Проект

ЦЕНТРАЛЬНЫЙ БАНК РОССИЙСКОЙ ФЕДЕРАЦИИ
(БАНК РОССИИ)

П О Л О Ж Е Н И Е

« » _____ 2023 г. № _____-П

г. Москва

О требованиях к обеспечению защиты информации для участников платформы цифрового рубля

Настоящее Положение на основании пункта 7 части 1, части 3 статьи 30^7 Федерального закона от 27 июня 2011 года № 161-ФЗ «О национальной платежной системе», части пятой статьи 5 Федерального закона от 2 декабря 1990 года № 395-I «О банках и банковской деятельности» устанавливает требования к обеспечению защиты информации для участников платформы цифрового рубля.

1. Требования к обеспечению защиты информации для участников платформы цифрового рубля (далее – требования к защите информации) должны выполнять участники платформы цифрового рубля, являющиеся кредитными организациями (далее – участники платформы цифрового рубля).

2. Требования к защите информации распространяются на автоматизированные системы, программное обеспечение, средства вычислительной техники, телекоммуникационное оборудование, эксплуатация которых обеспечивается участником платформы цифрового рубля и которые используются при формировании (подготовке), обработке, передаче и хранении защищаемой информации (далее – объекты информационной инфраструктуры):

информации, содержащейся в документах, составленных при осуществлении операций с цифровыми рублями, формируемых участником платформы цифрового рубля, пользователями платформы цифрового рубля и оператором платформы цифрового рубля;

информации, необходимой для идентификации, аутентификации и авторизации пользователей платформы цифрового рубля при совершении действий в целях осуществления операций с цифровыми рублями;

о приостановлении, возобновлении или прекращении доступа к платформе цифрового рубля, закрытии счета цифрового рубля (далее – статус счета цифрового рубля), а также о статусе операций с цифровыми рублями;

об исполненных и планируемых к исполнению сделках, содержащих условия, предусмотренные абзацем вторым статьи 309 Гражданского кодекса Российской Федерации;

об операциях с цифровыми рублями и остатке цифровых рублей на счете цифрового рубля (далее – остаток цифровых рублей);

ключевой информации средств криптографической защиты информации (далее – СКЗИ), используемых для обеспечения криптографической защиты операций с цифровыми рублями;

о конфигурации, определяющей параметры работы объектов информационной инфраструктуры, а также информации о конфигурации, определяющей параметры работы технических средств защиты информации.

При обеспечении безопасности объектов информационной инфраструктуры, эксплуатация которых обеспечивается участниками платформы цифрового рубля, являющихся объектами критической информационной инфраструктуры, настоящее Положение применяется наряду с требованиями, предусмотренными Федеральным законом от 26 июля 2017 года № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».

3. Участники платформы цифрового рубля при обеспечении

возможности совершения операций с цифровыми рублями должны размещать объекты информационной инфраструктуры в выделенных сегментах (группах сегментов) вычислительных сетей.

Для объектов информационной инфраструктуры в пределах выделенного сегмента (группы сегментов) вычислительных сетей участники платформы цифрового рубля должны применять меры защиты информации, реализующие стандартный 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», утвержденного приказом Федерального агентства по техническому регулированию и метрологии от 8 августа 2017 года № 822-ст «Об утверждении национального стандарта Российской Федерации»[1] и введенного в действие 1 января 2018 года (далее – ГОСТ Р 57580.1-2017).

Для объектов информационной инфраструктуры в пределах выделенного сегмента (группы сегментов) вычислительных сетей участники платформы цифрового рубля, являющиеся системно значимыми кредитными организациями и (или) кредитными организациями, значимыми на рынке платежных услуг, должны применять меры защиты информации, реализующие усиленный уровень защиты информации, предусмотренный пунктом 6.7 раздела 6 ГОСТ Р 57580.1-2017.

4. Участники платформы цифрового рубля во внутренних документах должны определить состав организационных мер защиты информации и порядок их применения, а также состав технических средств защиты информации и порядок их использования.

Участники платформы цифрового рубля при разработке внутренних документов должны определить:

[1] М., ФГУП «Стандартинформ», 2017.

порядок подготовки, обработки, передачи и хранения сообщений, связанных с осуществлением операций с цифровыми рублями (далее – электронные сообщения), и защищаемой информации на объектах информационной инфраструктуры;

список лиц, допущенных к работе с СКЗИ, с определением прав использования криптографических ключей;

список лиц, ответственных за обеспечение функционирования и безопасности СКЗИ (ответственные пользователи СКЗИ);

список лиц, обладающих правами по управлению криптографическими ключами, в том числе список лиц, ответственных за формирование криптографических ключей и обеспечение безопасности криптографических ключей;

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.

5. Защита информации с использованием СКЗИ должна обеспечиваться участниками платформы цифрового рубля в соответствии с Положением о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005), утвержденным приказом Федеральной службы безопасности Российской Федерации от 9 февраля 2005 года № 66[1], и технической документацией на СКЗИ.

6. Формирование и обработка электронных сообщений участников платформы цифрового рубля и пользователей платформы цифрового рубля, а также уведомлений, направляемых пользователю платформы цифрового

[1] Зарегистрирован Минюстом России 3 марта 2005 года, регистрационный № 6382, с изменениями, внесенными приказом ФСБ России от 12 апреля 2010 года № 173 (зарегистрирован Минюстом России 25 мая 2010 года, регистрационный № 17350).

рубля, должны осуществляться в соответствии с Альбомом электронных сообщений, предусмотренным частью 6 статьи 30^7 Федерального закона от 27 июня 2011 года № 161-ФЗ «О национальной платежной системе» (далее соответственно – Альбом электронных сообщений, Федеральный закон № 161-ФЗ).

7. Формирование и подписание электронных сообщений участника платформы цифрового рубля должны осуществляться в автоматизированной системе участника платформы цифрового рубля.

Формирование и подписание электронных сообщений пользователя платформы цифрового рубля должны осуществляться пользователем платформы цифрового рубля с использованием электронного средства 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).

8. Участники платформы цифрового рубля должны хранить входящие и исходящие электронные сообщения, подписанные электронной подписью в соответствии с частью 2 статьи 6 Федерального закона от 6 апреля 2011 года № 63-ФЗ «Об электронной подписи», и средства, обеспечивающие проверку электронной подписи, не менее пяти лет с даты подписания электронных сообщений.

9. Участники платформы цифрового рубля должны осуществлять сбор, передачу на платформу цифрового рубля и обновление идентификационной информации устройства пользователя платформы цифрового рубля, сформированной в виде производного значения из значений параметров устройства, позволяющего идентифицировать устройство пользователя при совершении операций с цифровыми рублями (далее − цифровой отпечаток устройства), используемых при совершении операций с цифровыми рублями с использованием мобильного приложения.

В целях осуществления передачи и обновления цифрового отпечатка устройства, хранимого на платформе цифрового рубля, участник платформы цифрового рубля должен удостовериться, что устройство принадлежит данному пользователю платформы цифрового рубля.

10. При обмене электронными сообщениями участником платформы цифрового рубля должна применяться электронная подпись, сертификат ключа проверки которой выдан удостоверяющим центром Банка России.

При обмене электронными сообщениями пользователем платформы цифрового рубля должна применяться электронная подпись, сертификат ключа проверки которой выдан удостоверяющим центром участника платформы цифрового рубля. Контроль срока действия сертификата ключа проверки электронной подписи пользователя платформы цифрового рубля должен осуществляться участником платформы цифрового рубля.

Удостоверяющий центр участника платформы цифрового рубля и удостоверяющий центр Банка России должны быть реализованы с использованием средств удостоверяющего центра класса 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[1] (далее – приказ ФСБ России от 27 декабря 2011 года № 796).

Для создания сертификатов ключей проверки электронных подписей пользователей платформы цифрового рубля удостоверяющий центр участника платформы цифрового рубля должен использовать ключ электронной подписи, сертификат которого выдан удостоверяющим центром Банка России.

При взаимодействии между участниками платформы цифрового рубля и пользователями платформы цифрового рубля с использованием приложения

[1] Зарегистрирован Минюстом России 9 февраля 2012 года, регистрационный № 23191, с изменениями, внесенными приказами ФСБ России от 4 декабря 2020 года № 555 (зарегистрирован Минюстом России 30 декабря 2020 года, регистрационный № 61972), от 13 апреля 2021 года № 142 (зарегистрирован Минюстом России 20 мая 2021 года, регистрационный № 63528), от 13 апреля 2022 года № 179 (зарегистрирован Минюстом России 11 мая 2022 года, регистрационный № 68446).

клиента изготовление и использование криптографических ключей пользователя платформы цифрового рубля, предназначенных для подписания (проверки подписи) и (или) шифрования (расшифрования) на прикладном уровне электронных сообщений, должны осуществляться с применением СКЗИ, имеющих подтверждение соответствия требованиям, установленным федеральным органом исполнительной власти 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 в области обеспечения безопасности).

Хранение криптографических ключей пользователя платформы цифрового рубля, предназначенных для подписания (проверки подписи) и (или) шифрования (расшифрования) на прикладном уровне электронных сообщений в системе ДБО участника платформы цифрового рубля, должно осуществляться на устройстве пользователя платформы цифрового рубля или внешних отчуждаемых носителях ключевой информации пользователя платформы цифрового рубля в соответствии с требованиями эксплуатационной документации к используемым СКЗИ, прошедшим процедуру оценки соответствия требованиям, установленным федеральным органом исполнительной власти в области обеспечения безопасности. Участники платформы цифрового рубля должны обеспечивать невозможность экспорта криптографических ключей из устройства пользователя платформы цифрового рубля или из внешних отчуждаемых носителях ключевой информации пользователя платформы цифрового рубля.

Изготовление, хранение и использование криптографических ключей участника платформы цифрового рубля, предназначенных для подписания (проверки подписи) и (или) шифрования (расшифрования) на прикладном уровне электронных сообщений, должны осуществляться с использованием объектов информационной инфраструктуры участника платформы цифрового

рубля.

Запрос на выдачу сертификата ключа проверки электронной подписи пользователя платформы цифрового рубля инициируется пользователем платформы цифрового рубля и передается в удостоверяющий центр участника платформы цифрового рубля с использованием приложения участника платформы цифрового рубля.

В случае аннулирования сертификата ключа проверки электронной подписи пользователя платформы цифрового рубля удостоверяющий центр участника платформы цифрового рубля должен предоставить на платформу цифрового рубля информацию о таком сертификате ключа проверки электронной подписи.

11. Организационные меры и (или) технические средства защиты информации, используемые при обмене электронными сообщениями при осуществлении операций с цифровыми рублями, применяются с соблюдением следующих требований:

11.1. Участники платформы цифрового рубля должны обеспечивать защиту электронных сообщений при передаче между участниками платформы цифрового рубля и платформой цифрового рубля посредством:

использования усиленной неквалифицированной электронной подписи для контроля целостности и подтверждения подлинности электронных сообщений, в том числе применяемой для контроля целостности и подтверждения подлинности электронных сообщений пользователей платформы цифрового рубля;

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 от 27 декабря 2011 года № 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 цифрового рубля;

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», принятого постановлением Государственного комитета Российской Федерации по стандартизации и метрологии от 18 марта 1999 года № 78[1] и введенного в действие 1 января 2000 года (далее – ГОСТ Р ИСО/МЭК 7498-1-99), с использованием СКЗИ, прошедших процедуру оценки соответствия требованиям, установленным федеральным органом исполнительной власти в области обеспечения безопасности;

шифрования (расшифрования) электронных сообщений на прикладном уровне в 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, 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 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[2] (далее – Состав и содержание организационных и технических мер), прошедших процедуру оценки соответствия требованиям, установленным федеральным органом исполнительной власти в области обеспечения безопасности;

обработки электронных сообщений и контроля реквизитов

[1] М., ИПК Издательство стандартов, 1999.
[2] Зарегистрирован Минюстом России 18 августа 2014 года, регистрационный № 33620.

электронных сообщений с использованием объектов информационной инфраструктуры в соответствии с Правилами материально-технического обеспечения обработки электронных сообщений и контроля реквизитов электронных сообщений в информационной инфраструктуре участника платформы цифрового рубля, установленными приложением 1 к настоящему Положению;

использования технологии виртуальных частных сетей между участником платформы цифрового рубля и платформой цифрового рубля с применением криптографических алгоритмов, определенных национальными стандартами Российской Федерации, реализуемых с использованием СКЗИ класса не ниже КС2, предусмотренного пунктом 11 Состава и содержания организационных и технических мер.

11.2. Участники платформы цифрового рубля должны обеспечивать защиту электронных сообщений при их передаче между пользователями платформы цифрового рубля и участниками платформы цифрового рубля посредством:

использования усиленной неквалифицированной электронной подписи, реализуемой средствами электронной подписи класса не ниже КС3 на стороне участника платформы цифрового рубля и средствами электронной подписи класса не ниже КС1 на стороне пользователя платформы цифрового рубля, предусмотренными соответственно пунктами 15 и 13 Требований к средствам электронной подписи, для контроля целостности и подтверждения подлинности электронных сообщений;

шифрования (расшифрования) электронных сообщений на прикладном уровне в 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 участника платформы цифрового рубля и СКЗИ класса не ниже КС1 на стороне пользователя платформы цифрового рубля, предусмотренных соответственно пунктами 12 и 10 Состава и содержания организационных и технических мер, прошедших

процедуру оценки соответствия требованиям, установленным федеральным органом исполнительной власти в области обеспечения безопасности;

применения средств криптографической защиты информации класса предусмотренного пунктом 11 Состава и содержания организационных и технических мер, не ниже КС2 на стороне участника платформы цифрового рубля и средств защиты информации класса не ниже КС1 на стороне пользователя платформы цифрового рубля, посредством использования которых реализуется 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 в области обеспечения безопасности.

12. Участники платформы цифрового рубля должны проводить оценку выполнения ими требований к защите информации при обеспечении возможности совершения операций с цифровыми рублями (далее – оценка соответствия) не реже одного раза в два года с привлечением сторонних организаций, имеющих лицензию на проведение работ и услуг, предусмотренных подпунктом «б» пункта 4 Положения о лицензировании деятельности по технической защите конфиденциальной информации, утвержденного постановлением Правительства Российской Федерации от 3 февраля 2012 года № 79 «О лицензировании деятельности по технической защите конфиденциальной информации» (далее – проверяющая организация).

Участники платформы цифрового рубля должны проводить оценку соответствия с учетом следующих требований:

оценка соответствия должна проводиться в пределах выделенных сегментов (группы сегментов) вычислительных сетей;

оценка соответствия должна осуществляться в соответствии с разделом 6 национального стандарта Российской Федерации ГОСТ Р 57580.2-2018 «Безопасность финансовых (банковских) операций. Защита информации

финансовых организаций. Методика оценки соответствия», утвержденного приказом Федерального агентства по техническому регулированию и метрологии от 28 марта 2018 года № 156-ст[1] и введенного в действие 1 сентября 2018 года (далее – ГОСТ Р 57580.2-2018);

участники платформы цифрового рубля должны обеспечивать хранение отчета, подготовленного проверяющей организацией по результатам оценки соответствия, не менее пяти лет, начиная с даты его выдачи проверяющей организацией.

Участники платформы цифрового рубля должны обеспечивать для объектов информационной инфраструктуры, размещенных в выделенных сегментах (группах сегментов) вычислительных сетей, указанных в пункте 3 настоящего Положения, уровень соответствия не ниже третьего уровня соответствия, предусмотренного подпунктом «г» пункта 6.9 раздела 6 ГОСТ Р 57580.2-2018.

Участники платформы цифрового рубля должны обеспечивать для объектов информационной инфраструктуры, размещенных в выделенных сегментах (группах сегментов) вычислительных сетей, указанных в пункте 3 настоящего Положения, уровень соответствия не ниже четвертого уровня соответствия, предусмотренного подпунктом «д» пункта 6.9 раздела 6 ГОСТ Р 57580.2-2018.

Участники платформы цифрового рубля должны обеспечить ежегодное тестирование на проникновение и анализ уязвимостей информационной безопасности объектов информационной инфраструктуры, размещенных в отдельных выделенных сегментах (группах сегментов) вычислительных сетей.

13. Участники платформы цифрового рубля должны обеспечить соответствие приложения клиента требованиям, установленным в приложении 2 к настоящему Положению.

[1] М., ФГУП «Стандартинформ», 2018.

14. Настоящее Положение подлежит официальному опубликованию и вступает в силу по истечении 10 дней после дня его официального опубликования, за исключением положений, для которых настоящим пунктом установлены иные сроки вступления в силу.

Абзац второй пункта 9, абзац четвертый подпункта 11.2 пункта 11, абзац седьмой пункта 12 вступают в силу с 1 января 2024 года.

Абзацы второй и четвертый подпункта 11.1 пункта 11 утрачивают силу 30 июня 2024 года.

Абзацы третий и пятый подпункта 11.1 пункта 11 вступают в силу с 1 июля 2024 года.

Председатель
Центрального банка
Российской Федерации Э.С. Набиуллина

Согласовано:

Директор
Федеральной службы безопасности
Российской Федерации
_____ А.В. Бортников
_____ 2023 г.

Директор
Федеральной службы по техническому
и экспортному контролю
Российской Федерации
_____ В.В. Селин
_____ 2023 г.

Приложение 1
к Положению Банка России
от «___» _____ 2023 года № ___-П
«О требованиях к обеспечению защиты
информации для участников платформы
цифрового рубля»

Правила материально-технического обеспечения обработки электронных сообщений и контроля реквизитов электронных сообщений в информационной инфраструктуре участника платформы цифрового рубля

Для обеспечения безопасности технологии обработки и передачи электронных сообщений с использованием объектов информационной инфраструктуры участником платформы цифрового рубля должны быть реализованы два выделенных контура: контур контроля и контур обработки.

Контур контроля и контур обработки реализуются с учетом следующих требований:

1. Контур контроля и контур обработки в информационной инфраструктуре участника платформы цифрового рубля реализуются с использованием разных рабочих мест, разных криптографических ключей и с привлечением отдельных работников для каждого из контуров.

2. Объекты информационной инфраструктуры контура обработки и контура контроля размещаются в разных сегментах вычислительных сетей, в том числе реализованных с использованием технологии виртуализации. Способ допустимого информационного взаимодействия между указанными сегментами вычислительных сетей оформляется документально и согласовывается со службой информационной безопасности участника платформы цифрового рубля.

3. Направление и обработка электронных сообщений должны осуществляться участниками платформы цифрового рубля таким образом, чтобы все исходящие электронные сообщения на платформу цифрового рубля

поступали в контур контроля только из контура обработки, а все входящие электронные сообщения из платформы цифрового рубля из контура контроля передавались только в контур обработки, в том числе для последующей передачи пользователю платформы цифрового рубля (при необходимости).

4. Для исходящих электронных сообщений, направляемых участником платформы цифрового рубля на платформу цифрового рубля, в контуре обработки должны быть реализованы:

расшифрование электронного сообщения;

проверка электронной подписи, с использованием которой удостоверено электронное сообщение;

структурный контроль электронного сообщения;

проверка правильности заполнения полей электронного сообщения;

подписание электронного сообщения электронной подписью;

направление электронного сообщения в контур контроля.

5. Для исходящих электронных сообщений, направляемых участником платформы цифрового рубля на платформу цифрового рубля, в контуре контроля должны быть реализованы:

проверка электронной подписи, с использованием которой удостоверено электронное сообщение;

структурный контроль электронного сообщения;

проверка правильности заполнения полей электронного сообщения;

контроль отсутствия дублирования электронного сообщения;

подписание электронного сообщения электронной подписью;

шифрование электронного сообщения, передаваемого на платформу цифрового рубля.

6. Для входящих электронных сообщений, получаемых участником платформы цифрового рубля из платформы цифрового рубля, в контуре контроля должны осуществляться:

расшифрование электронного сообщения;

проверка электронной подписи, с использованием которой удостоверено

электронное сообщение;

структурный контроль электронного сообщения;

подписание электронного сообщения электронной подписью;

направление электронного сообщения в контур обработки.

7. Для входящих электронных сообщений, получаемых участником платформы цифрового рубля из платформы цифрового рубля, в контуре обработки должны осуществляться:

проверка электронной подписи, с использованием которой удостоверено электронное сообщение;

структурный контроль электронного сообщения;

проверка правильности заполнения полей электронного сообщения;

контроль отсутствия дублирования электронного сообщения;

шифрование электронного сообщения, передаваемого пользователю платформы цифрового рубля.

8. Состав и виды электронных подписей, указанных в пунктах 4−7 настоящего приложения, определяются в соответствии с Альбомом электронных сообщений, используемых для взаимодействия субъектов платформы цифрового рубля.

Приложение 2
к Положению Банка России
от «___» _____ 2023 года № ___-П
«О требованиях к обеспечению защиты информации для участников платформы цифрового рубля»

Требования к электронному средству 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

1. Участник платформы цифрового рубля должен выполнять следующие требования к электронному средства 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). Приложением клиента является система дистанционного банковского обслуживания (далее − ДБО участника платформы цифрового рубля), включая в том числе программное обеспечение для мобильных устройств (далее – мобильное приложение).

1.1. Участник платформы цифрового рубля должен иметь документированный процесс разработки, тестирования и эксплуатации приложения клиента, включая описания реализуемых мер, контролей и проверок по обеспечению информационной безопасности.

Участник платформы цифрового рубля должен иметь документированный процесс управления версиями и изменениями программного обеспечения, в том числе приложения клиента.

Инфраструктура участника платформы цифрового рубля, на которой выполняются процессы разработки, тестирования и развертывания, а также среды постоянной эксплуатации финансовой организации должна

соответствовать требованиям ГОСТ Р 57580.1-2017 с учетом определенного уровня защиты информации для финансовой организации и иметь соответствующее подтверждение оценки соответствия по ГОСТ Р 57580.2-2018. Инфраструктурные системы по обеспечению информационной безопасности и соответствующие требования к ним должны быть документированы.

1.2. Реализация механизма доставки уведомлений пользователям платформы цифрового рубля об операциях с цифровыми рублями.

1.3. Реализация механизма обработки ошибок и (или) исключений, которые могут возникать в процессе работы систем ДБО участника платформы цифрового рубля, в рамках которого обеспечивается корректная обработка и информирование пользователей платформы цифрового рубля об ошибках, в том числе о сбоях при подключении к системе ДБО участника платформы цифрового рубля, недоступности системы ДБО участника платформы цифрового рубля.

1.4. Реализация механизма проверки корректности данных, вводимых пользователем платформы цифрового рубля в систему ДБО участника платформы цифрового рубля.

1.5. Применение для хранения криптографических ключей пользователей платформы цифрового рубля внешних отчуждаемых ключевых носителей информации, сертифицированных в соответствии с требованиями федерального органа исполнительной власти, уполномоченного в области обеспечения безопасности, и/или федерального органа исполнительной власти, уполномоченного в области противодействия техническим разведкам и технической защиты информации, и разрешенных технической документацией к СКЗИ, либо реализация защищенного хранилища ключей в выделенной области долговременной памяти устройства пользователя платформы цифрового рубля, в случае если создание ключей электронной подписи осуществляется на этом устройстве.

1.6. Регистрация событий безопасности (в том числе событий

аутентификации и авторизации, ошибок управления доступом и проверки входных данных) применительно к компонентам системы ДБО участника платформы цифрового рубля, обеспечивающим осуществление операций с цифровыми рублями.

1.7. Реализация механизма незамедлительной блокировки и последующего аннулирования сертификата ключа проверки электронной подписи пользователя платформы цифрового рубля в случае компрометации закрытого ключа электронной подписи.

1.8. Аннулирование сертификата ключа проверки электронной подписи пользователя платформы цифрового рубля и смена аутентификационных данных для доступа пользователя платформы цифрового рубля к системе ДБО участника платформы цифрового рубля при изменении состава уполномоченных лиц пользователя платформы цифрового рубля – юридического лица, обладающих правом использования электронной подписи пользователя платформы цифрового рубля.

2. Участник платформы цифрового рубля должен выполнять следующие требования к мобильному приложению участника платформы цифрового рубля:

2.1. Реализация механизма информирования пользователей платформы цифрового рубля о необходимости обновления мобильного приложения участника платформы цифрового рубля, связанной с обеспечением информационной безопасности.

2.2. Реализация альтернативных способов обновления и (или) скачивания мобильного приложения участника платформы цифрового рубля в случае ограничений обновления и (или) скачивания мобильного приложения из основного источника.

2.3. Реализация механизма, исключающего возможность использования сторонних программных средств ввода и отключения механизма регистрации истории ввода при вводе данных пользователей платформы цифрового рубля, в том числе аутентификационных данных

пользователя платформы цифрового рубля.

2.4. Осуществление контроля целостности прикладного программного обеспечения и среды его функционирования при запуске мобильного приложения участника платформы цифрового рубля до момента обращения пользователя платформы цифрового рубля к его функционалу.

2.5. Реализация механизма блокировки доступа к мобильному приложению участника платформы цифрового рубля при неоднократных попытках аутентификации.

Пояснительная записка к проекту положения Банка России «О требованиях к обеспечению защиты информации для участников платформы цифрового рубля»

Банк России разработал проект положения Банка России «О требованиях к обеспечению защиты информации для участников платформы цифрового рубля» (далее – проект).

Полномочия Банка России по разработке проекта и принятию акта установлены пунктом 7 части 1, частью 3 статьи 30^7 Федерального закона от 27 июня 2011 года № 161-ФЗ «О национальной платежной системе».

В ходе весенней сессии 2023 года принят Федеральный закон «О внесении изменений в отдельные законодательные акты Российской Федерации в связи с внедрением цифрового рубля» (проект № 270838-8). Данный Федеральный закон вступает в силу с 1 августа 2023 года (за исключением отдельных положений) и содержит положения, наделяющие Банк России полномочиями по изданию нормативных актов.

Проект является частью правил платформы цифрового рубля.

Действие проекта распространяется на участников платформы цифрового рубля, являющихся кредитными организациями.

Проект разработан в целях установления требований к:

размещению объектов информационной инфраструктуры, используемых при осуществлении операций с цифровыми рублями;

определению состава и порядка применения организационных мер защиты информации, а также состава и порядка использования технических средств защиты информации;

использованию средств криптографической защиты информации;

применению электронной подписи участниками платформы цифрового рубля;

оценке участниками платформы цифрового рубля выполнения ими требований к обеспечению защиты информации при осуществлении операций с цифровыми рублями;

материально-техническому обеспечению обработки электронных сообщений и контроля реквизитов электронных сообщений в информационной инфраструктуре участника платформы цифрового рубля.

Ответственное структурное подразделение Банка России по проекту – Департамент информационной безопасности.

Предложения и замечания по проекту в рамках его публичного обсуждения в целях оценки регулирующего воздействия принимаются до 11 августа 2023 года по адресам: nikitinavl@cbr.ru и polivanovave@cbr.ru.