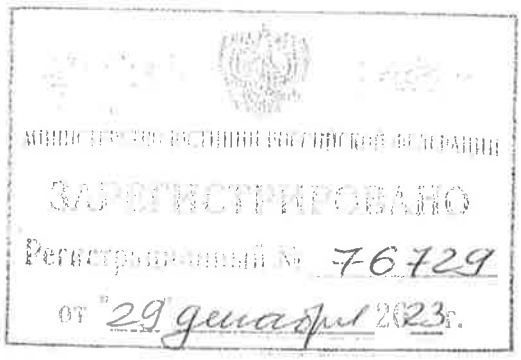
**ЦЕНТРАЛЬНЫЙ БАНК РОССИЙСКОЙ ФЕДЕРАЦИИ**
**(БАНК РОССИИ)**

# П О Л О Ж Е Н И Е

«7» декабря 2023 г. № 833-П

г. Москва




## О требованиях к обеспечению защиты информации для участников платформы цифрового рубля

Настоящее Положение на основании статьи $82^{10}$ Федерального закона от 10 июля 2002 года № 86-ФЗ «О Центральном банке Российской Федерации (Банке России)», пункта 7 части 1, части 3 статьи $30^{7}$ Федерального закона от 27 июня 2011 года № 161-ФЗ «О национальной платежной системе» и в соответствии с решением Совета директоров Банка России (протокол заседания Совета директоров Банка России от 27 сентября 2023 года

№ ПСД-39) 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 обеспечению защиты информации) должны выполнять участники платформы цифрового рубля, являющиеся кредитными организациями (далее – участники платформы).

2. Требования к обеспечению защиты информации распространяются на автоматизированные системы, программное обеспечение, средства вычислительной техники, телекоммуникационное оборудование, эксплуатация которых осуществляется участниками платформы и которые используются при формировании (подготовке), обработке, передаче и хранении следующей защищаемой информации (далее – объекты информационной инфраструктуры):

информации, содержащейся в документах, составленных при осуществлении операций с цифровыми рублями, формируемых участниками платформы, 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;

информации о предоставлении, приостановлении, возобновлении или прекращении доступа к платформе цифрового рубля, о счете цифрового рубля, об остатке цифровых рублей на счете цифрового рубля, а также о совершенных операциях с цифровыми рублями;

информации об исполненных и планируемых к исполнению сделках, содержащих условия, предусмотренные частью второй статьи 309 Гражданского кодекса Российской Федерации;

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

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

3. При обеспечении безопасности объектов информационной инфраструктуры, эксплуатация которых осуществляется участниками платформы и которые являются объектами критической информационной инфраструктуры Российской Федерации, применяются в том числе требования и порядок, установленные органами государственной власти Российской Федерации в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации в соответствии со статьей 6 Федерального закона от 26 июля 2017 года № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».

4. Участники платформы должны размещать объекты информационной инфраструктуры, используемые при обеспечении возможности совершения операций с цифровыми рублями, в выделенных сегментах (группах сегментов) вычислительных сетей.

4.1. Для объектов информационной инфраструктуры в пределах выделенного сегмента (группы сегментов) вычислительных сетей участники платформы, являющиеся кредитными организациями, которые определены как системно значимые 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) значимые на рынке платежных услуг в соответствии с частью 2 статьи $30^5$ Федерального закона от 27 июня

2011 года № 161-ФЗ «О национальной платежной системе» (далее – Федеральный закон № 161-ФЗ), должны применять организационные и технические меры, реализующие 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»[1] (далее – ГОСТ Р 57580.1-2017).

4.2. Для объектов информационной инфраструктуры в пределах выделенного сегмента (группы сегментов) вычислительных сетей участники платформы, не указанные в подпункте 4.1 настоящего пункта, в целях обеспечения защиты информации должны применять меры защиты информации, реализующие стандартный уровень защиты информации, предусмотренный пунктом 6.7 раздела 6 ГОСТ Р 57580.1-2017.

5. Участники платформы должны определить во внутренних документах:

состав организационных мер защиты информации и порядок их применения, а также состав технических средств защиты информации и порядок их использования;

порядок подготовки, обработки, передачи и хранения сообщений в электронном виде, связанных с осуществлением операций с цифровыми рублями (далее – электронные сообщения), и защищаемой информации, предусмотренной пунктом 2 настоящего Положения, с использованием объектов информационной инфраструктуры;

список лиц (за исключением пользователей платформы цифрового рубля), допущенных к работе с СКЗИ, с определением прав использования криптографических ключей;

---

[1] Утвержден приказом Федерального агентства по техническому регулированию и метрологии от 8 августа 2017 года № 822-ст (М., ФГУП «Стандартинформ», 2017) и введен в действие 1 января 2018 года.

список лиц (за исключением пользователей платформы цифрового рубля), ответственных за обеспечение функционирования и безопасности СКЗИ (ответственные пользователи СКЗИ);

список лиц (за исключением пользователей платформы цифрового рубля), обладающих правами по управлению криптографическими ключами, в том числе 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.

6. Обеспечение защиты информации участниками платформы с использованием СКЗИ должно осуществляться 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[2], требованиями технической документации на СКЗИ, включая требования к проведению оценки влияния аппаратных, программно-аппаратных и программных средств сети (систем) конфиденциальной связи, совместно с которыми предполагается штатное функционирование СКЗИ, на выполнение предъявленных к ним требований.

[2] 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).

7. Участники платформы должны обеспечивать защиту электронных сообщений в соответствии с альбомом электронных сообщений, предусмотренным частью 6 статьи $30^7$ Федерального закона № 161-ФЗ.

8. Участник платформы должен осуществлять формирование и подписание электронных сообщений участника платформы с использованием автоматизированной системы участника платформы.

9. Участник платформы должен обеспечивать формирование и подписание электронных сообщений пользователя платформы цифрового рубля в электронном средстве платежа на основе программного обеспечения, позволяющего пользователю платформы цифрового рубля составлять, удостоверять и передавать распоряжения, установленного на техническом устройстве пользователя платформы цифрового рубля (включая смартфон, планшетный компьютер) или в другой системе дистанционного банковского обслуживания (далее – приложение клиента), с использованием ключа электронной подписи пользователя платформы цифрового рубля или в автоматизированной системе участника платформы с использованием ключа электронной подписи участника платформы (при составлении участником платформы распоряжений от имени пользователя платформы цифрового рубля в соответствии с частью 5 статьи $7^1$ Федерального закона № 161-ФЗ).

При подписании электронных сообщений пользователя платформы цифрового рубля в приложении клиента, являющемся программным обеспечением для мобильных устройств (далее – мобильное приложение), участник платформы должен обеспечивать применение программного обеспечения, распространяемого оператором платформы цифрового рубля, в составе мобильного приложения.

10. Участники платформы должны хранить электронные сообщения, подписанные электронной подписью и признаваемые 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 средства, обеспечивающие 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» (далее – Федеральный закон № 125-ФЗ).

11. Участники платформы должны осуществлять сбор, передачу оператору платформы цифрового рубля и обновление идентификационной информации устройства пользователя платформы цифрового рубля, на котором установлено мобильное приложение, сформированной в виде производного значения из значений параметров такого устройства, позволяющего идентифицировать устройство пользователя платформы цифрового рубля при совершении операций с цифровыми рублями (далее – цифровой отпечаток устройства).

12. В целях осуществления передачи цифрового отпечатка устройства и обновления цифрового отпечатка устройства, хранимого на платформе цифрового рубля, участники платформы должны удостовериться на основе информации, указанной в абзаце третьем пункта 2 настоящего Положения, что устройство используется пользователем платформы цифрового рубля, указанным в договоре счета цифрового рубля, предусмотренном статьей $30^8$ Федерального закона № 161-ФЗ.

13. При обмене электронными сообщениями между участником платформы и пользователем платформы цифрового рубля участник платформы должен обеспечивать защиту электронных сообщений с применением электронной подписи с соблюдением следующих требований:

13.1. Участник платформы должен подписывать электронные сообщения участника платформы электронной подписью, сертификат ключа проверки которой выдан удостоверяющим центром Банка России в соответствии со статьей 13 Федерального закона № 63-ФЗ.

13.2. Участник платформы должен обеспечивать подписание электронных сообщений пользователя платформы цифрового рубля электронной подписью, сертификат ключа проверки которой выдан удостоверяющим центром участника платформы, подчиненным удостоверяющему центру Банка России.

13.3. Участник платформы должен осуществлять контроль срока действия ключа электронной подписи пользователя платформы цифрового рубля и ключа проверки электронной подписи пользователя платформы цифрового рубля.

13.4. Участник платформы при создании и функционировании удостоверяющего центра участника платформы должен использовать средства 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[3] (далее – приказ ФСБ России № 796).

13.5. Участник платформы при эксплуатации средств удостоверяющего центра должен использовать информацию о точном значении московского времени и календарной дате, распространяемую 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».

---

[3] 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). В соответствии с пунктом 2 приказа ФСБ России № 796 данный акт действует до 1 января 2027 года.

13.6. Для подписания сертификатов ключей проверки электронных подписей пользователей платформы цифрового рубля в удостоверяющем центре участника платформы участник платформы должен использовать ключ электронной подписи, соответствующий ключу проверки электронной подписи, указанному в сертификате, выданном удостоверяющим центром Банка России в соответствии со статьей 13 Федерального закона № 63-ФЗ.

13.7. При взаимодействии между участником платформы и пользователем платформы цифрового рубля с использованием приложения клиента участник платформы должен обеспечивать изготовление и использование криптографических ключей пользователя платформы цифрового рубля, 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).

13.8. Участник платформы должен обеспечивать применение программного обеспечения, распространяемого оператором платформы цифрового рубля, для хранения криптографических ключей пользователя платформы цифрового рубля, в иных случаях участник платформы вправе применять организационно-технические меры для осуществления хранения

криптографических ключей на внешних отчуждаемых носителях ключевой информации пользователя платформы цифрового рубля в дополнение к требованиям эксплуатационной документации на используемые СКЗИ.

13.9. Участник платформы должен осуществлять изготовление, хранение и использование криптографических ключей участника платформы, 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 участника платформы, с применением СКЗИ, прошедших процедуру оценки соответствия требованиям, установленным федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности.

13.10. Участник платформы должен обеспечивать возможность передачи в удостоверяющий центр участника платформы запроса на выдачу сертификата ключа проверки электронной подписи пользователя платформы цифрового рубля, инициируемого пользователем платформы цифрового рубля, с использованием приложения клиента.

13.11. В случае досрочного прекращения действия или аннулирования сертификата ключа проверки электронной подписи пользователя платформы цифрового рубля в соответствии со статьей 13 Федерального закона № 63-ФЗ участник платформы должен незамедлительно представить на платформу цифрового рубля информацию о таком досрочном прекращении действия или аннулировании сертификата ключа проверки электронной подписи.

14. Участник платформы должен применять организационные меры и (или) технические средства защиты информации, используемые при обмене

электронными сообщениями при осуществлении операций с цифровыми рублями, с соблюдением следующих требований:

14.1. Участник платформы должен обеспечивать защиту электронных сообщений при их передаче между участником платформы и оператором платформы цифрового рубля посредством:

использования усиленной неквалифицированной электронной подписи, реализуемой средствами электронной подписи не ниже класса КС2, предусмотренного пунктом 14 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 цифрового рубля;

использования усиленной неквалифицированной электронной подписи, реализуемой средствами электронной подписи не ниже класса 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 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»[4] (далее – ГОСТ Р ИСО/МЭК 7498-1-99), с использованием СКЗИ не ниже класса КС2, предусмотренного пунктом 11 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[5] (далее – Состав и содержание организационных и технических мер), прошедших процедуру оценки соответствия требованиям, установленным федеральным органом исполнительной власти, уполномоченным 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 государственного стандарта Российской Федерации ГОСТ Р ИСО/МЭК 7498-1-99 «Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 1. Базовая модель»[6] (далее – ГОСТ Р ИСО/МЭК 7498-1-99), с использованием СКЗИ не ниже класса 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

---

[4] Принят постановлением Государственного комитета Российской Федерации по стандартизации и метрологии от 18 марта 1999 года № 78 (М., ИПК «Издательство стандартов», 1999) и введен в действие 1 января 2000 года.

[5] Зарегистрирован Минюстом России 18 августа 2014 года, регистрационный № 33620.

[6] Принят постановлением Государственного комитета Российской Федерации по стандартизации и метрологии от 18 марта 1999 года № 78 (М., ИПК «Издательство стандартов», 1999) и введен в действие 1 января 2000 года.

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[7] (далее – Состав и содержание организационных и технических мер), прошедших процедуру оценки соответствия требованиям, установленным федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности;

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 приложением 1 к настоящему Положению;

использования технологии виртуальных частных сетей между участником платформы и оператором платформы цифрового рубля с использованием СКЗИ не ниже класса КС2, предусмотренного пунктом 11 Состава и содержания организационных и технических мер.

14.2. Участник платформы должен обеспечивать защиту электронных сообщений при их передаче между пользователем платформы цифрового рубля и участником платформы посредством:

использования усиленной неквалифицированной электронной подписи, реализуемой средствами электронной подписи не ниже класса КС2 на стороне участника платформы и средствами электронной подписи не ниже класса КС1 на стороне пользователя платформы цифрового рубля, предусмотренных соответственно пунктами 14 и 13 Требований к средствам электронной подписи, для контроля целостности и подтверждения подлинности электронных сообщений;

---

[7] Зарегистрирован Минюстом России 18 августа 2014 года, регистрационный № 33620.

использования усиленной неквалифицированной электронной подписи, реализуемой средствами электронной подписи не ниже класса КС3 на стороне участника платформы и средствами электронной подписи не ниже класса КС1 на стороне пользователя платформы цифрового рубля, предусмотренных 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 не ниже класса КС2 на стороне участника платформы и СКЗИ не ниже класса КС1 на стороне пользователя платформы цифрового рубля, предусмотренных соответственно пунктами 11 и 10 Состава и содержания организационных и технических мер, прошедших процедуру оценки соответствия требованиям, установленным федеральным органом исполнительной власти, уполномоченным 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 не ниже класса КС3 на стороне участника платформы и СКЗИ не ниже класса 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, уполномоченным в области обеспечения безопасности;

применения СКЗИ не ниже класса КС2, предусмотренного пунктом 11 Состава и содержания организационных и технических мер, на стороне участника платформы и СКЗИ не ниже класса КС1, предусмотренного пунктом 10 Состава и содержания организационных и технических мер, на стороне пользователя платформы цифрового рубля, 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.

15. Участники платформы должны проводить оценку выполнения ими требований к обеспечению защиты 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 (далее – проверяющая организация).

16. Участники платформы должны проводить оценку соответствия согласно следующим требованиям:

оценка соответствия должна проводиться в пределах выделенных сегментов (групп сегментов) вычислительных сетей, указанных в пункте 5 настоящего Положения;

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»[8] (далее – ГОСТ Р 57580.2-2018).

17. Участники платформы должны хранить отчет, подготовленный проверяющей организацией по результатам проведения оценки соответствия, не менее пяти лет начиная с даты его выдачи проверяющей организацией в соответствии со сроками хранения документов из перечня документов, предусмотренного частью $1^1$ статьи 23 Федерального закона № 125-ФЗ.

18. Участники платформы должны обеспечивать для объектов информационной инфраструктуры, размещенных в выделенных сегментах (группах сегментов) вычислительных сетей, указанных в пункте 4 настоящего Положения, уровень соответствия не ниже четвертого, предусмотренного подпунктом «д» пункта 6.9 раздела 6 ГОСТ Р 57580.2-2018.

19. Участники платформы должны проводить ежегодное тестирование на проникновение и анализ уязвимостей информационной безопасности объектов информационной инфраструктуры, размещенных в отдельных выделенных сегментах (группах сегментов) вычислительных сетей, указанных в пункте 4 настоящего Положения.

20. Участники платформы должны выполнять требования к обеспечению защиты информации, применяемые в отношении приложения клиента, предусмотренные приложением 2 к настоящему Положению.

21. Настоящее Положение подлежит официальному опубликованию и вступает в силу с 1 января 2024 года, за исключением положений, для которых настоящим пунктом установлен иной срок вступления их в силу.

Абзацы третий и пятый подпункта 14.1, абзацы третий и пятый подпункта 14.2 пункта 14 настоящего Положения вступают в силу с 1 января 2025 года.

---

[8] Утвержден приказом Федерального агентства по техническому регулированию и метрологии от 28 марта 2018 года № 156-ст (М., ФГУП «Стандартинформ», 2018) и введен в действие 1 сентября 2018 года.

Абзацы второй и четвертый подпункта 14.1, абзацы второй и четвертый подпункта 14.2 пункта 14 настоящего Положения действуют по 31 декабря 2024 года.

Председатель
Центрального банка
Российской Федерации Э.С. Набиуллина

Приложение 1
к Положению Банка России
от «7» декабря 2023 года № 833-П
«О требованиях к обеспечению защиты информации для участников платформы цифрового рубля»

**Требования к обеспечению защиты информации, применяемые в отношении технологии обработки и передачи электронных сообщений при осуществлении операций с цифровыми рублями**

1. Участник платформы для обеспечения безопасности технологии обработки и передачи электронных сообщений при осуществлении операций с цифровыми рублями должен реализовать в своей информационной инфраструктуре два выделенных контура: контур контроля и контур обработки.

2. Участник платформы должен реализовать 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.

3. Участник платформы должен разместить объекты информационной инфраструктуры контура обработки и контура контроля в разных сегментах вычислительной сети. Способ допустимого информационного взаимодействия между указанными сегментами вычислительной сети оформляется документально и согласовывается со службой информационной безопасности участника платформы.

4. Участник платформы при направлении и обработке электронных сообщений должен соблюдать следующие условия:

4.1. Исходящие электронные сообщения, направляемые участником платформы на платформу цифрового рубля, должны поступать в контур контроля только из контура обработки.

4.2. Входящие электронные сообщения, получаемые участником платформы от платформы цифрового рубля, из контура контроля должны передаваться только в контур обработки, в том числе для последующей передачи пользователю платформы цифрового рубля (при необходимости).

5. Участник платформы в контуре обработки для исходящих электронных сообщений, направляемых участником платформы на платформу цифрового рубля, должен реализовать:

расшифрование электронного сообщения;

проверку электронной подписи, с использованием которой подписано электронное сообщение;

структурный контроль электронного сообщения;

проверку правильности заполнения полей электронного сообщения;

подписание электронного сообщения электронной подписью участника платформы;

направление электронного сообщения в контур контроля.

6. Участник платформы в контуре контроля для исходящих электронных сообщений, направляемых участником платформы на платформу цифрового рубля, должен реализовать:

проверку электронной подписи, с использованием которой подписано электронное сообщение;

структурный контроль электронного сообщения;

проверку правильности заполнения полей электронного сообщения;

контроль отсутствия дублирования электронного сообщения;

подписание электронного сообщения электронной подписью участника платформы;

шифрование электронного сообщения, передаваемого на платформу цифрового рубля.

7. Участник платформы в контуре контроля для входящих электронных сообщений, получаемых участником платформы от платформы цифрового рубля, должен осуществлять:

расшифрование электронного сообщения;

проверку электронной подписи, с использованием которой подписано электронное сообщение;

структурный контроль электронного сообщения;

подписание электронного сообщения электронной подписью участника платформы;

направление электронного сообщения в контур обработки.

8. Участник платформы в контуре обработки для входящих электронных сообщений, получаемых участником платформы от платформы цифрового рубля, должен осуществлять:

проверку электронной подписи, с использованием которой подписано электронное сообщение;

структурный контроль электронного сообщения;

проверку правильности заполнения полей электронного сообщения;

контроль отсутствия дублирования электронного сообщения;

шифрование электронного сообщения, передаваемого пользователю платформы цифрового рубля.

Приложение 2
к Положению Банка России
от «7» декабря 2023 года № 833-П
«О требованиях к обеспечению защиты информации для участников платформы цифрового рубля»

## Требования к обеспечению защиты информации, применяемые в отношении приложения клиента

1. Участник платформы для обеспечения безопасности приложения клиента должен выполнять следующие требования к процессу разработки, тестирования и эксплуатации приложения клиента:

иметь 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;

применять меры защиты информации в соответствии с подпунктами 4.1 и 4.2 пункта 4 настоящего Положения для объектов информационной инфраструктуры, с использованием которых обеспечиваются эксплуатация и функционирование приложения клиента.

2. Участник платформы должен выполнять следующие требования к безопасности приложения клиента:

реализовать механизм доставки пользователю платформы цифрового рубля уведомлений об операциях с цифровыми рублями;

реализовать механизм обработки ошибок и (или) исключений, возникающих в процессе работы приложения клиента, в рамках которого обеспечиваются корректная обработка и информирование пользователя платформы цифрового рубля об ошибках, в том числе о сбоях

при подключении к приложению клиента, недоступности приложения клиента;

реализовать механизм проверки корректности данных, вводимых пользователем платформы цифрового рубля в приложении клиента;

регистрировать события защиты информации (в том числе события, связанные с неуспешной аутентификацией и авторизацией, ошибками при управлении доступом и проверке входных данных) при функционировании приложения клиента;

реализовать механизм незамедлительной блокировки и последующего досрочного прекращения действия или аннулирования сертификата ключа проверки электронной подписи пользователя платформы цифрового рубля в случае компрометации ключа электронной подписи;

досрочно прекратить действие сертификата ключа проверки электронной подписи пользователя платформы цифрового рубля – юридического лица и сменить аутентификационные данные для доступа пользователя платформы цифрового рубля – юридического лица к приложению клиента при обращении пользователя платформы цифрового рубля – юридического лица к участнику платформы.

3. Участник платформы вправе принимать организационно-технические меры, направленные на соответствие требованиям к безопасности мобильного приложения, в том числе в части наличия возможности:

реализации механизма информирования пользователя платформы цифрового рубля о необходимости применения обновлений мобильного приложения, связанных с обеспечением защиты информации;

реализации альтернативных способов обновления и (или) установки мобильного приложения в случае наличия ограничений обновления и (или) установки мобильного приложения из основного источника;

реализации механизма, исключающего возможность использования сторонних программных средств ввода и отключения механизма регистрации истории ввода при вводе данных пользователя платформы цифрового рубля, в том числе аутентификационных данных пользователя платформы цифрового рубля;

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

реализации механизма блокировки доступа к мобильному приложению при неоднократных неуспешных попытках аутентификации.