.7 раздела 6 ГОСТ Р 57580.1-2017.	
3	Клиентом определены во внутренних документах:	
3.1	Состав организационных мер защиты информации и порядок их применения, а также состав технических средств защиты информации и порядок их использования.	
3.2	Порядок подготовки, обработки, передачи и хранения сообщений в электронном виде, связанных с осуществлением операций с цифровыми рублями (далее – электронные сообщения), и защищаемой информации, предусмотренной нормативным актом Банка России, устанавливающим требования к обеспечению защиты информации для участников платформы цифрового рубля, с использованием объектов информационной инфраструктуры.	
3.3	Список лиц (за исключением пользователей платформы цифрового рубля (далее – пользователь платформы)), допущенных к работе со средствами криптографической защиты информации (далее – СКЗИ), с определением прав использования криптографических ключей.	
3.4	Список лиц (за исключением пользователей платформы), ответственных за обеспечение функционирования и безопасности СКЗИ (ответственные пользователи СКЗИ).	
3.5	Список лиц (за исключением пользователей платформы), обладающих правами по управлению криптографическими ключами, в том числе ответственных за формирование криптографических ключей и обеспечение безопасности криптографических ключей.	
3.6	Состав технологических мер защиты информации, используемых для контроля целостности, подтверждения подлинности и обеспечения конфиденциальности электронных сообщений на этапах их подготовки, обработки, передачи и хранения, и правила их применения, в том числе порядок применения СКЗИ и управления ключевой информацией СКЗИ.	
3.7	Создание и уровень подчинения отдельной службы безопасности и контроля при	

№ п/п	Требования к обеспечению защиты информации	Сведения и/или документы, подтверждающие готовность выполнения Клиентом требований к обеспечению защиты информации
	использовании Клиентом стандарта платформы цифрового рубля «Порядок проведения работ по оценке влияния аппаратных, программно-аппаратных и программных средств сети (системы) конфиденциальной связи, совместно с которыми предполагается штатное функционирование программного модуля Банка России, на выполнение предъявленных к входящему в его состав средству криптографической защиты информации требований».	
4	Защита электронных сообщений обеспечивается Клиентом в соответствии с альбомом электронных сообщений, предусмотренным частью 6 статьи 30.7 Федерального закона № 161-ФЗ.	
5	Формирование и подписание электронных сообщений Клиента обеспечено Клиентом с использованием автоматизированной системы Клиента.	
6	Формирование и подписание электронных сообщений пользователя платформы обеспечено Клиентом в электронном средстве платежа на основе программного обеспечения, позволяющего пользователю платформы составлять, удостоверять и передавать распоряжения, установленного на техническом устройстве пользователя платформы (включая смартфон, планшетный компьютер) или в другой системе дистанционного банковского обслуживания (далее – приложение Клиента) с использованием ключа электронной подписи пользователя платформы или в автоматизированной системе Клиента с использованием ключа электронной подписи Клиента (при составлении Клиентом распоряжений от имени пользователя платформы в соответствии с частью 5 статьи 7.1 Федерального закона № 161-ФЗ).	
7	При подписании электронных сообщений пользователя платформы в приложении Клиента, являющемся программным обеспечением для мобильных устройств (далее – мобильное приложение), Клиентом	

№ п/п	Требования к обеспечению защиты информации	Сведения и/или документы, подтверждающие готовность выполнения Клиентом требований к обеспечению защиты информации
	обеспечено применение программного обеспечения, распространяемого оператором платформы цифрового рубля (далее – оператор платформы), в составе мобильного приложения.	
8	Клиентом обеспечено хранение электронных сообщений, подписываемых электронной подписью и признаваемых в соответствии со статьей 6 Федерального закона от 6 апреля 2011 года № 63-ФЗ «Об электронной подписи» (далее – Федеральный закон № 63-ФЗ) электронными документами, равнозначными документам на бумажном носителе, подписанным собственноручной подписью, и средств, обеспечивающих проверку электронной подписи, не менее пяти лет с даты подписания электронных сообщений в соответствии со сроками хранения документов из перечня документов, предусмотренного частью 1.1 статьи 23 Федерального закона от 22 октября 2004 года № 125-ФЗ «Об архивном деле в Российской Федерации».	
9	Клиентом обеспечено осуществление сбора, передачи оператору платформы и обновление идентификационной информации устройства пользователя платформы, на котором установлено мобильное приложение, сформированной в виде производного значения из значений параметров такого устройства, позволяющего идентифицировать устройство пользователя платформы при совершении операций с цифровыми рублями (далее − цифровой отпечаток устройства).	
10	В целях осуществления передачи цифрового отпечатка устройства и обновления цифрового отпечатка устройства, хранимого на платформе цифрового рубля, Клиентом обеспечено удостоверение того, что устройство используется пользователем платформы, указанным в договоре счета цифрового рубля, предусмотренном статьей 30.8 Федерального закона № 161-ФЗ.	
11	Клиентом обеспечено подписание электронных сообщений Клиента электронной подписью, сертификат ключа	

№ п/п	Требования к обеспечению защиты информации	Сведения и/или документы, подтверждающие готовность выполнения Клиентом требований к обеспечению защиты информации
	проверки которой выдан удостоверяющим центром Банка России в соответствии со статьей 13 Федерального закона № 63-ФЗ.	
12	Клиентом обеспечено подписание электронных сообщений пользователя платформы электронной подписью, сертификат ключа проверки которой выдан удостоверяющим центром Клиента, подчиненным удостоверяющему центру Банка России.	
13	Клиентом обеспечено осуществление контроля срока действия ключа электронной подписи пользователя платформы и ключа проверки электронной подписи пользователя платформы.	
14	Клиентом при создании и функционировании удостоверяющего центра Клиента обеспечено использование средств удостоверяющего центра не ниже класса КС3, предусмотренного пунктом 11 Требований к средствам удостоверяющего центра, утвержденных приказом Федеральной службы безопасности Российской Федерации от 27 декабря 2011 года № 796 (далее – приказ ФСБ России № 796).	
15	Клиентом при эксплуатации средств удостоверяющего центра обеспечено использование информации о точном значении московского времени и календарной дате, распространяемой Государственной службой времени, частоты и определения параметров вращения Земли в соответствии с частью 3 статьи 6 Федерального закона от 3 июня 2011 года № 107-ФЗ «Об исчислении времени».	
16	Для подписания сертификатов ключей проверки электронных подписей пользователей платформы в удостоверяющем центре Клиента обеспечено использование ключа электронной подписи, соответствующего ключу проверки электронной подписи, указанному в сертификате, выданном удостоверяющим центром Банка России в соответствии со статьей 13 Федерального закона № 63-ФЗ.	
17	При взаимодействии между Клиентом и	

№ п/п	Требования к обеспечению защиты информации	Сведения и/или документы, подтверждающие готовность выполнения Клиентом требований к обеспечению защиты информации
	пользователем платформы с использованием приложения Клиента Клиентом обеспечено изготовление и использование криптографических ключей пользователя платформы, включая ключи электронных подписей, ключи проверки электронных подписей и криптографические ключи, предназначенные для шифрования (расшифрования) на прикладном уровне электронных сообщений, с применением СКЗИ, прошедших процедуру оценки соответствия требованиям, установленным федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, при осуществлении регулирования в соответствии с пунктом «ш» части первой статьи 13 Федерального закона от 3 апреля 1995 года № 40-ФЗ «О федеральной службе безопасности» (далее – требования, установленные федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности).	
18	Клиентом обеспечено применение программного обеспечения, распространяемого оператором платформы, для хранения криптографических ключей пользователя платформы, в иных случаях Клиент вправе применять организационно-технические меры для осуществления хранения криптографических ключей на внешних отчуждаемых носителях ключевой информации пользователя платформы в дополнение к требованиям эксплуатационной документации на используемые СКЗИ.	
19	Клиентом обеспечено изготовление, хранение и использование криптографических ключей Клиента, включая ключи электронных подписей, ключи проверки электронных подписей и криптографические ключи, предназначенные для шифрования (расшифрования) на прикладном уровне электронных сообщений, с использованием объектов информационной инфраструктуры Клиента, с применением СКЗИ, прошедших процедуру оценки соответствия требованиям,	

№ п/п	Требования к обеспечению защиты информации	Сведения и/или документы, подтверждающие готовность выполнения Клиентом требований к обеспечению защиты информации
	установленным федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности.	
20	Клиентом обеспечена возможность передачи в удостоверяющий центр Клиента запроса на выдачу сертификата ключа проверки электронной подписи пользователя платформы, инициируемого пользователем платформы, с использованием приложения Клиента.	
21	Клиентом обеспечена защита электронных сообщений при передаче между Клиентом и оператором платформы посредством:	
21.1	Использования усиленной неквалифицированной электронной подписи, реализуемой средствами электронной подписи класса не ниже КС3, предусмотренного пунктом 15 Требований к средствам электронной подписи, утвержденных приказом ФСБ России № 796 (далее – Требования к средствам электронной подписи), для контроля целостности и подтверждения подлинности электронных сообщений, в том числе применяемой для контроля целостности и подтверждения подлинности электронных сообщений пользователей платформы.	
21.2	Шифрования (расшифрования) электронных сообщений на прикладном уровне в соответствии с эталонной моделью взаимосвязи открытых систем, предусмотренной пунктом 1.7 раздела 1 государственного стандарта Российской Федерации ГОСТ Р ИСО/МЭК 7498-1-99 «Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 1. Базовая модель» (далее – ГОСТ Р ИСО/МЭК 7498-1-99), с использованием СКЗИ класса не ниже КС3, предусмотренного пунктом 12 Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством	

№ п/п	Требования к обеспечению защиты информации	Сведения и/или документы, подтверждающие готовность выполнения Клиентом требований к обеспечению защиты информации
	Российской Федерации требований к защите персональных данных для каждого из уровней защищенности, утвержденных приказом Федеральной службы безопасности Российской Федерации от 10 июля 2014 года № 378 (далее – Состав и содержание организационных и технических мер), прошедших процедуру оценки соответствия требованиям, установленным федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности.	
21.3	Обработки электронных сообщений и контроля реквизитов электронных сообщений с использованием объектов информационной инфраструктуры в соответствии с Требованиями к обеспечению защиты информации, применяемыми в отношении технологии обработки и передачи электронных сообщений при осуществлении операций с цифровыми рублями, предусмотренными нормативным актом Банка России, устанавливающим требования к обеспечению защиты информации для участников платформы цифрового рубля.	
21.4	Использования технологии виртуальных частных сетей между Клиентом и оператором платформы с использованием СКЗИ класса не ниже КС2, предусмотренного пунктом 11 Состава и содержания организационных и технических мер.	
22	Клиентом обеспечена защита электронных сообщений при их передаче между пользователем платформы и Клиентом посредством:	
22.1	Использования усиленной неквалифицированной электронной подписи, реализуемой средствами электронной подписи класса не ниже КС3 на стороне Клиента и средствами электронной подписи класса не ниже КС1 на стороне пользователя платформы, предусмотренными пунктами 15 и 13 Требований к средствам электронной подписи соответственно, для контроля целостности и подтверждения подлинности электронных сообщений.	
22.2	Шифрования (расшифрования) электронных сообщений на прикладном уровне в	

№ п/п	Требования к обеспечению защиты информации	Сведения и/или документы, подтверждающие готовность выполнения Клиентом требований к обеспечению защиты информации
	соответствии с эталонной моделью взаимосвязи открытых систем, предусмотренной пунктом 1.7 раздела 1 ГОСТ Р ИСО/МЭК 7498-1-99, с использованием СКЗИ класса не ниже КС3 на стороне Клиента и СКЗИ класса не ниже КС1 на стороне пользователя платформы, предусмотренных пунктами 12 и 10 Состава и содержания организационных и технических мер соответственно, прошедших процедуру оценки соответствия требованиям, установленным федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности.	
22.3	Применения СКЗИ класса не ниже КС2, предусмотренного пунктом 11 Состава и содержания организационных и технических мер, на стороне Клиента и СКЗИ класса не ниже КС1, предусмотренного пунктом 10 Состава и содержания организационных и технических мер, на стороне пользователя платформы, через использование которых реализуются двухсторонняя аутентификация и шифрование информации на уровне представления или ниже, в соответствии с эталонной моделью взаимосвязи открытых систем, предусмотренной пунктом 1.7 раздела 1 ГОСТ Р ИСО/МЭК 7498-1-99, прошедших процедуру оценки соответствия требованиям, установленным федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности.	
23	Клиентом обеспечен для объектов информационной инфраструктуры, размещенных в выделенных сегментах (группах сегментов) вычислительных сетей, указанных в пунктах 1, 2 настоящей таблицы, уровень соответствия не ниже четвертого, предусмотренного подпунктом «д» пункта 6.9 раздела 6 национального стандарта Российской Федерации ГОСТ Р 57580.2-2018 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Методика оценки соответствия».	

№ п/п	Требования к обеспечению защиты информации	Сведения и/или документы, подтверждающие готовность выполнения Клиентом требований к обеспечению защиты информации
24	Клиентом для обеспечения безопасности технологии обработки и передачи электронных сообщений при осуществлении операций с цифровыми рублями реализованы в своей информационной инфраструктуре два выделенных контура: контур контроля и контур обработки.	
25	Клиентом реализованы в своей информационной инфраструктуре контур контроля и контур обработки с использованием разных рабочих мест, разных криптографических ключей и с привлечением отдельных работников для каждого из контуров.	
26	Объекты информационной инфраструктуры контура обработки и контура контроля размещены Клиентом в разных сегментах вычислительной сети. Способ допустимого информационного взаимодействия между указанными сегментами вычислительной сети оформлен документально и согласован со службой информационной безопасности Клиента.	
27	Клиентом обеспечено соблюдение следующих условий при направлении и обработке электронных сообщений:	
27.1	Исходящие электронные сообщения, направляемые Клиентом на платформу цифрового рубля, поступают в контур контроля только из контура обработки.	
27.2	Входящие электронные сообщения, получаемые Клиентом от платформы цифрового рубля, из контура контроля передаются только в контур обработки, в том числе для последующей передачи пользователю платформы (при необходимости).	
28	Клиентом в контуре обработки для исходящих электронных сообщений, направляемых Клиентом на платформу цифрового рубля, реализованы:	
28.1	Расшифрование электронного сообщения.	
28.2	Проверка электронной подписи, с использованием которой подписано электронное сообщение.	
28.3	Структурный контроль электронного сообщения.	
28.4	Проверка правильности заполнения полей электронного сообщения.	

№ п/п	Требования к обеспечению защиты информации	Сведения и/или документы, подтверждающие готовность выполнения Клиентом требований к обеспечению защиты информации
28.5	Подписание электронного сообщения электронной подписью Клиента.	
28.6	Направление электронного сообщения в контур контроля.	
29	Клиентом в контуре контроля для исходящих электронных сообщений, направляемых Клиентом на платформу цифрового рубля, реализованы:	
29.1	Проверка электронной подписи, с использованием которой подписано электронное сообщение.	
29.2	Структурный контроль электронного сообщения.	
29.3	Проверка правильности заполнения полей электронного сообщения.	
29.4	Контроль отсутствия дублирования электронного сообщения.	
29.5	Подписание электронного сообщения электронной подписью Клиента.	
29.6	Шифрование электронного сообщения, передаваемого на платформу цифрового рубля.	
30	Клиентом в контуре контроля для входящих электронных сообщений, получаемых Клиентом от платформы цифрового рубля, обеспечены:	
30.1	Расшифрование электронного сообщения.	
30.2	Проверка электронной подписи, с использованием которой подписано электронное сообщение.	
30.3	Структурный контроль электронного сообщения.	
30.4	Подписание электронного сообщения электронной подписью Клиента.	
30.5	Направление электронного сообщения в контур обработки.	
31	Клиентом в контуре обработки для входящих электронных сообщений, получаемых Клиентом от платформы цифрового рубля, обеспечены:	
31.1	Проверка электронной подписи, с использованием которой подписано электронное сообщение.	
31.2	Структурный контроль электронного сообщения.	
31.3	Проверка правильности заполнения полей электронного сообщения.	
31.4	Контроль отсутствия дублирования электронного сообщения.	
31.5	Шифрование электронного сообщения, передаваемого пользователю платформы.	

№ п/п	Требования к обеспечению защиты информации	Сведения и/или документы, подтверждающие готовность выполнения Клиентом требований к обеспечению защиты информации
32	Клиент для обеспечения безопасности приложения Клиента:	
32.1	Имеет документированный процесс разработки, тестирования и эксплуатации приложения Клиента, включая описания реализуемых мер, контролей и проверок по обеспечению защиты информации, а также процесс управления версиями и изменениями программного обеспечения, реализующего приложение Клиента.	
32.2	Применяет меры защиты информации в соответствии с пунктом 2 настоящей таблицы для объектов информационной инфраструктуры, с использованием которых обеспечиваются эксплуатация и функционирование приложения Клиента.	
33	Клиентом обеспечено выполнение следующих требований к безопасности приложения Клиента:	
33.1	Реализован механизм доставки пользователям платформы уведомлений об операциях с цифровыми рублями.	
33.2	Реализован механизм обработки ошибок и (или) исключений, возникающих в процессе работы приложения Клиента, в рамках которого обеспечиваются корректная обработка и информирование пользователей платформы об ошибках, в том числе о сбоях при подключении к приложению Клиента, недоступности приложения Клиента.	
33.3	Реализован механизм проверки корректности данных, вводимых пользователем платформы в приложении Клиента.	
33.4	Осуществляется регистрация событий защиты информации (в том числе событий, связанных с неуспешной аутентификацией и авторизацией, ошибками при управлении доступом и проверке входных данных) при функционировании приложения Клиента.	
33.5	Реализован механизм незамедлительной блокировки и последующего досрочного прекращения действия или аннулирования сертификата ключа проверки электронной подписи пользователя платформы в случае компрометации ключа электронной подписи.	
34	Клиент вправе принимать организационно-технические меры, направленные на соответствие требованиям к безопасности мобильного приложения, в том числе в части наличия возможности:	

№ п/п	Требования к обеспечению защиты информации	Сведения и/или документы, подтверждающие готовность выполнения Клиентом требований к обеспечению защиты информации
34.1	Реализации механизма информирования пользователя платформы о необходимости применения обновлений мобильного приложения, связанных с обеспечением защиты информации.	
34.2	Реализации альтернативных способов обновления и (или) установки мобильного приложения в случае наличия ограничений обновления и (или) установки мобильного приложения из основного источника.	
34.3	Реализации механизма, исключающего возможность использования сторонних программных средств ввода и отключения механизма регистрации истории ввода при вводе данных пользователей платформы, в том числе аутентификационных данных пользователя платформы.	
34.4	Обеспечения контроля целостности прикладного программного обеспечения и контроля среды его функционирования при запуске мобильного приложения до момента обращения пользователя платформы к его функционалу.	
34.5	Реализации механизма блокировки доступа к мобильному приложению при неоднократных неуспешных попытках аутентификации.	

Заключение

Комиссия считает, что _____
(указывается полное фирменное наименование кредитной организации)
готова выполнить требования к обеспечению защиты информации для участников платформы цифрового рубля.

Руководитель Комиссии

Члены Комиссии:

_____ (инициалы, фамилия)	_____ (подпись, дата)
_____ (инициалы, фамилия)	_____ (подпись, дата)
_____ (инициалы, фамилия)	_____ (подпись, дата)
_____ (инициалы, фамилия)	_____ (подпись, дата)

Приложения:

1. Документы, подтверждающие полномочия заместителя руководителя Клиента на утверждение акта.
2. Распорядительный документ о создании комиссии для проверки готовности выполнения требований к обеспечению защиты информации для участников платформы цифрового рубля.
3. Документы, подтверждающие готовность выполнения требований к обеспечению защиты информации для участников платформы цифрового рубля.