Саморегулируемая организация
НАУФОР
Национальная ассоциация
участников фондового рынка

Россия, 109004, Москва, ул. Земляной Вал, д.65, стр.2
Тел.: (495) 787-77-75, 787-77-74
Internet: www.naufor.ru

Первому заместителю
Директора департамента по
информационной безопасности
Банка России
Сычеву А.М.

Исх. № 503 от 19 августа 2020 года

Уважаемый Артем Михайлович!

В связи с многочисленными обращениями профессиональных участников рынка ценных бумаг, управляющих компаний и специализированных депозитариев, являющихся членами НАУФОР, просим рассмотреть возможность внести в Положение Банка России от 17 апреля 2019 года №684-П «Об установлении обязательных для некредитных финансовых организаций требований к обеспечению защиты информации при осуществлении деятельности в сфере финансовых рынков в целях противодействия осуществлению незаконных финансовых операций», следующие изменения, направленные на уточнение требований к информационной безопасности некредитных финансовых организаций.

1. Повышение минимальных значений показателей для отнесения профессиональных участников рынка ценных бумаг к числу финансовых организаций, применяющих стандартный уровень защиты.

Установленная Положением граница между применением минимального и стандартного уровня защиты (количество клиентов или сумма сделок с ценными бумагами) неоптимальна, вследствии чего значительное количество профессиональных участников рынка ценных бумаг могут попасть в категорию лиц, применяющих стандартный уровень защиты, что повлечет для них дополнительные финансовые и операционные затраты. Полагаем, что повышенные требования (стандартный уровень защиты) должны применяться к действительно крупным финансовым организациям, имеющим широкую клиентскую базу и значительную долю в обороте финансовых

инструментов, что в полной мере соответствовало бы риск-ориентированному подходу в регулировании и надзоре за финансовым рынком.

В связи с вышеизложенным, просим рассмотреть возможность внесения следующих изменений в подпункт 5.3 пункта 5 Положения для повышения минимальных значений показателей для отнесения некредитных финансовых организаций к числу лиц, применяющих стандартный уровень защиты:

а) в абзаце «брокеры, которые в течение трех последних кварталов по состоянию на 31 декабря года, предшествующего дате определения уровня защиты информации, заключили сделки купли-продажи ценных бумаг за счет своих клиентов при осуществлении брокерской деятельности в объеме «более 100 000 миллионов рублей» заменить на «более 200 миллиардов рублей» в квартал и (или) которые в течение трех последних кварталов по состоянию 31 декабря года, предшествующего дате определения уровня защиты информации, осуществляли брокерское обслуживание «более чем 100 000 лиц» на «более чем 200 000 лиц»,

б) в абзаце «дилеры, которые в течение последних трех кварталов по состоянию на 31 декабря года, предшествующего дате определения уровня защиты информации, заключали за свой счет на организованных торгах сделки купли-продажи ценных бумаг в объеме «более 200 000 миллионов рублей в квартал» на «более 500 миллиардов рублей в квартал»,

в) в абзаце «депозитарии (в том числе расчетные депозитарии), осуществившие в течение трех последних кварталов по состоянию на 31 декабря года, предшествующего дате определения уровня защиты информации, учет ценных бумаг на счетах, предусмотренных пунктом 2.1 и абзацами вторым - пятым пункта 2.2 Положения Банка России от 13 ноября 2015 года № 503-П "О порядке открытия и ведения депозитариями счетов депо и иных счетов", зарегистрированного Министерством юстиции Российской Федерации 16 декабря 2015 года № 40137, открытых в депозитарии, стоимость которых превышала «500 000 миллионов рублей» заменить на «500 миллиардов рублей»;

г) в абзаце «управляющие, которые в течение трех последних кварталов по состоянию на 31 декабря года, предшествующего дате определения уровня защиты информации, заключали сделки купли-продажи ценных бумаг при осуществлении деятельности по управлению ценными бумагами в объеме более «20 000 миллионов рублей» заменить на «200 миллиардов рублей» в квартал и (или) которые в течение трех последних кварталов по состоянию на 31 декабря года, предшествующего дате определения уровня защиты информации, осуществляли доверительное управление

ценными бумагами и денежными средствами более чем «100 000 лиц» заменить на «200 000 лиц», с которыми заключены договоры доверительного управления.».

2. Пункт 5.3 Положения относит все специализированные депозитарии к числу лиц, применяющих стандартный уровень защиты. По нашему мнению, это не вполне соответствует риск-ориентированному подходу, в соответствии с которым повышенные требования предъявляются к крупным и системно-значимым участникам рынка. Так в отношении негосударственных пенсионных фондов, активы которых учитываются в специализированных депозитариях, профессиональных участников рынка ценных бумаг, страховых организаций установлена граница, превышение которой переводит соответствующее лицо из категории минимального уровня защиты к стандартному. Предлагаем рассмотреть возможность установления указанной границы и для специализированных депозитариев, по аналогии с обычными депозитариями (с учетом предложения пункта 1 настоящего письма), – превышение стоимости учитываемых ценных бумаг 500 миллиардов рублей.

3. Изменение оценочного уровня доверия с ОУД 4 на ОУД 3 для некредитных финансовых организаций, применяющих стандартный уровень защиты.

Требования, установленные как ГОСТ 15408, так и «Профилем защиты прикладного программного обеспечения автоматизированных систем и приложений некредитных финансовых организаций» (далее по тексту – «Профиль защиты»), по проведению анализа уязвимостей в некредитных финансовых организациях» изначально основаны на подходах, применяемых к защите информации кредитными организациями, и не в полной мере учитывают:

1) специфику работы и существующие у некредитных финансовых организаций модели разработки программного обеспечения,

2) аспекты использования иностранных проприетарных систем, без которых невозможно осуществлять торги на иностранных площадках,

3) профиль риска некредитных финансовых организаций.

Все это, в практическом плане и при безальтернативном применении ГОСТ 15408, делает процесс анализа уязвимостей программного обеспечения профессиональными участниками рынка ценных бумаг или дорогим, или формальным, а значит не эффективным.

Указанный ГОСТ в отличие от более гибких стандартов PA-DSS, используемых

международными платежными системами, такими как SWIFT, Mastercard, VISA, не учитывает постоянные изменения в программном обеспечении, которые требуются для финансовых структур. Применение оценочного уровня доверия ОУД 4 по требованиям ГОСТа приведет к необходимости вкладывать значительные средства в защиту всех секторов информационных систем некредитных финансовых организаций, даже не нуждающихся в усиленном или стандартном уровне обеспечения защиты информации, что значительно увеличит операционные расходы.

В связи с вышеизложенным, просим рассмотреть возможность внесения изменений в пункт 9 Положения, предусматривающих, проведение анализа уязвимостей по требованиям к оценочному уровню доверия не ниже чем ОУД 4 для лиц с усиленным уровнем защиты, а для лиц со стандартным уровнем защиты - не ниже чем ОУД 3.

4. Применить для некредитных финансовых организаций подход к использованию электронной почты, аналогичный походу для кредитных организаций, который анонсирован в проекте 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», а именно:

а) пункт 10 дополнить абзацем следующего содержания:

«В целях обеспечения контроля целостности электронных сообщений и подтверждения составления электронного сообщения уполномоченным на это лицом некредитные финансовые организации должны обеспечивать использование усиленной электронной подписи или с соблюдением применяемой технологии обработки защищаемой информации простой электронной подписи, иных аналогов собственноручной подписи, кодов, паролей и других средств при подписании электронных сообщений.»,

б) подпункт 11.2 пункта 11 дополнить абзацем следующего содержания:

«При осуществлении некредитными финансовыми организациями подтверждения совершения финансовых операций с использованием электронной почты, в том числе при представлении клиентам справок (выписок) по финансовым операциям и счетам, некредитные финансовые организации должны реализовывать механизмы подтверждения принадлежности клиенту адреса электронной почты, на который некредитной финансовой организацией направляются уведомления о совершенных

финансовых операциях.».

5. Также, принимая во внимание необходимость проведения некредитными финансовыми организациями масштабных работ по внедрению требований Положения, просим продлить сроки вступления в силу пунктов 5 и 6, а также абзаца первого и второго пункта 8 на один год.

С уважением,

Президент  А.В. Тимофеев