Таблица замечаний и предложений по проекту указания Банка России «О внесении изменений в Положение Банка России от 9 января 2019 года № 672-П «О требованиях к защите информации в платежной системе Банка России» (далее – проект)

№ п/п	Структурная единица Проекта	Содержание замечания или предложения	Решение	Пояснение
1	2	3	5	6
Ассоциация банков России				
1.	Пункт 1.9 проекта	(пункт 12 Положения) Необходимо перефразировать абзац 3 для однозначного толкования. Не ясно каким сертификатом должен подписывать сообщение ОУИО в рамках оказания услуг «по обеспечению подписания исходящих электронных сообщений и (или) зашифрования на прикладном уровне электронных сообщений, проверки электронной подписи во входящих электронных сообщениях и (или) расшифрования на прикладном уровне входящих электронных сообщений»? Если ОУИО СБП оказывает услуги по «обеспечению подписания исходящих электронных сообщений и (или) зашифрования на прикладном уровне электронных сообщений, проверки электронной подписи во входящих электронных сообщениях и (или) расшифрования на прикладном уровне входящих электронных сообщений», то возникает ситуация, когда Участник СБП должен передать в ОУИО сообщение для подписания и шифрования. Но, судя по первой части требования, при обмене между участниками СБП и ОУИО СБП должна применяться ЭП, сертификат проверки которой выдан ОПКЦ. Получается, что Участник СБП должен передать для подписания и шифрования в ОУИО СБП уже подписанное сообщение.	Учтено частично Предоставлено пояснение	Редакция пункта изменена. При обмене электронными сообщениями электронная подпись должна применяться между операционным центром, платежным клиринговым центром другой платежной системы при предоставлении операционных услуг и услуг платежного клиринга при переводе денежных средств с использованием сервиса быстрых платежей (далее – ОПКЦ) и участниками обмена при осуществлении переводов денежных средств с использованием сервиса быстрых платежей (далее – участник СБП), и между ОПКЦ и оператором услуг информационного обмена при предоставлении участникам обмена услуг информационного обмена при осуществлении переводов денежных средств с использованием сервиса быстрых платежей (далее – ОУИО СБП)
2.	Пункт 1.9 проекта	(пункт 12 Положения) Вопрос по абзацу 4: Может ли быть предоставлен доступ к криптографическим ключам ОУИО в целях оказания им услуг по обеспечению подписания и шифрования сообщений в рамках договора между ОУИО и Участником СБП?	Предоставлено пояснение	Непосредственный доступ к ключам имеется только для участника СБП. ОУИО СБП при оказании услуг по подписанию и шифрованию косвенно использует ключи участника СБП путем обращения к аппаратному модулю безопасности (далее – HSM) для выполнения в нем соответствующих

				операций с использованием хранимых в HSM ключей.
3.	Пункт 1.9 проекта	(пункт 12 Положения) Кредитные организации просят указать класс защиты аппаратных модулей безопасности (КС). Существующая неопределенность может повлечь трудности при взаимодействии с ФСБ России.	Отклонено.	Считаем целесообразным в Положении Банка России от 9 января 2019 года № 672-П «О требованиях к защите информации в платежной системе Банка России» (далее – Положение Банка России № 672-П) отразить только функционал без определения конкретного класса защиты, данный подход согласован с Федеральной службой безопасности при разработке Положения Банка России от 9 июня 2012 года № 382-П «О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств». Конкретный класс защиты устанавливается в соответствии с приложением к Приказу ФСБ России от 10.07.2014 № 378 «Об утверждении 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».

4.	Пункт 1.11 проекта	(подпункт 14.2 пункта 14) Изложить абзац 4 в следующей редакции: «применением средств защиты информации, реализующих двухстороннюю аутентификацию». Требования по шифрованию и оценке соответствия СКЗИ для двусторонней аутентификации и шифрования значительно ограничат выбор таких СКЗИ.	Отклонено.	Требование необходимо для двухсторонней аутентификации на более ранней стадии, то есть на уровне терминирующего устройства (расшифрования), до попадания данных в прикладные системы. Наряду с некоторыми маловероятными рисками, это требование также минимизирует возможность атак непосредственно на прикладное программное обеспечение, используемое у участника. При этом, ряд участников уже реализовали данное требование, установленное в действующей редакции Положения Банка России № 672-П.
5.	Пункт 1.12 проекта	(пункт 17 Положения) Предлагается разработать рекомендации для кредитных организаций, по оценке степени риска. В Проекте предлагается банку получателя и банку отправителя оценивать степень риска операции в рамках реализуемой им системы управления рисками при осуществлении переводов денежных средств с использованием сервиса быстрых платежей. Может возникнуть ситуация, что одна и та же операция в одном банке не будет считаться рискованной, в то время, как в системе другого банка, подобная операция была бы запрещена.	Отклонено.	В настоящий момент считаем разработку рекомендаций нецелесообразной. В дальнейшем Банком России будет рассмотрен вопрос необходимости разработки данных рекомендаций.
6.	Пункт 1.12 проекта	(пункт 17 Положения) В абзаце 5 и 16 заменить слова «частью 5.1» на слова «частью 5». В таком случае будет представлена более полная ссылка на регламент приостановления операции и учет сроков приостановления.	Отклонено.	Изменение ссылки с части 5.1 статьи 8 Федерального закона от 27.06.2011 №161-ФЗ «О национальной платежной системе» (далее – Федеральный закон № 161-ФЗ) на ссылку часть 5 стати 8 Федерального закона № 161-ФЗ считаем не целесообразным. Порядок приостановления операции установлен частью 5.1 статьи 8 Федерального закона №161-ФЗ, в том числе в соответствии с частью 5.1 статьи 8 Федерального закона

				№ 161-ФЗ Банк России устанавливает признаки осуществления перевода без согласия клиента. Пункт 17 Положения устанавливает требования при реализации мер по противодействию осуществлению переводов денежных средств без согласия клиента при осуществлении переводов денежных средств с использованием сервиса быстрых платежей. В связи с этим ссылка на часть 5.1 статьи 8 Федерального закона № 161-ФЗ указана в части порядка приостановления операции на основе признаков осуществления перевода денежных средств без согласия клиента установленных Банком России и в рамках реализуемой системы управления рисками.
7.	Пункт 1.12 проекта	(пункт 17 Положения) Предлагается исключить абзац 15 п.17, невозможно осуществить полноценную оценку риска по операции силами ОУИО СБП, поскольку ОУИО СБП будет известна информация только по тем платежам клиентов, которые осуществлены через СБП. Платежи клиента в других системах (карточные операции, внутрибанковские переводы и т.д.) и дополнительная информация о клиенте может быть известна только банку - участнику.	Отклонено.	Исключение абзаца 15 пункта 17 Положения считаем не целесообразно. В случае если формирование электронного сообщения осуществляется ОУИО СБ и ОУИО СБП является непосредственной стороной взаимодействия в СБП и оказывает услуги по формированию сообщения, то ОУИО СБП должен обеспечить работу заложенных механизмов противодействия мошенничеству. При наличии необходимости у ОУИО СБП в получении дополнительных данных от Участника СБП, ОУИО СБП могут включить соответствующие требования в договор с Участником СБП. Также отмечаем, что данная норма не снимает обязанности

				выполнения требований, установленные для участника СБП.
8.	Пункт 1.14 проекта	(пункт 18 Положения) Предлагается исключить пункт 18. ОУИО СБП не сможет производить полноценную оценку риска по операциям, т.к. располагает информацией только по операциям клиента в СБП, а также ОУИО СБП не сможет отслеживать смену идентификатора устройства клиента.	Отклонено.	С учетом пояснения к вопросу 7. В случае если ОУИО и не имеет возможности проводить оценку риска полноценно, информирование участника СБП остается обязанностью ОУИО в рамках договора. В свою очередь участник СБП с учетом реализуемой системы управления рисками может принимать решение о допустимости осуществления перевода денежных средств.
9.	Пункт 2 проекта	(п. 17, 17.1 и п. 17^1 Положения) Дополнить абзацем следующего содержания: «пункты 1.12 (п. 17 и 17.1 Положения) и 1.13 (п. 17^1 Положения) настоящего Указания вступают в силу по истечении 1 года после дня его официального опубликования.». Кредитные организации просят предоставить им минимум 1 год для внедрения необходимых значительных доработок программного обеспечения и ИТ-систем в части реализации требований о направлении и обработке индикаторов степени риска, а также сведений о смене идентификатора устройств.	Учтено частично.	Пункт 17^1 Положения исключен из проекта указания. Пункт 17, подпункт 17.1 пункта 17 Положения вступают в силу с 1 января 2021 года.
10.	Пункт 1.12 проекта	(пункт 17 Положения) Требования абзаца 5 сложно реализуемы на практике, так как денежные средства в рамках СБП зачисляются практически моментально.	Отклонено. Предоставлено пояснение.	Участник СБП оценивает операцию на предмет соответствия признакам осуществления перевода денежных средств без согласия клиента с учетом реализованной системы управления рисками, по результатам которой «индикатор об уровне риска операции» будет отображаться в соответствующее поле электронного сообщения, передаваемого между Участниками СБП и ОПКЦ.
11.	Пункт 1.12 проекта	(пункт 17.1 Положения) Кредитные организации просят пояснить по каким критериям должен выявляться подозрительный клиент, и каковы должны быть масштабы переборов идентификаторов клиентов участника СБП, описанные в абзаце 19?	Отклонено. Предоставлено пояснение.	Участник СБП самостоятельно определяет критерии выявления переборов идентификаторов клиентов участника СБП в рамках реализуемой им системы управления рисками.

		Кредитные организации отмечают дублирование функций мониторинга одного и того же процесса участником СБП и ОПКЦ. В данном случае не ясна необходимость проработки и выстраивания мониторинга переборов идентификаторов клиентов участника СБП с поиском и привлечением соответствующих ресурсов при наличии существующей рабочей и зарекомендовавшей себя системы мониторинга со стороны ОПКЦ.		
12.	Пункт 1.13 проекта	(пункт 17^1 Положения) В целях реализации требований данного пункта необходима более детальная информация по механизмам и алгоритму отслеживания смены идентификатора устройства клиента. Информирование о каждом факте смены устройства, IP-адреса, номера телефона и т.д повлечет формирование огромного количества срабатываний, в связи с чем, может возникнуть нагрузка на системы при формировании и отправке информационных сообщений. Если клиент использует несколько IP-адресов, сам факт смены является основанием для информирования ОПКЦ или условием является новизна IP-адреса (ранее не встречался)? Аналогичный вопрос возникает в случае, когда периодически клиент использует разные устройства. Перечисленные идентификаторы анализируется вместе или по отдельности? Если при анализе выяснится, что IP-адрес прежний, но устройство новое (например, это IP-адрес мобильного оператора) или IP-адрес новый, но устройство прежнее (это динамический IP оператора) или номер телефона клиента поменялся, но устройство то же, является ли это основанием для отправки информационного сообщения?	Учтено.	Пункт 17^1 Положения исключен из проекта указания.