Ирина Балина,
Славянский университет РМ

МЕТОДОЛОГИЯ АНАЛИЗА БАНКОВСКИХ РИСКОВ

In work definition of bank risk is made, classification is considered. Examples of carrying out of calculations of operational risk by 2 methods - estimations on the basis of expected cases of losses and an estimation of a deviation of standard results are presented.

Риск является неотъемлемой характеристикой банковской деятельности. Он играет определяющую роль в формировании финансовых результатов деятельности банков, служит важной характеристикой качества активов и пассивов банков и, таким образом, должен использоваться при сравнительном анализе их финансового состояния, положения на рынке банковских услуг.

Основная цель проводимого исследования заключается в подробном анализе методики и современных тенденций в области управления банковскими операционными рисками.

Поставленная цель работы предопределила ряд взаимосвязанных задач:

1. Провести анализ существующих определений и систем классификации риска, определить сущность управления операционными рисками;
2. Рассмотреть и проанализировать современные тенденции управления операционными рисками в банковской деятельности на контрольном примере.

Наиболее полным является следующее определение понятия «банковский риск»: банковский риск – неопределенность в отношении будущих денежных потоков, вероятность потерь или недополучения доходов по сравнению с планируемыми, или вероятность возникновения непредвиденных расходов при осуществлении определенных банковских операций, представленная в стоимостном выражении.

В теории существует большое число различных классификаций банковских рисков, построенных на выделении тех или иных системообразующих факторов. Обычно риски подразделяются на три категории: **1) финансовый** (виды: кредитный, ликвидности, рыночный, процентный, валютный, инфляции, неплатежеспособности); **2) функциональный** (виды: стратегический, технологический, операционный, внедрения новых продуктов и технологий – внедренческий) и **3) прочие** (внешние по отношению к банку) риски.

Проведенные исследования базируются на основе анализа операционных и накладных расходов – операционного риска. Используется 2 метода анализа:

1. Метод оценки на основе ожидаемых случаев потерь, при-

веденных к году – составляется таблица (Таблица 1), в которой оцениваются операционные потери банка за период, например неделю, в размере 100 леев. За 5 лет, предположительная потеря банка может составить 50 тыс. леев, а за период в 10 лет может произойти случай, когда банк потеряет 90 тыс. леев. Затем все это приводится к 1 году, т.е. можно определить величину потерь за год.

Таблица 1

Таблица ожидаемых потерь от операционных рисков

Потери	Период							
	Больше 10 лет	**10 лет**	**5 лет**	**1 год**	**квартал**	**месяц**	**неделя**	**день**
Крупные		90 000,00 леев						
Средние			50 000,00 леев				100,00 леев	
Мелкие								

Проводим следующие расчеты: 100 × 48 недель = 4800 леев. 50 тыс. / 5 лет = 10 000 леев. 90 тыс./10 лет = 9 000 леев. Всего получается 23 800 леев за один год. Проблема для полученного значения в том, что невозможно указать величину доверия. Какова величина вероятности – 60%, 80%, 90% или 99%? Значение является лишь прогнозным, т.е. нельзя точно определить, какие потери по операционным рискам понесет банк через определенный период. Для того, чтобы определить отклонение прогнозного значения от фактического применяют второй количественный метод.

2. Метод оценки отклонения стандартных результатов – этот метод требует знаний стандартных затрат и, следовательно, наличия детального планирования в банке. Подразумевается, что результаты операционных ошибок отражаются в отклонении от запланированных стандартных значений. Как известно, распределения операционных рисков носят асимметрический характер, но за счет используемого подхода в виде разницы плановых и фактических значений мы получаем распределение, близкое к нормальному распределению, и можем использовать аналитический расчет значения риска.

Результат риска = стандартные расходы – фактические расходы (1)

Например, по данным расчетов, на сбои в компьютерном оборудовании планировалось затратить 1500 леев, фактические расходы составили 1450 леев, т.е. фактический результат риска – 50 леев, а отклонение факта от плана составило 3,33%. Такие выводы можно сделать по всем категориям операционных рисков. Данные сопоставляются по нескольким периодам и предопределяют точность планирования расходов на

операционные риски. Анализ расходов позволяет выявить источники операционных рисков, а также дать количественную или статистическую оценку. В результате получается база данных расходов по рискам, с помощью которой проводится анализ величины расходов по месяцам, годам и принимаются решения по снижению рисков. По данным таблицам составляются консолидированные сводные таблицы, в которые заносится информация по разным годам. Затем по сводным таблицам составляются диаграммы. Диаграммы позволяют сопоставить отдельные виды рисков по месяцам, а также более детально их проанализировать.

Таким образом, грамотное управление операционными рисками способствует минимизации информационных и финансовых потерь, связанных с отражением банковских операций на счетах бухгалтерского учета, а также адекватности отражения учетной информации в различных формах отчетности с эксплуатацией программного обеспечения, использованием в деятельности банка технических средств и высокотехнологического оборудования при реализации банковских услуг.

Независимые исследования, проведенные на территории СНГ и стран Балтии, показали, что, если результатом преднамеренных или случайных действий системного администратора, вирусной атаки или аппаратного сбоя явилось уничтожение базы данных информационной системы банка, то:

- лишь 15% банков смогли бы восстановить операционную деятельность день в день;
- 60% банков понадобилось бы для этого от двух до четырех дней;
- 25% банков восстанавливали бы свою деятельность пять и более рабочих дней.

Что характерно, в числе лидеров по скорости восстановления операционной деятельности находятся дочерние зарубежные банки или банки, подконтрольные западным финансовым группам.

Следует отметить, что рассмотренные методы требуют дальнейшего совершенствования, так как не могут дать полного представления о рисках, их характере и причинах возникновения, а дают лишь количественную оценку потерь. Качественные методы анализа, к сожалению, не используются широко в банках. Это связано с недостаточным объемом статистических данных – банки имеют небольшую современную историю. К тому же, в начале своей деятельности никто не вел сбора информации по операционным рискам, отсутствуют полные данные за длительный период и добровольно представленные данные по ошибкам других банков. Например: о взломах информационных систем, воровстве клиентских денег нечистоплотности сотрудников банка и т.д.

Это предопределяет в качестве основной тенденции современного банковского риск-менеджмента концентрацию на задачах правильного создания ведения баз данных по имеющимся рискам, качественных оценках и внедрению культуры риска в банке.

Литература:

1. Грюнинг Х. ван, Брайович Братанович С. *Анализ банковских рисков. Система оценки корпоративного управления и управления финансовым риском*. – М.: Весь Мир, 2007. – 304 с.
2. Смирнов А. *Операционные риски и ИТ-инфраструктура банка* // Корпоративные системы. – Киев, 2008, № 1.
3. www.inmar.ru

Светлана Голубева,
Технический Университет Молдовы

ИССЛЕДОВАНИЕ СОВРЕМЕННЫХ МЕТОДОВ ЗАЩИТЫ ОТ DDOS

DDOS is a great problem for commercial and governmental INTERNET resources in our days. There doesn't exist any universal algorisms for defending against DDOS for one server. This article describes the possibilities for common and distributed defense against DDOS attacks.

Ключевые слова: *DDoS-атака, защита, CAPTCHA, «Оверле́йная сеть», рассредоточение.*

1. Введение

Год за годом, мы становимся все более зависимыми от интернет сервисов, таких как: различные финансовые инструменты, IP-телефония, получение новостей, электронное правительство и т.д. Все эти сервисы представляют интерес для злоумышленников и нуждаются надежной защите. Наиболее часто Интернет-сервисы подвергаются, так называемым, DoS-атакам или DDoS-атакам[1].

DoS-атака (от англ. Denial of Service) и DDoS-атака (от англ. Distributed Denial of Service) – это разновидности атак злоумышленника на компьютерные системы. Цель этих атак – довести систему до отказа, то есть, создание таких условий, при которых легитимные (правомерные) пользователи системы не могут получить доступ к предоставляемым системой ресурсам, либо этот доступ затруднён. Если атака производится одновременно с большого количества IP-адресов, то в этом случае она называется распределённой атакой на отказ в обслуживании (DDoS) [2].

Различные компании и производители предлагают и разрабатывают свои решения защиты. Проводятся тщательные исследования трафика. Составляется схема уже произошедших атак. Проводится анализ статистических данных как: частота атак определенного ресурса, количество вовлеченных в атаку компьютеров, а также качество методов, предотвративших атаку [5].