ПАРТАД

115419, г. Москва
ул. Орджоникидзе, д. 11, стр. 1А
Бизнес-парк "Орджоникидзе 11"
115162, г. Москва, а/я 23
+7 (495) 789 68 85
www.partad.ru info@partad.ru

Исх. № 123 -б от « 17 » сентября 2018 г.

Директору Департамента рынка ценных бумаг и товарного рынка Банка России

Л.К. Селютиной

Уважаемая Лариса Константиновна!

В рамках рассмотрения членами СРО ПАРТАД проекта Положения Банка России «Об установлении обязательных для некредитных финансовых организаций требований к обеспечению защиты информации при осуществлении деятельности в сфере финансовых рынков» был подготовлен ряд предложений и комментариев. Предлагаем учесть направляемые предложения (см. Приложение) при дальнейшей работе над указанным проектом Банка России.

Приложение: *Предложения членов ПАРТАД к проекту Положения Банка России «Об установлении обязательных для некредитных финансовых организаций требований к обеспечению защиты информации при осуществлении деятельности в сфере финансовых рынков» - на 11 стр.*

С уважением,
Председатель Правления

П.В. Дубонос

Приложение

Предложения членов ПАРТАД к проекту Положения Банка России «Об установлении обязательных для некредитных финансовых организаций требований к обеспечению защиты информации при осуществлении деятельности в сфере финансовых рынков»

пункт	Проект Положения	Предложения/ комментарии
п. 1.	На основании статьи 76.4-1 Федерального закона от 10 июля 2002 года № 86-ФЗ «О Центральном банке Российской Федерации (Банке России)» (Собрание законодательства Российской Федерации, 2002, № 28, ст. 2790; 2004, № 31, ст. 3233; 2005, № 25, ст. 2426; 2007, № 1, ст. 10; 2008, № 42, ст. 4696; № 44, ст. 4982; 2009, № 1, ст. 25; 2010, № 45, ст. 5756; 2011, № 7, ст. 907; № 48, ст. 6728; 2012, № 53, ст. 7591; 2013, № 27, ст. 3438; № 30, ст. 4084; № 49, ст. 6336; № 51, ст. 6695; № 52, ст. 6975; 2014, № 30, ст. 4219; № 45, ст. 6154; № 52, ст. 7543; 2015, № 1, ст. 4, 37; № 27, ст. 3958; № 29, ст. 4348, 4357; 2016, № 1, ст. 46, 50; № 26, ст. 3891; № 27, ст. 4225, 4295; 2017, № 18, ст. 2661, 2669; № 30, ст. 4456; № 31, ст. 4830; 2018, № 11, ст. 1584, 1588; 2018, № 24, ст. 3400; 2018, № 27, ст. 3950) (далее – Федеральный закон № 86-ФЗ) настоящее Положение устанавливает обязательные для некредитных финансовых организаций требования к обеспечению защиты информации при осуществлении деятельности в сфере финансовых рынков, предусмотренных статьей 76.1 Федерального закона № 86-ФЗ (далее – деятельность в сфере финансовых рынков), в целях противодействия незаконным финансовым операциям, за исключением требований к обеспечению защиты информации, установленных федеральными законами и принятыми в соответствии с ними нормативными правовыми актами (далее - требования к защите информации при осуществлении деятельности в сфере финансовых рынков).	Рассматривая указанные нормативные акты в совокупности, вправе ли Регистратор осуществлять защиту информации, относящуюся к финансовым операциям и одновременно относящуюся к персональным данным, руководствуясь требованиями вышестоящего по отношению к Проекту Положения, нормативными актами – Федеральным законом 152-ФЗ и постановлением Правительства №1119, выполняя мероприятия по защите финансовых операций исключительно в отношении актуальных угроз безопасности и в соответствии с уровнем защищенности информационной системы?
п.3.,	3. Требования к защите информации при осуществлении	Распространяются ли требования Проекта Положения на информацию,

п.11.2., п.12.3.	деятельности в сфере финансовых рынков применяются для обеспечения защиты следующей информации (далее – защищаемая информация): информации, подготавливаемой, обрабатываемой и хранимой в целях осуществления операций, реализуемых для осуществления деятельности в сфере финансовых рынков (**далее – финансовые операции**); … 11.2. При реализации ограничений по параметрам финансовых операций могут применяться следующие ограничения: на максимальную сумму за одну финансовую операцию и (или) за определенный период времени; … 12.3. Некредитные финансовые организации, указанные в подпунктах 4.1, 4.2 пункта 4 настоящего Положения, обеспечивают регистрацию инцидентов, связанных с нарушениями требований к защите информации при осуществлении деятельности в сфере финансовых рынков, в том числе событий, которые привели или могут привести к осуществлению финансовых операций без согласия клиента, неоказанию услуг по осуществлению финансовых операций. По каждому инциденту, указанному в настоящем подпункте, некредитные финансовые организации обеспечивают регистрацию, в том числе: ... результата реагирования на инцидент, связанный с осуществлением финансовой операции без согласия клиента, в том числе по возврату денежных средств или электронных денежных средств.	содержащуюся на бумажных носителях? Необходимо дать развернутое определение понятия «финансовые операции», которое бы учитывало специфику деятельности разных тиов некредитных финансовых организаций.
п. 4., п. 17.	4.Для объектов информационной инфраструктуры, а также автоматизированных систем, используемых для осуществления	Установить определение групп НФО в отдельном разделе/пункте, так как п. 4 вступает в силу только с 01.01.2021 либо уточнить в проекте какой

	финансовых операций в целях обработки, передачи, хранения защищаемой информации, некредитные финансовые организации обеспечивают следующие уровни защиты информации, определенные национальным стандартом Российской Федерации ГОСТ Р 57580.1-2017 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер», утвержденным приказом Росстандарта от 8 августа 2017 года № 822-ст «Об утверждении национального стандарта» (М., ФГУП «Стандартинформ», 2017). 17. … Пункт 4, подпункты 16.1, 16.2 пункта 16 настоящего Положения вступают в силу с 1 января 2021 года.	уровень защиты информации будет применятся НФО до вступлению в силу указанного пункта.
п. 5	Некредитные финансовые организации, указанные в подпунктах 4.1, 4.2 пункта 4 настоящего Положения, на стадиях создания и эксплуатации объектов информационной инфраструктуры обеспечивают: использование для осуществления финансовых операций прикладного программного обеспечения автоматизированных систем и приложений, 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 недекларированных возможностей, в соответствии с законодательством Российской Федерации или в отношении которых проведен анализ уязвимостей 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 «Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных	Предлагается следующая редакция: «*использование для осуществления финансовых операций* ***средств защиты информации и (или)*** *прикладного программного обеспечения автоматизированных систем и приложений, сертифицированных…»* В проекте Положения не описаны условия, при наличии которых организация имеет право самостоятельно проводить анализ уязвимостей в прикладном программном обеспечении автоматизированных систем и приложений. Предлагаем дополнить пункт: «…либо самостоятельно при наличии у организации лицензии 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». В целом выполнение данного требования означает, что все прикладное ПО, которое используется компанией для осуществления финансовых операций, должно быть сертифицировано ФСТЭК. Для компаний, использующих

	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); … Для проведения анализа уязвимостей в прикладном программном обеспечении автоматизированных систем и приложений некредитные финансовые организации,…, могут привлекать организацию, имеющую лицензию на осуществление деятельности по технической защите конфиденциальной информации…	указанное ПО собственные разработки, данное требование трудновыполнимое. Тем более до 01.01.2020г. Процедура получения сертификации дорогая и продолжительная. Каким образом будет осуществляться ФСТЭК массовая сертификация указанного ПО в такой короткий срок? Кроме того, сертификация будет действовать на конкретную версию, актуальную в настоящее время. При внесении плановых изменений, например, в связи с новыми требованиями регуляторов, необходимо проходить процедуру повторной сертификации. Каким образом это может быть реализовано? В целом, считаем данное требование ненужным, так как защита информации при осуществлении финансовых операций обеспечивается в том числе средствами информационной безопасности, функционирующими совместно с указанным прикладным ПО и имеющими необходимые сертификаты ОУД и НДВ.
п. 6.	Некредитные финансовые организации, указанные в подпунктах 4.1, 4.2 пункта 4 настоящего Положения, программного обеспечения, используемого клиентом при осуществлении финансовых операций, в том числе при разработке изменений указанного программного обеспечения, обеспечивают реализацию в указанном программном обеспечении функций, связанных: с выполнением требований к защите информации при осуществлении финансовых операций; … Некредитные финансовые организации,…, контролируют реализацию указанных функций при разработке программного обеспечения с привлечением сторонней организации, а также при закупке готового к использованию программного обеспечения без дополнительной доработки.	О каких конкретно требованиях идет речь в данном пункте? В проекте не учены следующие вопросы, требующие разъяснения: - Не указано, какую организацию (тип организации) можно привлечь. - Должна ли сторонняя организация иметь лицензию на осуществление деятельности по технической защите конфиденциальной информации? - Какова роль этой организации при разработке (модернизации) программного обеспечения? Предлагаем дополнить проект требованиями к типу, полномочиям и роли сторонней организации при разработке и модернизации ПО.
п. 7.	Некредитные финансовые организации обеспечивают регистрацию своих работников, обладающих правами по формированию электронных сообщений, содержащих первичные	Проектом не предусмотрено, каким образом НФО должны осуществлять обозначенную регистрацию. Предлагаем дополнить проект требованиями к предлагаемому порядку

	документы на осуществление финансовых операций (далее – электронные сообщения.	регистрации, а также добавить ссылку на подпункт 12.2.1., в котором указано, какие данные о действиях работников должны регистрироваться при осуществлении финансовых операций.
п. 9.2.	9.2. Криптографические ключи изготавливаются клиентом (самостоятельно) и (или) некредитной финансовой организацией.	Необходимо уточнить порядок изготовления криптографических ключей клиентом. Уточнение «(самостоятельно)» исключает возможность обращения клиента для изготовления криптографических ключей, например, в сторонний аккредитованный удостоверяющий центр.
п. 11.	Некредитные финансовые организации, указанные в подпунктах 4.1, 4.2 пункта 4 настоящего Положения, при осуществлении деятельности в сфере финансовых рынков с использованием сети «Интернет» и размещении программного обеспечения, используемого клиентом при осуществлении финансовых операций на средствах вычислительной техники, для которых некредитными финансовыми организациями не обеспечивается непосредственный контроль защиты информации от воздействия вредоносного кода, обеспечивают реализацию технологических мер по использованию раздельных информационно-коммуникационных технологий для подготовки электронных сообщений и передачи клиентами подтверждений **об исполнении** первичных документов на осуществление финансовых операций (далее – технологические меры по использованию раздельных технологий) и (или) реализовывают ограничения по параметрам финансовых операций, определяемые договором некредитной финансовой организации с клиентом, а также обеспечивают возможность установления указанных ограничений по инициативе клиента.	Предлагается изложить п. 11 проекта в следующей редакции: «*Некредитные финансовые организации, указанные в подпунктах 4.1, 4.2 пункта 4 настоящего Положения, при осуществлении деятельности в сфере финансовых рынков с использованием сети «Интернет» и размещении программного обеспечения, используемого клиентом при осуществлении финансовых операций на средствах вычислительной техники, для которых некредитными финансовыми организациями не обеспечивается непосредственный контроль защиты информации от воздействия вредоносного кода, обеспечивают реализацию технологических мер по использованию раздельных информационно-коммуникационных технологий для подготовки электронных сообщений и передачи клиентами подтверждений* ***для исполнения*** *первичных документов на осуществление финансовых операций (далее – технологические меры по использованию раздельных технологий) и (или) реализовывают ограничения по параметрам финансовых операций, определяемые договором некредитной финансовой организации с клиентом, а также обеспечивают возможность установления указанных ограничений по инициативе клиента*».
п. 11.1.	Реализуемые некредитными финансовыми организациями, указанными в подпунктах 4.1, 4.2 пункта 4 настоящего Положения, технологические меры по использованию раздельных технологий должны обеспечивать:	Предлагается изложить абз. 6 п. 11.1. проекта в следующей редакции: «*осуществление некредитной финансовой организацией финансовых операций только в случае положительных результатов аутентификации входных электронных сообщений (пакета электронных сообщений)*».

	… удостоверение некредитной финансовой организацией в праве клиента осуществлять финансовые операции только в случае положительных результатов аутентификации входных электронных сообщений (пакета электронных сообщений).	
п. 12.	Некредитные финансовые организации, указанные в подпунктах 4.1, 4.2 пункта 4 настоящего Положения, обеспечивают регламентацию, реализацию, контроль (мониторинг) технологии безопасной обработки защищаемой информации, указанной в абзацах втором, третьем, четвертом пункта 3 настоящего Положения, в том числе содержащейся в электронных сообщениях, на следующих этапах осуществления финансовых операций: формирование (подготовка) защищаемой информации, в том числе содержащейся в электронных сообщениях; передача защищаемой информации, в том числе содержащейся в электронных сообщениях; идентификация, аутентификация и авторизация клиентов при осуществлении финансовых операций; получение подтверждения клиента об исполнении первичных документов на осуществление финансовых операций; уведомление клиента об осуществленных финансовых операциях; обработка защищаемой информации, в том числе содержащейся в электронных сообщениях; хранение электронных сообщений.	Согласно пункту 12 проекта НФО должны обеспечивать регламентацию, реализацию, контроль (мониторинг) технологии безопасной обработки защищаемой информации, указанной в абзацах втором, третьем, четвертом пункта 3 Положения, **в том числе** на этапах осуществления финансовых операций, среди которых указан и этап «идентификация, аутентификация и авторизация клиентов при осуществлении финансовых операций». Но, согласно пункту 3 Положения «информация, необходимая для идентификации и аутентификации клиентов…» является **пятым** абзацем и не может входить в перечисленные в пункте 12 этапы осуществления финансовых операций. Для устранения нестыковки предлагаем добавить по тексту пункта ссылку на пятый абзац пункта 3 Положения либо убрать из пункта этап «идентификация, аутентификация и авторизация клиентов при осуществлении финансовых операций». Предлагается изложить абз. 5 п. 12. проекта в следующей редакции: «*получение подтверждения клиента* ***для исполнения*** *первичных документов на осуществление финансовых операций*».
пп. 12.2.2, п. 12.3.	12.2.2. Регистрации подлежат, в том числе следующие данные о действиях клиентов, выполняемых с использованием автоматизированных систем, программного обеспечения: дата (день, месяц, год) и время (часы, минуты, секунды) осуществления клиентом финансовой операции; набор символов, присвоенный клиенту и позволяющий идентифицировать его в автоматизированной системе,	В Положении не установлено, каким образом НФО должны осуществлять обозначенную регистрацию. Предлагаем уточнить порядок регистрации данных о действиях клиентов и инцидентов, связанных с нарушениями требований к защите информации.

	программном обеспечении; уникальный идентификатор финансовой операции; код, соответствующий этапу осуществления финансовой операции; результат осуществления клиентом финансовой операции (успешная или неуспешная); идентификационная информация, используемая для адресации устройства, с использованием которого осуществлен доступ к автоматизированной системе, программному обеспечению с целью осуществления финансовых операций, которой в зависимости от технической возможности является IP-адрес, MAC-адрес, номер SIM-карты, номер телефона и (или) иной идентификатор устройства. 12.3. Некредитные финансовые организации, указанные в подпунктах 4.1, 4.2 пункта 4 настоящего Положения, обеспечивают регистрацию инцидентов, связанных с нарушениями требований к защите информации при осуществлении деятельности в сфере финансовых рынков, в том числе событий, которые привели или могут привести к осуществлению финансовых операций без согласия клиента, неоказанию услуг по осуществлению финансовых операций. По каждому инциденту, указанному в настоящем подпункте, некредитные финансовые организации обеспечивают регистрацию, в том числе: уникального идентификатора осуществления финансовой операции без согласия клиента; этапа (этапов) осуществления финансовой операции, на котором(ых) произошел несанкционированный доступ к защищаемой информации; результата реагирования на инцидент, связанный с осуществлением финансовой операции без согласия клиента, в том числе по возврату денежных средств или электронных денежных средств.	

п. 13.	Некредитные финансовые организации, указанные в подпунктах 4.1, 4.2 пункта 4 настоящего Положения: … участвовать в действиях, связанных с восстановлением предоставления услуг автоматизированных систем после сбоев и (или) отказов в работе объектов информационной инфраструктуры.	Считаем, что подразделение (работник), ответственное за организацию и контроль обеспечения защиты информации в организации, не должно участвовать в восстановлении функционирования автоматизированных систем в случае сбоев и реализации угроз, не связанных с нарушениями требований к защите информации. Предлагаем изменить формулировку абзаца на следующую: «участвовать в действиях, связанных с восстановлением предоставления услуг автоматизированных систем после сбоев и (или) отказов в работе объектов информационной инфраструктуры, произошедших в результате реализации угроз, **связанных с нарушениями требований к защите информации при осуществлении деятельности в сфере финансовых рынков**».
п. 15.	Некредитные финансовые организации к инцидентам, связанным с нарушениями требований к защите информации при осуществлении деятельности в сфере финансовых рынков, должны относить события, которые привели или могут привести к осуществлению финансовых операций без согласия клиента, неоказанию услуг по осуществлению финансовых операций, в том числе включенные в перечень инцидентов, согласованный с федеральным органом исполнительной власти, уполномоченным в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, и размещаемый Банком России на официальном сайте Банка России в информационно-телекоммуникационной сети «Интернет» (далее – перечень инцидентов). Некредитные финансовые организации осуществляют информирование Банка России: о выявленных инцидентах, связанных с нарушением требований к защите информации при осуществлении деятельности в сфере финансовых рынков, в том числе включенных в перечень инцидентов; о планируемых мероприятиях по раскрытию информации об	Необходимо уточнить, в какой срок и в каком разделе официального сайта Банка России в сети «Интернет» будет размещена информация о перечне инцидентов. Нарушения клиентом или НФО? Согласно пункту 24 Приложения 1 к Указанию Банка России от 28.12.2015

	инцидентах, связанных с нарушением требований к защите информации при осуществлении деятельности в сфере финансовых рынков, включая размещение информации на официальных сайтах в информационно-телекоммуникационной сети «Интернет», выпуск пресс-релизов и проведение пресс-конференций не позднее одного рабочего дня до проведения мероприятия.	№3921-У профессиональные участники рынка ценных бумаг обязаны раскрывать на своем сайте в сети Интернет, в том числе: «Информация о технических сбоях в автоматизированных системах профессионального участника рынка ценных бумаг, которые повлекли прекращение (ограничение) работоспособности таких систем, что привело к отсутствию возможности осуществления деятельности профессионального участника рынка ценных бумаг в отношении всех клиентов профессионального участника рынка ценных бумаг, с указанием даты, времени и причин прекращения работоспособности. В течение часа с момента выявления технического сбоя». Возможен конфликт двух нормативных документов так как технические сбои могут привести одновременно к нарушению требований к защите информации и, одновременно, невозможности осуществления деятельности профучастника.
п. 15.	Информирование осуществляется в форме предоставления некредитной финансовой организацией в Банк России сведений, указанных в абзацах третьем и четвертом настоящего пункта. Информация о форме и сроке предоставления указанных сведений подлежит согласованию с федеральным органом исполнительной власти, уполномоченным в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации согласно части 6 статьи 5 Федерального закона от 26 июля 2017 года № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» (Собрание законодательства Российской Федерации, 2017, № 31, ст. 4736), и размещается на официальном сайте Банка России в сети «Интернет».	Необходимо уточнить, в какой срок и в каком разделе официального сайта Банка России в сети «Интернет» будет размещена информация о форме и сроке предоставления сведений.
п. 16	Некредитные финансовые организации обеспечивают проведение оценки соответствия уровню защиты информации, установленному в пункте 4 настоящего Положения (далее – оценка соответствия защиты информации), не реже одного раза в	Предлагаем установить периодичность проведения оценки «не реже одного раза в три года» по аналогии со сроком, указанным в пункте 17 Постановления Правительства РФ от 01.11.2012 №1119 и сертификацией на соответствие требованиям ISO 27001.

	два года.	
п. 16	Некредитные финансовые организации, указанные в подпунктах 4.1, 4.2 пункта 4 настоящего Положения, осуществляют оценку соответствия защиты информации с привлечением 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).	Предлагаем включить в п.16 возможность проведения оценки уровня защиты информации силами специалистов профильных СРО.
Без пункта		Также предлагаем дополнить проект Положения разделом «Тезаурус» с установлением определений следующих понятий: a. Первичные документы (*бумажные или электронные*). b. Электронные сообщения (*это файл, запись в базе данных*?). c. Электронные сообщения, содержащие первичные документы. d. Клиенты НФО (*это лица с которыми у НФО заключены договоры об обслуживании или это вообще все контрагенты: трансфер-агенты, номинальные держатели и т.д.*) e. Идентификация и аутентификация. f. Удостоверение клиентами права на осуществление финансовых операций. g. Объекты информационный инфраструктуры. h. Прикладное программное обеспечение.
Без пункта		Проведя изучение проекта Положения считаем, что обязательные требования по реализации мер защиты финансовых операций (например, требование об обязательной сертификации прикладного ПО для выполнения финансовых операций) не учитывают подходов об адекватности принимаемых мер защиты и объема и ценности защищаемой информации, которые предусматриваются другими нормативными актами по защите информации в частности: п.5 ст. 10 федерального закона 98-ФЗ «О коммерческой тайне»: «Меры по

		охране конфиденциальной информации признаются разумно достаточными…»; п.2. постановления Правительства №1119 от 01.10.2012: «…Безопасность персональных данных при их обработке в информационной системе обеспечивается с помощью системы защиты …, нейтрализующей актуальные угрозы…»; п.2.4. Руководящего документа Гостехкомиссии России (СТР-К): «…Уровень технической защиты конфиденциальной информации, а также перечень необходимых мер защиты определяется дифференцированно по результатам обследования объекта информатизации с учетом соотношения затрат на организацию защиты информации и величину ущерба, который может быть нанесен собственнику информационных ресурсов…»; и другими нормативными актами, такими как 152-ФЗ «О персональных данных», 149-ФЗ «Об информации, информационных технологиях и защите информации», 63-ФЗ «Об электронной подписи». Учитывая, изложенное предлагается пересмотреть подход, не учитывающий объемы операций и объемы информации конкретной НФО, к разумно-достаточному подходу по нейтрализации только актуальных угроз, определенных индивидуально для каждой организации. При этом можно предусмотреть, что оценка адекватности предпринятых мер защиты оценивается лицензиатом ФСТЭК, имеющим соответствующую лицензию.