Саморегулируемая организация
НАУФОР
Национальная ассоциация
участников фондового рынка

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

Исх. № 696 от 18 сентября 2018 года

Первому заместителю
Председателя Банка России

Скоробогатовой О.Н.

Уважаемая Ольга Николаевна!

В связи с опубликованием на сайте Банка России для публичного обсуждения проекта положения Банка России «Об установлении обязательных для некредитных финансовых организаций требований к обеспечению защиты информации при осуществлении деятельности в сфере финансовых рынков» (далее – Проект) просим рассмотреть предложения НАУФОР по корректировке указанного Проекта.

1. Пункт 4 Проекта, устанавливая обязанность применения финансовыми организациями национального стандарта Российской Федерации ГОСТ Р 57580.1-2017, определяет три уровня защиты информации и относит профессиональных участников рынка ценных бумаг и управляющие компании к стандартному уровню защиты (усиленный уровень реализуется системно значимыми инфраструктурными организациями финансового рынка, минимальный уровень – микрофинансовыми организациями, ломбардами и некоторыми другими финансовыми организациями).

Следует отметить, что Проект содержит абсолютно идентичные требования к организациям, реализующими как стандартный, так и усиленный уровни защиты информации (пункты 5 – 6, 11 – 14 и 16). Таким образом, профессиональные участники рынка ценных бумаг и управляющие компании фактически приравниваются к системно значимым инфраструктурными организациями финансового рынка (таким как, центральный контрагент, центральный депозитарий, репозитарий) с точки зрения обязанностей по защите информации и сопутствующих затрат. Считаем необходимым значительно снизить требования к организациям, реализующим стандартный уровень защиты, а также провести аудит с участием представителей финансовой индустрии используемых профессиональными участниками рынка ценных бумаг и управляющими компаниями средств обработки и хранения информации с целью выявления критически важных областей, нуждающихся в повышенной

защите по национальному стандарту, и иных некритических процессов, уровень защиты которых может определяться самими организациями.

2. Проект относит все категории профессиональных участников рынка ценных бумаг и управляющие компании к единой группе организаций, реализующих стандартный уровень защиты информации. Это вступает в противоречие с Концепцией пропорционального регулирования и риск-ориентированного надзора за некредитными финансовыми организациями, разработанной Банком России, предусматривающей дифференциацию требований к участникам финансового рынка в зависимости от принимаемой ими степени риска. Следует отметить, что указанная концепция получила одобрение финансовой индустрии и учитывается профильными департаментами Банка России при подготовке проектов нормативных актов. Так, например, проект указания «О внесении изменений в Положение Банка России от 27 июля 2015 года №481-П «О лицензионных требованиях и условиях осуществления профессиональной деятельности на рынке ценных бумаг, ограничениях на совмещение отдельных видов профессиональной деятельности на рынке ценных бумаг, а также о порядке и сроках представления в Банк России отчетов о прекращении обязательств, связанных с осуществлением профессиональной деятельности на рынке ценных бумаг, в случае аннулирования лицензии профессионального участника рынка ценных бумаг»» предусматривает разделение профессиональных участников рынка ценных бумаг на три категории:

1) малые,

2) средние,

3) крупные и системно-значимые.

Указанные категории учитывают объем рисков, возникающих в деятельности профессиональных участников на основе двух факторов – объема прав, набора операций, которые они осуществляют, и масштаба деятельности. В зависимости от отнесения к одной из вышеуказанных категорий дифференцируются и установленные к финансовым организациям требования.

Считаем необходимым доработать Проект, дифференцировав требования по защите безопасности, предъявляемые к различным категориям профессиональных участников рынка ценных бумаг и управляющих компаний.

3. Исходя из формулировки пункта 3 Проекта относительно информации, подлежащей защите, а также операций с данной информацией, следует, что защите подлежат все информационные системы финансовой организации, как предназначенные для использования ее клиентами, так и внутренние учетные системы (внутренний учет, депозитарный учет)

и системы, используемые самой финансовой организацией для осуществления финансовой операции (в том числе терминалы иностранных систем Bloomberg, Reuters и др.).

Проектом вводится большой набор требований как к методике разработки систем, так и к контрольным механизмам, которые должны быть заложены в системы. При этом предусмотрены два варианта обеспечения соответствия систем установленным требованиям: наличие сертификации программного обеспечения в системе сертификации ФСТЭК, либо проведение анализа 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. Для компаний, применяющих существенно модифицированные ИТ-решения единственным вариантом становится проверка на соответствие ОУД 4. При этом процедура проверки на соответствие ОУД 4 включает целый набор процедур, которые должны исполняться в процессе разработки. Применение данных требований к ранее разработанному программному обеспечению является крайне затруднительным.

Проектом также предусмотрены требования построения и организации двух раздельных контуров формирования и подтверждения операций клиентом, расширение перечня аналитик, фиксируемых по каждой операции в информационных системах, существенное расширение перечня операций подтверждаемых клиентом с использованием ключей, хранение информации обо всех регистрируемых событиях не менее пяти лет. Данные требования подразумевают кардинальный пересмотр технической архитектуры многих решений. При этом в отношении большей части действующих систем реализация данных требований становится невозможной ввиду того, что данная функциональность не предусматривалась на момент их проектирования.

Кроме того, исполнение установленного пунктом 10 Проекта требования обеспечить целостность данных возможно только при условии использования усиленной квалифицированной электронной подписи, что, учитывая широкое использование на рынке усиленной неквалифицированной электронной подписи и простой электронной подписи, особенно распространённой при использовании упрощенной идентификации клиентов через СМЭВ/ЕСИА, не позволит их использование в работе с клиентами, усложнит удаленную работу с клиентами и, как следствие, может привести к уменьшению доступности финансовых услуг населению.

Фактически, исполнение требований Проекта потребует от профессиональных участников рынка ценных бумаг и управляющих компаний изменения многих бизнес-процессов, пересмотра архитектуры и полной переработки большинства действующих информационных систем и сервисов с нуля. В свою очередь это повлечет необходимость

выделения существенных ресурсов на анализ, планирование, разработку новых систем, а также ресурсов для дублирования операций в действующих системах.

Реализация установленных требований к сроку вступления соответствующих требований в силу (2019, 2020 и 2021 годы) представляется невозможной. С учетом изложенного, считаем необходимым пересмотреть перечень реализуемых некредитными финансовыми организациями мер по защите информации, сохранив требования только в отношении критически важных областей, нуждающихся в повышенной защите, а в отношении менее важных процессов предоставить право финансовым организациям самим определять уровень защиты, а предоставить финансовым организациям срок не менее пяти лет для приведения своей деятельности в соответствие с новыми требованиями.

С уважением,

Президент А.В. Тимофеев

Исп. Зверев К.В.
Тел (495) 787-77-74 доб. 5160