Приложение 2 к Договору

_____ от «____» _____20__г.

Условия по защите информации[1]

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»[2] 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,

[1] 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.

[2] 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[3])

_____
(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[4] _____, 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)

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

[3] 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.

[4] 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.