

УДК 336.77

О некоторых особенностях смешанного подхода оценки операционного риска в финансовых организациях

Иванников Вячеслав Юрьевич

Академия управления МВД России,

Россия, 125993, г. Москва, ул. Зои и Александра Космодемьянских, д. 8;

Магистрант, второй факультет, slavaivannikov@yandex.ru

Аннотация. В статье рассмотрены понятия риска в финансовых организациях, а также некоторые методики оценки операционного риска. Предложен авторский подход к заданию лингвистических переменных для построения модели самооценки (Self Assessment) при выявлении, анализе и оценке операционных рисков.

Ключевые слова. Банковское дело, операционные риски, методы оценки операционного риска, выявление и анализ причин операционных рисков, самооценка деятельности, планы обеспечения непрерывности деятельности.

On some features of a mixed approach to assessing operational risk in financial institutions

Ivannikov Vyacheslav Yurievich

Management Academy of the Ministry of the Interior of Russia,

Russia, 125993, Moskva, ul. Zoi i Aleksandra Kosmodem'yanskikh, d. 8;

Master student, 2nd faculty, slavaivannikov@yandex.ru

Annotation. The article discusses the concepts of risk in financial institutions, as well as some methods for assessing operational risk. An author's approach to setting linguistic variables to build a Self Assessment model for identifying, analyzing and evaluating operational risks is proposed.

Keywords: Banking, operational risks, methods for assessing operational risks, identifying and analyzing the causes of operational risks, self-assessment of activities, plans for business continuity.

Практически любая деятельность, в области финансов, подразумевает риск того или иного рода. При этом риск означает вероятность наступления того или иного события, которое может неблагоприятно сказаться на прибыли, капитале или репутации; привести к финансовым потерям и оттоку клиентов. Среди множества классифицированных видов рисков особо выделяется операционный риск – относительно новый и еще недостаточно изученный вид риска. К таким рискам относятся преступная деятельность, воровство или мошенничество со стороны сотрудников, клиентов или внешних мошенников, к примеру, кибератаки. Существует возможность вовлечения банка в юридическую тяжбу, приведшую к дорогостоящему судебному процессу. Социальные беспорядки, отказ компьютерной системы, открытое преступное посягательство на банк - все эти факторы входят в данную категорию. Если происходит сбой в компьютерной системе в разгар рабочего дня, организация подвергается серьезному риску в случае отсутствия дублирующей системы. Особенностью операционного риска является сложность его идентификации и оценки, разработка действенной модели прогнозирования и минимизации.

Общий недостаток всех методов оценки операционного риска, основывается только на информации о понесенных организацией потерях, и заключаются в их неспособности оценивать риск тех потерь, которые еще не происходили. Учет такого рода событий исключительно важен при оценке риска, поскольку они обычно лежат в области неожиданных потерь, имеют большую величину и могут привести к приостановке деятельности финансовой организации. Выявлению таких событий служит метод сценарного анализа, который позволяет путем проигрывания сценариев “что будет, если ...”, в связке с данными о случаях реализации крупных потерь или катастрофических событий в отрасли, оценить, каким потерям может подвергаться финансовая организация [1]. На все выявленные случаи катастрофических событий должны быть разработаны планы обеспечения

непрерывности деятельности, позволяющие клиентам получить необходимое обслуживание уже в период реализации событий, для чего финансовая структура должна быть способна:

- управлять персоналом, бизнесом, филиалами, активами и учетом;
- информировать сотрудников о новых или запасном офисе, резервных номерах телефонов, контактных лицах. необходимых изменениях в организационной структуре, перераспределение обязанностей и полномочий;
- информировать клиентов и если необходимо, изменить способы обслуживания;
- восстановить важнейшую бумажную документацию;
- восстановить электронные базы данных, включая систему бухгалтерского учета, реестры, информацию о клиентах и поставщиках, персонале.

Сценарный анализ может проводиться в виде направляемых дискуссий, мозговых штурмов или в форме опроса, участниками которого являются менеджеры финансовой организации. Для получения аналитических выводов рекомендуется применять следующие методы:

- изучение частоты происшествий (катастроф, аварий) и анализ скорости их распространения;
- оценка продолжительности событий;
- анализ последствий происшествия, исходя из сценариев, что важнейшие записи уничтожены;
- оценка последствий, включающая пострадавших сотрудников, потерю операционной способности, потерю активов, повреждение офисов.

Однако сценарий анализа, или точнее говоря его сценарное моделирование может использоваться и для расчетов капитала под операционный риск для тех категорий событий, которые лежат в области неожиданных потерь, характеризуется малой частотностью и не являются

катастрофическими. Финансовая организация может иметь по ним небольшое количество данных по потерям, не позволяющее напрямую восстановить функцию плотности распределения частоты и величины потерь, но дающее менеджменту возможность сформировать экспертные знания о событиях такого типа [2]. Именно такого рода сценарный анализ используется для численного моделирования в смешанном (гибридном) подходе моделирования кривой распределения потерь от операционного риска.

Первым шагом в реализации сценарного моделирования является выделение множества тех событий, по которым недостаточно данных, и объединение их в сценарии в соответствии с классификацией категорий операционных рисков финансовой организации. Под сценарием понимается случай реализации операционного риска и вся цепочка последствий его реализации, которая отслеживается по всем единицам портфеля операционного риска (примем в данном случае для простоты за такую единицу структурные подразделения организации). Когда сценарий прописаны, менеджеры должны на основе имеющегося небольшого объема данных и/или экспертных знаний оценить частоту возникновения событий, а также величину возможных потерь в затрагиваемых этим сценарием структурных подразделениях. При этом необходимо указывать как типичную частоту возникновения случаев и величины потерь, так и верхнюю и, желательно, нижнюю границу. Любая недооценка или переоценка частоты, или величины потерь должна быть скорректирована. Используя принцип «второго глаза»: внутренний аудит процесса оценки сценариев, сравнение с данными проверок службы внутреннего контроля организации, сравнение экспертных оценок и данных по потерям (внутренних и внешних) и пр. В результате получают распределение потерь трех типов: построенные экспертным способом; построенные частично экспертным способом и частично на основе данных; построенные на основе данных по потерям. На основе таких построенных гибридным способом (экспертные знания плюс данные по потерям)

распределений частоты и величины потерь методом симуляции Монте-Карло далее могут быть построены функции распределения потерь от операционного риска в разрезе сценарных классов и подразделений финансовой организации.

Нельзя отрицать, что оценка операционного риска путем построения функций распределения потерь по категориям риска/единицам портфеля (бизнес-процессам, подразделениям, бизнес-линиям) финансовой организации и последующим расчетом потерь на основе меры Value at Risk (VaR) является наиболее адекватной для управленческих целей. Однако проблема заключается в том, что российскими финансовыми организациями пока не накоплены данные для построения таких моделей. Это основная причина, которая не позволяет в рамках продвинутых подходов унифицировать расчет основных видов рисков.

Эффективный способ приблизить момент возможности точной количественной оценки операционных рисков – создание или внедрение систем, позволяющих систематически отслеживать и регистрировать в базе данных частотность, величину потерь и другую релевантную информацию по отдельным событиям. К сожалению, финансовые организации не обмениваются между собой информацией по операционным потерям, а в открытых источниках они могут почерпнуть искаженную, неполную и в силу этого нерелевантную информацию, которую вряд ли можно использовать для дополнения внутренних данных по потерям внешними с целью построения функции распределения потерь от операционного риска или даже сценарного анализа.

В западной практике использование внешних данных для оценки операционных рисков конкретным финансовым институтом уже достаточно широко распространено, т.к. имеются сервисы с базами отраслевых данных по потерям в результате реализации операционных рисков, и разработаны подходы к «смешиванию» внутренних и внешних данных и шкалированию данных.

В части прочих методов выявления, анализа и оценки операционных рисков наиболее интересна методика самооценки.

Методика самооценки, известная в западной практике как "self-assessment", представляет собой экспертный балльно-весовой метод, позволяющий оценить уровень контроля операционных рисков. Использует этот метод более 70% крупных западных финансовых корпораций. Оценка осуществляется путем выставления баллов по каждому из факторов, которые в той или иной мере влияют на контрольную среду, что учитывается посредством весов данных факторов. Факторы объединяются в группы, каждая из которых также может иметь свой вес, а суммарный получаемый балл отражает уровень контроля операционных рисков. Подверженность остаточному риску тем выше, чем ниже балл. Чтобы применять данный метод на практике в первую очередь необходимо выделить те зоны операционной среды, которые будут оцениваться, и которые будут образовывать группы факторов. Эти зоны должны быть непересекающимися. К ним можно отнести, например, «Качество управления», «Степень/качество наблюдения», «Характеристика продуктов», «Особенности систем», «Объемы транзакций», «Бизнес-процессы» (регламентирование, рутинность, уровень автоматизации) и др. Далее для каждой зоны нужно определить тот круг вопросов, которые влияют на контрольную среду в каждой зоне, и, в конечном итоге, позволят оценить качество контрольной среды финансовой организации [2].

Приведем пример описания ситуации в лингвистическую переменную для построения модели самооценки в Таблице 1.

Таблица 1. Задание лингвистических переменных для построения модели самооценки (составлена автором).

Оценка показателя «Регламентация»	Очень незначительная регламентация или отсутствие регламентов	Не все ключевые области покрыты	Регламентирована большая часть основных областей	Регламенты покрывают все основные области	Полное регламентирование
Оценка уровня контроля	минимальный	Низкий	средний	очень высокий	высокий
Подверженность операционному риску	очень высокая	Высокая	средняя	низкая	минимальная

Но прежде чем подойти к шкалированию, необходимо путем открытых опросов экспертов выявить зоны операционной среды, затем отранжировать их в ходе закрытого опроса и определить веса наиболее значимых зон, которые будут использованы в карте самооценки. Следующим шагом должно быть выявление круга вопросов (факторов контрольной среды), которые будут оцениваться, опять же в форме опроса экспертов, их ранжирование и определение веса каждого вопроса (фактора). Правильно сформулировать и структурировать опросы помогает рассмотрение истории операционных потерь в финансовой организации на основе информации базы данных, что позволяет заранее понять некоторые слабые стороны контроля в различных структурных подразделениях; анализ результатов мониторинга ключевых показателей операционных рисков в динамике; изучение отчетов службы внутреннего контроля (аудита); анализ внешних данных [3].

Когда модель и опросники на ее основе готовы, они предъявляются менеджерам в закрытом виде, однако, сама процедура выставления баллов может проходить неформально. Приветствуется проведение специализированных семинаров, где в ходе управляемой дискуссии

обсуждаются наиболее актуальные области возникновения операционного риска, выявляются слабости контроля и управления. Больших интеллектуальных усилий и ресурсов требует проведение сценарного анализа, чтобы понять, какой уровень контроля имеет место в отношении той или иной категории рисков или в каком-то подразделении, бизнес-процессе. Результатом всех процедур являются выставленные баллы, по которым можно рассчитать баллы по зонам контроля, отдельным факторам (или другим единицам портфеля рисков).

Нельзя, конечно, отрицать и ценности проведения самооценки в неформализованном виде, когда модели нет, и объективная балльная оценка невозможна, поскольку направляемые дискуссии, круглые столы, проведение сценарного анализа, проведение опросов в открытой форме и т.п. способствуют повышению рискованной культуры и выработке стратегии управления операционными рисками.

Список литературы

1. Стрелков С.В. Анализ и качественная оценка операционных рисков КО: риски информационных систем. Режим доступа: <http://www.e-rej.ru/Articles/2009/Strelkov.pdf>
2. Баско О.В. Управление рисками в банке: учебно-методическое пособие.- Азов: ООО «Азов-Печать», 2015. – 212 с.
3. Баско О.В. Кредитование как банковский бизнес-процесс: учебно-методическое пособие. – Азов: ООО «Азов-Печать», 2015. 132 с.

References

1. Strelkov, S.V. (2009). Analiz i kachestvennaya otsenka operatsionnykh riskov KO: riski informatsionnykh sistem. [Analysis and qualitative assessment of operational risks of corporate equity: risks of information systems]. Available at: <http://www.e-rej.ru/Articles/2009/Strelkov.pdf>

2. Basko, O.V. (2015). *Upravleniye riskami v banke: uchebno-metodicheskoye posobiye* [Risk management in the bank: a training manual]. Azov: OOO «Azov-Pechat'».
3. Basko, O.V (2015). *Kreditovaniye kak bankovskiy biznes-protsess: uchebno-metodicheskoye posobiye* [Lending as a banking business process: a teaching tool]. Azov: OOO «Azov-Pechat'».