Значение информационных технологий растёт по всем направлениям государственного регулирования, контроля и надзора на финансовом рынке: в его развитии отрасли, расширении доступности сервисов, в отношении профессиональных участников и в защите прав потребителей. Всё больший удельный вес занимает электронный документооборот, а бумажный сокращается.

Однако вместе с этим растут и киберугрозы. Растущая зависимость от технологий, а также увеличивающийся масштаб их применения в различных секторах экономики означают потенциальное увеличение киберрисков в ближайшем будущем. Поэтому возрастает значение управления такими рисками, выстраивания соответствующих систем.

СТРАТЕГИЮ ОБЕСПЕЧИТЬ БЕЗОПАСНОСТЬЮ

В наши дни киберпреступность «обходится» глобальной экономике в $ 445 млрд ежегодно *(The Center for Strategic and International Studies and McAfee).* Риски масштабных кибератак названы наиболее значимыми рисками для ведения бизнеса в 18 странами с ведущими экономиками, включая G7 *(The World Economic Forum's 2016 Global Risk Report).* Порядка $ 294 млрд ВВП крупнейших городов мира подвержены масштабным кибератакам *(Lloyd's City Risk Index).*

Для реализации упомянутых функций Банка России **в сфере развития финансового рынка была принята стратегия - документ под названием «Основные направления развития финансового рынка на период 2016-2018 годов».** В нём указаны десять основных направлений работы, и практически в каждом всё больше применяются информационные технологии, которым сопутствуют киберриски. Перечисленные направления могут развиваться только на базе учёта подобных рисков и их минимизации. В полной мере относится и к отдельным инновационным финансовым продуктам.

Принципиально важно заниматься киберрисками на всех уровнях инфраструктуры финансового рынка – как банков, так и некредитных финансовых организаций, включая организаторов электронных торгов, бирж, депозитариев, которые работают с огромными базами критических данных. Эти участники рынка, в частности, биржи, в свою очередь прилагают значительные усилия для управления операционными киберрисками.

Местами выстроенные ими системы обеспечения информационной безопасности не хуже, чем у крупных банков, а по ряду показателей и лучше. Потому что эта работа курируется на уровнях правления, совета директоров, в неё вкладываются солидные средства. Что значит идти в ногу со временем, соответствовать современным требованиям к развитию информационных технологий.

ЭЛЕКТРОННОЕ ОСАГО: УДОБСТВА БЕЗ ИЗДЕРЖЕК

Управление киберрисками важно как для организаций – участников рынка, так и для отдельных инновационных финансовых продуктах. Так, среди электронных средств платежа, электронных технологий в практике продаж и предоставлении финансовых продуктов и услуг присутствует **электронный полис ОСАГО.** С 1 января 2017 года такой полис стал обязательным для страховых компаний, работающих на рынке ОСАГО, они обязаны любому потребителю его предоставлять.

Возможности электронного полиса ОСАГО позволяют профессиональным участникам финансового рынка не тратиться на содержание офисов и армии страховых агентов: такие

услуги можно предоставлять через интернет. Но вместе с тем возникают серьёзные проблемы, связанные с возможными мошенничествами. Появились поддельные сайты страховых компаний, где продавались фальшивые электронные полисы ОСАГО. Злоумышленники даже сделали клон сайта Российского союза автостраховщиков.

Задачей Банка России - Службы по защите прав потребителей финансовых услуг и миноритарных акционеров, а также Департамента страхового рынка Банка России - является обеспечение непрерывности деятельности сайтов страховщиков, через которые потребитель может эту услугу приобрести. Совместные действия с участниками рынка позволили оперативно заблокировать деятельность упомянутого мошеннического интернет-ресурса. Но ясно, что требуется постоянный мониторинг интернета и готовность к блокировке новых попыток подобных мошенничеств.

Следующий риск - высокая убыточность реализации электронных полисов страхования недобросовестным клиентам, скрывающим предыдущие страховые случаи. Необходима процедура оперативной дистанционной проверки «страховой истории» покупателя электронного полиса ОСАГО.

Ещё один риск – нестыковка баз данных автостраховщиков и дорожной полиции. По закону, купив электронный полис, достаточно предъявить его распечатку. Были случаи, когда сотрудники дорожной полиции не принимали такие распечатки, а требовали предоставить полис на бланке. Чтобы потребитель доверял электронным полисам ОСАГО, федеральные органы исполнительной власти, включая Банк России, должны навести порядок в этой процедуре.

В целом реализация электронных полисов ОСАГО стартовала удовлетворительно, сняв ряд проблем в регионах. За первые полтора месяца 2017 года было продано около 300 000 полисов – очень много. Это столько же, сколько за весь прошлый год, когда страховые компании предлагали этот продукт не в обязательном, а в добровольном порядке. Теперь вопрос в том, насколько хорошо – удобно для потребителей работают сайты страховщиков.

Для контроля продажи электронных полисов ОСАГО Банком России созданы специальные алгоритмы проверки, с использованием автоматизированного мониторинга и анализа. Есть процедура запроса у страховой компании журналов электронных событий, в том числе сведений, кто, когда заходил на сайт, сколько времени там провёл т.п. Для того, чтобы выявить факты проблем с покупками, установить сторону ответственности – покупателя или продавца, выяснить причины не предоставления услуги.

ПЕНСИОННОЙ ПРИВАТНОСТИ - НЕПРИСТУПНОСТЬ

Ещё один пример – задача обеспечить информационную безопасность процесса **инновации системы обязательных накоплений, использования индивидуального пенсионного капитала.** Предполагается создание **единого пенсионного администратора - специализированной организации**, которая будет вести базу данных, предоставлять информацию гражданам и негосударственным пенсионным фондам о наличии, принадлежности и характере пенсионных прав, операциях с ними. Такой оператор-администратор может быть создан на базе федерального органа исполнительной власти или государственной корпорации, возможно как отдельное юридическое лицо.

Очевидно, что такой единый пенсионный администратор может эффективно работать только посредством электронных технологий. Множество проблем Пенсионного фонда России, пока ведущего учёт пенсионных прав граждан, связано с большой долей бумажного

документооборота, недостаточным использованием автоматизированных информационных систем. Многие из тех, которые уже работают, устарели, децентрализованы.

Бумажный век уходит в прошлое. Создаваемый пенсионный администратор должен работать посредством больших баз данных, самыми передовыми информационными технологиями. Востребован высокий уровень защиты от несанкционированного вмешательства, способного привести к нарушениям функционирования, искажению данным, кражам информации и другому ущербу. Вопросы киберрисков встают остро и выходят на передний план.

Один из таких вопросов – **безопасность личных кабинетов клиентов.** На смену бумажному документообороту всё больше приходит электронный, а почтовому адресу офиса или квартиры – личный кабинет. Сегодня предписание должно в электронном виде помещаться в личный кабинет, и, согласно действующим общим правилам, профессиональным участникам рынка ? страховой компании, пенсионному фонду, другой некредитной финансовой организациям - даётся 24 часа на ознакомление. Предполагается, что в течение этого срока отправление будет доставлено адресату.

С одной стороны, такой порядок упрощает всем жизнь. Сокращаются организационно-административные расходы и государственных регуляторов, и профессиональных участников рынка. С другой стороны, серьёзно встаёт вопрос о поддержании личных кабинетов в нормальном рабочем состоянии, об обеспечении их непрерывной деятельности. Банк России со своей стороны должен обеспечить информационную безопасность этих сервисов, и необходимая для этого работа ведётся.

ГОТОВИТЬ НОВЫХ ПРОФЕССИОНАЛОВ

Противодействие киберпреступности - отдельное направление в рамках развития финансовых рынков. Порой к операционным рискам относятся как к чему-то второстепенному по отношению к финансовым рискам. Риски операционные редко делят на различные детализированные «подриски», каждый из которых должен специально обрабатываться. Наверное, это именно тот случай, когда подход и государственного регулятора, и участников рынка заслуживает коренного пересмотра.

Благодаря повышению ответственности к регулированию операционных рисков, в том числе используя механизмы саморегулирования, можно заметно повысить эффективность противодействия киберпреступности. У Банка России уже есть неплохие наработки, нужно активизировать и работу отраслевых саморегулируемых организаций в этом направлении.

Развивая нормативно-правовую базу, контрольно-надзорную деятельности, мы можем вывести нашу работу на новый уровень. А именно, **ориентируя профессиональных участников финансового рынка на целенаправленное формирование политик и процедур управления операционных рисков – киберрисков.** Тех, что существуют по причине активности киберпреступников, «высокотехнологичных» мошенников.

Рассмотрим подробнее вопрос **программы обучения специалистов.** Точно так же, как в компаниях действуют подразделения и специалисты по информационной безопасности, должны работать и сотрудники, занимающиеся противодействием киберпреступности, кибермошенничествам.

Это новая специализация, но некоторое время назад на финансовом рынке не было и таких профессий, как актуарий ? страховой математик или специалист по финансовому моделированию. Сегодня без таких сотрудников немыслима нормальная работа банков,

страховых компаний, пенсионных фондов. Востребованы специалисты, которые умеют создавать внутренние рейтинговые модели, необходимые для управления рисками, включая киберриски.

Однако к такой профессии пока целенаправленно не готовят! Впрочем, таким же образом государственному регулятору до сих пор не хватает профессиональных специалистов по надзору. А страховым компаниям – специалистов по медицинскому страхованию, которые бы обладали компетенциями и в страховом деле, и в медицине. Организация подготовки профессионалов востребованных на рынке профилей – актуальная задача, её решение – вопрос времени.

Хотелось бы, чтобы специалистов по такому направлению кибербезопасности, как киберриски, начали готовить по возможности скорее, начиная с программ профессиональной переподготовки. В текущем 2017 году Банк России будет участвовать в разработке профессионального стандарта «Специалист по информационной безопасности». Этой работу ведёт комиссия по банкам и банковской деятельности Российского союза промышленников и предпринимателей, с участием представителей финансового рынка.

«ВСЕОБУЧ» ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Следующее важное направление обеспечения стратегия развития финансового рынка - повышение финансовой грамотности его участников, пользователей и клиентов. За происходящими изменениями, не во всём поспевают не только граждане, но и корпорации, не в полной мере осознавая новые финансовые инструменты и процедуры. Возникают конфликты, связанные с продажами профессиональными участниками рынка ценных бумаг сложных финансовых продуктов предпринимателям. Дело доходит до судебных разбирательств, в ходе которых выясняется, что продавцы не полностью раскрыли покупателям информацию, не объяснили всю сложность продукта, его функционирования.

Подчёркиваю, что покупатели – это юридические лица, сотрудники которых являются профессионалами. Что же тогда говорить о потребителях финансовых услуг - физических лицах? Очевидно, что они – «слабое звено», в том числе в вопросах безопасности. Имеет смысл на определённое время административно ограничить их доступ к сложным, структурированным финансовым продуктам. До тех пор, пока не будет создан эффективный механизм информирования потребителей обо всех главных особенностях новых финансовых продуктов, то есть повышения их финансовой грамотности, включая вопросы безопасности.

Эти вопросы с точки зрения защиты прав потребителей подведомственны Банку России, так называемому поведенческому надзору. Краеугольным камнем является защита прав потребителей: оказание качественных услуг, раскрытие полной существенной информации о продукте. В доступной, понятной форме, чтобы такие сведения не нужно было долго-долго искать и вчитываться в пресловутый «мелкий шрифт».

Такая задача несколько отличается от классического надзора за банками, страховыми компаниями, пенсионными фондами, у которого другая задача - обеспечить устойчивость финансовую и бизнес-процессов в целом, чтобы они могли должным образом исполнять свои обязательства. Поведенческий надзор государственного регулятора имеет другую цель: чтобы юридические лица оказывали потребителям качественные финансовые услуги, что предполагает раскрытие важной информации. В наши дни не выполнить этого считается не меньшим риском, чем не обеспечить устойчивость бизнес-процессов.

В 9-11 классах средних образовательных школ внедряется учебный курс финансовой

грамотности, подготовленный Банком России совместно с Министерством образования и науки РФ. Пилотный проект был выполнен успешно, и к 2019 году этот курс будет преподаваться во всех школах, в разделе «Экономика» предмета «Обществознание».

Уже сегодня понятно, как дальше должна развиваться образовательная работа в финансовой сфере. Школьный курс финансовой грамотности посвящён чисто финансовым инструментам: вкладам, облигациям, ценным бумагам. Уже ясно, что не меньше внимания должно быть уделено вопросу, как их использовать.

Пока что в школьном учебнике, - не в методическом комплекте для учителей, а в самом учебнике, - про киберриски информационных технологиям практически не говорится. Очевидно, что применение информационных технологий в финансовой сфере становится практически всеобъемлющим. Значит, школьный курс финансовой грамотности должен рассказывать о том, как они работают, о киберрисках, о мерах информационной безопасности. Далее, следующий шаг – распространение такого курса на высшие учебные заведения. И на взрослых, включая «ликбез» информационной безопасности для пенсионеров.