

...и непрерывности бизнеса компании, а на-  
...грамм, несколько грамотно построены бизнес-  
...процессы компании. Таким образом, представ-  
...ленная модель является не только инструмен-  
...том, позволяющим дать количественную оценку  
...ОР, но и оценить, соответствует ли бизнес-  
...архитектура компании (совокупность бизнес-  
...процессов, ресурсов, временных рамок их реа-  
...низации) IT-архитектуре и требованиям непре-  
...рывности бизнеса, исходя из которых устанавли-  
...ваются требования к классу надежности IT-  
...систем, поддерживающих данный бизнес.

*Данное исследование проводилось в рамках договора  
№ 13.G25.31.0096 с Министерством образования  
и науки Российской Федерации о "Создании  
высокотехнологичного производства кросс-платфор-  
менных систем обработки неструктурированной*

обеспечения для повышения эффективности  
управления инновационной деятельностью  
предприятия в современной России".

#### Литература

1. Лаврушина Я. Н., Макарова А. А. Методологические подходы к анализу и оценке операционных рисков в статистически некорректной среде // Журнал "Информатика", 2011. № 2 (16).
2. Bontl G., Kalkbrener M., Lotz C., Stahl G. Credit concentrations under stress // Journal of Credit Risk No. 2 (3). P. 115—136.
3. Frachot A., Georges P., Roncalli T. Loss distribution approach for operational risk (March 30, 2001). Available SSRN: <http://ssrn.com/abstract=1032523>. 39 p.
4. Marrison C. The fundamentals of risk management // McGraw-Hill, 2002. — 415 p.
5. Operational Risk — Supervisory Guidelines Advanced Measurement Approaches. Basel Committee Banking Supervision, June, 2001.

## AN APPROACH TO QUALIFICATION OF OPERATING RISK IN STATISTICAL INCORRECT MEDIA (INTERRUPT IN IT-SERVICE)

Ya. N. Lavrushina, A. A. Makarova  
"Gazpromexport" PLC, Moscow, Russia

A. V. Kulikov

Moscow Institute of Physics and Technology (State University), MIPT (SU),  
Moscow region, Dolgoprudny, Russia

A. I. Gromov

BPM Chairman, National Research University, Moscow, Russia

*The article is dedicated to quantitative assessment of operational risk in statistical incorrect environment specified by insufficiency of data: IT-system failure/breakdown and time to recovery. System capabilities provided by manufacturer as well as Company's business continuity reliability specifications were used as the input data for the model. The authors used their own experience of operational risk evaluation for nonfinancial business. The given research was held in a frame of the contract № 13.G25.31.0096 with the Ministry for Education and Science of Russian Federation "Deployment of hi-tech manufacture of unstructured information processing in cross-platform system on the free software basis due to increase management efficiency of innovative activity of the enterprises in modern Russia economy".*

**Keywords:** quantitative assessment, operational risk exposure, expected and unexpected losses (operational risk), IT-system failure/breakdown probability, mean downtime, business continuity matrix.

Лаврушина Яна Николаевна, старший менеджер отдела операционных и кредитных рисков.

E-mail: [ya.lavrushina@gazpromexport.com](mailto:ya.lavrushina@gazpromexport.com)

Макарова Анастасия Александровна, главный специалист отдела операционных и кредитных рисков.

E-mail: [a.makarova@gazpromexport.com](mailto:a.makarova@gazpromexport.com)

Куликов Александр Владимирович, ассистент кафедры высшей математики.

E-mail: [a.kulikov@gazpromexport.com](mailto:a.kulikov@gazpromexport.com)

Громов Александр Игоревич, проф., зав. кафедрой моделирования и оптимизации бизнес-процессов.



Информационные технологии представляют собой не только средство автоматизации бизнес-процессов, но и сами становятся интегрированной частью данных процессов. Таким образом, информационные технологии, с одной стороны, позволяют компании выйти на новый уровень развития, а с другой — делают ее бизнесе зависимым от безотказности и бесперебойности в работе оборудования, инфраструктурных и конечных пользовательских систем. По своей природе риск возникновения потерь, связанных со сбоями и ошибками в программном обеспечении, остановками или сбоями в работе ИТ, систем передачи информации, внутренними инцидентами в сфере информационной безопасности, остановками и сбоями коммуникационных систем, безопасности здания относится к операционному риску (технический риск).

Такое положение вещей влечет за собой потребность в постоянной оценке вероятности наступления негативного события вследствие отказа в работе ИТ-систем, а также оценке последствий реализации такого события.

Операционные потери — относительно редкое явление (но возможное), тогда как потери вследствие ОР чаще всего весьма значительны (рис. 1). Свойства распределений потерь вследствие различных видов риска были рассмотрены в работах [2—4].

присвоения ей кредитного рейтинга, не дает адекватную оценку требованиям к экономическому капиталу на покрытие ОР. Поэтому во избежание проблем, связанных с малой репрезентативностью данных для анализа, необходимо использовать такую модель оценки ОР, результаты методов оценки которой будут давать реальное представление о его уровне.

### Основные компоненты количественной оценки технического риска

Технический риск представляет собой функцию от следующих параметров:

- вероятность наступления операционного события с определенным уровнем потерь  $P_i(C_i, (p_1, \dots, p_n), (1/\lambda_1, \dots, 1/\lambda_n), \tau)$  — вероятность того, что существует риск нарушения непрерывности реализации  $i$ -го бизнес-процесса компании в критичные временные рамки вследствие наступления событий, относящихся к ОР с уровнем потерь (подверженностью ОР)  $C_i$ , зависящая от  $(p_1, \dots, p_n), (1/\lambda_1, \dots, 1/\lambda_n), \tau$ ;
- подверженность ОР ( $C_i$ ) — стоимость проведенных внешнеэкономических операций, подверженных ОР вследствие некорректного исполнения  $i$ -го бизнес-процесса;

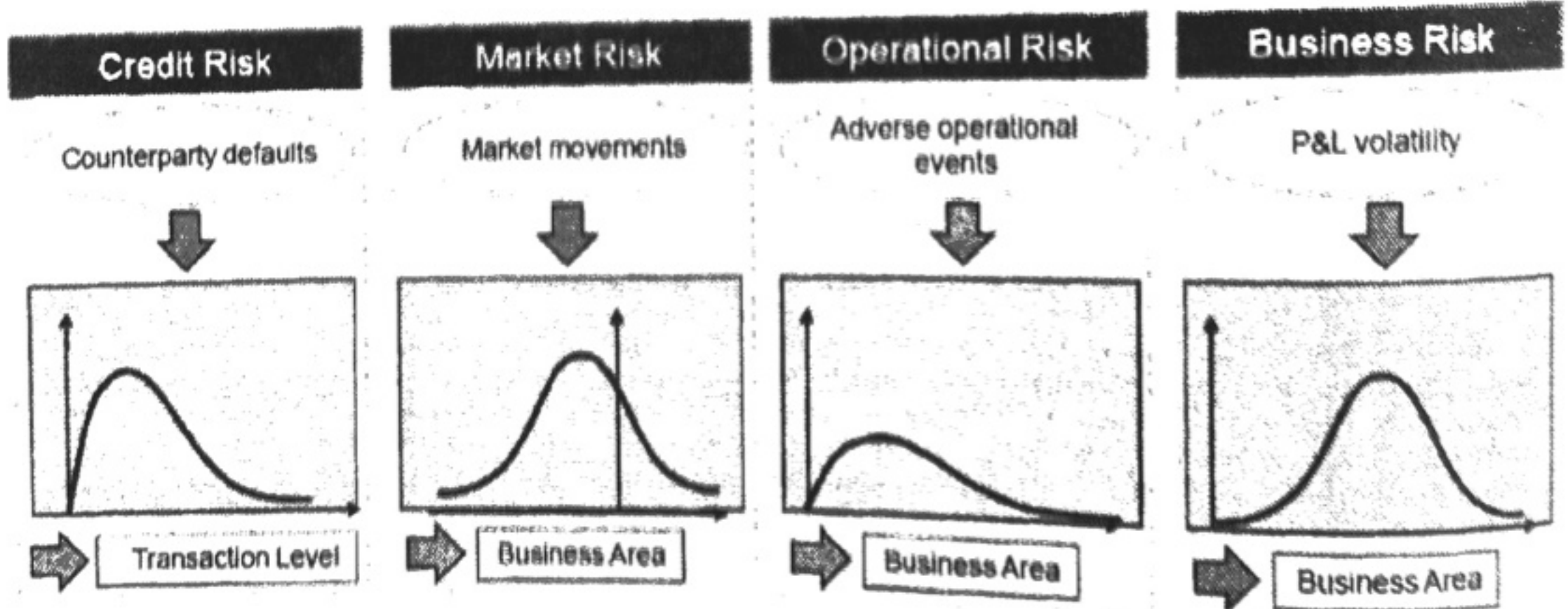


Рис. 1. Сравнение распределений потерь вследствие основных видов риска

Чаще всего маловероятные события, приводящие к операционным потерям, находятся "в хвосте" статистического распределения, т. е. за пределами разумного доверительного интервала. Однако большинство операционных событий вносит существенный вклад "в хвост" распределения убытков, и отсутствие учета ОР может привести к банкротству компании при реализации того или иного операционного события. В связи с этим использование классических оценок риска, таких как *среднее* или *operational value at risk* уровня  $1 - \lambda$ , где  $\lambda$  — вероятность, соответствующая вероятности дефолта компании при

- вероятность выхода  $j$ -й ИТ-системы из строя ( $p_j$ ) — вероятность того, что в какой-то определенный день  $j$ -я ИТ-система может выйти из строя;
- среднее время простоя  $j$ -й ИТ-системы ( $1/\lambda_j$ ) — среднее время технического сбоя (в связи с реализацией операционного события)/ремонта ИТ-системы, отвечающей за корректную реализацию бизнес-процесса;
- $\tau$  — временные рамки, обусловленные бизнес-процессами компании. ОР выражается величиной операционных потерь ( $S$ ), для расчета которых необходима оценка



на всех вышеперечисленных компонент риска. Потери можно представить в виде формулы:

$$S = \sum C_i \cdot \xi_i,$$

где  $\xi_i$  — бернуллиевская случайная величина, принимающая значение 1 в случае наступления операционного события (т. е. с вероятностью  $P_i$ ) и 0 в противном случае;

$C_i$  — соответствующая подверженность.

Основными показателями количественной оценки величины ОР являются:

- ожидаемые потери — средний размер потерь. Данные потери рассматриваются как часть общих издержек компании. Однако данные потери не несут никакой информации об ОР компании, так как распределение потерь имеет слишком тяжелые хвосты;

- непредвиденные потери (операционный  $V(@R)$ ) — максимальный размер потерь с заданной доверительной вероятностью. Для оценки непредвиденных потерь Базельский комитет рекомендует брать доверительный интервал на уровне 0,1 % с годовым периодом моделирования [5]. Однако такие критерии оценки применимы для финансовых (банковских) институтов, где операционные события часты, а потери от них незначительны и ведется статистическая база по ним.

Ниже рассматривается модель количественной оценки операционного риска в статистически некорректной среде с достаточно редким проявлением операционного события, но со значительными последствиями. В виду отсутствия внутренней статистики по событиям ОР предлагается использовать технические характеристики систем, представленные изготовителем (продавцом) данных систем при их установке. Поэтому для оценки непредвиденных потерь предлагается брать доверительный интервал, соответствующий классу надежности систем, принятому в компании в целях обеспечения непрерывности бизнеса. Рассматривается оценка ОР для систем с классом надежности 99,99 %. Таким образом, для оценки непредвиденных потерь берется доверительный интервал на уровне 0,01 % с годовым периодом моделирования.

Подверженность ОР представляет собой стоимостную оценку величины принимаемого риска от операций, подверженных ОР в случае реализации операционного события.

Потенциальная подверженность (potential exposure) рискам возникает в будущем исходя из реализации того или иного бизнес-процесса в соответствии с бизнес-картой компании и носит случайный характер. Оценка будущей подверженности ОР требует нахождения вероятностного распределения будущих денежных потоков. При дальнейшем моделировании распределения потерь от ОР выделяются следующие два вида потенциальной подверженности:

- ожидаемая подверженность операционному риску — средняя стоимость проведенных

внешнеэкономических операций, подверженных ОР в случае реализации операционного события;

- наибольшая подверженность операционному риску — максимальная величина подверженности при заданной доверительной вероятности.

### Переход от качественной к количественной оценке технического риска

В нефинансовых структурах процесс мониторинга и сбора статистических данных о событиях и негативных последствиях ОР, как правило, не налажен и затруднен. В таких случаях идентификацию и качественную оценку технического риска следует проводить в соответствии "Методикой качественной оценки ОР в статистически некорректной среде" [1]. Особенность данной методики заключается в том, что в разрезе каждого бизнес-процесса "взвешивается" уровень операционного риска каждого вида относительно всех операционных рисков, выявленных в процессе идентификации рисков данного бизнес-процесса в разрезе бизнес-функций.

### Построение матрицы непрерывности бизнеса

Для оценки потерь компании вследствие реализации событий ОР строится сценарная матрица непрерывности бизнеса (матрица А), исходя из хронологической и функциональной взаимосвязи бизнес-процессов и бизнес-функций. За основу построения матрицы непрерывности бизнеса берется бизнес-карта компании, где все бизнес-функции, входящие в бизнес-процессы каждой рассматриваемой бизнес-линии, выстраиваются в хронологическом порядке.

Исходя из целей бизнеса и конечного результата на выходе бизнес-линии и на основании бизнес-карты компании проводится анализ сценариев, который является универсальным и отражает зависимость непрерывности бизнеса от сбоя (невозможность реализации) отдельных бизнес-функций. При этом не имеет значения, по какой именно причине вышеупомянутый сбой происходит (табл. 1).

Таблица 1

Матрица А. Матрица непрерывности бизнеса

Бизнес-процесс	Бизнес-функция	Сценарии						
		1	2	3	4	5	6	7
БП1	БФ1.1	1						
	БФ1.2	1	1					
	БФ1.3		1	1				
БП2	БФ2.1	1			1			
	БФ2.2		1		1	1		
	БФ2.3	1	1		1		1	
БП3	БФ3.1		1		1	1		1

Обозначим матрицу непрерывности бизнеса через  $A = (a_{ij})$ . Каждому сценарию соответствуют последствия в виде нарушения непрерывности бизнеса на каждой конкретной бизнес-функции цепочки, т. е. если нереализация  $i$ -й бизнес-функции ведет к нарушению  $j$ -го сценария, то  $a_{ij} = 1$ , иначе 0.



Исходя из непрерывности бизнеса проводится выделение бизнес-функций, критичных ко времени их реализации, а также назначение критических временных периодов и допустимого времени сбоя/восстановления инфраструктурных и зависимых от них пользовательских сервисов. Для решения данной задачи необходимо наложить полученную матрицу непрерывности бизнеса на IT-архитектуру компании, т. е. выяснить, какие именно пользовательские сервисы автоматизируют каждую бизнес-функцию, а также выяснить, как сбои и остановки в их работе могут повлиять на бизнес компании.

**Построение матрицы зависимости бизнес-функций от пользовательских сервисов**

В качестве исходных данных для построения матрицы В используются результаты экспертной оценки степени влияния факторов риска на реализацию бизнес-процессов в разрезе бизнес-функций [1]. Данная оценка проводилась представителями подразделений-владельцев бизнес-процессов на основании шкалы (табл. 2), основанной на критериальности, разработанной исходя из гипотетической возможности нарушения непрерывности бизнеса.

Таблица 2

**Шкала оценки степени влияния фактора риска на реализацию бизнес-функции и бизнес-процесса**

Критерий	Степень влияния	Балл
Невозможность выполнения бизнес-функции и, как следствие, невозможность осуществления бизнес-процесса	Высокая	4
Некорректное выполнение бизнес-функции и, как следствие, невозможность осуществления бизнес-процесса	Выше средней	3
Невозможность выполнения бизнес-функции, но при этом отсутствует влияние на ход осуществления бизнес-процесса	Средняя	2
Некорректное выполнение бизнес-функции, но при этом отсутствует влияние на ход осуществления бизнес-процесса	Низкая	1

Данные экспертной оценки заносятся в форму, представляющую собой таблицу, где в строках указаны выстроенные в хронологическом порядке бизнес-процессы с составляющими их бизнес-функциями, в столбцах перечислены все факторы технического риска, а на пересечении строк и столбцов стоят результаты вышеописанной экспертной оценки (табл. 3).

Таблица 3

**Матрица В. Матрица влияния факторов риска на реализацию того или иного бизнес-процесса или бизнес-функции**

Бизнес-функции, бизнес-процессы	Факторы технического риска							
	ФР1	ФР2	ФР3	ФР4	ФР5	ФР6	ФР7	ФР8
БФ1.1	2		3		2	2	4	3
БФ1.2	4	1	2	1				
БФ1.3								1
БФ2.1		1			3	1		
БФ2.2		1			4		3	
БФ2.3								
БП3.1	2	4	1	4	4	4	2	
БП3.2		2	1	2	4			1



Обозначим эту матрицу за  $B = (b_{jk})$ , где  $b_{jk}$  — степень влияния  $k$ -го фактора риска на исполнение  $j$ -й бизнес-функции (0 означает, что данный фактор риска не влияет на исполнение данной бизнес-функции).

Следует отметить, что в качестве факторов технического риска в данной работе рассматриваются невозможности доступа к пользовательским сервисам. Таким образом, построенная матрица В не только содержит данные о том, какие пользовательские сервисы участвуют в бизнесе компании при исполнении каждой бизнес-функции, а также дает представление о степени их влияния на непрерывность бизнеса.

**Построение матрицы зависимости пользовательских сервисов от инфраструктурных сервисов**

Для построения матрицы С используются данные об инфраструктурных и пользовательских сервисах, предназначенных для автоматизации бизнес-процессов компании, и данные об их функциональной зависимости (табл. 4).

Таблица 4

**Матрица С. Матрица зависимости пользовательских сервисов (User Services) от инфраструктурных сервисов (Support Services)**

Инфраструктурные сервисы (Support Services)	Пользовательские сервисы (User Services)							
	US1	US2	US3	US4	US5	US6	US7	US8
SS1	1							
SS2	1	1	1	1	1	1	1	1
SS3								
SS4	1	1	1	1	1	1	1	1
SS5	1							
SS6			1	1	1			1
SS7	1		1					1

Обозначим эту матрицу за  $C = (c_{ik})$ , где  $c_{ik} = 1$  означает, что  $k$ -й инфраструктурный сервис влияет на  $i$ -й пользовательский сервис, т. е. выход его из строя будет означать невозможность доступа к  $i$ -му пользовательскому сервису (0 означает, что данный инфраструктурный сервис не влияет на работу данного пользовательского сервиса).

**Получение матрицы зависимости реализации операционных сценариев от инфраструктурных сервисов**

Используя матрицы А, В и С, определяется возможность реализации того или иного операционного сценария в зависимости от невозможности доступа к тому или иному инфраструктурному сервису (табл. 5).

Таблица 5

**Матрица D зависимости реализации операционных сценариев от инфраструктурных сервисов**

Инфраструктурные сервисы (Support Services)	Сценарии							
	1	2	3	4	5	6	7	8
SS1								
SS2	2	4					2	4
	4	4		3	4		4	4



Окончание табл. 5

Инфраструктурные сервисы (Support Services)	Сценарии							
	1	2	3	4	5	6	7	8
SS3		1					4	2
SS4	4	4		3	4		4	4
SS5	2	4					2	
SS6	3	2		3	4		4	4
SS7	3	4					2	1

Обозначим эту матрицу за  $D = (d_{ij})$ , где  $d_{ij}$  — степень влияния 1-го инфраструктурного сервиса на реализацию  $i$ -го сценария (0 означает, что невозможность доступа к данному инфраструктурному сервису не влияет на реализацию данного сценария). Данная Матрица  $D$  строится следующим образом:  $D = C \bullet B^T \bullet A$ , где обозначенная операция " $\bullet$ " означает, что для произвольных матриц  $G$  и  $H$  матрица  $F = G \bullet H$  определяется следующим образом:  $f_{ik} = \max_j (g_{ij} \cdot h_{jk})$ , т. е. при перемножении матриц определяется максимальное влияние исходного инфраструктурного сервиса на реализацию конечного сценария (при перемножении матриц учитывается тот факт, что невозможность доступа к пользовательскому интерфейсу и фактор риска представляет собой суть одного и того же).

**Количественная оценка операционного риска**

**Выбор минимальной степени влияния фактора риска на реализацию бизнес-функции и бизнес-процесса, критичной для непрерывности бизнеса компании**

Основным критерием нарушения непрерывности бизнеса компании в связи с наступлением операционного события, произошедшим вследствие сбоя ИТ-системы (нарушение доступности), является невозможность осуществления бизнес-процесса. Для количественной оценки ОР необходимо сначала найти ту минимальную степень влияния фактора технического риска на реализацию бизнес-функции и бизнес-процесса, которая приводит к нарушению непрерывности бизнеса. Непрерывность бизнеса нарушается при степени влияния факторов риска на реализацию бизнес-функций и бизнес-процессов с высокой (4 балла) и выше средней (3 балла) оценкой (см. табл. 2). Таким образом, наименьшим баллом критичности для всех рассматриваемых операционных сценариев является балл 3, что будет использоваться при моделировании подверженности операционному риску.

**Описание состояний инфраструктурных сервисов**

Возьмем за  $\xi_i^t$  — состояние  $i$ -го инфраструктурного сервиса в момент времени  $t$  ( $\xi_i^t = 0$ , если сервис доступен; 1, иначе). Будем считать, что инфраструктурные сервисы выходят из строя независимо, и время выхода из строя  $i$ -го инфраструктурного сервиса имеет экспоненциальное распределение с параметром  $\lambda_i^t$ . Также

будем считать, что при выходе из строя инфраструктурные сервисы ремонтируются независимо, и время восстановления функциональности  $i$ -го инфраструктурного сервиса имеет экспоненциальное распределение с параметром  $\lambda_i^r$ . Предположим, что  $\xi_0^i = 0$ . Соответственно,  $\tau_0^i$  — время до  $k$ -го выхода из строя инфраструктурного сервиса,  $\tau_1^i$  — время восстановления функциональности инфраструктурного сервиса после  $k$ -го выхода из строя ( $E \tau_0^i = 1/\lambda_0^i$ ,  $E \tau_1^i = 1/\lambda_1^i$ ,  $\lambda_0^i \ll \lambda_1^i$ ). Тогда

$$\xi_i^t = 0, \text{ если } t < \tau_0^i,$$

$$\xi_i^t = 1, \text{ если } \tau_0^i \leq t < \tau_0^i + \tau_1^i,$$

$$\xi_i^t = 0, \text{ если } \sum(\tau_0^i + \tau_1^i) \leq t < \sum(\tau_0^i + \tau_1^i) + \tau_0^i,$$

$$\xi_i^t = 1, \text{ если } \sum(\tau_0^i + \tau_1^i) + \tau_0^i \leq t < \sum(\tau_0^i + \tau_1^i) + \tau_0^i + \tau_1^i.$$

Таким образом, для моделирования процессов работы инфраструктурных сервисов необходимо знать параметры выхода из строя и восстановления данных сервисов.

**Оценка параметров выхода из строя и восстановления инфраструктурных сервисов**

При наличии достаточной статистики по выходам из строя инфраструктурных сервисов среднее количество выходов из строя  $i$ -го инфраструктурного сервиса за 1 день равно  $\lambda_0^i$  (выходы из строя имеют экспоненциальное распределение; среднее время простоя  $i$ -го инфраструктурного сервиса много меньше среднего времени до нового выхода из строя). Данная оценка параметра  $\lambda_0^i$  является состоятельной, т. е. с увеличением объема полученных статистических данных оценка становится все ближе к неизвестному значению оцениваемого параметра. Аналогичным образом получаем среднее время (в днях) восстановления функциональности  $i$ -го инфраструктурного сервиса, равное  $1/\lambda_1^i$  (время восстановления имеет экспоненциальное распределение). Полученная из этого соотношения оценка параметра  $\lambda_1^i$  также является состоятельной.

Однако не всегда имеется база статистических данных по выходам из строя/ремонту инфраструктурных сервисов, или она недостаточна репрезентативна. Во-первых, это происходит из-за того, что выходы из строя происходят очень редко (параметр  $\lambda_0^i \approx 10^{-3}$ ), а время наблюдения за данными сервисами недостаточно велико (не более 2—3 лет). Вторая причина состоит в том, что в некоторых случаях обслуживание инфраструктурных сервисов отдается на аутсорсинг и компания не располагает статистическими данными по выходам из строя/ремонту данных инфраструктурных сервисов. В данном случае в качестве параметров выхода из строя берутся параметры, предоставляемые изготовителем (продавцом) (количество сбоев в год и среднее время недоступности данных инфраструктурных сервисов).



**Моделирование поведения бизнес-среды, подверженной техническому риску**

Наступление операционного события с заданным уровнем потерь  $C_i$  происходит вследствие реализации  $i$ -го сценария во временные рамки  $t$ . Используя полученную матрицу  $D$  и выбранную минимальную степень влияния фактора риска на реализацию бизнес-функции и бизнес-процесса (критичной для непрерывности бизнеса компании), можно сделать вывод о том, недоступность каких инфраструктурных сервисов во временные рамки  $t$  приводит к наступлению операционного события с заданным уровнем потерь  $C_i$  (недоступность  $j$ -го инфраструктурного сервиса приводит к реализации  $i$ -го сценария, если  $d_{ij} \geq 3$ ).

Соответственно, реализация  $i$ -го сценария с подверженностью  $C_i$  происходит в том случае, если для любого момента времени  $t$ , принадлежащего временным рамкам  $t$ , существует такой инфраструктурный сервис  $j$ , что  $\xi_{ij}^t = 1$  (т. е.  $j$ -й инфраструктурный сервис недоступен в момент  $t$ ) и  $d_{ij} \geq 3$  (его влияние на  $i$ -й сценарий представляется критичным). Оценка вероятности осуществления того или иного сценария вследствие реализации события технического риска осуществляется по результатам моделирования времени выхода из строя инфраструктурных сервисов, влияющих на конечные ИТ-услуги с учетом матрицы  $D$ . Распределение подверженности ОР вследствие технического риска — результат моделирования методом Монте-Карло большого числа возможного поведения инфраструктурных сервисов с учетом их влияния на бизнес-среду компании. Оценив распределение потерь по месяцам и считая, что они независимы (доступ к инфраструктурным сервисам в разные месяцы считается независимым), можно провести оценку подверженности операционному риску по итогам года.

**Результаты количественной оценки технического риска (сбои ИТ-услуг)**

Среднее данного смоделированного распределения будет являться оценкой ожидаемых потерь, рассматриваемых как часть общих издержек компании, а квантиль уровня 99,99 % будет являться оценкой непредвиденных потерь. Таким образом, потери вследствие ОР не могут составить более чем непредвиденные потери. Пример распределения потерь вследствие ОР представлен на рис. 2.

Из графика видно, что в большинстве случаев потерь вследствие реализации операционного события нет, а ожидаемые потери не несут никакой информации о структуре бизнес-среды компании, подверженной ОР. Однако наличие операционного события является критическим

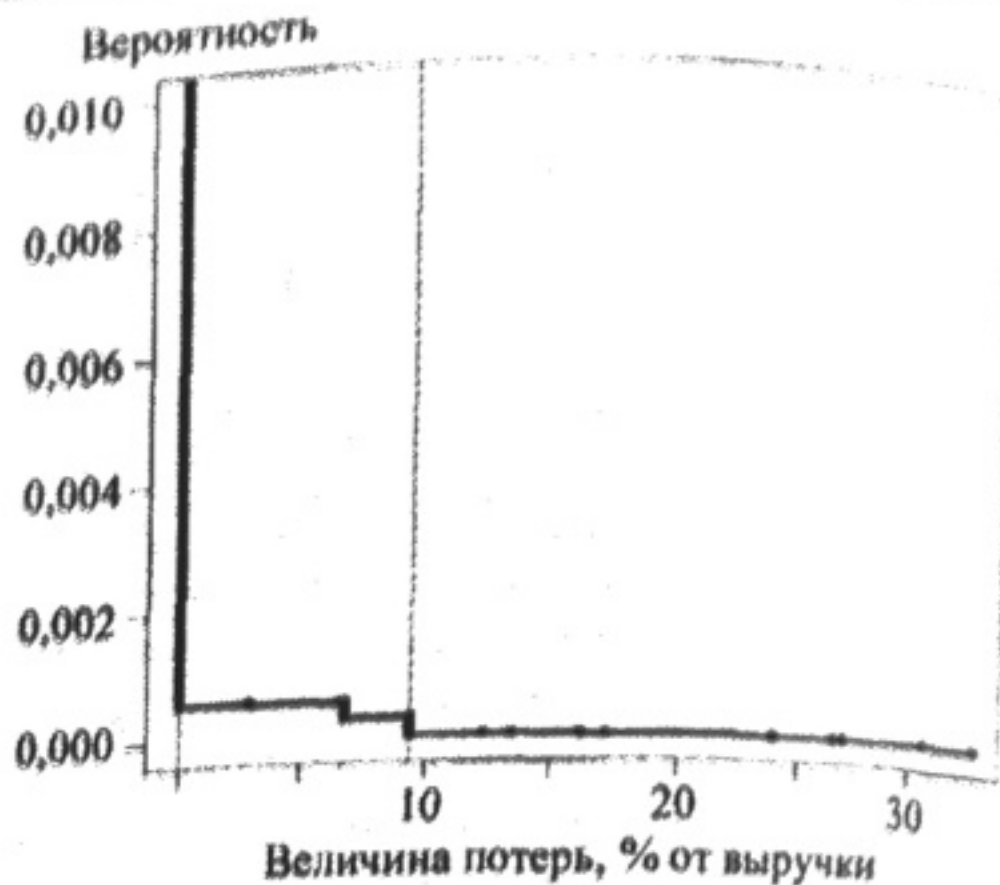


Рис. 2. График функции потерь вследствие технического риска (сбои в предоставлении ИТ-услуг) при годовом периоде моделирования

**Заключение**

Рассматриваемая в статье модель количественной оценки технического риска позволяет компании небанковского сектора решить проблему статистически некорректной среды и произвести адекватную оценку ожидаемых и непредвиденных потерь вследствие реализации технического риска. В случае, когда компания не обладает достаточными статистическими данными по отказам и времени восстановления систем, являющихся компонентами ее ИТ-архитектуры, возможно использование технических характеристик систем, представленных изготовителем (продавцом) данных систем при их установке.

Для оценки потерь моделируются состояния инфраструктурных сервисов в определенные (критичные к реализации бизнес-процессов) временные интервалы). Подверженность рассчитывается исходя из матрицы  $D$ , определяющей возможность реализации того или иного операционного сценария в зависимости от невозможности доступа к тому или иному инфраструктурному сервису. Данная матрица получается на основе матрицы непрерывности бизнес-матрицы влияния факторов риска на реализацию бизнес-процесса или бизнес-функции и матрицы зависимости пользовательских сервисов (User Services) от инфраструктурных сервисов (Support Services).

Для оценки непредвиденных потерь на базе рассматриваемой модели количественной оценки ОР в статистически некорректной среде предлагается брать доверительный интервал соответствующий классу надежности систем, принятому в компании в целях обеспечения непрерывности



делается не на проверке технических характеристик ИТ-систем и их соответствия требованиями непрерывности бизнеса компании, а на том, насколько грамотно построены бизнес-процессы компании. Таким образом, представленная модель является не только инструментом, позволяющим дать количественную оценку ОР, но и оценить, соответствует ли бизнес-архитектура компании (совокупность бизнес-процессов, ресурсов, временных рамок их реализации) ИТ-архитектуре и требованиям непрерывности бизнеса, исходя из которых устанавливаются требования к классу надежности ИТ-систем, поддерживающих данный бизнес.

*Данное исследование проводилось в рамках договора № 13.G25.31.0096 с Министерством образования и науки Российской Федерации о "Создании высокотехнологичного производства кросс-платформенных систем обработки неструктурированной*

*информации на основе свободного программного обеспечения для повышения эффективности управления инновационной деятельностью предприятия в современной России".*

**Литература**

1. Лаврушина Я. Н., Макарова А. А. Методологические подходы к анализу и оценке операционных рисков компании в статистически некорректной среде // Журнал "Бизнес информатика", 2011. № 2 (16).
2. Bonn G., Kalbrenner M., Lutz C., Stahl G. Credit risk concentrations under stress // Journal of Credit Risk, 2001. No. 2 (8). P. 115-136.
3. Frachot A., Georges P., Volcaill T. Loss distribution approach for operational risk (March 20, 2001). Available SSRN: <http://ssrn.com/abstract=1022523>. 29 p.
4. Morrison C. The fundamentals of risk management // McGraw-Hill, 2002. — 415 p.
5. Operational Risk — Supervisory Guidelines for Advanced Measurement Approaches. Basel Committee Banking Supervision, June, 2001.

**AN APPROACH TO QUALIFICATION OF OPERATING RISK IN STATISTICALLY INCORRECT MEDIA (INTERRUPT IN IT-SERVICE)**

Ya. N. Lavrushina, A. A. Makarova  
"Gazpromexport" PLC, Moscow, Russia

A. V. Kulikov  
Moscow Institute of Physics and Technology (State University), MIPT (SU),  
Moscow region, Dolgoprudny, Russia

A. I. Gromov  
BPM Chairman, National Research University, Moscow, Russia

*The article is dedicated to quantitative assessment of operational risk in statistical incorrect environment specified by insufficiency of data: IT-system failure/breakdown and time to recovery. System capabilities provided by manufacturer as well as Company's business continuity reliability specifications were used as the input data for the model. The authors used their own experience of operational risk evaluation for nonfinancial business. The given research was held in a frame of the contract № 13.G25.31.0096 with the Ministry for Education and Science of Russian Federation "Deployment of hi-tech manufacture of unstructured information processing in cross-platform system on the free software basis due to increase management efficiency of innovative activity of the enterprises in modern Russia economy".*

**Keywords:** quantitative assessment, operational risk exposure, expected and unexpected losses (operation V@R), IT-system failure/breakdown probability, mean downtime, business continuity matrix.

**Лаврушина Яна Николаевна**, старший менеджер отдела операционных и кредитных рисков.

E-mail: [ya.lavrushina@gazpromexport.com](mailto:ya.lavrushina@gazpromexport.com)

**Макарова Анастасия Александровна**, главный специалист отдела операционных и кредитных рисков.

E-mail: [a.makarova@gazpromexport.com](mailto:a.makarova@gazpromexport.com)

**Куликов Александр Владимирович**, ассистент кафедры высшей математики.

E-mail: [a.kulikov@gazpromexport.com](mailto:a.kulikov@gazpromexport.com)

**Громов Александр Игоревич**, проф., зав. кафедрой моделирования и оптимизации бизнес-процессов.

E-mail: [agromov@hse.ru](mailto:agromov@hse.ru)



# ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

в проектировании и производстве

№ 2' 2012

