Найти точку соприкосновения

В НАУФОР состоялся круглый стол, посвященный обсуждению нового регулирования защиты информации для некредитных финансовых организаций

Участники: Михаил Шабанов (член Совета директоров НАУФОР, председатель комитета по экономической и информационной безопасности НАУФОР), Сергей Демидов (Московская биржа), Владимир Дюков (УК «Альфа Капитал»); Дмитрий Кухтенков (АЛОР Групп).

Модератор — Михаил Шабанов.

Михаил Шабанов. Добрый день. Сегодня мы обсуждаем вопросы обеспечения информационной безопасности некредитных финансовых организаций. Обсуждение инициировано в свете публикации на сайте Банка России проекта Положения об установлении обязательных для некредитных финансовых организаций (далее в обсуждении допускается использовать аббревиатуру «НФО») требований к обеспечению защиты информации при осуществлении деятельности в сфере финансового рынка.

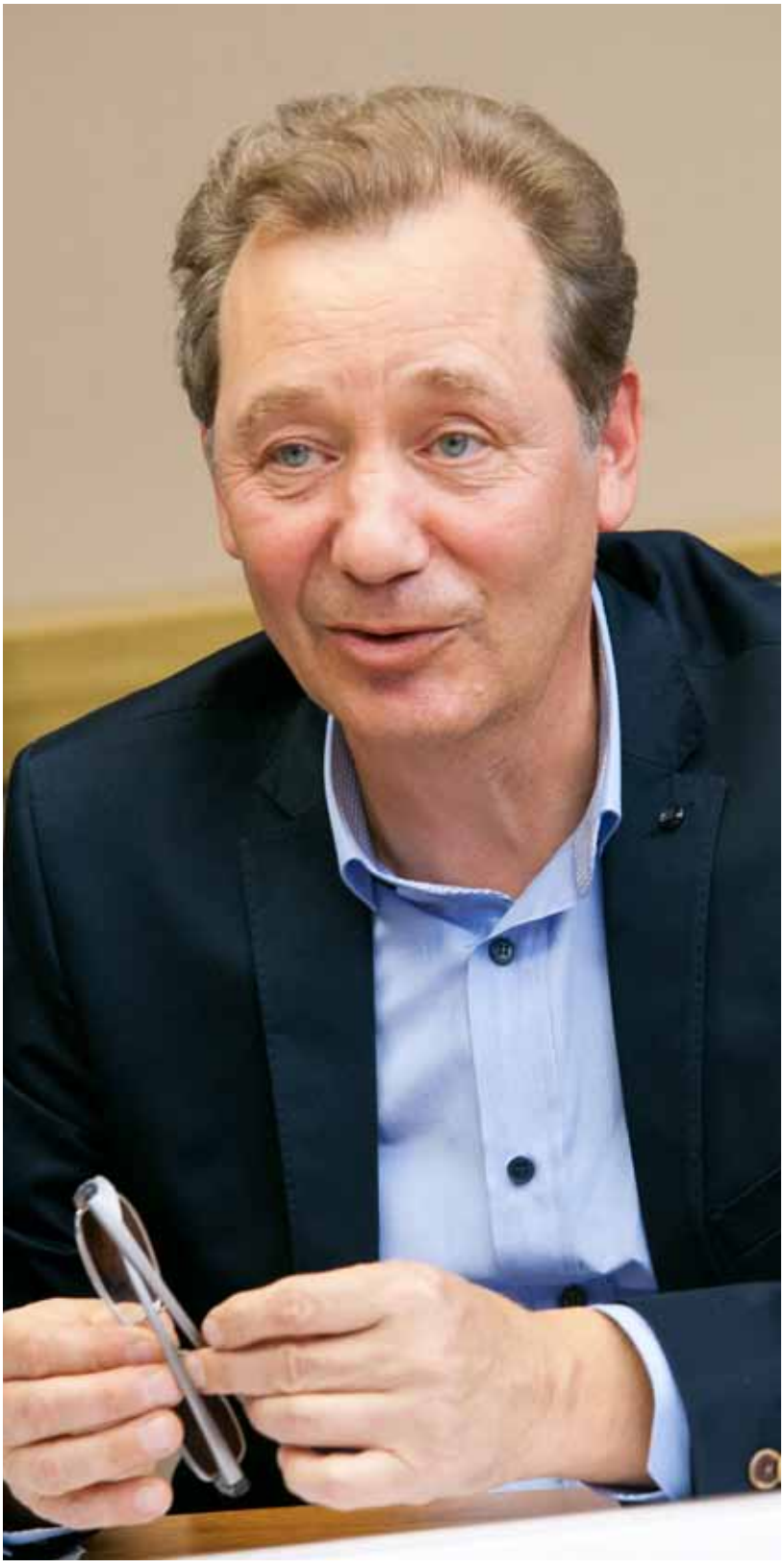
Мы детально обсудили проект в начале сентября на заседании комитета по экономической и информационной безопасности НАУФОР. И направили в Центральный банк соответствующие предложения о внесении изменений, необходимых для успешного внедрения представленных требований.

Я бы предложил начать наше обсуждение, передвигаясь от общего к частному. Вначале выяснить, насколько сегодня рынок ценных бумаг в целом готов соответствовать требованиям стандартов Российской Федерации, касающихся информационной безопасности. А затем обсудить степень готовности российских НФО к исполнению требований, представленных в проекте Положения Банка России.

В частности, существует опыт, полученный после того, как в мае 2018 года наш комитета был создан и начал обсуждать с компаниями-членами НАУФОР вопросы обеспечения экономической и информационной безопасности. Этот опыт свидетельствует о том, что существует очень большое разнообразие в вопросе, за кем и как закреплены соответствующие функции. Или, если выразиться иначе, налицо полное отсутствие единообразия в этом вопросе. Например, ответственными за обеспечение информационной безопасности в компаниях являются разные люди — это может быть генеральный директор,

директор, специалист по информационным технологиям (подразделение IT-службы), представитель службы безопасности, даже главный специалист административно-хозяйственного отдела. Это свидетельствует, что не всегда вопросами информационной безопасности занимается специалист в области именно информационной безопасности. Но это и понятно: если сравнивать, с одной стороны, небольшую брокерскую компанию, в которой работает 5 штатных сотрудников, а с другой стороны, крупные брокерские дома, системообразующие компании, где работают сотни человек, то очевидно, что их возможности существенно отличаются. И распределение обязанностей зависит от того, как именно понимает собственник и исполнительный орган компании задачи, связанные с обеспечением информационной безопасности.

Это первый и очень важный вопрос. Поэтому я бы хотел начать именно с этого. А далее плавно перейти к главному — обсуждению того, каким образом вот сейчас, в наше время, наши компании соответствуют критериям обеспечения информационной безопасности, которые уже введены соответствующими ГОСТами (здесь следует назвать тот же Р57580.1 – 2017). Обсудить, что мы уже можем предъявить в качестве готового обеспечения по вопросам информационной безопасности. А также, что необходимо сделать, чтобы соответствовать требованиям, изложенным в проекте Положения Банка России.



Опять же, ни для кого не секрет, что многие брокерские компании, депозитарии, управляющие компании входят в финансовые группы, в состав которых включен также банк. А банки уже много лет занимаются вопросами обеспечения требований стандартов информационной безопасности, утвержденных Банком России. Ясно, что в какие-то моменты в этих финансовых группах было обращено внимание и на брокерские компании; в связи с этим, скажем, соответствующие программно-аппаратные средства, возможно, уже были подготовлены и внедрены. Вот очень интересно понять, каким образом и в какой степени готовности сейчас обстоят дела по обеспечению информационной безопасности у профучастников российского рынка ценных бумаг?

Сергей, предлагаю начать вам, потому что Московская биржа озаботилась этим вопросом чуть раньше, чем появился проект положения.

Сергей Демидов. Московская биржа как организатор торгов сосредоточивает рынок вокруг себя. И, безусловно, все заботы этого рынка так или иначе влияют на наш бизнес. Соответственно, мы стараемся планомерно защищать интересы профессиональных участников рынка, поскольку зачастую глубже, чем регулятор, понимаем технические особенности работы этого рынка, специфику деятельности самих брокеров.

Действительно, мы начали заниматься вопросом информационной безопасности давно. В первую очередь здесь, наверное, важно понимать (это как ответ на первый ваш вопрос), зачем и как устроен этот рынок. Чтобы ответить на него, нужно понимать, от каких угроз в принципе защищаются сейчас участники финансового рынка. Эти угрозы различаются, они разные для банков и для брокеров. По нашим данным, брокерское сообщество сейчас страдает от угроз кибербезопасности

далеко не в той степени, нежели банки. По банкам собрана статистика, в ней фигурируют колоссальные цифры. В прошлом году регулятор даже назвал эти цифры публично — там фигурировали сотни миллионов рублей потерь от краж вследствие кибератак.

По брокерскому сообществу, безусловно, такой страшной картины нет. Если подобные кейсы и существуют, то они единичны.

Михаил Шабанов. Кейсы точно есть.

Сергей Демидов. Есть, но все-таки убытки по ним составляют далеко не сотни миллионов рублей. Поэтому и реакция на разные кейсы должна быть пропорциональной. Для того сегмента рынка, на котором актуальны угрозы многомиллионных потерь по линии кибербезопасности, нельзя принимать те же самые стандарты, которые принимаются для другого сегмента рынка, с другими рисками.

С другой стороны, обязательность защиты от этих рисков вводится сейчас и для небанковского сообщества, причем вводятся ровно те же самые ГОСТы. Банк России, так или иначе, пытался сделать стандарты обязательными через механизмы добровольного к ним присоединения и следования. Формат этих стандартов всегда был в некоторой степени рекомендательным. Поэтому, в принципе, предлагаемые стандарты — это сейчас общая беда всего финансового рынка.

Говорить о том, что банки в какой-то степени больше подготовлены к киберугрозам, — наверное, справедливо. Но вот с точки зрения регулирования проблема информационной защиты для банков и небанков абсолютно равнозначна. В то же время говорить о том, что ГОСТ, единый для всех типов участников рынка, непременно принесет благо всему сообществу, что станут защищены все его члены, — наверное, неправомерно. Наверное, суть состоит именно в том, каковы конкретные механизмы применения стандартов защиты; как именно разные категории участников рынка будут соблюдать эти стандарты; как регулятор будет контролировать их соблюдение. Вопрос состоит в том, что, в принципе, угрозы для разных типов участников — все-таки разные. А стандарты, получается, сейчас для всех одни и те же. Здесь, конечно, есть диссонанс.

Михаил Шабанов. Полностью соглашусь с этой постановкой вопроса!

Мы действительно ощущаем, что налицо определенные перекосы. В обсуждаемом проекте Положения, в том числе, не в полной мере отражены подходы, заявленные в концепции пропорционального регулирования и риск-ориентированного надзора за небанковскими финансовыми организациями, которые были ранее декларированы Банком России. По сути, проект относит все категории профессиональных участников рынка ценных бумаг к единой группе организаций, реализующих стандартный уровень защиты информации. То есть, разделение профессиональных участников рынка ценных бумаг на малые, средние, крупные или системообразующие компании — отсутствует.

Сергей Демидов. Когда этот стандарт еще обсуждался в рамках технического комитета, там присутствовало некое разделение на три категории. Однако вопросу категоризации не было уделено достаточного внимания. Никто в полной мере не олицетворял себя со второй категорией (категория «средняя компания»), многие думали: «ну, мы являемся небольшим брокером, наши объемы операций идут исключительно на собственную позицию, внешних клиентов мы не привлекаем, — стало быть, относимся к категории «мелкая компания».

Сейчас вышел проект регуляторного акта — и стал в некоторой степени сюрпризом, потому что он уравнял всех брокеров, всех их приписав ко второй категории, которая предполагает значительную регуляторную нагрузку.

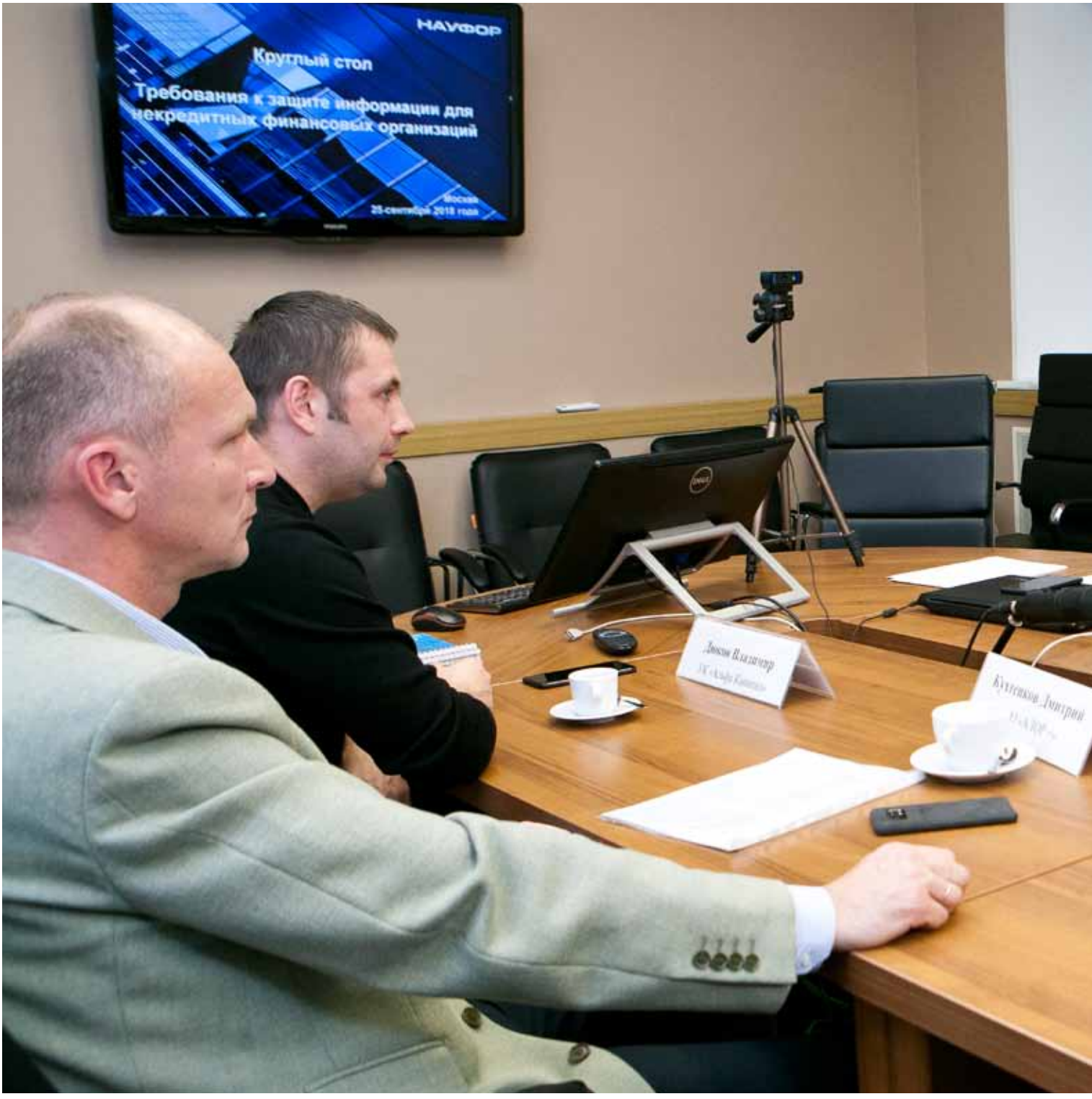
Мы же на бирже хорошо понимаем, что мелкий брокер — это компания с реально небольшим штатом, в которой нет существенных рисков. Мы это знаем, потому что периодически проводим аудит использования биржевой информации, потому что видим этот рынок. Мы видим брокерские компании, в штате которых нет выделенной штатной единицы на информационную безопасность. Но у таких компаний нет и угроз.

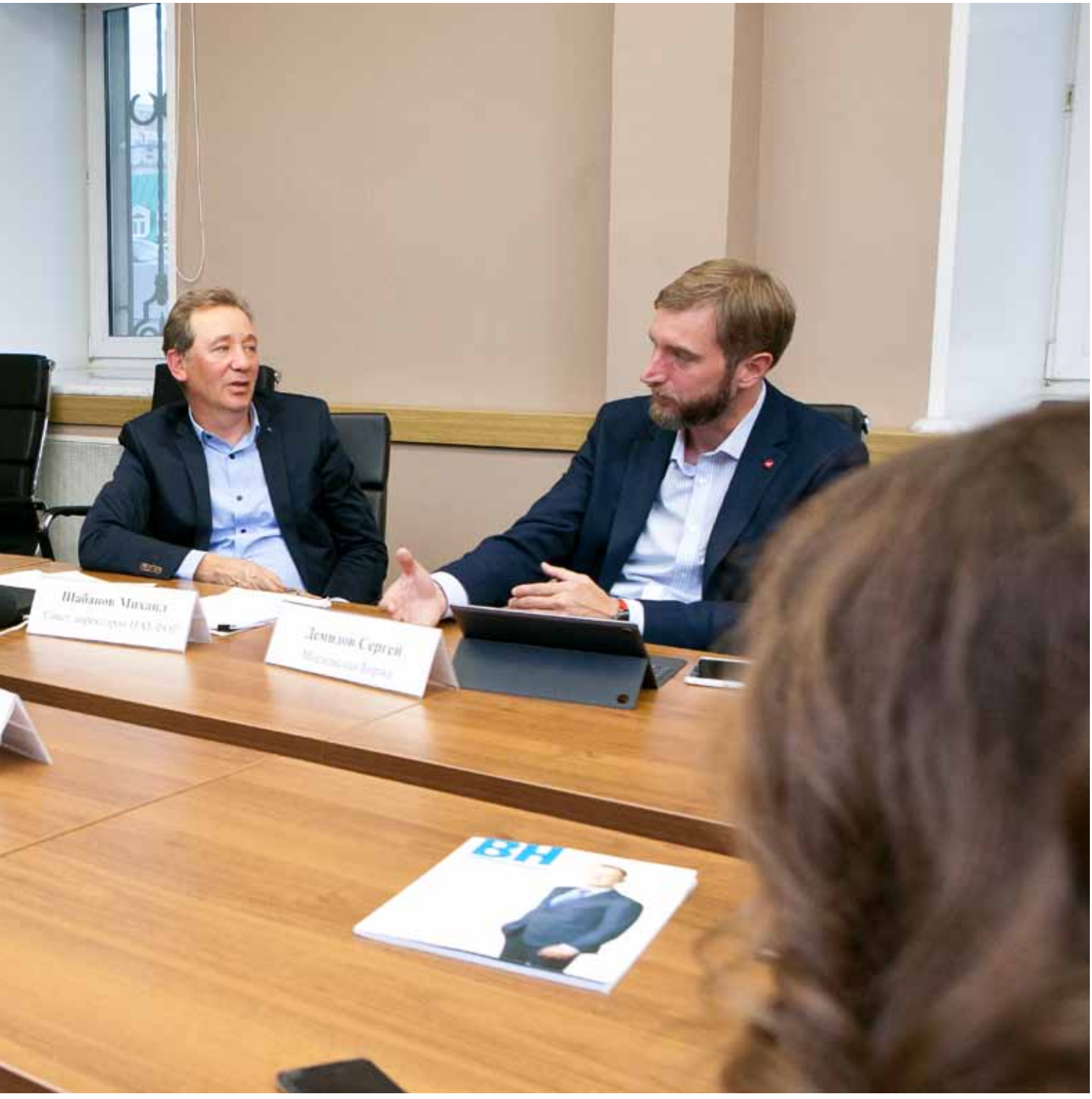
Михаил Шабанов. Их угрозы непропорциональны.

Сергей Демидов. За вывеской брокерской компании вполне может стоять просто человек, физическое лицо, который накопил, скажем, 15 млн рублей, зарегистрировал юрлицо, торгует на своей позиции, зарабатывает деньги и оплачивает услуги сотрудников, которые ему помогают торговать. Он не привлекает клиентов со стороны. Если он не будет инвестировать достаточные средства в защиту и его в результате атакуют хакеры, то они украдут лишь его собственные деньги. Это его собственный бизнес-риск. Он не хочет инвестировать миллионы рублей в информационную защиту просто потому, что понимает: столько он не заработает. Он готов рискнуть, но это его личный бизнес-риск, он не подставляет клиентов.

Михаил Шабанов. Коллеги, речь действительно идет именно об этом типе бизнеса: в такой брокерской компании и руководитель, и собственник — это одно лицо. Его клиентская база минимальна, поэтому потери на самом деле складываются только из тех потерь, которые он получит самостоятельно. Владимир, пожалуйста, присоединяйся к дискуссии.

Владимир Дюков. Я предлагаю сравнить степень вероятности угрозы атак на брокерские счета и на банковские счета.


НАУФОР
Круглый стол
Требования к защите информации для некредитных финансовых организаций


ВН

Если говорить в общем, то для того, чтобы заработать какие-то денежные средства, необходимо вначале вложить какие-то деньги. В том числе, это приходится делать и профессиональным жуликам, хакерам. Вопрос в том, что проще сделать. Либо (в случае с банком) создать какую-то вредоносную программу, внедриться в интернет-банк, поменять платежную форму и вывести денежные средства со счета клиента на подконтрольный счет злоумышленника. Либо (в случае брокера) осуществить значительно больше телодвижений: взять под контроль брокерский счет какого-то клиента, осуществить какие-то операции на бирже (продать бумаги либо выйти из инвестиционных продуктов), далее вывести эти денежные средства на банковский счет — и уже только с банковского счета перевести денежные средства на счет, подконтрольный злоумышленнику. Во втором случае — слишком много действий.

Мошенничать с управляющими компаниями еще сложнее по той простой причине, что денежные средства клиентов управляющей компании выводятся на их же счета в банке.

Сергей Демидов. В большинстве случаев та же самая схема действует даже с брокерами .

Несколько лет назад Московская биржа собрала рабочую группу крупных ритейловых брокеров, в рамках которой участники договорились о механизме противодействия кибератакам, еще до того, как это стало актуальной угрозой. Мы поняли, что когда биржа видит подозрительные операции, то это в основном операции в неликвидных инструментах, это попытки передачи активов с одного субброкерского счета физического лица на другой субброкерский счет. Мы поняли, что схему можно заметить на трех этапах: во-первых, биржа может заметить нетипичную операцию в неликвидных инструментах; во-вторых, брокер может заметить, с чьего счета деньги приходят; в-третьих, брокер может видеть, на чей счет эти деньги зачисляют.

Собственно говоря, на каждом этапе описанной цепочки платеж можно остановить. Поэтому в такой конфигурации схема действительно превращается в экономически не очень интересный для злоумышленника механизм, при этом он рискует быть пойманным. То есть при взаимодействии с брокером ему нужно проинвестировать ровно ту же сумму денег, что и для атаки на систему банк-клиент, но при этом его риск не получить деньги из-за того, что его поймают за руку, гораздо больше.

Владимир Дюков. Кроме того, злоумышленникам необходимы элементарные знания форматов торговли на бирже либо осуществления внебиржевых сделок, а это увеличивает группу участников противоправных действий

Сергей Демидов. Да, конечно.

Михаил Шабанов. Коллеги, давайте обсудим ситуацию, что может случиться, если все же в том или ином виде это Положение будет принято. Есть ли уже четкое понимание, насколько может пострадать клиентская база, особенно в крупных брокерских компаниях? Из-за чего это может случиться? Мы прекрасно понимаем, что в настоящее время очень активно используются различные виды дистанционного обслуживания клиентов, их идентификация происходит дистанционно. А здесь вводятся новые инструменты, которые до этого ни брокер, ни управляющие компании в свое программное обеспечение не закладывали.

Сергей Демидов. Мы сертифицируем все брокерские системы, которые к нам приходят. На безопасность на текущий момент мы их не проверяем, но анализируем соответствующие аспекты для того, чтобы просто накапливать статистику.

На самом деле основные системы, которые используются в ритейле сейчас, обладают усиленными методами аутентификации. Поэтому новшества, которые мы обсуждаем, не будут для рынка какой-то огромной неожиданностью.

Дополнительные меры для аутентификации — это, по большому счету, эсэмэска, которая приходит на телефон клиента, когда он пытается сделать платеж или зайти в систему. Могут быть использованы разные методы аутентификации: посредством sms-сообщения, через использование USB-флеш-накопителя, через отпечатки пальцев. То есть методы различные, но они есть. Мы знаем рынок и можем утверждать, что основные клиентские системы позволяют сейчас делать названные операции.

Михаил Шабанов. То есть здесь проблем вы не видите?

Сергей Демидов. Технологических проблем здесь нет.

Михаил Шабанов. Ну, технологических проблем действительно нет. Но если говорить о проблемах финансовых с точки зрения материальных затрат, то при введении новых правил потребуются дополнительные сотрудники и, как следствие, незапланированные денежные траты. Понятно, что для крупных брокерских домов это вопрос решаемый. А вот если это коснется средних и малых компаний, то у них могут возникнуть проблемы, вплоть до ухода с рынка.

Сергей Демидов. С точки зрения затрат мне кажется более серьезной в плане стоимости вся совокупность мер. Не конкретное влияние внедрения аутентификации, а именно совокупность предлагаемых мер. Ведь по большому счету новые требования регулятора

предполагают достаточно большой объем технических мер — от применения межсетевых экранов и заканчивая средствами контроля, мониторинга и сбора лотов. На мой взгляд, по совокупности они-то и несут в себе дополнительные затраты.

Найти на рынке компанию, которая на сто процентов соответствует сейчас всем предлагаемым требованиям, я думаю, будет тяжело. Кто-то придумал одни меры, кто-то другие, кто-то соответствует одним критериям, кто-то не соответствует другим критериям. Соответственно, сейчас проблема будет заключаться в том, что инвестировать в информационную безопасность придется всему рынку.

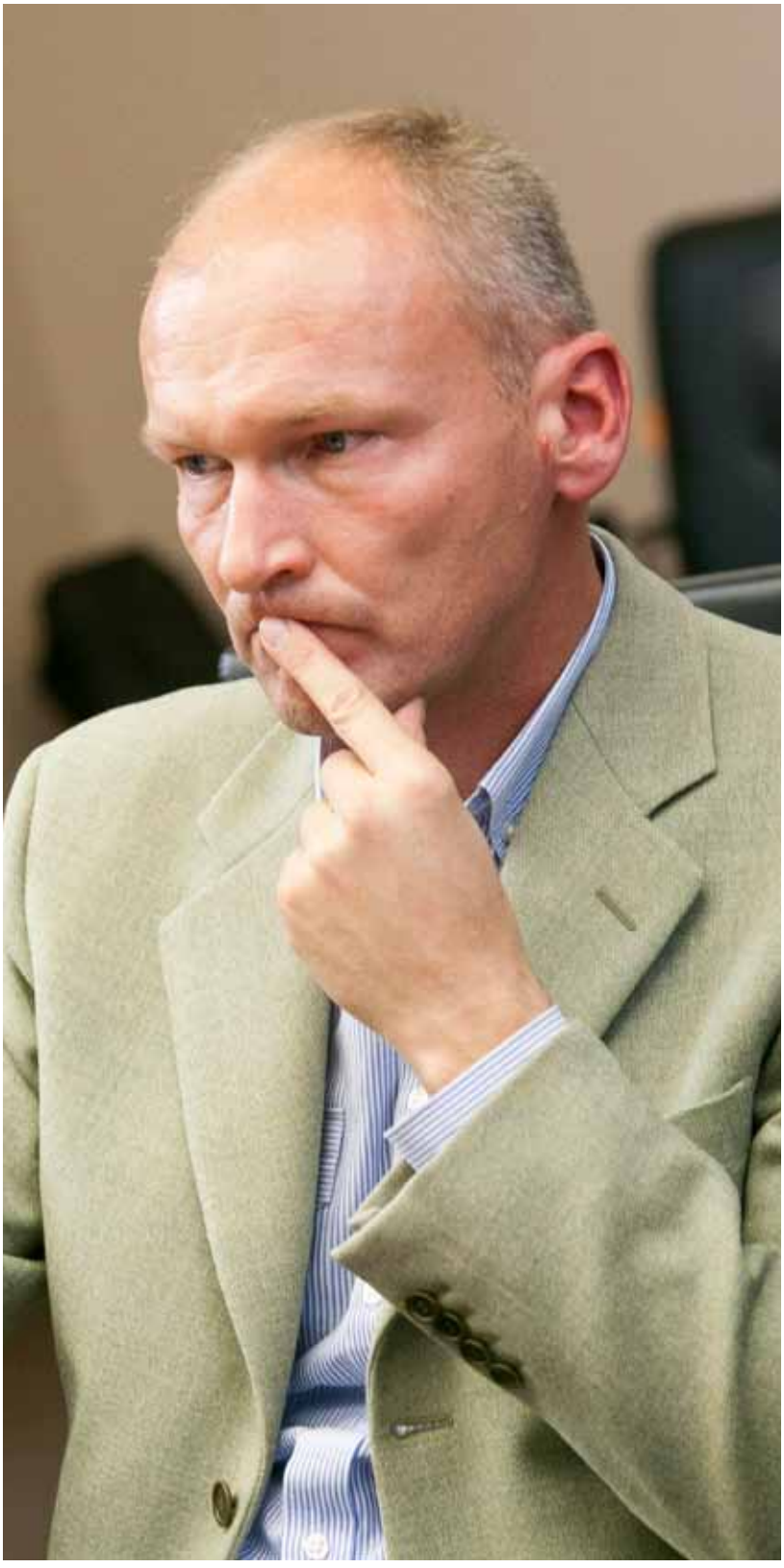
Владимир Дюков. Да, и притом инвестировать достаточно серьезные деньги.

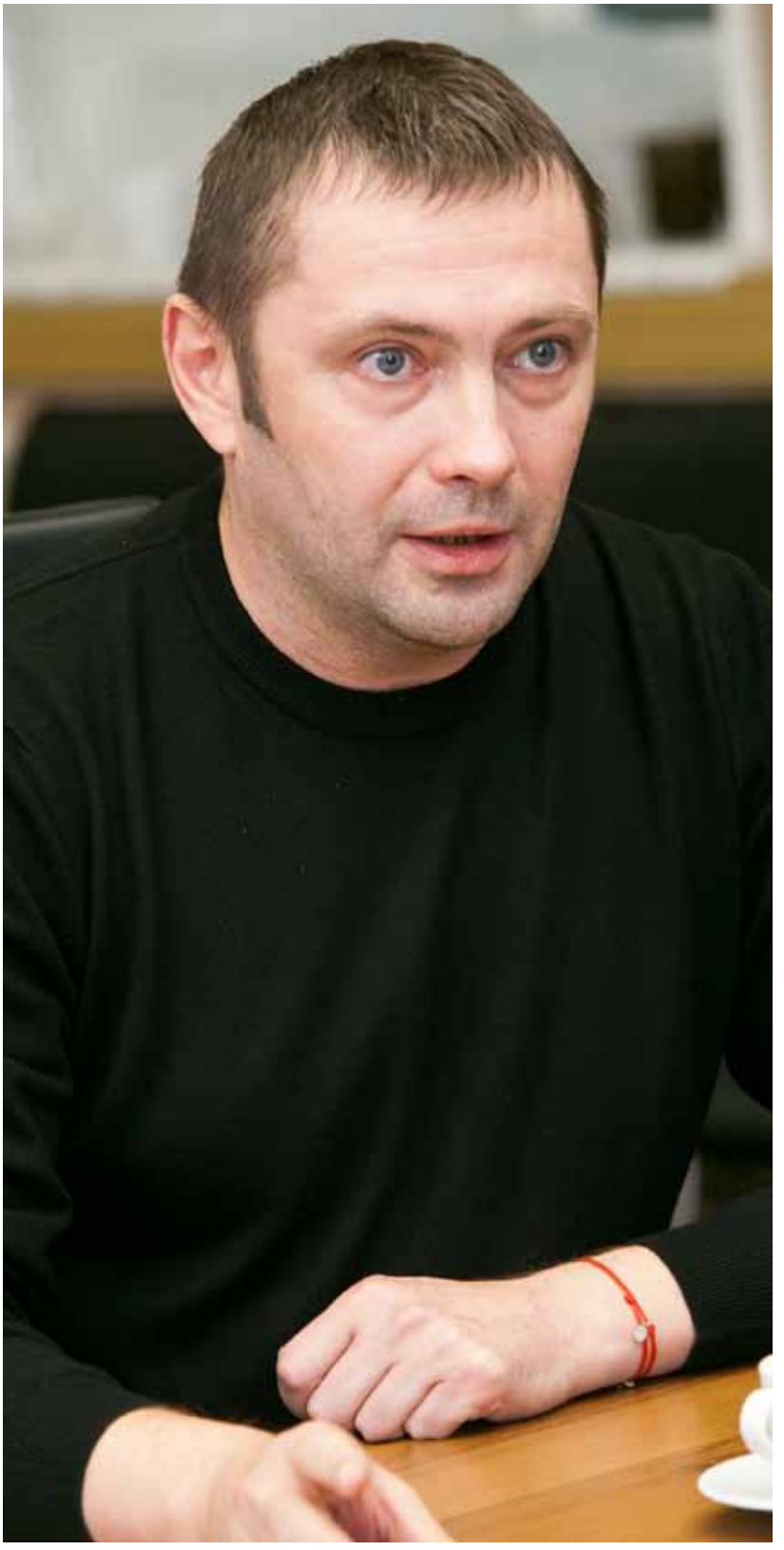
Сергей Демидов. Притом, что рост экономики сейчас не очень велик, а фондовый рынок во многом зависит, в том числе, именно от роста экономики страны. Получается, что рынок сейчас пытаются заставить внедрять дополнительные меры, которые стоят денег. А рынок при этом не сильно растет.

Вот это — одно из обстоятельств, которые вызывают наше беспокойство: то, что инвестировать придется всему рынку.

Владимир Дюков. Теперь, касательно сроков. Банки шли к внедрению ГОСТа по защите информации, по-моему, с 1998 года, если мне память не изменяет. А профучастникам предлагается пройти этот же путь за три года.

Сергей Демидов. Ну, банки к этому шли в рамках Стандарта Банка России по обеспечению информационной безопасности организаций банковской системы Российской Федерации. Это преимущественно системный стандарт, давайте здесь все-таки расставлять точки над «I». Потому что СТО БР — это, в значительной степени, копия международного стандарта ISO





27000 [ISO — серия международных стандартов, включающая стандарты по информационной безопасности]. А в стандарте, который мы сейчас обсуждаем, говорится, главным образом, про систему: как нужно построить информационную безопасность, как система информационной безопасности должна быть отделена от других систем. А ГОСТ получился чисто технический: грубо говоря, там прописано, какого типа межсетевые экраны следует использовать в части защиты разных сегментов сети. Вот это страшно.

Михаил Шабанов. В целом я соглашусь с Владимиром, что все-таки у банков срок внедрения стандарта был существенно растянут. Профучастникам предлагается уложиться всего за три года. За три года мы должны перейти на новый уровень и соответствовать всем требованиям ГОСТов по обеспечению информационной безопасности. А если соответствия нет, то значит, и никакую профессиональную деятельность на рынке ценных бумаг дальше уже вести будет невозможно.

Владимир Дюков. Открытым остается вопрос, связанный непосредственно с сертификацией программного обеспечения. Кто готов передать ядро своей программы? Программное обеспечение может быть разработано не российским вендором, и очевидно, что не все западные вендоры будут готовы передавать ядро на исследование.

Сергей Демидов. Я больше скажу. Проблема состоит еще и в том, что испытательных лабораторий сейчас существует всего десять на всю страну, и срок сертификации там — порядка шести месяцев. Таким образом, процедура постановки в очередь, процедура проведения сертификации — все это будет влиять на безопасность отрицательно, потому что те уязвимости, которые существуют внутри программного обеспечения...

Михаил Шабанов. …будут вскрыты.
Сергей Демидов. Не в этом даже дело. На самом деле уязвимости программных продуктов регулярно выявляются и сейчас. Вот буквально вчера компания Microsoft выпустила перечень ежемесячных обновлений, который содержит исправления критических уязвимостей ее программных продуктов. Это достаточно серьезный документ. И такие уязвимости (разной степени критичности) обнаруживаются в разных продуктах, в принципе, каждую неделю. Но проблема в том, что если компания отдала свое программное обеспечение на сертификацию, то она уже не может заменить этот продукт. Придется дождаться сертификации, подавать на ресертификацию и снова ждать шесть месяцев, чтобы новые продукты были сертифицированы. В течение этого срока брокер не может исправлять программный продукт, потому что он тут же превратится в несертифицированный.
Михаил Шабанов. Согласен. Кроме того, у небольших брокеров есть еще одна очень большая проблема — они используют инхаусное программное обеспечение, которое было разработано 10, 15, 20 лет назад. Исходных кодов порой не найти. И проблема связана с тем, что уже и переписать это ПО невозможно, и перейти на новый продукт также затруднительно из-за системных надстроек. А если осуществить переход на другую платформу, то это порой может вылиться в очень серьезные затраты.
Владимир Дюков. Менять программу — это частично парализовать производственную деятельность.
Михаил Шабанов. Да. И мы прекрасно понимаем, что в каждой брокерской компании необходимо обеспечить программно-аппаратными средствами бэк-офис, депозитарий, а также фронт-офис. Кроме того, есть множество иных программных продуктов, используемых в работе клиентских подразделений, бухгалтерии, маркетинга. И еще есть торговые терминалы. Я даже не знаю, озаботились ли там вопросами сертификации своих программных продуктов или нет.

А ведь есть еще западные торговые платформы.
Владимир Дюков. В любом случае, любая брокерская или управляющая компания всегда заинтересована в собственной информационной безопасности. И осуществляет определенные меры по защите своего программного обеспечения, своей клиентской базы и клиентских средств.

Если сейчас обязать все компании выполнять жесткие стандарты на ограниченном периоде времени, то вполне возможно, что индустрия небольших брокеров и маленьких управляющих компаний может быть частично парализована. Либо они будут вынуждены вообще уйти с рынка.
Сергей Демидов. Здесь вопрос опять же таки того, как компании в конечном итоге будут эти нормы примерять на себя. Мы прекрасно знаем, как соответствующая норма, предписывающая сертификацию по недекларированной возможности, работает в банковской среде. Там, по большому счету, это все вылилось в то, что все банки несут на сертификацию только определенную часть программного кода, но не код всей своей АБС (автоматизированная банковская система). Потому что это нереалистичный сценарий — проверить весь код автоматизированной системы, который защищен авторскими правами, причем не самого банка, а компании-разработчика. В том числе, из-за того сценария, о котором я уже сказал: что за время, когда уязвимости будут проверяться, их нельзя будет исправить. И это тоже страшно, на самом деле.

Ни один бизнес не хочет, чтобы механизм сертификации защиты от риска, наоборот, подставлял его под риск.

Соответственно, скорее всего, большинство игроков будет определять какой-нибудь один модуль. Скорее всего, это может быть модуль интеграции с Московской биржей. Мы будем добровольно сдавать его на подобный анализ. И в нем, вне сомнения, будут каждый раз успешно констатировать отсутствие недекларированных возможностей, — потому что в этом конкретном модуле всего 100 строк кода. А дальше мы будем сертифицировать каждую его версию. Но это же, наверное, не то, чего хотел регулятор. Мне кажется, что в интересах и регулятора, и рынка найти точку соприкосновения, в которой комфорт был бы обеспечен обеим сторонам. Чтобы и регулятор понимал, что рынок либо защищен, либо угрозы для него несущественны. И чтобы рынок тоже понимал: регулятор пытается защитить его и слышит голос рынка. К сожалению, сейчас этот диалог сильно разорван.

Михаил Шабанов. Таким образом, один из важных выводов нашего круглого стола таков. Мы подготовим соответствующее обращение к Банку России. В этом обращении мы заявим о нашей готовности на любой площадке — на площадке НАУФОР или площадке Банка России — организовать общение специалистов по информационной безопасности небанковских финансовых организаций. В виде рабочей группы или ином виде, это неважно. Но нам важно донести до надзорного органа нашу обеспокоенность той ситуацией, которая сложилась сегодня. Потому что, если Московская биржа приступила к обсуждению ГОСТов информационной безопасности еще в 2016 – 2017 годах на Техническом комитете, то для нас, брокерских и управляющих компаний, публикация этого проекта положения была, в определенной степени, неожиданностью. Появился проект. При этом нам дали всего неделю на то, чтобы мы этот документ изучили и представили свои предложения в Банк России. Всего неделю. Ну, этого мало, согласитесь.

Абсолютно необходимо провести серьезное обсуждение проекта Положения с участниками финансового рынка и представителями надзорных органов. Для того чтобы найти необходимые компромиссы, прийти к пониманию достаточности мер и средств для обеспечения информационной безопасности в НФО в соответствии с концепцией пропорционального регулирования, а также по вопросам сертификации и лицензирования программно-аппаратных средств.

Дмитрий Кухтенков. При подготовке ГОСТа, который действует для банков, анализировались те риски, которые свойственны именно банковской сфере. При подготовке же ГОСТа для брокеров и других некредитных финансовых организаций, похоже, такой подход просто не применялся. То есть, не анализировались те риски, те угрозы, которые существенны именно для НФО. Поэтому и получилось так, что документ полностью скопирован, на мой взгляд, с банковского ГОСТа. И, по сути, для участников фондового рынка, для их безопасности ничего не дает.

У брокеров нет движения денег в том формате, в каком это движение реализуется в банках. Соответственно, из брокера невозможно вывести деньги таким же образом [как из банка]. В то же время банковский ГОСТ, в первую очередь, предназначен для защиты от кражи денег в чистом виде. Поэтому в подготовке ГОСТа для профучастников фондового рынка необходимо было исходить именно из тех угроз, тех рисков, которые свойственны именно брокерскому бизнесу.

Сергей Демидов. Я вам даже больше скажу — это просто один и тот же ГОСТ, он всего лишь вводится разными нормативными актами. Но сам по себе ГОСТ для банков и для брокеров — абсолютно один и тот же.

В защиту регулятора скажу следующее. Ведь как работает механизм согласования таких инструментов, как ГОСТ? Есть технический комитет Банка России №122 «Стандарты финансовых операций», куда ЦБ РФ приглашает много экспертов. В рамках комитета работает подгруппа по техническим стандартам, подгруппа по стандартам информационной безопасности. Там присутствуют представители брокеров, представители ломбардов, банков, — то есть, в комитете достаточно представителей всех рыночных специальностей. Далее, там присутствуют производители программных средств, представители Федеральной службы по техническому и экспортному контролю (ФСТЭК), представители других федеральных органов исполнительной власти. Обсуждение новых стандартов в рамках работы комитета было достаточно бурным. К моменту голосования «против» этого ГОСТа проголосовало трое участников, одним из них был я, еще одним — представитель ФСТЭК. Все остальные либо воздержались, либо проголосовали «за».

У Московской биржи есть комитет по информационно-технологическим сервисам, который объединяет пользователей, представителей ИТ-подразделений брокерских компаний. Я этим людям объяснил суть разрабатываемого стандарта, объяснил, в чем заключаются риски, упомянул, что [при вступлении стандарта в силу] будут нужны достаточно большие инвестиции. Получил небольшое количество комментариев, с которыми смог вернуться на технический комитет Банка России, где их озвучил, — но я был в меньшинстве. Нас там не услышали. Если бы брокера участвовали в работе над стандартами информационной безопасности, то это было бы гораздо эффективнее. Таких комитетов в стране, на самом деле, несколько. Есть технический комитет ФСТЭК, там тоже эти вопросы обсуждаются. Но если брокера на такие обсуждения не ходят, — извините, тогда они не будут услышаны.

Сейчас, когда ГОСТ вышел уже в виде нормативного акта, мы еще раз вышли на перечисленные комитеты. Призвали брокеров давать комментарии, в том числе, о том, что ГОСТ в некоторой степени не отвечает требованиям пропорциональности регулирования, которые были заявлены Банком России. Надо было эти комментарии направлять на сайт регулятора. Насколько мне известно, комментарии там все-таки появились, но их было не очень много. А когда регулятор не видит сильного сопротивления нормативному акту (который фактически сейчас пошел уже дальше, на утверждение других ведомств), — то, скорее всего, этот акт будет утвержден. Мы бежим за поездом, который уже тронулся. Надо, мне кажется, более оперативно реагировать на инициативы регулятора на ранних стадиях, а не когда законопроект уже находится фактически на финальной стадии согласования.

Михаил Шабанов. Замечание, по моему мнению, справедливое. Есть, однако, нюансы. Мы сегодня говорили о тех брокерских и управляющих компаниях, объемы операционной деятельности которых незначительны и численность работающих там сотрудников минимальна. Но при этом им требуется (скажем, с точки зрения своей профессиональной деятельности) охватить невероятный объем операций, в том числе, связанных с передачей информации.

Сергей Демидов. Мы общались с Банком России уже постфактум, когда

проект был выложен на портале регулятора. И обсуждали, каким образом, собственно говоря, мелкие участники смогут реагировать на эту норму. На самом деле, были предусмотрены определенные нюансы внутри самого ГОСТа, которые позволяют участникам, если конкретные риски для них не применимы, отдельные нормы к себе не применять. Это положения 6.2 и 6.3 самого ГОСТа, которые предусматривают для брокера возможность в своей модели угроз указать, что конкретная угроза к его работе не применима. Это дает возможность не следовать следующим пунктам документа, фактически не исполнять следующие пункты. Соответственно, небольшие участники торгов, небольшие брокерские фирмы смогут проанализировать свою инфраструктуру в этом ключе. Либо сделать это самостоятельно, либо нанять фирму, которая поможет оценить отдельные угрозы, составить аккуратное описание, почему брокерская компания не считает эти угрозы применимыми для себя. И далее выполнять только те требования, которые для них актуальны.

Михаил Шабанов. Это сложный момент.

Сергей Демидов. Это сложный момент, но он важен с одной-единственной точки зрения: как эта процедура будет проверяться.

Михаил Шабанов. Конечно. Надзорный орган, который не посчитает возможным применить эти исключения, скажет: «Коллеги, существует единый финансовый рынок и единые требования к финансовым операциям на нем. Требования по обеспечению информационной безопасности должны быть одинаковыми: что для маленького брокера, что для компании «Сбербанк – Управление активами» или «БКС».

Сергей Демидов. Вот где наш «поезд» еще не ушел — так это в определении формата проверок, определении порядка, в котором брокеров будут проверять. Этого стандарта еще нет. Его еще нет в нормативном акте. А надо понимать, что Банк России — очень разнородная внутри себя организация, у нее много разных подразделений. Подразделения, которые выпускали ГОСТ, — это не совсем те подразделения, которые проверяют соответствие стандарту. И вот того стандарта, по которому нас будут проверять, пока нет. И если мы сейчас, на данном этапе, убедим «второе крыло» регулятора в том, что проверять нужно, именно исходя из модели конкретных рисков, из модели конкретных угроз, — то, в принципе, масштаб бедствия может оказаться не таким большим.

Мы сейчас призываем постараться развернуть поезд в обратную сторону: не утверждать ГОСТ, ввести пропорциональное регулирование. Но план «Б» в этой ситуации состоит в том, что если разворот поезда не удастся, то следует хотя бы сейчас отработать ту норму, которая изначально была заложена в ГОСТ, а именно 6.2 и 6.3. Эта норма позволяет не реализовывать меры, которые не являются необходимыми для конкретной модели защиты от угроз конкретной организации.

Михаил Шабанов. Разумное предложение. Я думаю, что мы будем учитывать все сказанное здесь. И постараемся наладить соответствующую работу с Банком России.

Владимир Дюков. В любом случае необходимо создать, прописать соответствующую модель угроз, — может быть, универсальную. А далее уже предложить профучастникам отметить профильные для них угрозы, в формате самооценки.

Михаил Шабанов. Коллеги, думаю, что на уровне Комитета по экономической и информационной безопасности НАУФОР мы постараемся разработать некие шаблоны стандартных документов, связанных с введением норм представленного Банком России положения. Но это работу необходимо проводить совместно со специалистами Банка России.

Владимир Дюков. Крупный брокер либо управляющая компания может себе позволить, в том числе, разработать по данному шаблону свою карту угроз. Но небольшие компании такими возможностями не обладают. Например, управляющие компании с парой фондов в управлении не обладают ресурсом содержать штат профильных специалистов безопасности. Там таких специалистов просто нет.

Дмитрий Кухтенков. Им придется нанимать стороннюю организацию для того, чтобы она провела эту работу. И это, конечно, дополнительные затраты.

Сергей Демидов. Здесь можно попробовать выступить от лица всего профессионального сообщества. Я пока, наверное, не могу говорить, сможет ли Московская биржа разработать какие-то шаблоны. Но, если масштаб бедствия действительно будет большим, думаю, что мы можем над этим подумать и оказать методологическую помощь мелким организациям. Сделать какие-то разъяснения, согласовать подходы с Банком России, помочь защитить именно вот этих мелких брокеров. Чтобы нововведения не оказали существенного влияния на их бизнес.

Дмитрий Кухтенков. Согласен.

Михаил Шабанов. Коллеги, какие еще важные вопросы мы не затронули?

Владимир Дюков. Вопрос сроков вступления данного положения в силу.

Михаил Шабанов. В письме НАУФОР в Центральный банк мы попросили пересмотреть эти сроки именно для того, чтобы фигурировали не три года, которые отведены в документе в отношении ряда положений. Опять же, если работа над Положением будет

продолжена, то я надеюсь, что наше мнение будет услышано и нам удастся повлиять на введение Положения в приемлемые сроки.

Сергей Демидов. Но здесь опять же нужно учитывать и позицию ФСТЭК в части аккредитованных центров. Потому что, если центров по-прежнему будет всего десять и цикл их работы останется прежним, полугодовым, — то это может нарушить развитие рынка.

Владимир Дюков. Вариантов немного. Либо будут увеличивать количество центров...

Сергей Демидов. …либо ускорять темп их работы.

Михаил Шабанов. Как именно следует сертифицировать программное обеспечение?

Как я понимаю, существуют определенные жесткие требования к этой процедуре со стороны Федеральной службы по техническому и экспортному контролю?

Сергей Демидов. Нет, это просто механизм. Просто в этом же ГОСТе предписано, что процедуру анализа декларированных возможностей можно делать через центры, аккредитованные ФСТЭК. Наш поиск показал, что существует 10 аккредитованных центров, а реально действующих — еще меньше. Соответственно нужно, конечно, у Федеральной службы по контролю получить разъяснения на тему того, будет ли создан этот рынок, появятся ли аккредитованные центры, долгим ли будет ожидание появления этих центров.

Потому что сама по себе эта работа очень специфичная, существуют достаточно сложные коды. На площадке Московской биржи, например, существует очень много торговых систем, алгороботов, которые вообще работают чуть ли не на видеокартах. Соответственно, каким образом работники аналитического центра будут проверять такие алгоритмы?

Московская биржа обязана следить преимущественно за тем, чтобы алгоритмы не вредили другим участникам торгов и средствам проведения торгов. Внутрь алгоритмов мы не заглядываем. А тут получается, что алгоритм – это часть программы.

Михаил Шабанов. Но, как я понимаю, Московская биржа алгоритмы все-таки проверяет?

Сергей Демидов. Мы поверяем результат работы, а не алгоритм. Алгоритм мы не аудируем. На Бирже производится 100-процентная предпроверка рисков; соответственно, от работы алгоритма Московская биржа защищена тем, что активы, превышающие его позицию, игрок в такой ситуации потерять не сможет.

Соответственно, в итоге риск не очень велик.

Михаил Шабанов. Войти на рынок аккредитованных сертифицированных центров очень тяжело. Он очень зарегулирован. Я не знаю, какова ситуация в Москве, но в Санкт-Петербурге было несколько скандалов по этому поводу, когда Федеральная комиссия по контролю сертифицировал эти компании, а потом они оказывались несостоятельными с точки зрения проведения различных анализов и вынесения заключений по сертификации в отношении других компаний.

Владимир Дюков. Но, в конечном итоге, пострадавшими окажутся профучастники.

Михаил Шабанов. Да, к сожалению, тут, как всегда, все обычно складывается достаточно традиционно: страдают те компании, которые обязаны исполнять требования нормативных актов, издаваемых надзорными органами.

Владимир Дюков. Регулятор, как можно уверенно предположить, не будет спрашивать о причинах неисполнения своих указаний и постановлений.

Михаил Шабанов. Конечно, причины никого волновать не будут. Брокерская компания лицензию получила? В ситуации, когда лицензия имеется, вы должны исполнять соответствующие лицензионные требования. А в лицензионные требования будут включаться элементы, касающиеся обеспечения информационной безопасности.

На этом я завершаю наш «круглый стол». Думаю, мы достаточно детально обсудили вопросы обеспечения информационной безопасности в некредитных финансовых организациях. И сможем наладить рабочий диалог с регулятором для успешного внедрения требований, изложенных в проекте Положения Банка России.

Коллеги, большое спасибо за участие.