Кибербезопасно

25 апреля НАУФОР провела круглый стол, посвященный вопросам кибербезопасности в некредитных финансовых организациях и регуляторным вызовам, связанным с новыми требованиями в области информбезопасности

Фотографии **Павел Перов**

Участники: Сергей Демидов (заместитель Председателя правления по информационной безопасности, Московская Биржа); Андрей Ковешников (начальник отдела информационных технологий АО «УК «Регионфинансресурс»); Андрей Киселев (директор по информационной безопасности АО «НРК - Р.О.С.Т.».); Антон Чернодед (Департамент информационной безопасности Банка России); Георгий Ерохин (Департамент информационной безопасности Банка России), члены комитета НАУФОР по экономической и информационной безопасности.

Модератор — Михаил Шабанов, председатель комитета НАУФОР по информационной и экономической безопасности.

Михаил Шабанов. Коллеги, здравствуйте!

Тема нашего круглого стола навеяна итогами Уральского форума «Кибербезопасность в финансах 2023». Наша сессия, которая впервые проходила на Уральском форуме и была посвящена некредитным финансовым организациям, выявила достаточно много вопросов как со стороны слушателей, так и среди участников дискуссии.

Сегодня на круглом столе предлагаю обсудить следующие темы. Во-первых, «Глобальные тренды кибербезопасности и их влияние на деятельность некредитных финансовых организаций». Во-вторых, «Что делать или с какими сложностями столкнулись некредитные финансовые организации при реализации требований Положения Банка России 757-П и 779-П, а также иных нормативных документов». Третья тема: «Как правильно совместить требования по обе-

спечению информационной безопасности и риск-менеджмент по операционной надежности при построении комплексной системы обеспечения информационной безопасности в НФО». Хотелось бы коснуться, если у нас хватит времени, темы реализации Банком России надзора в области обеспечения информационной безопасности в некредитных финансовых организациях, с учетом того письма, которое касалось нашей индустрии, о неприменении мер. Если я правильно понимаю, то с 1 апреля уже идут проверки и могут последовать наказания. Но здесь я бы хотел обратиться к представителям Департамента информационной безопасности Банка России с просьбой дать, может быть, пару комментариев.

Антон Чернодед. Все верно, с 1 апреля прекратил свое действие мораторий на проверочные мероприятия и применение мер воздействия. Соответственно, на текущий момент планово ведутся контактные проверки некредитных финансовых организаций. В случае если выявляются нарушения, которые ведут к системным либо существенным рискам, то к организации применяются различные меры воздействия.

Но проверяющий обращает внимание на состав нарушения. Были ли у организации возможности выполнить установленные требования в связи с последними событиями, связанными с импортозамещением, операционной надежностью и так далее. То есть если, по мнению проверяющего, организация вполне могла выполнить установленное требование, не было никаких объективных факторов, которые препятствовали выполнению, то, соответственно, применяются меры воздействия, формируется план мероприятий по устранению и ведется дистанционный надзор по данному направлению.

Михаил Шабанов. Стандартная процедура проверки не поменялась? То есть, после выявления нарушения регулятор дает свои рекомендации, дает какой-

то срок на исправление нарушений. Наказание (или иная мера воздействия) осуществляется, если исправления не последовали, верно?

Антон Чернодед. Само предписание тоже является мерой воздействия. Есть достаточно большой диапазон мер воздействия — от предписания, штрафа до более тяжелых. Это зависит от тяжести нарушения требования.

Михаил Шабанов. Хорошо, спасибо. Коллеги, итак, приступаем тогда к обсуждению нашей первой темы.

Глобальные тренды кибербезопасности и их влияние на деятельность некредитных финансовых организаций

Все ли киберриски отражены в проекте «Основных направлений развития информационной безопасности кредитно-финансовой сферы на период 2023-2025 годов»? Я знаю, что соответствующий проект документа обсуждался, мы принимали в нем достаточно активное участие, но тогда он, правда, был прописан на период 2022-2024 годов. Понимаю, что он изменился, какие-то наши пожелания были в нем, надеюсь, учтены. Будет ли проходить повторное обсуждение или документ будет приниматься сразу?

Антон Чернодед. На текущий момент проект проходит процедуру согласования и утверждения в Банке России. Планируется в ближайшее время эту процедуру финализировать. И как только он будет утвержден, то сразу будет доступен.

Говорить о том, что проект учитывает все имеющиеся риски, не совсем корректно. Это именно основные направления развития на ближайшие три года.

Михаил Шабанов. То есть повторного обсуждения не предполагается?

Антон Чернодед. Да, повторное обсуждение не планируется.

Михаил Шабанов. Я понял. Вопрос, наверное, звучит не совсем корректно, но какие-то основные моменты, которые связаны именно с некредитными финансовыми организациями, наше профсообщество волнуют и беспокоят. Мы на них неоднократно обращали внимание, в том числе, и Банка России, и Департамента информационной безопасности. Такая переписка ведется, по-моему, с 2019 года.

Как формируется безопасная киберсреда в кредитно-финансовой сфере, и что необходимо предпринять надзорным органам и НФО для обеспечения информационной безопасности в ближайшее время?

Представитель комитета. Не стоит ли вернуться к теме формирования некой постоянно действующей рабочей группы? Для того, чтобы участники рынка могли скоординировать и наши инициативы, которые могут возникать, исходя из событий, которые мы видим «на земле». И, возможно, на ранних этапах получать от регулятора какую-то информацию, для того, чтобы какие-то новшества можно было проверить в виде «пилота», скажем так, и получить обратную связь от тех экспертов, которые обладают реальным опытом реальной работы в тех или иных компаниях-профучастниках.

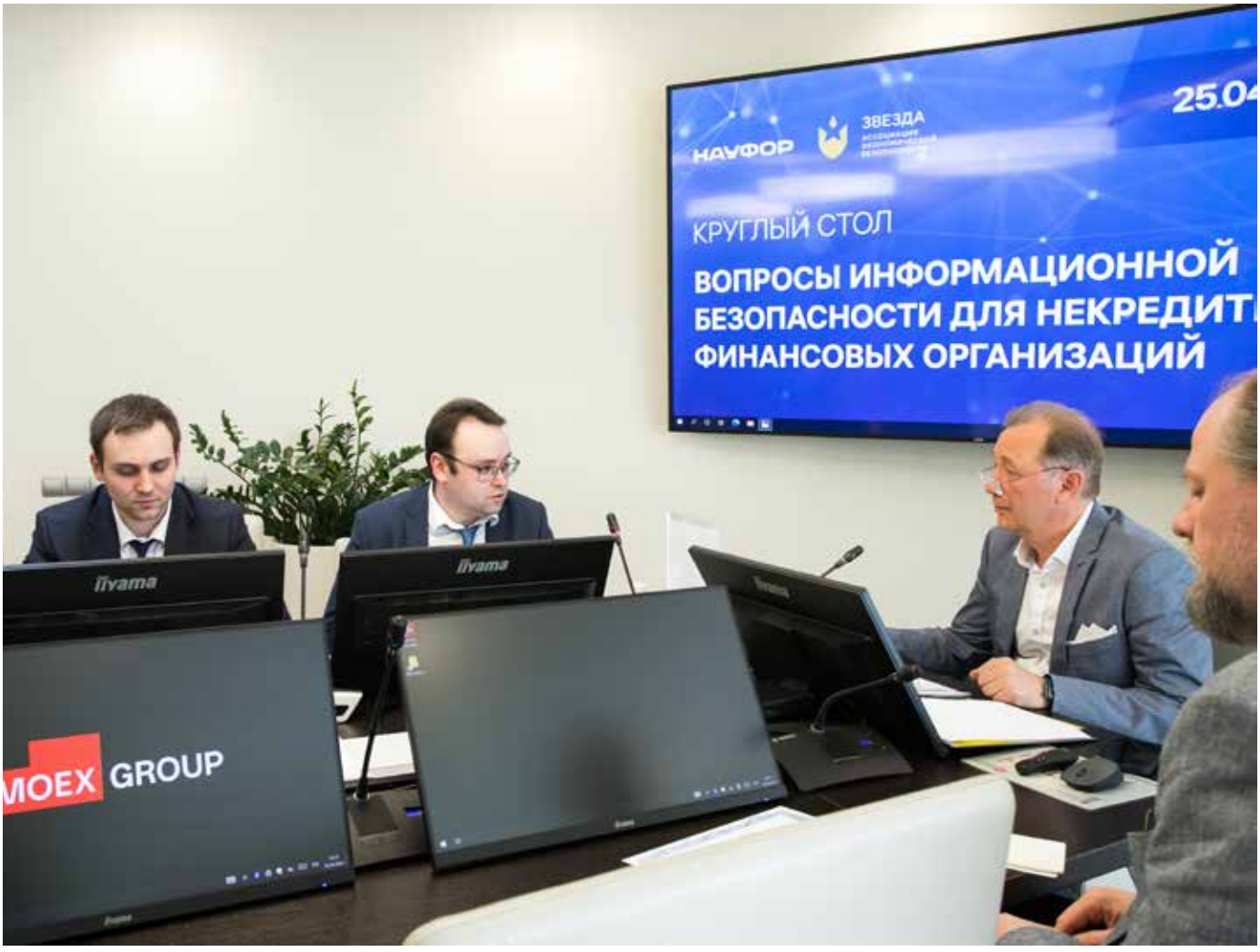
Эта тема в прошлый раз всплыла на поверхность и потом ушла в небытие. Поэтому хотелось бы, если есть такая возможность, обсудить, как вернуться к этому и насколько это интересно?

Михаил Шабанов. Есть вопрос создания некой рабочей группы между ДИБом и НАУФОР (может быть, еще какими-то саморегулируемыми организациями) для обмена, в том числе, пилотными проектами. Чтобы прежде, чем принимать и полностью внедрять в отрасль какое-то решение, прокатать его на небольшой группе, как это делается в кредитных организациях. Почему бы эту практику не использовать в некредитных финансовых организациях?

Мы тогда соответствующее предложение подготовили и отправили в Банк России, но, к сожалению, ответа не получили, так что результатом похвастаться пока не получается.

Сергей Демидов. Действительно, на мой взгляд, стратегия Банка России (поскольку нас тоже привлекали к ее обсуждению) не должна быть подвешена в воздухе и реализована в отрыве от финансового сектора. Потому что, помимо обеспечения безопасности финансового сектора, ответственностью Банка России является также и развитие финансового сектора, и обеспечение защиты прав потребителей финансовых услуг. Это не всегда обусловлено только безопасностью, о чем много говорил Кирилл Пронин на недавних встречах. Повышение качества цифровых сервисов, которые используются на отечественном финансовом рынке, — тоже одна из задач Банка России. В этом смысле иногда почему-то, к сожалению, выглядит ортогональным движение между нуждами информационной безопасности и действиями подразделений Департамента финансовых технологий Банка России. Наверное, и стратегия, и тактика должна обсуждаться с рынком более широко. И, конечно, хотелось бы, чтобы Департамент информационной безопасности не был замкнут.

Если говорить конкретно, а не сферически в вакууме, то недавнее письмо про запрет простой электронной подписи до сих пор заставляет нас внутренне рефлектировать на тему того, как это вообще может работать. [*Имеется в виду Информационное письмо Банка России от 16.03.2023 N ИН-017-56/22 «О применении требований нормативных актов Банка России об обеспечении целостности электронных сообщений и подтверждения их составления уполно-*



моченным на это лицом». — Прим. ред.]. И о чем думали коллеги, не проведя это положение через предварительные обсуждения. Потому что, в принципе, сейчас весь финансовый сектор одномоментно начнет этот запрет нарушать.

А в преддверии того, что, как вы сказали, с апреля возобновляются проверки, понятно: будут лететь головы. И дефицит трудовых ресурсов, который сейчас сложился в Российской Федерации в силу понятных событий, усугубится.

Поэтому, конечно, хотелось бы большей кооперации, не знаю, в какой форме. Это может быть формат или рабочей группы, или вновь созданного технического комитета. Ведь есть же хорошие примеры форматов, в которых подобные проблемы обсуждаются. Но хотелось бы все-таки, чтобы имело место реальное обсуждение документов: от уровня стратегии до уровня нормативов. И в формате не только «давайте всех защитим, чтобы стало невозможно работать», но и в контексте поиска баланса. Баланса между соблюдением прав потребителей финансовых услуг и требованиями безопасности для тех же потребителей финансовых услуг.

Михаил Шабанов. Спасибо, Сергей!

Коллеги, если есть по этой теме (и с учетом тех вопросов, которые прозвучали) мысли, то прошу высказаться. Пока комментариев нет? Тогда даем возможность комментария представителям Департамента информационной безопасности Банка России.

Георгий Ерохин. Касательно вопросов, связанных с тем, чтобы департамент был более открытым. Мы, со своей стороны, хотели бы упомянуть некоторые наши усилия, направленные на то, чтобы наши документы были применимыми на практике.

В частности, наша работа по разработке национальных стандартов и стандартов Банка России, которая осуществляется на площадке Технического комитета, в рамках Подкомитета № 1, ведется с учетом замечаний и предло-

жений экспертов со стороны рынка. Не только финансового рынка, но и отдельных организаций, осуществляющих последующую проверку этих требований. В рамках данной работы активное участие и представление предложений ожидается от каждого из участников. На практике за время работы над стандартами по обеспечению операционной надежности, по управлению риском реализации информационных угроз мы такую обратную связь получали в виде значительного объема замечаний и предложений, который затем обрабатывали для совершенствования документов. При этом документы выносились на рассмотрение экспертам на всех стадиях проектов, даже на стадии чернового варианта, чтобы проработать документ, собрать обратную связь, учесть пожелания рынка, экспертизу, базирующуюся на международном опыте и лучших практиках в отрасли.

Касательно проработки нормативных актов. Есть процедура, в рамках которой мы ведем свою работу. Согласно указанной процедуры нормативные акты перед их вынесением на утверждение и направлением на регистрацию в Минюст России должны проходить процедуру антикоррупционной экспертизы и оценки регулирующего воздействия. Мы придерживаемся этой процедуры. И сейчас, помимо стандартного размещения на сайте regulation.gov и на сайте Банка России, наш департамент также осуществляет рассылку проектов нормативных актов через АСОИ ФинЦЕРТ по организациям, которые подпадают под регулирование указанных нормативных актов. [*АСОИ ФинЦЕРТ, автоматизированная система обработки инцидентов — основной канал передачи информации об инцидентах в Банк России. — Прим.ред.*].

Михаил Шабанов. Спасибо, Георгий Игоревич.

Сергей Демидов. Здесь на самом деле вот что важно. Я сказал довольно длинную фразу, наверное, в ней не все можно было уловить. Вот смотрите, появляются какие-то нормативные акты, — тот же стандарт по риску информационной безопасности. В принципе, он как методологический документ, наверное, нормальный. Но что мы упустили? Мы упустили вопрос, состоялось ли нормальное, обстоятельное обсуждение вопроса, какие риски применимы к рынку НФО и насколько на нем действительно нужны дополнительные стандарты. Потому что еще после внедрения 757-П на самом деле не было пропорционального регулирования, 757-П был калькой 683-П.

Потом, тоже через разного рода ассоциации, Департамент инфраструктуры финансового рынка получил сигнал, который добавил туда пропорциональное регулирование. После этого было много дискуссий, насколько вообще применимы эти форматы. Мы прожили какое-то количество времени (наверное, около двух лет) и поняли, что инциденты не возникают. Как их не было до момента появления этого стандарта, так они и не стали возникать на рынке НФО. Получается, что регуляторное воздействие, даже несмотря на пропорциональное регулирование, оказалось излишним, оно никакой реальный риск не закрывало, никаких реальных проблем не решало. ОК, хорошо, этот опыт мы получили.

Но дальше появляется 779-П. Поэтому мне кажется, что нужно не просто призывать прокомментировать нормативный акт, а сначала вернуться на предыдущий этап стратегии и понять: действительно ли этот рынок должен быть под таким жестким регулированием? Если жесткое регулирование все же должно быть, то на какие конкретные области оно должно быть направлено. Вот этого обсуждения не происходило и не происходит.

Да, ТК 122 существует. Я напомню его состав: в нем 2/3 — это поставщики. При мне вносился стандарт профбезопасности [*речь идет об утвержденном в 2022 году профессиональном стандарте «Специалист по информационной безопасности в кредитно-финансовой сфере». — Прим. ред.*], и тут же включалось мощнейшее лобби людей, которые владеют обучающими структурами. Они лоббируют, что нужно сделать обязательным и обучение в объеме 512 часов, и чтобы его проходили все сотрудники всех финансовых организаций. Потому что они увидели рынок, увидели деньги. А мы говорим о тех, на кого это регулирование направлено, и кто страдает от этих стандартов. Мне кажется, что этой дискуссии нет, и пока нет органа, где можно этот вопрос поднять.

Реплика с места. Представительство профучастников в ТК 122 совсем мизерное. Я бы сказал, там мы играем на третьей линии. В то время как специфика работы комитета ТК 122 была именно банковская.

Существует специфика небанковских организаций. Страховая деятельность тоже отличается от банковской деятельности, у них своя специфика, свои типы мошенничества. Если говорить про страховые организации, то там больше проблем, связанных не с информационной безопасностью, а с другими аспектами. Но это уже отдельная тема.

Михаил Шабанов. Хочу выступить в защиту Банка России и, в частности, Департамента информационной безопасности. Андрей Выборнов (замдиректора департамента ДИБ) говорил, что, коллеги, если хотите попасть в 122-й, то, пожалуйста, обращайтесь. Есть возможность обратиться, подать заявку и войти. И мы несколько раз такие объявления в нашем комитете делали. Коллеги,

если вы хотите участвовать в работе Комитета 122, то пожалуйста.

Представитель комитета. Все равно даже банки с большим трудом могут провести через этот комитет свои инициативы. И даже если туда войдут представители НАУФОР, то все равно комитет занят скорее сбором обратной связи, скажем так, которая отличается от пилотирования. У пилотного проекта есть конкретное ТЗ, есть конкретный отчет, по которому корректируется та или иная норма, которая тестировалась через пилотирование. Это нормальная западная практика.

Когда я работал в компании, которая подпадала под регулирование британских законов по кибербезу, там однозначно все новшества по кибербезу проходили именно через «пилоты». Выделялись фокус-группы (по желанию), в них внедряли элементы стандарта, собирали анкеты, дальше приходили люди из надзора и проводили беседу: а если у вас будет такая норма, то как вы с ней будете жить, как она повлияет на PNL, как у вас CAPEX, OPEX из-за этого поедут вверх-вниз? Потом они все эти отзывы собирали, передавали наверх и уже только тогда принимали то или иное окончательное решение. Почему внедрен первичный стандарт? Потому что при его разработке имел место инженерный подход. Очень важно подходить к нормотворчеству именно с точки зрения того, что не получается закрыть все возможные уязвимости без их, скажем так, соотнесения с теми или иными аспектами бизнес-деятельности. То же самое страхование. Если, например, компания страхуется и у нее есть страховой резерв, то это тоже элемент управления риском.

Возвращаясь к тому, что говорил Сергей: через ТК 122 вряд ли именно НАУФОР сможет донести свою боль. Потому что даже если НАУФОР туда и придет, все равно ее представителей там будет не так много по отношению к общему количеству участников. И второе: все-таки обсуждение там идет в рамках формата. Я сам был участником этого комитета, там огромный зал, и даже чтобы к микрофону прорваться, нужны большие усилия.

А когда есть пилотирование, то у него есть конкретная методика, есть конкретная обратная связь. И можно обсудить конкретные результаты реализации той или иной нормы. Вот об этом речь.

Михаил Шабанов. Коллеги, коль мы затронули 122-й, я бы хотел обсудить вопрос о рабочей группе, которая была создана в рамках комитета 122 для обсуждения решений по применению простой электронной подписи в веб-приложениях, используемых НФО, но ее работа почему-то была приостановлена. Буквально два слова.

Реплика с места. Недавно пришел отчет, что возобновление работы ожидается, если на, то будут основания. Основания, мне кажется, сейчас имеются — и обязательные, и очень насущные. Рынку нужен ответ, какую ПЭП (простую электронную подпись) мы можем использовать, где располагать СКЗИ (средства криптографической защиты информации), как это будет принимать Банк России. Поэтому если есть такая возможность, то мы бы просили восстановить деятельность этой рабочей группы. Мы бы обязательно приняли участие в её работе.

Сергей Демидов. Механизм экспериментальных правовых режимов используется недостаточно. Потому что он был заявлен чуть иначе, чем воплотился. Я напомню, что первым пионером в области экспериментальных правовых режимов как раз был Банк России, который анонсировал эту идею как историю с двумя вариантами реализации.

Первый вариант — это режим, который пытался функционировать. Когда создается экспериментальный документ и можно сделать новый вид бизнеса, используя этот режим для того, чтобы попробовать какую-то новую нишу, в том числе для финансовых технологий. Так называемый ФинТех.

Второй режим, который не запустился, — это о том, что прежде, чем внедрять регулирование, надо поэкспериментировать, что будет, если вот такое конкретное регулирование будет действовать для всего рынка.

И вот второй вариант не случился совсем. Вполне вероятно, что над тем, о чем мы здесь говорим, следовало бы подумать коллегам из Банка России. И может быть, вернуться к этому механизму: назвал бы его механизмом апробации воздействия нормативных актов. Потому что не всегда возможно в моменте посчитать сумму регуляторного воздействия, особенно для всего рынка, и сказать, что, скажем, новый нормативный акт по операционной надежности для страховых компаний будет стоить 500 млн рублей на весь рынок. Такое утверждение всегда ставится под сомнение людьми, особенно в правительстве. Они смотрят технико-экономическое обоснование, не верят цифрам, спрашивают, как подсчитали? И в результате на сайте regulation.gov.ru этот проект уже оказывается с оценкой, что никакого воздействия на рынок не происходит. Мы понимаем, что так работает механизм, такова государственная бюрократия.

Но вместе с тем, если бы была возможность, чтобы новые нормативные акты предварительно обкатывались на небольшой группе компаний, например, как наша. Мы большие, мы стерпим, это нормально. Но вместе с тем бывает ситуация, когда такой же нормативный акт одновременно выходит и для мелких брокерских компаний, в которых работают по три человека (реально три: генеральный директор, контролер, бухгалтер). Причем весь «хвост» брокерской


НАУФОР
ЗВЕЗДА
КРУГЛЫЙ СТОЛ

индустрии состоит из таких компаний. Каковы могут быть для такого брокера требования к операционной надежности, я не понимаю.

Но это можно было бы понять, если бы такой нормативный акт сначала вышел в виде предварительного регулирования. Когда бы весь рынок вместе с регулятором осознал, что, наверное, для «хвоста» брокеров такое регулирование не очень релевантно, — тогда была бы возможность пересмотреть баланс этого пропорционального регулирования.

Андрей Ковешников. Вы говорите, что нужны пилоты и нужно выделить фокус-группу. А есть какие-нибудь предложения по выделению этой фокус-группы на рынке? Я так понимаю, что если кто-то из желающих скажет, что хочет, то, наверное, может обратиться в ДИБ ЦБ или в ЦБ напрямую, и попытаться вопрос для себя решить. Но что, если ДИБ ЦБ будет играть в рулетку под девизом: «Кто будет представителями фокус-группы?»

Сергей Демидов. Это тоже практика западных рынков, где такие фокус-группы существуют. На практике для тех, кто является участником таких фокус-групп, вводятся определенные послабления. Это не должна быть игра в одни ворота. Если компания на предварительном этапе берет на себя какие-то дополнительные обязательства (обкатать новую норму, утвердить необходимые документы и тому подобное), то дальше вопрос в том, какой пряник она за это получает. Очевидно, что фокус-группа не будет состоять только из крупных компаний, она может состоять также из мелких.

Что получает такая фокус-группа? Они получают пряник в виде чего-то вроде индульгенции за нарушения на какой-то промежуток времени по тому же самому нормативному акту. Или, например, компания типа биржи получает на том рынке, где она оперирует, реализацию принципа пропорционального регулирования. И вместо того, чтобы инвестировать непонятно во что, брокерские компании будут инвестировать деньги в основной бизнес. Это тоже прибыль, косвенная, но прибыль.

Что получает регулятор? Регулятор получает математически обоснованную цифру воздействия на рынок, с которой уже не стыдно идти в правительство. Не стыдно на уровне правительственных комиссий рассказывать: вот прошла фокус-группа и там посчитали, что на средние компании это регулирование влияет на сумму X рублей, на мелкие компании влияет на сумму Y рублей и так далее. И дальше меры, проверенные на фокус-группах, оформляются уже в виде пропорционального регулирования, в котором регуляторное воздействие взвешенно и сбалансировано.

Андрей Ковешников. Я с вами согласен. Но пока то, что вы называли пряником, никак не анонсировали. И как его может анонсировать ЦБ, мне не совсем понятно.

Реплика с места. Мы же сейчас не пытаемся изобразить всю модель на пальцах… Мы пытаемся посеять реальный западный опыт, который достаточно эффективно работает на конкретных рынках в конкретных направлениях. И показать, что возможна определенная стратегия. Мы говорим о том, что опыт применения 757-П и последующих документов показывает, что они, на наш взгляд, немножко непропорциональны с точки зрения тех требований и тех рисков, которые за этим стоят. Грубо говоря, мы пытаемся бульдозером выкорчевывать борщевик. И вот ездит трясущийся бульдозер, он стоит дорого, от него разит соляркой, а вокруг колосится борщевик как ни в чем не бывало. Было бы гораздо эффективнее просто просеять заросшие участки правильным не очень дорогим гербицидом, и борщевик пропадет.

Опять же возвращаясь именно к тому, что мы сейчас не будем обсуждать всю модель и всю схему. Но, на мой взгляд, есть компании, которые согласятся войти в такие фокус-группы. Если у ЦБ будет желание, то можно найти пряник, который позволит компенсировать этим компаниям их участие в проекте. Поэтому хотелось бы, чтобы у коллег появилось позитивное отношение к такому ходу событий. Регулирование — это реальные люди, которые, скажем так, обслуживают те или иные сектора экономики. Соответственно, действия, которые отражаются в нормативной базе, потом ложатся (так или на иначе) на PNL конкретных компаний.

Антон Чернодед. Прокомментирую. Банк России не против создания рабочей группы. Даже больше скажу: есть практический опыт в части обсуждения насущных вопросов на базе различных ассоциаций. Мы, со своей стороны, готовы «провалидировать» те модели, которые сейчас заложены в нормативных актах Банка России.

Михаил Шабанов. У меня завтра планируется встреча в ДИБе, я эту инициативу, естественно, постараюсь там озвучить. Надеюсь, что вы поддержите эту идею, для того чтобы мы в НАУФОР могли создать эту рабочую группу и она была эффективной. Хорошо. Спасибо.

Тогда переходим к обсуждению следующей темы.

Итак, вторая тема нашего обсуждения.

С какими сложностями столкнулись некредитные финансовые организации при реализации требований Положения Банка России 757-П и 779-П.

Надо обсудить, как реализован в этих документах риск-ориентированный подход и концепция пропорционального регулирования. Следующий пункт

обсуждения: что необходимо знать о практике проведения оценки соответствия использования в НФО программного обеспечения приложений по ОУД4 (оценочный уровень доверия).

Следующий вопрос: как обеспечить исполнение требований п. 1.9 Положения Банка России 757-П в соответствии с Письмом Банка России от 16 марта 2023 года № ИН01756/22. Это об использовании СКЗИ как раз.

И еще один вопрос: возможно ли преодолеть кадровый голод в области информационной безопасности в кредитно-финансовой сфере, или как сильно повлияет на деятельность НФО вступление в силу профессионального стандарта для специалистов по информационной безопасности в финансовой сфере.

Вот такие вопросы. Да, пожалуйста, Андрей.

Андрей Киселев. Я представляю несколько компаний: регистратор, депозитарий и спецдепозитарий, поэтому есть опыт работы в средних и малых компаниях. Хочу сразу сказать, что занимаюсь информационной безопасностью достаточно давно. За 20 лет инциденты с информационной безопасностью у нас были, и все они были связаны с человеческим фактором: внутренним нарушителем. Были сотрудники, которые пытались распечатать и вынести документы с конфиденциальной информацией. В 2009 году один сотрудник даже пытался продавать реестры. С помощью правоохранительных органов его поймали, было уголовное дело, штраф, лишение аттестата. Понятно, что в компании есть технический набор защит: антивирус, файервол, системы предотвращения вторжений, системы предотвращения утечек, системы корреляции событий и так далее.

С чем мы столкнулись? В 757-П говорится, что нужно проходить оценку соответствия ГОСТу 57580. В нашей компании еще в 2019 году руководство определило, в каком направлении должна развиваться информационная

безопасность. Мы выбрали на то время зарубежный стандарт ISO 27001, потому что рынок сказал, что 27001 — это про безопасность, а 57580 — непонятно про что. Мы решили: будем готовиться и к тому, и к другому, так как регулятор требует соответствия стандарту 57580. В итоге в 2021 году мы получили сертификат соответствия стандарту ISO 27001:2013.

Хочу сравнить эти два стандарта.

Затраты по времени и объему подготовки были примерно одинаковыми. Чтобы пройти процедуру соответствия стандарту 27001, нам потребовалось две недели работы с аудитором в достаточно комфортной обстановке. Аудитор у нас был от BSI (Национальный орган по стандартизации Великобритании). Что у них хорошо. BSI утверждает, что ни одна компания сразу не может соответствовать стандарту 27001 на 100%, они понимают, что поначалу несоответствий будет достаточно много, аудитор не может проверить все требования к этому стандарту. Но они проверяют главные требования, а также, что сам процесс запущен, что руководство компании понимает необходимость заниматься информационной безопасностью. Если аудиторы BSI видят, что процесс идет и соблюдаются основные требования, то выдают сертификат соответствия и в дальнейшем проверяют соблюдение требований стандарта раз в год, постепенно доводя систему до совершенства. В дальнейшем они тщательно проверяют каждую область требований стандарта. В нашей компании, например, на второй год нам сделали меньше замечаний (несоответствий).

Теперь что не понравилось в стандарте 57580. Мы долго выбирали аудитора, посмотрели много компаний. Во-первых, это дороже, чем аудит по стандарту 27001, притом, что это российский стандарт и только для некредитных финансовых организаций и банков. Во-вторых, аудиторы сказали: вы будете собирать все свидетельства в течение трех месяцев самостоятельно. А в прошлом году случилась СВО, и нам было не до сбора свидетельств, мы просто не могли выделить столько времени. Аудит для НФО стандартного уровня защиты информации должен проводиться раз в три года. Я обсуждал эту тему с другими директорами по информационной безопасности, они тоже говорят, что все очень сложно, что на это надо убить полгода времени.

А какой результат? Аудиторы говорят: у вашей компании будет отчет, мы знаем требования ЦБ, если ЦБ придет к вам с проверкой, вы им покажете отчет, они зададут вопросы, мы вам скажем, что ответить. То есть, польза от этого аудита имеется только в плане защиты от регуляторного риска. Понятно, что защита от других рисков иллюзорна: могут взломать, а могут не взломать, хакеры могут появиться или не появиться. На эти риски у нас, соответственно, есть бэкапы и внедренные средства защиты. Остальные риски понятны, мы их можем регулировать, а регуляторные не можем. Например, приходит Банк России, мы все бросаем, чтобы собирать для него данные, отвечать на его вопросы, а ресурсов мало. То есть мы работаем на бумагу. И многим безопасникам это очень не нравится, вот прямо совсем.

Реплика с места. Сами требования понятны. Хотя даже для того, чтобы читать язык ГОСТов (сам 57580 и следующий ГОСТ на проверку), аналитик должен быть выше среднего, чтобы как рыба в воде плавать из одного документа в другой. И для того, чтобы войти в диалог с Банком России и доказать: то, что заявлено, реально существует. Начинается игра в своего рода «Монополию», не реальная проверка безопасности, как сказал коллега, а именно квест.

И следующий момент. СВИФТ определил, что-такой-то процент требований (не очень большой) является обязательным для компании в первый год. Компания должна проинформировать всех участников альянса о том, какое у нее имеется соответствие обязательным требованиям, необязательным требованиям. И рынок начинает стимулировать наличие соответствия. Все смотрят друг на друга и говорят: «Этот уже выполнил обязательные требования. А тот не выполнил. Наверное, с тем, кто не выполнил, я не буду общаться, ограничу с ним операции по СВИФТу».

То есть, нужно иметь в виду, что важно использовать и так называемые мягкие методы мотивации. Хороший вариант: информирование о реальном уровне соответствия. Вот есть три уровня, и первый уровень надо сразу полностью реализовать. Но проще сказать руководству, что первые три уровня контроля мы делаем в течение восьми месяцев, следующие четыре обязательных контроля делаем еще через год, на третий год — еще пять обязательных контролей. Важно чувствовать эту ситуацию.

Андрей Киселев. Пример по ОУД4. Российский регистраторский рынок — небольшой. Наша компания купила программу, которая с помощью квалифицированной электронной подписи обеспечивает передаточные распоряжения (то, что касается финансовых операций). Регулятор выпустил положение 757-П, в соответствии с которым нужно делать оценку таких программ по ОУД4. Программа стоила 700 тысяч рублей. Разработчик говорит: «Если вы хотите получить оценку ОУД4, то такая оценка будет стоить 7 млн». А на нашем рынке мало клиентов. Ради них платить еще 7 млн? и руководство говорит: «Надо подумать о закрытии сервиса».

Сейчас то же самое происходит с ПЭПом, после письма Банка России от

16.03.2023 № ИН-017-56/22 думаем над закрытием соответствующего сервиса. Получается, что регулирование просто убивает цифровые сервисы в регистраторском бизнесе.

Сергей Демидов. Коллеги привели хорошие примеры, мне даже добавить нечего. Действительно, в ГОСТе есть элементы, которые защищают непонятно от чего. Например, прямое указание на централизованное управление мобильными устройствами. Но если у меня в почте нет ничего конфиденциального, зачем мне принудительно включать на мобильном устройстве систему MDM? Очевидно, что риски могут купироваться другими способами.

Реально в ГОСТе много таких вещей: практически в каждой из восьми глав есть излишние нормы. Я предлагал бы пересмотреть их вместе с рынком. Мы даже готовы потратить время и пересмотреть еще раз, что действительно требуется, что действительно защищает от каких-либо рисков, а что является избыточным и должно оставаться на усмотрение организации.

Риск-ориентированный подход как раз в этом и заключается, что каждая организация в состоянии сама посмотреть на свои риски. И если у меня в почте не ходит конфиденциальная информация, если технически реализовано именно это, то не заставляйте меня внедрять MDM (Mobile Device Management – управление мобильными устройствами). Это касается рисков.

По поводу ОУД4 — отдельная история.

С одной стороны, мы поддерживали эту историю, потому что это было попыткой заменить требования к конкретному проверяемому объекту на требования к процессу. Сначала говорили, что давайте Банк России сделает стандарт, как правильно разрабатывать ПО. И если компания следует этому стандарту, то автоматом получает ПО, согласованное к использованию. Это действительно сейчас реализовано через ОУД4. Но, кроме нас, это так никто и не прочитал. Это говорит, может быть, и о нас не очень хорошо. Но в целом неочевидно сейчас, что получилось именно так. Поэтому очевидно второе пожелание: над этим нормативным актом тоже нужно работать.

Ну, и скажу честно, я ожидаю, когда в нашу компанию придет проверка, даже с нетерпением. Потому что, по всей видимости, даже несмотря на то, что у нас сделана сертифицированная ФСТЭК лаборатория, скорее всего, при проверке в ОУД4 даже она нам не поможет. Просто потому, что требования избыточны, они являются калькой с требований ФСТЭКа. А требования ФСТЭК — соответствуют процессу создания, скажем, программы управления ядерными ракетами Российской Федерации. И непонятно, зачем систему, которая обрабатывает нефинансовую транзакцию пользователя (на российском рынке транзакция не приводит к финансовому результату единомоментно, она приводит только к рыночному риску), проверять с точки зрения кода так же, как систему запуска ядерных ракет. Мне никто, наверное, на этот вопрос не ответит.

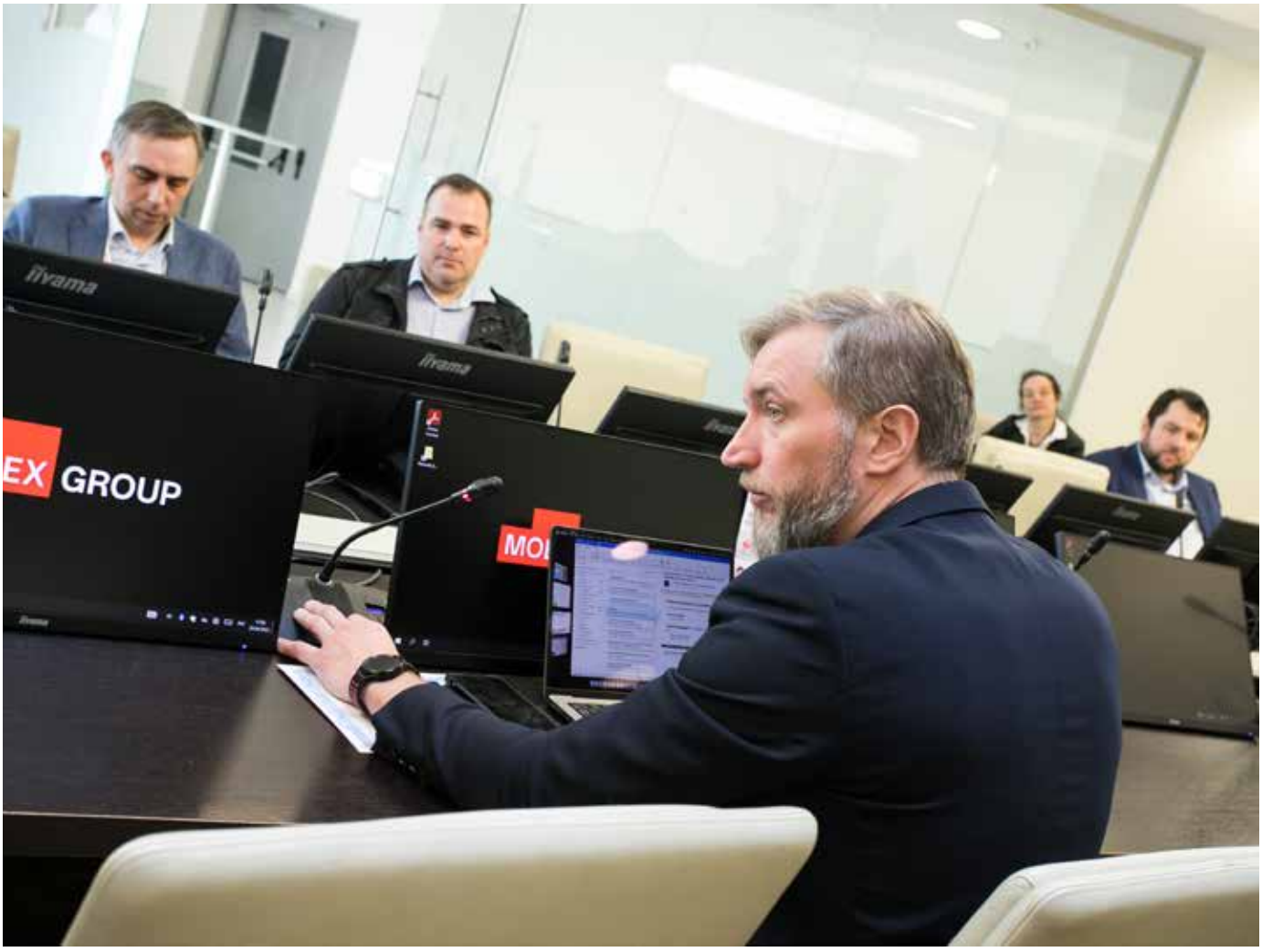
Это другой рынок. Даже если злоумышленник захватил торговый терминал и сделал транзакцию, то, повторюсь, это рыночный риск. Это риск того, что к тому моменту, когда вы опомнитесь и продадите этот актив обратно в рынок, произойдет какое-то движение рыночных цен. Вопрос про риск-ориентированный подход — ровно про это. Рынок чуть другой, единомоментной утечки денег не существует, именно поэтому на этом рынке очень мало случаев реального мошенничества. Поэтому нормы регулирования для нас выглядят чуть-чуть излишними, и мы об этом раз от раза говорим.

Представитель комитета. Я бы сказал даже больше. Реальный и наиболее критичный риск, по-моему, чисто экспертному мнению, связан именно с инсайдом. Это неправомерное использование информации для того, чтобы увидеть ход рынка, кому-то слить, чтобы кто-то купил, зная, что, например, сейчас кто-то будет покупать много акций той или иной компании. Или, наоборот, есть так называемые «черные» брокеры, которые пытаются собрать деньги, говоря о том, что будут делать фонд. А на самом деле у них нет ни лицензии, ничего: они деньги собрали под видом сервисов, которые связаны с криптой или еще с чем-то.

Реальный объем потерь для населения, скорее всего (это мое субъективное мнение, я статистикой не владею), связан именно с тем, что есть попытка слить именно рыночную информацию, инсайд.

Сергей, может быть, сейчас меня поправит.

Сергей Демидов. У меня очень много чего есть по этому поводу рассказать. В нашей компании есть действующая «горячая линия», куда обращаются обиженные «физики», которых развели под видом инвестиций. И этот поток растет. Он растет существенно, пропорционально приходу «физиков» на фондовый рынок. Сейчас на рынке порядка 22 миллионов частных инвесторов, если мне память не изменяет. Но мы ожидаем, что до конца года их численность дойдет до 25 миллионов. Это значит, что уже половина экономически активного населения нашей страны в том или ином виде соприкоснулось с инвестиционным рынком. Их разводят через WhatsApp, аналогичными приемам «следователей» и «служ-



бы безопасности Сбербанка» и т.д.... Повторюсь, объем обманутых растет, потому что мы видим, как поступают обращения. Помочь мы им ничем не можем, они не являются стороной по договору, они не попали на фишинговый сайт. Просто человеку звонит «аналитик Московской биржи…». Сейчас такие действия под регулирование Банка России не попадают, я даже сообщать об этом не должен, потому что я не сторона этого инцидента, просто получил информацию.

Проблема в этом, что нужно развивать финансовую грамотность. Но, честно говоря, несмотря на то, что мы активный участник программ по финансовой грамотности, я пока так и не придумал, куда можно вставить информацию о методах противодействия таким методам. Господин Мамут этим занимается, Валерий Лях тоже активно участвует во всех программах финансовой грамотности, но там нет привязки к информационной безопасности. В общественном транспорте размещается информация о том, что не надо сообщать номер карточки. Но когда не просили сообщить номер карточки, а сказали: «Вы сейчас заработаете на акциях «Газпрома» за счет инсайда 700%», то это другой уровень. Программа финансовой грамотности, очевидно, должна быть адаптивной. Потому что, как только мы расскажем в метро о том, что нужно опасаться звонков о росте акций «Газпрома», злоумышленники тут же придумают что-то новое. И это всегда будет вокруг денег.

Здесь, наверное, важна роль Банка России. Мы стоим на переднем плане, собирая информацию, и готовы ею делиться, вообще готовы помогать. Но мы не сделаем это одни, у нас не хватит бюджетов, чтобы делать рекламу в метро. Это может сделать только государство.

Михаил Шабанов. Сергей, большое спасибо! Возвращаюсь к Уральскому форуму. Я был на сессии, в которой участвовали представители правоох-

ранительных органов, и познакомился там с представителем нашего МВД. Там создано специальное подразделение, их работа посвящена именно мошенничеству на основе социальной инженерии.

Мы можем с ними по этому поводу общаться. Я взял телефон, можем пригласить людей из этого подразделения на комитет, можем как угодно организовать контакты. Но придется учитывать, что у них пока еще совсем малочисленный состав.

Сергей Демидов. Я считаю, что, во-первых, это задача Банка России. Во-вторых, то, что делает МВД, извините, называется «искать ключи под фонарем», а не там, где потеряли. Здесь вполне очевидная история, про которую говорят все. Про это говорит Греф, про это говорит Кулик. Себя в их ряд ставить не буду, но я тоже об этом много говорю.

Проблема в чем? В том, что мошеннические колл-центры находятся вне досягаемости российского права. Сбор доказательной базы или цифровых свидетельств, как это модно сейчас говорить, в отношении всех этих инцидентов абсолютно бесполезен. Самым эффективным методом борьбы действительно выглядит финансовая грамотность населения. Все равно останется «икс» процентов людей, который будут ошибаться, но, тем не менее, грамотность достаточно сильно снижает процент таких кейсов.

Второе — это деятельность уже кредитных организаций, где мошенническая схема преобразуется непосредственно в кэш. Например, Кулик и другие люди рассказывали о том, что в Сбере и ВТБ стоят уже системы фрод-мониторинга, которые выявляют аномалии в процессах съема денег. То есть бабушка раньше в течение 10 лет снимала с карточки кэшем по 10 тысяч рублей в месяц и в «Пятерочке» тратила еще 5 тысяч, а тут — бац — и сняла всю пенсию. Очевидно, что это является потенциальным риском, abnormal deviation (отклонение от средней величины). Коммерческие банки учатся с этим бороться. Но работа должна быть слаженной. И да, те 12 человек из МВД, наверное, в какой-то момент к ней тоже должны подключиться. Но сейчас нам нужно, скорее, Министерство обороны.

Реплика с места. У нас имеет место реальная нехватка киберполигонов.

Антон Чернодед. Особенно актуален вопрос касательно социальной инженерии. Не соглашусь, что Банк России не регулирует данную область. Есть достаточно богатая нормативная база по данному направлению. Возможно, коллеги с ней не знакомы, потому что они работают на бирже, но кредитные организации с ней работают активно.

Для Банка России на текущий момент есть три основных направления надзора. Первое направление как раз связано с социальной инженерией, с несанкционированными операциями, в первую очередь, в отношении физических лиц. Это одно из основных направлений работы моего департамента. Есть действующие нормы в части обязательного наличия систем фрод-мониторинга кредитных организаций. Они присутствуют не только в крупных банках. Банки реализовали системы фрод-мониторинга не потому, что это была их инициатива, а в связи с требованием Банка России. Это же требование распространяется и на другие кредитные организации.

Со своей стороны Банк России проводит работу в части надзора за кредитными организациями, причем не формальную (в плане наличия тех или иных документов), а в плане оценки эффективности системы фрод-мониторинга. У нас есть достаточно богатая статистика по всем кредитным организациям: кто насколько успешно борется с мошенничеством, которое осуществляется с применением методов социальной инженерии. И мы ведем активную работу по данному направлению.

Есть регулярный сбор данных по операциям без согласия клиента, есть форма отчетности, которая предоставляется на ежеквартальной основе всеми кредитными организациями. Банк России ведет регулярный мониторинг данных операций в рамках форм отчетности, у нас есть отдельно выделенный канал в рамках АСОИ ФинЦЕРТ, на ежедневной основе.

Дополнительно сейчас Банк России прорабатывает вопрос в рамках Указания Банка России №4336-У. Речь идет об оценке экономического положения банков, чтобы вопросы фрод-мониторинга непосредственно влияли на кредитные организации, чтобы они были мотивированы эффективно бороться с фродом.

В части повышения финансовой грамотности населения. В департаменте есть отдельное подразделение, которое занимается данной задачей и уже много лет ведет активную работу по повышению киберграмотности населения. Отдельно взаимодействуем по данному вопросу с МВД.

Есть ряд проектов по внесению изменений в нормативные акты именно технической направленности, чтобы также повысить эффективность по данному направлению.

И мы видим, что наша работа дает определенные положительные плоды. Но есть над чем еще работать.

Теперь то, о чем рассказывали коллеги из Московской биржи…

Михаил Шабанов. Не только они, у некоторых организаций — членов НАУФОР такие звонки тоже существуют: когда прикрываются названиями компаний и используют приемы так называемых «черных» брокеров.

Антон Чернодед. Да, есть различные схемы введения в заблуждение физических лиц, в том числе связанные с различными инвестиционными активами, Московская биржа с этим соприкасается. Существует не единственная мошенническая схема.

Вся эта статистика попадает в форму отчетности кредитной организации. Когда выявлено, что операция была без согласия клиента, то дальше физическое лицо обращается в МВД, обращается в кредитные организации, пишет жалобы в Банк России. Соответственно, каждый подобный случай учитывается в общей статистике.

Есть отдельные нормы, касающиеся таких ситуаций, в рамках 161 Федерального закона. При определенных условиях клиент может перенести финансовую ответственность на кредитную организацию, и тогда кредитная организация обязана возместить потери.

Михаил Шабанов. Но статистика по этим делам не очень. Та статистика за прошлый год, которую публиковал ФинЦЕРТ. Реальный объем того, что компенсировали кредитные организации, очень незначителен.

Антон Чернодед. Сейчас проходит, скажем так, постепенное совершенствование законодательства в области антифрода. Вносятся соответствующие изменения в 8 и 9 статьи 161 Федерального закона, в результате процедура (в том числе, связанная с возвратом денежных средств клиентам), по нашему мнению, и с учетом мнения отрасли будет более, скажем так, совершенна и более применима в текущей деятельности.

Михаил Шабанов. Вопрос подмены телефонного номера тоже сдвинулся с мертвой точки? Понятно, что четыре крупных отечественных провайдера услуг связи обязаны проводить антифрод и прочие меры, не давать возможность переадресации, скажем, мелким провайдерам связи. Но вместе с тем, когда я находился на Уральском форуме, мне в очередной раз звонили мошенники с использованием методов социальной инженерии (звонок из правоохранительных органов) и подменой номера через «Мегафон». Я обращаюсь к представителю «Мегафон», прошу проверить. Как же так, звонят мошенники прямо на Уральском форуме. Проверили: «Да, мошенники». Ну не срабатывает система.

Представитель комитета. Это треугольник: есть возможность нарушить, есть возможность остаться безнаказанным и есть мотив. В рамках этого треугольника очень важно то, о чем сказал Сергей. Это, на мой взгляд, критично: то, что колл-центры находятся за пределами РФ. И да, мы опускаем руки и говорим, что ничего сделать не можем. Но вот представитель из Белоруссии говорил на одном мероприятии, что там на техническом уровне сделали так, что внешние колл-центры внутрь Белоруссии звонить не могут. Надо бы как-то доносить до МВД и до Минсвязи именно эту тему. Что важно локализовать звонки, чтобы фрод-мониторинг ставился не только в кредитных организациях, но и у операторов связи, особенно тех, которые обеспечивают стык с зарубежными провайдерами.

Михаил Шабанов. Именно такое обязательство и есть сейчас в законе. Но под эти требования попали только крупные провайдеры. Так получилось (по крайней мере, такое утверждение прозвучало на Уральском форуме), что из положений федерального законодательства выпали мелкие, небольшие провайдеры услуг связи.

Реплика с места. Когда крупный оператор получает звонок-переадресацию от мелкого оператора, он уже не видит, откуда идет звонок, и не может ничего сделать. Это как раз ложится в концепцию риск-ориентированного подхода, о чем коллеги говорили. Не всем нужна антифрод-система за 20 млн рублей. К примеру, у некредитной организации нет клиентов-физлиц, в большинстве ее клиентами являются обычные ИП-шники, средний бизнес. То есть там реально все клиенты, которые подключаются, сами по себе имеют системы антифрода.

По поводу мошенничества. Видно, что с каждым годом увеличивается нагрузка на кредитные организации относительно объемов, которые мы должны возмещать. Всегда ли прав клиент? а может быть, он неправ. Ведь может быть и мошенничество со стороны клиента: он отправил деньги, потом заявляет, что его обманули, а на самом деле это просто одна из схем развода. И мошенничество всегда будет впереди, как ни настраивайте антифрод-систему, это тоже нельзя упускать из вида. Я прямо сейчас могу сгенерировать схему, которую не поймает ни одна антифрод-система, но она будет мошеннической. Просто у меня есть значительный опыт…

Как видите, именно тема мошенничества отразилась в сердцах. Все присутствующие включились, и это свидетельство того, что никто не сговорился, а это реальный риск. Это не риск того, что случится попытка хакеров «расковырять» межсетевой экран, добраться до целевой системы, получить удаленный доступ и начать какие-то злонамеренные действия. Львиная доля всего того, что происходит, связана либо с инсайдом (об этом больше молчат, потому что это не очень хорошо), либо с социальной инженерией.

Социальная инженерия для профучастников отличается от происходящего в кредитных организациях. Мошенники, работающие через кредитные организации, до последнего времени пытались получить данные

кредитной карты и дальше уже отдельно что-либо делать с этими данными, чтобы их монетизировать. Что касается клиентов профучастников, то там, как цыгане, пытаются человека ввести в состояние зомбирования. Чтобы он передал этим людям как можно больше денег, или продал свои активы, или отдал их какому-то левому финансовому советнику. Как пример, такого звонка, этот якобы финансовый советник говорит: «…дай мне доступ в систему, напиши на меня доверенность, я буду за тебя торговать, у меня стоят супертерминалы Bloomberg, я по-английски шпарю, у меня консультанты из Англии и так далее». И люди переводят свой «кэш» (денежные средства) такому «советнику» несколько месяцев…

Михаил Шабанов. Кэш виртуальный. Реплика с места. Да, виртуальный. Человек видит, что его счет растет, какую-то часть этих денег может реально каждый месяц сбрасывать «советнику». А потом — бац, на счете все пропало. Человек не знает просто, что такое крипта. Люди теряют таким образом по 50, по 100 миллионов.

Антон Чернодед. Правильно я понимаю, участники рынка хотят, чтобы Банк России регулировал информационную безопасность в части крипты?

Михаил Шабанов. Нет, речь идет о том, что баланс рисков лежит не в части ГОСТов, а именно в части того, что происходит в жизни. Банк России говорит, что одна из его задач — помочь вкладчикам, гражданам России. В стране больше 20 миллионов граждан уже вышли на инвестиционный рынок. Для них более серьезной проблемой является не эксплойт: потому что там есть шифровальщики, устанавливаются бэкапы (Backup — это резервная копия данных), и потери реально будут не такими большими. Более серьезные потери клиенты несут сейчас из-за специфики социальной инженерии. Телефонное мошенничество типа «я оперуполномоченный УБЭП, дайте номер вашей кредитной карты» сни-

зится, это сто процентов. Но схемы разводки через Телеграм, через Авито, через те или иные манипуляции в части фондового рынка будут, наоборот, расти. И если мы эту точку не поймаем и не сместим акцент в регулировании, если мы по-прежнему будем трактором давить борщевик, то так и будет продолжаться.

Антон Чернодед. Для каждого вида деятельности есть свои риски. Когда мы говорим про участников НАУФОРа, у них совершенно другие риски, поэтому требования по фроду на них не распространяются.

Есть другие риски: виртуальные, связанные с хищением денежных средств, либо с вопросами операционной надежности. На эти риски распространяются другие меры защиты.

Возвращаясь к ранее озвученному вопросу о ГОСТе по защите информации, в сравнении с требованиями СВИФТ. Вы правильно заметили, что, когда в рамках СВИФТ появляются новые требования, то организации дается один год на выполнение новых рекомендаций, после чего данное требование становится обязательным. Замечу, что в рамках нормативной базы Банка России есть аналогичная конструкция, когда требование вступает в силу, во-первых, не сразу, дается определенный временной период на его выполнение. Во-вторых, в последнее время было достаточно много мораториев в части применения мер воздействия, они применялись достаточно длительное время. В-третьих, та же оценка соответствия. Для большинства участников НАУФОР актуален стандартный, либо минимальный уровень защиты информации. Оценка соответствия для стандартного уровня защиты информации проводится раз в три года. Что это означает? Что после того как требование вступило в силу, у организации есть три года на проведение оценки соответствия. Это гораздо больше, чем для члена СВИФТ, где на аналогичные мероприятия дается один год. Поэтому здесь, на мой взгляд, конструкция достаточная. Если не согласны, готов подискутировать.

Представитель комитета. Проще взять небольшой кусок документа, который реально реализован. Потому что, когда компания читает весь документ, то говорит: ОК, у нас есть три года на выполнение. И ничего не делает. Если мы действительно хотим, чтобы что-то внедрялось, то лучше разбивать пул задач на реализуемые мелкие части.

Мое экспертное мнение таково. Для мелких и для средних компаний было бы хорошо еще раз посмотреть внимательно на новые требования. Возможно, какие-то формулировки поправить, что-то упростить или уточнить. Итоговые задачи разбить на блоки: не на три года, а одну часть на полгода, потом еще одну часть на полгода, и так далее. Чтобы внедрялся, грубо говоря, один блок, потом второй блок, потом третий. Но это опять же рекомендация.

Если мы действительно хотим, чтобы рынок включился в эту работу, то важно, чтобы она стоила разумных денег. Коллеги же рассказали тут, что решили не внедрять программу, которая стоит 700 тысяч, потому что проверка по ОУД4 будет стоить 5 миллионов. Это реальные цены, мы тоже спрашивали, ценник меньше 5 миллионов рублей за такие работы действительно не получишь…

Антон Чернодед. Хороший пример, сразу возвращаюсь к нему. Здесь важно не то, что стоимость данного программного обеспечения составляет 700 тысяч рублей, а к каким рискам приведет невыполнение в компании требований информационной безопасности. Если, условно, риски минимальные, если клиенты в случае реализации инцидента в области информационной безопасности не понесут никаких финансовых потерь либо потери будут минимальны, то это не приведет к банкротству самой финансовой организации. Почему же эти риски, скажем, не застраховать? Если страховка будет стоить дешевле, чем выполнение требования кибербезопасности, то это тоже определенная компенсирующая мера.

Сергей Демидов. Не работает в проверках так. Вообще компенсирующие меры, я считаю, пока являются теоретической историей, которая очень слабо зашита в нормативные акты. Вопрос неиспользования/неисполнения отдельных пунктов требований Банка России сейчас действительно есть в самом в ГОСТе. Но при этом, когда приходит проверка, она очень смотрит не на то, что прописано в нормативном акте, а на документ, на который ссылается нормативный акт.

Мало того, честно скажу, наша компания не первый год делает киберстраховку. Я верю в нее, считаю, что за этим будущее, что страховаться надо всем. Но сейчас такой рынок, что можно застраховаться, а выплату не получить. Ну, давайте без иллюзий. Большинство кейсов, от которых страхуют страховые компании, реально никогда не кончатся возмещением.

Была целая панель на том же Уральском форуме, посвященная этой истории, где, собственно говоря, даже коллеги из ЦБ подтвердили, что сейчас рынок в зачаточном состоянии. Да, наверное, какие-то положительные кейсы тоже существуют, я даже спорить не буду.

Мы, прорабатывая этот сюжет, просто пригласили независимых юристов и проанализировали договор страхования. Расписали, что реально может случиться в сегменте кибербезопасности, вот прямо по пунктам. Пункт

a: хакер что-то подломал, пункт b: мошенник вывел деньги. И так далее. Дальше попросили внешних юристов оценить, насколько велика реальность получения страховых выплат по этим пунктам. Они сделали вывод, что выплат не будет практически нигде. Полноценная приостановка деятельности — вот, наверное, единственный реальный сценарий получения страховых выплат. Если реально деятельность компании будет остановлена на восемь часов. При этом на страхуемом лежит бремя доказательства, что остановка действительно случилась, что действительно все зашифровалось, из-за этого никак нельзя было оказывать деятельность, что виновного в бездействии нет и так далее.

Вот только в этих условиях можно было бы получить выплату.

Антон Чернодед. Сейчас в рамках Департамента информационной безопасности ведется активная работа в части развития рынка страхования кибербеза. Если коллеги готовы поучаствовать в данной активности, мы только за. Готовы их вовлечь в рамках, в том числе, НАУФОР.

Михаил Шабанов. Хорошо. Предварительно договорились, а дальше уже в рабочем порядке обсудим эти вопросы.

Андрей Киселев. Я бы хотел добавить пожелание по ГОСТу 57580. В международном опыте, когда внедряется какое-то ISO, то есть организация, которая сертифицирует аудиторов. Не мог бы Банк России тоже сертифицировать аудиторов, сказать: вот сто аудиторов, выбирайте любого, он проведет в вашей компании аудит и будет отвечать за результат. Сейчас рынок работает таким образом: вот этот аудитор нормальный, после его аудита не было проблем в Банке России, а вот этот накосячил: мы ему заплатили, а потом штрафы получили.

Сергей Демидов. На самом деле есть же успешный пример. Я эту тему несколько раз задвигал, есть успешный пример в другом департаменте Банка России, Ассоциация XBRL. Банк России создал некоммерческую ассоциацию, которая собрала вокруг себя сообщество разработчиков программного обеспечения, запустила программу платного тестирования и сертификации этих средств и выдает заключение о соответствии тем требованиям и тем форматам, которые используются в формате отчетности XBRL. В целом ассоциация живет уже достаточно долго, председатель наблюдательного совета там госпожа Юдаева. Можно у нее спросить, чего им стоило это сделать. Но, в принципе, пример есть.

Георгий Ерохин. Прокомментирую. На текущий момент действует требование для финансовых организаций, обязанных соблюдать усиленный и стандартный уровень защиты информации, привлекать к проведению оценки по ГОСТ Р 57580.1-2017 проверяющие организации, которые имеют лицензию ФСТЭК по технической защите конфиденциальной информации.

Рекомендовать конкретные проверяющие организации, которых лучше привлекать для оценки соответствия ГОСТ 5780.1-2017, Банк России не сможет с учетом того, что это является вмешательством в рыночные взаимоотношения.

Сейчас в Банке России проводится работа над тем, чтобы выработать концепцию совершенствования системы проведения внешней оценки, в частности оценки соответствия ГОСТ Р 57580.1-2017. Работа направлена, в первую очередь, на то, чтобы определить стандарт, согласно которому будут вести свою деятельность организации, привлекаемые для проведения оценки по ГОСТ Р 57580.1-2017. Различные способы того, каким образом создать условия для совершенствования системы проведения внешней оценки сейчас прорабатываются. Так как конечные решения на данный момент еще не сформулированы, озвучить их здесь не представляется возможным.

Но хотелось бы отметить, что в первую очередь Банк России стремится определить стандарт, которому проверяющая организация должна будет дополнительно соответствовать. Планируется, что при привлечении проверяющих организаций, чья деятельность соответствует стандарту, результаты оценки соответствия ГОСТ 57580.1-2017 будут признаваться Банком России безусловно достоверными.

Отчет, который получает некредитная финансовая организация по результатам оценки, предоставляется в Банк России в форме отчетности. Эти результаты используются Банком России для того, чтобы оценить соблюдение отдельных требований Положения Банка России № 757-П.

На данном этапе механизма дифференциации результатов оценок в зависимости от того, какой проверяющей организацией проведена оценка, не предусмотрено. В этой связи получаемые Банком России результаты оценки по ГОСТ Р 57580.1-2017 рассматриваются в равной степени достоверными.

Михаил Шабанов. Понятно, спасибо!

Да, мы эту тему начинали продвигать в Центральном банке еще в 2019 году. Но где-то примерно в 2020 году, к сожалению, пришло понимание того, что это будет нерыночный метод. И тогда от этой идеи отказались. Так что снова поднимать эту тему достаточно сложно.

Другой вопрос, соглашусь с Сергеем, что, может быть, опыт XBRL как-то

можно было бы использовать не в самом Банке России, а через некоммерческие организации или объединения.

Не знаю, может быть, имело бы смысл отдать это на откуп саморегулируемым организациям либо еще какой-то ассоциации, которая бы объединила лицензированные ФСТЭК-ом компании. Объединила именно те компании, которые специализируются на проверке соответствия некредитных финансовых организаций требованиям кибербезопасности. Возможно, и кредитных организаций. Но нам важнее, конечно, некредитные финансовые организации.

Сергей Демидов. С другой стороны, когда нужно будет подтянуть какой-то рейтинг, а на рынке умеют это делать всего пять организаций, ты не сможешь найти шестую, которая тебе поставит нужную оценку. Здесь любые ограничения всегда работают в обе стороны.

Михаил Шабанов. Да, это чревато. Все так.

Коллеги, еще какие-то мысли, идеи, предложения имеются по этой теме?

Сергей Демидов. В конце всех озвученных вопросов обсуждали, как жить с запретом ПЭП (буду называть соответствующий документ письмом). Это действительно серьезная головная боль. И, собственно говоря, в отношении этого письма сегодня звучали два вопроса: во-первых, почему получилось так, что предварительного обсуждения ни в каком из известных нам кружков не велось, а во-вторых, оно (письмо) сильно сейчас противоречит реальной практике. И я однозначно понимаю, что многие организации сейчас просто умышленно закроют глаза. Потому что идея встроить криптографию, например, в мобильные приложения, включая приложения под Apple, которые пока еще используют граждане Российской Федерации, выглядит пока не очень реализуемой. Поэтому хочется понять.

При этом все-таки с точки зрения буквы закона изначально, когда обсуждали этот пункт 757-П, всегда имели в виду, что под имитозащитой имеется в виду RSA-криптография. Именно за счет того, что тогда все понимали, что SSL-сертификаты (сейчас RSL-сертификаты) продолжают использоваться, в том числе, Банком России. Личный кабинет Банка России использует, насколько я помню, SSL-сертификат. И вместе с тем вышло вот это письмо, которое, по сути, запрещает эту практику и заставляет переходить на ГОСТ TLS.

Георгий Ерохин. В настоящее время в Положении Банка России № 757-П предусмотрено, что в целях обеспечения целостности электронных сообщений и подтверждения их составления уполномоченным на это лицом, должны использоваться либо УКЭП, либо УНЭП, либо иные СКЗИ с имитозащитой и аутентификацией отправителя. Хочу отметить, это требование касается только организаций, которые реализуют стандартный и усиленный уровень защиты информации по ГОСТ Р 57580.1-2017, при обработке защищаемой информации. Виды защищаемой информации перечислены в явном виде в Положении Банка России № 757-П.

В нашем понимании, используя ПЭП, мы не сможем обеспечить целостность, так как ПЭП может быть реализован различными способами реализации этого механизма. В этой связи для того, чтобы целостность электронного сообщения была обеспечена, предусматривается необходимость применения СКЗИ с функцией имитозащиты и аутентификацией отправителя наряду с ПЭП.

Сергей Демидов. В письме употребляется слово «сертифицированная». Оно ключевое и оно все ломает. Потому что GlobalSign (я проверил), который используется сейчас порталом 5 Банка России, ни разу не сертифицирован, насколько я понимаю. А вы говорите, что все вебы PIA(?), которые сейчас используются на финансовом рынке (как кредитными, так и некредитными финансовыми организациями), должны резко стать сертифицированными. Хотя даже для госорганов с учетом GlobalSign, это, по всей видимости, не является требованием. И вот именно это проблема. ПЭП не обеспечивает целостность, поэтому трафик все время гнали в SSL-каналах, но сертификаты там такие же GlobalSign, как и у ЦБ.

Георгий Ерохин. Относительно вопросов сертификации в настоящее время в Положении Банка России №757-П установлена обязанность использования сертифицированных средств защиты информации в отношении тех СКЗИ, которые разработаны и произведены на территории Российской Федерации. Соответственно, если такая разработка ведется в соответствии с ПКЗ-2005, то соответствующие СКЗИ должны пройти сертификацию уполномоченного органа.

Сергей Демидов. Это, к сожалению, нереализуемая задача в рамках ПКЗ-2005, должен быть контроль встраивания, и, очевидно, что на обработку сертификатов, выданных GlobalSign, вам никто исходный код не передаст. И веб-сервисы, которые обеспечивают работу международных RSA-сертификатов, в большинстве своем, на 99%, все-таки писаны не здесь. Это действительность текущего рынка. Можно сейчас открыть сайт Минцифры в режиме девелоперс(?) и посмотреть, что там ровно те же самые веб-сервисы, и они не канонические, как принято сейчас говорить, а выпущены где-то там, за нашими рубежами.

У нас наверняка будет какой-то, что называется по-русски, аутком с сегодняшней встречи. Позволю себе

освежить в памяти вопросы, которые мы сегодня обсудили и по которым хотелось бы получить обратную связь, а коллеги добавят. Хотелось бы все-таки получить либо разъяснение, либо уточнение, либо возможность переговоров, потому что проблема выглядит общей. Наверное, остальные боятся ее поднимать открыто. А мы готовы обсудить. Но хотелось бы с кем-то сначала проговорить, что все-таки запрещено, а что разрешено. И что произойдет, если вдруг мы действительно запретим обрабатывать веб-сервисы с использованием RSA-сертификатов на ИБ криптографии. Вот это очень важно. Это требует не ответа, а желания проработать.

Второе, что сегодня обсуждали: у рынка есть желание наладить регулярное институализированное общение в виде комитета либо группы, в рамках которого можно было бы предметно обсуждать проблемы именно НФО. Потому что ТК 122 хороший орган, но он слишком большой. И внутри самого Технического комитета существуют слишком противоречивые мнения, для того чтобы он объективно учитывал потребности, которые возникли на рынке. Вместе с тем, такой орган (если и когда он будет создан), в том числе, мог бы включать в повестку обсуждение стратегии. А не просто получать на согласование правку запятых в нормативном акте, который находится уже в высокой степени готовности. Интересы сектора должны учитывать, в том числе при разработке нормативного регулирования или стратегий нормативного регулирования, если хотите.

Вот два пункта, которые я запомнил.

Михаил Шабанов. Сергей большое спасибо. Но мы еще не закончили, у нас есть еще один вопрос…

Сергей Демидов. Я просто к тому, что иногда пора давать промежуточные итоги. Позволил себе объединить темы, просто чтобы сейчас мы не перекидывались тезисами впустую. Мы обозначили проблему, не требуем срочного ответа, но желательно ее где-то обсудить.

Михаил Шабанов. Я согласен, да, но хочу напомнить, что мы на заседании комитета приняли решение, о проведении в мае встречи (в рамках комитета НАУФОР) на которую мы хотим пригласить компании разработчики СКЗИ и провайдеров различных IT- услуг, таких, как АРКА и прочих. Тех, кто разрабатывает клиентские приложения для проведения различных финансовых операций. Для того чтобы понять, как они видят «картину мира» с учетом выхода этого Письма и исполнения требования 1.9 пункта 757-П. Потому что здесь безусловной есть, о чем поговорить, и проблема существует. И как-то для всех оказалось неожиданным это мартовское письмо.

Вопросы импортозамещения

Коллеги, из третьей темы, как мне кажется, есть смысл обсудить только вопрос импортозамещения, поговорить именно об этом. О том, что касается программного обеспечения и «железа». Какие здесь есть проблемы, и помогает ли, скажем так, заполнение тех же функциональных технологических карт (ФТК)? удалось ли всем (включая НФО) это переварить и понять, куда мы движемся? Есть ли решения, есть ли понимание задач, которые сейчас стоят перед рынком. Давайте поговорим об этом.

Пожалуйста, коллеги. Или уже все «импортозаместились», заполнили функциональные технологические карты и успокоились на этом?

Сергей Демидов. Здесь основной вопрос к коллегам из ЦБ относительно многократно озвученного тезиса о том, что будут введены предельные сроки перехода на преимущественное использование отечественного программного обеспечения. Вместе с тем двигается законодательная инициатива внутри Государственной думы, там до 3 мая происходит сбор обратной связи от профильных комитетов. Это значит, что есть шанс попадания этого законопроекта во второе чтение еще в весеннюю сессию. То есть достаточно быстро может случиться, что Банк России получит полномочия установки сроков. Напомню, сейчас у Банка России нет права устанавливать сроки по импортозамещению. Но этот законопроект продвигается.

Соответственно, вопрос: все-таки на основе чего будут ставиться эти сроки? Будет ли предварительная консультация с рынком, опять же желательно иметь какой-то совещательный орган. Комитет финансов похож в этом смысле на Технический комитет 122, он очень большой. Поэтому хотелось бы все-таки предметно проговорить тему в более узком составе, особенно в разрезе разных категорий этого участия.

Вот, собственно, основной вопрос: когда будут сроки?

Михаил Шабанов. Спасибо, Сергей. Я бы со своей стороны хотел еще обратить внимание вот на что. Когда мы встречались последний раз с представителями Департамента информационной безопасности, то речь шла о технологических картах (ФТК. О том, что у Банка России (у ДИБа, в частности) нет возможностей полностью проверить карты, которые подготовили и заполнили некредитные финансовые организации. Но вот заполнение прошло, мы даже дали какие-то дополнения к процедуре. Однако нет обратной реакции. Кто будет осуществлять проверку и выставлять свои замечания по этим технологическим процессам, я так и не понял. Ответной реакции пока нет. Карты заполнили, переправи-


КРУГЛЫЙ СТОЛ
5.04.2023
ВОПРОСЫ ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ ДЛЯ НЕКРЕДИТНЫХ
ФИНАНСОВЫХ ОРГАНИЗАЦИЙ

ли. Что дальше? Мы ждем, что кто-то будет проверять. А кто это будет делать, если тот же Уваров [директор Департамента информационной безопасности Банка России. — прим. ред.] говорил, что нет сил и возможностей проверить все ФТК; что касается ЦБ, то (через Комитет финансы) работа организована и ведется для системообразующих финансовых организаций (кредитных и некредитных). А вот что касается членов НАУФОР, средних и небольших финансовых организаций, то с ними, работа организована слабо, исходя из того, что сами саморегулируемые организации разберутся со своими членами. Но как они разберутся? Вроде бы полномочий не было дано, реальных предложений в этом плане не прозвучало.

Антон Чернодед. Относительно небольших организаций. Есть нормативное требование в части технологической независимости значимых объектов КИИ. Небольшие организации не обладают значимыми объектами КИИ, поэтому им жить несколько проще.

В части валидации технологических карт. Вы хотите, чтобы Банк России сделал валидацию по каким критериям?

Михаил Шабанов. Ну для чего-то же мы это делали. Наши некредитные финансовые организации заполняли карты (ФТК), мучились, было много проблем, они просили дать разъяснения, как заполнять правильно. Оказалось, что все очень непросто. Но все-таки, большинство заполнило эти технологические карты. Теперь хочется понять, что дальше? Компании просто для себя это делали, чтобы «выпустить пар» или понять, что как у них внутри организовано в плане кибербезопасности? Либо все-таки будет какая-то проверка, будут сделаны какие-то замечания. И после того, как проверка пройдет, будут разрабатываться уже «дорожные карты» на основании выявленных процессов. Ведь после проверки готовится «дорожная карта», правильно? Как я понимаю, процесс именно так подготовлен? Если Банк России не готов был проверять (по крайней мере это так звучало, может, я неправильно понял, но это звучало так), то что дальше?

Антон Чернодед. В рамках Департамента информационной безопасности был создан в прошлом году отдельный центр импортозамещения, его возглавляет наш коллега Морозов Савва Александрович. К сожалению, на все вопросы по его направлению я ответить не смогу, но отвечу в части той информации по инфраструктуре, которая собиралась.

Сейчас для некредитных финансовых организаций вышли формы отчетности по операционной надежности. Для большинства некредитных финансовых организаций, за исключением страховых, они вступили в силу 1 апреля этого года. Организации должны будут представить информацию в июле месяце, после завершения второго отчетного квартала. В рамках данных форм отчетности будет собираться информация, в том числе по информационной инфраструктуре, в различных разрезах. Фактически работа, которая проводилась в рамках импортозамещения, была обкаткой этих вопросов, и мы ее сейчас отдельно учитываем.

В дополнение к этим формам отчетности сейчас планируется выход методических рекомендаций, которые будут более детализировано прописывать, в каком формате вести учет объектов информационной инфраструктуры. Здесь регулятор будет учитывать опыт, который был реализован в рамках импортозамещения. Одна из целей сбора информации об инфраструктуре — как раз вопросы импортозамещения. После чего эта информация будет в рамках формы отчетности собираться на регулярной основе, и планируется валидация этой информации, чтобы получать с каждым кварталом более качественные данные.

В части формирования «дорожных карт» поостерегусь комментировать, чтобы не ввести вас в заблуждение. У организаций, которые непосредственно участвуют в работе в рамках Отраслевого комитета финансов, есть контакт нашего коллеги, он может все прокомментировать более детально.

Михаил Шабанов. Хорошо. Спасибо!

Георгий Ерохин. Я дополнительно прокомментирую относительно целей этой деятельности. Законопроектом предусматриваются полномочия Банка России в области обеспечения технологического суверенитета, с целью поддержания обеспечения операционной надежности. Следовательно, какие риски усматриваются? В плане идентификации критичной архитектуры целью являлось определение насколько она зависима от иностранных поставщиков, которые в тот или иной момент могут прекратить либо уже прекратили свою деятельность на территории Российской Федерации. Следовательно, предпринимаемые Банком России действия направлены на то, чтобы оценить как развитие текущей ситуации влияет на деятельность финансовых организаций.

Следующий шаг по построению «дорожных карт» подразумевает, что финансовая организация в плановом порядке вырабатывает подход, который позволит ей осуществить переход, минимизировав влияние на целевые показатели операционной надежности, которые предусмотрены нормативными актами Банка России.

Михаил Шабанов. Спасибо!

Сергей Демидов. Небольшой комментарий. Буквально недавно обсуждали

изменения в требования к проведению операционного аудита в отношении центрального депозитария. Там в документ тоже изначально закладывался смысл, что, типа, нужно обязательно убрать зависимость от иностранных компонентов. Но, с другой стороны, мы оказались в абсолютно идентичной истории. Если говорить про инфраструктуру Банка России (я сейчас не буду вываливать все инсайды, которыми обладаю), то очевидно, что зависимость инфраструктуры Банка России от иностранных технологий тоже велика. И когда мы обсуждали этот документ вместе с коллегами из Департамента информационной безопасности, то достигли взаимопонимания. Основа взаимопонимания такова: вместо планов заместить какой-то объем технологий к какой-то дате, наверное, организации было бы правильнее показать, что она умеет бороться с этим риском. А с риском можно бороться по-разному. В том числе сохраняя часть компонентов, но, например, уведя их из критически важных элементов инфраструктуры, либо запустив серые схемы обновления. Тем не менее, этим риском можно управлять.

Здесь хочу высказать одно из пожеланий, которое можно было бы обсудить, если бы существовал тот самый регулярный кружок по проблемам НФО. Требования обязательного замещения в формате «заместите обязательно, потому что иначе ой-ой-ой и ужас-ужас» лучше бы поменять на «ОК, покажите, что вы умеете управлять этим риском». Мы все оказались в одной ситуации. Можно сделать методологические рекомендации, в которых прописать разные элементы управления риском (серые обновления, изоляцию отдельных элементов и так далее), это более гибкий метод.

А ведь есть такие команды (не буду называть), где, если появл ется какая-то угроза, то они на третий день выпускают серый стандарт и говорят, что это драфт, но уже начинают руководствоваться этим драфтом. Там требование к безопасности Кубера появляется, извините, на второй день. А где требования Банка России к безопасности Кубера? Нигде. Причем сама технология используется уже везде. Думаю, процентов 80 финансового рынка используют эту технологию, в том числе в корпоративных системах. [*Kubernetes, Кубер — это ПО, позволяющее гибко управлять контейнеризированными приложениями. — прим. ред.*]

Поэтому я предлагаю переходить от механизма запретительных норм на механизм управления риском, о чем Андрей говорил в самом начале. Это тоже пожелание. Вырабатывать такие нормы управления риском можно путем здравого обмена экспертным мнением в рамках какого-то органа, где такое возможно.

Михаил Шабанов. Спасибо, Сергей!

Андрей Ковешников. Поддержу Сергея. Вопрос в том, что мы сейчас должны выработать план и его придерживаться. Сейчас, на мой взгляд, есть три основных вопроса, которые требуется решить.

Первый — это отсутствие отечественных микропроцессоров как таковых, в рамках которых мы можем развернуть и импортозаместить все пользовательское оборудование, которое у нас есть. Что будет сделано энное количество микропроцессоров, которые будут работать в роутерах, еще где-то, — мы в это верим. Что можно заместить все компьютеры, все железо в течение двух лет, — мы в этом сомневаемся.

Второй момент: очень большой сегмент импортозамещения сейчас зиждется именно на перекомпиляции свободного программного обеспечения с некоторыми доработками. И когда мы говорим про серьезные доработки в части замкнутой программной среды Astra Linux, то возникает вопрос, что даже 1С с ним работать на текущий момент не может. А если она и сможет работать, то в рамках работ для госзаказчиков, типа «Росатома» или Минфина, или в Федеральном казначействе. Для отраслевых решений, для того же финансового рынка, пока даже речи о сертификации 1С:СЛК под защищенную систему Astra Linux нет.

И третий ключевой момент: российский финансовый рынок очень сильно зависит от вендоров программного обеспечения, которые не подпадают под регулирование Банка России. Влиять на них мы можем только через профильные ассоциации. Да, можно сказать, что есть другие заказчики, для общего программного обеспечения это пройдет. Но что делать с отраслевыми программными средствами — вопрос, конечно, очень непростой. И надо на него искать ответ всем, начиная от разработчиков, которые могут вымереть, если все клиенты уйдут. И компаниям надо искать, на что переходить, так же как Банку России искать, кого в этом случае он будет регулировать.

Михаил Шабанов. Спасибо, Андрей! Коллеги, есть еще какие-то идеи, мысли?

Андрей Киселев. Небольшой комментарий. Вообще нужно еще определение, что есть отечественная разработка. Тот же Astra Linux: ядро у него Linux, оно не отечественное. Open source (открытое программное обеспечение — программное обеспечение с открытым исходным кодом) относится ли к отечественным, можно ли его использовать, нельзя ли?

Ну, и такой сюжет: один из отечественных производителей оборудования нам говорит: «Хотите, поставим Hewlett-Packard, хотите, поставим Dell; наклеим свой «шилдик» и будут у вас как бы отечественные сервера». Будет ли это оборудование отечественным или нет?

Михаил Шабанов. Не будет. Это уже оговаривается, есть уже определение, что является российским, что российским не является.

Сергей Демидов. Давайте будем реалистами: в реестре Минцифры значится 50 российских операционных систем. Я этому верю и не хочу дальше лезть.

Второе. Проблема Open source существует и, к сожалению, сейчас решается в плоскости не Банка России. Банк России сейчас чуть-чуть передал пальму первенства Минцифры, которое (в силу распределения обязанностей внутри правительства Российской Федерации и всех ФАИПов) лидирует в этой теме. И внутри Минцифры вопрос регулирования опенсорса попал в ту ветку, которая менее доступна нам для контактов. Поэтому ЦБ помогает.

В чем проблема? Проблема в том, что на Отраслевом комитете «Финансы», на котором многие из нас присутствуют, проводился опрос. И выяснилось, что от 70% до 90% опенсорса используется финансовыми организациями, в том числе на тех элементах, которые попадают под требования 757-П и 683-П. Что это значит? Что, в принципе, под эти требования подпадает основной объем открытых исходников, которые использует индустрия. При этом код, очевидно, не российский. Тут же ко мне даже в Минцифры пришли люди на уровне замминистра и сказали: «Да вы «отфоркайте» всё» [*форк — это собственная параллельная версия какого-то софта. — прим. ред.*]

Дальше я начал чисто математически показывать, что в России не хватит программистов отфоркать Кубера, что даже если мы сейчас в моменте сделаем форк, то через полгода эта версия будет дырявой, меня взломают, и мы создадим угрозу всей инфраструктуре. Что даже если мы объединимся со Сбером и ВТБ, в которых работают десятки тысяч программистов, и там «отфоркаем», то все равно мы не сможем дальше жить без международного опенсорса. Либо мы сознательно себя погружаем в XX каменный век и начинаем дальше программировать на перфокартах. Но мы не хотим, наверное, этого отставания. Здесь большая проблема, она измеряется сотнями миллиардов рублей, если считать затраты на всю индустрию. Понимаю, что коллеги из Банка России, наверное, даже больше, чем Минцифры, нас понимают и осознают масштаб проблемы.

Но проблема существует.

Второе: проблема аутсорсинга. Не хватает российского оборудования. Эта тема, в принципе, должна была решиться в предыдущем году. У отдельных руководителей внутри ЦБ даже стоял КР урегулировать аутсорсинг (аутсорсинг — это не только персонал, это, в том числе, облака). К сожалению, в прошлом году она так и не была урегулирована. Но сейчас она опять появилась, как раз в том стратегическом документе, который был представлен на Уральском форуме. Все-таки нам обещают, что в каком-то виде (именно из-за того, что оборудования недостаточно, вычислительных ресурсов недостаточно) облака для финансового сектора должны быть разрешены. Надеюсь, в том числе для сведений, которые составляют банковскую и иную тайну в силу законодательства.

На мой взгляд, здесь видны направления, в которых идет Банк России. Конечно, хотелось бы, чтобы мы получали ответы более быстро.

Михаил Шабанов. Спасибо, Сергей!

Коллеги, будут какие-то комментарии? Нет? Спасибо!

Коллеги, мы с вами работаем уже почти два часа (без пяти минут). Я предлагаю на этом, наверное, завершить заседание нашего круглого стола. Хочу выразить благодарность представителям Департамента информационной безопасности Банка России за активное участие. Вам, коллеги, тоже выражаю благодарность. Надеюсь, что опыт нашей дискуссии будет полезен всем. Надеюсь, что мы продолжим встречаться. Всем хорошей, плодотворной работы. До свидания. ◻