ЦЕНТРАЛЬНЫЙ БАНК РОССИЙСКОЙ ФЕДЕРАЦИИ (БАНК РОССИИ)

Департамент информационной безопасности

107016, Москва, ул. Неглинная, 12
www.cbr.ru
тел.: (499) 300-30-00, 8 (800) 300-30-00

от 21.07.2021 № 56-26/616
на № 02-05/608 от 22.06.2021

Президенту Ассоциации банков России (Ассоциация «Россия»)

Г.И. Лунтовскому

ул. Большая Якиманка, д 23,
Москва, 119180

О рассмотрении предложений в проект нормативного акта и вопросов кредитных организаций

Уважаемый Георгий Иванович!

Департамент информационной безопасности рассмотрел предложения в проект указания Банка России «О внесении изменений в Положение Банка России от 17 апреля 2019 года № 683-П «Об установлении обязательных для кредитных организаций требований к обеспечению защиты информации при осуществлении банковской деятельности в целях противодействия осуществлению переводов денежных средств без согласия клиента» (далее – Проект), а также вопросы кредитных организаций по Проекту и направляет Вам информацию о результатах рассмотрения.

Приложение: на 8 л.

С уважением,

Директор Департамента информационной безопасности В.А. Уваров

02-04/1088
27 07 21

Сводная таблица замечаний и предложений
по проекту указания Банка России «О внесении изменений
в Положение Банка России от 17 апреля 2019 года № 683-П «Об установлении обязательных для кредитных организаций
требований к обеспечению защиты информации при осуществлении банковской деятельности в целях противодействия осуществлению
переводов денежных средств без согласия клиента» (далее - Проект)

№ п/п	Структурная единица Проекта	Содержание замечания или предложения	Решение	Пояснение
1	2	3	5	6
Ассоциация «Россия»				
1.	п. 1.1 (п. 4.1 Положения)	Кредитные организации предлагают сохранить формулировку «анализ уязвимостей» вместо «оценка соответствия», а также уточнить в формулировках либо дать пояснения на предмет возможности проведения оценки соответствия информационных систем, имеющих короткие релизные циклы разработки и agile-ориентированные подходы, а также имеющих микросервисную архитектуру. Многие кредитные организации используют в своих процессах разработки agile-ориентированные подходы, а также короткий релизный цикл. Так как оценка соответствия по ГОСТ Р ИСО/МЭК 15408-3-2013 предполагает анализ конкретного релиза, кредитные организации физически не смогут проводить данную оценку каждого выпущенного релиза. Более того, в соответствии с ГОСТ Р ИСО/МЭК 15408-3-2013 оценке подлежат информационные системы в комплексе. Стандарт не учитывает возможности микросервисной архитектуры, в рамках которой информационные системы могут состоять из отдельных независимых сервисов, часть которых подлежит оценке в соответствии с требованиями, а часть нет. Тем организациям, которые уже внедрили в свой жизненный цикл информационных систем процессы безопасной разработки, учитывающие все особенности своих бизнес процессов и архитектуры информационных систем, необходимо будет пересмотреть данные процессы для их формализации в соответствии с ГОСТ Р ИСО/МЭК 15408-3-2013, что может повлечь удорожание разработки продукта и увеличение сроков выхода на рынок новых продуктов. В связи с вышеуказанным, кредитные организации считают, что полная оценка соответствия вместо анализа уязвимостей является избыточной и не учитывает современные мировые практики, подходы и особенности технологий в области разработки программного обеспечения.	Отклонено	Анализ уязвимостей является составной частью оценки соответствия по ОУД4 по требованиям к оценочному уровню доверия не ниже чем ОУД 4 в соответствии с требованиями национального стандарта Российской Федерации ГОСТ Р ИСО/МЭК 15408-3-2013. При этом указанный подход согласован со ФСТЭК России и в настоящее время уже используется в Положениях Банка России от 04.06.2020 № 719-П и от 20.04.2021 № 757-П.

2.	п. 1.1 (п. 4.1 Положения)	Предлагается дополнить абзацы первый и второй подпункта 4.1. пункта 4 Положения 683-П в редакции Проекта словами «в случае, когда применение данных мер необходимо для нейтрализации актуальных угроз и минимизации рисков информационной безопасности.» Вносимые правки в части проведения оценки соответствия фактически означают подтверждение соответствия (статья 20 Федерального закона от 27.12.2002 № 184-ФЗ «О техническом регулировании») и могут носить добровольный (в форме добровольной сертификации) или обязательный характер (в форме декларирования соответствия и в форме обязательной сертификации), что является аналогичным требованием «сертифицированных в системе сертификации Федеральной службы по техническому и экспортному контролю на соответствие требованиям по безопасности информации, включая требования по анализу уязвимостей и контролю отсутствия не декларированных возможностей».	Отклонено	Данное требование является обязательным и устанавливается в целях противодействия осуществлению переводов денежных средств без согласия клиента.
3.	п. 1.1 а (п. 4.1 Положения)	По мнению кредитных организаций, целесообразно добавить ссылку на соответствие каким требованиям и критериям необходимо проводить оценку соответствия и сертификацию Кредитные организации отметили, что новая редакция не содержит конкретики: «прошедших сертификацию в системе сертификации Федеральной службы по техническому и экспортному контролю или оценку соответствия». Кроме того, с учетом предлагаемых Проектом изменений возникает неясность в отношении положений пунктов 4.1 и 4.3 Положения № 683-П. Так, в пункте 4.1. Положения № 683-П предусмотрена необходимость сертификации в системе сертификации Федеральной службы по техническому и экспортному контролю или оценку соответствия по требованиям к оценочному уровню доверия (далее - ОУД) не ниже чем ОУД 4 в соответствии с требованиями национального стандарта Российской Федерации ГОСТ Р ИСО/МЭК 15408-3-2013 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности», утвержденного приказом Федерального агентства по техническому регулированию и метрологии от 8 ноября 2013 года № 1340-ст «Об утверждении национального стандарта» (М., ФГУП «Стандартинформ», 2014). В то же время, в пункте 4.3 Положения № 683-П предусмотрено, что кредитные организации «должны обеспечить сертификацию программного обеспечения автоматизированных систем и приложений не ниже 4 уровня доверия в соответствии с приказом Федеральной службы по техническому и экспортному контролю от 2 июня 2020 года № 76 «Об утверждении Требований по безопасности информации, устанавливающих уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий», зарегистрированным Министерством юстиции Российской Федерации 11 сентября 2020 года № 59772 (далее – приказ ФСТЭК России № 76).»	Отклонено	Для выполнения пункта 4.1, с учетом предлагаемых Проектом изменений, необходимо проводить либо оценку соответствия по требованиям к оценочному уровню доверия (далее - ОУД) не ниже чем ОУД 4 в соответствии с требованиями национального стандарта Российской Федерации ГОСТ Р ИСО/МЭК 15408-3-2013, либо сертификацию в системе сертификации Федеральной службы по техническому и экспортному контролю. Проектируемый пункт 4.3 устанавливает требования к проведению сертификации в случае принятия решения о необходимости ее проведения.

4.	п. 1.2 (п. 4.2 Положения)	«По решению кредитной организации оценка соответствия программного обеспечения автоматизированных систем и приложений проводится самостоятельно или с привлечением организации». Кредитные организации просят уточнить, в каких случаях разрешается проводить самостоятельную оценку соответствия. В этих целях предлагается дополнить Проект отдельным пунктом, содержащим пояснение для указанной формулировки. Кроме того, в случае самостоятельного проведения кредитной организацией оценки соответствия, кредитные организации просят представить разъяснения по следующим вопросам: 1. Требуется ли наличие у кредитной организации лицензии на осуществление деятельности по технической защите конфиденциальной информации на проведение работ и услуг, предусмотренных подпунктами «б», «д» или «е» пункта 4 Положения о лицензировании деятельности по технической защите конфиденциальной информации, утвержденного постановлением Правительства Российской Федерации от 03.02. 2012 № 79 «О лицензировании деятельности по технической защите конфиденциальной информации»? 2. В каком формате должен быть оформлен результат оценки соответствия? 3. Обязательно ли для оценки соответствия разрабатывать задание по безопасности на основе методического документа «Профиль защиты прикладного программного обеспечения автоматизированных систем и приложений кредитных организаций и некредитных финансовых организаций»?	Даны пояснения	Для выполнения пункта 4.1, с учетом предлагаемых Проектом изменений, необходимо проводить либо оценку соответствия по требованиям к оценочному уровню доверия (далее - ОУД) не ниже чем ОУД 4 в соответствии с требованиями национального стандарта Российской Федерации ГОСТ Р ИСО/МЭК 15408-3-2013, либо сертификацию в системе сертификации Федеральной службы по техническому и экспортному контролю. Решение о возможности проведения самостоятельной оценки соответствия программного обеспечения автоматизированных систем и приложений принимается организаций самостоятельно с учетом наличия работников, имеющих квалификацию для проведения указанных работ, а также на основе анализа рисков.
5.	п.1.5 (п. 5.2.1 Положения)	«В случае если банковская операция осуществляется с мобильных (переносных) устройств вычислительной техники кредитные организации в рамках реализуемой ими системы управления рисками должны обеспечить проверку используемого клиентом – физическим лицом абонентского номера подвижной радиотелефонной связи на основе анализа характера, параметров и объема совершаемых их клиентами операций (осуществляемой клиентами деятельности).» Абзац 3 пункта 1.3 Проекта не учитывает, что мобильные устройства могут быть без возможности подтверждения номера по телефону (планшет без сим-карты, использующий полноценную версию сайта интернет-банкинга). Предлагается изложить в редакции «при использовании мобильной версии приложения» или «при использовании приложения, установка (вход) которого невозможна без указания номера мобильного телефона».	Учтено в редакции	

6.	п. 1.4 (п. 5.1 Положения)	«В целях обеспечения целостности электронных сообщений и подтверждения их составления уполномоченным на это лицом кредитные организации должны обеспечивать реализацию мер по использованию усиленной квалифицированной электронной подписи, усиленной неквалифицированной электронной подписи или иных средств криптографической защиты информации (СКЗИ), реализующих функцию имитозащиты информации с аутентификацией отправителя сообщения.» Кредитные организации просят уточнить в Проекте возможность применения механизмов простой электронной подписи, а также что подразумевается под понятием «иных СКЗИ». В случае, если имеется в виду использование симметричных алгоритмов, остается неясным достаточно ли будет использовать связку простая электронная подпись для аутентификации отправителя сообщения и симметричная криптография для имитозащиты и обеспечения целостности.	Даны пояснения	Предложенный вариант применения механизмов использования простой электронной подписи соответствует требованиям проектируемой нормы.
7.	п. 1.4 (п. 5.1 Положения)	Предлагается исключить из второго и третьего абзацев подпункта 5.1 пункта 5 Положения № 683-П в редакции Проекта слово «иных» применительно к СКЗИ. Усиленная квалифицированная и усиленная неквалифицированная электронные подписи не являются средством криптографической защиты информации, они формируются с помощью таких средств.	Учтено	
8.	п. 1.4 (п. 5.1 Положения)	«Указанные в абзаце втором настоящего пункта требования по реализации мер по использованию усиленной квалифицированной электронной подписи, усиленной неквалифицированной электронной подписи или иных СКЗИ, реализующих функцию имитозащиты информации с аутентификацией отправителя сообщения, не применяются в случае, если в целях обеспечения целостности электронных сообщений и подтверждения их составления уполномоченным на это лицом при передаче электронных сообщений используются выделенные сегменты вычислительных сетей и указанные меры определены кредитными организациями как неактуальные в модели угроз и нарушителей безопасности информации.» По мнению кредитных организаций, остается неясным, что подразумевает понятие «выделенные сегменты вычислительных сетей»: 1. выделенный сегмент технологического участка дистанционного банковского обслуживания; 2. выделенный сегмент программного обеспечения, обрабатывающего защищаемую информацию на участках, используемых для приема электронных сообщений, к исполнению в автоматизированных системах и приложениях с использованием информационно-телекоммуникационной сети «Интернет».		Абзац исключен

9.	п. 1.4 (п. 5.1 Положения)	Предлагается оставить пункт 5.1 Положения №683-П в текущей редакции: «5.1. Кредитные организации должны обеспечивать подписание электронных сообщений способом, позволяющим обеспечить целостность и подтвердить составление указанного электронного сообщения уполномоченным на это лицом. Признание электронных сообщений, подписанных электронной подписью, равнозначными документам на бумажном носителе, подписанным собственноручной подписью, должно осуществляться в соответствии со статьей 6 Федерального закона от 6 апреля 2011 года № 63-ФЗ «Об электронной подписи» (Собрание законодательства Российской Федерации, 2011, № 15, ст. 2036; № 27, ст. 3880; 2012, № 29, ст. 3988; 2013, № 14, ст. 1668; № 27, ст. 3463, ст. 3477; 2014, № 11, ст. 1098; № 26, ст. 3390; 2016, № 1, ст. 65; № 26, ст. 3889) (далее - Федеральный закон «Об электронной подписи»).» Согласно пояснительной записке к проекту, Банком России вносятся изменения, в частности, уточнения требований, предъявляемых к обеспечению целостности электронных сообщений, которыми обмениваются кредитные организации со своими клиентами. Согласно изменениям, для обеспечения целостности должны использоваться СКЗИ, что исключает использование простой электронной подписи. Стоит отметить, что в информационном письме от 30.01.2020 № ИН-014-56/4 Банком России были даны разъяснения относительно возможности обеспечения целостности при использовании простой электронной подписи и аналогов собственноручной подписи. Согласно абзацу первому подпункта 5.1 пункта 5 Положения № 683-П, абзацу первому пункта 10 Положения № 684-П, кредитные организации, а также некредитные финансовые организации, реализующие усиленный и стандартный уровни защиты информации (далее – некредитные финансовые организации), должны обеспечивать подписание электронных сообщений способом, позволяющим обеспечить целостность и подтвердить составление указанного электронного сообщения уполномоченным на это лицом. В целях обеспечения контроля целостности электронных сообщений и подтверждения составления электронного сообщения уполномоченным на это лицом кредитным организациям, некредитным финансовым организациям рекомендуется обеспечивать использование усиленной электронной подписи или с соблюдением применяемой технологии обработки защищаемой информации иных аналогов собственноручной подписи, кодов, паролей и других средств при подписании электронных сообщений. С учетом системной связи положений части 1 статьи 5 Федерального закона «Об электронной подписи» о видах электронной подписи и положений части 4 статьи 11 Федерального закона от 27 июля 2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» к аналогу собственноручной подписи относится, в частности, простая электронная подпись. Таким образом, в новой редакции Положения № 683-П Банком России исключается использование простой электронной подписи и иных аналогов собственноручной подписи, не использующих СКЗИ, при том, что они, в сочетании с другими средствами, используемыми при подписании электронных сообщений, могут обеспечить целостность электронных сообщений. Кредитные организации считают, что не стоит ограничивать использование простой электронной подписи и иных аналогов собственноручной подписи, если они могут обеспечить выполнение требований, предъявляемых к электронным сообщениям.	Отклонено	Изменения вносятся с целью реализации возможности применения простой электронной подписи.

10.	п. 1.5 (п. 5.2.1 Положения)	В случае если банковская операция осуществляется с мобильных (переносных) устройств вычислительной техники кредитные организации в рамках реализуемой ими системы управления рисками должны обеспечить проверку используемого клиентом – физическим лицом абонентского номера подвижной радиотелефонной связи на основе анализа характера, параметров и объема совершаемых их клиентами операций (осуществляемой клиентами деятельности). К мобильным (переносным устройствам) относятся и ноутбуки. Возможно использование смартфонов и планшетов через wifi соединение. Учитывая изложенное, представленная в Проекте формулировка, по мнению кредитных организаций, не является в полной степени корректной и требует доработки.	Учтено	
11.	п. 1.5 (п. 5.2.1 Положения)	«Технология обработки защищаемой информации, применяемая на технологическом участке, указанном в абзаце втором подпункта 5.2 настоящего пункта, дополнительно должна обеспечивать идентификацию устройств клиентов при осуществлении банковских операций с использованием удаленного доступа клиентов к объектам информационной инфраструктуры кредитных организаций.» Из текста Проекта остается неясным, что подразумевается под понятием «удаленный доступ к объектам информационной инфраструктуры кредитных организаций» с учетом того, что это касается технологического участка «идентификация, аутентификация и авторизация клиентов при совершении действий в целях осуществления банковских операций». Имелась ли в виду ситуация, когда происходит попытка входа в систему интернет-банк через мобильное приложение или толстый клиент системы дистанционного банковского обслуживания через сессию удаленного доступа к клиентской рабочей станции?	Учтено в редакции	
12.	п. 1.5 (п. 5.2.1 Положения)	«В случае если банковская операция осуществляется с мобильных (переносных) устройств вычислительной техники кредитные организации в рамках реализуемой ими системы управления рисками должны обеспечить проверку используемого клиентом – физическим лицом абонентского номера подвижной радиотелефонной связи на основе анализа характера, параметров и объема совершаемых их клиентами операций (осуществляемой клиентами деятельности).» Кредитные организации просят пояснить, что подразумевается под проверкой используемого абонентского номера, а также какие способы проверки предлагаются.	Даны пояснения	Подразумевается проверка принадлежности клиенту абонентского номера, в том числе с путем непосредственного взаимодействия кредитных организаций с операторами связи.

13.	п. 1.5 (п. 5.2.1 Положения)	«Кредитные организации должны реализовывать механизмы подтверждения принадлежности клиенту адреса электронной почты, на который кредитной организацией направляются уведомления о совершаемых банковских операциях, справки (выписки) по совершенным банковским операциям» Кредитные организации просят уточнить, достаточно ли будет в рамках реализации требования наличия разового письменного подтверждения клиентом адреса электронной почты.	Даны пояснения	Реализация разового письменного подтверждения клиентом адреса электронной почты будет являться выполнением данного требования. При этом кредитные организации могут осуществлять периодическое повторное подтверждение адресов электронной почты клиентов в целях снижения вероятности возникновения рисков, связанных с отправкой уведомлений о совершаемых банковских операциях, справок (выписок) по совершенным банковским операциям на электронные адреса неиспользуемые клиентами. О проверке адреса электронной почты Банком России было опубликовано информационно письмо от 12.02.2020 № ИН-014-56/6 «Информационное письмо о проверке кредитными организациями и некредитными финансовыми организациями принадлежности клиенту адреса электронной почты».
14.	п. 1.6 (п. 5.2.3 Положения)	Кредитные организации считают целесообразным раскрыть определение «код банковской операции» или указать ссылку на нормативный правовой акт, в котором дано определение. Среди регистрируемых данных по действиям работников указан «код банковской операции», определение которого в Положении № 683-П не приведено.	Учтено в редакции	Определение «код банковской операции» исключено из проекта.
15.	п. 1.8	«Кредитные организации на основании заявлений клиентов, переданных способами, определенными договорами кредитных организаций с клиентами, должны установить ограничения по осуществлению операций клиентами либо максимальную сумму перевода денежных средств за одну операцию и (или) за определенный период времени, осуществляемых с использованием удаленного доступа клиентов к объектам информационной инфраструктуры кредитных организаций.» Аналогично замечанию к пункту 1.5 Проекта из текста остается неясным, что подразумевается под понятием «удаленный доступ к объектам информационной инфраструктуры кредитных организаций» с учетом того, что это касается технологического участка «идентификация, аутентификация и авторизация клиентов при совершении действий в целях осуществления банковских операций».	Учтено в редакции	

16.	п. 1.8	Предлагается изложить пункт 1.8 Проекта следующим образом: «7[1]. Кредитные организации на основании заявлений клиентов, переданных способами, определенными договорами кредитных организаций с клиентами, должны установить ограничения по осуществлению операций клиентами либо максимальную сумму перевода денежных средств за одну операцию и (или) за определенный период времени, осуществляемых с использованием удаленного доступа клиентов к объектам информационной инфраструктуры кредитных организаций. Лимиты могут быть установлены как на все операции клиентов, так и в разрезе видов операций.» Предлагаемая редакция позволяет предусмотреть возможность устанавливать отдельные лимиты на различные виды операций.	Учтено в редакции	
17.	п. 1.9 (п. 8 Положения)	Представляется необходимым согласовать указанные в Проекте варианты ведения базы данных инцидентов с нормами Положения Банка России от 08.04.2020 № 716-П «О требованиях к системе управления операционным риском в кредитной организации и банковской группе» Абзац 2 пункта 8 Положения № 683-П в редакции Проекта предписывает направление информации об инциденте информационной безопасности в службу управления рисками для внесения в их базу данных, в то время как Положение № 716-П позволяет выбрать, кто именно ведет базу данных по рискам информационной безопасности - служба рисков или служба информационной безопасности.	Учтено в редакции	
18.	п. 1.10 (п. 9 Положения)	Проектом предлагается в пункте 9 Положения № 683-П слова «сторонних организаций, имеющих лицензию на проведение работ и услуг, предусмотренных подпунктами «б», «д» или «е» пункта 4 Положения о лицензировании деятельности по технической защите конфиденциальной информации, утвержденного постановлением Правительства Российской Федерации № 79 (далее – проверяющая организация)» заменить словами «проверяющих организаций». В случае изменения всего пункта исчезают квалификационные требования к «проверяющим организациям». Предлагается заменить слова «сторонних организаций» на «проверяющих организаций» и исключить слова «(далее - проверяющая организация)».	Отклонено	Сокращение «проверяющая организация» в соответствии с п. 1.2 Проекта переносится в п. 4.2 Положения № 683-П. Таким образом квалификационные требования к «проверяющим организациям» не исключаются из Положения № 683-П.