

Риски быстрого реагирования

«Агрессивная внешняя среда» и бурное развитие технологий приводят к тому, что какие-то из операционных рисков периодически выходят на передний план. «Б.О» расспросил экспертов об основных вызовах для отрасли

Текст
ЕКАТЕРИНА КАЦ,
ОБОЗРЕВАТЕЛЬ «Б.О.»

«С

егодня, как и всегда, актуальными остаются вопросы обеспечения соответствия системы управления рисками банков состоянию внутренней и внешней экономической среды России: эффективной адаптации процессов управления ими в условиях изменения бизнес-процессов, а также предотвращения потенциальных финансовых потерь посредством разработки и реализации комплекса мер, направленных на снижение негативного влияния неопределенности», — перечислил Борис Богоутдинов, управляющий партнер Консалтинговой компании «2Б Диалог».

Профильные специалисты финансовых структур видят, как в их организациях меняются приоритеты и перестраиваются бизнес-процессы под текущие геополитические и макроэкономические условия, а также под новые регуляторные требования, напрямую с этим не связанные. А некоторые ранее волновавшие специалистов проблемы уже «отработаны» настолько, что не представляют угрозы — как, например, контроль эффективности работы службы риск-менеджмента в условиях удаленной работы.



Регламентировано «Базелем»

Что бы ни происходило в России и в мире, базельские нормативы в этой части отечественный регулятор вводит. «Текущие требования ЦБ предписывают строгое выполнение Положения № 716-П «О требованиях к системе управления операционным риском в кредитной организации и банковской группе», вступившего в силу 1 октября 2020 года», — напомнил Борис Богоутдинов.

Речь идет как раз о внедрении SMA-подхода (Standardized Measurement Approach), который и должен был стать обязательным для универсальных банков с 2023 года. Впрочем, наиболее продвинутые финансовые структуры получили право работать по-новому досрочно, уже начиная с 2021 года. Первым модель расчета тогда испробовал ВТБ. В банке отмечали среди преимуществ снижение нагрузки на капитал, поскольку подход позволяет рассчитывать величину средств, необходимых для покрытия операционного риска, исходя из статистики внутренних потерь (КВП).

Светлана Белялова, директор департамента управления операционными рисками Росбанка, сейчас называет актуальным для большинства банков в плане операционных рисков именно переход на расчетный КВП.

Регуляторная канва от Центробанка

Вера Замигулова, директор департамента риск-менеджмента Реалист Банка, напомнила, что из-за непредсказуемых событий 2022 года «законодатели и Банк России выпустили существенный объем нормативных актов/законов/постановлений/указов, ограничивающих и изменяющих правила осуществления операций в условиях санкционного давления».

Среди нормативных актов Банка России, которые «задали общую канву, правила и терминологию в части операционного риска», она назвала помимо упомянутого выше Положения № 716-П также:

- Положение № 744-П «О порядке расчета размера операционного риска («Базель III») и осуществления Банком России надзора за его соблюдением», тоже принятое в 2020 году;
- документ, опубликованный в январе и вступивший в силу в октябре прошлого года, — Положение № 787-П «Об обязательных для кредитных организаций требованиях к операционной надежности при осуществлении банковской деятельности в целях обеспечения непрерывности оказания банковских услуг».

К ним прилагаются еще «сопутствующие разъяснения и рекомендации регулятора», добавила эксперт. «Все это задает общие правила игры, но в то же время все «игроки» разные, у каждого свои процессы, распределение функционала, информационные системы, объем и специфика сделок, а также своя база событий операционных рисков и потерь, связанных с этим видом риска. Поэтому каждая кредитная организация индивидуально выстраивает процессы управления операционным риском и подходит к оптимизации бизнес-процессов, базируясь на своем опыте и своей специфике, а также на имеющихся ресурсах, в том числе и финансовых», — подвела итог Вера Замигулова.

Регуляторика как фактор новых рисков

«Регулирование оказывает исключительно положительное влияние. Банкам с долгой историей управления операционным риском появление новых проектов нормативных актов регулятора помогает донстроить действующие процессы», — считают в Банке «ЗЕНИТ». Со стороны подобная перестройка «выглядит» достаточно глобальной: в частности, в «ЗЕНИТЕ» отмечают, что после вступления в силу требования Положения № 787-П по операционной надежности трансформации подверглись процессы не только в профильном под-

разделении, но и в смежных: IT, кибербезопасности, рисков, бизнес-подразделениях.

«Необходимость осуществлять перестройку процессов потенциально может повлечь проявление операционного риска. И чем больше изменений в регулировании, тем выше вероятность ошибки, особенно в ситуации ограниченности времени и ресурсов для проведения адаптивных процедур», — заметила Вера Замигулова. — Очень помогает введение регулятором «моратория»: неприменения мер воздействия к кредитным организациям за те или иные нарушения. Это позволяет в «боевом» режиме совершать операции, выявлять ошибки, которые далеко не всегда обнаруживаются при тестировании, производить доработку систем, а также задавать вопросы регулятору в целях подтверждения своего понимания того или иного аспекта нового нормативного акта в привязке к реальной ситуации и реальному событию».

Смена вендора как вызов

«Для банковской системы в целом основные вопросы, связанные с высокими операционными рисками, лежат в плоскости технологического обеспечения и информационной безопасности организаций, что продиктовано ограничениями, вытекающими из необходимости импортозамещения технологий и оборудования вендоров, прекративших деятельность в РФ», — полагает Светлана Белялова (Росбанк).

В «ЗЕНИТе» говорят, что в прошлом году вопрос импортозамещения автоматизированной системы по управлению операционным риском действительно стоял остро. Но предложений от российских разработчиков было достаточно, чтобы в сжатые сроки провести тендер и выбрать нового поставщика, полностью отвечающего требованиям регулятора и самого банка. Это, впрочем, не значит, что у всех структур сектора было достаточно возможностей, в том числе финансовых, быстро перестроиться.

Борис Богоутдинов тоже оптимистично комментирует вопросы, связанные с оптимизацией бизнес-процессов и повышением эффективности работы систем по управлению операционными рисками в финансовом секторе, в том числе в контексте регуляторных и санкционных изменений. Внедряемые сегодня IT-решения разрабатываются непосредственно под выполнение требований положения № 716-П, поэтому никак не влияют на текущие бизнес-процессы банков, которые перешли на новые СУБД (системы управления базами данных), заверил эксперт.

«Современные IT-системы повсеместно внедряют планы обеспечения непрерывности и восстановления деятельности, а также



результаты тестирования таких планов. Это, в свою очередь, обеспечивает контроль резервных ресурсов, оперативный мониторинг влияния чрезвычайных ситуаций на IT-инфраструктуру банка, — пояснил Борис Богоутдинов. — Процесс импортозамещения IT-систем начался еще в начале 2021 года с постепенного перехода на PostgreSQL как прямую альтернативу Oracle. Это позволяет оперативно регистрировать данные о рисковых событиях, в том числе о причинах их возникновения; о финансовых и нефинансовых последствиях; о страховых и нестраховых возмещениях. Кроме того, крупными банками ведутся мониторинг ключевых индикаторов риска и единый реестр рисков, а также централизация учета планов ОНИВД (обеспечения непрерывности бизнеса. — *Ред.*)».

Digital-процессы: прогресс, «настоящий» на рисках

Борис Богоутдинов сказал о необходимости банковской цифровизации словами писателя Викентия Вересаева: «Не было бы риска — не было бы и прогресса». Действительно, цифровизация как тренд современного мира, с одной стороны, облегчает и ускоряет процессы взаимодействия, получения, обработки и анализа информации, а также заключения сделок и совершения операций. Но, с другой стороны, возникают новые угрозы, связанные с цифровыми технологиями. Вера Замигулова среди основных причин их появления назвала:

- недостатки или устаревание используемого программного обеспечения;
- ошибочные либо несоответствующие реалиям алгоритмы в обработке данных;
- увеличение объемов и способов осуществления мошеннических платежей, случаев кражи;
- имитацию поведения и данных человека для получения доступа к его банковской информации.

В связи с уходом иностранных поставщиков с российского рынка в части управления операционным риском на первый план вышли вопросы надежности и безотказности работы информационных систем, информационной безопасности, конфиденциальности и защиты данных клиентов, а также обучения персонала,

введения дополнительных контрольных процедур, перечислила эксперт из Реалист Банка.

Актуальные риски периода структурной трансформации

«В период масштабной перестройки экономических взаимосвязей, пожалуй, наибольшую угрозу операционных потерь представляют внешние события. Главным образом это риск мошенничества и правовой риск — рост судебных процессов вследствие неисполнения своих обязательств контрагентами», — считает Светлана Васильченко, начальник отдела контроля операционных рисков службы управления рисками АКБ «Держава».

Вера Замигулова не сбрасывает со счетов и проблемы, вызванные нарушением цепочек проведения платежей в иностранных валютах. «Ну и, конечно, текущие задачи и изменения никто не отменял. Как пример: переход на новый формат взаимодействия с БКИ, введение макропруденциальных лимитов (МПЛ). Все это требует от банковского сообщества практически мгновенной реакции и адаптации, изменения процессов, правил, процедур, внутренних документов и конечно, автоматизации и цифровизации», — перечислила она.

Основные вызовы на среднесрочную перспективу связаны с обеспечением непрерывности деятельности и операционной надежности банка, в том числе с построением процессов контроля и мониторинга технологических процессов, уверена Светлана Белялова. По-прежнему актуален для Росбанка вопрос, связанный с внедрением новых технологий и клиентских сервисов. Также

для кредитной организации характерен фокус на развитие сервисов с использованием цифрового рубля и иных цифровых активов, дополнила список Светлана Белялова.

В банке «ЗЕНИТ» одним из рисков на ближайшие годы считают аутсорсинг, при этом подчеркивают, что в их кредитной организации с этим нет проблем. Выход проекта требований регулятора по управлению рисками аутсорсинга позволил провести GAP-анализ действующей системы и составить план действий по приведению процессов банка в соответствие требованиям, рассказали «Б.О» в «ЗЕНИТе».

Аутсорсинг: проверки от входа до выхода

Светлана Белялова видит, что «высока актуальность вопросов, связанных с управлением рисками аутсорсинга в связи с необходимостью организации процедур оценки рисков и их митигации в масштабах кредитной организации».

Передача банками поставщикам специализированных услуг части бизнес-функций приводит к сокращению затрат на реализацию проектов, но также и к появлению новых рисков в деятельности заказчика, пояснила Вера Замигулова. Стандартное решение: разработка внутренней методологии и документов, определяющих политику организации по привлечению поставщиков

услуг. Неотъемлемый инструмент управления рисками при аутсорсинге — проведение анализа деятельности потенциальных контрагентов банка. Их проверяют на предмет репутационных, правовых, комплаенс-рисков и ошибок внутреннего контроля, а также рисков информационной безопасности и информационных систем, конкретизировал Борис Богоутдинов. Также банки, по словам спикера, «пользуются стратегиями выхода, включающими действия по прекращению сотрудничества с поставщиком или альтернативной его замене».

Вера Замигулова отметила необходимость оценки экономической эффективности аутсорсинга, дальнейшего мониторинга качества получаемых услуг. «Важно сохранять баланс между оптимизацией денежных и временных затрат, преимуществами привлечения внешних специалистов с требуемыми компетенциями, которых в текущий момент в банке нет и/или которых сложно найти и теми рисками, которые несет аутсорсинг: утрата контроля над процессом, появление зависимости от поставщика, ошибки и недостатки в системах и процессах поставщика услуг, нарушение сохранности конфиденциальной информации и прочее», — пояснила она.

В Реалист Банке функционирует технологический комитет, который дает возможность, привлекая к обсуждению специалистов различных подразделений, например бизнес-подразделения, IT-департамента, службы управления рисками, взвешивать все плюсы и минусы и принимать обоснованное решение по данному вопросу, поделилась «рецептом» Вера Замигулова.

В Росбанке, как сообщила Светлана Белялова, при управлении рисками аутсорсинга используют лучшие международные практики, основанные на оценке рисков третьих лиц при передаче критически важных процессов банка, и внедряют новые требования Банка России к управлению рисками аутсорсинга. **Б.О.**