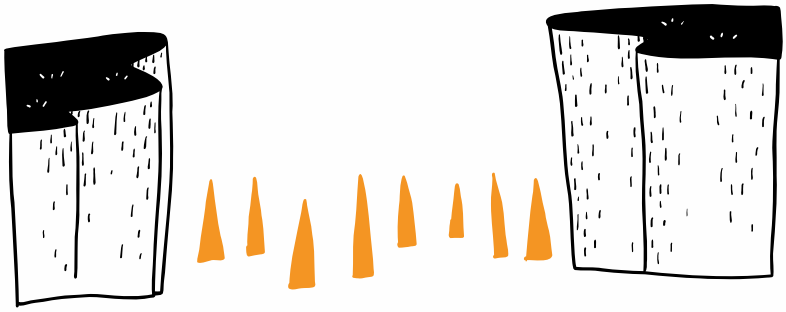
В целом согласен, но... есть риски

Операционные риски проникают буквально во все бизнес-процессы банков, а управление ими превращается не только в выполнение нормативных актов регуляторов, но и в способ предвидеть будущее в крайне изменчивой ситуации



Текст
ВАДИМ ФЕРЕНЕЦ,
ОБОЗРЕВАТЕЛЬ **«Б.О»**





Группа компаний «Б1», бывшая российская практика международного аналитического агентства EY, и Ассоциация риск-менеджмента «Русское общество управления рисками» («РусРиск») представили результаты своих исследований, касающихся сферы управления операционными рисками (ОР).

Презентация итогов этой работы состоялась 22 мая 2025 года в Москве на втором форуме по управлению ОР в кредитно-финансовой сфере. Особый интерес представляла реакция на основные выводы со стороны представителей крупнейших отечественных финансовых организаций.

Международная практика vs отечественная

ГК «Б1» проводила свое исследование в виде опроса руководителей направлений риск-менеджмента (CRO) на тему того, что именно происходит в этой сфере менеджмента, а также выявления трендов, которые движут этим рынком.

Михаил Цибулевский, партнер, руководитель группы консультационных услуг для организаций финансового сектора, отметил: «Ранее компания ежегодно проводила Risk Officer Survey среди топ-100 мировых банков. В нынешнем году эта практика была продолжена, были опрошены CRO из 25 крупных российских банков, которые консолидировали около 80% активов всего банковского сектора страны. Цель опроса — понять актуальную повестку CRO, а также определить вызовы и возможности риск-менеджмента на ближайшее время».

Ключевым вопросом аналитиков к банкирам стал такой: «Какова значимость рисков для вашей организации?» Выяснилось, что в список из топ-5 позиций помимо традиционных кредитного, процентного и риска ликвидности вошли новые два подвида ОР: риски кибербезопасности (РИБ) и риски информационных систем (РИС).

Более 60% респондентов обозначили РИБ как «значимый», а более 40% дали аналогичную оценку РИС. Причины в целом

понятны. Во-первых, цифровизация в банках достигла крайне высокого уровня. Во-вторых, успешно и неумолимо идущий процесс импортозамещения ПО. В-третьих, проблемы в работе с международными вендорами в рамках доработок и обслуживания их решений.

В результате РИБ вышел далеко за рамки технологической повестки и стал серьезно влиять на уровни как операционной устойчивости, так и финансовой стабильности. Мало того, грамотное управление РИБ стало преимуществом банка в конкурентной борьбе.

Например, Банк России дал среднюю по рынку эффективность антифрода в 2024 году в 99,7%. При этом сами коммерческие банки посчитали эту оценку недостаточной для себя, поскольку в рамках мошеннических схем злоумышленники стали активно использовать ИИ, например, для преодоления языкового барьера.

При этом обозначился парадокс: хотя кредитный риск выявлен как наиболее значимый для банков, они тратят заметно существенные бюджеты на управление РИС и РИБ, хотя ПВР-повестка (ПВР — подход на основе внутренних рейтингов) до сих пор остается весьма важным элементом риск-менеджмента. По итогам 2024 года ГК «Б1» оценила затраты на ИБ-софт в целом по стране в 300 млрд рублей, что вывело Россию на девятое место в мире по этому показателю.

Еще один зафиксированный парадокс от ГК «Б1» заключается в том, что ни один банк не выделил как «значимый» поведенческий риск. Вероятно, это связано с тем, что в данный момент Банк России выставил довольно скромные штрафы за нарушения предельных показателей, хотя дискуссии внутри регулятора говорят о возможном повышении сумм рестрикций и даже привязке их к уровню капитала банка на уровне 0,1%.

Риск аутсорсинга указали на уровне значимого всего лишь 12% банков, несмотря на новое Положение ЦБ № 716-П. Модельный риск и риск ИИ обозначили 30% и 12% банков соответственно. Разделение этих сфер аналитиками вызвано международной практикой, хотя отечественные организации считают их в совокупности. Западные банки выделяют ИИ отдельно, поскольку эта технология существенно влияет на этические и поведенческие вопросы, а также на безопасность и конфиденциальность данных.

В качестве одной из основных повесток отечественных CRO, по мнению Михаила Цибулевского, становится дальнейшее выстраивание взаимодействия и углубление коллабораций с центрами компетенций в областях ИБ, IT, разработки и валидации моделей ИИ, а также с подразделениями закупок.

Операционные vs нефинансовые риски

Исследование «РусРиск», представленное **Ириной Андроповой,** членом правления этой ассоциации, было посвящено практикам управления операционными и нефинансовыми рисками.

Международная практика показала, что общая подверженность ОР снизилась, несмотря на рост инцидентов, а совокупные потери удается сдерживать за счет лучших практик. Сказалось и ужесточение санкций за недобросовестное поведение и повышение наказания за манипуляции на рынке, мисселинг, отмывание денег и т.д. При этом изменилась структура потерь: на первый план по объему вышли риски операционных сбоев и ошибок транзакций. «Средний чек» уменьшается, а вот частота подобных событий выросла. В их число прочно вошло внешнее мошенничество, особенно карточный и онлайн фрод.

В России же статистика только собирается, но первые данные говорят о схожих тенденциях: уровень операционных потерь отечественных банков заметно снижается начиная с 2022-2023 годов. Структура прямых потерь схожа с международной, за исключением повышенного уровня сбоев систем и оборудования. Что касается РИБ, то подтверждаются тренды, озвученные ранее ГК «Б1». В «РусРиск» полагают, что скоро дадут о себе знать мошенничество и злоупотребления, а также риски бизнес-процессов и системные сбои. Поэтому особую важность приобретает тестирование систем на предмет устойчивости к новым угрозам.

Мнение CRO

Исследователи имели возможность получить обратную связь от представителей Т-Банка, МКБ, Альфа-Банка, МТС Банка, ГПБ, а также Московской биржи.

Общее мнение можно сформулировать примерно так: «В целом согласен, но…». В частности, **Станислав Шигаев,** руководитель управления интегрированного риск-менеджмента Т-Банка, в качестве «но» указал на то, что такие уникальные случаи, как присоединение Росбанка к Т-Банку, которые оцениваются аналитиками в доли процента, на самом деле позволяют выявить такие ОР, которые в принципе не могли бы быть вычислены иным способом. Основная причина этого — различия в корпоративной в риск-культуре, поскольку они уникальны для каждого банка.

Сергей Демидов, заместитель председателя правления по ИБ Московской биржи, отметил: «В традиционных попытках разделить риски по видам мы за деревьями не можем увидеть леса. А лес заключается в том, что в 2025 году, по нашему мнению, наступает некая критическая точка, после которой будет необходимо вообще переосмыслить роль риск-менеджмента в крайне динамичном мире. Поэтому придется вспомнить, с чего он начинался, и вернуться к истокам: “Учиться предвидеть события и их последствия”».

Что касается рисков ИИ, то мнение всех участников было единым и совпало с видением **Эльвиры Набиуллиной,** главы Банка России, озвученным ей на недавнем «Альфа-Саммите»: «Регулятор использует возможности ИИ, но технология не может принимать решения вместо экспертов, в частности, по ключевой ставке».

Действительно, ИИ способен изменить многое, как и квантовые вычисления, и многие другие новинки, но при этом все они — не более чем технологии, опирающиеся на «исторические данные». А вот увидеть и оценить ситуацию в динамике может только человек.

В связи с этим в Московской бирже в дополнение к выводам аналитиков полагают: «Роль риск-менеджмента должна эволюционировать в масштабах, сопоставимых с подвижками в технологиях! Мы должны научиться “сильно далеко” предвидеть в “сильно неопределенном” мире!». Б.О