МИНИСТЕРСТВО ВЫСШЕГО И СРЕДНЕГО СПЕЦИАЛЬНОГО ОБРАЗОВАНИЯ РЕСПУБЛИКИ УЗБЕКИСТАН

ТАШКЕНТСКИЙ ФИНАНСОВЫЙ ИНСТИТУТ

КРЕДИТНО-ЭКОНОМИЧЕСКИЙ ФАКУЛЬТЕТ

“УТВЕРЖДАЮ”
в.и.о. декана кредитно-экономического
факультета проф. Каралиев Т.М._____
“____” _____2015г.

КАФЕДРА “БАНКОВСКОЕ ДЕЛО”

САБИТОВА ГУЛНОЗА МАЪРУФДЖАНОВА

ОПЕРАЦИОННЫЕ РИСКИ В СИСТЕМЕ РИСК МЕНЕДЖМЕНТ И СОВЕРШЕНТВОВАНИЕ УПРАВЛЕНИЕЯ ИМИ

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА

на соискание степени бакалавра по направлению
5230700 – “Банковское дело”

Научный руководитель:
Арзуманян.С.Ю_____
“___” _____ 2015г.

“Рекомендуется к защите”
Заведующий кафедрой
к.э.н., доц. Саидов Д. _____
“___” __ _____ 2015г.

ТАШКЕНТ – 2015

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Операционный риск - риск возникновения убытков в результате несоответствия характеру и масштабам деятельности Банка и (или) требованиям действующего законодательства внутренних порядков и процедур проведения банковских операций и других сделок, их нарушения служащими Банка и иными лицами (вследствие непреднамеренных или умышленных действий или бездействия), несоразмерности (недостаточности) функциональных возможностей (характеристик) применяемых Банком информационных, технологических и других систем и их отказов (нарушений функционирования), а также в результате воздействия внешних событий.

Динамичный рост банковских услуг за последнее годы достигается, наряду с традиционными, расширением спектра и качества оказываемых услуг с широким применением информационно-коммуникационных технологий.

В настоящее время банки активно развивают удобные для клиентов формы услуг, которые позволяют владельцам банковских счетов осуществлять операции со своих счетов по программной сети «банк-клиент» не приходя в учреждения банков и получать информацию о банковских счетах через мобильные и электронные связи в режиме реального времени. Количество пользователей ими за 2014 год увеличилось более чем в 2 раза и составило 519 тыс. клиентов.

Важнейшим фактором, обеспечивающим устойчивые темпы роста экономики, явилось реформирование банковской системы, в результате чего рост совокупного капитала коммерческих банков составил почти 25 процентов.

Укрепление банковской системы создало необходимые предпосылки для снижения в 2014 году ставки рефинансирования Центрального банка с 12

до 10 процентов и соответствующего уменьшения процентной ставки по кредитам коммерческих банков.

По сравнению с 2013 годом объемы кредитов, выделенных банками только на финансирование программ модернизации и технологического обновления производств, увеличились в 1,2 раза, а на пополнение оборотных средств – более чем в 1,3 раза.

На протяжении последних лет ведущие рейтинговые агентства «Мудис», «Стандарт энд Пурс» и «Фитч рейтингс» оценивают деятельность банковской системы Узбекистана как «стабильная».

В 2011 году высокие рейтинговые оценки имели 13 коммерческих банков, то в настоящее время все 26 банков республики удостоены такой оценки.[1]

Система управления операционными рисками намного сложнее, чем, например рыночными или кредитными рисками, так как операционный риск является внутренним риском для финансовой организации, поэтому крайне сложно создать универсальный перечень причин возникновения данного риска. К тому же операционный риск крайне сложно оценить количественным методом.

Управление операционным риском является наименее изученным аспектом риск-менеджмента. Одновременно с этим, становится очевидным, что им необходимо заниматься профессионально, так как отсутствие действенных моделей возникновения операционных рисков может привести к катастрофическим последствиям для финансового учреждения.

Необходимость работы с операционными рисками произрастает из самой специфики банковской деятельности и всевозможных, имеющихся сегодня потерь, связанных с информационными системами, персоналом, бизнес-процессами и внешними воздействиями. Это и физический ущерб

[1]Каримов И.А, Создание в 2015 году широких возможностей для развития частной собственности и частного предпринимательства путем осуществления коренных структурных преобразований в экономике страны, последовательного продолжения процессов модернизации и диверсификации – наша приоритетная задача, Ташкент.: Узбекистан, 2015, С.-42.

дорогостоящему оборудованию, и вынужденные задержки осуществления операций, и потеря данных, ошибочные расчеты, обязательные платежи за разрешения, лицензии, и другие неприятные события, которые сопровождают работу финансовых учреждений. Таким образом, реалии сегодняшней банковской системы Украины подталкивают банкиров к обмену опытом и скорейшему началу разрешения вопросов, связанных с управлением операционными рисками.

Ключевым этапом риск-менеджмента считается этап выбора методов и инструментов управления риском. Базовыми методами риск-менеджмента являются отказ от риска, снижение, передача и принятие.Риск-инструментарий значительно шире. Он включает политические, организационные, правовые, экономические, социальные инструменты, причём риск-менеджмент как система допускает возможность одновременного применения нескольких методов и инструментов риск-менеджмента.

Целью работы является изучение теоретических и практических проблем организации, осуществления и управления рисками, а также выработка предложений по повышению эффективности их управления.

В соответствие с целью исследования в выпускной квалификационной работе поставлены следующие **задачи**:

– уточнение содержания основополагающих понятий и определений, в том числе «риск», «операционный риск»;

– исследование основных видов рисков и их взаимосвязи;

– изучение практики применения норм, регулирующих управление конкретных предложений по совершенствованию рисков;

– систематизация основных направлений совершенствования управления рисками;

– исследование перспектив уменьшения рисков.

Объектом работы являются коммерческие банки.

Предметом выпускной квалификационной работы являются организация, осуществление и совершенствование практики управления рисками в коммерческих банках.

Информационную базу работы составили законодательные и нормативные акты Республики Узбекистан, нормативные документы Центрального Банка Республики Узбекистан, публикации в отечественной и иностранной периодической печати, а также практические материалы отечественных коммерческих банков по рассматриваемым проблемам.

В выпускной работе:

– показана экономическая основа рисков, в том числе операционного;

– предложена классификация рисков, имеющих место в операциях коммерческих банков, в зависимости от основных факторов, определяющих данные риски;

– разработаны методические подходы, позволяющие улучшить деятельность по управлению операционными рисками;

– сформулированы и систематизированы основные направления совершенствования организации и управления рисками .

Практическая значимость выпускной квалификационной работы. Сформулированные в работе предложения по улучшению управлению рисками в Узбекистане могут быть использованы в работе коммерческих банков для оптимизации организации и осуществления международных операций и адаптации банковской практики к мировым стандартам, а также отечественными экспортерами и импортерами для минимизации рисков, связанных с проведением внешнеэкономической деятельности.

Выпускная квалификационная работа состоит из введения, трех глав, выводов и предложений, списка литературы.

ГЛАВА 1. ТЕОРЕТИЧЕСКИЕ ОСНОВЫ УПРАВЛЕНИЯ БАНКОВСКИМИ РИСКАМИ

1.1 Сущность и содержание банковских рисков

Любой экономический субъект в своей деятельности сталкивается с событиями и факторами, которые он не в состоянии регулировать и точно предсказывать. Более того, это происходит при любой его деятельности и в каждый момент времени. В современных теориях стало принято учитывать влияние таких неопределенностей на функционирование организаций и предлагать различные методы по снижению их неблагоприятного воздействия на результат. Таким образом, было введено понятие риска.

Риск – это неуверенность (возможность больших или меньших отклонений) в том, что управляемый процесс или наблюдаемое событие пройдет по запланированному сценарию и даст ожидаемый результат, причем последствия этих отклонений негативно скажутся на состоянии управляемого объекта. Так родоначальники предпринимательства Р. Кантильон, И. Тюнен и Ф. Найт источником предпринимательского дохода считали реализацию в процессе воспроизводства способности предпринимателя к обоснованному риску. В этом контексте уместно добавить, что в знаменитом словаре В. Даля риск определяется, с одной стороны, как опасность чего-либо, с другой стороны, как действие наудачу, требующее смелости, решительности, предприимчивости в надежде на счастливый исход.

В учебном издании К.Р. Тагирбекова риск определяется как «порождаемая неопределенностью проявлений агрессивных факторов внешних и внутренних сред возможность отклонения реального протекания управляемого процесса от предполагаемого сценария и в итоге от результата (цели)»[2].

[2] Тагирбеков К.Р. Организация деятельности коммерческого банка. – Москва: Весь Мир, 2004. – С 671

Столь сложно структурированное, многокомпонентное выражение сущности категории риска для использования научных работах требует определенной конкретизации и концентрированности. Компоненты базовой трактовки категории риск обладают определенной иерархией по их значимости и функциональности. Риск при этом трактуется, как уже было сказано выше как более или менее сильная неуверенность в том, что наблюдаемый процесс произойдет по плану и приведет к ожидаемым последствиям.

Итак, в современной теории традиционно выделяют два определения риска. Первое базируется на причинах риска и их неопределенности. Второе определение риска основывается на самом воздействии на риск. Отсюда риск – это негативные отклонения от поставленной цели.

И.Т. Балабанов в книге «Риск-менеджмент»[3] пишет, что «как экономическая категория риск представляет собой событие, которое может произойти или не произойти. В случае совершения такого события возможны три экономических результата отрицательный (проигрыш, ущерб, убыток), нулевой, положительный (выигрыш, выгода, прибыль)».

В итоге риск можно охарактеризовать как опасность потенциально возможной, вероятной потери ресурсов или недополучения доходов по сравнению с вариантом, рассчитанным на рациональное использование ресурсов в данном виде деятельности.

Синонимом риску является неуверенность, невозможность предсказать со 100% точностью, произойдет ли событие или нет. Некоторые события, конечно, являются полностью предсказуемыми и, соответственно, не влекут за собой никакого риска.

В банковском деле риск означает вероятность того, что произойдут события, которые неблагоприятно скажутся на конечном результате деятельности банка (прибыли) или капитале, то есть будет существовать возможность нарушения ликвидности и (или) финансовых потерь.

[3] http://www.znay.ru/library/books/0023.shtml

Существует такая базовая фраза: «Принятие рисков - основа банковского дела»[4]. Банки имеют успех тогда, когда принимаемые ими риски разумны, контролируемы и находятся в пределах их финансовых возможностей и компетенции.

Банки стремятся получить наибольшую прибыль. Но это стремление ограничивается возможностью понести убытки. Риск банковской деятельности и означает вероятность того, что фактическая прибыль банка окажется меньше запланированной, ожидаемой. Чем выше ожидаемая прибыль, тем выше риск. Связь между доходностью операций банка и его риском в очень упрощенном варианте может быть выражена прямолинейной зависимостью.

Уровень риска увеличивается, если:

- проблемы возникают внезапно и вопреки ожиданиям;
- поставлены новые задачи, не соответствующие прошлому опыту банка;
- руководство не в состоянии принять необходимые и срочные меры, что может привести к финансовому ущербу (ухудшению возможностей получения необходимой и/или дополнительной прибыли);
- существующий порядок деятельности банка или несовершенство законодательства мешает принятию некоторых оптимальных для конкретной ситуации мер.

Последствия неверных оценок рисков или отсутствия возможности противопоставить действенные меры могут быть самыми неприятными. Приведем несколько соответствующих примеров из практики западных банков.

В 1989 г. Британский Midland Bank потерял 116 млн.ф.ст. в результате ошибочного прогноза в отношении уровня ссудного процента по кредитам.

[4] http://www.poluchi5.ru/000356-1.html

В феврале 1990 г. После неудачной попытки найти финансовую поддержку рухнул крупный американский банк Drexel Burnham Lambert ,который доминировал на рынке так называемых сомнительных облигаций небольших и малоизвестных фирм, капиталовложения в акции которых были связаны с большим риском, но с повышенным дивидендом. Крах рынка в результате финансовых злоупотреблений привел к краху самого банка, а также поставил под угрозу существование целого ряда сберегательных банков, поместивших свои средства в эти акции под гарантии DBL.

В январе 1991 г. Американский Bank of New England предупредил своих клиентов, что после списания невозвратных кредитов в 4 квартале 1990 г его потери составили 450 млн. долл. В последовавшей затем панике его клиенты изъяли со счетов более 1 млрд. Долл., и банк обанкротился. Потребовалось вмешательство федерального правительства и оказание банку помощи в размере 2,3 млрд. долл., чтобы предотвратить цепную реакцию банковских крахов по стране. Банк сохранил свое существование, но полностью утратил независимость.

В прошлом году, 2007, Английский Банк Northern Rock потерпел крушение, потерял огромную часть привличенных средств (депозитной базы), в последующим был спасен потеряв свою независимость Банком Англии из за распростронение шума среди простого народа о том, что банк стоит на грани банкротства по причине владения subprime mortgage based securities, то есть субстандартных (неликвидных) ипотечных ценных бумаг, которые были выкуплены у американских инвестиционных банков. Известно, что ипотечный кризис возник из за чрезмерной выдачи ссуд заемщикам, которые входили во вторую, то ли не в третью группу кредитоспособности в течение 3-4 лет. Следовательно, по нынешний день, огромная волна заёмщиков по ипотечному кредиту не в состоянии погасит свои задолженности.

Во всех случаях риск должен быть определен и измерен. Анализ и оценка риска в значительной мере основаны на систематическом статистическом

методе определения вероятности того, что какое-то событие в будущем произойдет. Обычно эта вероятность выражается в процентах. Соответствующая работа может вестись, если выработаны критерии риска. Позволяющие ранжировать альтернативные события в зависимости от степени риска. Однако исходным пунктом работы является предварительный статистический анализ конкретной ситуации.

1.2 Место операционных рисков в системе банковских рисков

Риски операционной среды банк принимает на себя как регулируемая фирма, являющаяся ключевым звеном платежной системы. Они объединяют в себе те риски, которые стоят на страже интересов банка, но посредством которых над банком осуществляется контроль, а также те, которые генерируются средой деятельности коммерческого банка.

Ниже приведена схема видов операционных рисков.

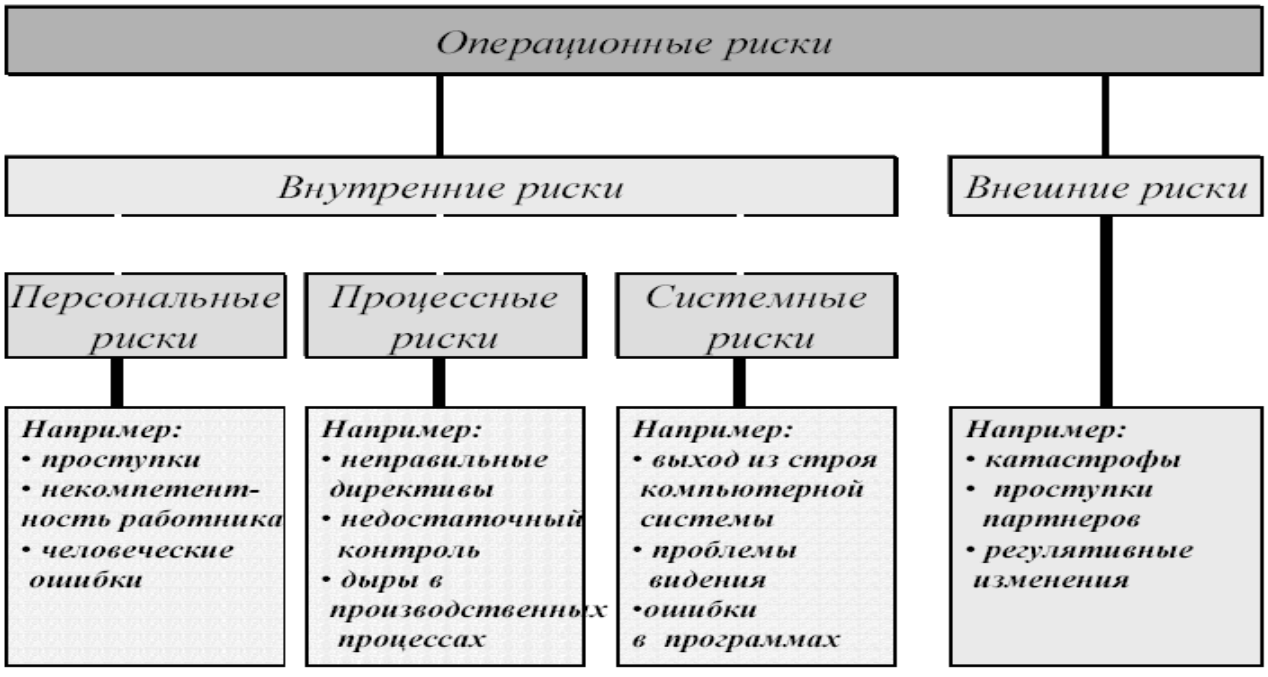

Рис. 1 Виды операционных рисков [5]

В литературе приводится множественность определений операционного риска в банке:

[5] Тагирбеков К.Р. Организация деятельности коммерческого банка. – Москва: Весь Мир, 2004. – С 671

• ОР есть риск враждебного влияния/действия на бизнес как последствие ведения его ненадлежащим и неадекватным способом, и может быть результатом внешних факторов (Credit Suisse Group).
• ОР - любой риск за исключением кредитного и рыночного рисков
• ОР - это риск, ассоциированный с операционным управлением
• ОР это риск проявляющийся в потерях из-за недостатков в информационной системе или внутреннем контроле. Риск ассоциируется с человеческими ошибками, недостатками систем и неадекватными процессами и контролем. (Базельский комитет).
• ОР - это риск прямых или непрямых потерь как результат неадекватности или ошибочности процессов, персонала и систем или внешних событий (Ассоциация риск менеджеров- RMA, Ассоциация британских банков, ISDA).

На примере одной из таких программ рассмотрим алгоритм оценки и управления операционными рисками:

В первую очередь, пользователь программы (сотрудники различных отделов банка, например кредитный инспектор, операционист и т.д.), регистрирует события на ежедневной основе. Например, «Ошибочная операция из-за изменения правил формирования проводки». Далее, событие должно быть заполнено риск-факторами, например «Риск методологии или документооборота». Должна быть указана причина события, например «Не было своевременно сообщено об изменениях». И наконец, причина риска, например «Ошибки в распределении полномочий и ответственности, функций». Рассмотрим алгоритм регистрации события более подробно.

1. Риск-факторы

«Риск-факторы» представляют собой классификацию источников операционного риска, объединенных в риск-группы.

Наименование риск-фактора

Функционирование систем и оборудования

1. Технологический риск сбоев оборудования (банкоматы, компьютерное и телекоммуникационное оборудование, и т.д.)
2. Технологический риск сбоев (отказов) программного обеспечения и информационных технологий.

Внутренние системы

1. Риск методологии (технологии) осуществления того или иного процесса, порядков, регламентов и методов расчета и т.д. (методология осуществления того или иного процесса отсутствует, либо принятая методология устарела и/или не соответствует процедуре выполнения процесса на практике и требует оптимизации).
2. Риск неверной организационной структуры банка, области ответственности и распределения полномочий должностных лиц и подразделений банка (наличие ошибок в системе распределения функций, ответственности, полномочий, приводящих либо к их дублированию, либо к их исключению (потере) функций в реализуемых бизнес-процессах).
3. Отсутствие (несовершенство) системы защиты информации и (или) порядка доступа к информации, неправильная организация информационных потоков внутри Банка.

Внешняя среда

1. Риск несанкционированного проникновения в процессы банка (электронные базы данных, архивы, хранилище, помещения и т.д.)
2. Риск хищения активов (наличные средства, безналичные платежи, ценные бумаги, имущество и т.д.).
3. Риск неблагоприятных действий со стороны клиентов, пользователей, контрагентов (нарушения со стороны уполномоченных лиц клиентов/контрагентов, отказ от выполнения контрактных обязательств и т.д.).
4. Риск предоставления клиентом неверной и/или неполной информации.

5. Риск возникновения потерь и неблагоприятных ситуаций из-за техногенных катастроф и т.д.

Персонал

1. Риск недобросовестного исполнения служебных обязанностей или установленных правил и процедур.
2. Риск недостаточной квалификации работников, осуществляющих данную операцию (вероятность потери средств либо возникновения косвенных убытков вследствие низкой квалификации имеющихся сотрудников, несущих ответственность за выполнение работы на определенном участке бизнес-процесса).
3. Риск недостатка (нехватки) ключевых и/или квалифицированных сотрудников на конкретном участке.
4. Риск перегрузки персонала, выполняющего объем (количество) операций, больше чем это допускается психофизиологическими нормами.
5. Риск мошенничества (риск возникновения убытков (недополучения прибыли) вследствие умышленных действий сотрудников).
6. Риск ошибки

Правовой риск

Внутренние факторы

1. Риск несоответствия внутренних нормативных документов банка действующему законодательству.
2. Неэффективная организация правовой работы, приводящая к правовым ошибкам в деятельности Банка вследствие действий служащих или органов управления кредитной организации;
3. Нарушение банком условий договоров;

Внешние факторы

1. Несовершенство правовой системы (отсутствие достаточного правового регулирования, противоречивость законодательства РФ, его подверженность изменениям, в том числе в части несовершенства

методов государственного регулирования и (или) надзора, некорректное применение законодательства иностранного государства и (или) норм международного права), невозможность решения отдельных вопросов путем переговоров и как результат - обращение кредитной организации в судебные органы для их урегулирования;

2. Нарушение клиентами, контрагентами условий договоров;
3. Нахождение Банка, его филиалов, дочерних и зависимых организаций, клиентов и контрагентов под юрисдикцией различных государств.

Другие источники

Риск-факторы выявляются для каждого банковского продукта, например:

- агентские услуги - депозитарий, аренда сейфовых ячеек, хранение ценных бумаг, прочее
- брокерская деятельность – сделки РЕПО, ценные бумаги, дополнительные услуги, прочее
- коммерческое банковское обслуживание – аккредитивы, гарантии, валютный контроль, конверсионные операции, договор цессии, векселя, факторинг, эквайринг, привлечение депозитов, кассовое обслуживание, расчетное обслуживание, прочее
- обслуживание физических лиц – кредитование физ.лиц, гарантии, банковские карты, вклады, прочее
- операции и сделки на рынке ценных бумаг – привлечение и размещение межбанковских средств, прочее
- управление активами – доверительное управление, ПИФЫ, прочее

2. Операционные потери

При выявлении риск-фактора, оцениваются операционные потери, которые представляют собой классификацию операционных событий по типам.

- Наименование риск-фактора
- Общее
- Сбой оборудования
- Банкоматы

- Нарушены условия эксплуатации. отсутствие системы контроля и диагностики, несвоевременная диагностика; отсутствие предупредительного, планового ремонта
- Износ оборудования
- Качество приобретаемого оборудования
- Ошибки в программном обеспечении (персонал)
- Некорректная установка программ (персонал)
- Физические воздействия (внешние факторы - стихийных бедствий, акты вандализма, кражи)
- Нарушения в кабельных системах
- Технические ошибки

Компьютерное оборудование

- Сбои в работе программного обеспечения,
- Поломка оборудования;
- Износ оборудования;
- Различные аварии сетевого напряжения,
- Сбои в работе аппаратного обеспечения компьютеров и серверов,
- Несоблюдение требований условий эксплуатации (например: отсутствие своевременной очистки систем вентиляции и охлаждения)
- компьютерные вирусы;
- Не обеспечено надлежащее техническое обслуживание компьютеров, не проводятся профилактические (регламентные) работы;
- Неграмотные действия пользователей или персонала по обслуживанию компьютерного оборудования (системы)
- Преднамеренные противоправные действия персонала
- аварийный отказ аппаратуры;
- повреждение внешних носителей памяти (например, в результате поломки головок дисковых накопителей)

Телекоммуникационное оборудование

- Нарушение средств коммуникации;

- Неправильные коммуникации;
- Поломка оборудования
- Коммутационное оборудование

Сбой (отказ) программного обеспечения и информационных технологий

- Аварийное отключение электрического питания
- Внешние факторы
- Неустранимый сбой процессора
- Недостаток оперативной памяти
- Неисправности аппаратного обеспечения
- Неисправности систем связи; каналов связи
- Нехватка системных ресурсов
- Недостаточно грамотная настройка
- Намеренные действия злоумышленников (сотрудников)
- Некорректная работа пользователей

Внутренние системы

Риск методологии (технологии)

- Несоблюдение иили нарушение единства подходов, методов ведения бизнеса, совершения операций
- Дублирование функций
- Исключение (потеря) функций
- Нарушение законодательства
- Неправильная организация информационных потоков

Неверная организационная структура

- Невозможность определить области ответственности и полномочий
- Ошибки в распределении полномочий и ответственности, функций
- Дублирование функций
- Исключение (потеря) функций
- Ошибки в предоставлении доступа к информации
- Неправильная организация информационных потоков

Персонал

- Несоблюдение, нарушение единства подходов, методов
- Недобросовестное исполнение должностных обязанностей
- Потери вследствие низкой квалификации
- Недостаток персонала
- Перегрузка персонала
- Нарушение законодательства
- Неверный ввод информации
- Неправильная деловая или рыночная практика

Преднамеренные противоправные действия персонала

- Несанкционированное вторжение в системы
- Сбой оборудования
- Мошеннические действия, хищение, вымогательство, присвоение активов сотрудниками Банка
- Злоупотребление служебным положением
- Неразрешенные операции
- Искажение отчетности
- Умышленное уничтожение активов сотрудниками Банка
- Подделка документов сотрудниками Банка
- Раскрытие конфиденциальной в т.ч. личной информации, банковской тайны, злоупотребление конфиденциальной информацией
- Превышение лимитов (совершения операций, полномочий)
- Нарушение сроков или обязательств
- Несанкционированное использование информационных систем и ресурсов, неавторизованный (несанкционированный) доступ к счетам
- Преднамеренное сокрытие фактов совершения банковских операций и других сделок
- Нарушение инструкций; законодательства

Внешняя среда

- Выход из строя, сбой (отказ) систем, оборудования
- Нарушение процессов банка

- Повреждение, утрата основных средств и других материальных активов
- Неисполнение или ненадлежащее исполнение банковских функций, законодотельства
- Неисполнение или ненадлежащее исполнение возникающих из договоров обязательств
- Ненадлежащее использование конфиденциальной информации, банковской тайны
- Сговор
- Непредоставление информации, предоставление заведомо ложной, информации; предоставление не полной информации; предоставление неверной информации
- Противоправные действия сторонних по отношению к банку (третьих) лиц
- Подделка платежных и иных документов
- Нарушение клиентами (третьими лицами) законодательства (в том числе банковского, антимонопольного, по противодействию легализации (отмыванию) доходов, полученных преступным путем, и финансирования терроризма
- Потери в результате техногенных катастроф, стихийных бедствий, пожара, актов терроризма

3. Финансовая классификация потерь

Потери могут быть классифицированы следующим образом: расходы, связанные с внешними и внутренними убытками.

Наименование потери

- Возмещение ущерба другой стороне
- Затраты на устранение
- Прочие расходы и убытки
- Списание на убытки
- Судебные издержки, взыскания по решению суда

- Утрата и/или обесценивание обеспечения, залога
- Ущерб материальным активам
- Штрафы

4. Косвенные потери

В отдельную группы могут быть выделены «Косвенные потери», которые представляют собой балльную классификацию косвенных убытков.

Примечание

- Потери оказывают критическое влияние на деятельность Банка. Существенный ущерб деловой репутации Банка, крупномасштабная потеря клиентов. Упущенная выгода и снижение доходов будущих периодов. Потери препятствуют достижению стратегических целей Банка.
- Потери оказывают значительное влияние на деятельность Банка. Ущерб деловой репутации банка, потеря части клиентов. Упущенная выгода и снижение доходов. Потери затрудняют достижение стратегических целей Банка.
- Потери оказывают заметное влияние на деятельность Банка. Возможна потеря некоторого числа клиентов. Существенного влияния на репутацию Банка и достижение стратегических целей нет.
- Потери связаны с упущенной выгодой, снижением доходов будущих периодов. Ущерба репутации банка, потери клиентов, влияния на достижение стратегических целей нет.

5. Причины

Далее необходимо классифицировать причины реализации операционного риска.

Наименование риск-фактора

Функционирование систем и оборудования

- Технологический риск сбоев оборудования (банкоматы, компьютерное и телекоммуникационное оборудование, и т.д.)

- Технологический риск сбоев (отказов) программного обеспечения и информационных технологий.

Внутренние системы

- Риск методологии (технологии) осуществления того или иного процесса, порядков, регламентов и методов расчета и т.д. (методология осуществления того или иного процесса отсутствует, либо принятая методология устарела и/или не соответствует процедуре выполнения процесса на практике и требует оптимизации).
- Риск неверной организационной структуры банка, области ответственности и распределения полномочий должностных лиц и подразделений банка (наличие ошибок в системе распределения функций, ответственности, полномочий, приводящих либо к их дублированию, либо к их исключению (потере) функций в реализуемых бизнес-процессах).
- Отсутствие (несовершенство) системы защиты информации и (или) порядка доступа к информации, неправильная организация информационных потоков внутри Банка.

Внешняя среда

- Риск несанкционированного проникновения в процессы банка (электронные базы данных, архивы, хранилище, помещения и т.д.)
- Риск хищения активов (наличные средства, безналичные платежи, ценные бумаги, имущество и т.д.).
- Риск неблагоприятных действий со стороны клиентов, пользователей, контрагентов (нарушения со стороны уполномоченных лиц клиентов/контрагентов, отказ от выполнения контрактных обязательств и т.д.).
- Риск предоставления клиентом неверной и/или неполной информации.
- Риск возникновения потерь и неблагоприятных ситуаций из-за техногенных катастроф и т.д.

Персонал

- Риск недобросовестного исполнения служебных обязанностей или установленных правил и процедур.
- Риск недостаточной квалификации работников, осуществляющих данную операцию (вероятность потери средств либо возникновения косвенных убытков вследствие низкой квалификации имеющихся сотрудников, несущих ответственность за выполнение работы на определенном участке бизнес-процесса).
- Риск недостатка (нехватки) ключевых и/или квалифицированных сотрудников на конкретном участке.
- Риск перегрузки персонала, выполняющего объем (количество) операций, больше чем это допускается психофизиологическими нормами.
- Риск мошенничества (риск возникновения убытков (недополучения прибыли) вследствие умышленных действий сотрудников).
- Риск ошибки

Правовой риск

- Внутренние факторы
- Риск несоответствия внутренних нормативных документов банка действующему законодательству.
- Неэффективная организация правовой работы, приводящая к правовым ошибкам в деятельности Банка вследствие действий служащих или органов управления кредитной организации;
- Нарушение банком условий договоров;
- Внешние факторы
- Несовершенство правовой системы (отсутствие достаточного правового регулирования, противоречивость законодательства РФ, его подверженность изменениям, в том числе в части несовершенства методов государственного регулирования и (или) надзора, некорректное применение законодательства иностранного государства и (или) норм международного права), невозможность решения

отдельных вопросов путем переговоров и как результат - обращение кредитной организации в судебные органы для их урегулирования;

- Нарушение клиентами, контрагентами условий договоров;
- Нахождение Банка, его филиалов, дочерних и зависимых организаций, клиентов и контрагентов под юрисдикцией различных государств.

Другие источники

6. Связь с риском

Целесообразно при создании события по вышеуказанному алгоритму присвоить ему «связь с риском». Например, не связан, связан с кредитным, связан с рыночным или репутационным.

7. Потери. Потери необходимо классифицировать на потенциальные и фактические. Все события поступают риск-менеджеру, который проверяет правильность их заполнения и экспортирует в базу данных. Далее, рассматриваются способы снижения операционных рисков. И конечно же, моделируется вероятность их возникновения. Базельский комитет предлагает три подхода к расчету размера капитала на покрытие операционного риска. Рассмотрим их.

Подход на основе базового индикатора

Данный подход основан на прямой зависимости уровня операционного риска (коэффициента резервирования) от масштабов деятельности организации (валового дохода).

В настоящее время коэффициент резервирования капитала под операционный риск составляет 15% от средней величины валового дохода за три последних года.

Стандартный подход

В отличие от подхода на основе базового индикатора, стандартный подход позволяет учитывать особенности возникновения операционного риска в различных направлениях деятельности и определяет размер резервируемого капитала от валового дохода в разрезе стандартных видов деятельности банка.

Согласно определению Базельского комитета первой причиной операционного риска является ошибки во внутренних процессах. Под ними понимаются операционные потери из недостаточного контроля и исполнения, например, ошибочная или неполная передача информации или потери из-за недостаточного контроля рабочих результатов или излишней регламентации. Второй причиной операционного риска является человек. Из-за его мошеннических, небрежных или ошибочных действий могут возникать потери. Типичными рисками являются недостаточная мотивация, коррупция, воровство и несоблюдение нормативно-правовых актов. Третьей причиной операционных рисков являются системы (технологии). Под них попадают, например, провал или пробои в IT программах, устарелые soft или hard программное обеспечение, нестыковка программ. Четвертой причиной выступают внешнее окружение в виде, например, природные события (землетрясений, наводнений, урагана), пожар или террористические удары. Причинами для наступления событий имеют множество внутренних и внешних причин и очень часто носят комплексный характер. Примерами, могут быть недостаточные мероприятия предупреждения наступления операционных рисков, недостатки в работе, ошибки менеджмента и слабости в организации.

В определении Базельского комитета не учтены репутационный риски и риски стратегии. Возможно, что банку будет необходимо дать свое расширенное толкование определения для того, чтобы ясно очертить круг задач и дать единую терминологическую основу для коммуникации специалистов. По мере развития менеджмента операционных рисков банк будет расширять или изменять первоначальное определение и толкование операционного риска.

Ниже нам хотелось примерах операционных рисков, которые присутствуют в банковской практике.

Операционные риски прежде всего связаны с человеком: прямые и косвенные потери бизнеса возникают из-за ошибок персонала, менеджмента,

хищений и злоупотреблений. И даже в тех случаях, когда вызваны сбоями в работе телекоммуникаций, вычислительной техники и информационных систем, в основе их в большинстве случаев лежат ошибки людей.

Риск потерь, возникающих из-за сложности финансовых инструментов. В середине 90-х, когда в стране начались операции с производными финансовыми инструментами, в некоторых банках из-за неподготовленности информационных систем возросло количество ошибок в бухгалтерском учете. Более того, банковские аналитики не всегда могли иметь реальную картину валютных и процентных рисков, возросли сроки подготовки аналитической информации для руководства. Вывод здесь прост: нельзя начинать работу с новым инструментами, не убедившись, что информационные системы банка будут корректно его отражать. Полезный инструмент, снижающий этот риск, - отработанная процедура утверждения порядка работы с новыми для банка финансовыми инструментами. Очень нагляден "контрольный листок": в нем указываются все риски, требования к системам, документации, процедурам и т. д. Новый продукт запускается в работу, если контрольный листок подписан всеми должностными лицами банка, которые в нем указаны.

Непреднамеренная поставка (последствия ошибки перевода средств в случае неверного указания банка-контрагента). Даже если это нормально работающий банк, на их возврат требуется время. В практике же приходилось сталкиваться со случаями, когда деньги направлялись в проблемный банк и даже в банк, в отношении которого открыто конкурсное производство. Уменьшить риск ошибочного перечисления денежных средств в проблемный банк можно путем установки "блокировки" в информационную систему.

Некачественная юридическая документация. Этот риск снижает обычный для банков порядок обязательного визирования юристами договоров. Проблемы возникают либо из-за недостатка квалификации, либо из-за невнимательности (как правило, в случае перегрузки работников). Еще

одна причина - несвоевременное внесение изменений в документацию в условиях часто меняющегося законодательства - здесь может помочь грамотная процедура мониторинга нормативной базы. В целом же, профессионалы рекомендуют применять "правило существенности" - когда внимание юристов концентрируется на операциях, несущих значительный (для каждого банка индивидуальный) риск потери денежных средств, а также "правило особого подхода к нестандартным операциям" - для всех нестандартных договоров устанавливается индивидуальный порядок рассмотрения.

Несанкционированный доступ к информационным системам. Этот аспект проблемы достаточно многократно описан в профессиональной литературе. Но есть и недостаточно озвученная часть проблемы - несанкционированный доступ к используемым в аналитической работе математическим моделям. Например, специалисту банка показалось, что модель несовершенна, и он самостоятельно внес в нее изменения, а ничего не знающие об этом коллеги при подготовке информации для руководства использовали старые подходы, и в результате появились ошибки. Чем сложнее бизнес банка, чем больше инструментов им используется, тем более важной становится роль математических моделей для принятия решений. Поэтому доступ к моделям и порядок внесения в них изменений должен быть жестко регламентирован - это задача, прежде всего функции внутреннего контроля. Другой аспект: расчетные модели должны своевременно пересматриваться. Международная банковская практика последних лет показала, что некоторые модели, прекрасно работающие в условиях стабильного рынка, приводят к значительным искажениям аналитических данных в кризисных условиях.

Зависимость от ограниченного числа сотрудников. Специалисты в первую очередь выделяют работников, занимающихся информационными технологиями, и клиентских менеджеров. Вопрос очень важен, поэтому заслуживает отдельного обсуждения.

Достаточно часто программист становится "незаменимым" - в его отсутствие может остановиться технологический процесс. Немало банков несло потери, когда такой специалист неожиданно увольнялся. Работа с этой категорией специалистов имеет и другие особенности. Во-первых, их трудно приучить выполнять работу в установленные сроки. Во-вторых, сложно добиться сдачи всей необходимой документации по окончании работы над программным обеспечением. На практике задача решается разными способами. С одной стороны, максимально четко оговариваются условия труда, используются разные формы морального и материального стимулирования труда (включая внедрение аккордно-премиальной системы оплаты). С другой, внедряется порядок взаимозамещения сотрудников службы информационных технологий. Есть и глобальная альтернатива: разрабатывать программное обеспечение собственными силами или полностью поручить эту задачу специализированной фирме, обслуживающей банк? Здесь важна как "цена вопроса", так и стратегическое соотношение "затраты-риск".

Ошибки в компьютерных программах. Снизить эти риски позволяет жесткая система тестирования программ до их ввода в эксплуатацию, наличие адекватной технической документации и четкое фиксирование ответственности разработчика в соответствующих договорах.

Ошибки в формулах математических моделей - не редкость в банковской практике. Например, в середине 90-х годов "Нешнл Уэсминстер Бэнк" потерял более 80 млн. долл. из-за ошибки в модели, использованной для расчета стоимости портфеля производных финансовых инструментов. Практики считают, что для снижения подобного риска хорошо работает порядок приемки моделей, включающий ее проверку на "здравый смысл" - на самых простых и понятных даже неспециалистам примерах.

Неполная или не предоставленная в срок управленческая информация. Такая проблема, как показывает практика, возникает в случае недостаточной квалификации руководства банка или из-за низкого уровня

развития систем управленческой информации. Основное условие решения (неоднократно описанное в литературе) - политическая воля руководства, как владельцев, так и высшего менеджмента банка.

Отсутствие плана работы (его низкое качество) в случае сбоя информационных систем ведет к задержкам при принятии управленческих решений, что критично (полагаю, у аналитиков любого банка есть расчет, во сколько обойдется каждый день его простоя, а косвенные потери - деловой репутации, VIP-клиентов - вообще не поддаются количественной оценке). По мнению банкиров-практиков и сотрудников аудиторских фирм, узбекские банки в последние годы овладели основными стандартными приемами и достаточно оперативно выходят из подобных критических ситуаций, однако многое еще предстоит сделать. В том числе, и с позиций внесения определенности в трудовые отношения: практически после каждой нештатной ситуации следует "разбор полетов" - выявление причин и наказание провинившихся. Между тем, должная формализация планов и процедур действия в стрессовых ситуациях не только облегчает выявление проблемных аспектов, но и уменьшает риск возникновения трудовых конфликтов.

К главным причинам возникновения операционных рисков можно отнести:

• недостаточную квалификацию персонала финансовой организации и отсутствие регулярных тренингов и обучения. «Человеческий фактор» по-прежнему является основной бедой отечественного бизнеса, так как большинство сотрудников отечественных компаний и банков не обучены грамотному применению информационных технологий и их знания не распространяются дальше «владею Microsoft Word, Internet Explorer и ICQ»;

• непонимание важности информационной безопасности и недооценка существующих угроз. Отсутствие поддержки со стороны руководства приводит к ослаблению системы управления рисками, нехватке

финансирования и выполнению действий и мероприятий по повышению уровня защищенности «спустя рукава»;

• отсутствие или недостаточная проработка процедур управления рисками и в том числе политики безопасности. Отсутствие плана действий в случае наступления того или иного риска приводит к нерациональному решению, а зачастую и вообще отсутствию решения возникшей ситуации;

• отсутствие эшелонированной системы защиты информационных активов финансовой организации от всех перечисленных выше угроз. Безопасность компании равна безопасности самого слабого звена. Злоумышленнику достаточно найти всего одну слабость в системе управления рисками, и он сможет нанести ущерб банку, страховой компании или иному финансовому институту;

• наличие уязвимостей на различных уровнях инфраструктуры АБС. Выбрасывание на рынок «сырого» программного обеспечения приводит к обнаружению в нем большого числа дыр и уязвимостей, которыми пользуются злоумышленники для совершения своих «черных дел».

В результате перечисленных выше причин возникновения операционных рисков могут наступить следующие последствия:

• внутреннее и внешнее мошенничество;

• ошибки персонала (умышленные и в результате низкой квалификации);

• сбои автоматизированной банковской системы и других типов информационных систем;

• нарушение процессов обработки и хранения данных;

• недостаточная защищенность АБС или прорехи в рубежах ее обороны и т.д.

Все эти последствия приводят к нанесению компании прямого финансового или косвенного ущерба.

Примеры последних лет показали, что проблема нанесения ущерба финансовым структурам давно вышла за пределы детективов и голливудских боевиков и стала реальностью наших дней. Несмотря на молодость многих операционных рисков, они уже приносят не только головную боль

сотрудникам финансовых структур, вынужденных с ними бороться, но и серьезный материальный ущерб, исчисляемый миллионами долларов. Например, в отчете «Electronic Security: Risk Mitigation in Financial Transactions» приведены следующие примерные суммы потерь от атак «отказ в обслуживании» для различных типов финансовых структур:

• брокерская компания — $6,5 млн в час;

• процессинговый центр — $2,6 млн в час;

• банкомат — $14,5 тысяч в час;

• онлайн-аукцион — $70 тысяч в час.

Можно отойти от сухой статистики и привести несколько реальных случаев. Начиная с 2007 года и до начала 2012 года один из западных валютных трейдеров «играл» на нескольких трейдинговых площадках, необоснованно подтасовывая различные данные в информационных системах. В результате его противоправной деятельности ущерб составил около $600 млн.

Но помимо прямых финансовых потерь надо помнить и о косвенном ущербе, который может заключаться в отзыве лицензии на оказание тех или иных банковских услуг, снижении рейтинга, оттоке клиентуры (в том числе и к конкурентам), исках со стороны пострадавших клиентов и т.п.

В другом примере логическая бомба, установленная одним из сотрудников международной финансовой корпорации, привела к удалению в компьютерной системе 10 млрд файлов. Это произошло в марте 2012 года и повлекло за собой трехмиллионный ущерб, затронувший свыше 1300 компаний, обслуживаемых в данной системе. Однако гораздо более серьезными оказались снижение доверия к данной финансовой корпорации и отказ некоторых клиентов от ее услуг.

И хотя источники операционных рисков могут быть как внутренними, так и внешними, основная угроза исходит именно изнутри финансовой организации. В 2012 году Национальный центр оценки угроз секретной службы США (National Threats Assessment Center, NTAC) и

координационный центр CERT при Университете Карнеги–Меллона провели исследование множества внутренних инцидентов в различных финансовых структурах. Данный отчет показал ряд весьма любопытных фактов.

• Большинство инцидентов совершено людьми, не имеющими никакой или очень низкую техническую квалификацию:

— как правило, они использовали не технические уязвимости, а пробелы в политике организации в области информационной безопасности;

— в 87% случаев злоумышленники использовали разрешенные команды и программы;

— в 70% случаев внутренние нарушители использовали слабости в приложениях, а в 61% — дыры в сетевом оборудовании, системном программном обеспечении или аппаратуре;

— в 78% случаев нарушители имели учетные записи в атакуемой системе, а в 43% случаев действовали открыто — под своими именами. И только в 26% случаев была зафиксирована маскировка под других пользователей;

— только 23% нарушителей находились на технических должностях (17% имели права администратора);

— 39% нарушителей не подозревали о реализуемых в организации мерах по информационной безопасности.

• Большая часть всех инцидентов (81%) планировалась заранее. Причем в 85% этих случаев информация о планируемом преступлении была известна третьим лицам (коллегам, друзьям, членам семьи и т.д.).

• Основной мотив совершения преступления — жажда наживы (81%):

— 27% злоумышленников на момент совершения преступления имели серьезные финансовые трудности;

— в 23% случаев основным мотивом была месть, в 15% — недовольство руководством и порядками в компании;

— помимо финансовой выгоды были и другие цели: 27% злоумышленников хотели саботировать бизнес-процессы в компании, а 19% совершили кражу конфиденциальной информации.

• Возраст внутренних злоумышленников находится в разбросе от 18 до 59 лет. Причем 42% из них женщины (несмотря на это, миф о том, что все хакеры — мужчины, очень живуч), а 54% — не женаты/не замужем.

• В 61% инцидентов преступления были обнаружены людьми, не отвечающими за безопасность (коллегами, клиентами и т.п.):

— также в 61% случаев обнаружение было неавтоматизированным;

— процедуры аудита и мониторинга помогли в 22%;

— журналы регистрации помогли идентифицировать источник преступления в 74% случаев.

• Финансовый ущерб наступил практически во всех зафиксированных случаях — его размер варьировался от $168 до 691 млн.

• 83% всех инцидентов происходили изнутри атакованной организации и в 70% — в рабочее время.

• В 30% случаев доступ осуществлялся из дома нарушителя.

• Число атак никак не зависело от размера организации. Например, число преступлений в банках со 100 и с 10 000 сотрудников было одинаковым.

ГЛАВА 2. Методы оценки операционных рисков и управление в системе риск-менеджмента

2.1 Методы оценки операционного риска в коммерческом банке

Цели управления операционным риском могут иметь разный масштаб и приоритет (в зависимости от субъекта, который ставит такие цели). Для государства и общества целью управления операционными рисками в банках и компаниях является, прежде всего, обеспечение стабильности экономики.

Таблица 1

Формы проявления операционных рисков[6]

Уровень 1	Уровень 2	Уровень 3
Пресонал	Криминальные действия	Сговор с криминальной целью Воровство Подделка документов
	Ошибки (нарушения) персонала	Нарушение лимитов Неполный пакет документов
Системы	Отказ (некорректность) работы систем	Отказ программного обеспечения Отказ компьютерной сети Неправильные настройки
	Нарушения в защите систем	Несанкционированное изменение данных
Процессы	Методология	Отсутствие лимитов
Внешние риски	Юридический риск	Разная интерпретация законов

Для владельцев и менеджмента конкретной организации важны практические цели, достижение которых несёт экономические выгоды и поддаётся однозначной количественной или качественной оценке. Так, на практике менеджмент компаний обычно ставит следующие группы целей:

1. Минимизация убытков организации (в том числе устранение несовершенства процессов);
2. Обеспечение стабильности бизнеса;

[6] Волков А.А. Управление рисками в коммерческом банке. – М.: ОМЕГА-Л, 2013. с – 84

3. Обеспечение достаточности капитала для покрытия будущих убытков (максимально точная оценка будущих убытков);
4. Повышение статуса организации (для улучшения условий привлечения ресурсов, для получения различных режимов благоприятствования, для повышения рейтинга, например, перед IPO).

Очевидно, что для хорошего операционного риск-менеджмента необходимы качественные данные, так как без точной истории потерь невозможно оценить уровень операционных рисков. Собрать полный объем данных подчас весьма сложно и затратно, учитывая практическое отсутствие на рынке общедоступных баз данных. И если постоянно регистрировать внутренние события — это, по большому счету, не проблема, то данные по внешним потерям бывает довольно сложно получить ввиду того, что создание баз данных по операционным рискам находится в процессе становления, и многие из крупных банков лишь недавно озаботились этой проблемой.

Для менеджмента организации важна прозрачность и понятность задач, которые будут способствовать достижению указанных выше целей. Так, на практике менеджмент компаний обычно ставит задачи по внедрению в организации и поддержанию в эффективном состоянии следующих инструментов (или компонентов) управления операционным риском:

1. Эффективная работа с инцидентами (effective incident management system).
2. Выявление рисков и их устранение (risks identification and elimination system).
3. Организация раннего предупреждения рисков (an early warning system):
    - Самооценка рисков (risk and control self-assessment — RCSA);
    - Мониторинг ключевых индикаторов рисков (key risk indicators — KRIs);
    - Мониторинг ключевых показателей эффективности управления риском (key performance indicators — KPIs);

- Мониторинг ключевых контролей риска (key control indicators — KCIs);
- Сценарный анализ рисков и стресс-тестирование (scenario analysis, stress tests);
- Анализ внешних потерь от операционных рисков (external loss data analysis);
- Ведение и оценка карт рисков (реестра рисков) (risk maps);
- Расчёт размера операционного риска (calculation of the operation risk — VaR OpRisk).

4. Обеспечение непрерывности деятельности (business continuity).
5. Координация работы всех департаментов в управлении своими рисками (coordination all units of managing their risks).
6. Система отчётов и прогнозов, поддержание базы рисков (risks database and reports).
7. Контроль соблюдения стандартов минимизации рисков (risks standards).

Схема целей и задач управления операционным риском (с учётом практических приоритетов для менеджмента организаций) представлена на рисунке справа.

Основные факторы операционного риска связаны:

- со случайными или преднамеренными действиями людей или организаций, направленными против интересов организации, в том числе несоблюдением требований законодательства и предусмотренных внутренних правил и процедур;
- с несовершенством организационной структуры (распределения обязанностей подразделений и работников), порядков и процедур, а также их документирования, неэффективностью внутреннего контроля и т. д.;
- со сбоями в функционировании систем и оборудования;
- с внешними обстоятельствами вне контроля организации.

Система Операционного Риска (далее СОР) – предназначена для сбора информации о событиях операционного риска, ее анализа и расчета капитала под риском, а также создание системы КИРов (Ключевых индикаторов риска).

Риск персонала — риск потерь, связанный с ошибками и противоправными действиями работников Банка, их недостаточной квалификацией, излишней загруженностью, нерациональной организацией труда в Банке и т. д.

Риск процесса — риск потерь, связанный с ошибками в процессах проведения операций и расчётов по ним, их учёта, отчётности, ценообразования и т. д.

Риск систем — риск потерь, обусловленных несовершенством используемых в Банке технологий — недостаточной ёмкостью систем, их неадекватностью по отношению к проводимым операциям, грубости методов обработки данных, или низкого качества, или неадекватности используемых данных и т. д.

Риски внешней среды — риски потерь, связанные с изменениями в среде, в которой функционирует Банк — изменения в законодательстве, политике, экономике и т. д., а также риски внешнего физического вмешательства в деятельность организации.

Категории типов событий операционного риска согласно Базелю II:

- Внутреннее мошенничество (Internal Fraud)
- Внешнее мошенничество (External Fraud)
- Трудовое законодательство и безопасность труда (Employment Practices and Workplace Safety)
- Клиенты, продукты и правила бизнеса (Clients, Products, & Business Practice)
- Ущерб материальным активам (Damage to Physical Assets)
- Прерывание бизнеса и сбои систем (Business Disruption & Systems Failures)

- Управление исполнением, доставкой и процессами (Execution, Delivery, & Process Management)
- В самом общем случае, банки должны рассчитывать ожидаемы потери и неожидаемые потери от операционных рисков. Ожидаемые потери могут быть включены в премию на риск при расчете ценовой политики банка. Неожидаемые потери должны покрываться экономическим капиталом и/или быть желательно вынесены за счет их трансферта.

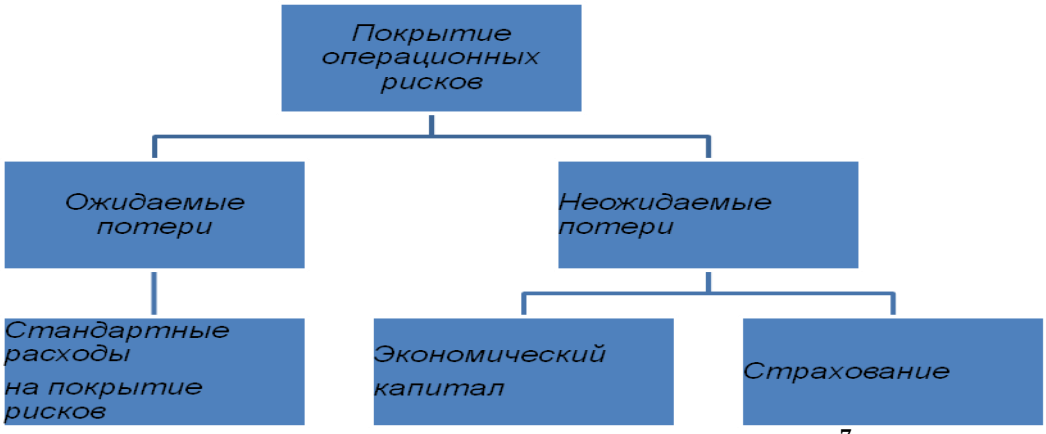

Рис. 2 Покрытие операционных рисков[7]

Базель 2 дает несколько подходов расчета операционных рисков:

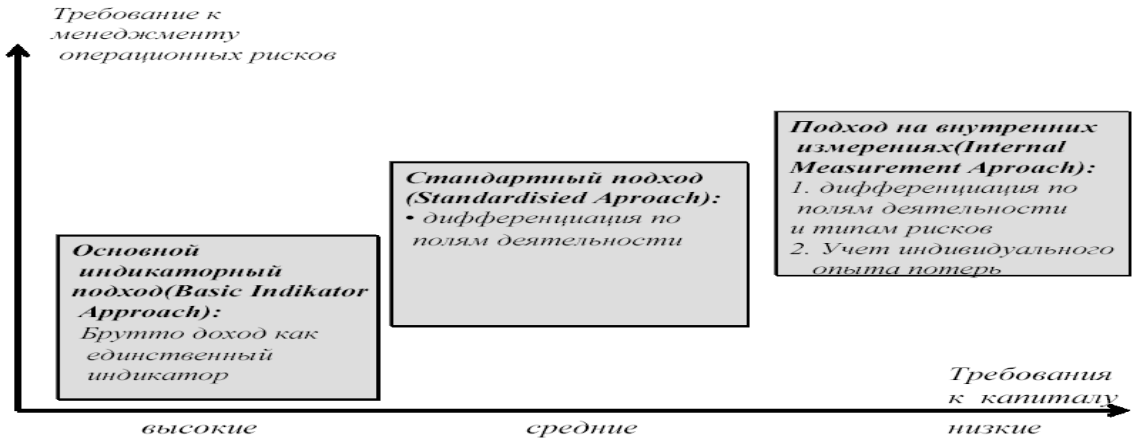

Рис. 3. Основные подходы для расчета операционных рисков.[8]

Этот подход часто критикуется за слишком грубое измерение без учета рисков в зависимости от проводимых операций банка. Поэтому предлагается стандартный подход с учетом проводимых операций банка.

[7] Беляков А.В. Банковские риски: проблемы учета, управления и регулирования (2-е изд): управленческая методическая разработка. – М.: БДЦ-пресс, 2004. С – 135.
[8] Там же

Для каждой области задано свое значения фактора риска при расчете адекватности капитала. По таблице 2 объём рисков в брутто-доходах должен не превышать 18 %, для частных лиц предел среднегодовой суммы баланса-12%.

Таблица 2

Расчёт операционных рисков согласно стандартному подходу[9]

Области деятельности	**Поля деятельности**	**Объем риска**	**Фактор капитала**
Investment Banking	**Финансирование предприятий**	Брутто доходы	18%
	Исходные данные	Брутто-доходы или VaR	18%
Banking	**Частные лица**	Среднегодовая сумма баланса	12%
	Commercial banking	Среднегодовая сумма баланса	15%
	Платежная система	Среднегодовой объем платежей	18%
Прочие	**Комиссионные сделки с ц/б**	Брутто доходы	12%
	Трастовые операции	Управляемый объем	12%

Предписания Базельского комитета для стандартного подхода рекомендуют категоризировать операции банка по трем областям:

• Investment Banking: Corporate Finance, Trading/Sales

• Banking: Retail banking, Commercial Banking, Payment/Settlement, Agency Servies

• Прочие области: Asset Management, Retail Brokerage

Наиболее сложным является расчет на основе внутренних измерений:

[9] Волков А.А. Управление рисками в коммерческом банке. – М.: ОМЕГА-Л, 2013. С – 43.

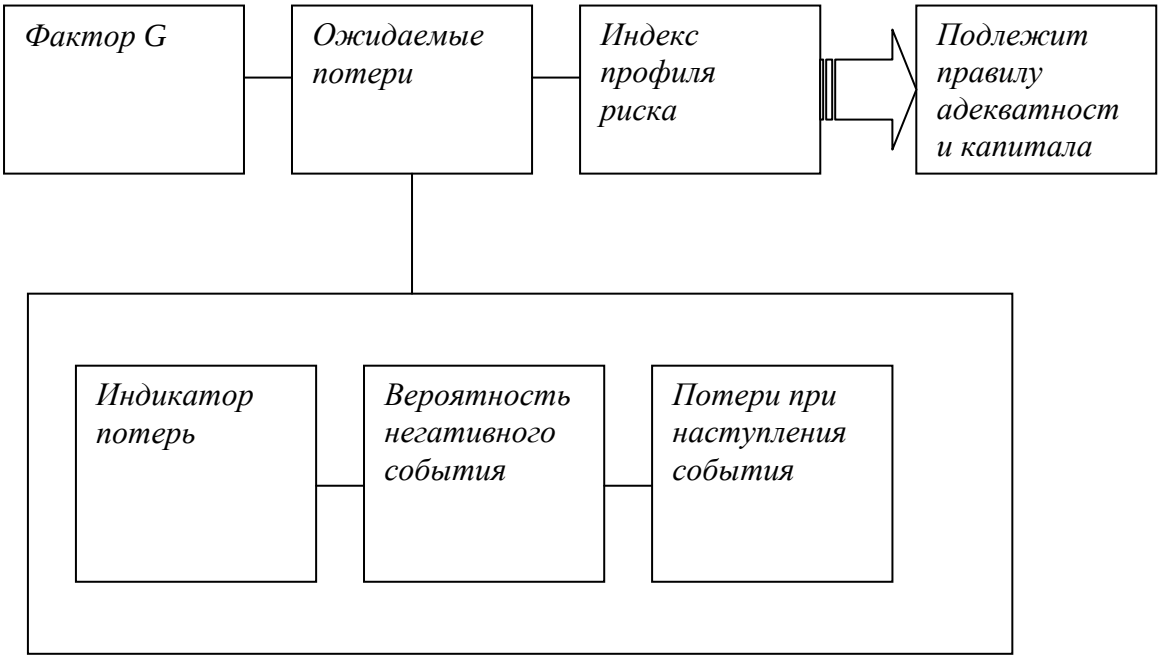

Рис. 4 Расчет операционных рисков согласно подхода на внутренних измерениях[10]

Также Базельский комитет идентифицировал виды потерь, которые конкретизируют понятие «операционного риска»:

• Write downs (амортизация): Прямое списание стоимости активов, например по причинам операционных рисков.

• Less of recourse (потери из прав регрессии): Потери по платежам, которые были направлены неправильным адресатам и которые невозможно получить обратно.

• Restitution (платежи по возмещениям): компенсационные платежи клиентам.

• Legal liabilities(Расходы по ответственности из закона):

• Regulatory&Compliance (штрафы): Денежные штрафы и прямые расходы прочих штрафов, например, отзыв лицензий.

• Loss of damage to assets (прямой вред имуществу): прямое снижение стоимости физического имущества, например, из-за пожара, землетрясения или наводнения.

[10] Димитриади Г.Г. Риски управления банком. – ЛКИ, 2010. – 240 с.

Для каждого вида потерь и области деятельности Базельский комитет идентифицировал индикаторы риска, которые служат приблизительной величиной для измерения объема подвергаемого операционному риску (Expouse-Indikator –индикатор потерь).

Таблица 3

Виды потерь, которые конкретизируют понятие «операционного риска»[11]

		Write Downs	**Loss of recourse**	**Restitution**	**Legal Liabilities**	**Regulatory &Compliance**	**Loss of or damage to assets**
Investment	Corporate finance	Объем новой сделки	Объем новой сделки	Объем новой сделки	Объем новой сделки	Объем новой сделки	Объем новой сделки
	Trading &Sales	Объем торгов	Объем торгов	Объем торгов	Объем торгов	Объем торгов	Стоимость основных средств
Banking	Retail Banking	Объем транзакций	Объем транзакций	Объем транзакций	Объем транзакций и сумма з/п	Число транзакций	Стоимость основных средств
	Commercial Banking	Объем транзакций	Объем транзакций	Объем транзакций	Объем транзакций и сумма з/п	Число транзакций	Стоимость основных средств
	Payment &Settlement	Объем транзакций	Объем транзакций	Объем транзакций	Объем транзакций (Обязательства клиентов)	Число транзакций	Стоимость основных средств
	Agency Services	Стоимость имущества в сохранении	Стоимость имущества в сохранении	Объем транзакций	Спорные суммы (Долговые обязательства	Число процессов	Стоимость основных средств
Another	Asset Management	Стоимость управляемого имущества	Стоимость управляемого имущества	Объем транзакций	Объем транзакций	Стоимость вверенных активов	Стоимость основных средств
	Retail Brokerage	Объем транзакций	Объем транзакций	Объем транзакций	Объем транзакций	Объем транзакций	Стоимость основных средств

[11] Димитриади Г.Г. Риски управления банком. – ЛКИ, 2010.С – 48

Для расчета «Expected loss- ожидаемых потерь» необходимо знать еще и «Probability of Loss Event - вероятность негативного события» и «Loss given event- потери при наступлении события». В настоящее время еще многие банки не могут оценить эти вероятностные величины.

В результате перемножения для каждой комбинации вида потерь и области деятельности получают свое значение «Expected loss- ожидаемых потерь». Это значение должно быть перемножено со средним значением для данной комбинации по всем банкам «фактором G», данным национальным органом надзора (в Узбекистане Центральным банком). Для учета специфики деятельности при имеющейся комбинации конкретного банка берется величина «Risk profile index (RPI)- индекс профиля риска».

Величина индикатора отображает отношение ожидаемых потерь при конкретной комбинации к неожидаемым потерям. Этот соотношение /профиль в конкретном банке сравнивается с такой же комбинацией предлагаемой национальным органом надзора как средняя величина по всем банкам, которая принимается равной единице. Если банк имеет нехорошее соотношение ожидаемых к неожидаемым потерям чем в среднем по банкам, то значение индикатора будет больше единицы и наоборот.

Так как нет эмпирически доказанных данных для расчета корреляции между операционными рисками, общее значение операционных рисков принимается равной простой сумме всех видов операционных рисков.

Другие подходы в расчете операционных рисков не используются. Причиной тому – недостаточный объем статистических данных.

Появившаяся новая составляющая в расчете адекватности капитала и даже еще не совсем ясные требования со стороны надзора по работе операционными рисками заставили банки заниматься данной областью. Появились объявления о найме персонала для управления операционными рисками.

Но здесь стоит задаться вопросом, а насколько высшее руководство банка готово уделять данному вопросу серьезное внимание? Не является ли

это просто данью новым веяниям, а не внутренними осознанными потребностями? Как оно понимает значение менеджмента операционных рисков и создаваемые преимущества для банка?

При неправильном отношении со стороны высшего руководства менеджмент операционных рисков обречен на прозябание и постоянные конфликты с остальными подразделениями банка, высокой степенью текучести специалистов по операционным рискам. Кому приятен человек, который настойчиво занимается поисками твоих ошибок и их причинами?

Что может дать банку правильное внедрение и текущая деятельность менеджмента операционных рисков? Снижение потерь от операционных рисков является только одной стороной медали. Другой стороной медали, является:

• внедрение культуры риска и

• создание атмосферы доверия и сотрудничества.

Эта сторона дает наибольший вклад в успешную деятельность банка.

Задайте себе следующие вопросы: насколько сегодня сотрудники банка не боятся говорить и признаваться о своих ошибках, насколько они открыты для общения и сотрудничества, передают ли они информацию на верхние уровни руководства? По историческим причинам у нас еще в управлении государственными и частными предприятиями, в самом обществе доминирует еще атмосфера поиска виновных и наказания за ошибки. Японский подход «не искать виновного, а исправлять ошибки и причины их возникновения» является новым и необходимым условием для успешной культуры на предприятии. В новых отношениях сотрудники будут сами устранять причины ошибок, больше делится информацией и охотней брать на себя ответственность а принимаемые решения. Все это даст колоссальный скачок в повышении качества правления банком. Можно сказать, что менеджмент операционных рисков создает основу “good management” и очень близок к менеджменту качества.

Операционные риски, как и иные риски, носят вероятностный характер, т.е. могут наступить или вообще не наступить. Это обстоятельство создает определенные трудности для менеджмента операционных рисков. Отсутствие ощутимых потерь от операционных рисков в течение времени, которое является успехом менеджмента операционных рисков, могут наоборот снизить внимание и придаваемое значение со стороны высшего руководства данной области управления рисками. К тому же, мы еще не имеем собственной истории скандальных потерь от операционных рисков.

Основой для количественного описания операционных рисков является наличие ожидаемых величин операционных потерь, а также возможность измерения вероятности наступления событий и эффективный размер потерь. На практике из теоретических соображений и из-за нехватки информации нет возможности осуществить полное количественное измерение.

Теоретические соображения:

• Неограниченное число возможных операционных потерь/ошибок

• Часто субъективный процесс оценки риска

• Недостаток информации об экстремальных потерях

• Экстремальная аккумуляция рисков на основе неудачного стечения комбинации определенных факторов

• Малая прогнозная очевидность прошлых событий

Таблица 4.

Подходы к измерению операционного риска[12]

	Количественное измерение	**Качественное измерение**
Top down	Подход на основе затрат и прибыли, Общие ожидаемые значения на годовой основе, Анализ чувствительности, Метод трех стоимостей, CAPM подход, Распределение вероятности,• База данных потерь	Ключевые индикаторы, Анализ полезности
Bottom up	Теория сложности • Анализ сценариев	Процессный анализ рисков • Опрос экспертов / интервью

[12] Севрук В.Т. Банковские риски. – М.: Дело ЛТД, 2007. С– 89

Каждый подход top-down или bottom-up имеют свои недостатки и преимущества. Так для методов bottom-up:

• можно быстро внедрить и концепция простая

• получаемые значения относятся ко всем категориям операционных рисков, т.е. рассматривают их в целом без конкретизации отдельных операционных рисков и без возможности оценки конкретных мероприятий контроля.

• существует стимул, расходы и доходы в отдельных областях деятельности сохранять на прежнем уровне (отказ на улучшение процессов)

• учитываются только влияние операционных рисков на отчет о прибылях и убытках. влияние на рыночную стоимость банка, например, потери репутации не принимаются во внимание.

• существует проблема признания методов со стороны сотрудников из-за непрозрачного результата.

В свою очередь bottom-up подход:

• работает с отдельными рисками через детальный анализ процессов

• количественная оценка с учетом существующего контроля и мероприятий

• связь агрегированного риска с отдельными рисками, его составляющего и соответственно лучшее признание результатов сотрудниками

• стимул к работе с признанными слабыми местами

• признание самих операционных рисков в самом банке, их причин и последствий

• однако, по сравнению с подходом top-down большие трудозатраты и расходы

Несмотря на проблемы с операционными рисками банки разрабатывают различные подходы для количественного измерения.

Признанной мерой количественной оценки риска является Value at Risk (VaR). Важным преимуществом расчета операционных рисков на основе

Value at Risk является включение операционных рисков в аллокацию экономического капитала на основе методов аллокации по концепции Value at Risk

Для расчета большинства операционных рисков лучше и естественней принять период в 1 год.

Для некоторых операционных рисков, например, ошибок при обработке торговых документарных операциях, можно принять меньший период рассмотрения. Значения VaR затем «растягивают» на период 1 год.

Все здесь зависит от конкретного случая и нет какого-либо стандартного подхода. Для расчета общего риска необходимо знать еще и корреляцию рисков. Знание корреляционных данных очень трудоемкая и затратная работа.

Одним из важных ограничений при использовании подавляющего числа методов расчета рисков на основе Value at Risk является нормальное распределение случайной величины. Данное требование не существенно для одного самого распространенного симуляционного метода Монте Карло. Но для него также необходимо также знать вид распределения случайных величин.

Сложностью для расчета операционных рисков на основе Value at Risk помимо нехватки статистических данных является высокая степень асимметрии распределения вероятности потерь, т.е. не нормальное распределение случайной величины.

Следующей сложность является знание значений корреляции для агрегации рисков на уровне портфеля и всего банка. Некоторые операционные риски могут иметь корреляцию между собой и это надо обосновать наблюдениями и расчетами. Также для агрегации рисков на уровне банка надо знать и корреляцию между рыночными, кредитными и операционными рисками. Естественно, такую агрегацию можно производить корректно только между значениями, имеющими одну основу в виде одной

единицы измерения, одинакового периода рассмотрения и одной величины доверительного интервала.

Существуют несколько широко употребляемых методов расчета операционного риска как величины Value at Risk (VaR):

• Базы данных по операционным рискам

• Симуляционные методы

• Актуарный метод

• Расчет на основе отклонения от стандартных величин

Но на сегодняшний день можно сказать, что в Казахстане и Кыргызстане использование моделей количественного расчета на основе VaR не дадут требуемого уровня доверия из- за отсутствия надежных данных. Такие модели требуют много временных ресурсов и трудозатрат, которые не оправдаются.

Можно использовать методы количественного расчета операционных рисков не на основе Value at Risk , но и для них есть проблема с данными и, главное, результат в виде величины показателя риска получается с отсутствием статистически обоснованного значения вероятности.

Поэтому на сегодняшний день лучше всего сконцентрироваться на задачах правильного внедрения, качественных оценках и внедрении культуры риска в банке, созданию и ведению базы данных по операционным рискам.

В Базеле II предусмотрены следующие подходы к оценке операционного риска банков:

Подход базового индикатора (BIA, Basic Indicator Approach)

Стандартизированный подход (TSA, The Standardized Approach) и альтернативный стандартизированный подход (ASA)

Продвинутые подходы (AMA, Advanced Measurement Approach), включающие в себя такие подходы как:

Подход внутреннего измерения (IMA, Internal Measurement Approach)

Подход на основе распределения потерь (LDA, Loss Distribution Approach)

Подход на основе моделирования сценариев (SBA, Scenario-based approach)

Подход оценочных карт или балльно-весовой подход (SCA, Scorecard Approach)

В документах Базеля предусмотрены три вида субъектов, управляющих операционными рисками (три линии защиты):

1-я линия защиты — все подразделения и сотрудники организации (они работают с операционными рисками на месте его возникновения).

2-я линия защиты — субъект, который координирует в целом всю систему управления операционными рисками.

3-я линия защиты — подразделение внутреннего аудита, которое осуществляет независимый аудит системы управления операционными рисками.

Довольно часто на практике возникают споры, кого относить ко второй линии защиты. Так, помимо подразделения по операционным рискам, во вторую линию защиты себя записывают служба безопасности, служба комплаенс и иные сервисные подразделения (не бизнес-подразделения). Они обосновывают такую позицию тем, что устанавливают обязательные для всех правила по курируемым ими профильным рискам, а значит занимают по отношению к таким подразделениям роль координатора в рамках предмета своих функций. Во-первых, множественность координаторов системы противоречит принципу единоначалия, согласно которому конечным координатором системы (ответственным) должен быть один субъект. Во-вторых, множественность субъектов во второй линии защиты противоречит требованиям нормативных документов (см. ссылку выше). В-третьих, факт того, что служба безопасности, служба комплаенс и иные сервисные подразделения устанавливают обязательные для всех правила по профильным рискам, не является в данном случае аргументом, так как если

развивать это обоснование дальше, то подразделение внутреннего аудита (3-я линия защиты) должно в таком случае «переместиться» в первую линию, так как для него также будут действовать требования безопасности или комплаенс.

Чтобы соблюсти с одной стороны логичное требование о единоначалии координатора системы, закреплённое в нормативных документах, а с другой стороны требования подразделений, управляющих профильными рисками об их вынесении во вторую линию защиты, нередко применяется условное выделение двух «подобластей» в рамках первой линии защиты (условно 1.1. и 1.2.). Так в состав линии 1.1. входят бизнес-подразделения, а в состав линии 1.2. входят владельцы профильных рисков. Схема субъектов, управляющих операционными рисками (с учётом особенностей первой линии защиты), представлена на схеме справа.

Организации сами определяют виды ответственных, их численность и особенности распределения прав и обязанностей внутри каждой линии защиты. Ниже представлен один из возможных вариантов такого распределения, который соответствует представленной справа схеме.

Первая «линия защиты» включает в себя процесс управления операционными рисками на уровне каждого подразделения организации, её процессов, средств и ресурсов (децентрализованный подход).

В рамках первой линии защиты в подразделениях организации операционными рисками управляют:

- риск-координаторы;
- эксперты по инцидентам;
- регистраторы.

Риск-координаторы — это сотрудники, которые отвечают за организацию управления операционными рисками конкретного департамента и региональных сотрудников, функционально подчинённых этому департаменту. Риск-координаторами являются руководитель департамента и

сотрудники, назначаемые им для выполнения обязанностей риск-координатора.

Обязанность риск-координатора — организовать и контролировать выполнение сотрудниками своего департамента и региональными сотрудниками следующих риск-процедур:

1. Эффективная работа с инцидентами.
2. Выявление рисков и их устранение.
3. Поддержание инструментов раннего предупреждения рисков.
4. Обеспечение непрерывности деятельности.
5. Координация работы всех функционально курируемых сотрудников в управлении их рисками.
6. Поддержание системы отчетов и прогнозов по рискам.
7. Контроль соблюдения стандартов минимизации рисков.

Эксперты по инцидентам — это сотрудники подразделений организации (находящиеся в Центральном или Головном офисе, региональных и иных подразделениях), которые в рамках своих полномочий занимаются устранением последствий произошедших инцидентов.

Обязанность эксперта по инцидентам — организовать и осуществлять эффективную работу с инцидентами (их идентификацию, минимизацию ущерба, расследование, отчёт об исполнении мер) и оказание помощи риск-координатору и риск-менеджеру в организации риск-процедур.

Регистраторы — это все сотрудники подразделений, так как в рамках выполнения своих функций они могут обнаруживать инциденты и проблемы, вызывающие операционный риск. Обязанность регистратора — незамедлительно сообщать эксперту по инцидентам и риск-координатору об обнаруженных инциденте, проблеме или риске (или регистрировать их).

Перечисленные субъекты первой линии защиты, безусловно, имеются во всех департаментах организации, так как каждый департамент в текущем состоянии уже производит разбирательства с инцидентами, проводит методологические и технологические улучшения своих процессов,

обеспечивает взаимозаменяемость сотрудников (в рамках непрерывности деятельности) и т. д. Если эти субъекты департаментов не оформлены должным образом, то риск-менеджеры оказывают помощь этому подразделению для соответствующего их оформления и обучения.

Вторая «линия защиты» включает в себя процесс координации системы управления операционными рисками в целом, проверку данных и отчетов об операционных рисках, организацию деятельности комитетов по риску, представление отчетности руководству организации (централизованный подход).

В рамках второй линии защиты операционными рисками управляют:

- комитет по рискам;
- директор по рискам (или заместитель председателя правления по рискам);
- риск-менеджеры (сотрудники подразделения по операционным рискам).

Комитет по рискам (или иной комитет, наделенный соответствующими полномочиями – далее – комитет по рискам).

Комитет по рискам (в рамках управления операционными рисками) – это высший коллегиальный орган, который принимает решения о действиях организации в отношении тех или иных рисков (в т.ч. операционных). Председателем комитета по рискам обычно является директор по рискам с правом вето на любые решения комитета.

Права комитета по рискам (в рамках управления операционными рисками):

1. Разрешает разногласия, возникающие в ходе процесса управления операционными рисками. Принимает решения по операционным рискам красной зоны, а также менее значимым рискам, когда они были эскалированы до уровня комитета.
2. Утверждает методологию управления операционными рисками для обеспечения общего понимания рисков.

3. Утверждает уровень операционного риска на год – риск-аппетит организации (пороговый риск в части разработки и утверждения мер по его минимизации).
4. Инициирует разработку стратегий, политики и основополагающих подходов к управлению операционными рисками организации и представляет их на согласование в Правление организации.
5. Осуществляет постоянный мониторинг соответствия подходов к управлению операционными рисками принятой стратегии.
6. Утверждает отчеты по управлению операционными рисками, подлежащими включению в отчет для Правления организации.
7. Инициирует разработку эффективных мер и осуществляет последующий контроль над операционными рисками в рамках заседаний комитета.
8. Утверждает сферу компетенции подразделений по управлению операционными рисками, а также обеспечивает наличие у них достаточных ресурсов и соответствующего доступа к информации для эффективного осуществления своих функций.

Директор по рискам (в рамках управления операционными рисками) – это лицо, которое принимает решения о действиях организации в отношении операционных рисков, относимых к рискам желтой зоны, а также по рискам зеленой зоны в случаях, когда они были эскалированы до уровня директора по рискам. Директор по рискам отвечает также за организацию управления операционными рисками во всей организации и за эффективность управления операционными рисками.

Риск-менеджеры – это сотрудники, которые отвечают за организацию управления операционными рисками во всей организации (в каждом подразделении и каждым сотрудником). Риск-менеджерами являются все сотрудники подразделения по операционным рискам.

Обязанность риск-менеджера – организовать и контролировать выполнение в каждом департаменте и подразделении организации следующих риск-процедур:

1. Эффективная работа с инцидентами.
2. Выявление рисков и их устранение.
3. Функционирование системы раннего предупреждения рисков.
4. Обеспечение непрерывности деятельности.
5. Координация всей работы в управлении операционными рисками.
6. Система отчетов и прогнозов, поддержание базы рисков.
7. Контроль соблюдения стандартов минимизации рисков.

Третья «линия защиты» включает в себя процесс независимого контроля и регулярного аудита эффективности всей системы управления операционными рисками и контроля её соответствия требованиям ЦБ РФ и Базельского комитета.

В третьей линии защиты, операционными рисками управляет подразделение по аудиту, а именно аудиторы.

Обязанность аудитора (в рамках управления операционными рисками) – осуществлять текущий независимый контроль и регулярный аудит эффективности всей системы управления операционными рисками и её соответствия требованиям ЦБ РФ и Базельского комитета, а также давать заключения о соответствии или несоответствии с замечаниями, которые должны быть устранены.

Операционные убытки:

Западная практика:

BARINGS PLC — 1995, USD 1.3 млрд. — несанкционированная торговля Nick Leighson.

Mizuho Securities — Декабрь 2005 (USD 250 млн.) — торговая ошибка (продал 620 тыс. акций за 1 иену вместо продажи 1 акции за 620 тыс. иен) —

проданные акции в 4 раза превышают объем акций компании, находящийся в обращении; синдром «толстого пальца» (тех. ошибки при биржевых операциях).

SG — 2008, 4.9 млрд. Евро за вычетом налогов (или 6.3 млрд до вычета налогов). Причины -: • несанкционированная торговля, поддельное хеджирование, риск, измеренный/оцененный на основе после выплаты налогов, • управление паролем и знание механизмов контроля • Слабые механизмы контроля; «культура терпимости», игнорирование сигналов предупреждения • структура поощрения трейдеров…. и т. д..

UBS — списание субстандартных кредитов, связанное с потерями при невыполнении обязательств (свыше $38 млрд.), S&P понизил рейтинг до AA- в связи с «упущениями в сфере управления рисками». Без увеличения капитала или коэффициент достаточности капитала 1 уровня упадет до 7 % (ОР в рамках убытка по кредитному риску).

Ипотечный кризис в США — регистрация залогов по ипотечным кредитам не в реестрах местных органов власти, а в принадлежащей банкам Электронной системе регистрации (64 млн ипотек).

2.2 Организация управления операционными рисками

Система управления операционными рисками — комплекс организационных, методических, информационных средств, направленных на предупреждение возможных операционных рисков, минимизацию отрицательных последствий и недопущения повторных инцидентов операционного риска.

Управление операционными рисками призвано обеспечить снижение убытков организаций от различного рода инцидентов операционного риска, обеспечить менеджмент компании системой формирования «планов мероприятий по предупреждению операционных рисков» и «планов действий при наступлении инцидентов операционного риска».

Принципы управления операционными рисками

Базельский комитет установил следующие основные принципы управления операционным риском в кредитной организации:

Принцип 1. Ключевая роль совета директоров в формировании и обеспечении развитой культуры управления операционным риском на всех уровнях организации

Принцип 2. Банки должны создавать, внедрять и использовать систему управления, полностью интегрированную в общий процесс управления рисками

Принцип 3. Совет директоров должен разработать и анализировать систему управления рисками и осуществлять контроль над исполнительными органами;

Принцип 4. Совет директоров должен установить риск-аппетит и допустимый уровень риска

Принцип 5. Исполнительный орган должен разработать и представить совету директоров четкую, эффективную и надежную управленческую структуру с точно определенными, прозрачными и непротиворечивыми сферами компетенции. Исполнительный орган несет ответственность за последовательное внедрение и применение принципов, процессов и систем управления операционным риском в соответствии с риск-аппетитом и допустимым уровнем риска.

Принцип 6. Исполнительный орган должен обеспечить выявление и оценку операционного риска с целью четкого понимания природы и факторов риска

Принцип 7. Исполнительный орган должен обеспечить одобрение нововведений с учетом операционных рисков

Принцип 8. Исполнительный орган должен организовать регулярный мониторинг операционного риска, включая систему отчетности подразделений.

Принцип 9. Наличие надежной системы внутреннего контроля, а также надлежащей системы снижения или передачи риска.

Принцип 10. Разработка планов обеспечения непрерывности и восстановления деятельности в случае реализации операционных рисков.

Принцип 11. Информация, публикуемая банком, должна позволять заинтересованным сторонам оценивать его подход к управлению операционным риском

Методы управления операционными рисками:

- Риск-аудит операций, процедур и направлений деятельности
- Сбор и анализ внутренних и внешних данных по операционным рискам
- Мониторинг ключевых индикаторов риска (KRI)
- Оценка (включая сценарный анализ) и самооценка операционного риска бизнес-подразделениями
- Регламентация бизнес-процессов (внутренних правил и процедур)
- Контроль соблюдения законодательства и внутренних правил и процедур
- Контроль информационно-технологических рисков
- Обучение и совершенствование системы мотивации персонала
- Автоматизация бизнес-процессов, в том числе отдельных (стандартных) процедур контроля
- Регулярная внутренняя отчетность по операционным рискам
- Разработка планов по обеспечению непрерывности деятельности и действий на случай реализации операционных рисков
- Страхование от операционных рисков
- Аутсорсинг отдельных функций

Ключевой индикатор операционного риска (KRI, в русском варианте — КИР или КИОР) — показатель, используемый для отслеживания и прогнозирования фактов реализации операционного риска.

Ключевые индикаторы риска используются для регулярного (с различной периодичностью — в зависимости от ключевого индикатора риска)

мониторинга подверженности риску, проявления риска и источников (причин) потерь.

Примеры ключевых индикаторов риска: текучесть кадров; количество сбоев оборудования; простои оборудования; количество исправительных ордеров; количество выявленных нарушений законодательства, внутренних документов и др.

Классификация риска

● Базельский комитет предлагает следующую классификацию источников операционного риска:

- персонал (намеренные действия сотрудников компании, которые могут нанести ущерб ее деятельности);
- процессы (ошибки и некорректное исполнение операций в ходе осуществления бизнес-процессов либо исполнения должностных обязанностей);
- системы (нарушение текущей деятельности в результате сбоя информационных систем или недоступности сервиса);
- внешняя среда (атаки либо иные угрозы, исходящие из внешней среды, которые не могут управляться компанией и выходят за рамки ее непосредственного контроля).

Внутренними и внешними источниками (причинами) операционного риска являются:

- случайные или преднамеренные действия физических или юридических лиц, направленные против интересов кредитной организации (риск недобросовестного исполнения персоналом банка своих служебных обязанностей, риск перегрузки персонала, риск ошибок при вводе данных, риск предоставления клиентом неверной или неполной информации и т.д.);
- несовершенство организационной структуры кредитной организации в части распределения полномочий подразделений и служащих (риск неверной организационной структуры банка); порядков и процедур

совершения банковских операций и других сделок, их документирования и отражения в учете (риск методологии, правовой риск и т.д.); несоблюдение служащими установленных порядков и процедур; неэффективность внутреннего контроля;

- сбои в функционировании систем и оборудования (технологический риск);
- неблагоприятные внешние обстоятельства, находящиеся вне контроля кредитной организации (риск хищения активов, риск несанкционированного проникновения в процессы банка и т.д.);
- прочее

Система управления операционным риском намного сложнее, чем, например, рыночным или кредитным, так как:

- операционный риск является внутренним риском для финансовой организации, поэтому крайне сложно создать универсальный перечень причин возникновения данного вида риска;
- операционный риск очень сложно оценить количественным методом.

Важной составляющей системы управления операционным риском является контроль и регулярная отчетность. Под управлением операционном риском понимается минимизация возможных операционных потерь. Она обеспечивается с помощью:

- комплекса мер, направленных на снижение вероятности наступления событий или обстоятельств, приводящих к операционным потерям, и (или) на уменьшение (ограничение) размера потенциальных операционных потерь;
- мер по обеспечению непрерывности финансово-хозяйственной деятельности при совершении банковских операций и других сделок;
- планирования и разработки сценариев на случай непредвиденных ситуаций;
- обеспечения оперативного восстановления бизнеса в случае наступления чрезвычайных ситуаций; - разработки и реализации

мероприятий по ограничению и нейтрализации выявленных критических зон риска;

- развития банковских технологий, правил и процедур совершения операций;
- защиту информации;
- развития системы автоматизации
- прочие меры

В целях мониторинга операционного риска применяется система индикаторов уровня операционного риска (фиксирования событий), т.е. показателей, которые связаны с уровнем операционного риска, принимаемого кредитной организацией. При определении индикатора риска формулируется гипотеза о существовании в банке объективного измеримого количественного показателя риска, который характеризует определенную группу потерь. В качестве индикаторов уровня операционного риска могут быть использованы:

- сведения о количестве несостоявшихся или незавершенных банковских операций и других сделок, увеличении их частоты или объемов;
- текучести кадров;
- частота допускаемых ошибок и нарушений;
- прочее.

Для каждого индикатора рекомендуется установить лимиты (пороговые значения), что позволит обеспечить выявление значимых для кредитной организации операционных рисков и своевременное адекватное воздействие на них.

Основным компонентом операционного риска, подлежащего регулированию, является совершение несанкционированных операций, ошибки в работе персонала, нарушения и сбои в работе компьютерных сетей и оборудования.

В целях минимизации операционного риска, а также исключения возможных убытков (потерь) в Банке на постоянной основе осуществляется

выявление и сбор данных о внутренних и внешних факторах операционного риска. На основе полученной информации формируется аналитическая база данных о понесенных операционных убытках, где отражаются сведения о видах и размерах операционных убытков в разрезе направлений деятельности Банка, отдельных банковских операций и других сделок, обстоятельств их возникновения и выявления. Риск-подразделение Банка осуществляет анализ и дает оценку операционного риска. Банк производит оценку операционного риска в соответствии с рекомендациями Базельского комитета по банковскому надзору (Базель II), а также оценку с использованием балльно-весового метода, сущность которого заключается в оценке операционного риска в сопоставлении с мерами по его минимизации. Применение балльно-весового метода оценки операционного риска позволяет выявить слабые и сильные стороны в его управлении. Банком устанавливается допустимый (нормальный) уровень операционного риска не выше 20%. Уровень операционного риска ниже допустимого (нормального) считается «низким», а уровень операционного риска выше допустимого уровня считается «высоким» уровнем, требующим применения мер по его минимизации. Операционным риском управляет Комитет по управлению рисками.

Целями управления и контроля над операционным риском являются минимизация информационных и финансовых потерь, связанных с отражением банковских операций на счетах бухгалтерского учета, а также адекватностью отражения учетной информации в различных формах отчетности, с эксплуатацией программного обеспечения, использованием в деятельности Банка технических средств и высокотехнологического оборудования при реализации банковских услуг. Управление данной категорией рисков осуществляется через принятие процедурных норм по операциям Банка и утверждения положений структурных подразделений, а также должностных инструкций сотрудников Банка с целью разграничения их функций и полномочий.

Одним из инструментов, позволяющих выявить операционные риски, является анализ административно-управленческих расходов на основе данных бухгалтерского или аналитического учета. Предметом данного анализа являются расходы, непосредственно связанные с операционными рисками (штрафы, пени и т.д.), а также операционные расходы (явные или вмененные), возникновение которых не может быть объяснено движениями рынков или кредитными событиями. Анализ расходов позволяет выявить источники операционных рисков, а также дать количественную или статистическую оценку.

Для минимизации операционного риска можно применить следующие основные инструменты:

- разграничение доступа к информации;
- разработка защиты от несанкционированного входа в информационную систему;
- разработка защиты от выполнения несанкционированных операций средствами информационной системы;
- организация контролирующих рабочих мест до исполнения документов;
- автоматическое выполнение рутинных повторяющихся действий;
- аудит (регистрация и мониторинг) действий пользователей.

В настоящее время коммерческие банки активно внедряют программы по оценке и управлению операционными рисками. Такие методики определяют порядок управления операционными рисками, в основе которого лежит качественное выявление всех внутренних процессов и операций банка, подверженных идентифицируемым источникам рисков, оценка данных рисков и выработка путей предотвращения их возникновения.

2.3 Модели управления операционными рисками

По состоянию на 1 января 2015 года совокупный капитал банковской системы составил 6,9 трлн. сум или увеличился за 2014 год на 25%.

Устойчивость коммерческих банков повысилась. В частности, достаточность капитала банковской системы составила 23,8% активов, взвешенных с учетом риска, что почти в 3 раза превышает общепринятые международные стандарты (8%). Показатель ликвидности банковской системы достиг 64,6% (при уровне индикаторной оценки «высокий» - 30%).

Таблица 5

Основные показатели финансовой устойчивости банковской системы Республики Узбекистан[13]

№ п/п	Показатели	на 1.01.2012	на 1.01. 2013	на 1.01. 2014	на 1.01. 2015
1.	Регулятивный капитал к активам, взвешенных с учетом риска	24,1%	24,3%	24,3%	23,8%
2.	Регулятивный капитал 1 - уровня к активам, взвешенных с учетом риска	21,8%	22,3%	22,5%	22,1%
3.	Недействующие ссуды за вычетом резервов/общий объем капитала	1,2%	1,0%	0,9%	0,9%
4.	Недействующие ссуды/общая сумма ссуд	0,7%	0,5%	0,4%	0,4%
5.	Рентабельность активов	1,9%	1,9%	1,95%	1,97%
6.	Рентабельность капитала	14,4%	16,3%	17,2%	17,6%
7.	Процентная маржа/валовой доход	35,2%	36,4%	36,4%	37,2%
8.	Непроцентные расходы/валовой доход	67,0%	65,6%	64,0%	60,2%
9.	Ликвидные активы/всего активы	31,2%	31,8%	31,9%	31,9%
10.	Ликвидные активы/краткосрочные обязательства	71,3%	73,4%	73,5%	74,7%
11.	Совокупный капитал на конец периода/всего активы	12,2%	11,4%	11,2%	11,7%

[13] МВФ и Центральный банк Республики Узбекистан

Устойчивость банковской системы обеспечена за счет повышения качества корпоративного управления в банках, повышение транспарентности структуры акционеров и обязательной продажи части акций (25%) на фондовом рынке, усиления контроля за формированием капиталов банков.

Рост совокупного капитала банков произошел, в основном, за счет увеличения банками уставного капитала путем выпуска дополнительных акций и размещения их среди инвесторов, а также за счет направления части прибыли на увеличение уставного капитала.

В декабре 2014 года рейтинговые агентства «Стандарт энд Пурс» и «Фитч рейтинг» еще раз оценили деятельность банковской системы Узбекистана как «стабильная». При этом эти рейтинговые агентства отмечают хорошие показатели прибыльности банков Узбекистана и качества их активов, стабильный уровень ликвидности, обеспеченный ростом клиентских депозитов и капитала, в качестве основных факторов устойчивости и развития банковской системы республики.

Динамичный рост банковских услуг за последнее годы достигается, наряду с традиционными, расширением спектра и качества оказываемых услуг с широким применением информационно-коммуникационных технологий.

Последние годы существенный вклад в рост объема услуг в республике вносят финансовые институты (банки, страховые и лизинговые компании) республики. В частности, только в 2014 году, объем банковских услуг возрос более чем в 1,3 раза. При этом в 2014 году доля банковских услуг, в общем объёме финансовых услуг выросла до 89 процентов.

Если по итогам 2011 года положительные рейтинги имели 13 коммерческих банков Узбекистана, то на 1 января 2014 года всем 26 банкам республики присвоены положительные рейтинговые оценки. Национальный банк внешнеэкономической деятельности, «Асакабанк»,

Узпромстройбанк, «Ипотекабанк», «Агробанк» и «Ипак йули банк» имеют положительные рейтинговые оценки одновременно от двух ведущих международных рейтинговых агентств.

Кроме того, оценка развития и деятельности банковской системы на основе разработанных согласно международным требованиям национальных индикаторов финансовой устойчивости и развития банковской системы, также соответствует уровню «высокий». Так, показатели ликвидности, достаточности совокупного капитала, динамики объемов депозитов и кредитных вложений банковской системы превышают критериев «высокого» уровня оценок.

Таблица **6**

Основные показатели развития банковской системы Республики Узбекистан (на конец периода) [14]

№	***Наименование показателей***	***2009***	***2010***	***2011***	***2012***	***2013***	***2014***
1	Количество банков	30	31	30	29	28	26
	из них:						
	государственные банки	3	3	3	3	3	3
	банки с участием иностранного капитала	5	5	5	4	4	5
	частные банки*	10	10	9	9	9	8
2	Количество банковских подразделений	7 383	7 510	7 781	8 058	8 152	8 211

В настоящее время банки активно развивают удобные для клиентов формы услуг, которые позволяют владельцам банковских счетов осуществлять операции со своих счетов по программной сети «банк-клиент» не приходя в учреждения банков и получать информацию о банковских счетах через мобильные и электронные связи в режиме реального времени. Количество пользователей ими за 2014 год увеличилось более чем в 2 раза и составило 519 тыс**.** клиентов.

Систему управления операционными рисками составляют следующие элементы:

[14] МВФ и Центральный банк Республики Узбекистан

1. Идентификация и оценка категорий источников операционных рисков
2. Составление каталога процессов и операций банка;
3. Идентификация проявления тех или иных категорий операционных рисков и оценка их уровня на конкретных процессах и операциях;
4. Выявление критических зон риска (или групп операций с повышенным уровнем риска);
5. Разработка и реализация мероприятий по ограничению и нейтрализации выявленных критических зон риска;
6. Внедрение инструментов контроля выявленных стандартных видов операционного риска, повышение надежности отдельных элементов процессов и технологий;
7. Разработка предложений по организационным преобразованиям с целью оптимизации осуществляемых бизнес-процессов, включающих документооборот, информационные потоки, распределение функций, полномочий и ответственности.

Базельский комитет предлагает следующие коэффициенты резервирования в разрезе восьми основных видов деятельности банка:

Таблица 7

Коэффициенты резервирования [15]

Направление деятельности	Резерв от валового дохода за три последних года
Корпоративные финансы	18 %
Торговые операции	18 %
Розничное банковское обслуживание	12 %
Коммерческое банковское обслуживание	15 %
Услуги по осуществлению платежей и расчетов	18 %
Агентские услуги	15 %
Управление активами	12 %
Розничные брокерские операции	12 %

[15] www.bis.org

Передовые подходы к оценке операционного риска предполагают использование собственных моделей анализа риска. Банки могут применять свои модели оценки операционного риска с разрешения надзорных органов при условии, что они удовлетворяют определенным количественным и качественным критериям. Внутрибанковские методы оценки риска должны основываться на статистике банка по операционным потерям в течении как минимум 5 лет.

Методы, основанные на применении статистического анализа распределения фактических убытков, позволяют сделать прогноз потенциальных операционных убытков исходя из размеров операционных убытков, имевших место в данной кредитной организации в прошлом. При применении этих методов в качестве исходных данных рекомендуется использовать информацию, накопленную в аналитической базе данных о понесенных операционных убытках.

Балльно-весовой метод (метод оценочных карт). Сущность балльно-весового метода заключается в оценке операционного риска в сопоставлении с мерами по его минимизации. На основе экспертного анализа выбираются информативные для целей управления операционным риском показатели и определяется их относительная значимость (весовые коэффициенты). Затем выбранные показатели сводятся в таблицы (оценочные карты) и оцениваются с использованием различных шкал. Полученные результаты обрабатываются с учетом весовых коэффициентов и сопоставляются в разрезе направлений деятельности кредитной организации, отдельных видов банковских операций и других сделок. Применение балльно-весового метода (метода оценочных карт) наряду с оценкой операционного риска позволяет выявить слабые и сильные стороны в управлении операционным риском.

Моделирование. В рамках метода моделирования на основе экспертного анализа для направлений деятельности кредитной организации, отдельных видов банковских операций и других сделок определяются возможные сценарии возникновения событий или обстоятельств, приводящих к

операционным убыткам, и разрабатывается модель распределения частоты возникновения и размеров убытков, которая затем используется для оценки операционного риска.

Операционные риски напрямую связаны с ошибками персонала, системы и технологий банка. У каждой конкретной финансовой организации имеется своя организационная структура, система, технологии, поэтому и операционные риски имеют свои особенности. Именно поэтому, невозможно основываясь на теоретических знаниях выработать стратегию по снижению уровня операционного риска. Необходим тщательный анализ всех составляющих в конкретной финансовой организации.

Операционные риски, в соответствие с общими принципами стандартов качества управления (ISO9000-2000), управляются процессным подходом. Таким образом, система управления операционными рисками состоит в единстве и взаимодействии шести основных методологических категорий:

1. Тип операционного события (type of event);
2. Объект риска (object of risk);
3. Источник (причина) риска (source of risk);
4. Понятие события или реализация риска (event of risk);
5. Результат (последствие) событий (result of event, type loss);
6. Оценка или мера риска (estimation or measure of risk).

В СОР задействованы все перечисленные методологии сбора информации о событиях операционного риска.

КИРы в управлении операционными рисками являются основными инструментами. С их помощью можно проводить широкий спектр измерений так часто, как это требуется. Что отражено на рисунке 5.

Рис. 5 Системы управления операционными рисками[16]

Целью КИРов является прогнозирование неблагоприятного события и предотвращение возможных потерь при его реализации.

Система Операционного риска включает в себя три модуля:

1. Модуль сбора данных о событиях операционного риска;
2. Модуль анкетирования;
3. Модуль КИРов.

Рис. 6 Модули системы управления систем операционных рисков [17]

Модуль сбора данных о событиях операционного риска включает в себя возможность регистрации события, ввода данных о событии, оценки финансовых потерь из-за наступления события, назначение ответственных за событие и ликвидацию его последствий, мониторинг ликвидации

[16] Волков А.А. Управление рисками в коммерческом банке. – М.: ОМЕГА-Л, 2013.С – 96
[17] Там же

последствия событий (значительная база событий операционного риска позволяет проводить оценку вероятности событий операционного риска не только экспертным методом, но и на основе статистического анализа).

Рис. 7 Модули сбора данных[18]

Модуль анкетирования включает конструктор анкет, настраиваемых сотрудниками банка, а также алгоритмы анализа статистических данных о событиях операционного риска и данных анкет.

Рис. 8 Модуль анкетирования[19]

Модуль КИРов (Ключевых индикаторов риска) – включает алгоритмы расчет КИРов, сигнализирующих о превышении допустимого уровня риска. А также алгоритмы расчета капитала под риском (Базель 2).

[18] www.bis.org
[19] www.bis.org

Рис. 9 Модуль КИРов[20]

В системе действуют методы оценки операционного риска, которые применены в международной банковской практике:

1. Статистический анализ распределения фактических убытков;
2. Балльно-весовой метод (метод оценочных карт);
3. Моделирование (сценарный анализ).

Рис. 10 Методы анализа операционных рисков[21]

Методы, основанные на применении статистического анализа распределений фактических убытков, позволяют сделать прогноз потенциальных операционных убытков исходя из размеров операционных убытков, имевших место в данной кредитной организации в прошлом. Статистические методы и модели активно используются в случае, если вероятность наступления конкретного вида операционного риска достаточно

[20] Волков А.А. Управление рисками в коммерческом банке. – М.: ОМЕГА-Л, 2013.С – 113
[21] Там же

велика, а его наступление носит на рынке массовый характер. В этом случае могут использоваться корреляционные модели, в которых функцией будет являться вероятность наступления операционного риска, а переменными – факторы, формирующие операционный риск (например, количество операций, прямо определяющее частоту ошибок персонала).

Безельный комитет выделил три различающихся по сложности подхода к расчета размера капитала на покрытие операционного риска:

1) Подход на основе базового индикатора (Basic Indicator Approach – BIA);

2) Стандартный подход (Standartized Approach – SIA);

3) Передовые подходы оценки операционного риска (Advanced Measurement Approach (AMA).

Сущность балльно-весового метода заключается в оценке операционного риска в сопоставлении с мерами по его минимизации. На основе экспертного анализа выбираются информативные для целей управления операционным риском показатели, и определяется их относительная значимость (весовые коэффициенты). Затем выбранные показатели сводятся в таблицы (оценочные карты) и оцениваются с использованием различных шкал. Полученные результаты обрабатываются с учетом весовых коэффициентов и сопоставляются в разрезе направлений деятельности кредитной организации, отдельных видов банковских операций и других сделок. Применение балльно-весового метода (метода оценочных карт) наряду с оценкой операционного риска позволяет выявить слабые и сильные стороны в управлении операционным риском.

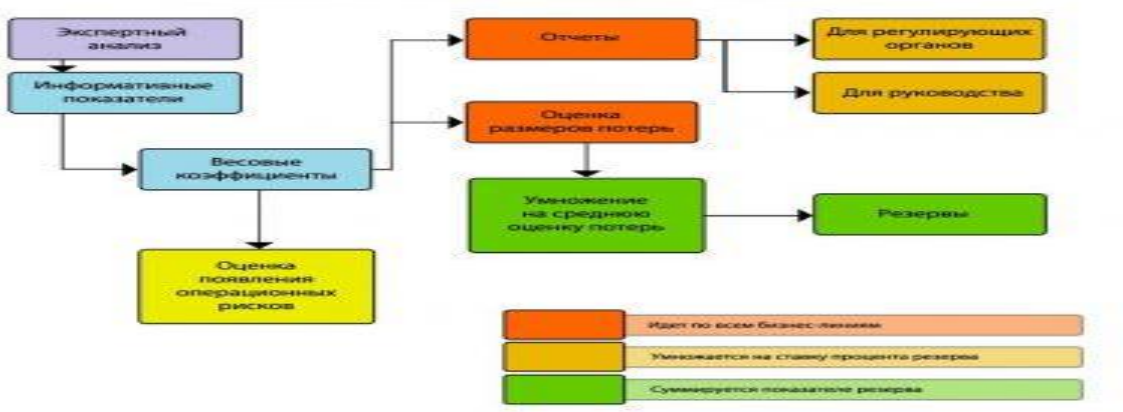

Рис.11 Балльно-весовой метод[22]

В рамках метода моделирования (сценарного анализа) на основе экспертного анализа для направлений деятельности кредитной организации, отдельных видов банковских операций и других сделок определяются возможные сценарии возникновения события или обстоятельств, приводящих к операционным убыткам, и разрабатывается модель распределения частоты возникновения и размеров убытков, которая затем используется для оценки операционного риска.

Существуют следующие типы сценариев:

- стандартный сценарий без кризисных ситуаций;
- сценарий «кризис в банке»: усиление оттока клиентских средств, закрытие ряда источников покупной ликвидности;
- сценарий «кризис рынка»: падение рыночных цен на финансовые инструменты, прекращение торгов, неликвидный рынок ценных бумаг, большой отток клиентских средств.

Рис. 12 Типы сценариев[23]

[22] Волков А.А. Управление рисками в коммерческом банке. – М.: ОМЕГА-Л, 2013.С – 211
[23] Там же

С помощью сценарного анализа выявляются факторы существенного риска, вокруг которых строится система КИРов, сигнализирующих о повышении вероятности реализации риска.

Другой целью построения системы операционных рисков является уменьшение резервных требований по операционному риску со стороны контролирующих органов, которое достигается прозрачным расчетом капитала под риском, согласно методологии анализа, принятой Базельским комитетом.

Тот факт, что операционный риск является наиболее важным компонентом, который отличает Базель 2 от его предшественника, значительно способствует развитию культуры понимания этого вида риска украинскими специалистами. Сегодня Базельский комитет по банковскому надзору уделяет первоочередное внимание проблеме операционных рисков. Но, несмотря на то, что выполнение положений документов этой организации для отечественных банков не является директивным и даже европейские банки предполагают полное внедрение Базеля 2 с 2008 года, рекомендации по управлению операционным риском становятся ключевым фактором, который повышает рейтинг надежности банка, вызывает доверие и интерес инвесторов.

По мнению экспертов, сегодня ситуация исторически сложилась так, что в зависимости от развития взглядов собственников на работу службы управления рисками, можно выделить три категории банков. Первая категория — банковские учреждения, которые в связи с выходом требований Национального банка о необходимости наличия службы управления рисками, привлекли к работе одного-двух человек для формального декларирования перед регулятором наличия такой службы. При этом у риск-менеджеров нет и не было никаких полномочий.

Вторая категория — это банки, которые внедрили службу риск-менеджмента после выхода требований ЦБ, однако при этом, понимая цели создания такого подразделения, не наделяют его необходимыми

полномочиями. И третья категория — банки, которые поняли необходимость системного подхода к управлению рисками, создали соответствующую службу и наделили ее четкими полномочиями вне зависимости от наличия постановлений ЦБ в сфере банковского надзора. Из работающих на рынке более полутора сот банковских учреждений могут похвастать принадлежностью к третьей группе лишь 10-15.

Ключевым фактором создания таких баз данных и важной задачей риск-менеджеров является разработка и согласование форматов данных, так как статистика должна быть пригодной для обработки и анализа. Необходимо создать внутренний реестр фактов реализации операционных рисков, в котором однозначно формализовать все поля.

Такими полями могут быть:

- категория операционного риска (в соответствии с классами потерь по Базелю);
- дата реализации риска;
- дата выявления реализации риска;
- подразделение главного офиса либо филиал, где выявлена реализация риска;
- ошибка либо нарушение;
- размер потери;
- возможная причина реализации риска;
- тип операции;
- источник информации;
- примечание.

При создании таких общедоступных баз данных роль банков сложно переоценить — они являются ключевыми институтами, от которых зависит разработка правил накопления и обмена информацией о фактах реализации операционных рисков. К примеру, в Великобритании вопросами улучшения процедур операционного риск-менеджмента вплотную занимаются два пула — Association of British Insurers, который выступает организатором

консорциума страховых организаций по операционному риск-менеджменту, и British Banker's Association, который постоянно актуализирует созданную в 2000 году Global Oprational Loss Database (Gold),— наиболее полную в Европе базу данных по потерям банков.

По мнению аналитиков, доступ к таким базам данных должен помочь ответить на следующие важные вопросы:

- Каковы ключевые события, приведшие к убыткам?
- Может ли риск, возникающий в системе, иметь место в моей организации?
- Какие операционные риски провоцируют наибольшие потери?
- Каким образом события, приведшие к убыткам, влияют на банковский бизнес?
- Какой банковский бизнес производят наибольшие риски?
- Каким образом риск репутации коррелирует с фактами потерь?

Интересно, что для использования информации из Gold не обязательно быть участником ассоциации BBA, база данных открыта для финансовых организаций из любой части мира. Финансовые учреждения ежеквартально передают информацию об операционных потерях в управление статистики BBA, где после проверки на точность и соответствие она обезличивается, а затем объединенный отчет становится доступным всем участникам сообщества Gold. Еще одна not-for-profit база данных была основана три года назад в Швейцарии и сейчас Operational Riskdata eXchange (ORX) насчитывает около 20 наибольших мировых банков среди своих подписчиков.

В актуальности таких баз данных для пользователей не приходится сомневаться, но есть один нюанс — многие эксперты по операционному риск-менеджменту солидарны в том, что интерес для банков представляют не столько факты потерь по системе других банков, а катастрофические ошибки, приведшие к дефолту. «Особого позитива от использования статистики по не катастрофическим событиям других банков нет, так как у

каждого кредитного учреждения свои требования к персоналу, свои бизнес-процессы, свое IT и видение профиля риска»,— говорит Евгений Матрос, независимый эксперт в области риск-менеджмента.— «Также, чтобы иметь такие общие базы данных, банкам необходимо накопить информацию и сделать ее доступной для использования, а это на данном этапе развития культуры операционного риск-менеджмента не представляется возможным».

Появление потребности в управлении операционными рисками можно отнести в большей мере к требованиям Базельского комитета и требованиям со стороны международных банков-кредиторов.

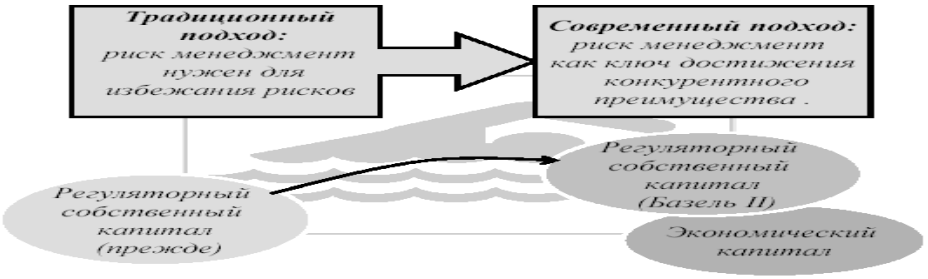

Рис. 13 БАЗЕЛЬ II[24]

По сравнению с Базель 1 в Базель 2 появились дополнения для расчета кредитного риска и новый показатель – операционный риск.

Расчет адекватности капитала (Базель II):

$$\text{Квота собственою капитала (мин.8\%)} = \frac{\text{Собственный капитал}}{\text{Кредитный риск} + \text{Рыночный риск} + \text{Операционный риск}}$$

В самом деле, как можно опираться на данные, если банки имеют небольшую современную историю. К тому же на заре своей деятельности никто не вел сбора информации по операционным рискам. Хватит ли данных для того, чтобы сказать, что они твердо дают закономерный характер поведения изучаемой величины? Для этого нужны полные данные за длительный период, а также данные других банков. Дадут ли банки

[24] www.bis.org

информацию о своих ошибках, например, о взломах своих информационных систем, воровстве клиентских денег нечистоплотными сотрудниками банка и т.д.? Трудно поверить что кто-то просто так желает «подмочить» свою репутацию за которую так упорно борется, но существуют некоторые межбанковские соглашения по сбору подобной информации.

Создание ведение базы данных операционных рисков рекомендуется по следующим полям:

Вид потерь, Место события, Время и частота событий, Объем потерь, Связь между различными причинами, местами и случаями

Наиболее простыми методами количественной оценки величины операционных рисков могут быть:

• Метод оценки на основе ожидаемых случаев потерь, приведенных к году(не как VaR).

• Метод отклонения стандартных результатов (как VaR).

Первый метод также очень прост в использовании. Вы составляете таблицу, в которой вы оцениваете операционные потери банка за период, например, неделю в размере 500 сум. За 20 лет, вы оцениваете, может произойти случай, когда банк потеряет 20 млн. сум. Ну а за период в 100 лет может произойти случай, когда банк потеряет 100 млн. сум. Затем, все это приводится к 1 году.

*500*56 недель = 28 тыс. сум.*
2 млн. / 20 лет = 100 тыс. сум.
100 млн./100 лет = 1 млн.
Всего получается 1 128 тыс. сум за один год.

Второй 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 упоминалось выше, 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 Value at Risk.

При этом следует отметить, что аналитические модели подходят только для расчетов нормально распределенных случайных величин. В ином случае, результаты вычислений будут некорректными по отношению к реальности.

Наиболее часто в банковской практике развитых стран используется симуляционный метод Монте Карло. С помощью его можно симулировать результаты различных видов распределений случайных величин. Однако и для него необходим знать лил предполагать параметры распределений вероятности.

Для операционных рисков, как правило, частотным распределением появления негативного случая выбирают распределение Пуассона, а распределением величины возможных потерь – логнормальное распределение. На их основе двухступенчатого метода Монте Карло получают распределение потерь, считая при этом что эти два распределения независимые. При симуляции из Пуассоновского распределения получают n значений негативных случаев. Далее уже из Логнормального распределения n раз выбирают потери. Процесс повторяют достаточное количество раз. Полученные в итоге значения упорядочивают по величинам в таблице. С требуемым уровнем доверия, как правило, в 99% из таблицы устанавливают уровень потерь.

Глава 3. Совершенствование методов управления операционным риском

Президент Узбекистана Ислам Каримов 6 мая подписал постановлению «О мерах по дальнейшему повышению финансовой устойчивости коммерческих банков и развитию их ресурсной базы», в котором предусматриваются меры по расширению системы безналичных расчетов. Принятое 6 мая 2015 года Постановление Президента Республики Узбекистан № ПП-2344 «О мерах по дальнейшему повышению финансовой устойчивости коммерческих банков и развитию их ресурсной базы» направлено на реализацию мер по укреплению своей ресурсной базы, широкому привлечению в банковский оборот свободных денежных средств населения и бизнеса.

Отмечено, что в 2015–2019 годах Центральным банком Республики Узбекистан будут поэтапно внедряться новые стандарты и рекомендации (стандарты Базель-III), разработанные Базельским комитетом по банковскому надзору, предусматривающие дальнейшее совершенствование нормативных требований, предъявляемых к коммерческим банкам, включая новые требования к достаточности капитала и ликвидности, оценки и управления рисками.

Особому отношению менеджмента крупнейших мировых банков к проблематике управления рисками персонала «поспособствовала» трагедия одного из старейших финансовых институтов Англии банка Barings. Тогда, в 1995 году, трейдер Ник Лисон (Nick Leeson) обанкротил Barings путем проведения огромных объемов незаконных операций с фьючерсами в Сингапуре. Размах работы Ника Лисона и по сей день ощутим, но уже совершенно в ином полюсе — он неизменный докладчик на различных конференциях и семинарах по операционному риск-менеджменту. К примеру, на будущей конференции в Гонг-Конге Ник Лисон презентует свой доклад о том, как контролировать амбиции персонала, если он является центром генерирования прибыли в компании и потенциально имеет все

возможности для мошеннических операций, а по его книге «Аферист» (Rogue Trader) в 1999 году был снят кинофильм. Да, экс-трейдер Barings оплатил свои ошибки дорогой ценой — он провел три года в тюрьме, от него ушла жена, и он серьезно заболел, но его настойчивость и упорство позволили заново отстроить жизнь в Ирландии, где он вылечился от рака, женился и даже состоял коммерческим директором футбольной команды Galway United. И когда через десять лет после того печального события, его просят назвать наиболее грозный риск для любой организации он неизменно отвечает — «люди». Самое трудное в компании, по его мнению, это заставить сотрудника попросить о помощи, так как все переживают за свою репутацию и компетентность. Многие думают, что смогут уладить свои промахи, но в результате оказываются вовлечены еще больше, а расплачивается за это в итоге банк.

С оглядкой на эту историю на первый план риск-менеджеры выводят самостоятельную оценку рисков подразделениями. Имеется ввиду внутренняя оценка и анализ работниками всех подразделений банка (департамента, управления, отдела или сектора, филиала или отделения) возможных операционных рисков, связанных с правильным построением бизнес-процессов, созданием эффективных процедур контроля, предотвращения технологических сбоев, несанкционированных действий персонала или негативного внешнего воздействия. Конечно, такая оценка работниками отдельного подразделения наверняка будет отчасти субъективна, но она должна основываться на внутренней заинтересованности подразделений и отдельных сотрудников в грамотном исполнении своих обязанностей. В конечном счете, основная деятельность осуществляется именно на уровне этих подразделений, и ее качество зависит от того, насколько правильно их персонал понимает свою работу и эффективно справляется с ней.

Меры по снижению операционных рисков:

- Многие (но не все) операционные риски отличает от прочих видов рисков, тот факт, что их источник лежит внутри самой организации и следовательно риск может быть снижен, за счет устранения причин его порождающих. Методы его снижения являются фактически методами внутреннего контроля и, как правило, для банка или иной финансовой организации подразумевают следующие меры:

- Разделение функций - проведение сделок, расчеты по ним и их учет должны производиться сотрудниками отдельных независимых подразделений. Отдельный сотрудник или подразделение не должен иметь возможность провести финансовую операцию от "начала до конца", не уведомив иных подразделений.

- Независимая оценка результатов деятельности - результаты деятельности сотрудника или подразделения должны оцениваться независимыми и не заинтересованными в искажении результатов подразделениями.

- Контроль рыночности цен - перед проведением сделок или перед проведением расчетов по ним, указанные в них цены должны подвергаться проверке на предмет адекватности рыночной конъюнктуры сот стороны независимого и незаинтересованного подразделения. Рыночные цены, используемые при проверке, должны быть получены из надежных внешних источников.

- Двойной ввод и подтверждение операций - параметры сделки должны подвергаться повторному контролю (подтверждению) со стороны независимого подразделения, а в случае автоматизированного учета и сопровождения операций их ключевые характеристики (суммы, валюты, даты расчетов и т.д.) должны вводиться повторно для выявления возможных ошибок.

- Контроль изменения условий операций - любое изменение условий уже заключенных сделок (в том числе перенос дат расчетов, пролонгации и т.д.) должно подвергаться пристальному контролю со стороны независимых

подразделений. В частности, внесение изменений в запись о сделке в автоматизированных системах учета и сопровождения операций должно быть невозможны в рамках прав сотрудников одного подразделения.

- Подтверждение сделки контрагентом - расчеты по сделке, заключенной с неким контрагентом должны производиться только по факту получения от него по надежным каналам связи подтверждения сделки с указанием её основных характеристик (суммы, активы, даты расчетов и т.д.).
- Контроль юридического оформления операций - все договора и прочие документы, подтверждающие проводимые операции должны быть одобрены юридической службой организации или соотвествовать типовым формам, утвержденным юридической службой, перед заключением сделки или проведением расчетов по ней должен проводиться соответствующий контроль договоров и иных документов. Юридическая служба должна быть независимым подразделением внутри организации.

Реализация одного из двух подходов к оценке рисков на основе самооценки (Self Assiessment Scorecard Approach), равно как и подход на основании накопленной статистики ошибок (Event-Loss-Data Approach) наталкивается на серьезные трудности. «Разрешить эти трудности практически невозможно без вовлечения топ-менеджмента. На практике, источниками информации об ошибках могут быть результаты проверок службой внутреннего аудита, целевые проверки главным офисом филиалов и информация от подразделений, которые сталкиваются с реализацией оперрисков»,— говорит Евгений Матрос.— «Если с получением информации от аудита вопросы более-менее решаются, то инициатива получения информации об ошибках от персонала банка практически изначально не реальна. Для банка важно показать, что цель накопления такой статистики — не наказание допустившего ошибку, а создание условий, при которых будет минимизирована вероятность допущения такой ошибки».

Наша банковская система конечно не исключение, но реализация человеческого фактора у нас приобретает менее замысловатые формы, чем случаи с Barings или похожие моменты в работе Sumitimo, Refco и Allied Irish Bank, риски персонала свойственны в главной мере карточному бизнесу. Иногда при загрузке банкомата наличными оператор ошибочно помещал в лоток с купюрами низкого номинала банкноты более высокого достоинства, еще более известными являются случаи с мошенничеством по счетам клиентов. Исходя из высокой частоты реализации этого вида оперрис-ков, отечественные риск-менеджеры в один голос называют внутренние риски, связанные с персоналом, одними из существенных в работе украинских банков, при этом замечая, что одинаково весомыми являются все виды рисков, будь это риски персонала, процедур или ИТ, так как они очень взаимозависимы. К примеру, автоматизируя ручные процессы можно повысить риск информационных систем. Поэтому, по словам Дмитрия Ганзи, управление операционными рисками, связанными с персоналом, в банке должно происходить с выполнением таких условий:

- четкое определение функциональных обязанностей каждого сотрудника банка; формирование общей корпоративной культуры;
- выделение каждому сотруднику доступов к информационным системам в зависимости от его функциональных обязанностей;
- выделения бюджета на посещение сотрудниками банка профилирующих семинаров, тренингов, конференций с целью повышения профессиональной квалификации и ознакомления с новыми банковскими технологиями и тенденциями;
- обязательное наличие технологических карт на проведение банковских операций;
- распределение полномочий на принятие максимальных объемов рисков между: коллегиальными органами банка, руководителями подразделений фронт-офиса, а также руководителями филиалов и отделений;

- наличие системы мотивации сотрудников в постоянном повышении профессиональной квалификации, проявлении разумной инициативы и неукоснительном выполнении собственных функциональных обязанностей.

При этом специалисты в большей мере акцентируют внимание на том, что для персонала, который сопровождает текущие операции, важна четкая и однозначная формализация всех бизнес-процессов. Сотрудник должен до автоматизма довести последовательность действий, избегая собственных интерпретаций. Выполнение такого бизнес-процесса не должно быть усложнено, так как при выполнении сложных процессов всегда больше ошибок, чем при выполнении простых. Важно и психологическое состояние персонала, его нацеленность на качественное выполнение процедуры.

О деятельности банка и существовании операционных рисков можно судить по трем основным индикаторам:

- Индикаторы текущей деятельности (key performance indicators) отражают наиболее значимые аспекты деятельности компании, по которым можно судить о ее текущем состоянии. Основное назначение таких индикаторов состоит в том, что они позволяют контролировать эффективность осуществляемых операций. Такими показателями могут служить: количество неправильных операций, рекламации от клиентов, текучесть кадров, суммарное время неработоспособности информационных систем и т. д.;
- Индикаторы эффективности контроля (key control indicators) показывают количество ошибок, которые были предотвращены благодаря системе внутреннего контроля. Такими индикаторами могут служить, например, количество исправленных операций, количество неподтвержденных сделок, расхождения при сверке данных, выявленные случаи несанкционированного доступа к данным и др.;
- Индикаторыриска (key risk indicators) являются опережающими показателями и строятся расчетным или аналитическим путем

сопоставления индикаторов текущей деятельности и эффективности контроля. Например, сопоставив информацию об одновременном увеличении объема операций, текучести кадров и количестве ошибок ввода данных, можно оценить уровень операционного риска для компании. Тем самым, можно создавать количественные модели для анализа и прогнозирования ситуации в области операционных рисков.

Все перечисленные индикаторы часто используются в целях контроля операционной деятельности. Это основано на допущении, что при появлении негативных сигналов от таких индикаторов возрастает вероятность событий, которые связаны с операционным риском. Соответственно, риск-менеджер может предотвратить такую опасность, усилив контроль над ситуацией. В настоящее время все основные операции в финансовых учреждениях — от заключения сделок до их отражения в бухгалтерском учете — в основном обрабатываются в компьютерных информационных системах. Такие системы являются важным предметом исследования операционного риск-менеджмента, ставящего своей целью контроль потоков информации.

Хранение информации в централизованной базе данных позволяет отслеживать всю деятельность компании и эффективно управлять рисками в целом по компании, имея возможность анализировать каждую операцию или сделку в отдельности. Именно централизованная база данных и является основным источником информации об операционных рисках.

Однако централизация информации еще не означает, что существует единое программное обеспечение, которое полностью автоматизирует обработку всех операций, осуществляемых в банке. «Поскольку различные системы могут использоваться для получения информации из внешних источников, обработки операций, подготовки аналитических отчетов и составления прогнозов, возникает проблема интеграции разнородных информационных ресурсов»,— говорит Дмитрий Ганзя,— «Полностью универсальные системы для учета всех продуктов, операций, всех стадий их обработки вряд ли существуют. В итоге, единая информационная сеть будет

представлять собой несколько взаимосвязанных многофункциональных приложений, работающих в режиме реального времени с централизованной базой данных. Поиск оптимального баланса между постоянством информационной системы и ее функциональностью, представляет собой сложную задачу, решение которой требует сочетания информационных технологий и методик управления финансовыми рисками».

Заключение

В течение последних десятилетий в мире отмечается интенсивное развитие процессов глобализации экономики, которые охватывают все большее число стран и влияют на многие сферы человеческой деятельности. Одной из таких сфер, где эти процессы проявились особенно сильно, являются банковские операции, обслуживающие реальное движение товаров, услуг и факторов производства.

На основе анализа организации, осуществления и совершенствования управления операционными рисками, проведенного в работе, автор считает целесообразным сделать следующие предложения.

1. Необходима разработка конкретных подходов к выбору стратегии защиты от рисков, имеющих место в практике, в частности в отношении принятия специальных мер по оценке рисков и выбора методов их уменьшения.

2. Внедрение в практику коммерческих банков модулей по управлению рисками.

3. Использовать зарубежный опыт по управлению операционным риском, где учитывается более глубокая специализация риск менеджера по видам банковских операций и их согласованность действий в рамках стратегии управления рисками коммерческого банка.

4. Дальнейшее совершенствование национально-правового регулирования в области рисков.

5. Учитывая, что от развития банковско-финансовой системы во многом зависит использование передовых и наиболее эффективных форм по управлению и страхованию рисков, целесообразным является дальнейшее укрепление капитальной базы коммерческих банков.

6. Необходимо уделить серьезное внимание повышению уровня квалификации банковских специалистов в области выявления, управления и минимизации рисков, а также росту экономической образованности клиентуры банков.

В качестве методов ограничения операционного риска можно предложить:

● Разделение функций по проведению сделок, которые должны производиться сотрудниками отдельных независимых подразделений, в целях персональной ответственности за каждую операцию и исключения возможности провести финансовую операцию от начала до конца, не уведомив иные подразделения;

● Создание контрольной среды, то есть наличие встроенной системы контроля в ежедневные операции в целях повторного контроля операций со стороны независимого контролера путем подтверждения или двойного ввода информации;

● Введение мер операционной, технической и физической безопасности (например, путем ограничения физического и логического доступа к информации с помощью шифрования, паролей и т.д.);

● Обеспечение хранения, обработки и передачи данных, наличие дублирующих мощностей в телекоммуникационных и вычислительных сетях, обеспечение целостности данных и программного обеспечения;

● Разработка планов и сценариев действий в чрезвычайных ситуациях и наличие возможности оперативного восстановления бизнеса в целях обеспечения непрерывности финансово-хозяйственной деятельности при совершении банковских операций и сделок;

● Определение приемлемого уровня операционных рисков, присущих деятельности банка на финансовых рынках, и установление лимитов.

● Для большинства операций достаточным лимитом будет служить объемный лимит, ограничивающий оборот в рамках той или иной деятельности или объемы вложений в определенные активы / пассивы. Целесообразным может быть лимитирование величин отдельных операций, проводимых под операционным риском;

● Юридический контроль оформления операций (договоры и прочие документы);

● Подтверждение сделки контрагентом, т.е. проведение расчетов только по факту получения от контрагента подтверждения сделки по надежным каналам связи;

● Наблюдение за операционными рисками с целью принятия мер по поддержанию рисков на приемлемом уровне;

● Контроль правильности, адекватности и полноты применения утвержденных процедур контроля и управления определенным уровнем рисков, а также независимая оценка результатов деятельности;

● Передача операционного риска третьим лицам путем страхования и аутсорсинга (привлечение специализированной сторонней организации для выполнения отдельных видов работ/услуг) или отказ от осуществления определенных видов сделок.

Список литературы

1. Закон Республики Узбекистан «О Центральном банке Республики Узбекистан» от 21 декабря 2005г. //Сборник законодательных актов по реформированию и либерализации банковской системы. Ташкент, 2000. С.7-30.
2. Закон Республики Узбекистан «О банках и банковской деятельности» от 25 апреля 2006 г.//Сборник законодательных актов по реформированию и либерализации банковской системы. Ташкент, 2000. С.30-48.
3. Постановление Президента Республики Узбекистан № ПП-23446 мая 2015 года «О мерах по дальнейшему повышению финансовой устойчивости коммерческих банков и развитию их ресурсной базы»
4. Указ Президента Республики Узбекистан от 27 июня 2002 г. № УП-3099 «О дополнительных мерах по упорядочению обращения в Республике Узбекистан наличной иностранной валюты”
5. Указ Президента Республики Узбекистан от 30 марта 2002 г. № УП-3047 «О мерах по ограничению роста денежной массы и повышению ответственности за соблюдение финансовой дисциплины”
6. Указ Президента Республики Узбекистан от 20 марта 1998 года № УП-1979 «О мерах по упорядочению ввоза и вывоза наличной иностранной валюты физическими лицами”
7. Указ Президента Республики Узбекистан от 31 мая 1996 г., № УП-1467 «О дополнительных мерах по стимулированию создания и деятельности предприятий с иностранными инвестициями”
8. Постановление Президента Республики Узбекистан от 26 марта 2012 г. № ПП-1731 «О дополнительных мерах по усилению стимулирования предприятий-экспортеров и расширению экспортных поставок конкурентоспособной продукции»
9. Постановление Президента Республики Узбекистан от 9 марта 2012 г. № ПП-1725 «О мерах по дальнейшему совершенствованию деятельности фонда реконструкции и развития Республики Узбекистан»
10. Постановление Президента Республики Узбекистан от 26 ноября 2010 г. № ПП-1438 «О приоритетных направлениях дальнейшего реформирования и повышения устойчивости финансово-банковской системы республики в 2011-2015 годах и достижения высоких международных рейтинговых показателей”
11. Постановление Президента Республики Узбекистан от 6 апреля 2010 г. № ПП-1317 «О мерах по дальнейшему повышению финансовой устойчивости и усилению инвестиционной активности банковской системы”
12. Постановление Президента Республики Узбекистан от 27 марта 2008 г. №ПП-822 «О дополнительных мерах по мобилизации и обеспечению потребности в наличных денежных средствах “

13. О мерах по Дальнейшему Расширению Деятельности И Укреплению Ресурсной Базы Фонда Реконструкции И Развития Республики Узбекистан: Постановление Президента Республики Узбекистан от 5 Марта 2008 Г., № ПП-811
14. О мерах по дальнейшему развитию банковской системы и вовлечению свободных денежных средств в банковский оборот: Постановление Президента Республики Узбекистан от 7 ноября 2007 г. №ПП-726
15. О мерах по дальнейшему повышению капитализации банков и активизации их участия в инвестиционных процессах по модернизации экономики: Постановление Президента Республики Узбекистан от 12 июля 2007 г. № ПП-670
16. О внесении изменений в Постановление Кабинета Министров от 15 января 1999 г. № 24 «О мерах по дальнейшему реформированию банковской системы» (Постановление Президента Республики Узбекистан от 8 октября 2008 г. № пп-975 «О мерах по дальнейшему повышению инвестиционной активности акционерно-коммерческих банков «Пахта-банк» и «Галла-банк») 20 ноября 2008 г., № 253
17. Каримов И.А. Наша главная цель – решительно следовать по пути широкомасштабных реформ и модернизации страны. – Ташкент: Узбекистон, 2013. – 64 с.
18. Ислам Каримов. Мировой финансово-экономический кризис, пути и меры по его преодолению в Условиях Узбекистана. – Ташкент: Узбекистан, 2009. – 48 с.
19. Абдуллаева Ш.З. Банк рисклари ва кредитлаш. Т.: Молия, 2002. – 304 с.
20. Абдуллаева Ш.З., Арзуманян С.Ю., Муругова И.А. Либерализация банковской системы республики в условиях углубления экономических реформ: Учеб. Пособие. – Т.: ТФИ, 2003. – 221 с.
21. Абдуназарова Г. Код доступа – Кредитная история // Налоговые и таможенные вести, 2009. – №51. – с.61-65.
22. Анализ кредитоспособности организации и группы компаний: учебное пособие / Д. А. Ендовицкий, К. В. Бахтин, Д. В. Ковтун; под ред. Д. А. Ендовицкого. — М.: КНОРУС, 2012. — 376 с.
23. Ангелиди М.С., Насиров Э.И., Жаббаров А.Т. Управление рисками инвестиций (вопросы и ответы). – Т.: ТФИ, 2007. – 68 с.
24. Арзуманян С.Ю. Банковские риски: учебное пособие. – Т.: Молия,
25. Балдин К.В., Воробьев С.Н. Риск-менеджмент: учебное пособие. – М.: Гардарики, 2005. — 285 с.
26. Банк и банковские операции: учебник / коллектив авторов; под ред. О.И. Лаврушина. — М.: КНОРУС, 2012. — 272 с.
27. Банки и банковское дело / Под ред. Балабанова И.Т. – СПб.: Питер, 2003. – 256 с.: ил. – (Серия «Краткий курс»)
28. Банковские операции / Ю. И. Коробов. — Москва: Магистр, 2007. — 446 с.

29. Банковские риски: учебник / коллектив авторов; под ред. О.И. Лаврушина, Н.И. Валенцевой. — 3-е изд., перераб. и доп. — М.: КНОРУС, 2013. — 296 с.
30. Банковский менеджмент. Учебник / Под ред. О.И. Лаврушина. 2-е изд. перераб. и доп. – М.: КНОРУС, 2009. – 560 с.
31. Банковский менеджмент: Учебное пособие / Под общей ред. Иода Е.В. Тамбов: Изд-во Тамбов. гос. техн. ун-та 2001, 192 с.
32. Банковское дело. Управление и технологии: учебник / под ред. Тавасиева А.М.. – 2-е изд., перераб. и доп. – М.: Юнити-Дана, 2005. — 671 с.
33. Банковское дело: кредитная деятельность коммерческих банков: учебное пособие / под ред. Л.П. Кроливецкой, Е.В. Тихомировой. – М.: КНОРУС, 2009. – 280 с.
34. Банковское дело: розничный бизнес: учебное пособие / под ред. Белоглазовой Г.Н. – М.: КНОРУС, 2013. – 416 с.
35. Банковское дело: современная система кредитования: учебное пособие / О.И.Лаврушин, О.Н. Афанасьева, С.Л. Корниенко; под ред. засл. деят. наук РФ, д-ра экон. наук, проф. О.И.Лаврушина. – 3-е изд., доп. – М.: КНОРУС, 2007. – 264 с.
36. Банковское дело: управление в современном банке: учебное пособие / Р.Г. Ольхова. — 2-е изд., перераб. и доп. — М.: КноРус, 2013. — 304 с.
37. Батракова Л.Г. Экономический анализ деятельности коммерческого банка. Изд. 2-е, перераб. и доп.: Учебник для вузов. – М.: Логос, 2011. – 368 с.
38. Беляков А.В. Банковские риски: проблемы учета, управления и регулирования (2-е изд): управленческая методическая разработка. – М.: БДЦ-пресс, 2004. – 256 с.
39. Бор М. З., Пятенко В. В. Менеджмент банков: организация, стратегия, планирование. – М.: Финансы, ЮНИТИ, 2003. – 471с.
40. Бригхэм Ю., Эрхардт М. Финансовый менеджмент. – 10-е изд. – СПб.: Питер, 2009. — 960 с.
41. Букирь М.Я. Кредитная работа в банке: методология и учет. — М.: КНОРУС, ЦИПСиР, 2012. — 240 с.
42. Бычков В. Резервы как элемент управления рисками банка // Проблемы теории и практики управления, 2006. – №12. – с. 36-42.
43. Вахабов А.В. Особенности управления рисками инвестиционных проектов в коммерческих банках. – Т.: IQTISOD-MOLIYA, 2009 г. – 152 с.
44. Волков А.А. Управление рисками в коммерческом банке. – М.: ОМЕГА-Л, 2013. – 156 с.
45. Джумакулов Т.Т., Сафарова З.Г. Использование трудов И.Каримова в преподавании экономической теории и его вклад в ее развитие: Учебное пособие. – Т.: Изд-во мед. лит-ры им. Абу Али ибн Сино, 2002. – 232 с.
46. Димитриади Г.Г. Риски управления банком. – ЛКИ, 2010. – 240 с.
47. Жарковская Е.П. Банковское дело: Учебно-методическое пособие. – М.: Издательство МФЮА, 2001. – 102 с.

48. Жуков Е.Ф. Банковский менеджмент: учебник. – 2-е изд., перераб. и доп. – М.: Юнити-Дана, 2008. – 258 с.
49. Костюченко Н.С. Анализ кредитных рисков. Часть 2. Проблемная задолженность. М.: Скифия, 2012. – 376 с.
50. Кредитная экспансия и управление кредитом: учебное пособие / коллектив авторов; под ред. О.И. Лаврушина. — М.: КНОРУС, 2013. — 264 с.
51. Кузнецова В.В., Ларина О.И.. Банковское дело. Практикум. М.: КноРус, 2007. — 264 с.
52. Норкобилов С., Дадабоева Х., Жураев У. Халкаро амалиётда банк назорати. Магистрлар учун дарслик. – Т.: “IQTISOD–MOLIYA”, 2007. – 180 с.
53. Норкобилов С.Х., Файзуллаева М.М. Надзор и анализ банков: учебное пособие. – Т.: «IQTISOD-MOLIYA», 2007. – 160 с.
54. Ольхова Р. Г. Банковское дело: управление в современном банке. — Москва: КноРус, 2008. — 288 с.
55. Севрук В.Т. Банковские риски. – М.: Дело ЛТД, 2007. – 238 с.
56. Турбанов А.В. Банковское дело: операции, технологии, управление. – М.: Альпина Паблишер, 2010. – 681 с.
57. Управление рисками в банковской деятельности: учебное пособие / Т.И. Леонович, В.М. Петрушина. – М.: Дикта, 2012. – 136 с.
58. Финансовое управление в коммерческом банке: учебное пособие / М.А. Поморина. — М.: КНОРУС, 2013. — 376 с.
59. Чернова Г.В., Кудрявцев А.А. Управление рисками. М.: Проспект, 2003. – 160 с.
60. Шевчук Д.А. Банковские операции: учебное пособие. – Ростов н/Д: Феникс, 2006. — 224 с.

Интернет-ресурсы

www.cbu.uz
www.bankir.uz
www.cps.uz
www.nbu.com
www.bis.org