**Таблица замечаний и предложений по проекту положения Банка России «О требованиях к обеспечению защиты информации для участников платформы цифрового рубля» (далее – Проект)**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| №п/п | Структурная единица **проекта** | **Содержание замечания или предложения** | **Решение** | **Пояснение** |
| 1 | 2 | 3 | 4 | 5 |
| Ассоциация банков России | | | | |
|  | Пункт 2 Проекта | Распространяются ли требования к защите информации на сетевую инфраструктуру (сетевое оборудование, сети) и средства защиты информации? | Представлено пояснение | Требования к защите информации распространяются на сетевую инфраструктуру и средства защиты информации. |
|  | Пункт 2 Проекта | Относится ли к защищаемой информации в понимании Проекта информация, передаваемая в процессе обмена клиентом безналичных денежных средств на цифровые рубли (далее – ЦР) между информационными системами участника платформы цифрового рубля (далее – ПЦР), в частности, автоматизированной банковской системой, и сегментом сети, в котором размещены объекты информационной инфраструктуры, которые непосредственно участвуют в формировании (подготовке), обработке, передаче и хранении электронных сообщений при осуществлении операций с ЦР? | Представлено пояснение | Данное положение регламентирует порядок обработки информации на информационных системах/средствах вычислительной техники, непосредственно задействованных в проведении операций с ЦР в соответствии с Альбомом электронных сообщений, используемых для взаимодействия субъектов платформы цифрового рубля. |
|  | Абзацы 4-6 пункта 4 Проекта | Предлагается конкретизировать состав списка лиц, который следует определить при работе с ПЦР, и изложить абзацы 4-6 в следующей редакции:  «список сотрудников участника платформы цифрового рубля, допущенных к работе с СКЗИ, с определением прав использования криптографических ключей;  список сотрудников участника платформы цифрового рубля, ответственных за обеспечение функционирования и безопасности СКЗИ (ответственные пользователи СКЗИ);  список сотрудников участника платформы цифрового рубля, обладающих правами по управлению криптографическими ключами, в том числе список лиц, ответственных за формирование криптографических ключей и обеспечение безопасности криптографических ключей;».  В текущей редакции возникает неопределенность относительно необходимости указания в списке лиц только сотрудников кредитной организации или всех клиентов участника ПЦР. | Учтено | Добавлено уточнение «за исключением пользователей платформы цифрового рубля». |
|  | Абзац 7 пункта 4 Проекта | Предлагается дополнить абзац после слов «на этапах их подготовки, обработки, передачи и хранения,» словами «а также для обеспечения разграничения доступа к средствам вычислительной техники, СКЗИ, ключевой информации и информации, обрабатываемой на средствах вычислительной техники, в соответствии с установленными правилами разграничения доступа,».  Текущая редакция пункта 4 Проекта, устанавливающего состав технических средств защиты информации и порядок их использования, не содержит требований к составу технологических мер разграничения доступа, призванных обеспечить защиту от несанкционированного доступа к средствам вычислительной техники и обрабатываемой на них информации, а также к средствам защиты информации. | Не учтено | Состав мер по разграничению доступа к объектам информационной инфраструктуры участника платформы цифрового рубля определен в рамках процесса 1 «Обеспечение защиты информации при управлении доступом» ГОСТ 57580.1-2017, требования которого являются обязательными к выполнению в соответствии с пунктом 3 настоящего проекта положения. |
|  | Пункт 5 Проекта | Предлагается заменить слова «Защита информации с использованием СКЗИ должна обеспечиваться участниками платформы цифрового рубля в соответствии с» словами «Разработка, производство, реализация и эксплуатация шифровальных (криптографических) средств защиты информации, используемых для защиты информации, должны обеспечиваться в соответствии с».  Положение ПКЗ-2005 устанавливает не требования к защите информации с использованием средств криптографической защиты информации (далее – СКЗИ), а требования к самим СКЗИ. | Не учтено | Данная формулировка используется по аналогии с иными нормативными актами Банка России и предполагает, что предметом нормативного акта является защита информации. При этом использование СКЗИ для указанных целей должно соответствовать требованиям Положения ПКЗ-2005. |
|  | Абзац 2  пункта 7 Проекта/ Пункт 1 Приложения 2 к Проекту | Участники опроса просят уточнить:   * возможно ли формирование и подписание электронных сообщений пользователем ПЦР с использованием web-версии системы дистанционного банковского обслуживания (далее – ДБО)? * что понимается под словами «или в другой системе дистанционного банковского обслуживания»? Может ли к ней относиться web-версия системы ДБО? * слова «(далее – приложение клиента)» относятся к словам «или в другой системе дистанционного банковского обслуживания» или ко всему перечисленному программному обеспечению? | Представлено пояснение | * да, возможно формирование и подписание электронных сообщений пользователем ПЦР с использованием web-версии системы дистанционного банковского обслуживания (далее – ДБО); * к понятию «другая система ДБО» может относиться web-версия системы ДБО; * ко всему перечисленному программному обеспечению. |
|  | Абзац 1 пункта 9 Проекта | Кредитные организации просят уточнить:   * способ передачи цифрового отпечатка на ПЦР; * необходимо ли передавать цифровой отпечаток каждого авторизованного устройства пользователя? | Представлено пояснение | Цифровой отпечаток устройства, с которого осуществляется взаимодействие с ПлЦР, должен передаваться в составе электронных сообщений в соответствии с Альбомом сообщений ПлЦР. |
|  | Абзац 2 пункта 9 Проекта | 1) Участники опроса просят определить способы и инструменты, с помощью которых необходимо удостовериться в принадлежности устройства конкретному пользователю ПЦР (или в использовании этого устройства конкретным пользователем ПЦР). Могут ли для этих целей использоваться данные об идентификационной информации устройства, предоставляемые операторами связи?  Например, при компрометации устройства (ключей электронной подписи) до обращения пользователя с заявлением о компрометации банк не сможет определить, что устройство попало к злоумышленникам и используется ими для совершения мошеннических операций.  2) Альтернативно предлагается использовать аутентификацию в системе ДБО в качестве проверки использования устройства пользователем ПЦР. В таком случае целесообразно заменить слова «принадлежит данному пользователю платформы цифрового рубля» словами «используется данным авторизованным пользователем платформы цифрового рубля. Указанная проверка должна осуществляться по результатам проведения аутентификации пользователя в системе дистанционного банковского обслуживания участника платформы цифрового рубля». | 1. Представлено пояснение  2. Учтено | 1. Способы и инструменты определяются участником ПлЦР.  2. Изложить абзац второй пункта 9 Проекта в следующей редакции:  «В целях осуществления передачи и обновления цифрового отпечатка устройства, хранимого на платформе цифрового рубля, участник платформы цифрового рубля должен удостовериться, что устройство **используется** данным пользователем платформы цифрового рубля.». |
|  | Абзац 2 пункта 10 Проекта | Участники опроса просят уточнить в чем заключается контроль срока действия сертификата ключа проверки электронной подписи пользователя ПЦР.  В данном пункте предполагается контроль использования действительных по сроку действия сертификатов или необходимость оповещения пользователей об окончании срока действия сертификата ключа проверки электронной подписи? | Учтено | Речь идет о контроле срока действия криптографического ключа электронной подписи пользователя.  Требование касается контроля использования действительных по сроку действия криптографического ключа электронной подписи пользователя при взаимодействии с ПлЦР.  Вместе с тем для улучшения клиентского пути предлагаем участникам дополнительно оповещать пользователей о приближении окончания срока действия ключа электронной подписи для его перевыпуска.  Абзац изложен в следующей редакции:  «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 криптографического ключа электронной подписи пользователя платформы цифрового рубля должен осуществляться участником платформы цифрового рубля». |
|  | Абзац 6 пункта 10 Проекта | Предлагается исключить или дать детальные пояснения по технологии хранения криптографических ключей.  По информации кредитных организаций, участник ПЦР не имеет возможности обеспечения надлежащего хранения криптографических ключей на устройстве пользователя ПЦР. Ключ электронной подписи формируется посредством СКЗИ, предоставленных участникам ПЦР. При этом не используются никакие функции по защите ключа. После формирования ключ электронной подписи хранится в виде файла в файловой системе устройства пользователя ПЦР. Данные файлы доступны к копированию, у участника ПЦР отсутствует техническая возможность защиты данных файлов и контроля их перемещения/ копирования.  В случае существования технологии, позволяющей реализовать требования данного абзаца, кредитные организации просят предоставить информацию о ней.  Альтернативно в качестве организационной, а не технической меры предлагается предусмотреть в договорной базе между пользователями ПЦР и участником ПЦР обязательства пользователя, в соответствии с которыми он обязан эксплуатировать мобильное приложение в соответствии с эксплуатационной документацией, в состав которой будут входить также формуляры на СКЗИ. | Учтено частично. | При разработке/доработке приложения клиента необходимо реализовать хранение криптографических ключей пользователя ПлЦР в соответствии с требованиями эксплуатационной документации к используемым СКЗИ.  Требование о невозможности экспорта криптографических ключей исключено из актуальной редакции Проекта. |
|  | Абзац 9 пункта 10 Проекта | Предлагается изложить в следующей редакции:  «В случае аннулирования сертификата ключа проверки электронной подписи пользователя платформы цифрового рубля **~~удостоверяющий центр~~ участник~~а~~** платформы цифрового рубля должен предоставить на платформу цифрового рубля информацию о таком сертификате ключа проверки электронной подписи **в формате и по каналам связи, установленным в соответствии с требованиями Банка России**.».  Целесообразно заменить удостоверяющий центр участника ПЦР на участника ПЦР, так как удостоверяющий центр не интегрирован напрямую с ПЦР. В целях исключения разночтений предлагается установить формат сообщения и канал связи в требованиях Банка России. В частности, это должно определяться регламентом информационного взаимодействия удостоверяющего центра ПЦР и участников ПЦР. | Учтено частично | Абзац изложен в следующей редакции:  «В случае аннулирования сертификата ключа проверки электронной подписи пользователя платформы цифрового рубля **участник** платформы цифрового рубля должен предоставить на платформу цифрового рубля информацию **об аннулировании** сертификата ключа проверки электронной подписи».  Форматы и каналы связи определяются регламентом взаимодействия. |
|  | Абзацы 2 и 3 пункта 11.1 Проекта | Предлагается в абзаце 2 пункта 11.1 Проекта заменить слова «для контроля целостности и подтверждения подлинности электронных сообщений, в том числе применяемой для контроля целостности и подтверждения подлинности электронных сообщений пользователей платформы цифрового рубля» словами «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)» из абзаца 3 пункта 11.1 Проекта.  Абзац 3 пункта 11.1 Проекта исключить.  Абзацы 2 и 3 пункта 11.1 Проекта целесообразно объединить ввиду схожести их требований или указать условия применимости их требований.  Кроме того, участники опроса отмечают, что при обмене электронными сообщениями между участником ПЦР и ПЦР не обеспечивается целостность сообщения пользователя ПЦР. Данное сообщение пользователя просто пересылается от участника ПЦР с добавлением усиленной неквалифицированной электронной подписи участника ПЦР. В этой связи предлагается исключить описание механизма защиты электронных сообщений пользователей ПЦР. | Не учтено | В соответствии с п. 3 ст. 5 Федерального закона от 06.04.2011 № 63-ФЗ «усиленная неквалифицированная электронная подпись позволяет обнаружить факт внесения изменений в электронный документ после момента его подписания», что и обеспечивает целостность передаваемых сообщений. Также в соответствии с абзацем третьим п. 4 приложения 1 к Положению участник обязан проверить подпись пользователя на электронном сообщении, прежде чем осуществить дальнейшую его обработку. |
|  | Абзацы 4 и 5 пункта 11.1 Проекта | Предлагается указать условия применимости требований абзаца 4 и абзаца 5 пункта 11.1 Проекта либо исключить абзац 4 пункта11.1 Проекта.  Абзац 5 повторяет требование абзаца 4 с уточнением, что СКЗИ должны быть сертифицированы по классу КС3. | Не учтено | Абзацы разделены, т.к. имеют различные сроки вступления в силу. Это сделано для упрощения процедуры перехода участника ПлЦР на более высокий класс защиты в соответствии с требованиями регулятора (ФСБ России) |
|  | Абзац 7 пункта 11.1 Проекта | Участники опроса просят детализировать перечень программных и/или программно-аппаратных комплексов, необходимых участникам ПЦР для реализации технологии виртуальных частных сетей с использованием СКЗИ класса не ниже КС2.  При выборе программных и/или программно-аппаратных комплексов для реализации технологии виртуальных частных сетей должна быть обеспечена совместимость решений между участниками ПЦР и ПЦР. | Представлено пояснение | Порядок подключения и варианты реализации данного требования указаны в пункте 7.2 документа «ЦВЦБ. Стандарт. Порядок подключения Финансового посредника к Платформе Цифрового Рубля», размещенного на официальном сайте Банка России. |
|  | Пункт 11.2 Проекта | В связи с наличием в Проекте требования по шифрованию электронных сообщений между участниками ПЦР и пользователями ПЦР на прикладном уровне с использованием СКЗИ классов КС3/КС1, по применению СКЗИ класса КС2 для реализации двухсторонней аутентификации и шифрования информации на уровне представления или ниже, а также по шифрованию на сетевом/канальном уровне предлагается дополнить Проект структурной схемой подключения для устранения неопределенности при выполнении требований Проекта. | Не учтено | Структурная схема подключения относится к категории документов, отличной от категории нормативных актов Банка России, ее включение в Проект полагаем нецелесообразным. |
|  | Абзац 4 пункта 11.2 Проекта | Кредитные организации просят уточнить, о каких средствах криптографической защиты информации класса не ниже КС2 на стороне участника ПЦР идет речь? На каком технологическом участке они применяются? Какие функции выполняют? | Представлено пояснение | Построение канала ГОСТ-TLS с двухсторонней аутентификацией на участке между пользователями платформы цифрового рубля и участниками платформы цифрового рубля. КС1 на стороне пользователя реализуется с помощью предоставляемого участникам программного модуля Банка России, КС2 на стороне участника реализуется в инфраструктуре участника с помощью средств криптографической защиты сетевого трафика с поддержкой российских алгоритмов шифрования. |
|  | Абзац 4 пункта 11.2 Проекта | Предлагается после слов «на стороне участника платформы цифрового рубля и средств» дополнить словами «криптографической».  Пропущено слово «криптографической» в указании класса средств защиты информации. | Учтено |  |
|  | Абзац 6 пункта 12 Проекта | Предлагается исключить абзац 6.  Абзац 6 пункта 12 Проекта обязывает обеспечивать уровень соответствия защиты информации не ниже третьего в соответствии с ГОСТ Р 57580.2-2018.  При этом согласно абзацу 7 пункта 12 и пункту 14 Проекта с 01.01.2024 необходимо обеспечить уровень соответствия защиты информации не ниже четвертого в соответствии с ГОСТ Р 57580.2-2018 (более высокий уровень защиты).  Таким образом, принимая во внимание ожидаемые сроки вступления Проекта в силу, требование об обеспечении уровня соответствия защиты информации не ниже третьего фактически будет действовать несколько месяцев (с осени 2023 года по 01.01.2024). За этот период кредитные организации даже не смогут завершить оценку соответствия, так как ее проведение занимает длительное время.  В этой связи предлагается исключить требование об обеспечении уровня соответствия защиты информации не ниже третьего ввиду практической невозможности его реализации и сохранить только требование об обеспечении уровня соответствия защиты информации не ниже четвертого, указанное в абзаце 7 пункта 12 Проекта.  Такой подход изначально обеспечит более высокий уровень безопасности и позволит кредитным организациям наиболее рационально использовать собственные ресурсы на проведение оценок соответствия защиты информации. | Не учтено | Так как требования будут применимы к участнику только после его подключения к ПлЦР, полагаем целесообразным сохранить срок вступления в силу нормы с 01.01.2024. |
|  | Пункт 14 Проекта | Предлагается исключить из абзаца 2 пункта 14 Проекта слова «абзац седьмой пункта 12» и дополнить пункт 14 Проекта новым абзацем следующего содержания:  «Абзац седьмой пункта 12 вступает в силу с 1 января 2025 года.».  Абзац 7 пункта 12 Проекта обязывает обеспечивать уровень соответствия защиты информации не ниже четвертого в соответствии с ГОСТ Р 57580.2-2018.  Принимая во внимание ожидаемые сроки вступления Проекта в силу (осень 2023 года) и длительное время, требуемое на проведение оценки соответствия, кредитные организации (особенно крупные) могут не успеть завершить оценку соответствия защиты информации не ниже четвертого уровня к 01.01.2024 года.  Кроме того, для успешного прохождения оценки соответствия кредитным организациям потребуется время для реализации мер защиты информации в соответствии с ГОСТ Р 57580.1-2017 , установленных пунктом 3 Проекта.  В этой связи предлагается перенести срок вступления в силу данного требования с 01.01.2024 на 12 месяцев до 01.01.2025. | Не учтено | Так как требования будут применимы к участнику только после его подключения к ПлЦР, полагаем целесообразным сохранить срок вступления в силу нормы с 01.01.2024. |
|  | Приложение 1 к Проекту | Кредитные организации просят развернуто описать функции и предназначение контуров контроля и обработки, а также уточнить подробные требования к обеспечению их независимости. В частности:   * на каком уровне эталонной модели взаимодействия открытых систем они должны быть разделены? * должно ли это быть разделение в виде IP-адресов одного сегмента сети или необходимо использовать разные сегменты?   должно ли это быть физическое разделение или можно разделить виртуальными машинами? | Представлено пояснение | 1. Реализация сетевого взаимодействия и сетевой изоляции на уровне не выше третьего (сетевой) по семиуровневой стандартной модели взаимодействия открытых систем, определенной в ГОСТ Р ИСО/МЭК 7498-1. 2. В соответствии с абзацем четвертым приложения 1 к Проекту объекты информационной инфраструктуры контура обработки и контура контроля размещаются в разных сегментах вычислительных сетей. 3. Банк России не устанавливает ограничений в отношении применяемой технологии разделения сегментов, однако с учетом используемых классов СКЗИ класса от КС2 и выше на данное время отсутствуют согласованные регулятором технические решения, позволяющие размещать их на виртуальных машинах. |
|  | Пункт 2 Приложения 1 к Проекту | Что понимается под термином «способ информационного взаимодействия» в данном пункте? Какие именно контроли должны выполняться службой информационной безопасности при согласовании способа допустимого информационного взаимодействия между контурами контроля и обработки?  В текущей редакции Проекта определено только требование к наличию документирования способа такого взаимодействия. | Представлено пояснение | Конкретную реализацию указанного требования участник платформы цифрового рубля выбирает самостоятельно и документально оформляет. |
|  | Пункт 2 Приложения 1 к Проекту | Предлагается в явном виде указать запрет на использование виртуальных сред.  В соответствии с требованиями эксплуатационной документации на СКЗИ класса КС2 и выше не допускается работа в виртуальной среде. | Не учтено | Банк России не устанавливает ограничений в отношении применяемой технологии разделения сегментов, однако с учетом используемых классов СКЗИ класса от КС2 и выше на данное время отсутствуют согласованные регулятором технические решения, позволяющие размещать их на виртуальных машинах.  В этой связи полагаем избыточным указание в Проекте явного запрета на использование виртуальных сред. |
|  | Абзац 3 пункта 4 Приложения 1 к Проекту | Предлагается изложить в следующей редакции: «проверка электронной подписи, с использованием которой **пользователем** удостоверено электронное сообщение».  В текущей редакции приведена одинаковая формулировка по проверке электронной подписи исходящего сообщения как в контуре обработке, так и в контуре контроля, что затрудняет понимание о какой именно подписи идет речь. В этой связи предлагается конкретизировать формулировки для каждого случая. | Не учтено | Полагаем избыточным. Состав и виды электронных подписей определяются в соответствии с Альбомом электронных сообщений, используемых для взаимодействия субъектов платформы цифрового рубля. |
|  | Абзац 2 пункта 5 Приложения 1 к Проекту | Предлагается изложить в следующей редакции: «проверка электронной подписи, с использованием которой **контуром обработки финансового посредника** удостоверено электронное сообщение».  В текущей редакции приведена одинаковая формулировка по проверке электронной подписи исходящего сообщения как в контуре обработке, так и в контуре контроля, что затрудняет понимание о какой именно подписи идет речь. В этой связи предлагается конкретизировать формулировки для каждого случая. | Не учтено | Полагаем избыточным. Состав и виды электронных подписей определяются в соответствии с Альбомом электронных сообщений, используемых для взаимодействия субъектов платформы цифрового рубля. |
|  | Абзац 3 пункта 6 Приложения 1 к Проекту | Предлагается изложить в следующей редакции: «проверка электронной подписи, с использованием которой **в контуре контроля платформы цифрового рубля** удостоверено электронное сообщение».  В текущей редакции приведена одинаковая формулировка по проверке электронной подписи входящего сообщения от платформы цифрового рубля как в контуре обработке, так и в контуре контроля, что затрудняет понимание о какой именно подписи идет речь. В этой связи предлагается конкретизировать формулировки для каждого случая. | Не учтено | Полагаем избыточным. Состав и виды электронных подписей определяются в соответствии с Альбомом электронных сообщений, используемых для взаимодействия субъектов платформы цифрового рубля. |
|  | Абзац 2 пункта 7 Приложения 1 к Проекту | Предлагается изложить в следующей редакции: «проверка электронной подписи, с использованием которой **контуром контроля финансового посредника** удостоверено электронное сообщение»  В текущей редакции приведена одинаковая формулировка по проверке электронной подписи входящего сообщения от платформы цифрового рубля как в контуре обработке, так и в контуре контроля, что затрудняет понимание о какой именно подписи идет речь. В этой связи предлагается конкретизировать формулировки для каждого случая. | Не учтено | Полагаем избыточным. Состав и виды электронных подписей определяются в соответствии с Альбомом электронных сообщений, используемых для взаимодействия субъектов платформы цифрового рубля. |
|  | Абзац 4 пункта 7 Приложения 1 к Проекту | Что имеется ввиду под проверкой правильности заполнения полей? Чем она отличается от структурного контроля? Что необходимо делать в случае, если входящее электронное сообщение не прошло проверку правильности заполнения полей? | Представлено пояснение | Структурный контроль подразумевает контроль соответствия структуры ЭС требованиям к форматам ЭС в части состава и длины полей, под контролем правильности заполнения подразумеваются логические контроли, основанные на контроле значений реквизитов и их взаимного соответствия. Правила поведения участников при обмене ЭС (в т.ч. в случаях отрицательных результатов контролей) устанавливаются иными документами Банка России, и в настоящий момент они определены в комплекте документов Альбома сообщений ПлЦР. |
|  | Пункт 1.1 Приложения 2 к Проекту | Необходимо ли предоставлять информацию, указанную в пункте 1.1 Приложения 2 к Проекту, пользователям ПЦР в случае поступления от них такого запроса? | Представлено пояснение | Проект не устанавливает требований по обязательному предоставлению документарных свидетельств выполнения требований п. 1.1 пользователям ПлЦР. |
|  | Пункт 1.5 Приложения 2 к Проекту | По информации кредитных организаций, хранение ключей на внешних носителях при использовании мобильного приложения невозможно.  Данное требование, по мнению участников опроса, применимо в частных случаях при реализации функционала работы с ЦР в desktop-версии ДБО для операционной системы Windows либо для web-версии ДБО. | Представлено пояснение | В указанном пункте сформулировано требование как для ДБО с применением внешних отчуждаемых ключевых носителей информации, так и для мобильного приложения.  Для мобильного приложения предусмотрен вариант с реализацией защищенного хранилища ключей в выделенной области долговременной памяти устройства пользователя платформы цифрового рубля (данный вариант предусмотрен программным модулем Банка России). |
|  | Пункт 1.5 Приложения 2 к Проекту | Участники опроса предлагают отразить в Проекте требования к реализации защищенного хранилища ключей в памяти устройства.  Реализация защищенного хранилища ключей в выделенной области долговременной памяти устройства пользователя требует наличия у разработчика лицензии на деятельность по разработке СКЗИ. | Не учтено | Реализация защищенного хранилища ключей в выделенной области долговременной памяти устройства реализуется с помощью предоставляемого участникам ПлЦР программного модуля Банка России. При этом участник ПлЦР должен иметь лицензию по п. 2 приложения к Положению № 313. |
|  | Пункт 1.7 Приложения 2 к Проекту | Требуется реализовать блокировку всего кошелька или именно сертификата клиента, ключ которого был скомпрометирован? | Представлено пояснение | Имеется в виду блокировка возможности проведения операций с использованием скомпрометированного ключа электронной подписи. |
|  | Пункт 1.8 Приложения 2 к Проекту | Кредитные организации просят уточнить, при изменении состава уполномоченных лиц пользователя ПЦР - юридического лица, обладающих правом использования электронной подписи пользователя ПЦР, должны аннулироваться сертификаты всех пользователей такого юридического лица или только тех пользователей, которые исключены из состава уполномоченных лиц?  Кроме того, изменение состава уполномоченных лиц – это не только сокращение, но и пополнение списка. При появлении новых уполномоченных лиц не требуется смена аутентификационных данных и аннулирование сертификата.  В случаях, когда система аутентификации участника ПЦР предполагает использование персонифицированных учетных записей и сертификатов для каждого уполномоченного лица, данное требование также теряет свою актуальность. | Учтено | Абзац изложен в следующей редакции:  «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 исключении из состава уполномоченных лиц пользователя платформы цифрового рубля – юридического лица, обладающих правом использования электронной подписи пользователя платформы цифрового рубля.». |
|  | Пункт 2.3 Приложения 2 к Проекту | Предлагается исключить или дать детальные пояснения по технологии реализация механизма, исключающего возможность использования сторонних программных средств ввода и отключения механизма регистрации истории ввода.  По информации участников опроса, участник ПЦР не имеет возможности контроля окружения пользователя, в котором пользователь запускает приложение. Существуют лишь ограниченные возможности отслеживания конкретных наименований программного обеспечения и некоторых настроек окружения в определенных операционных системах. При этом исполнить требование данного пункта в полном объеме участнику ПЦР они не позволяют.  В случае существования соответствующей технологии кредитные организации просят предоставить информацию о ней. | Не учтено | Под данным пунктом подразумевается использование собственной реализации клавиатуры в мобильном приложении участника платформы цифрового рубля, предназначенной для ввода чувствительной информации (пароль/PIN) с целью невозможности ее перехвата.  В том случае, если реализация такого функционала не представляется возможным, необходимо отключить кэш клавиатуры. |
|  | Пункт 2.4 Приложения 2 к Проекту | Предлагается исключить или дать детальные пояснения по технологии осуществление контроля целостности прикладного программного обеспечения и среды его функционирования.  По информации участников опроса, участник ПЦР не имеет возможности контроля окружения, в котором пользователь запускает приложение. В случае существования соответствующей технологии кредитные организации просят предоставить информацию о ней. | Не учтено | В частности, под контролем среды функционирования понимается в том числе проверка на отсутствие прав суперпользователя (ROOT) на устройствах с ОС Android, а также факта проведения операции Jailbreak, позволяющей получить доступ к файловой системе на устройствах с ОС IOS. |
|  | Пункт 2.5 Приложения 2 к Проекту | Предлагается определить точное количество попыток неудачной аутентификации в мобильном приложении, после которого необходимо заблокировать доступ к нему. | Не учтено | Участник платформы цифрового рубля вправе сам определить точное количество неудачных попыток аутентификации и время таймаута в соответствии с процессами, реализованными в рамках мобильного приложения участника платформы цифрового рубля. |
|  | Проект в целом | Предлагается дополнить Проект информацией о том, что программный модуль Банка России участники ПЦР должны получать в соответствии с требованиями и в порядке, определенном Банком России.  В настоящее время нигде не зафиксированы обязательства сторон, порядок реагирования и каналы получения участниками ПЦР данного модуля. | Не учтено | Программный модуль Банка России распространяется в соответствии с условиями передачи программного обеспечения клиенту Банка России при заключении договора с участником платформы цифрового рубля. |
|  | Проект в целом | Какие механизмы форматно-логического контроля необходимо применять для реализации требований Проекта? | Представлено пояснение | В соответствии с Альбомом сообщений осуществляется проверка на корректность данных, передаваемых/получаемых электронных сообщений. |
|  | Проект в целом | Распространяются ли положения Проекта на микрофинансовые организации (МФО)? Планируется ли включать МФО в число участников ПЦР и предъявлять к ним требования по обеспечению защиты информации? | Представлено пояснение | В соответствии с Федеральным законом от 27.07.2011 № 161-ФЗ  «О национальной платежной системе» участник платформы цифрового рубля – оператор по переводу денежных средств (за исключением Банка России) или иностранный банк, предоставляющие пользователям платформы цифрового рубля доступ к платформе цифрового рубля в целях совершения операций с цифровыми рублями.  Проект распространяется на операторов по переводу денежных средств. |