

**Катилова Наталия Валерьевна  
Сорин Энгел**

**РИСКИ И ТЕХНОЛОГИИ**

## **ПРАКТИКА КЛЮЧЕВЫХ ИНДИКАТОРОВ ДЛЯ ОПЕРАЦИОННЫХ РИСКОВ**

**КЛЮЧЕВЫЕ СЛОВА:** операционный риск,  
индикатор риска, «Базель II»

На основе практического опыта авторы статьи рассматривают около 100 ключевых индикаторов операционного риска, предлагая в зависимости от направлений деятельности банка конкретный план действий, включающий систему пороговых значений, оценку степени риска и тестирование для выбора оптимального индикатора (качественную и количественную оценки), с целью их эффективного использования в ежедневной работе с учетом требований «Базеля II».

**К**

лючевые индикаторы риска (КИРы) играют значительную роль в процессе управления любыми рисками. Индикаторы используются для отслеживания и прогнозирования различных операционных событий (рис. 1). Они дополняют процесс оценки постоянным мониторингом эффективности контроля. В этом отношении они существенно отличаются от индикаторов деятельности (Key Performance Indicators), которые являются более общими и сфокусированы скорее на прошлом, чем на будущем.

В управлении операционными рисками КИРы являются основными инструментами, с помощью которых можно осуществлять широкий спектр измерений. В отличие от аудиторских проверок и контрольных мероприятий, которые проводятся периодически, КИРы могут измеряться так часто, как это требуется (ежедневно, ежемесячно и т. д.).



**Катилова Н. В.** — ведущий консультант по управлению рисками SAS Institute GmbH, Ph.D. (University of Antwerpen, Belgium). Член AMS, EMS, Бельгийского Королевского математического сообщества. Автор публикаций в США, Франции, Германии, Новой Зеландии (г. Москва)

**Сорин Э.** — глава направления операционных рисков SAS International (Германия). Член PRIMIA, ACCA Financial Services Section (UK GAAP / IAS), International Fiscal Association. Автор публикаций в США, Бенилюксе, Великобритании, Румынии и Ирландии (г. Брюссель, Бельгия)

РИС. 1. ПРИМЕР ПРИМЕНЕНИЯ КЛЮЧЕВОГО ИНДИКАТОРА РИСКА



\* Одному клиенту могут звонить несколько раз

Использование индикаторов является составной частью процесса риск-менеджмента и ограничивается лишь назначенными критериями или пороговыми уровнями (Trigger Levels).

Как показало исследование, проведенное компанией Ernst & Young, банковские учреждения по всему миру активно применяют КИРы. Так, две трети опрошенных банков подтвердили, что операционный риск имеет приоритетный статус в их организации, а 50% респондентов указали также, что применяют самостоятельную практику оценки и контроля рисков (в том числе КИРы, сбор данных о потерях и сценарный анализ). И наконец, 75% мировых банков используют в процессе работы, связанной с управлением операционными рисками, высокие технологии. Важность КИРов в практической деятельности банков иллюстрирует рис. 2, приведенный в том же исследовании.

Не существует единственного и уникального индикатора, помогающего оценить одновременно все виды рисков, все регионы и все направления деятельности финансового учреждения. Зачастую индикаторы специфичны

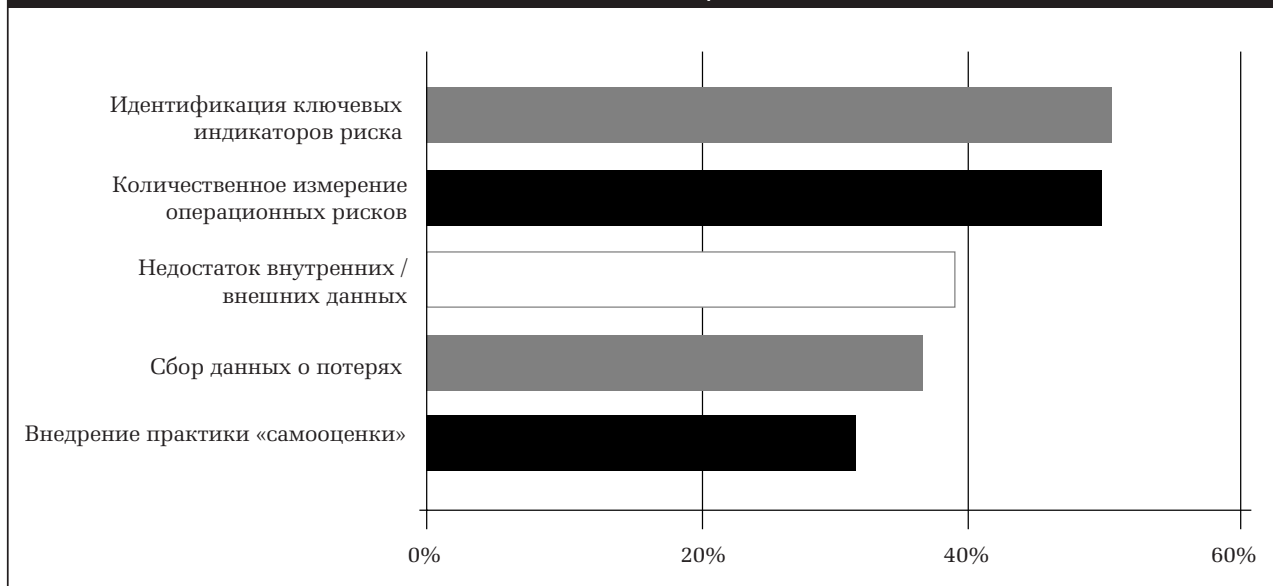
для видов деятельности или процессов. Для некоторых категорий риска подобрать подходящий индикатор гораздо легче, чем для других.

В любом случае основной целью КИРов является прогнозирование неблагоприятного события и предотвращение возможных потерь при его реализации. Но в этом же заключается и трудность — сложно понять, какие индикаторы можно считать предикативными и какие типы потерь они способны предсказать.

Кроме того, КИРы должны быть достаточно «чувствительными», чтобы отражать текущий «профиль» потерь, а также тип риска, свойственного данному бизнес-процессу.

Среди пользователей риск-индикаторов мы выделяем две основные группы: так называемые бизнес-пользователи, которые получают информацию о КИРах вместе с остальной отчетностью и используют ее в своей дальнейшей работе (пример консолидированного отчета показан на рис. 3), и аналитики, которые подбирают адекватные индикаторы соответствующего профиля и корректируют их по мере необходимости, изменяя пороговые значения и даже иногда удаляя

РИС. 2. ПЯТЕРКА НАИБОЛЕЕ ОСТРЫХ ПРОБЛЕМ В ОБЛАСТИ УПРАВЛЕНИЯ ОПЕРАЦИОННЫМИ РИСКАМИ



«устаревшие» индикаторы из набора практических инструментов.

Индикаторы по своей природе бывают опережающими (предикативными) и историческими (по факту). На практике индикаторы операционных рисков непосредственно связаны с потерями, которые по определению считаются реализованными. Поэтому средние значения исторических потерь служат, как правило, базой для оценки уровня ожидаемых потерь в будущем.

Существуют также индикаторы, ориентированные не на потери, а на бизнес-процессы. Например, часто меняющийся персонал банка трудно соотнести с какой-либо конкретной потерей, поскольку здесь мы имеем дело с процессом. Подобные индикаторы помогают оценить качество операций для всех видов риска. Они, как правило, тоже исторические, поскольку информируют нас о том, что уже произошло, но не указывают конкретно, на чем стоит сфокусировать свои усилия в будущем. В принципе, можно попытаться путем определенных трансформаций перевести их в разряд предикативных — например, зная число не совершенных из-за поломки в системе расчетных операций или неосуществленных

(«открытых») подтверждений мы можем трансформировать информацию, фокусируя внимание лишь на операциях, не осуществленных после определенного временного интервала (например, 24 часа), извлекая, таким образом, пользу не из потерь, которые еще не произошли, а из самого процесса непосредственно (рис. 4). Именно такие измерения, как число нереализованных событий, выходящее за определенные временные рамки, а также процент ошибок и надежность системы, могут послужить ориентирами в работе с бизнес-процессами.

Предикативными являются индикаторы окружения, такие как, например, число жалоб со стороны клиентов, удовлетворенность персонала своей работой, количество проведенных тренингов для сотрудников подразделения. Руководство финансовой организации должно использовать опережающие индикаторы с целью воздействия на профиль риска. Они строятся путем расчета для сопоставления с остальными индикаторами. Например, сопоставив информацию об одновременном увеличении объема операций, «текучки» кадров и количества ошибок ввода данных, можно оценить уровень операционного риска компании.



Примечание: слева сверху: гистограмма «10 основных рисков» отражает распределение «чистых» рисков (Residual Risk) по профилю рисков (горизонтальная ось);

слева внизу: график «Частота и размер операционных потерь за последние 12 месяцев» отражает размер потерь (вертикальная ось слева), частоту потерь (вертикальная ось справа) и месяцы, когда потери произошли (горизонтальная ось);

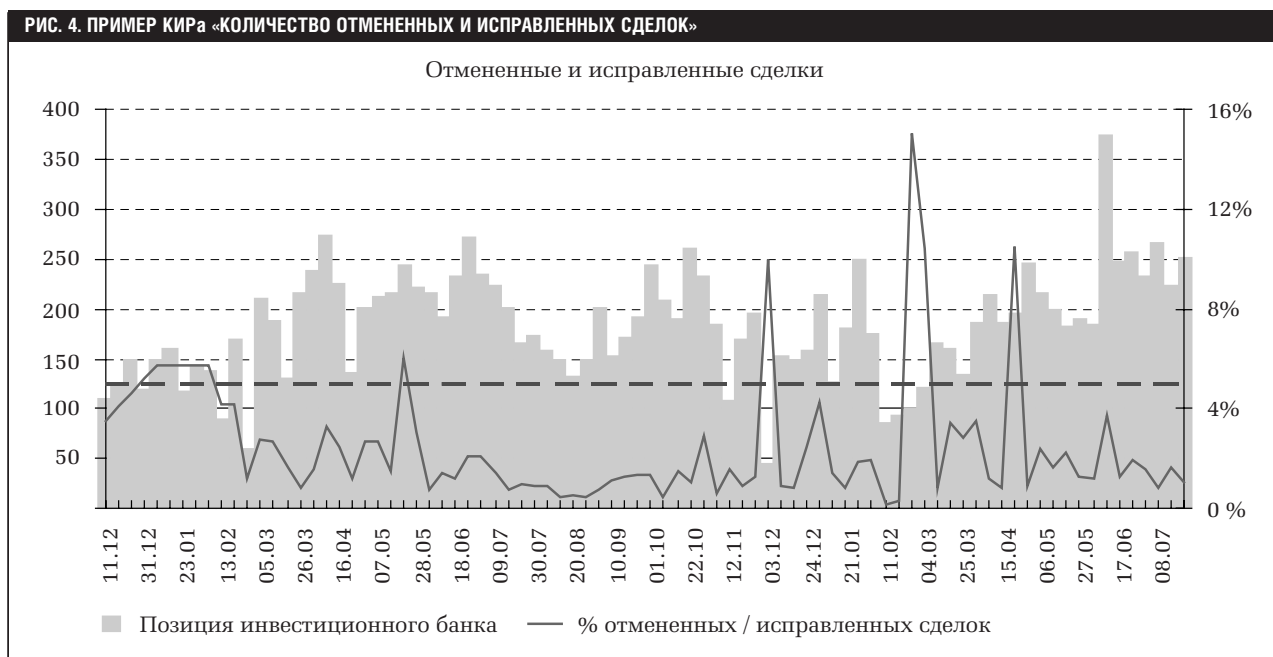
справа расположена таблица «Операционные КИРы» с указанием их динамики (текущее значение КИРа и его предыдущее значение).

Так можно создавать количественные модели для анализа и прогнозирования ситуации.

На практике эффективное использование индикаторов предусматривает одновременное использование как исторических, так и опережающих индикаторов. Чем более они специфичны и чем точнее отражают профиль соответствующего риска, тем более стабильна работа вашей системы. Так называемая «чувствительность» индикатора отражает эффективность его работы, а вот измерить

ее непросто, поэтому на практике оптимальные пороговые значения для индикаторов риска вначале определяются количественно, а затем корректируются в процессе моделирования.

Окончательное использование тех или иных КИРов в вашей организации подтверждается практикой. На рис. 5 изображена динамика развития успешного применения КИРов одной из крупнейших банковских корпораций за последние два года. Так, если в



2004 г. процент неэффективных КИРов составил в банке 1/4 от общего числа применяемых индикаторов риска, то в 2005 г. компания вышла на уровень 14%.

Правильно подобранные КИРы — это те, которые сопровождают риск на протяжении

долгого времени и не исчезают при повышении или понижении его уровня. Кроме того, успешное использование индикаторов риска требует четко структурированного подхода. Поэтому на основании мирового опыта, накопленного компанией SAS Institute при осуществлении различных проектов в области управления операционными рисками, для эффективного применения КИРов предлагается следующий план действий.

1. Составьте карту рисков вашего банковского учреждения: определите стандартные виды рисков, присущие вашей организации, и соотнесите их с направлениями деятельности в соответствии с внутренней структурой банка. В табл. 1 приведен возможный пример карты рисков на основе стандартной классификации рисков и стандартных направлений деятельности по «Базелю II».

Семь видов риска и восемь направлений деятельности определяют 56 возможных стандартных комбинаций (первый уровень «Базеля II»). Существует возможность перейти на более детальный (второй уровень «Базеля II»), но в этом случае число возможных комбинаций значительно возрастет.

ТАБЛИЦА 1. КАРТА РИСКОВ (РЕШЕНИЕ SAS OPRISK MANAGEMENT)										
		INTERNAL FRAUD	EXTERNAL FRAUD	EMPLOYMENT PRACTICES & BUSINESS PRACTICES	CLIENTS, PRODUCTS & BUSINESS PRACTICES	DAMAGE TO PHYSICAL ASSETS	EXECUTION, DELIVERY & PROCESS MANAGEMENT	BUSINESS DISRUPTION AND SYSTEM FAILURES	TOTAL	
Corporate Finance	Number	362	123	25	36	33	150	2	731	
	Mean	35,459	52,056	3,456	56,890	56,734	1,246	89,678	44,215	
	Standard Derivation	5,694	8,975	3,845	7,890	3,456	245	23,543	6,976	
Trading & Sales	Number	50	4	35	50	46	210	3	398	
	Mean	53,189	78,084	5,184	85,335	85,101	1,869	134,517	66,322	
	Standard Derivation	8,541	13,463	5,768	11,835	5,184	368	35,315	10,464	
Retail Banking	Number	45	4	32	45	42	189	3	360	
	Mean	47,870	70,276	4,666	76,802	76,591	1,682	121,065	59,690	
	Standard Derivation	7,687	12,116	5,191	10,652	4,666	331	31,783	9,417	
Commercial Banking	Number	41	3	28	41	37	170	2	322	
	Mean	43,083	63,248	4,199	69,121	68,932	1,514	108,959	53,721	
	Standard Derivation	6,918	10,905	4,672	9,586	4,199	298	28,605	8,476	
Payment & Settlement	Number	37	3	26	37	34	153	2	292	
	Mean	38,774	56,923	3,779	62,209	62,039	1,363	98,063	48,349	
	Standard Derivation	6,226	9,814	4,205	8,628	3,779	268	25,744	7,628	
Agency Services	Number	44	4	31	44	40	184	2	349	
	Mean	46,529	68,308	4,535	74,651	74,446	1,635	117,675	58,018	
	Standard Derivation	7,472	11,777	5,045	10,353	4,535	321	30,893	9,154	
Asset Management	Number	40	3	28	40	36	165	2	314	
	Mean	41,876	61,477	4,081	67,186	67,002	1,472	105,908	52,217	
	Standard Derivation	6,725	10,599	4,541	9,318	4,081	289	27,804	8,238	
Retail Brokerage	Number	48	4	33	48	44	198	3	378	
	Mean	50,252	73,773	4,898	80,623	80,402	1,766	127,090	62,660	
	Standard Derivation	8,069	12,719	5,449	11,182	4,898	347	33,365	9,886	
Insurance	Number	43	4	30	43	39	179	2	340	
	Mean	45,226	66,395	4,408	72,561	72,362	1,589	114,381	56,394	
	Standard Derivation	7,262	11,447	4,904	10,063	4,408	312	30,028	8,897	
Total	Number	710	152	268	384	351	1,598	21	3,484	
	Mean	45,653	67,021	4,450	73,245	73,044	1,604	115,459	56,926	
	Standard Derivation	7,331	11,555	4,950	10,158	4,450	315	30,311	8,981	

Примечание: строки: стандартная классификация направлений деятельности («Базель I»); столбцы: стандартная классификация по потерям («Базель II»);

внутри клетки: число потерь, средний размер потери и стандартное отклонение.

Аналогичную карту рисков можно составить также и по бизнес-процессам вашей организации, а также по регионам и другим измерениям (например, по дочерним компаниям крупной банковской структуры).

2. Распределите полученные результаты по приоритетности. Для того чтобы не усложнять анализ, присвойте клеткам одну из трех следующих категорий: «Низкая степень риска» (обычно отмечается зеленым цветом), «Средняя степень риска» (обычно отмечается желтым цветом) и «Высокая степень риска» (отмечается красным цветом). Подобная цветовая сигнализация получила название «Базельский светофор». У вас получится карта, изображенная на рис. 6. Некоторые средства программного обеспечения осуществляют подобную оценку автоматически (при этом следует предварительно задать пороговые значения для каждого уровня риска).

3. Теперь, когда основные проблемные области операционных рисков вашего учреждения выявлены, вам необходимо назначить ключевые индикаторы рисков для «красных» клеток. Главная задача на этом этапе — подобрать правильный КИР и протестировать его. В списке возможных индикаторов риска постарайтесь определить наиболее подходящие для каждой из «клеток высокого риска».

Ниже приведен список возможных ключевых индикаторов риска (КИРов), который разбит на следующие основные категории.

«**IT-системы**»: проводится идентификация КИРов по видам оборудования и причинам сбоев, а также по видам программных систем и технологий и причинам их сбоев (рис. 7). Например:

- процент неосуществленных операций в течение недели;

**РИС. 6. ОЦЕНКА СТЕПЕНИ РИСКА С ПОМОЩЬЮ РЕШЕНИЯ SAS OPRISK MANAGEMENT**

EventRiskCategories, EventRiskSubCategories, Risk	Asset Management	Retail Brokerage	Corporate Finance	Trading and Sales	Agency Services	Payment and Settlement	Retail Banking	Private Banking	Comm Bankir
Business Disruption and System Failures	0	0	0	0	0	1,008,000	50,232,000	0	16,200
Clients, Products and Business Practices	497,400,000	338,000,000	224,000,000	652,760,000	273,200,000	50,400,000	595,800,000	84,800,000	690,000
Damage to Physical Assets	25,200,000	1,200,000	0	0	0	0	20,400,000	0	40,000
Employment Practices and Workplace Safety	11,200,000	32,800,000	8,400,000	7,200,000	0	0	32,400,000	1,200,000	26,120
Execution, Delivery and Process Management	2,000,000	800,000	9,200,000	60,400,000	20,400,000	5,600,000	124,000,000	800,000	14,000
External Fraud	64,000,000	38,800,000	37,600,000	22,800,000	269,000,000	5,600,000	51,200,000	82,000,000	395,400
Internal Fraud	0	3,200,000	0	65,600,000	0	0	800,000	0	2,400

Примечание: название таблицы — «Общая карта рисков»;  
 строки: перечислены все стандартные типы потерь («Базель II»);  
 столбцы: стандартная классификация направлений деятельности («Базель II»).

РИС. 7. ПРИМЕР КИРа «КОЛИЧЕСТВО ПРОСТОЕВ КАНАЛОВ СВЯЗИ»



- процент операций, требующих ручного ввода данных;

- время неработоспособности IT-системы;

- количество сбоях программного обеспечения;

- процент неправильно переданных данных;

- число случаев, связанных с потерей данных;

- количество проведенных мероприятий, направленных на обеспечение безопасности работы системы;

- своевременное обновление процедур;

- среднее время реакции на технический сбой в системе;

- среднее время проведения одной расчетной операции;

- число поломок в системе;

- число случаев, связанных с нарушением энергоснабжения;

- частота обновления программного обеспечения банка;

- оценка напряженности трафика IT-системы.

**«Бизнес-процессы»:** проводится идентификация КИРов по видам внутренних процессов в банковской структуре (осуществление торговых операций на денежном рынке или

на рынке ценных бумаг, процессинг, операционно-кассовое обслуживание юридических лиц, операции по обмену валюты, налично-кассовое обслуживание, эквайринг пластиковых карт, инкассация, осуществление операций на межбанковском рынке, обслуживание через банкоматы, процесс бухгалтерского и управленческого учета и отчетности, внутренние процессы документооборота, административно-хозяйственная деятельность банка, процесс внутреннего контроля и т. д.). Например:

- количество электронных платежей, осуществленных через систему ЦБ;

- число клиентов, удовлетворенных продуктом;

- число проведенных контрольных мероприятий (за месяц / квартал / полугодие);

- процент осуществления клиентских платежей через систему «Клиент-банк»;

- число случаев мошенничества с использованием пластиковых карт;

- количество платежей с использованием аккредитивов / чеков;

- количество неправильно осуществленных расчетных операций, обнаруженных службой внутреннего контроля;

- число операционных задержек при выполнении расчетных операций;
  - количество осуществленных платежей через систему корреспондентских счетов ностро с банками-резидентами;
  - количество осуществленных платежей через систему корреспондентских счетов ностро с банками-нерезидентами;
  - ошибки в реквизитах платежей;
  - число реализованных «Планов действий» за квартал;
  - число обращений к расчетным счетам в онлайн-режиме;
  - число обращений клиентов в службу поддержки;
  - количество вновь открытых клиентских счетов;
  - соотношение фактически проведенных аудиторских проверок с их запланированным количеством;
  - число страховых контрактов;
  - внедрение протокола контроля фатальных рисков (Fatal Risk Control Protocol);
  - процент исследованных несчастных случаев на работе;
  - число потенциальных потерь в отчете;
  - количество повторяющихся инцидентов;
  - процент подтвержденных значительных потерь;
  - процент случайных потерь;
  - отношение предотвращенных потерь к общему числу потерь;
  - количество неправильно составленных контрактов;
  - сумма требований по страховым контрактам;
  - суммарное количество ДТП на уровне организации;
  - количество ДТП в расчете на 1 км пробега;
  - количество проверок вентиляционных систем;
  - количество проверок технического состояния корпоративных транспортных средств;
  - число созданных отчетов в течение заданного временного интервала;
  - общая сумма штрафов (в рублях);
  - среднее время рассмотрения рекламации;
  - средний объем операций на одного клиента.
- «Персонал»:** проводится идентификация КИРов по факторам, непосредственно связанным с сотрудниками компании. Например:
- процент «сменяемости» сотрудников;
  - процент неадекватных действий персонала, выявленных в ходе аудиторской проверки;
  - процент уровня некомпетентности сотрудника;
  - степень зависимости компании от определенного сотрудника;
  - число рабочих дней, пропущенных персоналом по уважительным причинам;
  - число позитивных оценок или полученных наград;
  - соотношение числа уволившихся сотрудников к общему числу работников;
  - суммарное количество нерабочих дней по причине болезни;
  - суммарное количество нерабочих дней по причине несчастных случаев на работе;
  - количество дисциплинарных взысканий, примененных к сотрудникам;
  - количество рацпредложений, поступивших от сотрудников;
  - отношение количества работоспособных сотрудников к общему числу персонала компании;
  - количество денежных средств, потраченных компанией на безопасность и здоровье персонала в расчете на одного служащего;
  - диспансеризация сотрудников;
  - отношение проведенных тренингов к их запланированному количеству;
  - процент дублирования функций сотрудников.
- «Внешние риски»:** проводится идентификация КИРов по внешним источникам воздействия. Например:
- число событий, произошедших из-за внешних факторов (в том числе социальных или политических событий);
  - число стихийных бедствий, нанесших ущерб организации;
  - число пожаров;

- количество несанкционированных проникновений в базу данных / архив банка;

- число взломов банкоматов (на каждую тысячу АТМ);

- число внешних хищений наличных средств / имущества;

- количество несанкционированных проникновений в помещения банка;

- количество поломок банкоматов.

Как видите, число КИРов достаточно велико. Библиотеки некоторых банков насчитывают до 2 тыс. индикаторов риска, поэтому целесообразно классифицировать их по направлениям деятельности вашего финансового учреждения. Мы приведем лишь несколько примеров.

#### **Направление деятельности «Розничный бизнес»:**

1) КИРы для бизнес-процессов:

- клиенты:

- неопознанные зачисления / списания;

- штрафы, уплаченные клиентами;

- некорректное поведение клиентов;

- некорректное выполнение обязательств со стороны банка;

- контрагенты + поставщики и подрядчики:

- платежные системы (Visa, Master Card, Western Union);

- инкассаторы;

- процессинговые компании;

- внутрибанковские процессы:

- претензии клиентов;

- штрафы, уплаченные клиентам (операционные потери);

- показатели объема операций: обороты по кассе, обороты по расчетным счетам, количество депозитов, количество переводов без открытия счетов;

- загруженность персонала фронт-офиса (кассиров, операционистов);

- загруженность персонала бэк-офиса (валютных контролеров, экономистов);

- загруженность персонала call-центра;

2) КИРы для IT-системы:

- сбои оборудования и инфраструктуры;

- сбои в работе программного обеспечения;

- внешние сбои (из-за каналов связи, провайдеров и т. д.);

3) КИРы для персонала:

- «текучка» кадров;

- обучение персонала;

- наличие конфликта интересов у сотрудников.

#### **Направление деятельности «Потребительское кредитование»:**

1) КИРы для бизнес-процессов:

- клиенты:

- фальсификация документов;

- контрагенты + поставщики и подрядчики:

- агентства по сбору платежей;

- некорректное поведение контрагентов (банков, платежных систем и т. д.);

- внутрибанковские процессы:

- претензии клиентов;

- штрафы, уплаченные клиентам (операционные потери);

- показатели объема операций: количество выданных / погашенных кредитов;

- загруженность персонала фронт-офиса;

- загруженность персонала бэк-офиса (экономистов);

- загруженность персонала call-центра;

- звонки по поводу просрочки;

- проверка номеров телефонов на этапе выдачи кредита;

2) КИРы для IT-системы:

- каналы связи, оборудование, программы;

- онлайн-работа модулей «Скоринг» и «Верификация»;

3) КИРы для персонала:

- «текучка» кадров;

- обучение персонала.

#### **Направление деятельности «Инвестиционный банк» (рис. 8):**

1) КИРы для бизнес-процессов:

- клиенты:

- задержка поставки / оплаты;

- штрафы, полученные от клиентов;

- контрагенты + поставщики и подрядчики:

- Bloomberg, Reuters;

- некорректное поведение поставщиков и подрядчиков;

РИС. 8. ПРИМЕР КИРа «КОЛИЧЕСТВО ЗАДЕРЖЕК ПОСТАВОК ЦЕННЫХ БУМАГ»



- внутрибанковские процессы:
  - штрафы, уплаченные клиентам (операционные потери);
  - показатели объема операций: количество сделок, размер позиции;
  - загруженность персонала фронт-офиса;
  - загруженность персонала бэк- и мидл-офиса (экономистов);
  - прецеденты нарушения лимитов;
- 2) КИРы для IT-системы:
  - каналы связи, оборудование, программы;
- 3) КИРы для персонала:
  - ротация кадров;
  - наличие конфликта интересов у сотрудников.

4. Выбрав наиболее подходящие, на ваш взгляд, КИРы, вы должны протестировать их, чтобы удостовериться в их действительной эффективности. Делается это с помощью системы внутренних рейтингов — проще говоря, путем присвоения баллов (от 1 до 5). Чем больше экспертов участвует в процессе оценки, тем лучше. Естественно, подразумевается, что КИРы, относящиеся к определенному отделу / подразделению, оцениваются именно работниками этого подразделения, а не какого-либо

другого (например, отдел по работе с персоналом присваивает баллы КИРа, связанным с сотрудниками / персоналом учреждения, и не участвует в оценке процедур банка, относящихся к отделу внутреннего контроля и аудита). КИРы, набравшие по итогам средний балл менее 4, рекомендуются исключить из анализа.

В табл. 2 приведен пример анкеты относительно возможности применения того или иного индикатора риска.

В указанном примере рекомендуется оставить только КИР 3, поскольку он набрал наибольшее число баллов. В связи с тем что в реальной жизни крупный банк сталкивается чуть ли не с тысячей всевозможных КИРов, соответствующих основным процессам, направлениям бизнеса, потерям и событиям, происходящим в организации, в идеале подобный процесс оценки рекомендуется проводить, основываясь на исторических данных, применяя статистические методики с использованием углубленного изучения данных — Data Mining, выявляющего взаимосвязи между данными (например, с помощью продукта SAS Enterprise Miner).

ТАБЛИЦА 2. ПРИМЕР АНКЕТЫ «АНАЛИЗ ВОЗМОЖНОСТИ ПРИМЕНЕНИЯ ИНДИКАТОРОВ РИСКА»

№	Параметр КИРа	Вопрос для оценки	Низкий уровень (балл 1)	Средний уровень (баллы 2–4)	Высокий уровень (балл 5)	КИР 1	КИР 2	КИР 3	КИР 4
1	Частота появления КИРа	Соответствует ли частота этого КИРа частоте возникновения риска на практике?	Частота КИРа трудно определена или недостаточно высока	Как минимум один раз в неделю, но при этом неясно, достаточно ли это часто	Ежедневно для указанного КИРа	3	2	5	4
2	Пороговые значения	Установлены ли пороговые значения для КИРа аналитическим путем?	Пороговые значения отсутствуют	Пороговые значения установлены, но не аналитическим путем	Пороговые значения установлены аналитическим путем	3	1	5	1
3	Тип	Является ли данный КИР опережающим индикатором?	Нет, это исторический индикатор (по факту)	Недостаточен для предсказания рисков события и требует преобразования	Опережающий индикатор	1	3	4	2
4	Отношение	Очевидно ли, к какому отделу относится данный КИР?	Связь не очевидна	Связь присутствует, но не однозначна (например, подходит нескольким отделам)	КИР четко отражает специфику отдела, к которому относится	5	5	5	3
5	Данные	Имеются ли в вашем банке исторические данные по этому КИРу?	Это новый КИР, и по нему пока нет данных	Есть данные, но они пока не извлечены / не обработаны	Имеется большой массив доступных для анализа данных	4	5	5	3
6	Чистота данных	Каково качество данных по этому КИРу?	Низкое качество	Среднее качество	Высокое качество	1	5	5	4
					<b>Средний балл</b>	<b>2,8</b>	<b>3,5</b>	<b>4,8</b>	<b>2,8</b>

Таким образом, в результате успешно проведенного анализа КИРов у вас останутся буквально один–два индикатора, которые будут действительно ключевыми для данного вида риска. Интересно отметить, что отбор КИРов можно производить не только при помощи качественной оценки.

Практический пример определения оптимального КИРа при помощи количественной оценки его значимости: один из российских банков предоставил нам для анализа информацию обо всех технологических сбоях во

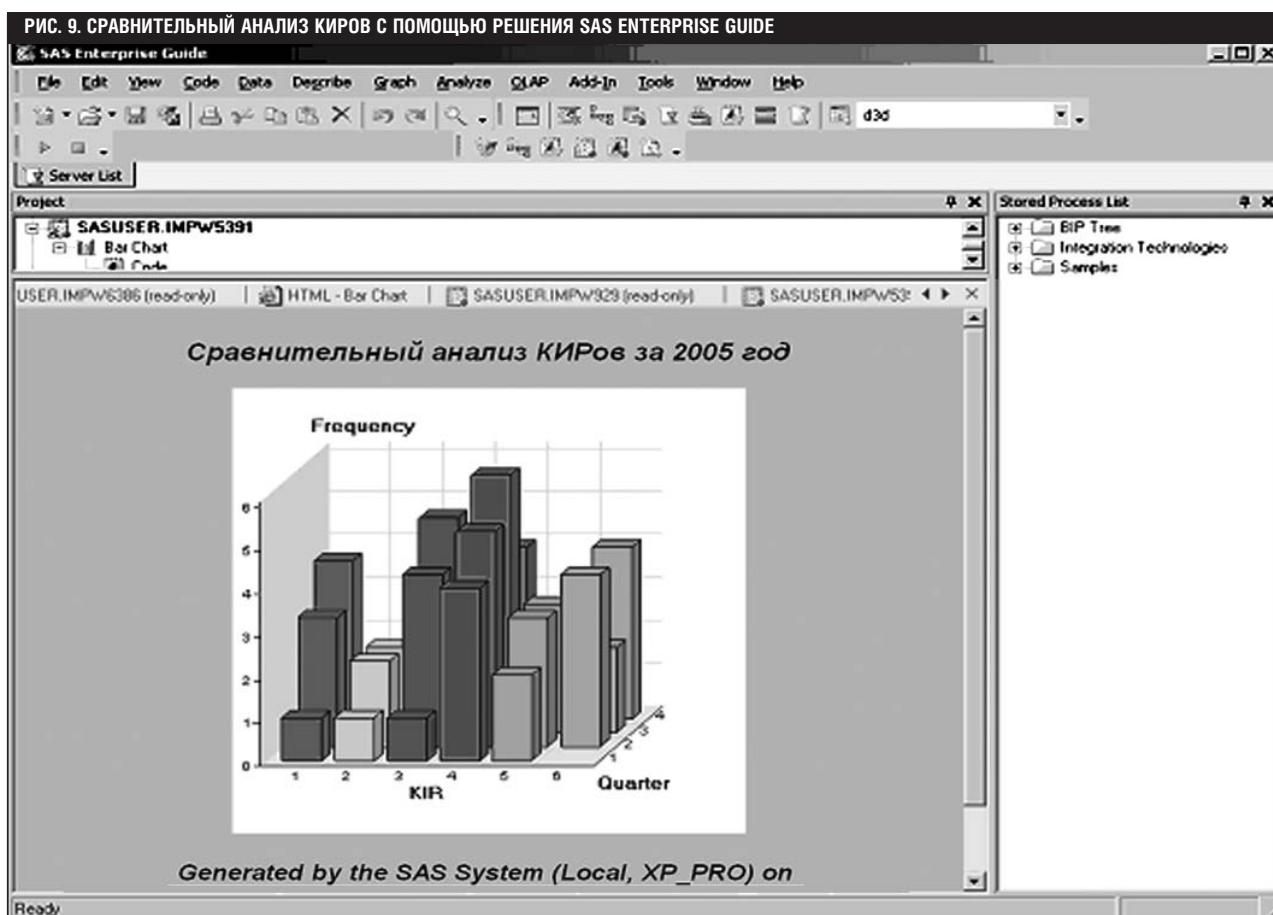
внутренней банковской системе за 2005 г. На основе имеющихся данных (более 3,5 тыс. записей) к анализу были допущены следующие шесть КИРов:

КИР 1 — «Общее время неработоспособности IT-системы»;

КИР 2 — «Количество «апгрейдов» существующего в банке программного обеспечения»;

КИР 3 — «Количество сбоев программного обеспечения»;

КИР 4 — «Оценка напряженности трафика IT-системы»;



Примечание: график распределения шести рассматриваемых КИРов по кварталам.

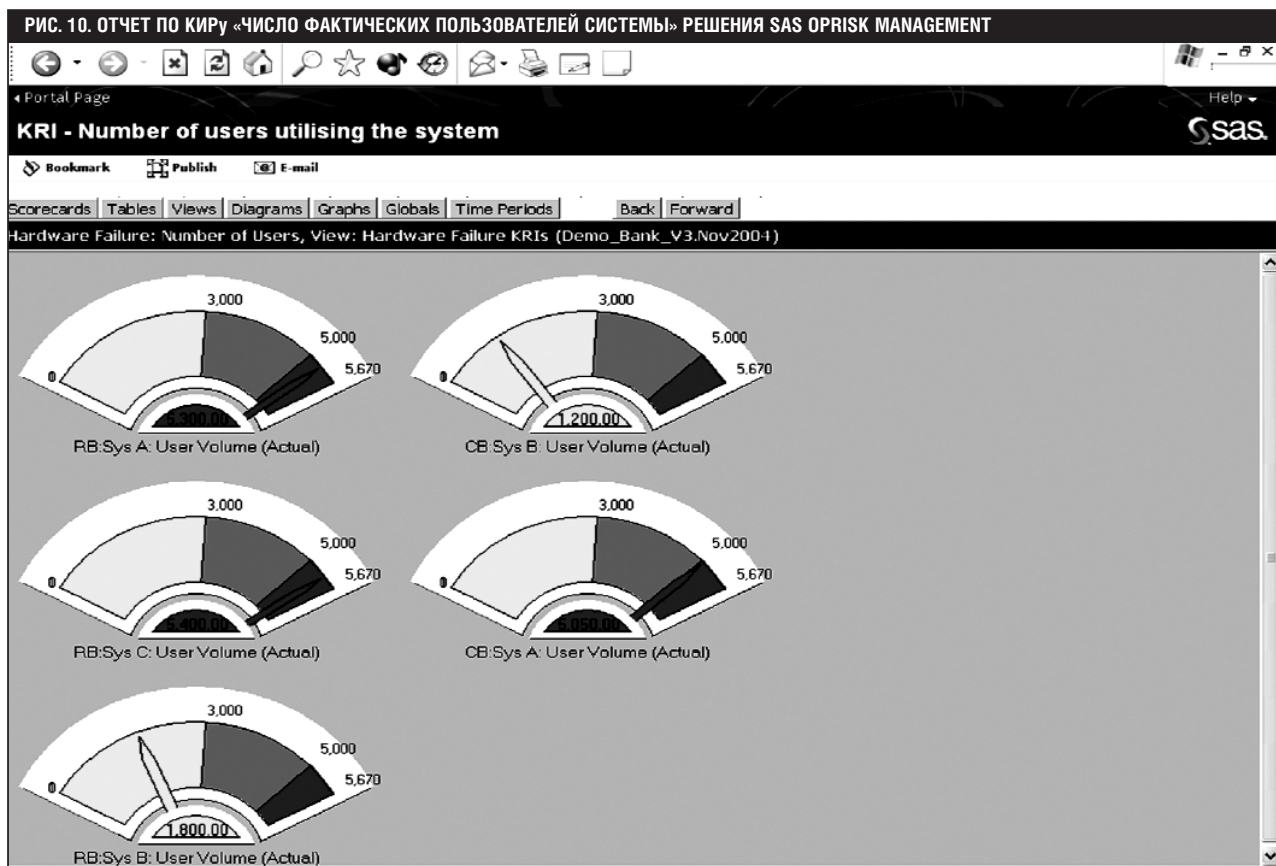
КИР 5 — «Среднее время реакции на технический сбой в системе»;

КИР 6 — «Число случаев потери данных / информации» (рис. 9).

В качестве входных переменных они были переданы на анализ вместе с бинарной целевой переменной SYS («IT-система работает / простаивает») и переменной частоты FREQ.

По отчетному графику мы можем проследить значимость того или иного КИРа, распределенную поквартально (четыре столбца для каждого КИРа). Подводя итоги, следует отметить, что КИР 4 и КИР 3 признаны наиболее «чувствительными» к технологическим операционным рискам и поэтому рекомендуются для использования.

5. Последним, но не менее важным шагом в работе с КИРами является составление консолидированной отчетности по результатам проведенного анализа (рис. 10). Вы выбрали адекватный КИР, успешно оценили деятельность работы отдела / подразделения / направления бизнеса организации, и теперь ваша задача — довести соответствующие выводы до сведения не только вышестоящего начальства, но и соответствующих бизнес-пользователей (в рамках установленного для них информационного доступа). Предполагается применение таблиц и графиков, отражающих адекватную картину рисков на уровне всей организации, с указанием «проблемных» зон высоких рисков и планов предпринятых действий (контрольных мероприятий).



*Примечание:* графики указывают реальное число пользователей для каждой из пяти банковских систем (RB SysA, RB SysB, RB SysC, CB SysA, CB SysB) в случае отказа работы системы (черный цвет). Светло-серый цвет означает, что данные системы в настоящий момент проблем с работой не имеют.

В заключение хотелось бы дать несколько полезных советов тем, кто хотел бы успешно внедрить систему ключевых индикаторов риска в работу своего учреждения.

- Используйте лишь те индикаторы, которые соответствуют профилю риска именно вашей компании (департамента, отдела и т. п.). Специфика КИРов различна для разных банков, пусть даже со сходным профилем.

- Применяйте лишь те индикаторы, по которым вы имеете достаточное количество данных, поскольку точность вычислений достигается благодаря достаточной репрезентативности.

- Чрезмерное использование многочисленных индикаторов также может сыграть с вами злую шутку: вы получите нечеткую (а может

быть, и противоречивую) общую картину рисков. Так, при осуществлении практических проектов специалисты SAS столкнулись с тем, что банки, применяющие более 1 тыс. КИРов, испытывают значительные трудности при составлении агрегированной оценки рисков или сводных отчетов об управлении рисками на уровне организации.

- Комбинируйте использование опережающих индикаторов с историческими КИРами, чтобы быть ближе к реалиям жизни.

- Заручитесь поддержкой начальства. Не каждому понравится, когда вы приметесь «измерять» его работу. Не исключено, что некоторые попытаются даже скрыть от вас реальную картину, немного приукрасив ее (например, уменьшая число неверных операций

и т. п.), поэтому по возможности опирайтесь на данные из независимых источников.

■ Не путайте индикаторы риска с индикаторами деятельности или контроля, т. к. у них разное назначение.

■ Избегайте излишне усложненных индикаторов. Ответность, которую вы предоставите по ним пользователям, должна быть понятной.

■ Для каждого используемого в практике КИРа должно быть ответственное лицо (KRI Owner). В его задачи входит не только корректная расстановка пороговых значений

для данного КИРа, но и принятие соответствующих мер в том случае, когда индикатор выходит за отведенные ему пределы. Ранее оповещение — это наилучшая мера предотвращения потери. На практике для этого используются всевозможные средства, включая электронную почту и SMS.

■ Если вы хотите получить надежный и адекватный индикатор, не пытайтесь вычислить КИРы вручную. Это трудоемкий процесс, отнимающий много времени и ресурсов. Предоставьте решение данной задачи профессиональному программному обеспечению.

## ЛИТЕРАТУРА

1. Банковские риски: оценить, управлять, контролировать: Аналитическая записка // Материалы международного форума «Управление рисками в России». — М., 2005.
2. Ernst & Young (2002). Leading practices in RM. Current Applications of *Enterprise Risk Management*, May, Netherlands.
3. Finlay M. (2005). Operational risk: next stop — benchmarking. *Global Risk Regulator*, September.
4. Katilova N. (2004). Finance Stochastique: Methodes Numeriques!. Research Report, LORIA, April. Nancy, France.
5. Mestchian P. (2003). SAS operational risk technology. *Operational Risk Magazine*.
6. Moorsel H., Visser C. A. (2002). Een theoretisch kader voor integraal risicomangement. Toegesplitst op de overheid.
7. Taylor C. (2004). Operational risk: KRIs move up a gear. *Global Risk Regulator*, November.
8. Taylor C., Davies J. (2003). Getting traction with KRIs: Laying the Groundwork. *The RMA Journal*, November.
9. The Basel Committee on Banking Supervision, Bank for International Settlements (2003). Sound Practices for the Management and Supervision of Operational Risk.
10. Walker E., Dutemple A.-F. (2006). Reducing operational risk. *SAS Business Intelligence Journal*, No. 2.
11. [www.bankir.ru](http://www.bankir.ru).
12. <http://www.bis.org/bcbs>.
13. <http://www.garp.com>.
14. <http://www.globalriskregulator.com>.
15. <http://www.KRIlex.org>.
16. <http://www.operationalriskonline.com>.
17. <http://www.prmia.org>.
18. <http://www.risk.net>.
19. [www.riskofficer.ru](http://www.riskofficer.ru).
20. [www.sas.com/russia](http://www.sas.com/russia).

### Благодарность

Авторы выражают особую признательность Оксане Старосельской, руководителю отдела операционных рисков «КМБ-Банка», за ценные практические советы при написании данной статьи.