

**НАУЧНАЯ МЫСЛЬ**

СЕРИЯ ОСНОВАНА В 2008 ГОДУ

**Д.В. СОКОЛОВ**

**А.В. БАРЧУКОВ**

**БАЗИСНАЯ СИСТЕМА  
РИСК-МЕНЕДЖМЕНТА  
ОРГАНИЗАЦИЙ РЕАЛЬНОГО  
СЕКТОРА ЭКОНОМИКИ**

МОНОГРАФИЯ

Электронно-  
Библиотечная  
Система  
**znanium.com**

Москва  
ИНФРА-М  
2016

УДК 65.0  
ББК 65.292  
С59

ФЗ  
№ 436-ФЗ

Издание не подлежит маркировке  
в соответствии с п. 1 ч. 2 ст. 1

С59 **Соколов Д.В., Барчуков А.В.**

Базисная система риск-менеджмента организаций реального сектора экономики: Монография. — М.: ИНФРА-М, 2016. — 125 с. — (Научная мысль).

ISBN 978-5-16-006862-6 (print)

ISBN 978-5-16-103503-0 (online)

В монографии предложен новый подход к классификации рисков организации и усовершенствована методика их выявления и оценки. Определены теоретические основы базисной системы риск-менеджмента, выявлены основные стороны и лица, принимающие участие в управлении рисками, сформулированы рекомендации, направленные на формирование подразделения по управлению рисками. Предложен новый подход к оценке эффективности базисной системы риск-менеджмента, сформулированы методические указания по проектированию внутренних нормативных документов и разработан Порядок по управлению операционными рисками для организаций реального сектора экономики. Издание предназначено для специалистов в сфере риск-менеджмента и может представлять интерес для преподавателей вузов.

УДК 65.0  
ББК 65.2902я

ISBN 978-5-16-006862-6 (print)

ISBN 978-5-16-103503-0 (online)

© Соколов Д.В., Барчуков А.В., 2013

---

Подписано в печать 20.10.2015.  
Формат 60×90/16. Печать цифровая. Бумага офсетная.  
Гарнитура *Newton*. Усл. печ. л. 7,813.  
ППТ24. Заказ № 00000  
ТК 212100-536598-250513

ООО «Научно-издательский центр ИНФРА-М»  
127282, Москва, ул. Полярная, д. 31В, стр. 1  
Тел.: (495) 280-15-96, 280-33-86. Факс: (495) 280-36-29  
E-mail: books@infra-m.ru <http://www.infra-m.ru>

Отпечатано в типографии ООО «Научно-издательский центр ИНФРА-М»  
127282, Москва, ул. Полярная, д. 31В, стр. 1  
Тел.: (495) 280-15-96, 280-33-86. Факс: (495) 280-36-29

## ОГЛАВЛЕНИЕ

Введение .....	4
<b>ГЛАВА 1</b>	
<b>ТЕОРЕТИКО-МЕТОДИЧЕСКИЕ ОСНОВЫ РИСК-МЕНЕДЖМЕНТА .....</b>	<b>7</b>
1.1. Риски: сущность и структурные компоненты .....	7
1.2. Многозадачная классификация рисков .....	12
1.3. Обоснование системного подхода к управлению рисками.....	24
Выводы к главе 1 .....	31
<b>ГЛАВА 2</b>	
<b>ФОРМИРОВАНИЕ БАЗИСНОЙ СИСТЕМЫ РИСК-МЕНЕДЖМЕНТА .....</b>	<b>32</b>
2.1. Основополагающая плоскость базисной системы риск-менеджмента .....	32
2.2. Организационная плоскость базисной системы риск-менеджмента .....	41
2.3. Процедурная плоскость базисной системы риск-менеджмента.....	52
2.4. Нормативная плоскость базисной системы риск-менеджмента.....	74
Выводы к главе 2 .....	84
<b>ГЛАВА 3</b>	
<b>ПОРЯДОК УПРАВЛЕНИЯ ОПЕРАЦИОННЫМИ РИСКАМИ</b>	
<b>В РАМКАХ БАЗИСНОЙ СИСТЕМЫ РИСК-МЕНЕДЖМЕНТА .....</b>	<b>85</b>
3.1. Основополагающие аспекты управления операционными рисками.....	85
3.2. Организационные аспекты управления операционными рисками .....	93
3.3. Процедурные аспекты управления операционными рисками.....	98
Выводы к главе 3 .....	105
Заключение .....	106
Библиографический список.....	107
ПРИЛОЖЕНИЕ 1 .....	118
ПРИЛОЖЕНИЕ 2.....	121

## Введение

Социальная и экономическая обстановка в России примерно в два раза более напряженная, чем в странах западной Европы и США, что подтверждается результатами исследований, проведенных в последние годы международными страховыми и консалтинговыми компаниями в области управления рисками, такими как March, Maplecroft, AIG и др. Как следствие, ведение хозяйственной деятельности в России сопряжено с множеством проблем, среди которых одной из наиболее сложных и актуальных является проблема управления рисками, некомпетентность в сфере которой делает отечественные организации уязвимыми перед конкурентами и глобальными угрозами, включая кризисы и катастрофы. Устойчивое и успешное развитие организаций реального сектора экономики напрямую зависит от системы управления рисками и как показал зарубежный опыт, риск-менеджмент является действенным и эффективным инструментом управления риском и экономическими отношениями, включающий стратегию и тактику управленческих действий. В России риск-менеджмент только начинает получать свое развитие, и отечественным организациям (за редким исключением) еще предстоит научиться управлять рисками, чтобы избежать возможных потерь.

Как показывает практика, необходимо управлять не только отдельными рисками, а всем их комплексом, а это можно сделать только внедрением системы риск-менеджмента, поскольку именно системное управление рисками позволяет наиболее эффективно оптимизировать комплекс рисков, принимаемых организацией на себя для достижения поставленных целей. Подавляющее большинство отечественных организаций не занимаются системным управлением рисками из-за отсутствия полноценной методологии управления ими, которая должна учитывать специфику функционирования и развития хозяйственной деятельности. Необходимо заметить, что наличие немногочисленных случаев удачного внедрения и применения крупнейшими российскими организациями систем риск-менеджмента является лишь адаптацией в российских условиях зарубежного опыта, поскольку в силу объективных причин он пока еще не доступен абсолютному большинству отечественных компаний.

Сегодня уже ни у кого не возникает сомнения, что основой составляющей любого системного знания, его «центральным ядром», выступает теория, позволяющая не только объяснить имеющиеся эмпирические факты и результаты научных исследований и экспериментов, но и предсказать их и дать прогноз на будущее. Только корректное понимание целей, критериев и путей развития организации как сложной системы сможет предохранить компанию от неоправданных рисков. Из сказанного следует, что существует объективная потребность создания базисной системы риск-менеджмента, которую организация любой отраслевой принадлежности сможет использовать как основу для создания своей частной системы управления рисками. Этим и определяется выбор авторами темы исследования и актуальность ее содержания.

Теории управления рисками были посвящены работы отечественных ученых: В. М. Ахундова, И. Т. Балабанова, Т. И. Бачкаи, В. Ф. Бадюкова, В. Е. Барбаумова, В. Н. Вяткина, В. А. Гамза, В. М. Гранатурова, М. В. Грачевой, Н. Г. Данилочкиной, О. Н. Дмитриева, Ю. Ю. Екатеринославского, А. А. Колобова, Б. А. Лагоша, А. А. Лобанова, В. В. Мыльник, И. Н. Омельченко, М. А. Рогова, А. С. Саркисян, Ю. В. Сидельникова, А. И. Соболев, Е. Д. Соложенцева, В. Л. Тамбовцева, Л. Н. Тэпман, Э. В. Уткина, С. Г. Фалько, Д. А. Фролова, Н. В. Хохлова, Е. Ю. Хрусталева, А. В. Чугунова, Э. М. Чуркина, Д. Ф. Щукина и др.

Зарубежные авторы, такие как Т. Бартон, П. Бернстайн, Р. Браймер, Ю. Бригхем, Р. Брейли, Л. Гапенски, К. Кац, С. Майерс, Ф. Найт, К. Рэдхэд, Г. Харрис, У. Шенкир, П. Уокер рассматривают главным образом прикладные стороны проблемы управления рисками, которые применительно к практике отечественного менеджмента требуют существенной доработки с учетом специфики ведения финансово-хозяйственной деятельности в России.

Исследования, затрагивающие в той или иной степени проблему системного управления рисками организаций, проводились отечественными и зарубежными исследователями: А. Г. Бадаловой, А. Бери, Г. Берк, С. М. Васиным, Ф. Джорион, А. С. Корезиным, А. А. Кудрявцевым, Е. Е. Куликовой, А. А. Лобановым, Д. Реувид, Э. Холмс, Г. В. Черновой, В. С. Шутовым.

Проведенный анализ отечественных и зарубежных источников показывает, что подавляющее большинство их посвящено рассмотрению отдельно взятых проблем риска, а ряд вопросов, связанных с построением системы управления рисками, был оставлен вне поля зрения, а именно:

1) возможно ли построить базисную систему риск-менеджмента, которая станет основой для создания частных систем управления рисками организаций реального сектора экономики?

2) какие элементы должны входить в эту базисную систему риск-менеджмента?

3) как они должны быть взаимосвязаны между собой.

Все эти вопросы обуславливают необходимость проведения соответствующего исследования, и при его проведении использовались такие методы, как анализ и синтез, сопоставление, обобщение, экспертные оценки, доказательство, графические и прочие научные методы.

В качестве источников информации использовались труды отечественных и зарубежных ученых, специализирующихся в перечисленных выше отраслях науки, обзорно-аналитические и статистические материалы, опубликованные в периодической печати, и результаты исследований, проведенных международными и отечественными профессиональными ассоциациями риск-менеджмента, а также материалы и рекомендации научно-практических конференций, семинаров, академических сессий и международных форумов.

В первой главе определены основные причины различного восприятия людьми категории «риск», уточнены определения понятий «риск организации» и «управление рисками», предложен новый подход к классификации рисков организации и усовершенствована методика их выявления и оценки, а также выявлена недостаточность теоретических и практических нормативно-методических разработок системного управления рисками отечественных организаций.

Во второй главе сформулированы и предложены теоретические основы базисной системы риск-менеджмента организации, выявлены основные стороны и лица, принимающие участие в управлении рисками деятельности организации, предложены рекомендации, направленные на формирование подразделения по управлению рисками, а также по должностным обязанностям специалистов данного подразделения, и установлен комплекс процедур базисной системы риск-менеджмента.

В третьей главе предложен новый подход к оценке эффективности функционирования базисной системы риск-менеджмента, определены основные внутренние нормативные документы, необходимые для внедрения и функционирования риск-менеджмента как элемента общей системы управления организацией, сформулированы рекомендации по разработке и утверждению внутренних нормативных документов и разработан Порядок по управлению операционными рисками для организаций реального сектора экономики.

Главная идея и теоретическая значимость монографии заключается в разработке объективного подхода, новых теоретических построений и методических рекомендаций по ведению системного управления рисками в организациях, в частности предложена концепция базисной системы риск-менеджмента, которая может быть использована как основа для дальнейших научно-теоретических и практических исследований.

Практическая ценность полученных результатов состоит в том, что выводы и обобщения, полученные в результате исследования, могут послужить практической основой при анализе и оценке рисков системного риск-менеджмента. Предложенная базисная система риск-менеджмента может быть использована организациями реального сектора экономики для создания своих частных систем управления рисками. Результаты проведенного исследования могут представлять интерес для преподавателей вузов и использоваться в учебном процессе.

Дальнейшее исследование хозяйственной деятельности в условиях риска и неопределенности, совершенствование концепции базисной системы риск-менеджмента может быть связано с углубленной разработкой теоретических и методических положений, например по управлению конкретными видами или группами рисков. Рассматриваемые положения монографического исследования актуальны при проведении научных исследований в рамках рассматриваемых проблем, постоянное совершенствование системы управления риском будет способствовать переходу теоретических положений в область практического применения и должно обеспечить стабильное функционирование российских организаций реального сектора экономики.

# Глава 1.

## ТЕОРЕТИКО-МЕТОДИЧЕСКИЕ ОСНОВЫ РИСК-МЕНЕДЖМЕНТА

### 1.1. Риски: сущность и структурные компоненты

Необходимо отметить, что на основании проанализированных источников, у исследователей нет единого мнения относительно сущности категории «риск» и, соответственно, его определения. Так отечественные и зарубежные исследователи [13; 25; 29; 30; 51; 52; 88; 94; 96 и др.] чаще всего определяют риск как:

– возможность или вероятность. Авторы определений, относимых в данную группу, отождествляют риск с возможностью или вероятностью наступления какого-либо события. Например, Г. В. Чернова под риском понимает некую возможность возникновения убытка, измеряемого в денежном выражении [96], а М. Г. Лапуста считает, что риск может нести в себе не только отрицательные последствия, но и вероятность превышения ожидаемой прибыли [52];

– угрозу. Представители этой группы придерживаются классической теории риска, они рассматривают риск только с позиции потенциальной опасности для чего-либо. Например, П. Г. Грабовой под риском подразумевает угрозу потери организацией части своих ресурсов и недополучения доходов или появления дополнительных расходов [29];

– событие. Здесь риск следует понимать как событие, которое может произойти, а может и не наступить. Например, по мнению Н. В. Хохлова, риск тождественен событию или группе случайных событий, наносящих ущерб объекту, обладающему данным риском [94];

– деятельность. Авторы определений данной группы связывают риск с опасениями, что экономическая деятельность может привести к убыткам или потерям. В частности, В. М. Гранатуров считает, что риск тождественен деятельности, связанной с преодолением неопределенности в ситуации неизбежного выбора [30].

Существование множества различных определений риска обусловлено его сложной природой. В целях формулирования уточненного определения категории «риск организации», следуя логике нашего исследования, рассмотрим наиболее существенные обстоятельства, влияющие на различное понимание сущности риска людьми.

1. Все люди по-разному воспринимают риски.

Так, например, Куликова Е. Е., раскрывая проблему различного восприятия рисков людьми, основными причинами, обуславливающими это различие, считает три обстоятельства [51]:

– информативность. Человеку свойственно переоценивать те события, о которых он чаще всего слышит, и, наоборот, события, о которых мало информации, недооцениваются;

– методы подачи информации. Если информация подается в «сухих» цифрах, опасность будет, скорее всего, недооценена. Однако если при-

водятся реальные примеры происшествий, то риск, может быть, и переоценен;

– проявление отрицательных последствий спустя время. Например, негативное воздействие ошибочных стратегических решений проявится только спустя какое-то время.

Нам представляется, что приведенный выше перечень необходимо дополнить еще двумя обстоятельствами.

Первое – склонность к риску, здесь нами понимается условная величина, которой готов пожертвовать субъект ради достижения желаемого результата в случае неудачного исхода. Каждый человек обладает индивидуальной склонностью к риску. О различии в восприятии рисков людьми писал в своих трудах Дж. М. Кейнс. Он связывал рискованные решения с психологическими характеристиками экономического агента и отмечал, что риск возникает вследствие сомнений предпринимателя насчет перспектив получения выгоды [133]. Очевидно, что склонность к риску также влияет на восприятие рисков людьми.

Второе – прикладное назначение или цель, применительно к которой субъект рассматривает риски. Например, И. Т. Балабанов [7], анализируя риск с позиции страховой деятельности, трактует его исключительно как возможную опасность потерь и не рассматривает проблему в контексте получения дополнительных выгод от принятия рисков.

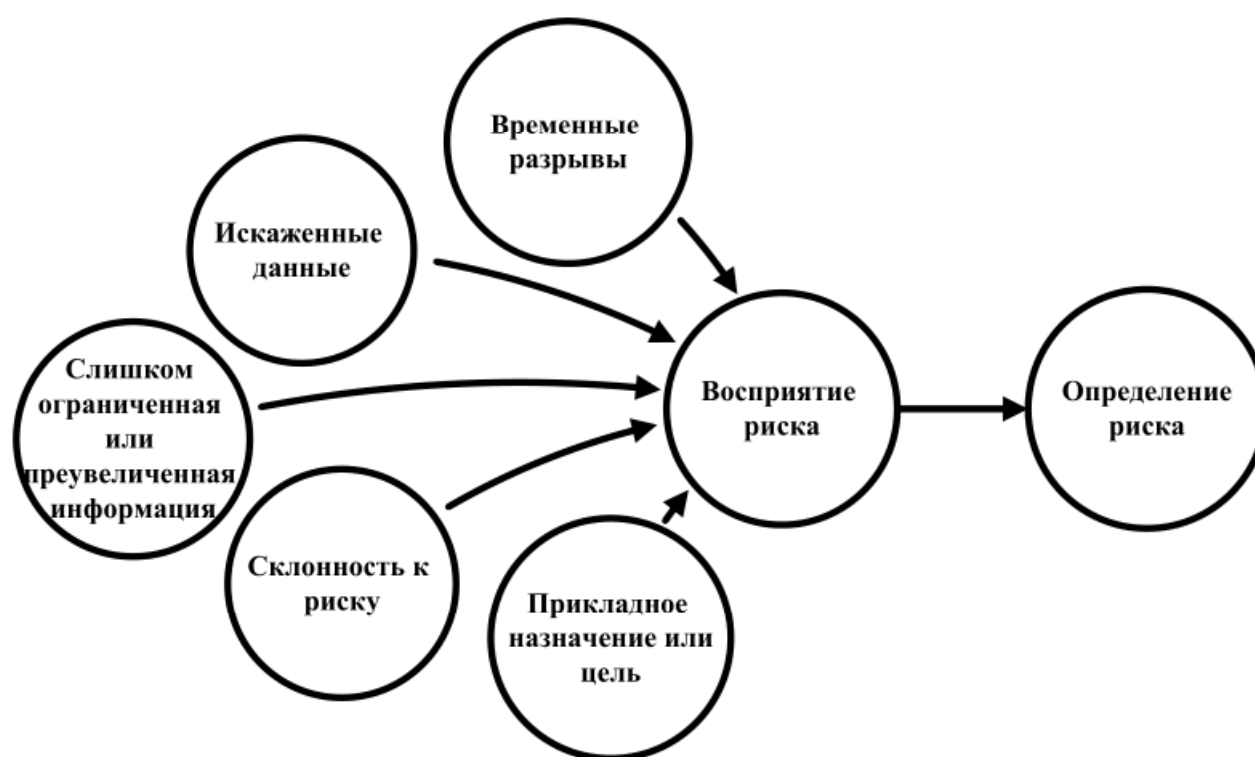


Рис. 1.1. Причины, влияющие на восприятие риска людьми

Из этого следует, что понимание сущности «риска» и возможность его определения напрямую зависят от причин, влияющих на восприятие, а именно (рис. 1.1):

– от временных разрывов;



- искаженных данных;
- слишком ограниченной или чрезмерно преувеличенной информации;
- степени склонности к риску;
- прикладного назначения или целей субъектов.

Все указанные причины ведут не только к неоднозначному восприятию рисков и формулировке различных определений, но и создают различные подходы к проблеме управления ими. Кроме того, проведенный нами анализ позволяет утверждать, что риски должны рассматриваться не только с позиции точных наук, таких как математика или статистика, но и с привлечением гуманитарных – психологии, истории, менеджмента и др.

## 2. Смещение категорий «риск» и «неопределенность».

Первым четко разграничил данные категории в своем исследовании Ф. Х. Найт, высказав мысль, что риск – это измеримая вероятность, неопределенность – неизмеримая вероятность, а прибыль, получаемая предпринимателем, является доходом за несение неопределенности [70].

В современных работах отечественных и зарубежных экономистов [19; 27; 52; 88; 94; 96; 143 и др.] неопределенность определяется как неполное знание о чем-либо, а риск – как возможность, вероятность, событие, деятельность в ситуации неопределенности. Полагаем, что категория «неопределенность» не тождественна категории «риск», поскольку может не содержать негативного элемента, а заключать в себе только благоприятные исходы, в то время как риск, по мнению всех исследователей, всегда включает в себя возможность отрицательных последствий. На этом основании можно утверждать, что употребление термина «неопределенность» вместо термина «риск» является не совсем корректным.

## 3. Неразграничение категорий «вероятность» и «возможность» при характеристике риска.

Согласно стандартам FERMA [119] и ISO/IEC Guide 73:2002 [126], риск – это комбинация вероятности события и его последствий. Приведенное определение соответствует доминирующему в настоящее время подходу к изучению рисков, основанному на математических, статистических и финансовых восприятиях и установках. Заметим, что использование в определении риска категории «вероятность» уместно, если речь идет о количественных методах измерения и оценки рисков, поскольку вероятность – это количественная мера риска в отличие от категории «возможность», которая является качественной мерой и потому ее правильнее применять при качественных методах измерения и оценке рисков.

Из этого следует, что, в целях более гибкого подхода при управлении рисками, категории «вероятность» и «возможность» следует разграничивать, помня, что их использование зависит от используемых приемов при измерении и оценке рисков.

4. Неучет всех особенностей при определении характера последствий реализации рисков.

Например, И. Т. Балабанов [7], Н. В. Хохлов [94] и Г. В. Чернова [96] делают основной акцент только на негативной стороне риска. Причина этого кроется в том, что понимание сущности риска сводится к категории исторической, т.е. риск представляет собой осознанную человеком возможную опасность. Между тем риск является, скорее, экономической категорией, чем исторической. В данном контексте он представляет собой возможность появления какого-либо события, предполагающего отрицательный, нулевой или положительный конечные результаты. Ключевым здесь является то, что риск, прежде всего, несет в себе возможность потерь, при этом давая шанс получить выгоды или доходы в результате умелого управления им. Данная точка зрения характерна для отечественных и иностранных исследователей [93; 100; 118; 135; 139; 143], и ею мы будем руководствоваться в контексте нашего исследования.

5. Формальное определение риска для анализа особенностей его распределения в пространстве и во времени.

В работах В. Ф. Бадюкова [5, 6], Е. Ф. Козловой [5], В. К. Белкина [6] посвященных раскрытию содержания риска определено, что формализованное определение риска является полезным инструментом для анализа и дает основание ввести определение риска как финансово-экономической категории. По их представлениям, риск – это субъективная оценка объективной неопределенности, описывающая множественность изменений равновесной устойчивости социально-экономической системы, выраженная в форме функции случайного события.

6. Выделение содержательных компонентов риска.

На основании проанализированных трудов (И. Т. Балабанов [7], Е. Е. Куликова [51], Э. Холмс [93], Н. В. Хохлов [94], Г. В. Чернова [96] и др.) нами выделены содержательные компоненты риска, воздействуя на которые им можно управлять. К ним относятся:

– факторы риска, т. е. обстоятельства, которые делают возникновение риска более вероятным, а его последствия более серьезными [135]. Из этого следует, что факторы влияют на риски, как до появления рисков событий, так и после их реализации. С. В. Валдайцев [17], О. В. Вишневская [22], Е. Е. Куликова [51], М. Мескон [66], Г. В. Чернова [96]. В. Е. Барбаумов [100] и другие классифицируют все факторы на внешние, воздействующие на организацию извне, и внутренние, воздействующие на организацию изнутри. По нашему мнению, факторы риска в рамках внутренней и внешней групп целесообразно подразделять на более мелкие подгруппы, которые должны быть сформированы таким образом, чтобы избежать одновременного отнесения одного и того же частного фактора в несколько подгрупп. Если этого не сделать, то факторный анализ будет недостоверным, займет много времени и средств, что снизит эффективность управления рисками;

– источники риска, создающие потенциальную угрозу и возможность, например конкуренты, персонал или поведение человека, средств-

ва управления, конкретные экономические и политические обстоятельства, технологические и технические проблемы, коммерческие и юридические отношения, общественная и профессиональная ответственность, хозяйственная деятельность организации;

– причина рискованного события, т. е. явление или совокупность явлений, обусловивших появление того или иного события, например действия человека, нехватка финансирования, отказ оборудования, нарушение договорных обязательств, введение законодательных ограничений;

– рискованное событие, появление которого обусловлено комбинацией факторов и источников риска, а также конкретных причин, например: потеря доли рынка, сбой в поставках комплектующих, переманивание сотрудников конкурентами, нарушение законодательства. Рискованное событие может быть определенным или неопределенным, единичным или многократным, предсказуемым или случайным [64]. Вероятность, связанная с рискованным событием, может быть оценена для конкретного интервала времени [28]. При прогнозировании рискованного события всегда следует задавать вопросы: где и когда оно может произойти;

– результат рискованного события, воздействующий на цели организации, ее бизнес-процессы или активы, а также на заинтересованных лиц [156]. В соответствии с ГОСТ Р 51897-2002 [28] результатом рискованного события может быть одно или более последствий, которые могут быть ранжированы от позитивных до негативных и выражены качественно или количественно. Также результатом рискованного события может стать возникновение нового риска для организации.

Нам представляется, что структурирование риска на основные содержательные компоненты позволяет наиболее полно описывать его сущность и, как следствие, эффективно управлять им. Взаимосвязь основных содержательных компонентов риска можно представить схематично на рис 1.2.

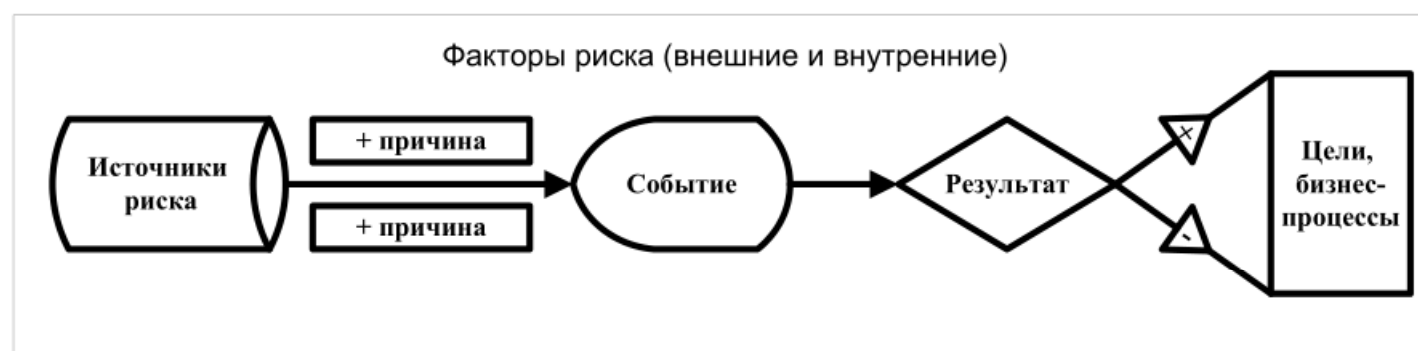


Рис. 1.2. Взаимосвязь основных содержательных компонентов риска

Таким образом, исходя из поставленных задач, в контексте нашего исследования и на основании изложенного выше, под «риском организации» необходимо понимать оцененную вероятность или возможность свершения рискованного события, возникающего в результате воздействия одной или нескольких причин на источник риска, и влияние данного рискованного события на достижение определенных целей в рамках существующих внешних и внутренних факторов.

## 1.2. Многозадачная классификация рисков

С начала активного развития риск-менеджмента в России в 90-е годы прошлого столетия большинство теоретических и практических работ отечественных авторов, например В. Ф. Бадюкова [5, 6], И. Т. Балабанова [7], И. А. Бланка [13], В. Г. Блохина [14], С. М. Бычковой [16], П. Г. Грабовый [29], С. Н. Кабушкиным [39], Н. П. Любушина [60], М. Хаертфельдер [92], Н. В. Хохлова [94] и других, было посвящено исследованию проблем управления финансовыми, инвестиционными, проектными и экологическими рисками. В последние годы более пристальное внимание исследователями [19; 35; 51; 79; 83; 135; 143 и др.] стало уделяться кадровым, операционным, юридическим видам рисков, а также тем, которые связаны с обеспечением платежеспособного спроса, поддержанием необходимого уровня оборотных средств, непрерывностью деятельности, коррупцией, рейдерством и т. д. Объяснить это можно несколькими причинами.

Первая причина – затяжной характер мирового экономического кризиса, возникшего из глобального финансового кризиса. До его наступления спрос превышал предложение, поэтому не было необходимости серьезно беспокоиться о большинстве рисков. И поскольку в условиях растущего бизнеса доходы организаций покрывали все нерациональные издержки, то их руководство не считало нужным тратить средства на управление рисками. Однако во время кризиса доходная часть существенно снизилась, что послужило причиной начала поиска путей экономии и повышения стабильности, в том числе через управление рисками.

Вторая причина – необходимость непрерывного финансирования деятельности. Каждая волна глобального финансового кризиса состоит из нескольких этапов. За кризисом краткосрочной ликвидности, заключающимся в неспособности банков исполнять свои текущие обязательства, следует кризис пассивов. Отсутствие пассивов у банковского сектора вызывает практически полное приостановление рефинансирования задолженностей реального сектора экономики. В таких условиях большинство организаций, неготовых к указанному риску, не способны исполнять свои обязательства перед контрагентами и, как следствие, – оказываются на грани дефолта или банкротства.

Третья причина – возросшая потребность снижения издержек, например, за счет сокращения численности персонала и оптимизации процессов в целях исключения возможности ошибок, дублирования функций и т. д.

Четвертая причина кроется в объективной необходимости формирования новых путей борьбы с коррупцией, это так называемый фактор риска коммерческой организации, являющийся огромным препятствием экономического роста и развития, способным поставить под угрозу любые преобразования.

Пятая причина, что подтверждается работами исследователей-экономистов [101; 108; 109; 110; 128; 129], связана с ростом общего ко-

личества глобальных рисков событий по всему миру, а также увеличением величины ущерба вследствие наступления каждого из них.

Таблица 1.1

**Возможные классификации рисков**

<i>Классификационный признак</i>	<i>Классификационные группы</i>
1	2
1. По типичности отрицательных последствий	Фундаментальные, корпоративные
2. По специфике исходов	Чистые, спекулятивные
3. По месту появления	Внутренние, внешние
4. По степени зависимости ущерба от исходного события	Первичные, вторичные
5. По характеру распределения бремени риска	Односторонние, двусторонние, многосторонние
6. По уровню проявления негативных последствий	Проекты, подразделения, фирмы, отрасли, страны, глобальный уровень
7. По степени влияния природной и социальной среды на риск	Прямые, косвенные
8. По степени учета временного фактора	Бессрочные, срочные
9. По зависимости уязвимости от времени	Статические, динамические
10. По продолжительности выявления и ликвидации отрицательных последствий	Краткосрочные, среднесрочные, долгосрочные
11. По степени распространенности	Массовые, уникальные
12. По характеру влияния на разные объекты	Общие, частные
13. По степени диверсифицируемости риска	Диверсифицируемые, недиверсифицируемые
14. По степени предсказуемости риска	Предсказуемые, непредсказуемые
15. По типу информации	Количественные, качественные
16. По степени достоверности информации	Достоверные, недостоверные
17. По частоте возникновения ущерба	Редкие, средней частоты, частые
18. По размеру (тяжести) ущерба	Малые, средние, высокие, катастрофические
19. По возможным финансовым последствиям	Прямые, косвенные
20. По характеру распределения расходов	Частные, общественные

1	2
21. По виду риска	Стратегические, финансовые, операционные, проектные и программные, экологические, репутационные, маркетинговые, юридические, технологические, технические и т. д.

Исходя из того, что актуальность частных рисков для организаций может меняться, специалистам в области управления рисками необходимо постоянно выявлять все риски, независимо от их приоритетности.

Организацию сопровождают не менее четырехсот частных рисков [139], которые с целью систематизации принято классифицировать.

В работах российских и иностранных авторов, например И. Т. Балабанова [7], С. М. Васина [19], Е. Е. Куликовой [51], Н. П. Любушина [60], Н. Н. Громова [65], Н. В. Хохлова [94], Г. В. Черновой [96], А. С. Шапкина [97], L. Condamin [135] и других, представлено многообразие вариантов классификаций рисков, что объясняется отсутствием единой точки зрения на классификационные признаки. Приведем наиболее часто встречающиеся варианты классификаций в табл. 1.1.

Несмотря на наличие большого количества классификационных признаков рисков, в отечественной литературе встречаются классификации, основанные на одном признаке, при этом выделяются различные классификационные группы, например классификации по причинам возникновения рисков (табл. 1.2).

Таблица 1.2

#### Классификации по причине возникновения рисков

<i>Автор</i>	<i>Классификационный признак</i>	<i>Классификационные группы</i>
И. Т. Балабанов, С. М. Васин, Л. Н. Тэпман, А. С. Шапкин	По основной причине возникновения рисков	Природно-естественные Экологические Транспортные Коммерческие Политические
Г. В. Чернова, А. А. Кудрявцев	По причине (природе) ущерба	Природные Политические Человеческий фактор Социальные Технические Экономическая активность
Н. В. Хохлов	По роду опасности	Техногенные Природные Смешанные

Также существует несколько схожих классификаций рисков по сферам деятельности. Например, Н. В. Хохловым была предложена классификация рисков по характеру деятельности, в которой риски группировались по следующим направлениям: предпринимательские, финансовые и коммерческие, профессиональные, инвестиционные, транспортные и промышленные [94]. Более узкая классификация по сфере деятельности, предложенная коллективом авторов в составе Н. П. Любушиной, В. Б. Лещева, В. Г. Дьякова, заключалась в выделении коммерческих, производственных, финансовых и рыночных рисков [60]. Классификация рисков по отношению к сферам человеческой деятельности, составленная М. А. Медведевой, может быть проведена по следующим направлениям: экономические, социально-бытовые, политические, технологические риски, риски в природопользовании [64].

Расхождения в вышеуказанных классификациях, свидетельствуют о том, что авторами по-разному идентифицируются и трактуются основные причины и сферы деятельности, по отношению к которым рассматриваются риски. Исходя из целей и задач настоящего исследования, приведенные классификации не могут быть использованы, поскольку они не содержат элемента универсальности.

Таблица 1.3

**Возможные классификации рисков, связанные с измерением и оценкой**

<i>Классификационный признак</i>	<i>Классификационные группы рисков</i>
По вероятности возникновения	Почти невозможные, маловероятные, вероятные, почти возможные, возможные
По величине потерь	Минимальные, низкие, средние, высокие, максимальные
По степени воздействия	Критические, существенные, умеренные, незначительные, игнорируемые
По уровню воздействия	Непереносимые, оправданные, приемлемые

Необходимо отметить, что классификации рисков, связанные с измерением и оценкой (табл. 1.3), не только не раскрывают сущности рисков, но и предоставляют неоднозначную информацию, поскольку интервалы на шкалах вероятностей и потерь рисков зависят от субъективных предпочтений оценщика, а количество классов может варьироваться в зависимости от целей и задач, поставленных перед специалистами в области управления рисками. Следовательно, эти классификации также не могут быть применены в контексте настоящего исследования.

Заметим, что проведенный обзор классификационных признаков не является полным. Можно выделить специфические риски по направлениям бизнеса, например для банков [50], факторинговых [55], лизинговых [34], фармацевтических [78], строительных [98] организаций, а также для компаний сферы услуг [52; 53; 73; 155] или связанных с реа-

лизацией проектов [85], т. е. которые отражают особенности деятельности организации.

В соответствии с задачами проводимого нами исследования существует актуальная потребность в создании классификации рисков как многозадачного инструмента, конкретизирующего объект управления и способствующего выявлению не только мест воздействия рисков на деятельность, но и путей наиболее эффективного управления рисками, а также определяющего зоны ответственности лиц, занимающихся их управлением, и имеющего механизмы адаптации к особенностям деятельности различных организаций. Многозадачная классификация рисков должна основываться на уже существующей классификации рисков по видам, как наиболее часто применяемой на практике.

И. А. Бланк [13], В. В. Бочаров [15], В. Е. Барбаумов [100], С. М. Бычкова [16], Н. Н. Громов [65], С. Н. Кабушкин [39], Н. П. Любушин [60], Э. Холмс [93], Н. В. Хохлов [94] и многие другие выделяют стратегические, проектные, программные, финансовые, экологические, технологические, операционные, кадровые, юридические, мерочные, репутационные и прочие виды рисков.

Полагаем, что одновременное применение всех указанных выше видов рисков сопряжено со следующими проблемами:

- большинство частных рисков уникальны и могут быть одновременно отнесены как к нескольким видам, так и стать абсолютно новым видом риска, что создает дополнительные трудности при идентификации и управлении ими;

- некоторые виды рисков могут быть включены в другие виды рисков, например, юридический риск, может быть в проектном или программном рисках, что может исказить его значимость.

Считаем, что с целью нивелирования данных проблем в основу многозадачной классификации должны быть положены только пять видов рисков: 1) стратегический; 2) финансовый; 3) юридический; 4) операционный; 5) репутационный, поскольку, с одной стороны, эти виды рисков можно отделить друг от друга, формализовав необходимые для этого границы, а с другой – любой частный риск организации может быть отнесен к одному из этих видов рисков. Рассмотрим их более подробно.

1. Стратегический риск – возможность возникновения у организации убытков в результате ошибок при выборе стратегии развития и ведения деятельности. Стратегический риск затрагивает всю деятельность организации [93; 112; 114], при этом он чаще всего связан:

- с изменениями предпочтений покупателей;
- политическими и регуляторными изменениями;
- маркетинговой и бренд-стратегиями;
- стратегией разработки и выпуска товара или услуги на рынок;
- моделью сделок по слиянию и поглощению;
- стратегией долгосрочного взаимодействия с контрагентами и партнерами.

Характер стратегического риска организации варьируется в зависимости от рынка, на котором он работает. Например, строительство,



фармацевтическая и финансовая отрасли строго регулируются законами, различными стандартами, требованиями, при этом фактором стратегического риска является государственное вмешательство в условия реализации каких-либо проектов.

Основная цель стратегического риск-менеджмента – увеличение рыночной стоимости организации [86; 89; 136]. Таким образом, управление стратегическим риском направлено, прежде всего, на удовлетворение интересов акционеров организации и должно выражаться в стабильном, выше среднерыночного росте акций или долей организации [130]. Ответственность за этот риск целиком и полностью возложена на руководство организации. Принимая во внимание нестабильность факторов внешней среды, стратегический риск важен как для давно работающих организаций, так и для недавно созданных, следовательно, его необходимо выделить в рамках многозадачной классификации рисков.

2. Финансовый риск – возможность возникновения убытков вследствие неблагоприятного развития и видоизменения финансовых рынков. Возникновение финансового риска обусловлено развитием и видоизменением финансовых рынков. Управление и моделирование финансовыми рисками требует использования тонких инструментов анализа, базирующихся на сложных математических моделях [8; 13].

Специалисты в области рисков, например В. Е. Барбаумов [100], И. А. Бланк [13], Л. Н. Красавина [8], Л. Н. Тэпман [88], Э. Холмс [93], выделяют следующие подгруппы финансового риска:

а) рыночный риск – это возможность потерь вследствие невыполнения контрагентом своих договорных обязательств, несоответствия характеристик экономического состояния объекта значениям, ожидаемым лицами, принимающими решения под воздействием рыночных факторов [97]. Выделяют следующие подвиды рыночного риска: процентный, валютный, фондовый; товарный, деривативов [6; 90; 97];

б) риск ликвидности включает в себя две разные составляющие [13; 93; 100]: первая – это способность организации аккумулировать средства для исполнения своих долговых обязательств перед контрагентами. Такой риск называют риском неплатежеспособности, или риском балансовой ликвидности; вторая – возможность того, что реальная цена сделки может сильно отличаться от рыночной цены, как в худшую, так и лучшую сторону. Данный риск называют еще риском рыночной ликвидности;

в) кредитный риск – это возможность потерь вследствие невыполнения контрагентом своих договорных обязательств [8; 88; 93; 100];

г) страновой риск возникает, когда деятельность организации выходит за пределы одной страны и характеризуется тесным переплетением множества финансовых, экономических, социальных и политических переменных. Выделяют шесть подвидов странового риска: риск местонахождения, или соседства с нестабильной страной, риск негативных изменений экономики страны, валютный риск, трансфертный риск, суверенный риск, политический риск [93].

Считаем, что отечественные организации недооценили финансовые риски в условиях глобального финансового кризиса, что привело к следующим негативным последствиям:

1) организациям стало трудно или же совсем невозможно привлекать заемные источники финансирования;

2) падение спроса на товары и услуги компаний, с одной стороны, и рост издержек производства, с другой, поставили многие организации в условие «ножниц цен»;

3) кредитные рейтинги организаций снизились, что обусловило существенный рост стоимости обслуживания их долга.

Как видим, финансовые риски играют очень важную роль в деятельности организаций. В связи с этим их целесообразно рассмотреть в рамках многозадачной классификации рисков.

3. Юридический риск – риск того, что в соответствии с действующими в данный момент законами партнер не обязан выполнять свои обязательства по сделке [76]. Данное определение затрагивает только одну сторону юридического риска, связанную с действиями контрагентов, следовательно, для многозадачной классификации рисков его необходимо доработать.

Базельский комитет [106] рассматривает юридические риски в составе операционных, что, по нашему мнению, усложняет анализ последних. Юридические риски, в отличие от операционных, в большей степени зависят от внешних факторов, которые часто обусловлены внутренними факторами. Также для управления юридическими рисками необходимы специалисты, разбирающиеся больше в тонкостях законодательства, в то время как для управления операционными рисками необходимы специалисты по бизнес-процессам и управлению системами и людьми. Очевидно, что юридические и операционные риски имеют разную природу возникновения, поэтому их необходимо рассматривать отдельно друг от друга.

Определение юридического риска как угрозы возникновения убытков в результате наступления обстоятельств, обусловленных причинами правового характера [69], также неприемлемо для многозадачной классификации, потому что оно не формирует четких границ между операционными и юридическими рисками. В целях разрешения данной проблемы мы должны исходить из того, что под юридическим риском следует понимать риск возникновения убытков, обусловленных неблагоприятным для организации применением норм действующего законодательства.

Возникновение юридического риска может быть вызвано:

– внутренними факторами, такими как несоответствие внутренних документов организации законодательству, а также неспособностью организации приводить свою деятельность в соответствие с изменениями законодательства;

– внешними факторами – несовершенство правовой системы, нарушения клиентами и контрагентами организации условий договоров, на-

хождение организации и ее филиалов под юрисдикцией различных государств.

4. Операционный риск – риск прямых или косвенных убытков в результате неверного построения бизнес-процессов или систем в организации, неэффективности процедур внутреннего контроля, технологических сбоев, ошибок и недостаточной квалификации персонала или внешнего воздействия [100]. Данное определение универсально и подходит для большинства видов хозяйственной деятельности. Оно отделяет операционные риски от стратегических, репутационных и финансовых, однако при этом оставляет возможность для включения в их состав юридических рисков. Поэтому для целей создания многозадачной классификации под операционным риском необходимо понимать риск прямых или косвенных потерь в результате неправильного действия или прекращения выполнения внутренних операционных процессов, неправильного поведения людей, нестабильного функционирования систем, а также неблагоприятных внешних событий, за исключением неблагоприятного для организации применения норм действующего законодательства.

Отличительная черта операционного риска в том, что он присутствует в деятельности любой организации [105; 122], поэтому его необходимо включить в состав многозадачной классификации. Согласно исследованиям аудиторской компании PricewaterhouseCoopers, сфера управления операционными рисками может быть поделена на два основных компонента, тесно связанных друг с другом:

1) операционная целостность, которая связана с адекватностью операционного контроля и корпоративного управления, в том числе организационная культура, деятельность менеджеров, ошибки, мошенничество, здоровье и безопасность, рекламации, природные бедствия и недостаточный внутренний контроль;

2) обслуживание производства, связанное с возможностью организации постоянно поддерживать его. Это включает операционные процессы, информационно-коммуникационные системы, проекты, отношения с поставщиками, персоналом и кризисы.

5. Репутационный риск представляет собой угрозу и/или возможность изменения деловой репутации организации со всеми вытекающими отсюда последствиями [104]. Данным риском необходимо управлять любой организации независимо от вида ее деятельности [93]. В настоящее время в России этим видом риска занимаются только крупные организации. В большинстве случаев управление возложено на конкретных сотрудников, ответственных за связи с общественностью, усилия которых могут быть непродуктивными, если прилагаются после свершения рискованного события, что является не управлением риском, а управлением кризисом – реактивный подход, при котором меры направлены на уменьшение ущерба [93; 96; 104].

Репутационные риски подразделяются на три группы [99]:

1) финансовые репутационные риски, которые очень тяжелы по своим последствиям. Самый опасный риск в этой группе для российского бизнеса – история создания организации;

2) корпоративные репутационные риски – находятся под управлением кадровых служб, которым легче всего бороться с риском отношений внутри организации;

3) рыночные репутационные риски – включают в себя качество продукции. Потери неизбежны, даже если потом будет доказано, что обвинения против качества работ организации были беспочвенными.

Для формирования многозадачной классификации рисков названные пять видов рисков целесообразно рассмотреть с позиции владельцев рисков, управляющих рисками, а также эндогенных и экзогенных источников рисков событий, о которых будет сказано ниже.

Под владельцем риска понимается лицо или орган управления, который в силу своих полномочий и должностных обязанностей может и должен принимать решения и нести ответственность за управление конкретным риском. По нашему мнению, в организации можно выделить следующие основные группы владельцев рисков: собственники, топ-менеджмент, внутренние аудиторы, подразделение риск-менеджмента и прочие структурные подразделения организации.

Остановимся на эндогенных источниках рисков, под которыми будем понимать бизнес-процессы, несущие в себе угрозы и положительные возможности. Классификацию бизнес-процессов представим с позиции максимальной универсальности, т.е. применимости для различных организаций. Так, например, В. М. Ковалевым [43] был рассмотрен подход, при котором бизнес-процессы подразделяют на четыре группы, каждая из которых обладает своими отличительными особенностями (рис. 1.3):



Рис. 1.3. Бизнес-процессы организации

1) основные бизнес-процессы – создают продукт или услугу, которые приносят доход, а также представляют ценность для внешнего клиента. За готовый продукт или услугу, полученные в результате осуществления данных процессов, внешний клиент готов заплатить денежные средства;

2) бизнес-процессы развития – участвуют в совершенствовании и развитии деятельности организации для получения прибыли в долгосрочной перспективе. Отличительная особенность бизнес-процессов развития в том, что они предназначены для внедрения и развития новых проектов;

3) бизнес-процессы управления – управляют конкретными объектами в деятельности организации, например денежными средствами, персоналом, клиентами, активами и т. д. Благодаря которым обеспечивается выживание, конкурентоспособность и развитие организации, а также регулируется ее текущая деятельность;

4) обеспечивающие бизнес-процессы – поддерживают инфраструктуру организации. Их клиентами являются основные бизнес-процессы, структурные подразделения и сотрудники организации. В случае наличия конкурентоспособных альтернатив на внешнем рынке исполнение данных процессов можно передать третьим лицам.

По нашему мнению, на этапе внедрения риск-менеджмент как бизнес-процесс необходимо рассматривать с позиции управления проектами, т.е. включать его в бизнес-процессы развития. После того как риск-менеджмент внедрен, его можно отнести к бизнес-процессам управления.

Рассмотренная выше классификация бизнес-процессов дает возможность выработать системный подход к управлению рисками, т.е. провести распределение рисков по квалификационным группам в зависимости от бизнес-процессов, являющихся источниками рисков. Практическую апробацию такой классификации бизнес-процессов провели ряд консалтинговых компаний. Полагаем, что ее применение не должно создать проблем при использовании в рамках многозадачной классификации рисков.

Анализ взаимосвязей основных видов рисков, их владельцев и бизнес-процессов позволил нам установить эндогенные риски организации, которые могут быть представлены в виде трехмерной матрицы классификации эндогенных рисков, представленной на рис. 1.4.

В ячейки представленной матрицы (рис. 1.4) на пересечении трех плоскостей заносятся частные эндогенные риски, относящиеся к определенному виду рисков, обусловленные соответствующим бизнес-процессом и находящиеся в непосредственном управлении владельца риска. В данные ячейки вместо наименований рисков могут быть внесены их величины, но только в случае применения организацией количественных показателей оценок рисков. В случае применения качественных оценок рисков заносить их величины не следует, поскольку это может вызвать проблемы с сопоставимостью данных показателей. В результате объединения частные эндогенные риски представляют

собой классификационные группы, свойственные соответствующим бизнес-процессам  $Bp(k)$ , видам рисков  $CR(m)$  и владельцам рисков  $RO(n)$ .

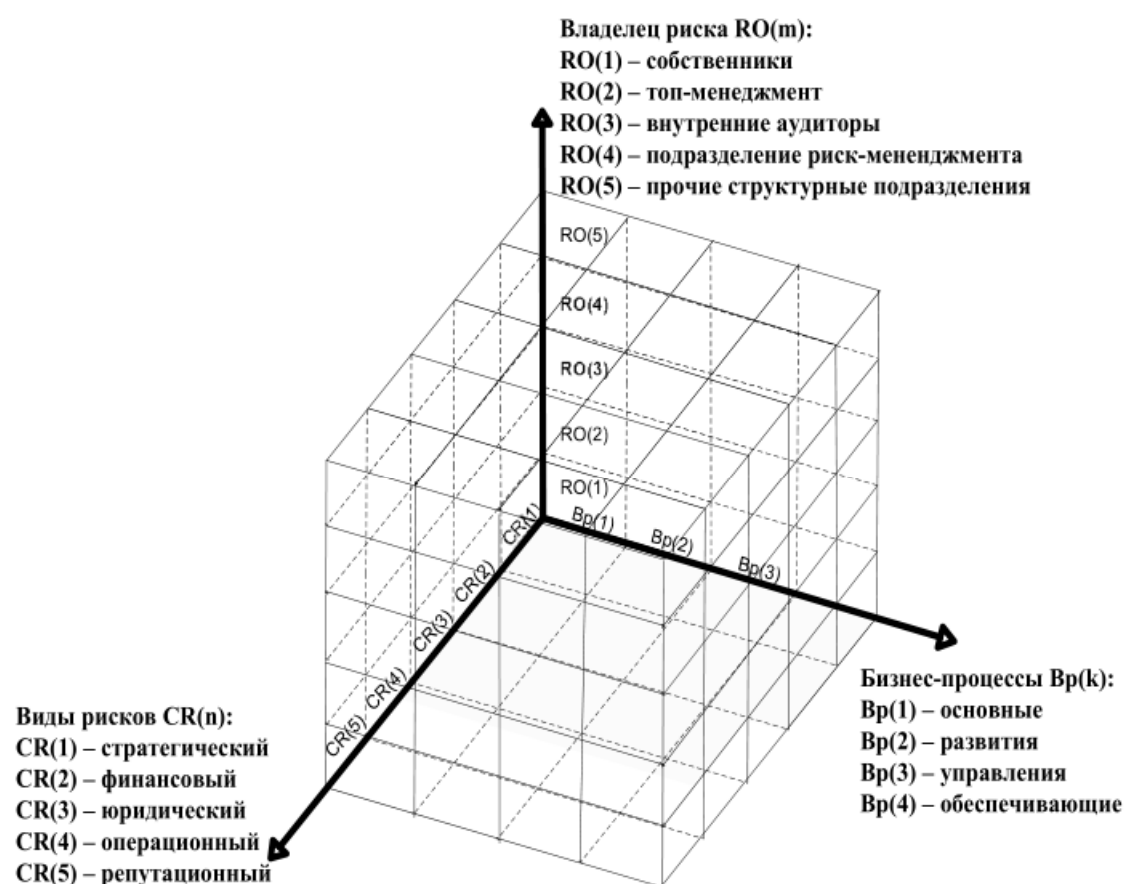


Рис. 1.4. Матрица классификации эндогенных рисков организации

В случае необходимости каждую группу бизнес-процессов и владельцев рисков можно подразделить на частные бизнес-процессы, что позволит понять специфику деятельности конкретной организации, а также даст возможность детально изучить наиболее рискованные бизнес-процессы и зоны ответственности владельцев рисков.

Экзогенные факторы, воздействующие на организацию извне, по мнению М. Мескона [66], классифицируются на следующие подгруппы: экономика, политика, рынок, технология, конкуренция, международное положение и социальное поведение. Заметим, что для целей формирования многозадачной классификации рисков подобное деление на подгруппы требует доработки. Во-первых, в рамках исследования будут рассматриваться не экзогенные факторы, а экзогенные источники рисков в соответствии с определением, представленным выше. Во-вторых, необходимо исключить подгруппы «рынок» и «международное положение». В-третьих, следует дополнить подгруппой «природно-экологические источники», включающие в себя угрозы и положительные возможности природного и экологического характера. Данные изменения позволят провести более четкие границы между классификационными группами и наилучшим образом акцентировать внимание на общих источниках для групп рисков, что положительно

скажется на управлении ими в целом. С учетом сказанного, основными экзогенными источниками рисков будут являться политические, экономические, технологические, конкурентные, социальные и природно-экологические (рис. 1.5).

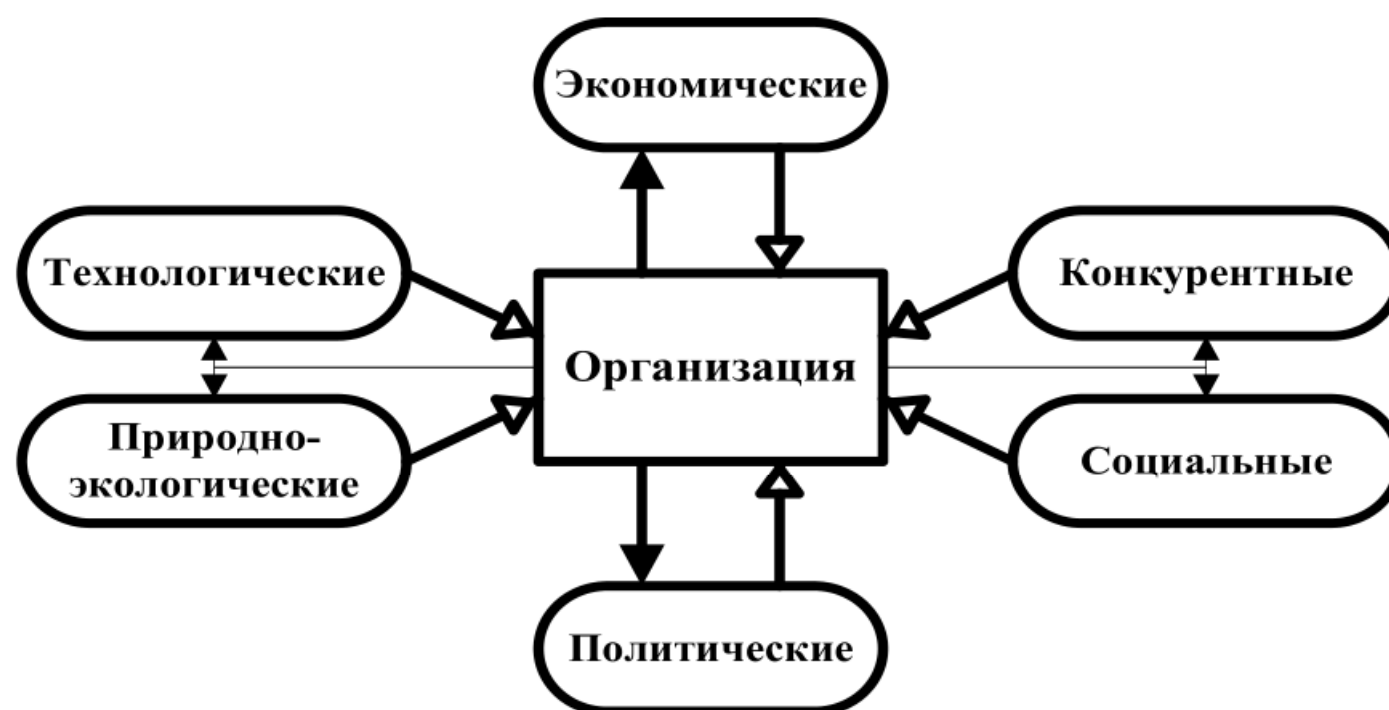


Рис. 1.5. Экзогенные источники

В результате совмещения экзогенных источников рисков с основными видами рисков и их владельцами образуется трехмерная матрица классификации экзогенных рисков организации (рис. 1.6).

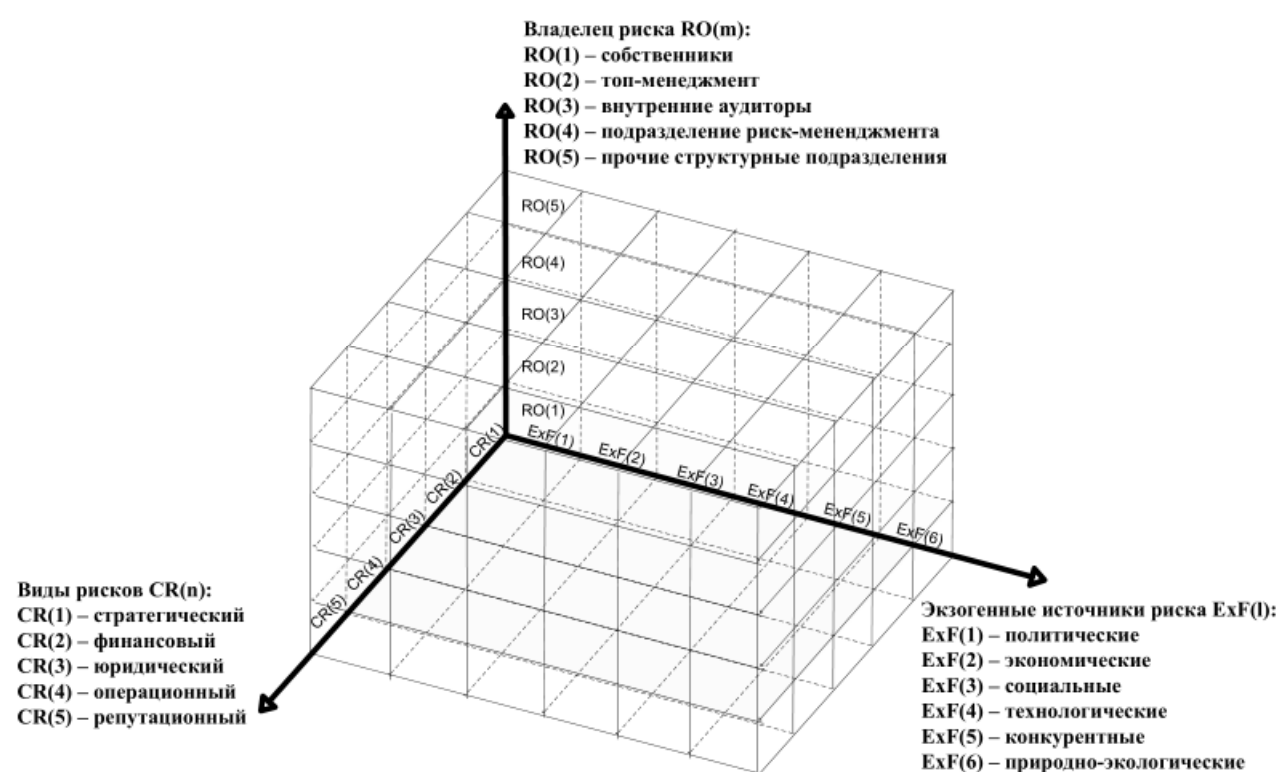


Рис. 1.6. Матрица классификации экзогенных рисков организации

На практике возможна ситуация, когда один частный риск возникает из нескольких источников одновременно. В таком случае возможны два варианта заполнения матриц (рис. 1.4 и 1.6):

1) риск относится в ячейку в соответствии с основным источником, воздействие на который позволяет наиболее эффективно управлять вероятностью и/или последствиями рискованного события;

2) риск относится в несколько ячеек, распределяясь между всеми источниками, воздействие на которые позволяет управлять вероятностью и/или последствиями изначального риска, пропорционально степени данного воздействия. При этом необходимо ввести соответствующие обозначения, позволяющие четко понимать причинно-следственные связи каждого источника с одним и тем же риском.

Организация сама определяет, какой вариант заполнения использовать. Однако необходимо понимать, что второй вариант заполнения матриц более трудоемок, чем первый. Его применение возможно только в условиях полной автоматизации процедур управления рисками и наличия обширной базы данных по взаимосвязям рисков.

Итак, рассмотрев основные виды рисков организации, а также бизнес-процессы и внешние угрозы и возможности, обуславливающие данные риски, мы получили многозадачную классификацию рисков для различных организаций, в которой предусмотрены механизмы, позволяющие дорабатывать ее в соответствии с особенностями деятельности каждой конкретной организации. При этом в многозадачной классификации должен быть сохранен единообразный подход, предложенный нами выше, благодаря которому возможно решение следующих задач:

1) конкретизировать риски как объект управления посредством определения и выделения ряда основных структурных компонентов риска, рассмотренных нами ранее, включая не только источники рисков, но и величину или вероятность последствий, а также владельцев риска;

2) определить воздействие рисков на бизнес-процессы организации, в результате чего могут быть установлены владельцы бизнес-процессов, создающих риски на всех уровнях управления;

3) определить наиболее агрессивные источники внешней среды;

4) определить общую величину рисков, связанных с деятельностью организации;

5) составить перечни рисков, находящихся под управлением владельцев рисков, а также определить величину данных рисков.

Однако следует заметить, что использование этой классификации не решает проблему управления рисками в целом, поскольку классификация является лишь одним из элементов системы риск-менеджмента организации.

### **1.3. Обоснование системного подхода к управлению рисками**

Собственники и руководители организации стараются не допускать или уменьшать возможные потери от реализации рискованных событий, а



также эффективно использовать предоставленные положительные возможности. Выполнить это возможно только путем принятия взвешенных управленческих решений, которые в контексте деятельности организации принято называть управление рисками или риск-менеджмент [36].

В International Risk Management Lexicon [125], подготовленном IFRIMA, приводится девять различных определений риск-менеджмента, а в DHS Risk Lexicon [115] и Risk Lexicon [154], подготовленных DHS Risk Steering Committee и UK MOD Defence Acquisition Community, приводится еще пять определений, что подтверждает отсутствие единой точки зрения на вопрос управления рисками у иностранных специалистов. Кроме того, у отечественных экономистов также нет единого мнения относительно определения «управление риском».

Таблица 1.4

**Сравнение определений понятия «управление риском»**

<i>Автор определения</i>	<i>Определение</i>
В. М. Гранатуров [30]	Управление риском можно охарактеризовать как совокупность методов, приемов и мероприятий, позволяющих в определенной степени прогнозировать наступление рискованных событий и предпринимать меры к исключению или снижению отрицательных последствий наступления таких событий
Л. Н. Тэпман [88]	Риск-менеджмент представляет систему оценки риска, управление риском и экономическими (точнее, финансовыми) отношениями, возникшими в процессе этого управления, и включает стратегию и тактику управленческих действий
Н. В. Хохлов [93]	Управление риском – синтетическая научная дисциплина, которая изучает влияние на различные сферы деятельности человека случайных событий, наносящих физический и материальный ущерб
Г. В. Чернова [96]	Управление рисками (риск-менеджмент) – процесс принятия и выполнения управленческих решений, которые минимизируют неблагоприятное влияние на организацию или лицо убытков, вызванных случайными событиями
И. А. Бланк [13]	Управление финансовыми рисками предприятия представляет собой систему принципов и методов разработки и реализации рискованных финансовых решений, обеспечивающих всестороннюю оценку различных видов финансовых рисков и нейтрализацию их возможных негативных финансовых последствий

На основании представленных в табл. 1.4 определений можно заключить, что ряд авторов под управлением рисками понимают,

прежде всего, процесс, направленный на минимизацию отрицательных последствий для организации. С нашей точки зрения, данное мнение частично ошибочно, поскольку цели и задачи управления рисками организации определяются лицами, непосредственно ответственными за данный процесс. В связи с этим возможна такая ситуация, при которой руководство организации занимается не снижением, а увеличением рисков ради достижения определенных целей или задач, скажем для увеличения прибыли.

Опираясь на анализ более чем тридцати пяти различных понятий «управления рисками» или «риск-менеджмента», представленных в работах отечественных и иностранных специалистов [7; 13; 14; 15; 16; 39; 58; 60; 94; 96; 100; 115; 125; 154 и др.], нами установлено, что управление рисками или риск-менеджмент должен обладать следующими ключевыми особенностями:

- осуществляться в рамках единой системы;
- использоваться при формировании и корректировке стратегии организации;
- сопровождать управленческие решения на всех уровнях менеджмента;
- способствовать достижению целей всех уровней и категорий;
- существовать в рамках внешних и внутренних ограничений, включая склонность к риску;
- давать разумную гарантию достижения каких-либо результатов;
- включать в себя процессы, осуществляемые людьми;
- не должен превалировать над общей системой менеджмента организации.

В соответствии с указанными выше особенностями считаем, что под управлением рисками или риск-менеджментом организации следует понимать экономически обоснованный процесс управления рисками, осуществляемый в рамках единой системы всеми сотрудниками, начиная от формирования стратегии до принятия решений на каждом уровне управления организации. Данный процесс должен создавать разумную гарантию достижения целей и задач организации в рамках заданного уровня склонности к риску.

Необходимо особо отметить, что большинство специалистов в области управления рисками, например С. М. Васин [19], Н. Н. Громов [65], Е. Е. Куликова [51], А. А. Лобанов [100], Э. Холмс [93], Н. В. Хохлов [94], Г. В. Чернова [96], А. С. Шапкин [97], Р. В. Кеу [132], Paul M. Collier [143] и многие другие едины во мнении, что процесс управления рисками может быть наиболее эффективен, если он осуществляется в рамках единой системы риск-менеджмента.

Кроме того, нами установлено, что среди отечественных специалистов, занимавшихся исследованием проблемы управления рисками [7; 8; 19; 13; 23; 38; 51; 60; 62; 65; 76; 94; 96; 100 и др.], комплексно системы риск-менеджмента были рассмотрены С. М. Васиным [19], В. Н. Вяткиным [23], Е. Е. Куликовой [51], Г. В. Черновой [96] и В. Е. Барбаумовым [100], при этом их работы содержат

в себе больше общих теоретических разработок, нежели практических. Полагаем, что основная причина этого в том, что в России управление рисками находится еще в стадии развития и требует квалифицированных и интенсивных наработок для практического применения. Необходимо иметь в виду и то, что, наряду с отсутствием достаточного практического опыта, имеющиеся наработки в области управления рисками и полученные результаты от их внедрения являются коммерческой тайной организаций, т. е. недоступны для общего пользования. Отсюда и информационный вакуум, создающий трудности для разработки частных систем риск-менеджмента организаций.

Разделяя точку зрения отечественных специалистов (И. Т. Балабанов [7], И. А. Бланк [13], С. М. Васин [19], Е. В. Иода [38], Е. Е. Куликова [51], Н. К. Печенин [75], Л. Н. Тэпман [88], С. С. Фролов [90]), важно указать, что структура системы риск-менеджмента (рис. 1.7) состоит:

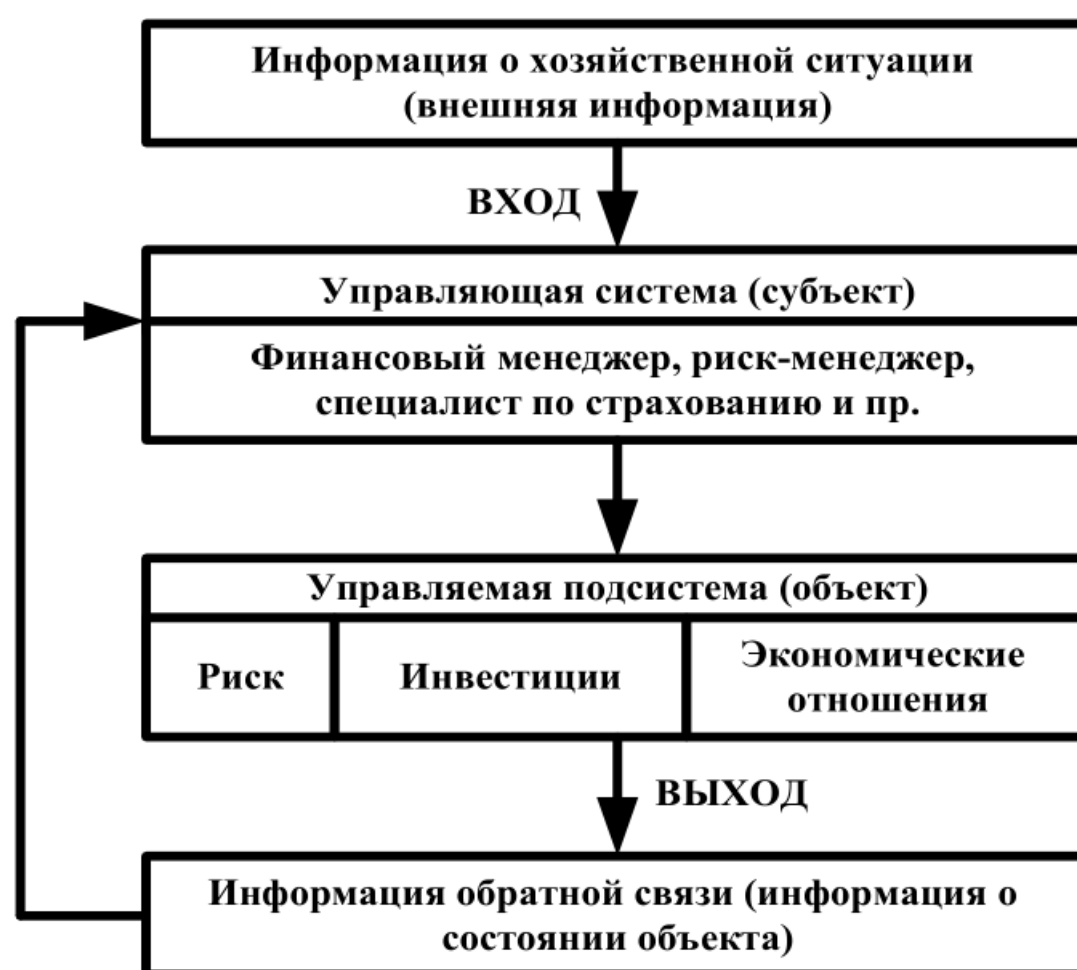


Рис. 1.7. Структурная схема системы управления рисками

1) из управляемой подсистемы – объект управления, которым могут являться вложения капитала и экономические отношения между хозяйствующими субъектами в процессе реализации риска. К таким экономическим отношениям относятся связи между организациями, организациями и органами власти, заемщиком и кредитором, конкурентами и прочими контрагентами;

2) управляющей подсистемы – субъект управления может состоять из группы руководителей (директор по управлению рисками, риск-

менеджер, финансовый менеджер, специалист по страхованию и т. д.), которая посредством различных вариантов своих действий осуществляет целенаправленное функционирование объекта управления.

Восприятие системы риск-менеджмента через призму управляющей и управляемой подсистем (рис. 1.7) позволяет установить ее участников, их функции, а также необходимость организации информационного поля между ними. Однако данная концепция, на наш взгляд, не дает четкого понимания целей, процессов и места системы риск-менеджмента в общей системе менеджмента, а также не раскрывает проблемы того, что субъект управления одновременно является и его объектом. В связи с этим можно констатировать, что восприятие системы риск-менеджмента через управляющую и управляемую подсистемы является поверхностным и для решения поставленной задачи требует определенной доработки.

Зарубежные специалисты (Э. Холмс [93], D. Aloini [103], J. David Cummins [131], L. Condamin [135], J. Reuvid [139] и Paul M. Collier [143]), в отличие от отечественных, в рамках единой системы рассматривают проблему управления рисками только с точки зрения узких прикладных специализаций. Более того, модели зарубежных специалистов, как правило, опираются на методологическую базу международных стандартов в области корпоративного управления рисками, например, BSI 31000 [113], COSO ERM [114], FERMA [119], AS/NZ [147], Turnbull report [153]. По нашему мнению, главный недостаток многих стандартов заключается в их нечеткости, т. е. для их интерпретации необходима помощь внешних консультантов или привлечение на работу специалистов, уже работавших с данными стандартами. Заметим, что таких специалистов в России очень мало, поэтому зарубежные системы риск-менеджмента в нашей стране практически не применяются, хотя опыт управления рисками доказывает, что даже эпизодическое и фрагментарное управление ими позволяет повысить эффективность функционирования организации, создавать и усиливать его конкурентные преимущества [48].

Важно подчеркнуть, что на сегодняшний день отечественная и зарубежная теория и практика управления рисками представляют собой, скорее всего, собрание разрозненных, во многом фрагментарных концепций, ориентированных на выбранные авторами отдельные аспекты, тогда как целостная научная система должна включать единые теоретические и методические подходы к построению системы риск-менеджмента организации.

В России давно существует потребность в разработке единого комплекса подходов к управлению рисками в организациях реального сектора экономики. Необходимо это, прежде всего, для активизации процесса массового внедрения управления рисками в целях поддержания конкурентоспособности отечественных предприятий в борьбе не только с зарубежными компаниями, которые уже длительное время занимаются риск-менеджментом, используя для этого весь спектр возможных средств и методов, но и с прочими глобальными внешними угрозами.

Формализованно единый комплекс подходов к управлению рисками может быть выражен в виде базисной системы риск-менеджмента (далее – БСРМ), которая сможет функционировать в отечественных организациях реального сектора экономики вне зависимости от их отраслевой принадлежности, и будет иметь механизмы адаптации к специфике деятельности в случае необходимости.

При создании БСРМ целесообразно использовать зарубежный опыт проектирования систем управления рисками, предварительно адаптировав его под российские особенности ведения финансово-хозяйственной деятельности организациями. Соответственно БСРМ должна отвечать двум требованиям, сформулированным нами, которые не противоречат международным стандартам в сфере риск-менеджмента (BSI 31000 [113], COSO ERM [114], FERMA [119], AS/NZ [147], Turnbull report [153]), а именно:

1) быть инвариантной, т. е. строиться на методической основе, единой для различных организаций;

2) быть адаптивной, т. е. настраиваемой под специфику каждой конкретной организации.

На основании анализа трудов С. М. Васина [19], Н. Н. Громова [65], Е. Е. Куликовой [51], А. А. Лобанова [100], Э. Холмса [93], Н. В. Хохлова [94], Г. В. Черновой [96], А. С. Шапкина [97], D. Aloini [103], L. Condamin [135] и других нами установлено, что данные авторы чаще всего рассматривают основополагающие, процедурные, нормативные и организационные аспекты системы управления рисками и значительно меньше уделяют внимания другим составляющим систему элементам. А это значит, что для эффективного функционирования БСРМ ее основу должны составлять указанные выше четыре ключевых аспекта (табл. 1.5).

Таблица 1.5

**Ключевые аспекты управления рисками организации**

<i>Ключевые аспекты</i>	<i>Назначение</i>
Основополагающие	Рисками управляют для достижения целей всех уровней управления. Внедрение системы риск-менеджмента осуществляется в силу добровольной осознанной необходимости
Процедурные	Процедуры осуществляются на постоянной основе с применением максимальной автоматизации
Нормативные	Единая база хранения четких формализованных правил управления рисками
Организационные	Управление рисками осуществляет каждый сотрудник или подразделение в рамках их компетенций

Базисная система риск-менеджмента в соответствии с содержанием ключевых аспектов управления рисками организации и предъявляемыми требованиями будет представлять собой совокупность обязательных основополагающих, организационных, процедурных и нормативных аспектов управления рисками, которые, в случае необходимости, могут быть адаптированы под особенности организаций реального сектора экономики для целей построения частных систем риск-менеджмента.

В нашем исследовании ключевые аспекты управления рисками организации (табл. 1.5) представляют собой основные системообразующие направления, которые должны быть проработаны с целью проектирования БСРМ. Такое восприятие позволяет представить БСРМ в виде тетраэдра (рис. 1.8), каждая из четырех сторон которого является группой ключевых аспектов управления рисками:

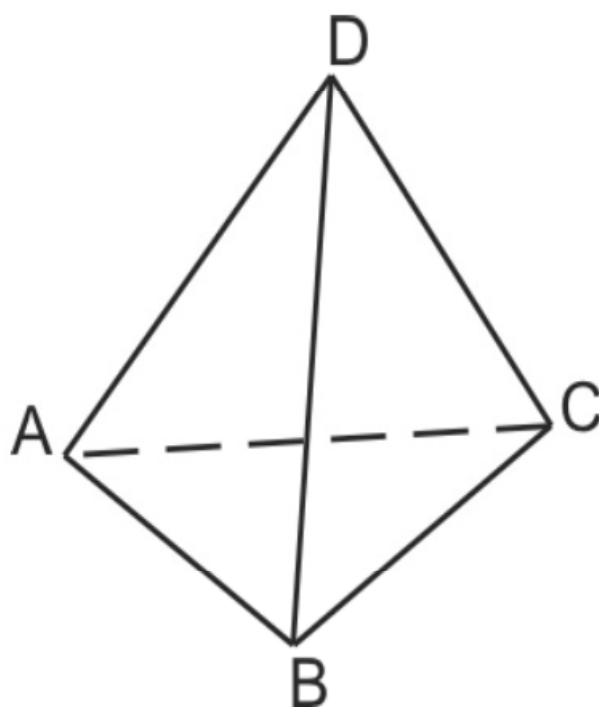


Рис. 1.8. Структура базисной системы риск-менеджмента

1) сторона ABC – основополагающая плоскость, содержащая в себе основные свойства, цели и задачи, принципы и правила, проектируемой системы риск-менеджмента;

2) сторона ABD – организационная плоскость, рассматривающая внутренних заинтересованных лиц и культуру риска;

3) сторона ACD – процедурная плоскость, раскрывающая основные процедуры, осуществляемые в рамках БСРМ;

4) сторона BCD – нормативная плоскость, охватывающая основные распорядительные документы организации.

Соприкосновение всех четырех сторон тетраэдра между собой позволяет говорить о тесной зависимости и взаимосвязи друг с другом, которые требуют детального рассмотрения при создании БСРМ. И только благодаря этому базисная система риск-менеджмента станет каркасом, на основе которого организация сможет сформировать свою частную систему управления рисками, дополняя уже существующие в

рамках БСРМ механизмы функционирования своими собственными элементами и необходимыми компонентами.

## **Выводы к главе 1**

1. Определены основные причины различного восприятия людьми категории «риск». Установлены основные структурные компоненты риска, посредством воздействия на которые им можно управлять. Уточнены определения понятий «риск организации» (оцененная вероятность или возможность свершения рискованного события, возникающего в результате воздействия одной или нескольких причин на источник риска, и влияние свершившегося рискованного события на достижение определенных целей в рамках существующих внешних и внутренних факторов) и «управление рисками» (экономически обоснованный процесс управления рисками, осуществляемый в рамках единой системы всеми сотрудниками, начиная от формирования стратегии и заканчивая принятием решений на каждом уровне управления организации, который должен создавать разумную гарантию достижения целей и задач организации в рамках заданного уровня склонности к риску).

2. Предложен новый подход к классификации рисков организации и усовершенствована методика их выявления и оценки. Для этого разграничены определения категорий «операционный риск» (риск прямых или косвенных потерь в результате неправильного действия или прекращения выполнения внутренних операционных процессов, неправильного поведения людей, нестабильного функционирования систем, а также неблагоприятных внешних событий, за исключением неблагоприятного применения норм действующего законодательства) и «юридический риск» (риск возникновения убытков, обусловленных неблагоприятным применением норм действующего законодательства). Предложенный подход к классификации обладает необходимым свойством универсальности, дающим возможность решать комплекс взаимосвязанных задач, включая управление рисковой нагрузкой любых частных или сгруппированных направлений деятельности организации, с учетом основных источников угроз. Предложенная методика выявления и оценки рисков определяет, какими методами наиболее эффективно выявлять и измерять риски конкретных классификационных групп.

3. Выявлена недостаточность теоретических и практических нормативно-методических разработок системного управления рисками отечественных организаций, что выражается в отсутствии национального стандарта в сфере управления рисками. В сложившейся ситуации необходима разработка концептуальных основ и целостной методики управления рисками в форме базисной системы риск-менеджмента, представляющей собой совокупность обязательных основополагающих, организационных, процедурных и нормативных аспектов управления рисками, которые, в случае необходимости, могут быть адаптированы к особенностям организаций реального сектора экономики при проектировании частных систем риск-менеджмента.

## Глава 2. ФОРМИРОВАНИЕ БАЗИСНОЙ СИСТЕМЫ РИСК-МЕНЕДЖМЕНТА

### 2.1. Основополагающая плоскость базисной системы риск-менеджмента

В предыдущей главе исследования нами было установлено, что для формирования БСРМ необходимо проработать четыре системообразующих направления, в которых ключевыми являются основополагающие аспекты, объединенные вместе в формате основополагающей плоскости (рис. 2.1), или основания тетраэдра (рис. 1.8).



Рис. 2.1. Основополагающая плоскость БСРМ

С. М. Васин [19] и Г. В. Чернова [96] отмечают, что система риск-менеджмента должна обладать следующими свойствами.

1. Для достижения системного характера управления рисками:

– целостностью, т. е. быть ориентированной на оценку всего комплекса рисков организации и преодоление негативных последствий реализации их рискованных событий, с учетом связей между указанными рисками;

– комплексностью, т. е. необходимо учитывать сложность объекта управления и рассматривать не только связи между частными рисками, возможными рискованными событиями и их последствиями, но и влияние приемов по управлению на частные риски, а также их совокупности (не исключая ситуации, при которых борьба с одними рисками порождает другие);

– способностью системы к интеграции новых элементов, что важно для адаптации указанной системы к изменяющимся условиям, связанным с появлением новых рисков (включая риски, создаваемые самой системой риск-менеджмента).



2. Система риск-менеджмента обладает сложной структурой, что наделяет ее следующими свойствами:

- многофункциональностью и универсальностью, т. е. способностью бороться с рисками разной природы и различными последствиями их реализации;

- модульностью, т. е. возможностью не только использовать различные комбинации процедур риск-менеджмента в зависимости от сложившихся обстоятельств, но и настраивать указанную систему на решение индивидуальных задач, стоящих перед владельцами рисков;

- многоуровневостью, т. е. способностью обеспечить подходящую иерархическую структуру принятия решений, которая позволит адекватно распределить полномочия и ответственность.

Полагаем, что, помимо вышеуказанных свойств, система должна обладать:

- иерархичностью, т. е., когда компонент системы может рассматриваться как система (подсистема) более широкой глобальной системы;

- эмерджентностью, т. е. появлением качественно новых свойств у системы управления рисками, отсутствующих у ее элементов. Система управления рисками позволяет решать задачи более высокого уровня, чем управление одним или несколькими рисками.

3. Для достижения высокой результативности система управления рисками должна обладать:

- гибкостью и адаптивностью, т. е. способностью к приспособлению к стремительно изменяющимся условиям, высокой скоростью реагирования, а также способностью быстро справляться с неблагоприятными ситуациями;

- адекватностью, т. е. соответствием процедур риск-менеджмента определенной ситуации, что выражается в возможности своевременно выделять необходимые для достижения поставленных целей и задач ресурсы;

- эффективностью, т. е. способностью справляться с негативными последствиями рискованных событий, используя для этого минимальный объем необходимых ресурсов и средств. Затраты на мероприятия по управлению риском должны быть меньше фактического изменения величины риска в результате осуществления этих мероприятий.

В дополнение к сказанному важно отметить, что система риск-менеджмента, несмотря на такие свойства, как гибкость и адаптивность, всегда будет стремиться сохранить свою структуру в соответствии с законом самосохранения. А это означает, что для поддержания гибкости и адаптивности БСРМ организации необходимо прилагать дополнительные усилия. Более того, наряду с указанными выше свойствами, система должна еще обладать следующим:

- синергичностью, т. е. однонаправленностью действий в системе, которая приводит к усилению конечного результата. Управление группой рисков создает более сильный эффект, чем такое же управление рисками, но по отдельности;

– неаддитивностью, т. е. принципиальной несводимостью свойств системы к сумме свойств составляющих ее компонентов, возникающая при наличии корреляции между различными рисками.

Следует отметить, что перечисленные свойства системы управления рисками являются общими и не меняются при любых особенностях финансово-хозяйственной деятельности организации, а следовательно, они могут применяться в БСРМ, поскольку соответствуют требованию инвариантности отдельных ее элементов.

По мнению Н. П. Веретенникова и Р. Г. Леонтьева [20], под целью понимается желаемый результат целесообразной деятельности по развитию системы, достигаемый в пределах некоторого интервала времени. Данное определение применимо и для целей БСРМ, которыми в большинстве случаев являются причины ее внедрения. Анализ опыта и практики российских и иностранных организаций позволил установить следующие наиболее характерные для этой системы причины внедрения [24; 121]:

- дополнительная эмиссия ценных бумаг и/или требования регулирующих органов;
- увеличение стоимости организации;
- обеспечение достижения стратегических целей;
- получение рейтинга специальных рейтинговых агентств;
- достижение финансовых целей.

Полагаем, что наличие указанных причин можно объяснить следующими предпосылками:

а) законодательство различных стран, включая Россию, предполагает проведение процедуры формального доказательства наличия системы риск-менеджмента и внутреннего контроля у эмитентов, проходящих процедуру листинга;

б) собственники желают повысить свое благосостояние за счет роста стоимости организации, который возможен только в случае достижения стратегических и финансовых показателей;

в) потенциальные инвесторы и кредиторы желают знать о существующих рисках в деятельности организации и мерах, предпринимаемых для управления ими.

Из этого следует, что причины внедрения системы риск-менеджмента можно условно разделить на обусловленные внешними требованиями и осуществляемые по инициативе организации. Есть все основания полагать, что причины, обусловленные внешними требованиями, могут помешать процессу формирования системы риск-менеджмента. Нередки случаи, когда организации, внедряющие системы риск-менеджмента по причине внешних требований (например, проведение дополнительной эмиссии ценных бумаг или получение рейтинга) после успешной демонстрации заинтересованным лицам формальных признаков управления рисками прекращают развивать системы риск-менеджмента (например, сдают в архив разработанные для демонстрации внешним пользователям информации документы и останавливают деятельность соответствующих органов управления рисками). Ос-

нованная причина этого заключается в том, что сам по себе процесс внедрения системы риск-менеджмента в организации является весьма растянутым во времени и может занимать от двух до пяти лет, а следовательно, и положительный эффект от внедрения системы риск-менеджмента не сможет проявиться раньше этого периода. Очевидно, что внешние обстоятельства не могут являться достаточно убедительным основанием для внедрения системы риск-менеджмента, если инициатива не принадлежит собственникам или топ-менеджменту организации.

Считаем, что внедрение и дальнейшее развитие БСРМ и систем риск-менеджмента должно происходить исключительно по инициативе собственников или топ-менеджмента организации, исходя из осознанной необходимости управления рисками, но с учетом внешних требований, так как их соблюдение позволяет организации расширять его возможности в решении многих вопросов, например таких, как привлечение капитала. Собственники и топ-менеджмент должны понимать, что управление рисками становится все более необходимым инструментом для эффективной деятельности организации. По мнению известных специалистов, В. Н. Вяткина [23], Э. Холмса [93], J. Reuvid [139], в ближайшие десятилетия системы управления рисками будут занимать такое же важное место в общей системе менеджмента организации, как например, системы управления качеством или инновациями.

Выше было определено, что в соответствии с назначением основополагающих аспектов (см. табл. 1.5) БСРМ затрагивает все уровни деятельности организации, а это значит, что ее цель не может ограничиваться только причинами внедрения. По нашему мнению, целью БСРМ является создание разумной гарантии достижения целей и задач на всех уровнях управления организацией, а также обоснованности тех или иных решений в вопросах, касающихся управления рисками. Важно понимать, что гарантия, предоставляемая БСРМ, является разумной, а не абсолютной, поскольку неопределенность и риск обусловлены неясными перспективами, которые никто не может предсказать с абсолютной уверенностью. Также ограничение по гарантии вызвано тем, что человеческое суждение в принятии решения может быть необъективным. Более того, просчеты могут быть вызваны сговором двух человек или более. Все эти причины позволяют рассматривать результаты работы БСРМ лишь как разумную гарантию достижения поставленных целей.

Принимая во внимание определение Р. Г. Леонтьева [57], который под задачей понимает желаемый результат деятельности, достигаемый за определенный период времени и характеризующийся комплексом количественных параметров этого результата, нами были сформулированы следующие основные задачи, решение которых направлено на достижение основной цели БСРМ:

- 1) снижение уровня неопределенности персонала. Сотрудники, имеющие четкое представление о своих рисках, связанных со здоровьем, профессиональным и карьерным ростом, благосостоянием и т. д.,

проявляют инициативу в вопросах управления рисками организации гораздо чаще, чем те, которые имеют нечеткое представление о своих персональных рисках;

2) снижение уровня неопределенности деятельности организации. Планирование и анализ сценариев развития организации позволяет не только установить возможные риски до момента их фактического свершения, но и проработать необходимые мероприятия по борьбе с негативными последствиями;

3) выявление и использование возможностей улучшения. Анализ рисков должен быть направлен на оценку возможностей наступления благоприятных событий. Выявить пути для развития благоприятных событий организации возможно лишь при условии, если сотрудники осознают риски и знают, как управлять ими;

4) разумное расходование средств. Расходы на управление рисками не должны превышать экономический эффект от проведения необходимых для этого мероприятий;

5) повышение качества информации для принятия решений. Процесс управления рисками будет эффективным лишь тогда, если он осуществляется на достоверной и доступной информации;

6) улучшение взаимоотношений с заинтересованными лицами. Необходимо постоянное проведение консультаций с заинтересованными лицами в целях определения их ожиданий и мнений по вопросам, касающимся управления рисками организации;

7) рост деловой репутации. Инвесторы, кредиторы, страховые компании, поставщики и прочие контрагенты охотнее сотрудничают с теми организациями, которые организовали у себя систему управления рисками;

8) долгосрочная поддержка руководством организации. Качественное управление рисками может быть обеспечено только при поддержке со стороны руководства, а также благодаря созданию контролируемых условий функционирования организации.

В соответствии с требованиями адаптивности БСРМ количественные данные или параметры результата достижения основных задач и цели БСРМ, а также цели и задачи более низких уровней организация определяет и утверждает самостоятельно, с учетом особенностей ее хозяйственной деятельности.

Организация может достигнуть цели и выполнить задачи БСРМ только в том случае, если будет придерживаться определенных принципов и правил. В контексте этого уместно рассмотреть принципы управления рисками, которые предлагают авторы Е. Е. Куликова [51], Э. Холмс [93], Г. В. Чернова [96], занимавшиеся исследованием данной проблемы.

1. Система управления риском должна являться частью процедур общего менеджмента организации, т. е. соответствовать стратегии развития организации и институциональным особенностям ее функционирования.

Чтобы не понимать упрощенно суть этого принципа, мы разделили его на две составляющие:

– систему управления рисками, которая соответствует стратегии развития организации. Собственники должны определить миссию организации и утвердить стратегические цели, достижение которых позволит выполнить данную миссию. В свою очередь руководители организации вырабатывают стратегию для достижения поставленных стратегических целей. Нет необходимости доказывать, что стратегия определяет все стороны функционирования организации, формируя тем самым цели более низкого уровня и методы их достижения в долгосрочной перспективе. Следовательно, стратегия задает особенности системы риск-менеджмента организации.

С другой стороны, система риск-менеджмента оказывает непосредственное влияние на выбор одной стратегии из нескольких альтернативных. Например, руководство организации может утвердить стратегическую цель – увеличить долю рынка, это может быть достигнуто при условии приобретения конкурента или предложения ему покинуть рынок за существенное вознаграждение. Система риск-менеджмента позволяет определить, какие угрозы и возможности несет в себе каждый из вариантов;

– система управления рисками должна соответствовать институциональным особенностям функционирования организации, т. е. она является важной составной частью общей системы управления.

Важно отметить, что единство системы риск-менеджмента и общей системы управления организации должно быть не только на уровне согласования целей, но и в увязке соответствующих процедур принятия решений. Это предполагает учет не только специфики организационной структуры организации, но и характера особенностей принятия решений руководителями при управлении рисками.

2. Особенности системы управления рисками должны проявляться в ее целях и задачах, а это обуславливает специализированный характер принятия решений в рамках системы риск-менеджмента, направленный на создание разумной гарантии достижения целей и задач организации.

3. При управлении риском следует учитывать внешние и внутренние ограничения, т. е. соответствующие специальные мероприятия должны согласовываться с возможностями и условиями функционирования организации.

Поясним это положение тем, что на систему управления риском оказывают влияние ограничения внешней среды (внешние ограничения, на которые организация не может влиять непосредственно) и внутренние особенности (внутренние ограничения, связанные с особенностями функционирования и принятием управленческих решений организации). Без учета указанных ограничений система управления рисками не будет эффективна. Примеры возможных ограничений представим в табличной форме (табл. 2.1).

Полагаем, что к третьему принципу, включающему внутренние ограничения, необходимо добавить еще одно – склонность к риску, о которой было сказано нами ранее в главе 1.

Таблица 2.1

**Внутренние и внешние ограничения БСРМ**

<i>Внешние ограничения</i>	<i>Внутренние ограничения</i>
Законодательные, представленные законодательными и нормативными актами, отражающими методы макро- и микроэкономического регулирования.	Институциональные, т. е. ограничения, обусловленные спецификой функционирования различных подразделений фирмы и механизмами их взаимодействия, целями, а также традициями данной фирмы в целом и стилем управления
Кризисные, которые особо значимо в период финансового кризиса, когда многие компании не способны исполнять свои обязательства перед контрагентами, чем побуждают последних в свою очередь не исполнять свои обязательства перед третьими лицами	Бюджетные, т. е. наличие лимита затрат на мероприятия по управлению рисками. Риск-менеджмент является частью общей системы управления в организации, и потому он должен вписываться в единую бюджетную модель
Конъюнктурные, связанные с особенностями макроэкономических процессов и спецификой развития тех или иных отраслей и рынков	Информационные, определяемые влиянием дефицита информации (недостаточный объем или состав данных) на принятие решений

4. Риск-менеджмент должен осуществляться в рамках единой политики по управлению рисками, что предполагает комплексное и одновременное управление всеми рисками.

В соответствии с принципом риски должны исследоваться с двух сторон:

1) проводится анализ рисков по отдельности, что создаст условия для понимания особенностей не только реализации любого рискового события, но и специфики его неблагоприятных последствий;

2) изучаются все риски в целом, что позволяет установить их общее влияние на организацию.

Изучение рисков организации означает, что анализ рисков ситуации предусматривает не только исследование источников рисков, но также и степень взаимосвязи между рисками. В большинстве случаев информации о такой взаимосвязи недостаточно, т. е. известно, что риски коррелированы, но не ясно, каким образом или какова природа взаимосвязи.

5. Процесс управления рисками должен носить динамический характер, поскольку связан с непрерывным принятием решений.

Риск-менеджмент необходимо рассматривать не как одномоментную процедуру, пусть даже детально проработанную и обоснованную.

В быстро изменяющихся условиях функционирования бизнеса такая статическая точка зрения мешает достижению результатов. Поэтому управление рисками организации представляет собой непрерывный процесс, охватывающий всю организацию.

Исходя из сказанного, мы попытались сформулировать основные принципы применения БСРМ:

- соответствовать стратегии развития организации;
- сопровождать решения на всех уровнях управления организацией;
- способствовать достижению целей всех уровней и категорий;
- существовать в рамках внешних и внутренних ограничений, включая склонность к риску;
- создавать разумную гарантию достижения каких-либо результатов;
- заниматься управлением всей совокупностью рисков, причем без исключений, сопутствующих деятельности организации;
- не превалировать над общей системой менеджмента организации.

Важно заметить, что организация вправе расширить перечень принципов БСРМ по своему усмотрению, но при этом новые принципы не должны противоречить или дублировать уже существующие.

Далее, на основе принципов БСРМ были сформулированы правила управления рисками. Для этого мы обратились к научным работам отечественных ученых (И. Т. Балабанов [7], И. А. Бланк [13], С. М. Васин [19], Е. В. Иода [38], Е. Е. Куликова [51], Л. Н. Тэпман [88], Э. А. Уткин [90]), рассматривавших правила и имеющих единую точку зрения на них, а именно:

1. Нельзя рисковать средствами большими, чем собственный капитал. Прежде чем принять решение об операции, несущей в себе риски, необходимо определить возможную максимальную величину убытка от указанных рисков, сопоставить ее с объемом инвестируемых средств, сравнить с имеющимся собственным капиталом и сделать вывод о вероятности банкротства в случае реализации рисков.

На наш взгляд, данное правило применимо только в отношении рисков, величину которых можно измерить и сопоставить с размером собственного капитала, например финансовые риски. Однако заметим, что организации приходится сталкиваться с такими рисками, как, например, деловая репутация или юридическими, для которых объективно точных методик вычисления вероятностей и последствий не существует [135]. Из этого следует, что организация не способна полностью применить данное правило. Приведем еще один аргумент исходя из того, что если собственники вправе индивидуально определять объем рисков, которые их организация может принять на себя, то возможна такая ситуация, когда объем рисков целенаправленно превысит объем собственного капитала организации, а это значит, что возможности управления рисками существенно ограничиваются, следовательно, в рамках БСРМ это правило не следует применять.

2. Необходимо думать о последствиях риска. Зная максимально возможную величину убытка, необходимо определить: к чему он (убыток) может привести, какова вероятность риска и только потом принять ре-

шение или об отказе от риска, или о принятии его на свою ответственность, или же о передаче его на ответственность другому лицу.

Мы придерживаемся такой точки зрения, что точно вычислить возможную максимальную величину убытка от реализации каждого из рисков организации проблематично, так как статистические данные по критическим величинам убытков в большинстве случаев отсутствуют, и специалистам для их вычисления приходится руководствоваться исключительно аналитическими методами. Процесс осложняется еще и тем, что последствия рискового события могут носить нематериальный характер, что затрудняет определение их величин. Из этого следует, что принимая на вооружение это правило, необходимо помнить, что максимально возможная величина убытка имеет, скорее всего, наименьшую вероятность реализации [135].

И, наконец, последний аргумент не в пользу этого правила: оно не дает четкого понимания относительно способов управления рисками, поскольку предлагает применять большую часть из них одновременно. С учетом этого в рамках БСРМ оно не применимо.

3. Нельзя рисковать многим ради малого. Действие данного правила можно проследить на примере страхования. В этом случае необходимо выбрать приемлемое для организации соотношение между страховой премией и возможными убытками.

Глобальный финансовый кризис показал, к каким катастрофичным последствиям может привести нарушение этого правила. Страховые компании, в частности American International Group Inc и банковский сектор, например Lehman Brothers Holdings Inc, Bank of America, Goldman Sachs и др. уже пострадали гораздо серьезнее других вследствие неправильной оценки принимаемых на себя рисков. Отсюда следует, что данное правило должно применяться в рамках БСРМ.

4. Положительное решение принимается лишь при отсутствии сомнения.

Как показывает практика, любой вопрос, связанный с областью управления рисками, всегда имеет несколько решений, оценка которых производится специалистами с разным уровнем склонности к риску [139]. Следовательно, уполномоченным лицам очень часто приходится принимать тяжелые, небесспорные решения в условиях цейтнота, которые могут вызывать сомнения. Следовательно, данное правило не может применяться в рамках БСРМ.

5. При наличии сомнений принимается отрицательное решение.

Данное правило полностью ограничивает возможность инновационной деятельности организации, всегда сопряженной с большей долей неясностей и сомнений. Между тем отсутствие инноваций в организации вызывает массу новых рисков, грозящих для нее полным прекращением деятельности [93]. В связи с этим данное правило не должно применяться в рамках БСРМ.

6. Всегда существует вероятность нескольких решений проблемы.

Для того чтобы определить альтернативные решения, необходимо рассмотреть проблему, используя мозговой штурм, структурное мыш-



ление, а также другие подходы. Определив альтернативные варианты, нужно свести к минимуму их количество, объединив похожие и исключив неправдоподобные или нереальные [93]. И только тогда данное правило будет соответствовать условиям БСРМ.

Как видим, в рамках БСРМ могут применяться только два правила из шести. Полагаем, что их необходимо дополнить еще тремя:

1) управлять необходимо в первую очередь теми рисками, которые действительно угрожают достижению поставленных целей, т.е. рисками, несущими наибольшие угрозы целям и задачам организации;

2) регулярно отслеживать риски, обладающие средним уровнем угрозы, с тем чтобы их повышение со среднего до высокого уровня было своевременно выявлено и приняты оперативные меры;

3) периодически осуществлять контроль рисков с низким уровнем угрозы, но не в ущерб рискам со средним и крупным уровнем. В ходе управления рисками необходимо исходить из того, что последствия реализации рискованных событий могут быть меньше затрат на их управление.

Кроме того, организация вправе, с учетом требования адаптивности БСРМ, дополнительно устанавливать свои собственные правила, которые должны не противоречить названным выше.

## **2.2. Организационная плоскость базисной системы риск-менеджмента**

Второй системообразующей плоскостью БСРМ организации, по нашему мнению, является организационная плоскость, которая должна включать два основных элемента (рис. 2.2).



Рис. 2.2. Организационная плоскость БСРМ

Первый – внутренние заинтересованные лица организации.

Всех заинтересованных лиц организации можно разделить на внешних и внутренних. По нашему мнению, внешние заинтересованные ли-

ца, как указано в работах М. Мескон [66] и С. А. Айвазяна [84], только создают риски организации, а непосредственным их управлением занимаются внутренние заинтересованные лица, ответственные в организации за внедрение и функционирование системы риск-менеджмента, следовательно, только они должны быть рассмотрены в рамках БСРМ. На основании проведенного анализа стандартов [106; 113; 114; 119; 147] в области управления рисками нами были определены обязанности и полномочия внутренних заинтересованных лиц организации, перечень которых приведен ниже:

1. Собственники или их представители несут ответственность за выработку общей стратегии развития, а также создание соответствующего климата и формирование основных принципов эффективного управления рисками [41, 139]. Они обязаны как минимум [119]:

- определить и оценить риски организации, которые могут привести к негативным последствиям;
- определить вероятность наступления негативных последствий;
- выработать политику организации в отношении рисков, несущих наибольший уровень угроз;
- дать оценку общей эффективности политики по управлению рисками;
- оценить эффективность стратегии в области управления рисками;
- обозначить свою позицию в отношении управленческих решений по вопросам риск-менеджмента, влияющим на долгосрочное развитие организации.

Полагаем, что указанное выше может быть осуществлено при наличии сформированного Комитета по управлению рисками, либо Комитета по аудиту при наблюдательном совете или совете директоров, рассматривающих комплексные вопросы управления рисками и дающих оценку эффективности функционирования БСРМ.

2. Топ-менеджеры должны обеспечить долгосрочную поддержку внедрения и обеспечения работоспособности БСРМ [111]. В главе 1 нами было обозначено, что для организации период внедрения БСРМ может занимать от двух до пяти лет. За это время поддержка может ослабнуть, что приведет либо к замораживанию, либо к крайне неэффективному внедрению БСРМ. Именно поэтому на самой начальной стадии топ-менеджмент должен определить и сформировать механизмы, гарантирующие долгосрочную поддержку этого процесса. При этом на самих топ-менеджерах должна лежать персональная ответственность за управление рисками в соответствии с блоком работ, которым они руководят.

Один из вариантов распределения полномочий по управлению рисками был предложен экспертами из Institute of Internal Auditors Research Foundations (права и обязанности генерального директора, финансового директора и прочих руководителей по вопросам управления рисками) [150]. Считаем, что он, может быть, применим и в рамках БСРМ. Однако при этом необходимо иметь в виду, что перечень топ-менеджеров может не соответствовать структуре организации, внедряющей БСРМ, поэтому лицу, ответственному за внедрение БСРМ,

необходимо предусмотреть, чтобы все риски были закреплены за определенными топ-менеджерами. Если в организации нет топ-менеджеров, на которых возлагаются права и обязанности по вопросам управления рисками, то необходимо провести следующие мероприятия:

- присвоить дополнительные обязанности конкретным руководителям;

- расширить полномочия конкретных руководителей.

В противном случае отсутствие персональной ответственности топ-менеджеров за управление рисками приведет к тому, что мероприятия по управлению ими периодически будут срываться, вследствие этого эффективность БСРМ будет снижена.

3. Структурное подразделение отвечает [119]:

- за каждодневную реализацию мероприятий по управлению рисками;

- повышение уровня осознания важности вопросов риск-менеджмента внутри организации;

- регулярный мониторинг состояния дел, обмен мнениями и опытом с другими структурными подразделениями организации;

- соответствующий процесс идентификации и анализ риска на самой ранней стадии реализации нового проекта и доведение сведений до соответствующих руководителей организации.

Эффективность любого структурного подразделения в вопросах управления рисками зависит от его непосредственного руководителя, поскольку именно на нем лежит ответственность за то, сколько времени и сил сотрудники будут уделять вопросам управления рисками и какими правами он будет наделен в части риск-менеджмента своего подразделения. Разделяя точку зрения Institute of Internal Auditors Research Foundations [150], считаем, что руководитель подразделения обязан:

- отвечать за управление операционными и функциональными рисками в пределах своей группы, отдела или управления;

- обсуждать любой риск, который влияет на деятельность всей организации, с руководителем подразделения по управлению рисками или иным лицом, ответственным за комплексное развитие БСРМ.

Руководителю структурного подразделения должны быть делегированы полномочия по управлению рисками, ограниченные его профессиональной компетенцией. Оценка профессиональной компетенции должна производиться руководителем подразделения по управлению рисками, а также топ-менеджером, которому подчиняется данное структурное подразделение.

4. Подразделение внутреннего аудита также участвует в постановке системы управления рисками путем проведения изменения системы внутренних проверок [72]. Роль внутреннего аудита может различаться в зависимости от специфики организации [119]. На подразделение внутреннего аудита должны быть возложены следующие задачи:

- концентрация работы на существенных рисках, определенных руководством компании, и аудит процессов управления рисками в организации;

- предоставление гарантий в управлении рисками;
- активная поддержка и участие в процессе управления рисками;
- содействие в идентификации и оценке рисков и в обучении персонала, задействованного в процессах управления рисками и внутреннего контроля;
- координация представления отчетов совету директоров, аудиторскому комитету и т. д.

У некоторых отечественных организаций подразделения по внутреннему аудиту и управлению рисками подчиняются одному лицу, входящему в состав высшего исполнительного органа организации [82]. Это делается с целью создания сильного подразделения, способного сопротивляться возможному противодействию топ-менеджеров в вопросах постановки внутреннего аудита и управления рисками. По нашему мнению, подразделения по внутреннему аудиту и управлению рисками должны быть в функциональном подчинении у совета директоров, а в административном – у генерального директора, что позволит объективно оценивать деятельность организации и предоставит неограниченный доступ к топ-менеджменту и совету директоров.

Организация, наряду с упомянутыми выше комитетами по рискам и аудиту, в рамках БСРМ может сформировать дополнительные коллегиальные органы управления. Такое решение будет обосновано тем, что, поскольку процесс риск-менеджмента затрагивает все направления деятельности организации, может возникнуть ситуация, при которой неизбежно возникает потребность в детальном управлении конкретным набором рисков. Из этого следует, что руководство должно осуществляться коллегиальным органом, сформированным на основе вертикальной субординации [93]. На практике встречаются комитеты по вопросам репутационных и стратегических рисков, по управлению операционными и юридическими рисками, по вопросам финансовых рисков и т. д.

##### 5. Подразделение по управлению рисками.

Нам представляется, что это ведущее подразделение в процессе риск-менеджмента организации.

Перечислим основные функции, которые должны выполняться специалистами подразделения по управлению рисками [119]:

- разрабатывать общие программы управления рисками и положения стратегии организации в области управления рисками;
- реализовывать программы управления рисками на стратегическом и операционном уровне;
- повышать осведомленность всех сотрудников организации в вопросах, касающихся риск-менеджмента;
- разрабатывать систему управления рисками и ее организационную структуру;
- проводить мониторинг эффективности реализации программы управления рисками; координировать взаимодействие различных структурных подразделений организации по вопросам управления рисками;

– разрабатывать программы снижения внеплановых потерь и мероприятия, направленные на поддержание непрерывности бизнес-процессов;

– готовить отчеты для внутренних пользователей и внешних контрагентов.

В зависимости от размера организации функции специалиста по управлению рисками могут быть возложены на одного сотрудника или на отдельно выделенное структурное подразделение.

Зарубежная практика управления рисками показывает, что эффективно управлять рисками средней или крупной организации могут два или три профессиональных сотрудника. Для малого бизнеса достаточно одного человека [144].

В России управлением рисками в крупных организациях занимаются целые отделы, состоящие из пяти и более человек [19; 51]. Такая ситуация, на наш взгляд, обусловлена тем, что российский рынок труда испытывает острый дефицит профессиональных специалистов по управлению рисками, программы подготовки которых не представлены на современном рынке образовательных услуг. В связи с этим организации вынуждены нанимать большое количество или недостаточно профессиональных в управлении рисками сотрудников, или вообще не имеющих опыта работы в этой сфере, или, как правило, имеющих опыт работы в какой-то смежной сфере, чтобы обеспечить своевременность решения задач в области управления рисками [19].

На основании анализа отечественной [13; 19; 51; 94; 96] и зарубежной [135; 139; 143] литературы, в которой рассматриваются вопросы формирования подразделения по управлению рисками, нами была определена возможная структура подразделения для отечественных организаций (рис. 2.3).



Рис. 2.3. Возможная структура подразделения по управлению рисками

Рассмотрим функциональные обязанности специалистов.

1. Руководитель подразделения по управлению рисками должен, прежде всего, обладать хорошими навыками менеджера, чтобы эффективно организовывать и контролировать деятельность своего подразделения. При этом он должен обеспечить гарантию того, что управление

рисками в организации осуществляется в полном соответствии с внутренними и внешними требованиями.

Экспертами Institute of Internal Auditors Research Foundations [150] и Federation of European Risk Management Associations [120] сформулированы основные обязанности руководителя подразделения по управлению рисками, которые были доработаны нами с учетом особенностей БСРМ:

- участвует в определении основных рисков БСРМ и разработке стратегии управления ими;

- контролирует эффективность функционирования БСРМ и инициирует, по мере необходимости, процесс ее модернизации.

2. Специалист по организации процедур измерения рисков должен иметь не только хорошие навыки математического моделирования, но и хорошие знания теории вероятности и математической статистики [135]. Вся информация, поступающая в подразделение по управлению рисками от прочих структурных подразделений, должна сначала попадать к данному сотруднику для того, что бы на ее основе и при помощи специалиста подразделения, подающего информацию, он создал модель измерения риска. В его обязанности также входит тесное сотрудничество как со специалистом по IT-поддержке БСРМ с целью автоматизации процесса сбора и измерения рисков организации, так и со специалистом по управлению рисками с целью построения математических моделей эффекта от мероприятий по управлению рисками.

3. Специалист по IT-поддержке БСРМ отвечает за работу IT-системы, поддерживающей процедуры управления рисками, а также за управление рисками информационной безопасности. Он должен обладать соответствующими знаниями в области программирования и проектирования баз данных. Если это возможно, с точки зрения выделения достаточных временных ресурсов, то данному специалисту желательно вменить обязанности по администрированию процедур управления рисками. Для этого он должен иметь хорошие организационные и координационные навыки, так как будет отвечать за правильное оформление реестра и карты рисков, своевременный сбор Комитета по рискам и рассылку приглашений на него, отслеживание формирования планов мероприятий по управлению рисками в едином формате и тому подобные административные функции [152].

4. Специалист по организации процедур управления рисками. Основной его обязанностью является разработка и мониторинг мероприятий по управлению рисками организации. Необходимо, чтобы данный сотрудник являлся экспертом в основной деятельности, которую осуществляет организация. Такой сотрудник может быть привлечен либо из соответствующих подразделений организации, либо из других организаций отрасли, но в любом случае должен обладать необходимыми знаниями деятельности.

По мере роста масштабов деятельности организации число сотрудников подразделения по управлению рисками может изменяться [103], например, дополнительно могут быть сформированы должности со-

трудников по производственным рискам, рискам охраны труда и промышленной безопасности, экологическим рискам, страхованию и т. д.

Независимо от численного состава подразделения по управлению рисками, каждый специалист в его составе должен:

1) периодически проходить внешнее обучение для постоянного повышения квалификации, включая обмен опытом со специалистами по управлению рисками других организаций;

2) обладать хорошими коммуникационными и организационными навыками, поскольку он является внутренним консультантом организации по рискам и должен уметь убедительно взаимодействовать на уровне горизонтальных связей с другими сотрудниками организации в рамках общего процесса управления рисками, особенно в процессах выявления рисков, планирования мероприятий по управлению ими и контроля выполнения этих мероприятий.

В заключение необходимо отметить, что в число внутренних заинтересованных лиц входят все владельцы рисков организации, о которых речь шла ранее в главе 1. В то же время необходимо отметить, что данные категории не тождественны, поскольку не все внутренние заинтересованные лица являются владельцами рисков.

Культура риска, второй элемент организационной плоскости БСРМ, характеризуется степенью осознания менеджментом потребности в необходимости эффективного управления рисками организации [93]. Сюда входит выяснение того, насколько организация склонна или толерантна к риску в своей повседневной деятельности и в рамках принятия управленческих решений. В организации с развитой культурой риска имеются стандарты идентификации, оценки и управления рисками [142; 144].

Полагаем, что под культурой риска следует понимать комплекс установок восприятия, оценок и действий, характеризующих отношение сотрудников организации к рискам в каждодневной деятельности.

Анализ практики управления рисками показывает, что во многих организациях культура риска воспринимается на неприятии рисков. С сотрудниками, которые потерпели неудачу в управлении рисками, обходятся чрезмерно строго. У организации нет культуры риска, если [51; 93; 139; 143]:

– сотрудники, которые приняли рискованные решения, были уволены вследствие этого;

– руководство организации категорически не приемлет принятие рискованных решений сотрудниками на местах;

– организация следует правилу сохранения одной и той же позиции в отношении рисков независимо от обстоятельств.

Из вышесказанного следует, что без культуры риска БСРМ будет менее эффективна. В то же время, если культура риска создана неверно, то любые из процессов управления рисками будут восприниматься сотрудниками как инструмент для прикрытия своих действий. Поэтому у руководства организации должно быть четкое понимание: что такое культура риска, и какой она должна быть в рамках БСРМ.

Для многих организаций культура риска, как считает Е. Е. Куликова, напрямую зависит от их уровня склонности к риску. В организациях, у которых связь между культурой риска и уровнем склонности к нему отсутствует, существует высокая вероятность возникновения ситуации, когда не только разные структурные подразделения имеют разную культуру риска, но и в рамках одного структурного подразделения риск воспринимается сотрудниками по-разному [51].

Мы согласны с указанным выше мнением и считаем, что восприятие рисков каждым сотрудником и соответственно культура риска всей организации зависят от комбинации четырех переменных.

1. На восприятие рисков, прежде всего, влияет то, в какой стране ведет деятельность организация. Особенности национальной культуры влияют на множество факторов, включая отношение к работе, взаимоотношения с деловыми партнерами, восприятие правовых норм и т. д. [145]. Культуры разных стран отличаются между собой, что делает ведение бизнеса в каждой из них уникальным. Гирт Хофстид предлагает рассматривать модель национальной культуры любой страны с помощью четырех переменных: дистанция силы; индивидуализм – коллективизм; маскулинизация – феминизация; избегание неопределенности [123]. Мы рассмотрели Россию с позиции данной модели и установили следующие специфические особенности:

- подчиненные согласны с неодинаковым распределением власти, что проявляется в их неготовности задавать вопросы своему руководству и оспаривать их решения в силу страха перед возможными репрессиями со стороны начальства;

- общество является коллективистским, в результате этого решения очень часто принимаются медленно. Доказательством коллективизма является доминирование семейных отношений, когда на важные должности назначаются, прежде всего, родственники или лояльные по отношению к семье люди независимо от уровня их профессиональной компетенции;

- российское общество является «мужским», что проявляется в приоритете работы перед домом и семьей, а также существенным превалянием числа мужчин-руководителей над женщинами;

- люди, проживающие в России, привыкли к чувству постоянной неопределенности и неуверенности в завтрашнем дне, в результате степень их желания избегать неопределенности и риски является низкой.

Из этого можно сделать заключение: культура России создает предпосылки к негативному восприятию риска, что подтверждается наличием коллективистского общества и открытым согласием с неравным распределением власти, но в то же время жизнь в условиях постоянной неопределенности и стремление выжить в таких условиях заставляет жителей России постоянно рисковать, в результате создается позитивное отношение к риску.

По нашему мнению, в современных условиях единственным способом сократить влияние названных аспектов культуры страны на



организацию является привлечение на работу иностранных специалистов. Правомерность этого подтверждается тем, что собственники крупных отечественных организаций приглашают иностранных специалистов на руководящие должности.

2. Культура организации определяет нормы поведения, существующие в ней, при этом каждая организация имеет свою собственную культуру, даже если она не занималась ее созданием [51; 93].

Менеджмент организации должен инициировать диагностику корпоративной культуры с целью выявления ее особенностей. Зная, к какому типу культуры относится организация, руководитель будет иметь достаточные основания для принятия решения о мерах по сглаживанию негативных сторон имеющейся культуры либо будет прилагать усилия с целью изменения типа культуры организации, а это – довольно сложная задача.

Существуют различные подходы при анализе уровня культуры организации [91], результаты которых можно переложить на особенности восприятия рисков. Так, например, в своей работе Роб Гоффи и Гаретт Джонс [148] предлагают модель культуры организации, основанную на двух понятиях – общительности и солидарности. Авторы считают, что проявлением степени общительности можно измерить уровень дружелюбия между сотрудниками организации. Солидарность заключается в готовности людей выполнять общие задания, в понимании общих целей организации, от которых выигрывают все сотрудники независимо от того, насколько они друг другу нравятся. В результате пересечения общительности и солидарности образуется матрица культуры организации (рис. 2.4).

<b>Общительность</b>	Сильно	Коммунальная	Сетевая
	Слабо	Коммерческая	Фрагментарная
		Сильно	Слабо
		<b>Солидарность</b>	

Рис. 2.4. Модель культуры организации

Как видим (рис. 2.4), коммунальная культура поощряет риск. Сотрудники в рамках данной культуры охотно идут на риск и стремятся учиться на своих ошибках. Они рассматривают риски в качестве неотъемлемой части своей деятельности. В рамках данной культуры

избегание риска воспринимается значительно большей проблемой, чем его принятие. В этом заключается основная проблема организаций с этой культурой – чрезмерное принятие рисков, которые в последующем невозможно контролировать.

Сетевая культура способствует принятию только хорошо просчитанных рисков. Анализ рисков требует больших временных и денежных затрат, что негативно сказывается на скорости принятия решений. Однако возможны исключения, возникающие вследствие воздействия внешних сил, например, начало мирового кризиса или возможность враждебного поглощения другой компанией. В данном случае организация вынуждена оперативно реагировать на возникшие угрозы.

Коммерческая культура создает жесткую атмосферу в коллективе, стимулирующую людей как можно лучше выполнять свои обязанности. Сотрудников, которые пошли на риск и потерпели неудачу, увольняют. В результате этого большинство сотрудников предпочитают не идти на риск, угрожающий их карьере, а в случае возникновения каких-либо проблем – скрывать их или пытаться исправить собственными силами.

Фрагментарная культура не приемлет риски в принципе. Сотрудники организации с данной культурой могут иметь две модели поведения. Первая модель предполагает избегание рискованных решений. Вторая – принятие решений, о которых не знает руководство. Поэтому необходимо постоянно контролировать индивидуальную склонность сотрудников к принятию рисков.

По нашему мнению, коммунальная культура является наиболее привлекательной для построения культуры риска организации. Топ-менеджмент должен стремиться к формированию данной модели культуры в организации, не забывая о том, что БСРМ приемлема и для оставшихся трех моделей, но при которых ее эффективность ниже. В частности, наименее эффективной будет фрагментарная культура, которая мешает формированию рациональной культуры риска, направленной на сбалансированное сочетание рисков и доходности, а также на делегирование полномочий по управлению рисками на местах. Именно поэтому она редко встречается в коммерческих структурах и свойственна структурам государственной власти.

3. Культура подразделения определяется его функциональными задачами, уровнем подготовки кадров и т. д. И как результат – образуются различные субкультуры в рамках одной организации. Основная задача организации заключается в создании сильной организационной культуры, которая способствует эффективному взаимодействию отдельных подразделений при управлении рисками [139].

В основе культуры подразделения, способного адекватно воспринимать риски в рамках всей организации, лежит правильный подбор сотрудников и их лидера. Только в культуре, построенной на принципах трансформационного лидерства, когда руководитель является истинным лидером, можно получить ту среду, где к ошибкам

относятся толерантно. В рамках такой культуры имеется понимание того, что каждый может извлечь пользу из своих ошибочных действий, которые часто могут быть результатом попыток выполнить свою работу более инновационным способом. В рамках такой культуры риски инноваций будут желаемыми [74].

4. Культура группы является последней переменной, лежащей в основе восприятия рисков сотрудниками.

В группах создается своя собственная микрокультура, которая формируется лидером команды, людьми, входящими в ее состав, характером их деятельности [142]. Групповая культура, подобно культуре в целом, позволяет участникам команды почувствовать свою приобщенность к общим задачам, одновременно отделяя их от прочих членов организации [93].

Основной задачей при формировании команды группы, так же как и при формировании команды подразделения, является подбор людей, обладающих необходимым набором навыков и установок. Ведь если участники команды подобраны неудачно, то риск провала проекта или программы может быть очень высоким. Правильный подбор участников команды позволит снизить риск провала, но не уберет его полностью [17].

Из вышеописанного видно, что культура риска, с одной стороны, напрямую зависит от людей, принимающих участие в процессе управления рисками, а с другой – она сама задает для данных людей модели поведения и восприятия угроз и возможностей. Из этого следует, что культура риска и люди являются одновременно объектами и субъектами управления по отношению друг к другу.

Согласно данным PricewaterhouseCoopers, существуют четыре основных характеристики сильной культуры риска [144]:

1) лидерство и стратегия. Это показатель этики и ценностей организации, а также того, как она доводит до заинтересованных лиц свою миссию и цели;

2) ответственность и система поощрения. Характеристика, показывающая способность организации устанавливать индивидуальную ответственность и систему измерения поощрения за выполнение поставленных задач;

3) люди и коммуникации. Показатель отображает, как организация делится знаниями и информацией и развивает компетентность своих сотрудников;

4) риск-менеджмент и инфраструктура. Характеристика показывает, насколько хорошо организация оценивает риски, а также ее способность предпринимать необходимые шаги для создания эффективных методов управления рисками.

Полагаем, что к названным характеристикам необходимо добавить и принципы культуры, которым должен следовать весь персонал организации. На наш взгляд, наиболее подходящие принципы культуры риска, удовлетворяющие требованиям БСРМ, сформулированы Э. Холмсом [93]:

1) никаких исключений. Каждый сотрудник активно берет на себя ответственность и управление рисками. Никому не приходится извиняться за то, что он обнаружил риски;

2) никаких жалоб. Каждый понимает, что иногда события могут разворачиваться не так, как хотелось бы, что можно допустить ошибку, и что иногда позитивные результаты оказываются иллюзорными;

3) никаких сокрытий. Все честно, открыто и искренно. Любые проблемы и сложные вопросы сразу же обсуждаются. Просьба о помощи не рассматривается как признак слабости;

4) нет никаких белых пятен. Каждый понимает, что принятие риска тесно связано с возможностью получить прибыль. И одновременно с поиском путей минимизации угроз сотрудники организации заняты поиском положительных возможностей.

Таким образом, менеджер, занимающийся вопросами риска, должен иметь право выбора решения и право ответственности за принимаемые решения, из-за того что коллективное решение в силу психологических особенностей отдельных лиц является более субъективным, чем решение, принимаемое отдельным специалистом. При этом задача руководителей заключается в поощрении и поддержании сотрудников, следующих принципам культуры риска, задача сотрудников – соблюдать данные принципы независимо от существующих обстоятельств.

### **2.3. Процедурная плоскость базисной системы риск-менеджмента**

Определение понятия «управление рисками», сформулированное нами в главе 1, акцентируется на том, что это процесс, который должен состоять из различных обязательных процедур и осуществляться на постоянной основе. Как форма предпринимательской деятельности, риск-менеджмент означает, что управление риском представляет собой творческую деятельность, эффективность которой зависит от быстроты реакции на изменение условий рынка, экономической ситуации, а также финансового состояния объекта управления. Риск-менеджмент весьма динамичен и эффективность его функционирования во многом зависит от быстроты реакции на изменения условий рынка, экономической ситуации, финансового состояния объекта управления.

По мнению специалистов в риск-менеджменте готовых правил и приемов нет и быть не может, поскольку он определяет как, зная методологию управления рисками тех или иных хозяйственных задач, добиться ощутимого успеха в конкретной хозяйственной ситуации, сделав ее для себя более определенной. В случаях, когда риск рассчитать невозможно, принятие решений происходит с помощью эвристики, которая представляет собой совокупность логических приемов и методических правил теоретического исследования и отыскания истины. Качество (успешность, эффективность) проверяется практикой, решением научно-практических задач – т. е. поиском принципов достижения цели, реализуемых в комплексе реальных дел и обстоятельств.

## Процедуры процесса управления рисками

<i>Автор</i> 1	<i>Процедуры процесса управления рисками</i> 2
В. Ф. Бадюков, Е. В. Козлова [5]	<ol style="list-style-type: none"> <li>1. Выявление цели риска и рискованных вложений капитала.</li> <li>2. Определение вероятности наступления события, степени и величины риска.</li> <li>3. Анализ окружающей обстановки.</li> <li>4. Выбор стратегии управления риском.</li> <li>5. Использование приемов управления риском и способов его понижения.</li> <li>6. Осуществление целенаправленного воздействия на риск</li> </ol>
В. Ф. Бадюков, К. В. Белкин [6]	<ol style="list-style-type: none"> <li>1. Выявление рисков.</li> <li>2. Классификация рисков.</li> <li>3. Выбор измерителей рисков.</li> <li>4. Измерение рисков.</li> <li>5. Выбор стратегий воздействия на риски.</li> <li>6. Использование выбранных стратегий.</li> <li>7. Анализ полученных результатов</li> </ol>
И. Т. Балабанов [7]	<ol style="list-style-type: none"> <li>1. Выработка цели риска и рискованных вложений капитала.</li> <li>2. Получение информации о хозяйственной ситуации и ее анализ.</li> <li>3. Выявление степени риска.</li> <li>4. Определение вероятности наступления события.</li> <li>5. Разработка и анализ вариантов сопоставления прибыли и риска по вложениям капитала.</li> <li>6. Определение стратегии управления риском.</li> <li>7. Выбор необходимых приемов управления риском и способов его минимизации.</li> <li>9. Учет психологического восприятия рискованных решений.</li> <li>10. Разработка программы действия по снижению риска.</li> <li>11. Организация выполнения намеченной программы.</li> <li>12. Контроль выполнения намеченной программы.</li> <li>13. Анализ и оценка результатов выбранного рискованного решения</li> </ol>
Н. В. Хохлов [94]	<ol style="list-style-type: none"> <li>1. Анализ риска.</li> <li>2. Выбор методов воздействия на риск при оценке их сравнительной эффективности.</li> <li>3. Принятие решения.</li> <li>4. Непосредственное воздействие на риск.</li> <li>5. Контроль результатов</li> </ol>

1	2
Г. В. Чернова, А. А. Кудрявцев [96]	1. Идентификация и анализ риска. 2. Анализ альтернативных методов управления риском. 3. Выбор методов управления риском. 4. Исполнение выбранного метода управления риском. 5. Мониторинг результатов и совершенствование системы управления риском

Существует множество точек зрения относительно процедур процесса управления рисками, которые в совокупности составляют этапы организации риск-менеджмента (табл. 2.2).

Проанализировав исследования названных авторов (табл. 2.2), нами выделены основные обязательные процедуры, которые формируют процедурную плоскость БСРМ (рис. 2.5). Процедуры не дублируют друг друга, что является обязательным условием для построения эффективной системы управления рисками [102].



Рис. 2.5. Основные обязательные процедуры процесса управления рисками

Важно заметить, что основной целью выявления рисков является формирование целостной картины о рисках, угрожающих имущественным интересам собственников (акционеров) организации, жизни и здоровью сотрудников, взаимоотношениям с контрагентами и т. д. [151]. В данном случае важен не столько перечень рисков, сколько информация о вероятности или возможности рисков событий, их последствиях, а также вариантах по снижению существующих угроз и повышению положительных возможностей.

В зависимости от объема информации И. А. Бланк [13], Е. Е. Куликова [51], Л. Н. Тэпман [88], Э. Холмс [93], Н. В. Хохлов [94], В. К. Чаа-

даев [95], S.-M. Huang [149] и другие предлагают использовать различные подходы (методы) для выявления рисков, из которых, по нашему мнению, наиболее значимыми для применения в рамках БСРМ и многозадачной классификации рисков, рассмотренной в главе 1, являются следующие:

- анализ сценариев – применим при разработке стратегии развития организации. В нем последовательно рассматриваются все возможные комбинации и анализируются потенциальные риски, которые сопоставляются с ожидаемыми результатами;

- PESTLE-анализ (политический, экономический, социальный, технологический, юридический, экологический) и ВPEST-анализ (бизнес, политический, экономический, социальный, технологический) – применимы при анализе рисков, обусловленных указанными в скобках факторами. PESTLE-анализ в случае необходимости может быть расширен до STEEPLED-анализа, который включает еще образовательный и демографический виды факторов;

- SWOT-анализ (сильные и слабые стороны, возможности и опасности) – является традиционным методом стратегического планирования, который может быть применен и для анализа рисков;

- планирование непрерывности деятельности – метод основан на выявлении возможных проблем, которые могут привести к кризису, связанному с невозможностью осуществлять деятельность на тех же условиях, что и раньше;

- HAZOP (hazard and operability study), или исследование опасностей и работоспособности – представляет собой процесс детализации и идентификации проблем опасности и работоспособности системы в целом для идентификации потенциальных отклонений от целей проекта, экспертизы их возможных причин и оценки их последствий;

- FMEA (от failure mode and effects analysis), или анализ видов и последствий отказов – применим для выявления всех возможных отказов или сбоев в технологическом процессе и оценке последствий их реализации;

- FTA (от fault tree analysis), или анализ дерева неисправности – применим для анализа комбинаций событий нижнего уровня, которые могут привести к нежелательному состоянию. Рассмотрение идет сверху вниз для каждого из событий, т.е. для определенного события, например взрыва, рассматриваются все возможные варианты, приводящие к нему;

- анкетирование – самый простой способ выявления рисков, основанный на опросе максимально широкого круга лиц для выявления их мнений относительно возможности наступления рискованных событий и величины их последствий;

- аудит и инспекция, расследование причин события – методы направлены на выявление текущих нарушений, а также причин совершившихся событий;

– анализ силового поля – направлен на определение сил, противодействующих внедрению какой-либо инновации, и разработку мероприятий по их нивелированию.

Риски, с которыми сталкивается организация, могут исчезать и появляться с течением времени [139]. Для выявления, измерения и оценки рисков необходимо использовать максимально полный комплекс внутренних и внешних источников информации (рис. 2.6).

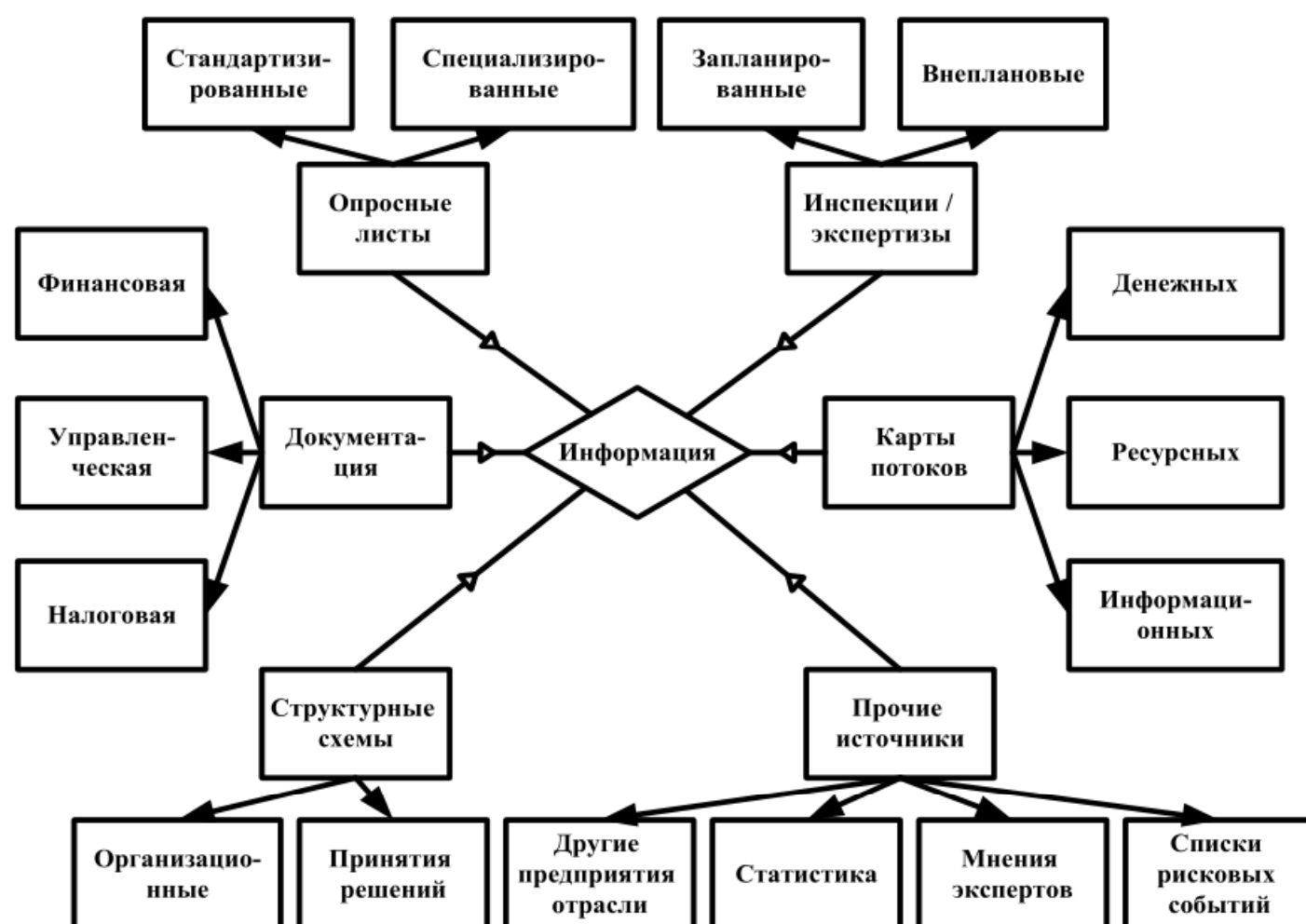


Рис. 2.6. Источники информации о рисках

Данные, получаемые из внутренних источников, учитывают все специфические особенности функционирования и развития организации [96]. Однако позволим себе не согласиться с этим, поскольку на практике нельзя ограничиваться только информацией из внутренних источников, так как этого недостаточно в силу следующих обстоятельств:

– ретроспективный анализ рисков на основе информации из внутренних источников связан с предположением, что наблюдавшиеся ранее тенденции сохранятся в будущем. Между тем их изменение может существенно ограничить полезность собранных данных, что отчетливо наблюдается в условиях мирового финансового кризиса;

– внутренние источники информации не предоставляют сведения о рисках, имеющих катастрофические или фатальные последствия для организации;



– специалистам в области управления рисками часто приходится работать в условиях дефицита доступной информации.

Как видим, для преодоления указанных обстоятельств внутренние источники информации о рисках следует дополнять сведениями из внешних источников, например, данными отраслевой статистики, информацией о деятельности конкурентов, авариях, глобальных потрясениях и т. п.

Далее, на стадии выявления рисков, должна быть проведена их классификация в соответствии с основными критериями, которые были рассмотрены нами ранее в главе 1. Анализ работ И. Т. Балабанова [7], С. М. Васина [19], Е. Е. Куликовой [51], Н. П. Любушина [60], Н. Н. Громова [65], Н. В. Хохлова [94], Г. В. Черновой [96], А. С. Шапкина [97], L. Condamin [135] и других позволил нам установить, какие подходы (методы) идентификации рисков наиболее оптимально подходят для каждой классификационной группы рисков:

- стратегические риски – сценарный анализ, SWOT-анализ;
- финансовые риски – анализ факторов, влияющих на финансовые показатели организации;
- операционные риски – поэтапное рассмотрение всех операций, начиная с самых важных до незначительных;
- репутационные риски – сценарный анализ, метод дерева решений;
- юридические риски – анализ действующего законодательства, сценарный анализ;
- риски основных и обеспечивающих бизнес-процессов – HAZOP, FTA, FMEA методы;
- риски бизнес-процессов управления и развития – метод планирования непрерывности деятельности, метод силового поля;
- риски, возникающие под воздействием внешних факторов – PESTLE-анализ, SWOT-анализ.

После стадии выявления рисков их необходимо измерить, при этом результаты измерения должны быть достоверными, объективными и экономически целесообразными (затраты на проведение анализа не должны превышать дополнительных доходов от использования результатов оценочной деятельности) [4; 12]. Методы измерения рисков, применяемые в рамках БСРМ, подразделяются на две категории.

1. Статистические методы – это присвоение значений вероятности и последствий на основании данных статистики [81]. К таким методам относятся различные методы теории вероятностей [45]. Наиболее распространенным методом является VaR (Value at Risk). Это выраженная в денежных единицах оценка величины, которую с заданной вероятностью не превысят ожидаемые в течение данного периода времени потери. Плюсы статистических методов – их точность, однако есть и значительные минусы: российская экономика не стабильна, поэтому статистический расчет какого-либо риска может не отражать фактического положения дел.

Статистические методы стали впервые применяться в финансовых институтах, но их применение может быть эффективным и в организациях реального сектора экономики, например для расчета финансовых рисков, или рисков, связанных с отказами оборудования, а также потерь от реализации операционных рисков в случае значительного количества операций и, соответственно, наличия статистики.

2. Экспертные методы – это присвоение значений возможности или вероятности и величины последствий на основании мнения специалистов. К таким методам относятся опросы, анкетирование, привлечение специалистов в определенных областях для анализа рисков и т. д. Положительной стороной методов является возможность расчета практически любого риска. В то же время есть отрицательная сторона: присваиваемые значения будут сильно отличаться в случае разных экспертных групп. Практика показывает, что оценка рисков, проведенная сотрудниками организации, значительно отличается от оценки рисков любых внешних консультантов [135].

На первом этапе основными применяемыми методами являются экспертные [71]. Поэтому необходимо обращать внимание на количество и квалификацию экспертов, т.е. необходимо получить несколько экспертных оценок, и не следует учитывать мнения некомпетентных сотрудников. Результатом измерения станут качественные, полуколичественные и количественные показатели вероятности рисков событий и их последствий (табл. 2.3).

Таблица 2.3

**Варианты измерения возможности, вероятности и последствий**

<i>Измерение</i>					
Возможности	Вероятности, %		Последствий		
Качественное	Полуколичественное	Количественное	Качественное	Полуколичественное, тыс. руб.	Количественное, тыс. руб.
Очень высокая	Более 75	80	Очень высокая	Более 100	100
Высокая	От 50 до 75	60	Высокая	От 10 до 100	50
Средняя	От 25 до 50	40	Средняя	От 1 до 10	5
Низкая	Менее 25	10	Низкая	Менее 1	1

Заметим, что разница между качественным и количественным измерением рисков существенна [134]. Качественное измерение подразумевает применение методов определения вероятности и последствий риска, основанных на субъективном мнении эксперта предметной области. Количественная оценка подразумевает применение математического моделирования для оценки вероятности и последствий риска с учетом всевозможных допущений.

Качественные показатели применяются в следующих случаях:

- при отсутствии необходимости получать количественные показатели;
- в случае составления приблизительного рискового профиля организации в целях дальнейшего, более детального, изучения;
- невозможности представления степени риска количественно, или когда количественная оценка будет недостоверной;
- несоизмеримости уровня риска с затратами на сбор и анализ количественной информации.

Анализ практики управления рисками [24; 121] показал, что отечественные организации на текущий момент измеряют свои риски только качественно и лишь немногие – количественно вследствие отсутствия методик количественного измерения рисков. Даже в случае если уровень риска может быть подсчитан, специалисты в области управления рисками отдают предпочтение полуколичественным или количественным показателям.

В стандарте FERMA [119] приведены таблицы, позволяющие сопоставлять качественные и количественные величины рисков. При этом в стандарте применяются трехуровневые шкалы величин, что, по мнению Э. Холмса [93], неправильно, так как при измерении риска возникает соблазн вывести среднюю величину. Принимая во внимание это обстоятельство, нами предлагаются доработанные варианты таблиц измерения последствий и вероятностей, состоящие из четырехуровневых шкал показателей вместо трехуровневых стандарта FERMA, которые можно применять в рамках БСРМ (см. прил. 1).

Рассмотрим варианты измерения применительно к видам рисков многозадачной классификации, которая разработана нами и представлена в главе 1:

1) стратегические риски, связанные с развитием и управлением, например такие как сделки слияния и поглощения, могут измеряться количественно [138]. Полагаем, что при этом измерение количественными методами некоторых стратегических рисков, обусловленных воздействием внешних сил, может быть проблематичным вследствие недостаточного объема информации, доступной риск-менеджеру. В этом случае для их оценки необходимо применять методы экспертной оценки с качественными показателями, с последующим переводом качественных измерений в количественные, если необходимо сопоставить полученные результаты;

2) финансовые риски можно также измерить количественно, оценив вероятность и последствия их реализации на основе известных причин и факторов их вызывающих. Как правило, по ним всегда имеется достаточное для расчета количество статистики и прогнозов поведения внешних макроэкономических показателей, влияющих на финансовые риски [37; 100; 135]. При этом необходимо отдавать отчет в том, что результат моделирования финансового риска в связи с нынешней высокой волатильностью макроэкономических показателей будет очень неопределенным;

3) большинство операционных рисков можно измерить количественно, если достаточен объем необходимых данных по этим рискам за прошедшие периоды [135]. Однако заметим, что среди операционных рисков есть и такие (как правило, они обусловлены внешними силами), которые практически не поддаются подсчету, например технологические риски (качество используемых технологий значительно отстает от используемых конкурентами);

4) репутационные риски на практике принято оценивать качественно в силу уникальности каждого рискованного события. Однако в настоящее время существуют методики по количественной оценке репутационных рисков организаций, акции которых котируются на фондовых площадках. Базой для оценки выступает капитализация организации и величина ее снижения в результате негативных для репутации событий [104];

5) в главе 1 нами было установлено, что юридические риски напрямую связаны с нормативным полем, в рамках которого ведет деятельность организация и ее контрагент. Исходя из того, что российское законодательство имеет правовые пробелы, то более точным является измерение юридических рисков качественными показателями. С другой стороны, в настоящее время имеются открытые информационные ресурсы по судебным практикам, позволяющие прогнозировать принятие решений органов власти в спорных ситуациях, а следовательно, и проводить количественную оценку юридических рисков организации.

Обобщив сказанное, приходим к выводу, что почти все риски можно измерить или качественно, или количественно, но за различный период времени. Следовательно, процессы измерения рисков должны проходить с минимальным количеством временных затрат, чтобы потом иметь достаточное количество времени на подготовку и проведение мероприятий по управлению ими.

Далее, после выявления и измерения рисков организации, необходимо уполномоченным органам и лицам, на основе полученных данных, принять решение об управлении конкретными рисками [124]. Для этого необходимо оценить риски.

Оценка рисков используется для принятия решений о значимости рисков, а также о том, можно ли принять последствия существования данного риска или предпринять шаги по изменению ситуации. Такая значимость устанавливается путем сравнения проведенного расчета рисков с определенными критериями. В соответствии со стандартом FERMA [119] критерии могут включать в себя учетную политику, себестоимость продукции, регулятивные требования, социально-экономические вопросы, экологический аспект, ожидания акционеров и других заинтересованных лиц и т. д. Критерии, переведенные в денежное выражение, принято называть склонностью к риску, или толерантностью к риску. Величина склонности к риску утверждается уполномоченным органом или лицом и выражается в виде процента [93; 135]:

- от капитализации (стоимости организации);
- доли стоимости чистых активов;

– вида прибыли, например чистой, до налогообложения, EBITDA и др.;

– конкретного финансового значения.

Уполномоченному органу или лицу необходимо точно установить склонность организации к риску. Неправильное определение величины склонности к риску или незнание данной величины ведет к двум основным негативным последствиям:

1) к неприятию рисков, когда организация становится более консервативной;

2) чрезмерному оптимизму, когда организация готова принимать больше рисков на себя, чем того требует стратегия развития.

Необходимо отметить, что четкое определение склонности к риску, с точки зрения формализации процесса управления рисками, помогает решать следующие задачи [93]:

1) выявление приоритетных рисков, благодаря этому организация может обращать внимание только на значимые для нее риски, управление которыми принесет наибольшую выгоду;

2) понимание каждым сотрудником организации того, какие риски она готова принять, на основе чего они смогут уточнить свои собственные подходы к рискам;

3) рост восприимчивости каждого сотрудника к тем рискам, которые считаются неприемлемыми.

Между тем, несмотря на очевидную необходимость определения склонности к риску, многие организации не уделяют достаточного внимания этой проблеме. Они исходят из того, что получение доходов всегда сопряжено с принятием рисков, которые рассматриваются как неизбежные угрозы, а не как возможности к росту и основания для принятия управленческих решений. Поэтому склонность к риску определяется руководством и собственниками организации неосознанно, без системного подхода [124].

Модель ранжирования всех организаций в зависимости от их склонности к риску была разработана компанией PricewaterhouseCoopers, которой установлено, что чем сложнее система управления рисками организации, тем сильнее его фокус смещается от рисков в роли угроз к рискам в роли возможностей [144]. Это, в свою очередь, оказывает прямое влияние на склонность руководства и владельцев организации к принятию рисков.

Склонность к риску организации принято изображать графически на Карте рисков, которая является одним из основных внутренних документов, рассматриваемых уполномоченным органом при принятии решения об управлении рисками.

После проведенной оценки рисков начинается следующая процедура – разработка и реализация мероприятий по управлению рисками.

В настоящее время мировая практика выработала широкий спектр подходов по управлению рисками. Почти все они требуют специальных разработок и материальных затрат. Поэтому необходимо четко понимать, что представляет собой каждый прием управления рисками.

Отечественные и зарубежные авторы, такие как Х. А. Абасова [1], В. Ф. Бадюков [5], М. А. Батьковский [10], Ю. В. Васильков [18], Е. Е. Загрязкина [33], Г. Ларионов [54], А. Ю. Рогачев [77], J. David Cummins [131] и другие выработали обширный перечень приемов управления рисками. В ходе анализа их трудов нами были отобраны наиболее часто встречающиеся приемы, которые могут применяться в БСРМ. Представим сгруппированные нами приемы в соответствии с их общим направлением воздействия на риски (рис. 2.7).



Рис. 2.7. Основные группы приемов управления рисками

Рассмотрим каждую группу приемов управления рисками, чтобы определить приемлемость их для тех или иных ситуаций при использовании в рамках БСРМ.

1. Прием уклонения от риска предусматривает следующее [68]:

- отказ от осуществления операций с высоким уровнем риска;
- отказ от продолжения отношений с партнерами, систематически нарушающими контрактные обязательства. Такая форма уклонения является одной из наиболее распространенных и доступных для применения;
- отказ от использования денежных средств в краткосрочных инвестиционных операциях. Эта мера позволяет уклониться от депозитного и процентного рисков, однако порождает потери от инфляционного риска, а также риска упущенной выгоды.

Уклонение от рисков лишает организацию дополнительных источников доходов, следовательно, может отрицательно влиять не только на рентабельность деятельности, но и на ее дальнейшее развитие.

Поэтому, принимая решение об отказе от риска, необходимо обратить свое внимание на следующие вопросы:

- возможно ли полностью уклониться от риска (для малых организаций это маловероятно);
- как соотносятся предполагаемая прибыль и убытки (прибыль может оказаться значительно выше возможных потерь и в этом случае данный метод не используется);
- приводит ли отказ от одного риска к возникновению других (например, отказ от риска, связанного с авиаперевозками, может повлечь риск, вызванный железнодорожными или автомобильными перевозками).

Итак, можно сделать вывод, что организации следует отказываться только от операций, несущих в себе риски, реализация которых влечет за собой катастрофические последствия для бизнеса.

2. Прием сокращения рисков направлен на уменьшение возможности наступления рискованных событий, либо на снижение их последствий [116] и при этом существуют следующие подходы.

2.1. Лимитирование как подход предполагает установление лимита, то есть неких предельных размеров инвестиций, партий закупаемых материальных ресурсов, товарных кредитов, сумм вложения капитала [65].

Система лимитирующих нормативов может определять [68]:

- максимальный объем заемных средств;
- минимальный объем высоколиквидных активов;
- предельный размер кредиторской или дебиторской задолженности, приходящейся на одного контрагента;
- наибольшую допустимую продолжительность задолженности контрагентов перед организацией и наоборот.

2.2. Самострахование – это создание запаса средств и времени для обеспечения возможности функционирования организации в случае нарушений и сбоев в хозяйственной деятельности. Запас создается за счет:

- резервирования средств и ресурсов (формирование собственных резервных фондов, неиспользуемых лимитов по кредитным линиям, выделение резервных мощностей) адекватных ожидаемым рискам;
- резервирование в производственных, коммерческих и финансовых планах времени на операции, сопряженные с повышенным риском.

К самострахованию обычно прибегают крупные организации. Основной проблемой при реализации подхода самострахования является определение величины резервируемых запасов. Излишние резервы приводят к иммобилизации средств и выводу их из оборота. Недостаточное резервирование не может способствовать сокращению рисков.

2.3. Диверсификация – это расширение сфер деятельности, номенклатуры продукции и выполняемых услуг [42]. При данном подходе производится:

- диверсификация рынка сбыта – работа одновременно на нескольких рынках сбыта (потери на одном из них могут быть компенсированы прибылью на других);
- диверсификация закупок сырья и материалов – взаимодействие с несколькими поставщиками, это позволяет ослабить зависимость организации от отдельных контрагентов;
- проведение биржевых операций, страхующих снабжение и сбыт;
- диверсификация деятельности – увеличение используемых технологий, расширение ассортимента выпускаемой продукции, ориентация на различные социальные группы.

В практической деятельности возможны случаи, когда диверсификация увеличивает риск. Например, если организация вкладывает средства в деятельность, где ее влияние ограничено.

3. Прием перераспределения рисков включает в себя следующие механизмы воздействия [111].

3.1. Страхование – один из наиболее распространенных методов воздействия на риск, позволяющий защищать объект риска от случайных воздействий. Наличие факторов риска и необходимость покрытия ущерба обуславливают потребность страхования. Предпосылками для защиты объектов собственности являются различные формы проявления рисков и тяжесть последствий их проявления.

Отсутствие непредвиденных рисков событий при некотором снижении прибыльности является благоприятной ситуацией для организации. Цель страхования – возмещение материального ущерба в результате проявления рисков событий. При этом страхование предполагает проведение мероприятий по снижению возможности наступления указанных событий, что также положительно сказывается на стабильности деятельности организации.

3.2. Трансферт – передача рисков. Он должен быть выгоден обоим участникам сделки, а его условия зафиксированы в договоре или контракте. Для осуществляющей трансферт организации передаваемые риски являются, скорее всего, существенными, в то время как для принимающей организации указанные риски являются не существенными, и она обладает лучшими возможностями для управления вероятностью наступления или величиной последствий рисков событий.

Рассмотрим способы трансферта риска. Первый способ – заключение контрактов со специально оговоренными условиями, которые различаются в зависимости от вида хозяйственной деятельности [80]:

1) в строительной отрасли от передаваемых заказчиком к принимаемым подрядчиком рискам, например можно отнести не только проблемы с поставками материалов, низкий уровень квалификации



персонала, возможные забастовки, но и уплату штрафов за задержку при сдаче готового объекта и т. д.;

2) в арендных отношениях арендодатель и арендатор могут разделить риски, например риск повреждений собственности принимается арендодателем, а риск снижения коммерческой ценности арендуемого имущества – арендатором, но только в пределах срока аренды;

3) при транспортировке и хранении грузов передаваемые риски могут быть прописаны не только в договоре, но и возникать в силу действующего законодательства. Например, транспортная компания может не принимать на себя риск снижения цены товара, вызванный задержкой доставки, если сроки транспортировки предварительно не были зафиксированы в договоре;

4) контракты на продажу, обслуживание, снабжение предполагают передачу рисков от потребителя, купившего товар, к производителю. Это происходит через установленную производителем гарантию на товар (устранение дефектов, замена недоброкачественного товара). Кроме того, есть и другие виды договоров, обеспечивающих передачу рисков. Одним из них является договор на сервисное обслуживание техники;

5) в контракте-поручительстве принимают участие три лица: поручитель, принципал и кредитор. Суть передачи риска заключается в том, что поручитель гарантирует кредитору, что принципал возвратит свой долг. Таким способом часть риска переносится на поручителя, остальную часть берет на себя принципал.

Второй способ – выбор организационной формы бизнеса. При ограниченной ответственности владельцы организации передают возможные потери, которые превышают активы организации, кредиторам бизнеса. В акционерном обществе мы можем наблюдать передачу рисков от руководителей организации к акционерам, которые в свою очередь могут передавать их биржевым дельцам.

3.3. Хеджирование, как еще один способ трансферта рисков, включает в себя, прежде всего, операции на валютных рынках, позволяющие застраховаться от изменения валютного курса [61]. Выделяют хеджирование на повышение, применяемое при необходимости страхования от возможного повышения цен в будущем и связанное с покупкой срочного контракта, и хеджирование на понижение, связанное с продажей срочного контракта.

Несмотря на все преимущества, хеджирование имеет ряд недостатков:

– организация, совершая операцию хеджирования, устраняет ценовой риск и принимает риск, связанный с владением базисом. Базисный риск возрастает при росте отличий сорта товара и спецификации фьючерсного контракта;

– заключение фьючерсного контракта предусматривает операционные расходы и расходы на клиринг. Кроме того, есть еще издержки, связанные с процентами на маржевые суммы;

– фьючерсные контракты не всегда совпадают с условиями обязательств на товарном рынке;

– в связи с ограниченностью фьючерсного рынка дневными колебаниями цен могут возникнуть ситуации, когда нельзя открыть или ликвидировать позицию в определенные дни из-за искажения соотношения цен товарного и фьючерсного рынков.

4. Прием принятия риска предусматривает принятие организацией на себя последствий от наступления рискованного события [111].

Владелец риска принимает риск в случае, если невозможно применить другие методы воздействия на риск либо когда он находится в приемлемых границах склонности к риску организации. Важно помнить, что принимаемый риск, в зависимости от уровня создаваемой угрозы, должен находиться под наблюдением в соответствии с правилами БСРМ, сформированными нами ранее в главе 2.

Для успешного принятия риска на себя организации необходимо располагать планом действий в случае наступления рискованных событий [157]. Указанный план снижает временные затраты на реагирование, что может положительно сказаться на экономии денежных средств.

В ходе исследования было установлено, что выбор того или иного приема управления рисками строится на сравнительном анализе эффекта от управления рисками и издержек всех выявленных вариантов управления, с учетом следующих необходимых условий:

1) затраты на управление рисками должны быть соразмерны получаемому эффекту;

2) в расчет должны приниматься все прямые и косвенные затраты и эффект от управления рисками, с учетом как материальных, так и нематериальных аспектов;

3) выгоды, получаемые в результате управления рисками, имеют различный уровень важности;

4) сравнительный анализ материальных и нематериальных издержек и эффекта от управления рисками не может быть проведен только средствами количественного анализа;

5) издержки и эффект от управления рисками проявляются в разные периоды времени, выгоды проявляются, чаще всего, позже;

6) управление одними рисками может создать новые риски, которые должны быть идентифицированы, оценены, стать объектом управления и мониторинга;

7) применение того или иного варианта управления должно согласовываться с общими целями и задачами организации.

После разработки мероприятий по управлению рисками, их необходимо согласовать с заинтересованными лицами, а затем вынести на утверждение уполномоченным органам или лицам. Только после утверждения мероприятия принимаются к исполнению.

Следующей обязательной процедурой процесса управления рисками является мониторинг, который представляет собой систематическое наблюдение за процессом с целью фиксации соответствия (или

несоответствия) результатов этого процесса первоначальным предположениям [49]. Мониторинг также служит основой для формирования обратной связи с заинтересованными лицами. Это очень важный этап, так как именно он обеспечивает гибкость и адаптивность управления рисками, а также динамический характер этого процесса [96].

Проведение мониторинга на регулярной основе позволяет выявлять различные изменения в деятельности организации, влияющие на работу БСРМ, например появление новых заинтересованных лиц или смена ответственных исполнителей, применение новых технологических процессов или действия со стороны конкурентов и так далее.

Все изменения можно условно классифицировать на внезапные и прогнозируемые, причем и те и другие могут иметь достаточно серьезные последствия для организации, так как оказывают влияние:

- на основные структурные компоненты риска (факторы, источники, причины, события и их последствия);
- целесообразность и эффективность приемов управления рисками.

В ходе мониторинга могут быть установлены новые обстоятельства, оказывающие существенное влияние на основные структурные компоненты рисков и приемы управления ими. Как следствие, риски должны быть заново идентифицированы и оценены, а планы управления рисками скорректированы.

На практике мониторинг принято проводить по двум направлениям [132]:

- 1) рутинные проверки;
- 2) специальные проверки.

Модель мониторинга управления рисками строится таким образом, чтобы в большинстве случаев обходиться только рутинными проверками. Чем выше эффективность рутинных проверок, тем меньше потребность в проведении специальных. Частота и количество специальных проверок, необходимых для разумной гарантии эффективности системы управления рисками, зависит от взглядов на эту потребность со стороны уполномоченных лиц организации [67]. Для того чтобы определить потребность, необходимо оценить:

- 1) суть и серьезность происходящих изменений;
- 2) профессиональный уровень и компетентность лиц, занимающихся управлением и контролем риска;
- 3) результаты рутинных проверок.

Как видим, только комбинация рутинных и специальных проверок гарантирует, что система управления рисками организации будет работать эффективно в течение заданного горизонта времени.

В ходе проведения мониторинга происходит обновление и пополнение информации о рисках, включая получение необходимой информации для их полной идентификации [47].

По нашему мнению, эффективность работы БСРМ необходимо проверять на периодической основе после завершения процедуры мониторинга. Эта проверка должна состоять из нескольких этапов.

**1 этап.** Определение эффективности мероприятий по управлению реализовавшимися рисками.

Ранее, в главе 2, нами отмечалось, что риск-менеджмент может быть эффективным только тогда, когда планируемые затраты на управление риском меньше или равны ожидаемому изменению величины этого риска после осуществления мероприятий по управлению им. Представим это в виде неравенства:

$$\Delta rP_i \geq exP_i, \quad (2.1)$$

где  $\Delta rP_i$  – ожидаемое изменение величины частного  $i$ -го риска после осуществления мероприятий по управлению им;  $exP_i$  – планируемые затраты на управление частным  $i$ -тым риском, вычисляемые по формуле:

$$exP_i = \sum_{\alpha=1}^l exP_{\alpha_i}, \quad (2.2)$$

где  $exP_{\alpha_i}$  – величина элемента затрат на управление частным  $i$ -тым риском (оплата труда, амортизация оборудования и др.);  $\alpha$  – порядковый номер элемента затрат по управлению риском.

В свою очередь, при эффективном управлении рисками ожидаемое изменение величины риска должно быть меньше или равно фактическому изменению в случае наступления рискованного события и его последствий. При этом фактические затраты должны быть меньше или равны планируемым затратам. Математически это может быть представлено в виде системы неравенств:

$$\begin{cases} \Delta rF_i \geq \Delta rP_i \\ exF_i \geq exP_i \\ rF_{i1} \neq 0 \end{cases}, \quad (2.3)$$

где  $exF_i$  – фактически понесенные затраты на управление частным  $i$ -тым риском, вычисляемые по формуле (2.2), но в расчетах участвуют фактические затраты, а не планируемые;  $\Delta rF_i$  – фактическое изменение величины реализовавшегося частного  $i$ -го риска в результате управления им, вычисляемое по формуле:

$$\Delta rF_i = rF_{i1} - rF_{i0}, \quad (2.4)$$

где  $rF_{i0}$  – смоделированная величина частного  $i$ -го риска, т.е. рассчитанная без учета эффекта от мероприятий по управлению им;  $rF_{i1}$  – фактическая величина реализовавшегося частного  $i$ -го риска.

Имея сведения о плановых и фактических изменениях величины частных рисков, а также о величинах затрат на управление ими, можно вычислить эффективность мероприятий управления всей совокупности реализовавшихся рисков в рамках БСРМ. Для этого из частных показателей необходимо получить общие, используя следующие формулы:

$$ExP = \sum_{i=1}^n exP_i ; \quad (2.5)$$

$$ExF = \sum_{i=1}^n exF_i ; \quad (2.6)$$

$$\Delta RP = \sum_{i=1}^n rP_i ; \quad (2.7)$$

$$\Delta RF = \sum_{i=1}^n rF_i , \quad (2.8)$$

где  $ExP$  – сумма затрат, которые были изначально запланированы на управление реализовавшимися рисками;  $ExF$  – сумма фактически понесенных затрат на управление реализовавшимися рисками;  $\Delta RP$  – сумма изменений величин реализовавшихся рисков, которую изначально запланировано получить после осуществления мероприятий по управлению ими;  $\Delta RF$  – сумма фактических изменений величин реализовавшихся рисков в результате управления ими.

Действуя, таким образом, можно составить неравенства, определяющие эффективность мероприятий по управлению рисками организации в рамках БСРМ. Наибольшая эффективность мероприятий может быть определена следующим неравенством, которое описывает идеальную ситуацию по управлению рисками:

$$\Delta RF \geq \Delta RP \geq ExP \geq ExF. \quad (2.9)$$

Вероятнее всего, организация получит результаты, соответствующие одному из следующих неравенств, которые указывают на относительную эффективность мероприятий по управлению реализовавшимися рисками:

$$\Delta RF \geq \Delta RP \geq ExF \geq ExP; \quad (2.10)$$

$$\Delta RF \geq ExF \geq \Delta RP \geq ExP. \quad (2.11)$$

Несмотря на то что фактическое изменение величин рисков больше фактических затрат на управление ими, возникла ситуация, при которой фактически понесенные затраты превысили не только планируемые [неравенство (2.10)], но и превысили величину ожидаемых изменений реализовавшихся рисков [неравенство (2.11)].

Полагаем, что во всех остальных случаях эффективность мероприятий по управлению реализовавшимися рисками может быть признана неудовлетворительной, так как к ней применимо следующее неравенство:

$$ExF \geq \Delta RF. \quad (2.12)$$

Аналогично анализируется эффективность мероприятий управления любым из реализовавшихся частных  $i$ -тым риском. Для этого в неравенства (2.9), (2.10), (2.11) и (2.12) вместо общих показателей заносятся соответствующие частные.

## 2 этап. Оценка качества анализа рисков.

Оценка качества анализа рисков должна производиться по следующим направлениям:

– показатель точности выявления рисков ( $QA$ ) вычисляется, %, по формуле:

$$QA = \frac{m}{n} \times 100 \% , \quad (2.13)$$

где  $m$  – количество предварительно выявленных реализовавшихся частных рисков;  $n$  – количество фактически реализовавшихся частных рисков.

Значение  $QA$  менее 100 % говорит о том, что не все реализовавшиеся риски были своевременно выявлены, а также о необходимости усиления процедуры выявления рисков. Организации необходимо контролировать динамику показателя  $QA$ . С течением времени величина показателя должна возрастать, что говорит о повышении качества процедуры выявления рисков;

– показатель точности прогноза величины последствий реализации рисков событий ( $RA$ ) определяется по формуле:

$$RA = \sum_{j=1}^m \frac{rA_j}{m} , \quad (2.14)$$

где  $RA$  – показатель точности прогноза величины последствий реализации рисков событий;  $m$  – количество предварительно выявленных реализовавшихся частных рисков;  $j$  – порядковый номер предварительно выявленного реализовавшегося частного риска;  $rA_j$  – показатель точности прогноза величины последствий рисков события предварительно выявленного частного  $j$ -того риска, вычисляемый по формуле:

$$rA_j = \frac{rF_j}{rP_j} , \quad (2.15)$$

где  $rF_j$  – фактическая величина последствий реализации рисков события частного  $j$ -того риска;  $rP_j$  – плановая величина последствий реализации рисков события частного  $j$ -того риска.

Показатель  $RA$  может принимать одно из трех возможных значений:

1) если  $RA > 1$ , то совокупная величина последствий реализации рисков была недооценена;

2) если  $RA = 1$ , то совокупная величина последствий реализации рисков была оценена верно;

3) если  $RA < 1$ , то совокупная величина последствий реализации рисков была переоценена.

При этом необходимо заметить, что для определения точных причин отклонений фактических величин от плановых анализ следует проводить в разрезе каждого частного  $j$ -того риска.

Показатель точности прогноза стоимости мероприятий по управлению рисками ( $ExA$ ) рассчитывается по формуле:

$$ExA = \sum_{j=1}^m \frac{exA_j}{m}, \quad (2.16)$$

где  $ExA$  – показатель точности прогноза величины стоимости мероприятий по управлению рисками;  $m$  – количество предварительно выявленных реализовавшихся частных рисков;  $j$  – порядковый номер предварительно выявленного реализовавшегося частного риска;  $exA_j$  – величина стоимости мероприятий по управлению частным  $j$ -тым риском, вычисляемая по формуле:

$$exA_j = \frac{exF_j}{exP_j}, \quad (2.17)$$

где  $exF_j$  – фактическая величина стоимости мероприятий по управлению частным  $j$ -тым риском;  $exP_j$  – плановая величина стоимости мероприятий по управлению частным  $j$ -тым риском.

Показатель  $ExA$  может принимать одно из трех возможных значений:

1) если  $ExA > 1$ , то совокупная величина стоимости мероприятий по управлению рисками была недооценена, либо было произведено излишнее финансирование;

2) если  $ExA = 1$ , то совокупная величина стоимости мероприятий по управлению рисками была оценена верно;

3) если  $ExA < 1$ , то совокупная величина стоимости мероприятий по управлению рисками была переоценена, либо произошло недофинансирование.

При этом заметим, что для определения точных причин отклонений фактических величин от плановых анализ также необходимо провести в разрезе каждого частного  $j$ -того риска.

**3 этап.** Оценка качества управления нереализовавшимися рисками не производится, поскольку отсутствуют данные для сравнительного анализа.

Все полученные показатели эффективности управления рисками в рамках БСРМ должны быть представлены уполномоченному органу для принятия им окончательного решения об эффективности риск-менеджмента в организации.

Целью оценки эффективности риск-менеджмента является адаптация системы управления риском к измененным условиям функционирования окружающей среды и совокупности влияющих на деятельность организации рисков. Этого можно добиться следующими действиями:

– заменой неэффективных мероприятий на более эффективные в рамках выделенного бюджета на программу управления риском. Такие мероприятия повышают общую результативность системы управления риском;

– изменением программы управления риском, поскольку она определяет специфику институционального фундамента защиты организации от соответствующих рисков.

Очень важной процедурой, необходимой для работы БСРМ, является управление информацией, поскольку без нее невозможно осуществить все другие процедуры, следовательно, она должна проводиться на постоянной основе.

Информация является ключевым аспектом при анализе рисков. Ее отсутствие делает невозможным принятие обоснованных решений по управлению рисками [96]. Содержание и объем необходимой информации всегда зависят от конкретных условий, но при этом они должны определяться рядом требований, которые мы сформулировали применительно к БСРМ, взяв за основу требования к финансовым рискам, указанные в работах [13; 100]:

1) значимостью, которая определяет существенность информации для принятия решений, например в процессе формирования стратегии, постановки целей и задач организации, составления планов по их достижению;

2) полнотой, которая характеризует достаточность информационных данных, необходимых для принятия взвешенных решений по вопросам, касающимся управления рисками;

3) достоверностью, определяющей в каком размере информация объективна при отражении реального состояния и результатов деятельности организации;

4) своевременностью, характеризующей соответствие информации и потребности в ней по периоду ее использования;

5) понятностью, заключающейся в простоте построения информации, ее соответствии принятым стандартам представления и в доступности для понимания и толкования заинтересованными лицами, которым она предназначена;

6) релевантностью, определяющей частоту использования информации в процессе риск-менеджмента;

7) сопоставимостью, которая определяет возможность сравнительной оценки показателей деятельности организации за различные периоды времени, возможность проведения сравнительного анализа с аналогичными организациями отрасли и т. д.;

8) эффективностью, которая, применительно к формированию модели управления информацией, означает, что затраты на получение информации не должны превышать эффект, получаемый в результате ее использования в процессе управления рисками.

Заметим, что сформулированные нами требования отчасти являются противоречивыми. Например, требование своевременности информации может не согласовываться с требованием полноты или достоверности, так как необходимая для принятия решений информация часто становится доступна слишком поздно. Таким образом, информационные источники и получаемые из них данные необходимо проанализировать в целях нахождения компромисса между указанными требованиями.



В рамках системы управления рисками одной из основных задач при работе с информацией является обеспечение постоянной и своевременной коммуникации между заинтересованными лицами [2]. Ряд специалистов в области управления рисками при работе с информацией во главу угла ставит сбор и обработку сведений со стороны внутренних служб организации, не рассматривая при этом коммуникации внутренних заинтересованных лиц с внешними [96; 100], либо рассматривает их, но исключительно с позиции возможности получения сведений, а не с позиции взаимного влияния друг на друга [13]. По нашему мнению, недопустимо уделять слишком большое внимание аспектам внутренних коммуникаций, оставляя без рассмотрения особенности обмена информации с внешними заинтересованными лицами.

Принципиальным моментом является то, что владельцы рисков должны иметь доступ к необходимой им информации на любом этапе процесса управления рисками, т.е. заинтересованные лица являются получателями и источниками информации одновременно. В связи с большим объемом информации, поступающей как из внешних, так и внутренних источников, основная цель управления информацией сводится к выделению из всего этого массива данных действительно необходимой информации и организации обмена ею между участниками процесса управления рисками [117].

Оперативный обмен информацией, необходимый для управления риском, возможен только тогда, когда для ее получения, обработки, хранения и распределения используются информационные технологии [32; 127], которые идентичны тем, которые используются в организации для постановки систем контроля, планирования и т.д. [87]. Они построены на обмене данными между рабочими местами посредством использования каналов связи, а также централизованных информационных баз данных. Подсистема управления информацией для работы БСРМ является частью общей информационной системы, и, следовательно, при ее построении необходимо учесть следующие существенные факторы [96]:

- особенности архитектуры применяемых информационных технологий, например форматы хранения данных, применяемые протоколы обмена информацией и т. д.;
- возможность использования меньшего количества различных программных продуктов;
- наличие ограничений к информации по управлению рисками в зависимости от уровня доступа.

Такая информационная подсистема будет обладать специфическими чертами, к которым можно отнести цели и методы обработки данных, а также некоторые особенности самой информации, например при учете потенциального ущерба и так далее.

К дополнительным преимуществам применения информационных технологий при управлении информацией можно отнести следующее [96; 137]:

- возможность быстрого изменения классификации рисков и приоритетности решения тех или иных задач по управлению риском;
- согласование результатов анализа рисков с административной информацией (например, учет подразделения фирмы, привязка к проекту и/или сфере деятельности);
- увязка результатов анализа рисков с маркетинговой информацией (данные о клиентах, конкурентах и т. д.);
- взаимосвязь результатов анализа рисков с экономической и финансовой информацией (оценка влияния рисков на процессы и персонал, связь с центрами прибыли и затрат);
- возможность оценки риска на разных уровнях (организация в целом и/или отдельные подразделения) и в соответствии с различными методиками, что делает процесс управления риском более гибким благодаря учету интересов разных работников и руководителей организации;
- обеспечение интеграции различных аспектов управления риском (количественная и качественная оценка рисков, анализ и выбор методов управления риском, определение эффективности этих методов и т. п.);
- облегчение процесса контроля, мониторинга и аудита мероприятий управления рисками, а также их соответствия необходимым ограничениям (юридическим, бюджетным и т. д.).

Вместе с тем применение информационных технологий для обеспечения работы БСРМ сопряжено с рядом недостатков, среди которых можно выделить следующие [32; 116]:

- система риск-менеджмента становится более уязвимой, например, перед операционными рисками (авария локальной сети или поломки компьютерного оборудования делают невозможным проведение процедур управления рисками);
- стоимость сбора и обработки информации на первоначальном этапе внедрения повышается (например, из-за необходимости обучения персонала, покупки дополнительной вычислительной техники, средств связи, программного обеспечения и т. д.);
- использование информационных технологий создает потребность в наличии четко формализованных моделей и процессов принятия решений, которые не всегда предусматривают пути решения всех проблем (например, возникающих в условиях форс-мажора).

Заметим, что преимущества от применения информационных технологий превосходят недостатки [117; 127], следовательно, целесообразность их применения для управления информацией, необходимой для работы БСРМ, неоспорима.

#### **2.4. Нормативная плоскость базисной системы риск-менеджмента**

Четвертой плоскостью БСРМ является нормативная плоскость, которая охватывает внутренние документы организации по вопросам управления рисками. В России пока нет своего национального стандар-

та по управлению рисками (но работы по его разработке уже ведутся [11; 31; 63]), поэтому при разработке нормативных документов отечественные специалисты по рискам руководствуются международными стандартами (табл. 2.4).

Таблица 2.4

**Основные стандарты в области управления рисками**

<i>Название стандарта</i>	<i>Краткое описание</i>
FERMA/AIRMIC/ALARM/IRM Risk Management Standard (FERMA)	Европейский стандарт, раскрывающий основные этапы процесса управления рисками, а также условия, необходимые для правильной организации данного процесса
ISO 31000 Risk management – Principles and guidelines (ISO 31000)	Британский стандарт, пришедший на смену FERMA /AIRMIC/ALARM/ IRM Risk Management Standard
The COSO Enterprise Risk Management - Integrated Framework (COSO ERM)	Является эволюцией более раннего стандарта по внутреннему аудиту «The COSO Internal Control – Integrated Framework». Он затрагивает внутренние системы контроля в компании (контроль факторов среды, оценка последствий рисков событий, мероприятия по контролю, передаче информации, мониторингу)
The Turnbull Report	Устанавливает требования к организации аудита и управлению рисками организаций, котирующихся на фондовых площадках
The Australia /New Zealand Standard AS/NZS 4360:2004	Цель стандарта – определение общих требований для выявления условий возникновения, идентификации, обмена информацией, анализа, мониторинга рисков
The Cadbury and the Combined Code	Стандарт аналогичен COSO. Основной акцент сделан на процесс внутреннего контроля и аудита
The Criteria of Control Board (CoCo)	Аналог COSO, предлагающий двадцать параметров эффективного внутреннего аудита, разбитых на четыре группы: возможность, обязательство, мониторинг и обучение
The Control objectives for information and related technologies (Cobit)	Устанавливает общие основы безопасности и контроля в сфере информационных технологий на международном уровне
BASEL II	Регламентирует управление рисками в банковском бизнесе, при этом ряд положений может быть применен и к другим отраслям

Необходимо отметить, что в связи с выпуском нового стандарта ISO 31000 Risk management – Principles and guidelines [113], поддержка организацией FERMA стандарта AIRMIC/IRM/ALARM Risk Management Standard была прекращена, однако никто не запрещал его применять на практике, а потому он до сих пор активно применяется, хотя количество организаций, следующих ему, сократилось.

Из стандартов, приведенных в табл. 2.4, на практике чаще всего используются следующие [59; 141; 147]:

- 1) AIRMIC/IRM/ALARM Risk Management Standard;
- 2) the Australia/New Zealand Standard AS/NZS 4360:2004;
- 3) the COSO Enterprise Risk Management – Integrated Framework.

При выборе того или иного стандарта необходимо руководствоваться тем, что каждый из них имеет свои отличительные особенности.

Во-первых, стандарт AIRMIC/IRM/ALARM Risk Management Standard разработан специалистами по управлению рисками для постановки системы риск-менеджмента любой организации. Стандарт The Australia/New Zealand Standard AS/NZS 4360:2004 во многом совпадает с предыдущим стандартом, но порядок ключевых процессов управления рисками несколько иной. Стандарт the COSO Enterprise Risk Management – Integrated Framework ориентирован, прежде всего, на повышение достоверности отчетности организаций и проведение аудиторских проверок. Поэтому первый и второй стандарты наиболее удобны для большинства сотрудников организации, а третий – для внутренних аудиторов.

Во-вторых, стандарт AIRMIC/IRM/ALARM Risk Management Standard обладает четко определенной последовательностью действий по постановке системы управления рисками и содержит конкретные рекомендации. Это позволяет использовать его при постановке системы управления рисками неподготовленному сотруднику. Внедрением стандартов The Australia/New Zealand Standard AS/NZS 4360:2004 и the COSO Enterprise Risk Management – Integrated Framework, по нашему мнению, должны заниматься опытные специалисты в области риск-менеджмента.

В-третьих, у каждого из этих стандартов разные пользователи и разные законодательные требования. Стандарты AIRMIC/IRM/ALARM Risk Management Standard и Australia/New Zealand Standard AS/NZS 4360:2004 предназначены, прежде всего, для специалистов по управлению рисками и фактически представляет собой необязательные рекомендации. Стандарт The COSO Enterprise Risk Management – Integrated Framework является обязательным для публичных организаций в США.

Все эти стандарты, несмотря на существенные различия, имеют много общего:

- дают определения базовым понятиям системы управления рисками;
- представляют управление рисками как процесс, отмечая необходимость применения гибкого подхода при выполнении тех или иных этапов процесса;

- могут быть применимы к широкому спектру организаций и отраслей;
- определяют место управления рисками в общей системе управления организацией;
- признают, что риски обладают двойственной природой, выражающейся в положительных или отрицательных результатах;
- излагают этапы процесса управления рисками, давая краткое описание каждого из них.

Ключевым моментом при работе с этими стандартами является то, что любой из них может стать основой для создания системы риск-менеджмента организации. При этом если цель организации – размещение акций на Нью-Йоркской фондовой бирже, то, разумеется, необходимо выбрать the COSO Enterprise Risk Management – Integrated Framework. Если же цель организации – построить систему управления рисками для внутреннего пользования, то целесообразно использовать AIRMIC/IRM/ALARM Risk Management Standard и Australia/New Zealand Standard AS/NZS 4360:2004, хотя и эти стандарты определяют требования к раскрытию информации. БСРМ, которую мы создаем, соответствует многим положениям вышеописанных стандартов.

На текущий момент отечественные организации чаще стремятся разработать и внедрить такие документы, как «Политика по управлению рисками», «Отчет о рисках» и «Карта рисков» [24]. Это можно объяснить тем, что российские специалисты по управлению рисками стараются начинать разработку документальной базы не с подробных правил и регламентов управления рисками, а со своеобразной подстраховки процесса внедрения системы риск-менеджмента – фиксирования объекта управления через документы «Отчет о рисках» и «Карта рисков». В то же время, организации на начальном этапе внедрения системы риск-менеджмента необходимо обеспечить гибкость этого процесса посредством простых правил управления рисками, формализованных в виде документа «Политика по управлению рисками», носящего общий характер.

По нашему мнению, в БСРМ, наряду с вышеназванными документами, должны входить «Стратегия в области управления рисками», которая будет носить более детальный характер в отличие от «Политики по управлению рисками», и «Карточка описания риска» (рис. 2.8).



Рис. 2.8. Нормативная плоскость БСРМ

Рассмотрим каждый из представленных документов более предметно.

1. «Политика по управлению рисками» служит основным определяющим документом организации по управлению рисками [146]. Она должна представлять собой общий концептуальный документ, содержащий единые подходы и принципы управления рисками, а также закрепляющий основные положения культуры риска.

Документ «Политика по управлению рисками» должен быть утвержден главным исполнительным органом организации и пересматриваться либо по инициативе собственников организации, либо по инициативе главного исполнительного органа, но не по инициативе подразделения по управлению рисками и не по инициативе внутреннего аудита организации.

Наличие «Политики по управлению рисками» предоставляет организации следующие преимущества [93]:

- руководство организации формализует и доводит до работников свою позицию относительно рисков, это фокусирует внимание последних на вопросах управления рисками;
- служит основой при подготовке прочих нормативных документов.

2. Под «Стратегией в области управления рисками» (далее – «Стратегия») понимается комплекс направлений и способов использования средств, взаимосвязанных принципов и методов, направленных на достижение поставленных целей [19]. Основной целью «Стратегии» является внедрение в организации эффективного механизма идентификации, оценки и контроля рисков. «Стратегия» в рамках БСРМ должна включать в себя основные подходы при организации управления группами и частными рисками.

«Стратегию в области управления рисками», как и большинство других видов стратегий, необходимо формализовать [21] в виде отдельного нормативного документа, что позволит зафиксировать в ней все аспекты

управления. В качестве приложения к ней могут выступать различные документы, необходимые для достижения определенных целей «Стратегии», например, «Порядок управления операционными рисками».

«Стратегию в области управления рисками» утверждает главный исполнительный орган организации, а пересмотр производится либо по инициативе собственников, либо главного исполнительного органа организации, но не по инициативе подразделения по управлению рисками и не по инициативе внутреннего аудита организации, но с учетом предложений подразделения по управлению рисками организации.

3. Вся информация, полученная в ходе качественного и количественного анализа рисков, должна быть записана [116]. Процесс записи полученных данных называется описанием рисков, а документы, в которые заносятся сведения, называются «Карточка описания риска» и «Отчет о рисках».

Описание рисков должно быть максимально подробным и выполнено в определенном формате, что позволит упростить дальнейшую работу с рисками [146]. Если принимать во внимание последствия и вероятность каждого из рисков, то надлежащий формат описания рисков даст возможность расставить приоритеты и выделить те риски, подробное изучение которых требуется.

Таблица 2.5

**Карточка описания риска**

<i>№ п/п</i>	<i>Наименование блока</i>	<i>Блок для заполнения</i>
1	Наименование риска	Идентификационный признак или номер риска
2	Основные структурные элементы риска	Факторы, источник и причины рисков событий
3	Описание риска	Качественное описание событий, их масштаба, типа, количества и сферы воздействия
4	Классификационная группа риска	Стратегический, финансовый, операционный, репутационный, юридический
5	Заинтересованные лица	Заинтересованные лица и их ожидания
6	Количественное / качественное определение риска	Существенность и вероятность / возможность
7	Данные о потерях	Аналогичные рискованные события, описания потерь предшествующих периодов

8	Допустимость и приемлемость риска	Потенциальные убытки и финансовое воздействие риска. Цена риска. Вероятность и объем потенциальных убытков / прибылей. Цель (цели) управления рисками и желаемый уровень исполнения поставленных задач. Склонность к риску
9	Механизмы управления и контроля над рисками	Первичные средства управления рисками, действующие в настоящее время. Степень надежности существующих механизмов контроля над рисками. Существующие протоколы учета и анализа контроля над риском
10	Возможности для улучшения	Рекомендации по снижению риска. Время, необходимое для внедрения рекомендаций. Лица, ответственные за улучшение

Стандарт FERMA [119] предлагает свой вариант «Карточки описания риска». Нами доработан этот вариант с учетом особенностей БСРМ, в частности добавлен раздел об основных содержательных компонентах риска, рассмотренных в главе 1 (табл. 2.5). Сделано это для того, чтобы можно было понять, с учетом каких факторов, источников и причин рисков событий риск-менеджер принимал решения по управлению рисками.

Информация, содержащаяся в «Карточке описания риска», переносится в «Отчет о рисках». Стандарты FERMA [116] и ISO 31000 [113, 152] не задают форму «Отчет о рисках», но задают требования к нему и предусматривают формирование его в двух вариантах для разных категорий пользователей:

1) «Отчет о рисках» для внутренних пользователей может быть представлен в виде таблицы с описанием рисков. На основании рекомендаций стандарта FERMA [119] нами разработана форма «Внутренний отчет о рисках (упрощенный)» (табл. 2.6).

Таблица 2.6

#### Внутренний отчет о рисках (упрощенный)

Номер на легенде	Наименование риска	Описание риска	Вероятность, %	Ущерб, руб.

В случае необходимости, например по итогам разработки мероприятий управления рисками, собственникам организации или главному исполнительному органу может быть представлена форма «Внутренний отчет о рисках (расширенный)» (табл. 2.7).



**Внутренний отчет о рисках (расширенный)**

<i>Номер на легенде</i>	<i>Наименование риска</i>	<i>Возможные мероприятия по управлению риском</i>	<i>Ориентировочная стоимость мероприятий, руб.</i>
<i>Текущее значение риска, руб.</i>	<i>Остаточный риск, руб.</i>	<i>Изменение математического ожидания, руб.</i>	<i>Отношение изменения к стоимости мероприятий</i>

2) «Отчет о рисках» публичных компаний для внешних пользователей должен отвечать требованиями законодательства. В России действует Приказ ФСФР «Об утверждении положения о раскрытии информации эмитентами эмиссионных ценных бумаг» от 10 октября 2006 г. № 06-117/пз-н, в котором указано, что проспект ценных бумаг должен содержать подробный анализ факторов риска, в частности отраслевых, страновых и региональных, финансовых, правовых, а также рисков, связанных с деятельностью эмитента. Кроме того, должна быть описана политика эмитента в области управления рисками.

В зарубежных странах принимают собственные правила по раскрытию информации в «Отчете о рисках» для внешних пользователей [119], а именно:

- методы контроля, в особенности касающиеся сферы ответственности в вопросе управления рисками;
- процессы, использовавшиеся для идентификации рисков, и то, каким образом они рассматриваются в рамках систем управления рисками;
- первичные системы контроля, предназначенные для управления значительными рисками;
- существующие системы мониторинга и обзора;
- любые значительные недостатки, выявленные системой, или недостатки самой системы вместе с мерами, предпринятыми компанией для исправления ситуации.

Заметим, что разработанная нами форма «Внутренний отчет о рисках (расширенный)» (табл. 2.7) нуждается всего лишь в незначительной доработке для соответствия требованиям внешних отчетов зарубежных стран.

4. «Карта рисков» содержит информацию о вероятности и последствиях каждого индивидуального риска из «Отчета о рисках» организации и позволяет проводить быстрое и удобное сопоставление величины рисков со склонностью к рискам всей организации.

Наиболее часто используемым вариантом построения «Карты рисков», если необходимо провести качественный анализ, является двухмерный график, где по оси «Х» откладывается шкала последствий (ущерба), а по оси «У» – возможность или вероятность. Риск

размещается в точку пересечения его возможности или вероятности и последствий.

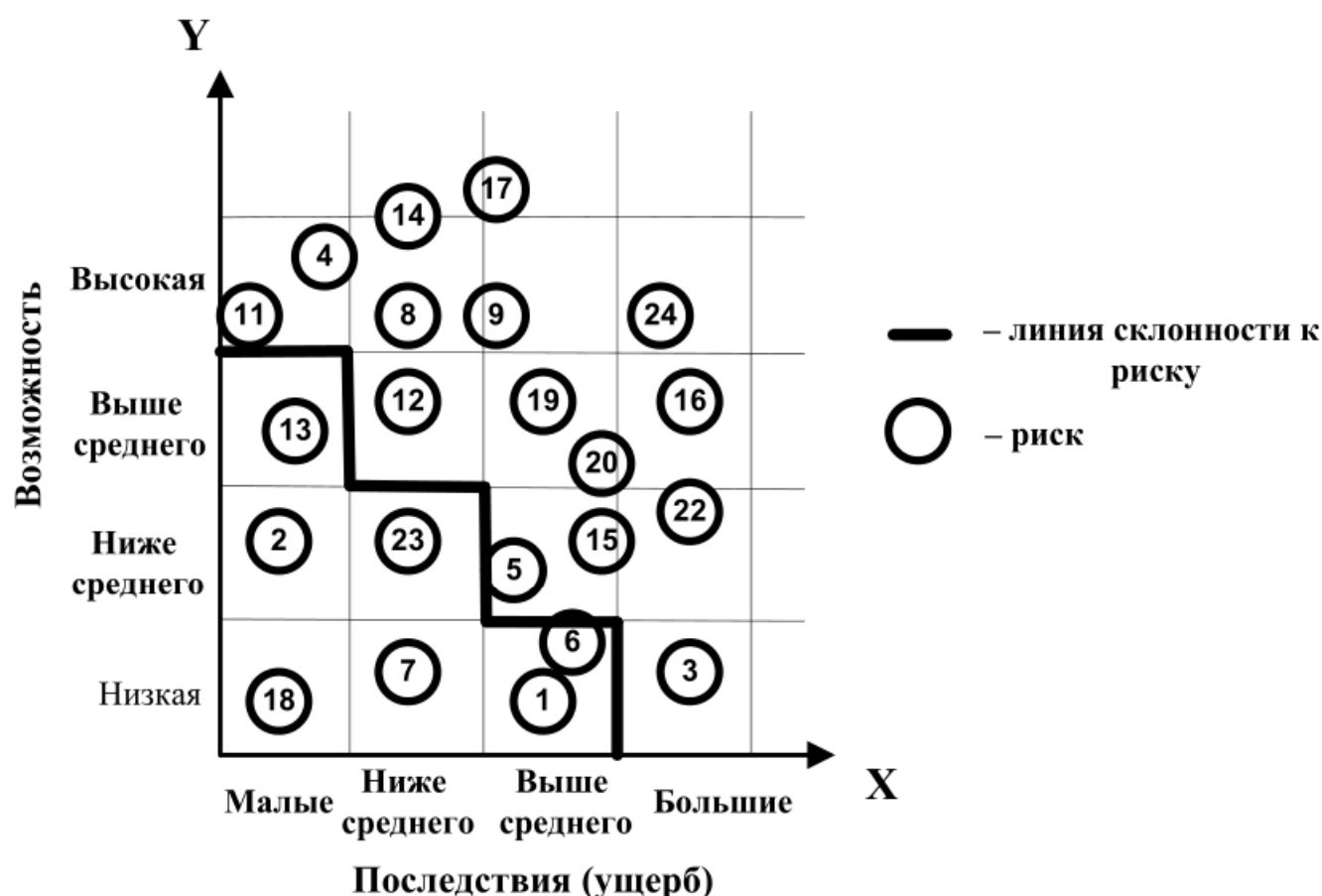


Рис. 2.9. Карта рисков качественной оценки

На «Карте рисков» размещается кривая линия, показывающая уровень склонности к риску. Риски, которые находятся выше данной кривой, считаются выше желаемых, а риски, расположенные ниже границы, воспринимаются как приемлемые. Разумеется, что в первую очередь должны разрабатываться программы по управлению рисками, находящимися выше кривой. Риски, расположенные ниже линии склонности, управляются в рабочем порядке.

Наряду с двухмерной «Картой рисков» может быть построена трехмерная карта, показывающая динамику изменения рисков с течением времени или различные сценарии развития событий. «Карта рисков» может быть построена либо для всей организации, либо для какого-либо подразделения. Кроме того, «Карты рисков» могут быть составлены для всех направлений деятельности организации или для отдельного проекта [51].

Наиболее простая «Карта рисков» возникает для качественного анализа. В этом случае шкалы возможности и последствий (ущерба) делятся на 2, 3, 4 или другое количество элементов, а каждый риск обозначается соответствующим ему порядковым номером и размещается в соответствующем квадрате. Выбор линии склонности к риску осуществляется решением руководства организации (рис. 2.9).

Если был проведен количественный расчет рисков, то карта будет иметь другой вид. В этом случае линия склонности будет выглядеть как

кривая. Шкала по вероятности всегда будет линейной. Шкала по последствиям (ущербу) может быть либо линейной (матрица слева на рис. 2.10), либо логарифмической (матрица справа на рис. 2.10).

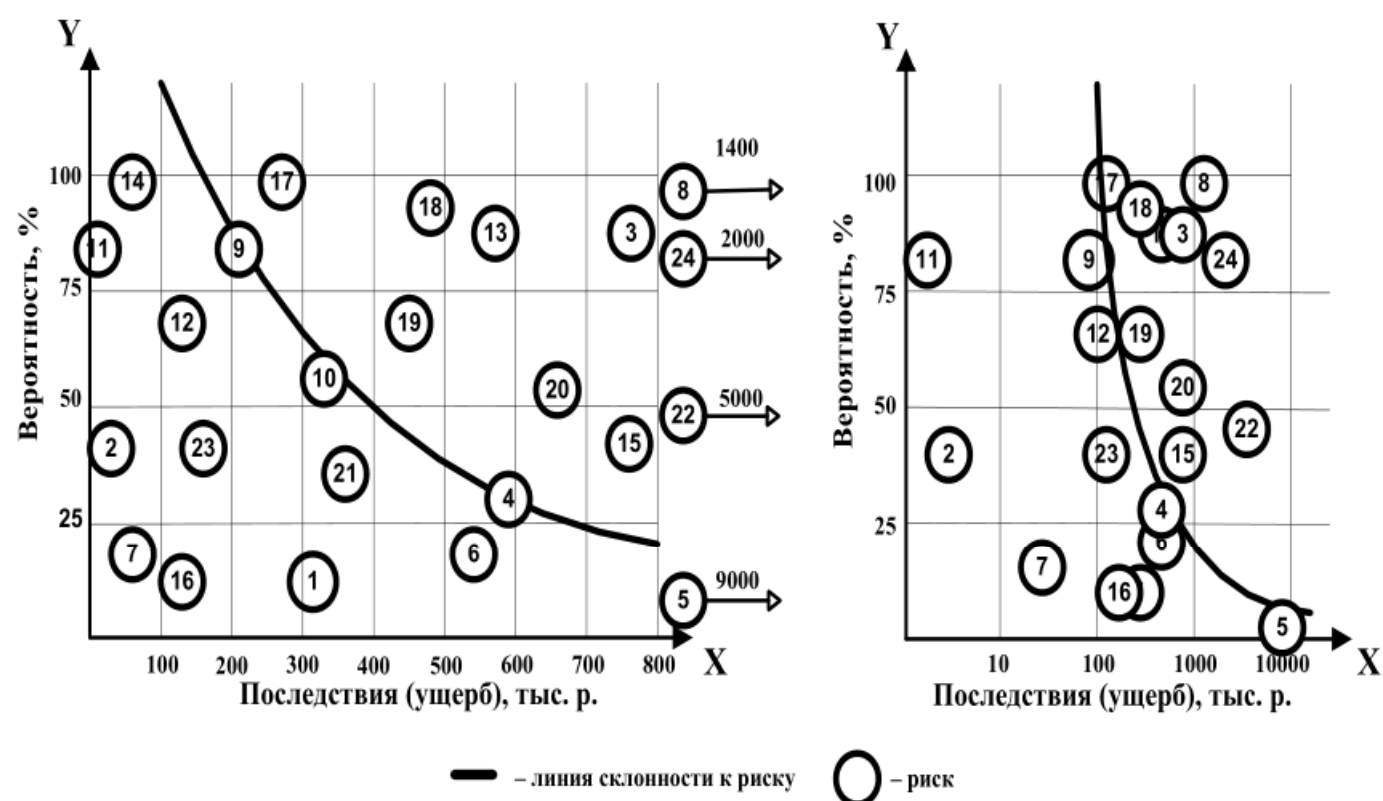


Рис. 2.10. Виды карт рисков количественной оценки

Более наглядной является «Карта рисков» с линейной шкалой, потому что на ней, в отличие от карты с логарифмической шкалой, одинаковые расстояния имеют и одинаковые масштабы. С учетом того, что склонность к риску ( $LfR$ ) является величиной постоянной, линия склонности к риску всегда будет гиперболой, строящейся по следующей формуле:

$$LfR = p(LfR) \cdot c(LfR), \quad (2.18)$$

где  $p(LfR)$  – вероятность, соответствующая заданному уровню склонности к риску и ущербу;  $c(LfR)$  – последствия (ущерб), соответствующие заданному уровню склонности к риску и вероятности.

«Карта рисков» должна разрабатываться, периодически обновляться и выноситься на рассмотрение уполномоченного органа в соответствии со сроками, закрепленными во внутренних документах организации. По нашему мнению, она должна пересматриваться не реже одного раза в месяц. «Карта рисков» помогает [51]:

- определить склонность к рискам по всем направлениям деятельности организации;
- выявить критически важные риски, смягчить их и обеспечивать управление ими;
- разработать динамическую модель рисков организации, влияющих на достижение целей.

## **Выводы к главе 2**

1. Сформированы и предложены теоретические основы системы управления рисками деятельности организации, включающие в себя свойства, цели и задачи, а также правила и принципы управления рисками – все это объединено в рамках основополагающей плоскости базисной системы риск-менеджмента.

2. Выявлены основные стороны и лица, принимающие участие в управлении рисками деятельности организации (собственники или их представители; топ-менеджеры; специалисты всех структурных подразделений, занимающиеся каждодневной реализацией мероприятий по управлению рисками; подразделение внутреннего аудита; подразделение по управлению рисками), определены их полномочия. Предложены рекомендации, направленные на формирование подразделения по управлению рисками, а также по должностным обязанностям специалистов данного подразделения. Установлены механизмы выявления и создания культуры риска как одного из ключевых элементов эффективной системы управления рисками.

3. Установлен комплекс процедур, состоящих из выявления, измерения и оценки рисков деятельности организации, разработки и реализации мероприятий управления ими, а также мониторинга, оценки эффективности базисной системы риск-менеджмента, контроль ее исполнения и управления информацией. Предложены методические рекомендации по вопросам очередности и осуществления данных процедур.

### Глава 3. ПОРЯДОК УПРАВЛЕНИЯ ОПЕРАЦИОННЫМИ РИСКАМИ В РАМКАХ БАЗИСНОЙ СИСТЕМЫ РИСК-МЕНЕДЖМЕНТА

#### 3.1. основополагающие аспекты управления операционными рисками

Хозяйственная деятельность компании – это оперативно-организационная деятельность по осуществлению операций обмена товарно-материальных ценностей в целях удовлетворения потребностей населения и получения прибыли. Как правило, цель хозяйственной деятельности представляет собой достижение наиболее высоких темпов роста, измеряемых через величины продаж, и ряд исследований, проведенных во многих странах на протяжении последних десятилетий, показали, что действительно такая цель может стать доминирующей. В этом контексте, на наш взгляд, особое внимание необходимо уделять организации управления операционными рисками, поскольку именно они являются одними из наиболее опасных [46; 98; 139].



Рис. 3.1. Схема осуществления разработки, контроля и реализации стратегического управления организации

При этом одним из решающих факторов эффективности и конкурентоспособности организации является проблема формирования системы взаимоотношений между менеджерами, акционерами и другими заинтересованными лицами, которые влияют на систему управления, в том числе на риск-менеджмент (рис. 3.1).

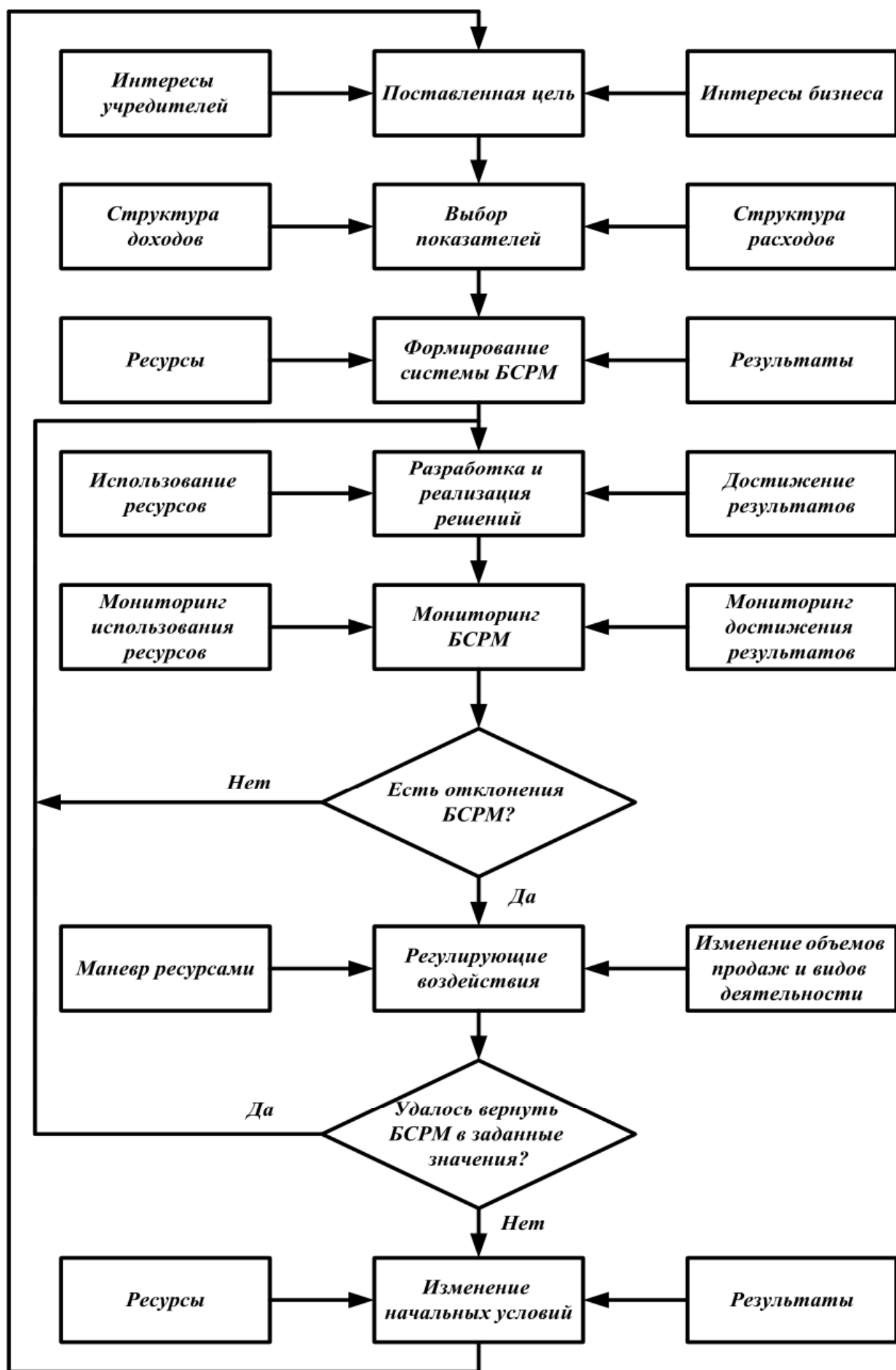


Рис. 3.2. Схема разработки, контроля и изменения параметров стратегического управления организацией

Хозяйствующему субъекту необходимо создать такую систему управления операционными рисками, помогающую определить достижение стратегических и тактических целей, использование которой дает возможность достигнуть целевых ориентиров, обосновать выбор стратегии функционирования и развития организации, а также осуществлять контроль ее исполнения (рис. 3.2) [9].

Можно назвать основные причины, мешающие созданию эффективного подхода к организации управления операционными рисками:

- операционные риски трудно поддаются определению;
- порядок сбора сведений об операционных потерях и событиях, связанных с операционным риском, либо отсутствует, либо представлен нечетко;
- внимание в большей степени уделяется стороне риска, связанной с убытками;
- применение математических моделей для управления операционными рисками ограничено особенностями реализации рисков событий [135].



Рис. 3.3. Аспекты порядка управления операционными рисками

Принимая во внимание указанные проблемы, нами разработан Порядок управления операционными рисками (далее – ПУОР), в рамках которого они могут быть решены, кроме того, сохранен элемент универсальности, необходимый для соответствия требованиям БСРМ. В основу ПУОР положены идеи Базельского комитета по банковскому надзору [106; 107] (с пониманием того, что эти идеи ориентированы на финансовый сектор экономики, а потому требуют доработки), а также

отечественных и зарубежных специалистов (К. В. Астахова [3], И. С. Крапчатова [46], А. Ю. Рогачев [79], В. Azvine [105], А. Н. Edmiston [117]). Необходимо учитывать, что ПУОР нуждается в последующей доработке для адаптирования к особенностям ведения деятельности организациями реального сектора экономики на территории Российской Федерации.

Кроме того, нами рассмотрены основополагающие, организационные и процедурные аспекты управления операционными рисками (рис. 3.3).

Как нам представляется, в ПУОР должны быть закреплены критерии отнесения рисков к классификационной группе операционных рисков. Это достигается формализацией следующих аспектов.

1. Определение категорий «операционный риск» и «операционное рисковое событие».

Таблица 3.1

**Факторы операционных рисков**

<i>Фактор риска</i>	<i>Критерии отнесения к факторам риска</i>
1	2
Бизнес-процессы	<ul style="list-style-type: none"> <li>– возможные недостатки в структуре и организации бизнес-процессов;</li> <li>– взаимосвязанность операций, зависимость сроков проведения и конечного результата операции от результатов и сроков проведения другой операции;</li> <li>– технологическая сложность и объемы проводимых операций;</li> <li>– недостаточная формализация порядка проведения операций;</li> <li>– частота использования экспертных оценок и субъективных суждений при принятии управленческих решений, предоставление завышенных полномочий работникам по принятию решения о проведении операции и определению ее рискованности;</li> <li>– новизна продукции и применяемых технологий;</li> <li>– отсутствие текущего контроля эффективности и рискованности проводимых операций</li> </ul>
Системы	<ul style="list-style-type: none"> <li>– низкие эффективность и работоспособность технических и информационных систем, обеспечивающих деятельность организации;</li> <li>– высокая зависимость результата деятельности организации от работоспособности информационных, коммуникационных или прочих обеспечивающих систем;</li> <li>– высокая загруженность систем, обеспечивающих деятельность организации, работа на пределе допустимых мощностей</li> </ul>



1	2
Персонал	<ul style="list-style-type: none"> <li>– отсутствие, недостаточность или неполнота имеющихся утвержденных инструктивных документов, регламентирующих должностные обязанности сотрудников;</li> <li>– низкая квалификация и некомпетентность персонала;</li> <li>– низкое качество подбора персонала (отсутствие установленных критериев квалификационных и личностных характеристик сотрудников в зависимости от содержания работы и объема ответственности, и т. д.);</li> <li>– высокая зависимость результата проводимой операции от эффективности работы персонала;</li> <li>– низкая взаимозаменяемость работников, замкнутость операций на отдельных сотрудниках, их знания и квалификацию</li> </ul>
Внешняя среда	<ul style="list-style-type: none"> <li>– социальная обстановка в местах ведения деятельности организации;</li> <li>– проведение мероприятий по предотвращению злоумышленных действий внешними лицами с целью причинения вреда организации или извлечения личной выгоды;</li> <li>– наличие охранных и противопожарных систем;</li> <li>– степень готовности к действиям в экстренных ситуациях (отсутствие детальных планов действий в штатных ситуациях, отсутствие резервных площадей для переноса деятельности организации в случае возникновения чрезвычайных ситуаций; отсутствие резервных технических и информационных систем и т. д.)</li> </ul>

Определение операционного риска было сформулировано нами ранее в главе 1, поскольку необходимость в нем должна была возникнуть далее – при составлении ПУОР. Согласно этому определению, источником операционного риска является область взаимодействия людей, процессов и технологий, участвующих в деятельности организации.

Под операционным рисковым событием мы понимаем событие, обусловленное операционным риском, т. е. повлекшее или способное повлечь за собой потери и произошедшее по причине ошибочности или сбоя внутренних процессов, действий людей или систем или по причине внешних событий, за исключением неблагоприятного для организации применения норм действующего законодательства. К рисковым событиям следует относить, например, нарушение регламента процедуры выполнения бизнес-процесса. В то же время к ним не относят расходы на улучшение процедур контроля, проведение превентивных мероприя-

тий, повышение качества продукции, инвестирование средств в новые производственные и информационные системы.

## 2. Основные факторы и источники операционных рисков.

По нашему мнению, структурирование риска является ключевым моментом в процессе осознания природы риска и возможностей управления им. Для этого необходимо сформировать классификацию основных содержательных компонентов риска, например факторов и источников, а также определить примерные критерии отнесения частных факторов и источников рисков к классификационным группам.

Учитывая сущность операционных рисков, в исследовании были выявлены рискообразующие факторы, которые влияют на величину и вероятность проявления операционных рисков, и приведем в табл. 3.1 их классификационные группы.

Таблица 3.2

### Классификация источников операционных рисков

<i>Источник риска</i>	<i>Критерии отнесения к источникам риска</i>
Бизнес-процессы	<ul style="list-style-type: none"> <li>– невозможность проведения операции или ошибки при ее проведении по причине неэффективности или ошибочности организации бизнес-процессов;</li> <li>– ущерб, нанесенный контрагентам по вине организации в ходе осуществления последним своей профессиональной деятельности</li> </ul>
Системы	– техническая невозможность проведения операций в рамках информационных систем (вследствие сбоя в работе оборудования, программного обеспечения, нарушений в работе каналов связи и т.д.)
Персонал	<ul style="list-style-type: none"> <li>– намеренное искажение отчетности о проводимых операциях;</li> <li>– проведение операций от лица организации в личных интересах;</li> <li>– ошибки в действиях работников вследствие их недостаточной квалификации, небрежности, недобросовестного исполнения должностных обязанностей</li> </ul>
Внешняя среда	<ul style="list-style-type: none"> <li>– умышленные противоправные действия внешних лиц, например кража, мошенничество, грабеж, вандализм, подделка платежных документов, компьютерные преступления, направленные на причинение ущерба организации или извлечение личной выгоды;</li> <li>– изменения в макроэкономических условиях деятельности организации, не относящиеся к стратегическим рискам;</li> <li>– события стихийного характера, например стихийные бедствия, пожар, затопление, землетрясения, не относящиеся к стратегическим рискам</li> </ul>

Выделение группы факторов риска проведено с тем, чтобы показать возможность их применения для анализа деятельности любой организации реального сектора экономики, как пример того, что любой частный фактор риска можно отнести к одной из четырех классификационных групп. Как было указано ранее в главе 1, в целях идентификации, оценки и мониторинга операционных рисков и их источников, в зависимости от направленности влияния факторов риска на организацию, их необходимо классифицировать на внутренние и внешние. Полагаем, что при этом источники операционного риска в зависимости от принадлежности факторов риска к различным компонентам или условиям процессов организации необходимо классифицировать на бизнес-процессы, персонал, системы и внешнюю среду (табл. 3.2).

Следует заметить, что совпадение наименований классификационных групп факторов и источников операционных рисков мы объясняем тем фактом, что одно явление может являться и источником, и фактором разных рисков одновременно, при этом источники рисков выделяются из состава факторов, поскольку понятие «фактор риска» шире, чем понятие «источник риска». Более того, формирование разных классификационных групп факторов и источников риска может запутать пользователя информации и тем самым предопределить принятие неверного решения.

### 3. Классификация рисков событий.

Рисковые события можно сгруппировать в зависимости от характера проявления и влияния на результат деятельности организации в рамках БСРМ (табл. 3.3).

Таблица 3.3

#### Классификация рисков событий

<i>Группа рисков события</i>	<i>Описание</i>
1	2
Внутреннее мошенничество	Злоупотребления или противоправные действия, осуществляемые работниками или с участием работников, в т. ч. совершенные в целях извлечения личной выгоды или нанесения ущерба организации
Внешнее мошенничество	Противоправные действия по отношению к организации внешними лицами
Ущерб, нанесенный материальным активам	Повреждение или утрата основных средств и других материальных активов по причинам стихийного или случайного характера (в т. ч. в результате актов терроризма, стихийных бедствий, пожара)
Нарушения, связанные с охраной труда, безопасностью рабочих мест и окружающей среды	Нарушение действующего законодательства в ходе осуществления деятельности организацией, внутренних норм безопасности рабочих мест, охраны труда и окружающей среды

1	2
Нарушение деятельности или функционирования систем	Выход из строя, сбой, отказ оборудования и систем, в т. ч. поломка оборудования и вычислительной техники, систем связи
Нарушения или ошибки, связанные с выполнением операций и допущенные в отношениях с поставщиками	Ненадлежащая организация деятельности, ошибки управления и/или исполнения, в т. ч. в результате несовершенства организации внутренних процессов, процедур или информационных потоков, отсутствия (не оптимального выбора) системы защиты и/или доступа к информации

Группировка является переработанной версией классификации рисков событий, предложенной Базельским комитетом по банковскому надзору [107], и представляет собой первый уровень многоуровневой классификации рисков событий (см. прил. 2).

#### 4. Формы проявления операционных рисков.

Таблица 3.4

#### Классификация операционных потерь

<i>Вид операционных потерь</i>	<i>Описание</i>
Снижение стоимости активов	Прямое уменьшение стоимости активов, в т. ч. вследствие противоправных или ошибочных действий работников и/или внешних лиц
Списание материальных активов	Потери, связанные с досрочным списанием (выбытием) материальных активов, в т. ч. уничтожение или прямое уменьшение стоимости материальных ценностей и активов организации вследствие преднамеренных действий работников или внешних лиц, событий стихийного и случайного характера
Внесудебные выплаты	Операционные потери в виде денежных выплат внешним лицам, а также работникам в целях компенсации им во внесудебном порядке убытков, понесенных ими по вине организации
Восстановительные затраты	Затраты на восстановление хозяйственной деятельности и устранение последствий рисков событий случайного характера (ошибки, аварии, стихийные бедствия и других аналогичные обстоятельства)
Прочие потери	Операционные потери, которые невозможно отнести ни к одной из вышеуказанных категорий

Прямым результатом проявления операционного риска являются операционные потери, которые ухудшают результаты деятельности организации. Чтобы эффективно управлять операционными рисками, необходимо их подразделять на прямые и косвенные. При этом под пря-

мыми потерями следует понимать уменьшение текущих доходов организации, а под косвенными – уменьшение ее потенциальных доходов вследствие недостатков при ведении операционной деятельности, а также возможных потерь в будущем в силу уже совершившихся рискованных событий [103]. Оптимальный вариант классификации операционных потерь, с нашей точки зрения, представлен в табл. 3.4.

### **3.2. Организационные аспекты управления операционными рисками**

Организационная структура управления операционными рисками, а также степень централизации и детализация исполнения функций зависят от специфики конкретного хозяйствующего субъекта, условиями ведения бизнеса отдельными подразделениями, профиля деятельности и функциональных взаимосвязей внутри организации. Как уже отмечалось выше, управление риском – это, прежде всего, система мер, позволяющая при правильном подходе к ее реализации максимально уменьшить размер упущенной прибыли или ограничить ее определенной величиной в случае неблагоприятного для организации развития рыночной ситуации.

Реализация ПУОР предполагает вовлечение в этот процесс всех направлений деятельности и структурных подразделений организации и должно охватывать:

- все категории операционных рисков;
- все направления бизнеса;
- все территориальные и структурные подразделения компании.

По нашему мнению, в ПУОР необходимо закрепить четыре основных организационных аспекта.

#### **1. Цели и задачи управления операционными рисками.**

Основной целью ПУОР является внедрение эффективного механизма идентификации, измерения, оценки, управления и мониторинга рисков, не относящихся к стратегическому, финансовому, юридическому и репутационному рискам. Данная цель достигается выполнением следующих задач:

- идентификация источников операционного риска (как в существующих, так и во внедряемых новых продуктах, операциях, автоматизированных системах и технологиях);
- выявление и регулирование концентрации операционного риска в разрезе направлений деятельности, операций и подразделений;
- осуществление количественной оценки операционного риска;
- анализ и контроль влияния операционного риска на устойчивость организации и результаты деятельности;
- выбор источников покрытия операционного риска и оценка их достаточности;
- разработка, реализация и оценка эффективности методов нейтрализации или снижения уровня операционного риска;

– мониторинг и контроль величины операционного риска, привлечение внимания руководства и подразделений к задачам управления и контролю операционных рисков.

## **2. Основные принципы управления операционными рисками.**

Рекомендации Базельского комитета по банковскому [106, 107] надзору содержат в себе ряд принципов, которыми необходимо руководствоваться при построении и совершенствовании процедур управления операционными рисками. Поскольку рекомендации рассчитаны на банковскую деятельность и рассматривают юридические риски в составе операционных, то принципы, содержащиеся в них, не могут быть полностью применены в рамках БСРМ.

Принимая во внимание это обстоятельство, нами сформулированы следующие принципы БСРМ, которые должны быть в ПУОР:

– управление операционными рисками должно обеспечивать рассмотрение операционного риска как отдельную и подлежащую управлению и контролю категорию риска. Основные требования, предъявляемые ко всем аспектам управления операционным риском, должны утверждаться и регулярно пересматриваться высшим исполнительным органом. Порядок, процедуры контроля и нейтрализации основных видов операционных рисков должны быть установлены соответствующими внутренними нормативными актами;

– управление операционными рисками должно основываться на едином определении операционного риска, единых принципах идентификации, оценки, мониторинга и контроля операционного риска, а также мерах по его нейтрализации;

– управление операционными рисками должно охватывать всю деятельность организации, а не отдельные ее направления;

– идентификация и оценка операционных рисков должны применяться по отношению ко всем существенным продуктам, операциям, процессам и системам организации. До начала проведения новых операций, внедрения новых продуктов, процессов или систем должна осуществляться их адекватная оценка на предмет величины связанного с ними операционного риска;

– управление операционными рисками должно на систематической и централизованной основе обеспечивать сбор данных, связанных с операционным риском. Механизм оценки величины операционного риска должен являться составной частью БСРМ. Результаты, полученные в ходе данной оценки, должны использоваться при осуществлении мониторинга и контроля величины операционного риска организации;

– управление операционными рисками должно предусматривать регулярный мониторинг состава и величины операционного риска, а также связанных с ним фактических и потенциальных потерь. На основе результатов мониторинга должна формироваться отчетность, обеспечивающая возможность принятия решений по управлению величиной и структурой операционного риска, с учетом прочих имеющихся у организации рисков. Отчеты о величине операционного риска должны на

регулярной основе представляться руководителям структурных подразделений, руководителям, курирующим их деятельность, и главному исполнительному органу в составе отчетности о рисках;

– функции и полномочия по управлению операционным риском должны быть четко сформулированы и распределены между структурными подразделениями. Должны существовать структурные подразделения, к функциям которых относятся реализация следующих мероприятий управления и контроля операционных рисков:

а) организация процедур внутреннего контроля операционных рисков;

б) разработка порядка идентификации, оценки, мониторинга и управления операционными рисками;

в) разработка проектов нормативных документов, устанавливающих порядок управления операционным риском;

г) разработка и внедрение внутренней методики оценки операционных рисков;

д) разработка и внедрение системы управленческой отчетности по операционным рискам;

е) контроль функционирования системы управления операционными рисками;

– порядок управления операционным риском должен быть формализован внутренними нормативными актами. Должен существовать механизм регулярного и независимого контроля соответствия процесса управления операционным риском по утвержденному набору документов, устанавливающих политику, порядок и процедуры управления операционными рисками, в том числе порядок принятия мер по устранению нарушений;

– управление операционными рисками должно включать в себя утвержденные планы действий и мероприятий на случай наступления чрезвычайных событий, обеспечивающие осуществление деятельности организации без перерывов, а также минимизацию потерь в случае наступления существенных сбоев в операционной работе.

Принципы, указанные выше, соответствуют общим принципам БСРМ и дополняют их по специфичным вопросам управления операционными рисками.

### **3. Участники процедур управления операционными рисками.**

Участниками процесса управления операционными рисками в ходе осуществления деятельности организации являются:

– топ-менеджеры;

– подразделение внутреннего аудита;

– подразделение по управлению рисками;

– прочие структурные подразделения, обуславливающие возникновение операционных рисков.

В целях эффективного управления операционными рисками необходимо распределить функции и полномочия коллегиальных органов и структурных подразделений. Представим сформированное нами оптимальное распределение полномочий (табл. 3.5).

Таблица 3.5

**Распределение функциональных обязанностей**

Участники	Функции, полномочия, компетенция и механизм их реализации
1	2
Топ-менеджеры	<ul style="list-style-type: none"> <li>– утверждение правил в области управления операционными рисками;</li> <li>– утверждение методики оценки риска;</li> <li>– утверждение нормативно-методологических документов, устанавливающих порядок оценки величины операционного риска;</li> <li>– принятие решений о мерах по управлению операционными рисками на основании предложений подразделения внутреннего аудита, подразделения по управлению рисками</li> </ul>
Подразделение внутреннего аудита	<ul style="list-style-type: none"> <li>– согласование методики и порядка оценки и мониторинга операционного риска;</li> <li>– анализ процедур управления операционными рисками, обеспечение контроля их адекватности;</li> <li>– выявление нарушений и недостатков в работе подразделений путем проведения ревизий и проверок, контроль их исправления;</li> <li>– аудит и утверждение разрабатываемых подразделениями внутренних инструкций по проведению операций, контроль их соблюдения;</li> <li>– идентификация источников операционных рисков, выявление факторов, влияющих на величину операционного риска, подготовка предложений по их минимизации;</li> <li>– выявление областей операционной деятельности с уровнем контроля, не соответствующим присутствующему в операциях риску;</li> <li>– принятие мер по совершенствованию систем контроля;</li> <li>– проверка адекватности и корректности методов оценки величины операционного риска и формируемой отчетности об операционных рисках;</li> <li>– рассмотрение существующих, а также разрабатываемых и внедряемых процессов и систем на предмет оценки сопряженного с ними операционного риска;</li> <li>– оценка применяемых процедур управления операционным риском на предмет их эффективности и целостности воплощения;</li> <li>– представление в подразделение по управлению рисками сведений о произошедших или вероятных рискованных событиях</li> </ul>



1	2
Подразделение по управлению рисками	<ul style="list-style-type: none"> <li>– разработка правил в области управления операционными рисками;</li> <li>– разработка методики качественной и количественной оценки величины операционных рисков;</li> <li>– разработка порядка, процедур и методик мониторинга величины операционных рисков, а также соответствующих нормативных документов;</li> <li>– подготовка нормативных документов по порядку сбора и представления данных;</li> <li>– организация системы сбора данных о рисковых событиях и операционных потерях и формирование информационной базы данных;</li> <li>– координация деятельности структурных подразделений при управлении операционных рисков;</li> <li>– оценка и анализ операционного риска в соответствии с разработанной методикой;</li> <li>– организация и проведение мониторинга операционных рисков;</li> <li>– разработка, внедрение и подготовка отчетности, характеризующей уровень операционных рисков;</li> <li>– обеспечение применения единых подходов к методике измерения и оценки операционных рисков в различных структурных подразделениях;</li> <li>– подготовка предложений подразделению внутреннего аудита по вопросам идентификации, измерения, оценки, управления и мониторинга операционных рисков, а также его минимизации;</li> <li>– представление подразделению внутреннего аудита сведений о произошедших или вероятных рисковых событиях, а также рекомендаций по проверке операций и/или процессов, требующих проведения документальных проверок со стороны указанного подразделения;</li> <li>– организация и координация мероприятий, направленных на снижение операционного риска путем его страхования;</li> <li>– координация действий со страховщиками;</li> <li>– анализ финансового состояния страховой компании;</li> <li>– количественная оценка операционных рисков в целях информационного обеспечения управленческих решений;</li> <li>– анализ опыта управления операционными рисками и разработка предложений по совершенствованию соответствующей работы</li> </ul>

1	2
Прочие структурные подразделения, обуславливающие возникновение операционных рисков	<ul style="list-style-type: none"> <li>– идентификация присутствующих в операциях подразделения источников операционного риска и предварительная оценка величины потерь;</li> <li>– осуществление текущего, дополнительного и последующего контроля в соответствии с решениями руководства;</li> <li>– представление в подразделение по управлению рисками сведений о произошедших или вероятных рисковомых событиях, факторах и источниках риска</li> </ul>

В конечном итоге, алгоритм принятия управленческих решений по предотвращению и минимизации операционного риска в общем виде сводится к сравнению дополнительных затрат на реализацию предложенных мероприятий с возможными потерями вследствие наступления рисковомых событий. На основании этого сопоставления принимается решение об осуществлении или отказе от антирисковомых мероприятий.

### 3.3. Процедурные аспекты управления операционными рисками

Управление операционными рисками осуществляется посредством выполнения на регулярной основе процедур идентификации риска, оценки и мониторинга его величины, контроля его соответствия допустимым значениям [105].

Таблица 3.6

#### Основные процедуры управления операционными рисками

Процедура	Краткое содержание
1	2
Идентификация риска	Идентификация операционных рисков как событий, произошедших или могущих произойти в ходе выполнения операций и вызвавших или способных вызвать потери, которая осуществляется на основе утвержденной единообразной классификации рисков
Измерение риска	Измерение величины потенциальных потерь от наступления рисковомого события, которое производится на основе исторических данных о рисковомых событиях. Измерение вероятности возникновения рисковомого события в течение заданного временного интервала в будущем, с учетом текущих параметров операционной деятельности, влияющих на возможность возникновения рисковомого события, и существующего уровня внутреннего контроля

Оценка риска и уровень его контроля	Оценка риска с позиции его приемлемости для деятельности организации и необходимости принятия мер по управлению им. Оценка применяемого в отношении данного вида операций уровня внутреннего контроля (предварительного, текущего, последующего) на предмет его способности предотвратить возникновение такого рисковогó события
Реализация мероприятий	Принятие мер по предотвращению возникновения рисковогó события в будущем
Мониторинг	Осуществление мониторинга операций на предмет наличия операционного риска

Укрупненная структура процедур управления операционными рисками может быть представлена в виде последовательности мероприятий (табл. 3.6).

По нашему мнению, в ПУОР должно быть раскрыто следующее.

### **1. Подходы к идентификации операционных рисков.**

Систематическая идентификация источников операционных рисков, измерение их совокупной величины по всей деятельности и величины в разрезе отдельных направлений деятельности требует применения единообразной и последовательной методики анализа. Результаты измерения операционного риска должны давать возможность не только сравнения величины операционного риска с результатами количественной оценки стратегического, финансового, юридического и репутационного рисков, но и получения оценки совокупного риска деятельности организации в целом.

Идентификация и измерение операционного риска основываются на одном из нижеследующих базовых подходов, или их комбинации [100]:

– «сверху вниз» – объектами оценки и анализа являются выявленные фактические или потенциальные рисковогó события. Рисковогó события подразумеваются как конечные проявления операционного риска, рассматриваемые с вершины организационной структуры деятельности организации;

– «снизу вверх» – объектами анализа являются отдельные факторы и источники риска, а также сферы их взаимодействия (люди, процессы, технологии). В отличие от подхода «сверху вниз», который ориентирует на проявления риска, данный подход концентрирует внимание на исходных внешних и внутренних риск-факторах, точки взаимодействия, которых основывают базу для идентификации, оценки вероятности и возможных последствий операционных рисков. Целью анализа является определение перечня потенциально опасных событий, которые могут помешать достигнуть поставленных целей. Каждому рисковогó событию ставится в соответствие иерархическая, основанная на логике, структура предшествующих событий, обусловивших величину операционных потерь или вероятность их возникновения. На основе анализа данной иерархии формируется дерево причинно-следственных связей,

создающее базу для принятия решений по управлению операционными рисками.

По нашему мнению, подход «сверху вниз» эффективнее применять при работе с изученными рисками, по которым имеется статистическая база данных. В свою очередь, подход «снизу вверх» дает большую возможность для выявления новых операционных рисков, следовательно, его применение целесообразно при анализе новых направлений и сфер деятельности организации.

Возможными способами идентификации операционных рисков могут являться:

- анализ централизованно формируемой базы данных о внутренних рискованных событиях, а также рискованных событиях сторонних организаций;

- опросы и консультации с представителями структурных подразделений, осуществляющих операционную деятельность;

- регулярные процедуры самооценки, проводимые в рамках структурных подразделений, с использованием анкетирования или средств информационных технологий.

В основе идентификации операционных рисков лежит декомпозиция деятельности на отдельные операционные направления – бизнес-процессы.

## **2. Методы измерения и оценки операционных рисков.**

Считаем, что применяемые методики измерения и оценки операционных рисков должны позволять определять величины операционных рисков и средств, необходимых на управление ими, а также давать возможность принятия решений по перераспределению рисков, управлению капиталом и контролю его достаточности, по управлению эффективностью операций, с учетом уровня риска. Методики должны обеспечивать возможность проведения сравнения величины операционных рисков с величиной прочих рисков: стратегического, финансового, юридического и репутационного.

Измерение величины операционных рисков на практике производится следующими количественными методами [100]:

- в методах, основанных на анализе волатильности доходов, величина операционных рисков рассматривается как волатильность дохода деятельности организации, очищенная от составляющих, обусловленных прочими рисками (в рамках БСРМ – стратегическим, финансовым, репутационным и юридическим). Указанные методы имеют существенный недостаток – они не позволяют установить причины негативного отклонения дохода, а, следовательно, на основе полученных результатов предотвратить эти отклонения практически невозможно. На практике данные методы измерения могут быть полезны только при распределении средств под возможные потери в результате различных факторов риска [100];

- параметрические методы анализа исторических данных о рискованных событиях предполагают измерение величины операционного риска на основе расчетных параметров вероятностно-статистического распреде-

ления операционных потерь, при этом прогноз ожидаемых убытков делается на основе величины средних убытков, а неожиданных – на основе стандартного отклонения или иного доверительного интервала. Распределение вероятностей убытков может быть определено анализом отдельных рисков событий, групп событий и бизнес-процессов, а также анализом всех агрегированных фактических и потенциальных потерь в ходе осуществления деятельности организации. Неполнота или отсутствие данных о потерях внутри организации могут быть компенсированы использованием верифицированной информации из сторонних баз данных, масштабированной применительно к условиям операционной деятельности организации;

– при сценарных методах анализа разрабатываются вероятные сценарии возникновения рисков событий, способных оказать существенное влияние на финансовый результат деятельности организации. Сценарии разрабатываются централизованно экспертным путем, в том числе на основе анализа структуры бизнес-процессов, баз данных о рисковых событиях и т. д.

В случаях невозможности адекватного применения указанных выше методов о величине операционных рисков можно судить по ключевым индикаторам деятельности [105]. Выделяют три основные группы данных индикаторов:

– индикаторы текущей деятельности – максимально допустимое число произошедших за установленный период времени отдельных наиболее важных рисков событий, при превышении которого следует принимать меры по нейтрализации операционного риска. Рисковыми событиями в рамках данного метода может быть количество сорванных сделок и жалоб клиентов, показатели текучести кадров, время простоя или число сбоев работы и время простоя производственного оборудования и информационных систем, число ошибок проводок или сделок. Частота проведения мониторинга индикаторов деятельности может различаться в зависимости от их степени влияния на результаты деятельности организации;

– индикаторы эффективности контроля – показатели, характеризующие качество и эффективность существующих механизмов внутреннего контроля. Такими индикаторами могут являться число выявленных нарушений сотрудниками своих должностных обязанностей и полномочий, число сторнировочных записей по счетам бухгалтерского учета, неподтвержденных контрагентами сделок и т.д.;

– комплексные индикаторы риска – комбинации отдельных индикаторов деятельности и контроля, мониторинг которых должен осуществляться наиболее часто.

Все перечисленные индикаторы чаще всего используются для контроля операционной деятельностью организации. При появлении негативных сигналов от указанных индикаторов возрастает вероятность операционных рисков событий. Соответственно, можно снизить такую вероятную опасность, усилив контроль ситуации [100].

Наиболее распространенным качественным методом измерения рисков является метод оценочных листов, который имеет целью определение наиболее существенных факторов и источников операционного риска, связанных с текущими условиями деятельности организации, а также позволяет осуществлять мониторинг изменения уровня операционного риска в разрезе различных бизнес-процессов. Метод предполагает заполнение структурными подразделениями централизованно разрабатываемых опросных листов, содержащих несколько десятков вопросов на качественную оценку уровня риска.

Перечень вопросов покрывает аспекты вероятности и существенности фактических и потенциальных рисков событий, уровня применяемого внутреннего контроля, а также возможных мер, направленных на снижение вероятности рисков событий и величины потенциальных операционных потерь. Риски идентифицируются и оцениваются на основании единой классификации операционных рисков. Полученные агрегированные результаты анализируются на предмет выявления в бизнес-процессах наиболее подверженных операционному риску зон, с последующим принятием мер по их устранению.

### **3. Методы управления операционными рисками.**

Основными методами управления операционными рисками являются:

- применение процедур внутреннего контроля и аудита бизнес-процессов;
- установление ограничений по срокам и объемам операций;
- поддержание баланса между единоличным и коллегиальным принятием решений;
- страхование операционных рисков, связанных с профессиональной и хозяйственной деятельностью;
- снижение операционных рисков, связанных с бизнес-процессами, проводимыми сторонними организациями.

### **4. Методы организации сбора информации, используемой для оценки и мониторинга операционных рисков.**

Управление операционными рисками должно основываться на систематическом сборе сведений о рискованных событиях, факторах и источниках операционного риска, включая сведения о фактических потерях, связанных с операционными рисками.

Возможными источниками данных о рискованных событиях, необходимых для анализа и оценки операционных рисков, должны быть следующие сведения:

- структурных подразделений о фактических и потенциальных рискованных событиях и операционных потерях, обусловленных проведением операций;
- бухгалтерского учета о прямых и косвенных операционных потерях, связанных с идентифицированными рискованными событиями;
- рискованных событиях, имевших место в сторонних организациях и масштабированные с учетом особенностей операционной деятельности и систем внутреннего контроля. Источниками этих сведений могут быть

бизнес-партнеры, контрагенты, страховые компании, средства массовой информации.

Сбор сведений о рискованных событиях должен охватывать все основные направления деятельности организации, т.е. наиболее существенные для нее результаты и достижения поставленных стратегических целей. Порядок сбора и представления сведений должен быть установлен внутренними нормативными документами.

Сбор и представление сведений должны осуществляться структурными подразделениями регулярно, без временных разрывов, и основываться на идентификации рискованных событий, связанных со всеми проводимыми операциями, на основе утвержденной классификации операционных рисков в разрезе видов рискованных событий, бизнес-процессов и источников риска (рис. 3.4).

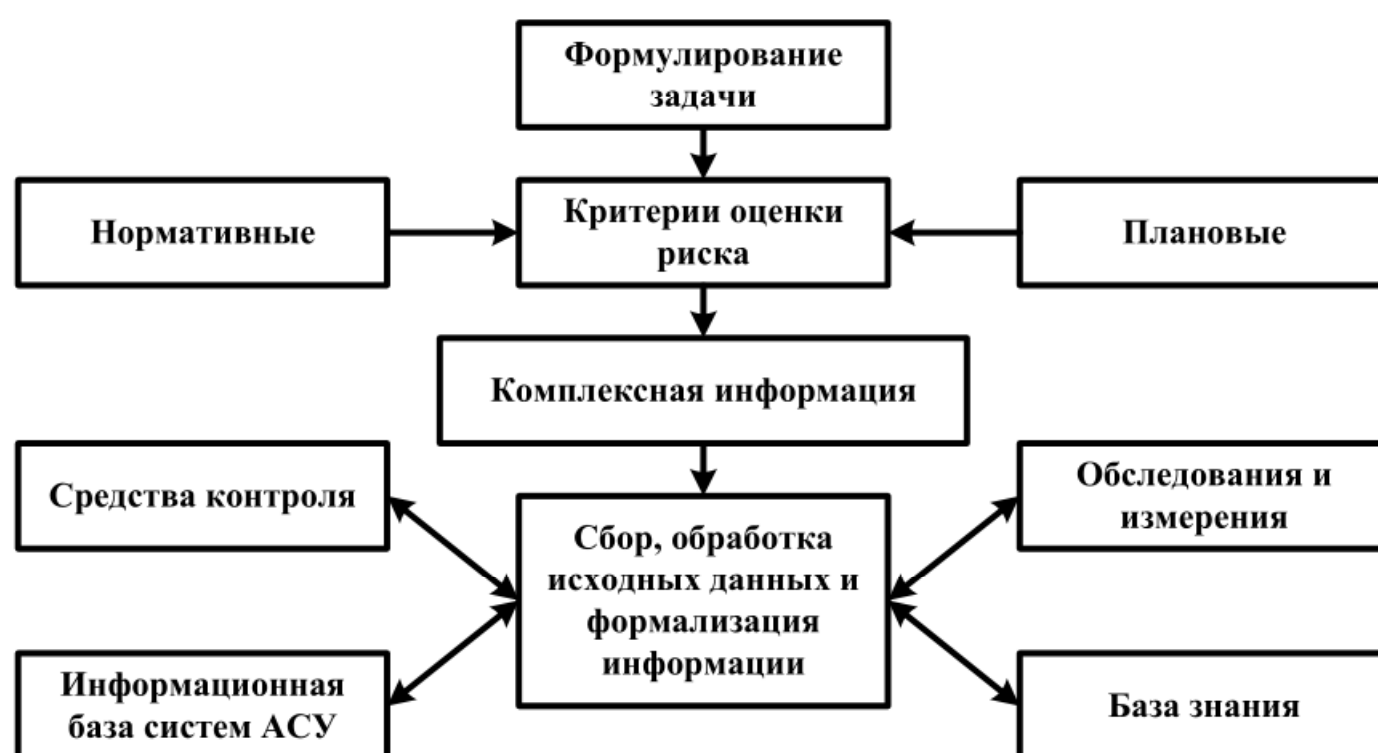


Рис. 3.4. Подготовка исходной информации

Представляемые в подразделение по управлению рисками сведения о рискованных событиях должны обладать достаточной детализацией для проведения их последующего анализа в целях определения величины и структуры риска в разрезе бизнес-процессов, структурных подразделений, временной структуры, географических мест возникновения и т. д.

В целях обеспечения унификации и полноты собираемых сведений о рискованных событиях подразделение по управлению рисками должно разработать нормативные документы, устанавливающие:

- классификационные перечни операционных рисков, рискованных событий и бизнес-процессов;
- минимальный перечень данных, необходимых для проведения оценки операционных рисков;
- порядок и регламент их представления в централизованную информационную базу.

Структурные подразделения, проводящие связанные с операционными рисками операции, в обязательном порядке должны осуществлять:

- анализ проводимых операций и условий их проведения на предмет идентификации и прогнозирования рисков событий;
- подготовку сведений в разрезе отдельных рисков событий (дата возникновения и выявления, сумма потерь, наличие страхового покрытия) с их предварительной классификацией (в разрезе видов рисков событий, бизнес-процессов, источников и факторов операционных рисков);
- представление информации в централизованную базу данных в соответствии с установленным порядком.

Ответственность за полноту, точность и своевременность представления информации несут структурные подразделения, операции которых обуславливают рискованные события.

Подразделение по управлению рисками должно провести предварительный анализ полученных данных на предмет недопущения дублирования сведений, связанных с одинаковыми рискованными событиями, а также исключения событий, связанных с рисками, отличными от операционного (стратегического, финансового, юридического и репутационного).



Рис. 3.5. Анализ показателей и принятие решения

Процедуры систематического сбора сведений о фактических и потенциальных рискованных событиях, идентифицированных структурными подразделениями, централизованное хранение и обработка данных, расчет показателей величины операционных рисков с последующим формированием отчетности должны проводиться в максимально полной мере при использовании возможности автоматизированных информационных систем. Полученный информационный массив является осно-



вой для анализа эффективности планирования и организации риск-менеджмента.

Таким образом, необходимость создания и внедрения системы управления операционными рисками организации реального сектора экономики определяется потребностью в консолидации усилий в этой сфере, создании стандартизированных подходов к выявлению и ликвидации угроз экономической безопасности в масштабах хозяйствующего субъекта. Основными целями построения системы управления операционным риском считается оптимизация процесса стратегического менеджмента в условиях действия внешних и внутренних угроз, достижение целевых критериев-ориентиров, предусмотренных долгосрочной программой развития организации, повышение эффективности хозяйственной деятельности и обеспечение системного подхода при принятии управленческих решений (рис. 3.5).

### **Выводы к главе 3**

1. Сформулирован подход к оценке эффективности функционирования базисной системы риск-менеджмента, основанный не только на сравнении плановых и фактических показателей затрат по управлению рисками и эффекта от управления ими, но и на вычислении показателей точности выявления рисков и прогноза по управлению ими.

2. Определены основные внутренние нормативные документы, необходимые для внедрения и функционирования базисной системы риск-менеджмента как элемента общей системы управления деятельностью организации. Предложены рекомендации по разработке и утверждению нормативных документов, а также раскрытию в них информации в целях их соответствия существующим международным стандартам по управлению рисками.

3. Разработан Порядок по управлению операционными рисками для организаций реального сектора экономики. В рамках Порядка определены границы операционного риска с целью его отделения от прочих классификационных групп, уточнено понятие «операционное рисковое событие» (обусловленное операционным риском событие, повлекшее или способное повлечь за собой потери и произошедшее по причине ошибочности или сбоя внутренних процессов, действий людей или систем, или по причине внешних событий, за исключением неблагоприятного для организации применения норм действующего законодательства), классифицированы факторы и источники операционных рисков и рисков событий, сформулированы основополагающие, организационные и процедурные аспекты управления операционными рисками.

## Заключение

В настоящее время проблема исследования рисков и их воздействия на хозяйствующие субъекты являются предметом изучения и пристального внимания многих отечественных ученых. Нельзя сказать, что в научных публикациях игнорировались методологические проблемы совершенствования организации риск-менеджмента – соответствующие экономические отношения, возникающие в процессе управления риском, подробно описаны учеными, занимающимися исследованиями в этой области научных знаний. Однако в результате авторских исследований выявлена недостаточность теоретических и практических нормативно-методических разработок системного риск-менеджмента отечественных организаций, что выражается в отсутствии национального стандарта в сфере управления рисками. Более того, несмотря на интерес к проблемам эффективной системы управления самыми опасными операционными рисками, а также относительный рост современных публикаций, затрагивающих эти вопросы, все же результаты анализа этих проблем не носят еще прикладного рекомендательного и системного характера.

В этих условиях особенно важным является попытка сформулировать новую, более полно отвечающую потребностям практической деятельности и основанную на иных, чем прежде, представлениях и подходах концепцию, которая позволила бы не только по-новому поставить, но и в значительной степени продвинуть решение заявленных целей и задач. Такая концепция, по мнению авторов, обязательно должна включить в свой научный инструментарий оправдавшие себя в прошлом методы, приемы и категории научного знания и дать возможность разработки новых теоретико-гносеологических и методических направлений, охватывающих и предоставляющих возможность изучить точнее, всестороннее и глубже внутренние взаимосвязи, противоречия и движущие силы процесса или явления. Этот подход, безусловно, имеет предметное содержание, так как он направлен на критический пересмотр существующего понятийного аппарата, известных предпосылок и сформулированных ранее подходов к интерпретации содержания соответствующей сферы науки.

Одной из таких новых концепций может стать Порядок управления операционными рисками, имеющий элемент универсальности, в основу которого положены идеи Базельского комитета по банковскому надзору. Полученные авторами результаты создают, на наш взгляд, надежную методическую основу для начала большой и важной практической работы по проектированию и внедрению базисной системы риск-менеджмента организациями реального сектора экономики. Очевидно, что ее успех и эффективность, а также конкретные результаты будут в значительной степени определяться не только пониманием менеджерами поставленных целей и задач, но и необходимым для этого проявлением воли владельцев бизнеса и мотивации работников, а также желанием изменить существующее положение самой организацией в целом, как социально-экономической системы.

## Библиографический список

1. Абасова Х. А. Методы управления финансовым риском на предприятии / Х. А. Абасова // Вопросы экономических наук. – 2010. – № 1. – С. 7–8.
2. Арькова Т. Ю. Изучение риск-менеджмента и необходимости контроля в новых условиях / Т. Ю. Арькова // Риск: Ресурсы, информация, снабжение, конкуренция. – 2009. – № 3. – С. 109–111.
3. Астахова К. В. Разработка и внедрение в банке системы управления операционными рисками «с нуля» / К. В. Астахова // Управление финансовыми рисками. – 2008. – № 4. – С. 290–307.
4. Афанасьев А. С. К проблеме измерения хозяйственного риска предприятий реального сектора экономики / А. С. Афанасьев // Известия Иркутской государственной экономической академии. – 2008. – № 3. – С. 87–90.
5. Бадюков В. Ф. Перестрахование в управлении рисками страховых организаций / В. Ф. Бадюков, Е. В. Козлова. – Хабаровск: РИЦ ХГАЭП, 2006.
6. Бадюков В. Ф. Ретроспективный анализ понятия риска и способы его уточнения / В. Ф. Бадюков, К. В. Белкин // Вестник ХГАЭП. – 2012. – № 4–5 (61). – С. 52–65.
7. Балабанов И. Т. Риск-менеджмент / И. Т. Балабанов. – М.: Финансы и статистика, 1996.
8. Банковские риски / Красавина Л. Н. [и др.]; под ред. О. И. Лаврушина, Н. И. Валенцевой. – М.: КноРус, 2007.
9. Барчуков, А. В. Организационно-методические подходы к формированию системы управления финансами в корпоративных образованиях / А. В. Барчуков // Вестник Сибирского института бизнеса и информационных технологий. – 2012. – № 3. – С. 7–12.
10. Батьковский М. А. Совершенствование управления финансовой устойчивостью предприятия в современных условиях с целью снижения рисков его деятельности / М. А. Батьковский, И. В. Булава, К. Н. Мингалиев // Риск: Ресурсы, информация, снабжения, конкуренция. – 2009. – № 3. – С. 50–52.
11. Белоусова Л. В. Проблема государственного регулирования и поддержки риск-менеджмента в России: исследование и анализ состояния отрасли / Л. В. Белоусова // Лизинг. – 2010. – № 9. – С. 12–25.
12. Белошевич М. М. Учет финансовых рисков при оценке финансовой устойчивости предприятия / М. М. Белошевич // Риск: Ресурсы, информация, снабжения, конкуренция. – 2010. – № 2. – С. 186–188.
13. Бланк И. А. Управление финансовыми рисками / И. А. Бланк. – Киев: Ника-Центр, 2005.
14. Блохина В. Г. Инвестиционный анализ / В. Г. Блохина. – Ростов н/Д: Феникс, 2004.
15. Бочаров В. В. Инвестиционный менеджмент / В. В. Бочаров. – СПб.: Питер, 2000.

16. Бычкова С. М. Риски в аудиторской деятельности / С. М. Бычкова, Л. Н. Растамханова; под ред. проф. С. М. Бычковой. – М.: Финансы и статистика, 2003.
17. Валдайцев С. В. Управление инновационным бизнесом / С. В. Валдайцев. – М.: ЮНИТИ-ДАНА, 2001.
18. Васильков Ю. В. Снижение внутренних рисков предприятия путем формирования менеджерских компетенций персонала / Ю. В. Васильков, Л. С. Гущина // Вестник Воронежского государственного университета. Серия «Экономика и управление». – 2010. – № 1. – С. 70–77.
19. Васин С. М. Управление рисками на предприятии / С. М. Васин, В. С. Шутов. – М.: КНОРУС, – 2010.
20. Веретенников Н. П. Корпорации: организационные формы, принципы и функции управления: монография / Н. П. Веретенников, Р. Г. Леонтьев. – М.: ВИНТИ РАН, 2003.
21. Виханский О. С. Менеджмент: человек, стратегия, организация, процесс / О. С. Виханский, А. И. Наумов. – М.: Гардарика, 1996.
22. Вишневская О. В. Антикризисное управление предприятием / О. В. Вишневская. – Ростов н / Д: Феникс, 2008.
23. Вяткин В. Н. Управление рисками фирмы. Программы интегративного риск-менеджмента / В. Н. Вяткин, В. А. Гамза, Ю. Ю. Екатеринославский. – М.: Финансы и статистика, 2006.
24. Гай Карпенгер, Оливер Вайман. Управление рисками. Состояние и развитие корпоративного риск менеджмента в России: отчет по результатам исследования Марш Риск Консалтинг по России и СНГ. При поддержке Русского общества управления рисками // Русское общество управления рисками: [сайт]. [2008]. URL: <http://rrms.ru/document/full/26> (дата обращения: 01.09.2011).
25. Галиева Г. М. Экономическая сущность и определение риска / Г. М. Галиева // Вопросы экономических наук. – 2009. – № 6. – С. 8–9.
26. Гамза В. А. Рисковый спектр коммерческих организаций / В. А. Гамза, Ю. Ю. Екатеринославский. – М.: Экономика, 2002.
27. Горбунов В. С. Влияние финансового риска на управленческие решения / В. С. Горбунов // Вестник Саратовского государственного социально-экономического университета. – 2010. – № 1. – С. 114–117.
28. ГОСТ Р 51897–2002. Менеджмент риска. Термины и определения. – Введ. 2003–01–01. – М.: Стандартинформ, 2003.
29. Грабовый П. Г. Риски в современном бизнесе / П. Г. Грабовый [и др.]. – М.: Атлас, 1994.
30. Гранатуров В. М. Экономический риск: сущность, методы измерения, пути снижения / В. М. Гранатуров. – М.: Дело и сервис, 2002.
31. Демчук И. Н. Риск-менеджмент и национальные стандарты менеджмента риска, применяемые в целях обеспечения конкурентоспособности, финансовой устойчивости и надежности коммерческих организаций / И. Н. Демчук, Н. В. Фадейкина // Сибирская финансовая школа. – 2009. – № 4. – С. 37–51.

32. Завгородний В. И. Системный анализ информационных рисков предприятия / В. И. Завгородний // Вестник Финансовой академии. – 2008. – № 4. – С. 102–109.
33. Загряжкина Е. Е. Теоретические основы управления предпринимательскими рисками / Е. Е. Загряжкина // Вестник Поволжского государственного университета сервиса. Серия «Экономика». – 2008. – № 4. – С. 64–88.
34. Зарипов Р. Я. Разработка и функционирование комплексной системы управления рисками в лизинговой компании / Р. Я. Зарипов // Проблемы анализа риска. – 2009. – Т. 6. – № 2. – С. 38–62.
35. Ивайловский Д. Г. Коррупция как фактор риска коммерческой организации / Д. Г. Ивайловский // Вестник Новосибирского государственного университета. Серия «Социально-экономические науки». – 2008. – Т. 8. – № 3. – С. 88–92.
36. Ивайловский Д. Г. Риск-менеджмент: становление нормальной науки / Д. Г. Ивайловский // Вестник Новосибирского государственного университета. Серия «Социально-экономические науки». – 2008. – Т. 8. – № 4. – С. 152–155.
37. Ильин В. В. Системный подход к оценке финансовых рисков / В. В. Ильин, Н. А. Сердюкова // Финансы. – 2008. – № 1. – С. 68–72.
38. Иода Е. В. Управление предпринимательскими рисками / Е. В. Иода [и др.]. – 2-е изд. испр. и перераб. – Тамбов: Тамбовский гос. техн. ун-т, 2002.
39. Кабушкин С. Н. Управление банковским кредитным риском / С. Н. Кабушкин. – М.: Новое знание, 2004.
40. Каранина Е. В. Формирование модели риск-системы предприятия в современных рыночных условиях / Е. В. Каранина // Наука и экономика. – 2010. – № 2. – С. 51–59.
41. Киселев К. М. Вопросы построения системы управления рисками корпоративного управления / К. М. Киселев // Вестник Финансовой академии. – 2010. – № 6. – С. 56–58.
42. Ковалев В. В. Управление активами фирмы / В. В. Ковалев. – М.: ТК Велби, Проспект, 2007.
43. Ковалев В. М., Ковалев С. М. Технология структуризации и описания организации – шаг за шагом // Консультант директора. – 2004. – № 8. – С. 24–36. URL: <http://www.betec.ru/index.php?id=06sid=20> (дата обращения: 01.09.2011).
44. Ковалевская О. С. Производственное предприятие: оценка хозяйственного риска / О. С. Ковалевская, А. С. Афанасьев // Вестник Новосибирского государственного университета. Серия «Социально-экономические науки». – 2008. – Т. 8. – № 2. – С. 118–123.
45. Колесников А. Н. Краткий курс математики для экономистов / А. Н. Колесников – М.: ИНФРА-М, 1997.
46. Крапчатова И. С. Процесс управления операционными рисками на предприятиях нефинансового сектора / И. С. Крапчатова // Управление финансовыми рисками. – 2008. – № 4. – С. 308–315.

47. Круглов М. Интегрированные системы менеджмента: движение в сторону финансов / М. Круглов // Уральский рынок металлов. – 2007. – № 10. – С. 82–87.
48. Крутилевич М. В. Особенности применения комплексной системы риск-менеджмента в производственно-предпринимательских структурах / М. В. Крутилевич // Вестник Омского университета. Серия «Экономика». – 2009. – № 1. – С. 88–91.
49. Крысин Л. П. Иллюстрированный толковый словарь иностранных слов / Л. П. Крысин. – М.: Эксмо, 2008.
50. Кулиева Ш. Т. Теоретические подходы к проблеме рисков и риск менеджменту / Ш. Т. Кулиева // Вестник Финансовой академии. – 2009. – № 4. – С. 43–45.
51. Куликова Е. Е. Управление рисками. Инновационный аспект / Е. Е. Куликова. – М.: Бератор-Паблишинг, 2008.
52. Лапуста М. Г. Предпринимательство / М. Г. Лапуста. – М.: ИНФРА-М. – 2009.
53. Лапуста М. Г. Риски в предпринимательской деятельности / М. Г. Лапуста, Л. Г. Шаркунова. – М.: ИНФРА-М, 1998.
54. Ларионов Г. Управление предпринимательскими рисками в бизнес-структурах / Г. Ларионов // Риск: Ресурсы, информация, снабжения, конкуренция. – 2010. – № 3. – С. 48–50.
55. Леднев М. В. Управление рисками деятельности факторинговой компании / М. В. Леднев // Управление финансовыми рисками. – 2010. – № 2. – С. 78–90
56. Лекарева Ю. С. Риск как объект экономического анализа / Ю. С. Лекарева // Вестник Российского государственного торгово-экономического университета. – 2008. – № 3. – С. 102–106.
57. Леонтьев Р. Г. Корпорации: Интеграция железнодорожной отрасли с малым бизнесом / Р. Г. Леонтьев, А. Н. Бессонова. – Хабаровск: Изд-во ДВГУПС, 2005.
58. Лиференко Г. Н. Финансовый анализ предприятия / Г. Н. Лиференко. – М.: Экзамен, 2005.
59. Логачев Н. Н. Нормативно-методическое обеспечение риск-менеджмента промышленных предприятий / Н. Н. Логачев // Проблемы анализа риска. – 2010. – Т. 7. – № 3. – С. 40–47.
60. Любушин Н. П. Анализ финансово-экономической деятельности предприятия / Н. П. Любушин, В. Б. Лещева, В. Г. Дьякова ; под ред. Н. П. Любушина. – М.: ЮНИТИ-ДАНА, 2000.
61. Максимова О. Управление финансовыми // Финансовый директор – 2008. – № 3. – С. 56–60. URL: <http://www.management.com.ua/finance/fin154.html> (дата обращения: 01.09.2011).
62. Мартынов С. А. Анализ причинно-следственных связей в механизме реализации риска / С. А. Мартынов // Управление финансовыми рисками. – 2008. – № 4. – С. 316–322.

63. Махутов Н. А. Научные основы и задачи по формированию системы оценки рисков / Н. А. Махутов // Проблемы анализа риска. – 2009. – Т. 6. – № 3. – С. 82–91.
64. Медведева А. М. Методология определения параметров конфигурации системы риск-менеджмента предприятия / А. М. Медведева // Учен. зап. Российской Академии предпринимательства. – 2010. – № 22. – С. 237–248.
65. Менеджмент на транспорте / Н. Н. Громов [и др.] ; под общ. ред. Н. Н. Громова, В. А. Персианова. – М.: Академия, 2003.
66. Мескон М. Основы менеджмента / Майкл Мескон, Майкл Альберт, Франклин Хедоури; пер. с англ. – М.: Дело, 1997. – 704 с. – Перевод изд.: Management / Michael H. Mescon, Michael Albert, Franklin Khedouri. New York City, 1988. – P. 777.
67. Михайлов И. В. Практика внедрения интегрированного управления рисками / И. В. Михайлов // Управление финансовыми рисками. – 2008. – № 3. – С. 130–136.
68. Моделирование экономических процессов / под ред. М. В. Грачевой, Л. Н. Фадеевой, Ю. Н. Черемных. – М.: ЮНИТИ-ДАНА, 2005.
69. Мосягин А. Управление правовым риском в кредитной организации / А. Мосягин // Корпоративный юрист. – 2008. – № 5. – С. 25–29.
70. Найт Ф. Х. Риск, неопределенность и прибыль / Ф. Х. Найт; пер. с англ. М. Я. Каждана – М.: Дело, 2003.
71. Наумов А. А. К оцениванию рисков бизнес-процессов / А. А. Наумов, Д. А. Шубин // Вестник Новосибирского государственного университета. Серия «Социально-экономические науки». – 2008. – Т. 8. – № 4. – С. 56–67.
72. Новоселов И. В. Системно-ориентированный внутренний аудит, основанный на риске / И. В. Новоселов // Известия Иркутской государственной экономической академии. – 2008. – № 3. – С. 21–24.
73. Овчаров А. О. Теоретико-методологические подходы к сущности рисков в сфере услуг и способам их оценки / А. О. Овчаров // Риск: Ресурсы, информация, снабжение, конкуренция. – 2010. – № 2. – С. 320–324.
74. Пэйн Рой. Эмоции и работа. Теории, исследования и методы применения / Рой Пэйн, Купер Кэрри; пер. с англ. – М.: Гуманитарный центр, 2008.
75. Печенин Н. К. Проблемы управления риском / Н. К. Печенин, А. Ю. Логвин // Проблемы анализа риска. – 2009. – Т. 6. – № 1. – С. 82–91.
76. Резниченко В. Ю. Риск-менеджмент / В. Ю. Резниченко. – М.: Моск. гос. ун-т экономики, статистики и информатики, 2004.
77. Рогачев А. Ю. Преимущества комплексного подхода к управлению рисками предприятия / А. Ю. Рогачев // Управление финансовыми рисками. – 2008. – № 1. – С. 66–71.
78. Рогачев А. Ю. Управление рисками предприятия: Опыт фармацевтической компании / А. Ю. Рогачев // Проблемы анализа риска. – 2008. – Т. 5. – № 4. – С. 30–38.

79. Рогачев А. Ю. Человеческий фактор в операционных рисках / А. Ю. Рогачев, М. И. Рогачева // Управление финансовыми рисками. – 2007. – № 1. – С. 78–83.
80. Сальникова Л. В. Как снизить риск неисполнения хозяйственного договора. / Л. В. Сальникова. – М.: Налоговый вестник, 2007.
81. Синеев, Д. М. Методы оценки риска: общие принципы / Д. М. Синеев // Вестник Российской академии им. Г. В. Плеханова. – 2009. – № 4. – С. 26–31.
82. Сонин А. М. Внутренний аудит: кому подчиняться? // Управление компанией. – 2006. – №7. – С. 47–50. URL: <http://www.cfin.ru/press/zhuk/2006-7/16.shtm> (дата обращения: 01.09.2011).
83. Старинов Г. П. Деликатные риски в экономических системах предприятий и организаций / Г. П. Старинов // Сибирская финансовая школа. – 2008. – № 6. – С. 118–119.
84. Стратегии бизнеса: аналитический справочник / С. А. Айвазян [и др.] ; под ред. Г. Б. Клейнера. – М.: КОНСЭКО, 1998. – 331 с. URL: <http://www.aup.ru/books/m71/> (дата обращения: 01.09.2011).
85. Товб А. С. Управление проектами: стандарты, методы, опыт / А. С. Товб, Г. Л. Ципес. – М.: Олимп-Бизнес, 2003. – 240 с.
86. Томпсон А. А. Стратегический менеджмент: концепции и ситуации / А. А. Томпсон, А. Д. Стрикленд; пер. с англ. – М.: Вильямс, 2006.
87. Туркина А. А. Риск-менеджмент и автоматизация системы внутреннего контроля в компаниях / А. А. Туркина // Управление финансовыми рисками. – 2008. – № 2. – С. 86–93.
88. Тэпман Л. Н. Риски в экономике / Л. Н. Тэпман ; под ред. В. А. Швандара. – М.: ЮНИТИ-ДАНА, 2002.
89. Управление организацией / под ред. А. Г. Поршнева, З. П. Румянцевой, Н. А. Саломатина. – М.: ИНФРА-М, 1998.
90. Уткин Э. А. Управление рисками предприятия / Э. А. Уткин, Д. А. Фролов. – М.: ТЕИС, 2003.
91. Фролов С. С. Социология организаций / С. С. Фролов. – М.: Гардарики, 2001.
92. Хаертфельдер М. Фундаментальный и технический анализ рынка ценных бумаг / М. Хаертфельдер, Е. С. Лозовская, Е. Хануш. – СПб.: Питер, 2005.
93. Холмс Э. Риск менеджмент / Э. Холмс; пер. с англ. В. В. Хмелевской. – М.: Эксмо, 2007.
94. Хохлов Н. В. Управление риском / Н. В. Хохлов. – М.: ЮНИТИ-ДАНА, 2001.
95. Чаадаев В. К. Бизнес-процессы в компаниях связи / В. К. Чаадаев. – М.: Эко-Трендз, 2004.
96. Чернова Г. В. Управление рисками / Г. В. Чернова, А. А. Кудрявцев. – М.: Велби: Проспект, 2005.
97. Шапкин, А. С. Экономические и финансовые риски. Оценка, управление, портфель инвестиций / А. С. Шапкин. – М.: Дашков и К, 2003.



98. Шелевой Д. Г. Механизм управления рисками строительных предприятий / Д. Г. Шелевой // Известия Иркутской государственной экономической академии (Байкальский государственный университет экономики и права): Электронный журнал. – 2010. – № 5. – С. 180–183.

99. Школин А. Что делать с репутационными рисками / А. Школин // Финанс. – 2004. – № 21 (62). – С. 21–15. URL: <http://www.finansmag.ru/6680> (дата обращения: 01.09.2011).

100. Энциклопедия финансового риск-менеджмента / В. Е. Барбаумов [и др.] ; под ред. А. А. Лобанова, А. В. Чугунова. – М: Альпина Паблшер, 2003.

101. Ягубов Ш. Р. Риски предприятий в глобальном рынке / Ш. Р. Ягубов // Вестник Саратовского государственного социально-экономического университета. – 2008. – № 5. – С. 96–98.

102. Abrams C. Optimized enterprise risk management / C. Abrams, J. von Känel, S. Müller, B. Pfitzmann, S. Ruschka-Taylor // IBM Systems Journal. – 2007. – Volume 46. – Issue 2. – P. 219–234.

103. Aloini D. Risk management in ERP project introduction: Review of the literature / Davide Aloini, Riccardo Dulmin, Valeria Mininno // Information Management. – 2007. – Volume 44. – Issue 6. – P. 547–567.

104. Arif Zaman. Reputational Risk: How To Manage For Value Creation (Management Briefings Executive Series) / Arif Zaman. – London: Financial Times Management, 2007. – P. 308.

105. Azvine, B. Operational risk management with real-time business intelligence / B. Azvine, Z. Cui, B. Majeed, M. Spott // BT Technology Journal. – 2007. – Volume 25. – Issue 1. – P. 154–167.

106. Basel Committee on Banking Supervision. International Convergence of Capital Measurement and Capital Standards. A Revised Framework Comprehensive Version. – Bank for International Settlements Press Communications, 2006. – P. 333.

107. Basel Committee on Banking Supervision. Sound Practices for the Management and Supervision of Operational Risk. – Bank for International Settlements Press Communications, 2003. – P. 14 (<http://www.bis.org/publ/bcbs96.pdf>). Проверено 01.09.2011.

108. Bill Coffin, Morgan O'Rourke. The Year in Risk 2007 [Electronic resource] // Risk Management Magazine: [site]. [2007]. URL: <http://www.rmmag.com/MGTemplate.cfm?Section=MagArchiveNavMenuID=304template=/Magazine/DisplayMagazines.cfmArchive=1IssueID=331AID=3825Volume=55ShowArticle=1> (reference date: 01.09.2011).

109. Bill Coffin, Morgan O'Rourke and Jared Wade. The Year in Risk 2008 [Electronic resource] // Risk Management Magazine: [site]. [2008]. URL: <http://www.rmmag.com/MGTemplate.cfm?Section=MagArchiveNavMenuID=304template=/Magazine/DisplayMagazines.cfmArchive=1IssueID=311AID=3540Volume=54ShowArticle=1> (reference date: 01.09.2011).

110. Bill Coffin, Jared Wade and Morgan O'Rourke. The Year in Risk 2009 [Electronic resource] // Risk Management Magazine: [site]. [2009]. URL: <http://www.rmmag.com/MGTemplate.cfm?Section=MagAr>

chiveNavMenuID=304template=/Magazine/DisplayMagazines.cfmArchive=1IssueID=341AID=4019Volume=56ShowArticle=1 (reference date: 01.09.2011).

111. Brian Ziberna. COSO ERM Framework [Electronic resource] // North Carolina State University: [site]. [2006]. URL: [http://mgt.ncsu.edu/erm/documents/COSOERMSynopsis\\_edit\\_MSD.pdf](http://mgt.ncsu.edu/erm/documents/COSOERMSynopsis_edit_MSD.pdf) (reference date: 01.09.2011).

112. Brooke, S. Pitfalls of rebranding / S. Brook // Financial Times. – 2002. – 3 October. – P. 15.

113. BS ISO 31000:2009. Risk management. Principles and guidelines. – Jointly published by BSI, 2010. – P. 38.

114. Committee of Sponsoring Organizations of the Treadway Commission. Enterprise Risk Management – Integrated Framework (2004). – Jointly published by American Institute of CPAs, 2004. – P. 103.

115. DHS Risk Steering Committee. DHS Risk Lexicon [Electronic resource] // US Department of Homeland Security: [site]. [2010]. URL: <http://www.dhs.gov/xlibrary/assets/dhs-risk-lexicon-2010.pdf> (reference date: 01.09.2011).

116. Drew, M. Information risk management and compliance — expect the unexpected / M. Drew // BT Technology Journal. – 2007. – Volume 25. – Issue 1. – P. 19–29.

117. Edmiston, A. H. The role of systems and applications monitoring in operational risk management / A. H. Edmiston // BT Technology Journal. – 2007. – Volume 25. – Issue 1. – P. 68–78.

118. Ericson, R. The architecture of risk management / Richard Ericson, Myles Leslie // Economy and Society. – 2008. – Volume 37. – Number 4. – P. 613–624.

119. Federation of European Risk Management Associations. A Risk Management Standard. [Electronic resource] // Federation of European Risk Management Associations: [site]. [2005]. URL: <http://ferma.eu/portals/2/documents/rms/rms-uk.22.12.05.pdf> (reference date: 01.09.2011).

120. Federation of European Risk Management Associations. European Confederation of Institutes of Internal Auditing. Guidance on the 8th EU Company Law Directive – article 41 [Electronic resource] // Federation of European Risk Management Associations: [site]. [2010]. URL: [http://ifrima.org/ESW/Files/Guidance\\_on\\_the\\_8th\\_EU\\_Company\\_Law\\_Directive.pdf](http://ifrima.org/ESW/Files/Guidance_on_the_8th_EU_Company_Law_Directive.pdf) (reference date: 01.09.2011).

121. Federation of European Risk Management Associations. FERMA European Risk Management Benchmarking Survey 2010 [Electronic resource] // Federation of European Risk Management Associations: [site]. [2010]. URL: <http://ferma.eu/Portals/2/documents/benchmarking-survey/ferma-european-risk-management-benchmarking-survey-2010.pdf> (reference date: 01.09.2011).

122. Fortin, J. The road to BPM: Model, integrate, ménage / J. Fortin // Business Process. – 2003. – June. – P. 24–25.

123. Geert Hofstede. Cultures and Organizations: Software of the Mind / Geert Hofstede, Gert Jan Hofstede, Michael Minkov. – New York City: McGraw-Hill, 2010. – P. 578.

124. Hamdi, M. Computer and network security risk management: Theory, challenges, and countermeasures / Mohamed Hamdi, Nouredine Boudriga // *International Journal of Communication Systems*. – 2005. – Volume 18. – Issue 8. – P. 763–793.
125. *International risk management lexicon* / [edited by] Kevin W. Knight. – Nundah, Qld: International Federation of Risk and Insurance Management Associations, 1994. – P. 97.
126. ISO/IEC Guide 73:2002. Risk management – Vocabulary – Guidelines for use in standards. – Jointly published by International Organization for Standardization, 2002. – P. 10.
127. Jafry Y. Hypo International Strengthens Risk Management with a Large-Scale, Secure Spreadsheet-Management Framework / Yusuf Jafry, Christopher Marrison, Ulrike Umkehrer-Neudeck // *Interfaces*. – 2008. – Volume 38. – Issue 4. – P. 281–288.
128. Jared Wade, Emily Holbrook and Morgan O'Rourke. The Year in Risk 2010 [Electronic resource] // *Risk Management Magazine*: [site]. [2010]. URL: <http://www.rmmag.com/MGTemplate.cfm?Section=RMMagazineNavMenuID=128template=/Magazine/DisplayMagazines.cfmIssueID=351AID=4217Volume=57ShowArticle=1>(reference date: 01.09.2011).
129. Jared Wade. The Year in Risk: Looking Back at the Top Stories of 2006 [Electronic resource] // *Risk Management Magazine*: [site]. [2006]. URL: <http://www.rmmag.com/MGTemplate.cfm?Section=MagArchiveNavMenuID=304template=/Magazine/DisplayMagazines.cfmArchive=1IssueID=284AID=3233Volume=53ShowArticle=1> (reference date: 01.09.2011).
130. Jimme A. Keizer. From experience: applying the risk diagnosing methodology / Jimme A. Keizer, Johannes I.M. Halman, Michael Song // *The Journal of Production Innovation Management*. – 2002. – Volume 19. – Issue 3. – P. 213–232.
131. J. David Cummins. Convergence of Insurance and Financial Markets: Hybrid and Securitized Risk-Transfer Solutions / J. David Cummins, Mary A. Weiss // *The Journal of Risk and Insurance*. – 2009. – Volume 76. – Number 3. – P. 493–545.
132. Keey, R. B. Risk Management – An Australasian View / R. B. Keey // *Process Safety and Environmental Protection*. – 2003. – Volume 81. – Issue B1. – P. 31–35.
133. Keynes, J. M. *The General Theory of Employment, Interest, and Money* / J. M. Keynes. – New York City: Prometheus Books, 1997. – P. 403.
134. Kim, S. Enterprise security architecture in business convergence environments / Sangkyun Kim, Choon Seong Leem // *Industrial Management Data Systems*. – 2005. – Volume 105. – Issue 7. – P. 919–936.
135. Laurent Condamin. Risk quantification: management, diagnosis hedging / Laurent Condamin, Jean-Paul Louisot, and Patrick Naim. – Chippenham: Antony Rowe Ltd, 2007. – P. 271.
136. Leung, F. Risk management in public sector research: approach and lessons learned at a national research organization / Flavia Leung, Frances Isaacs // *R D Management*. – 2008. – Volume 38. – Issue 5. – P. 510–519.

137. Lexicon Systems, LLC. ENTERPRISE RISK MANAGEMENT: THE NEW IMPERATIVE [Electronic resource] // Lexicon Systems, LLC: [site]. [2007]. URL: <http://www.lexicon-systems.com/pubs/white-papers/EnterpriseRiskManagementNewImperative.pdf> (reference date: 01.09.2011).
138. Louis Anthony Cox, Jr. What's Wrong with Risk Matrices? / Louis Anthony Cox, Jr. // *Risk Analysis*. – 2008. – Volume 28. – Issue 2. – P. 497–512.
139. Managing business risk: a practical guide to protecting your business / [edited by] Jonathan Reuvid. – 5th ed. – Aberystwyth: Cambrian Printers Ltd, 2008. – P. 269.
140. Maplecroft. Rising political risk sees Russia and Pakistan join Somalia, DR Congo and Iraq in Maplecroft ranking of 10 most volatile business environments [Electronic resource] // Maplecroft: [site]. [2011]. URL: [http://www.maplecroft.com/about/news/pra\\_2011.html](http://www.maplecroft.com/about/news/pra_2011.html) (reference date: 01.09.2011).
141. Mark S. Beasley, Bruce C. Branson, Bonnie V. Hancock. COSO's 2010 Report on ERM [Electronic resource] // Committee of Sponsoring Organizations of the Treadway Commission: [site]. [2010]. URL: <http://coso.org/documents/COSOSurveyReportFULL-Web-R6FINALforWEBPOSTING111710.pdf> (reference date: 01.09.2011).
142. Mikes Anette. Risk management and calculative cultures / Anette Mikes // *Management Accounting Research*. – 2009. – Volume 20. – Issue 1. – P. 18–40.
143. Paul M. Collier. Risk and Management Accounting: Best Practice Guidelines for Enterprise-wide Internal Control Procedures / Paul M. Collier, Anthony J. Berry, Gary T. Burke. – Oxford: Elsevier Ltd – 2007. – P. 160.
144. PricewaterhouseCooper CFO: Architect of the Corporation's Future / PricewaterhouseCoopers Financial Cost Management Team. – New York City: John Wiley Son, 1999. – P. 300.
145. Pat O'Malley. Uncertain subjects: risks, liberalism and contract / Pat O'Malley // *Economy and Society*. – 2000. – Volume 29. – Number 4. – P. 460–484.
146. Protiviti. Board Risk Oversight – A Progress report [Electronic resource] // Committee of Sponsoring Organizations of the Treadway Commission: [site]. [2010]. URL: [http://coso.org/documents/Board-Risk-Oversight-Survey-COSO-Protiviti\\_000.pdf](http://coso.org/documents/Board-Risk-Oversight-Survey-COSO-Protiviti_000.pdf) (reference date: 01.09.2011).
147. Risk Management Guidelines Companion to AS/NZS 4360:2004. – Jointly published by Standards Australia International Ltd and Standards New Zealand, 2005. – P. 120.
148. Rob Goffee. The Character of a Corporation: How Your Company's Culture Can Make or Break Your Business [Hardcover] / Rob Goffee, Gareth Jones. – Jointly published by Collins, 1998. – P. 256.
149. Shi-Ming Huang. Assessing risk in ERP projects: identify and prioritize the factors / Shi-Ming Huang, I-Chu Chang, Shing-Hani Li, Ming-Tong Lin // *Industrial Management Data Systems*. – 2004. – Volume 104. – Issue 8–9. – P. 681–688.

150. Steinberg R. Corporate Governance and the Board: What Works Best / R. Steinberg, C. Bromilow. – Florida: The Institute of Internal Auditors Research Foundations, 2000. – P. 107.

151. Steve G. Sutton. Risk Analysis in Extended Enterprise Environments: Identification of Critical Risk Factors in B2B Ecommerce Relationships / Steve G. Sutton, Deepak Khazanchi, Clark Hampton, Vicky Arnold // Journal of the Association for Information Systems. – 2008. – Volume 9. – Issue 3–4. – P. 151–174.

152. The Association of Insurance and Risk Managers. A structured approach to Enterprise Risk Management (ERM) and the requirements of ISO 31000 [Electronic resource] // The Association of Insurance and Risk Managers: [site]. [2010]. URL: [http://ferma.eu/Portals/2/documents/RMS/2010-SARM\(final\).pdf](http://ferma.eu/Portals/2/documents/RMS/2010-SARM(final).pdf) (reference date: 01.09.2011).

153. The Financial Reporting Council. Internal Control: Revised Guidance for Directors on the Combined Code (October 2005). – Jointly published by The Financial Reporting Council, 2005. – P. 47.

154. UK MOD Defence Acquisition Community. Risk Lexicon: Preferred Terminology and Authoritative Source Cross Reference Table [Electronic resource] // UK Ministry of Defence: [site]. [2008]. URL: [http://http://www.aof.mod.uk/aofcontent/tactical/risk/downloads/risk\\_lexicon\\_v1.pdf](http://http://www.aof.mod.uk/aofcontent/tactical/risk/downloads/risk_lexicon_v1.pdf) (reference date: 01.09.2011).

155. Voronova, I. Methods of analysis and estimation of risks at the enterprises of non-financial sphere of Latvia / Irina Voronova // Journal of Business Economics and Management. – 2008. – Volume 9. – Issue 4. – P. 319–326.

156. Woodruff, J.M. Consequence and likelihood in risk estimation: A matter of balance in UK health and safety risk assessment practice / Jason Michael Woodruff // Safety Science. – 2005. – Volume 43. – Issue 5–6. – P. 345–353.

157. Xiuwu Liao. Decision support for risk analysis on dynamic alliance / Yuan Li, Xiuwu Liao // Decision Support Systems. – 2007. – Volume 42. – Issue 4. – P. 2043–2059.

## ПРИЛОЖЕНИЕ 1

Таблица 1

### ИЗМЕРЕНИЕ ПОСЛЕДСТВИЙ: ОПАСНОСТИ И ПОЛОЖИТЕЛЬНЫЕ ВОЗМОЖНОСТИ

<i>Измерение</i>	<i>Описание</i>
Высокий уровень	Значение финансового воздействия на организацию превысит А рублей. Очень существенное воздействие на стратегию или операционную деятельность организации. Очень существенное влияние на проект
Выше среднего уровень	Значение финансового воздействия на организацию, вероятно, будет находиться между В рублей и А рублей. Существенное воздействие на стратегию или операционную деятельность организации. Существенное влияние на рассматриваемый проект
Ниже среднего уровень	Значение финансового воздействия на организацию, вероятно, будет находиться между С рублей и В рублей. Несущественное воздействие на стратегию или операционную деятельность организации. Несущественное влияние на рассматриваемый проект
Низкий уровень	Значение финансового воздействия на организацию, вероятно, будет меньше С рублей. Низкий уровень воздействия на стратегию или операционную деятельность организации. Низкий уровень влияния на рассматриваемый проект

Таблица 2

**ИЗМЕРЕНИЕ ВЕРОЯТНОСТЕЙ: ОПАСНОСТИ**

<i>Измерение</i>	<i>Описание</i>	<i>Показатели</i>
Высокий уровень	Вероятность наступления каждый год, или более 25% вероятности данного события	Возможность наступления события – несколько раз за промежуток времени, например за 10 лет. Данное событие недавно имело место
Выше среднего уровень	Вероятность наступления в течение 10 лет, или менее 25 %, но более 5 % вероятности данного события	Возможность наступления события – более одного раза за промежуток времени, например за 10 лет. Данное событие, возможно, недавно имело место
Ниже среднего уровень	Низкая вероятность наступления в течение 10 лет, или менее 5 %, но более 1 % вероятности данного события	Данное событие не происходило в прошлом, вероятность свершения низкая
Низкий уровень	Очень низкая вероятность наступления в течение 10 лет, или менее 1 % вероятности данного события	Данное событие не происходило в прошлом, вероятность свершения очень низкая

**ИЗМЕРЕНИЕ ВЕРОЯТНОСТЕЙ:  
ПОЛОЖИТЕЛЬНЫЕ ВОЗМОЖНОСТИ**

<i>Измерение</i>	<i>Описание</i>	<i>Показатели</i>
Высокий уровень	Высокая вероятность благоприятного исхода в течение года, или более 75 % вероятности данного события	Достаточная уверенность в существовании возможности наступления события в краткосрочном периоде при использовании текущих управленческих процессов
Выше среднего уровень	Вероятность благоприятного исхода в течение года выше среднего, или более 50 %, но менее 75 % вероятности данного события	Наступление данного события возможно, но требует тщательного управления. Возможности, которые могут возникнуть помимо запланированных
Ниже среднего уровень	Вероятность благоприятного исхода в течение года ниже среднего, или более 25 %, но менее 50 % вероятности данного события	Наступление данного события возможно, но требует очень тщательного управления. Возможности, которые могут возникнуть помимо запланированных
Низкий уровень	Некоторая вероятность достижения благоприятного исхода в течение года, или менее 25 % вероятности данного события	Предположительная возможность, требующая дополнительных исследований со стороны руководства. Маловероятная возможность, при текущем состоянии применяемых управленческих ресурсов



**ПРИЛОЖЕНИЕ 2**

**КЛАССИФИКАЦИОННЫЙ ПЕРЕЧЕНЬ РИСКОВЫХ СОБЫТИЙ,  
ОБУСЛОВЛИВАЮЩИХ ОПЕРАЦИОННЫЕ ПОТЕРИ**

<i>№</i>	<i>Категория РС 1-го уровня</i>	<i>№</i>	<i>Категория РС 2-го уровня</i>	<i>№</i>	<i>Категория РС 3-го уровня</i>
1	2	3	4	5	6
1	Внутреннее мошенничество	1.1	Несанкционированные преднамеренные операции сотрудников	1.1.1	Намеренное сокрытие / искажение сотрудником проведенных операций
				1.1.2	Проведение операций несанкционированного вида
				1.1.3	Намеренное проведение операций с несанкционированными контрагентами
				1.1.3	Намеренное нарушение/ игнорирование установленного порядка проведения операций
				1.1.4	Использование заведомо неверных аналитических моделей / параметров
				1.1.5	Прочее
		1.2	Кражи и мошенничества (преднамеренные действия с участием сотрудников)	1.2.1	Кражи материального имущества организации
				1.2.2	Кражи денежных средств / финансовых активов организации
				1.2.3	Подделка платежных документов
				1.2.4	Компьютерное мошенничество
				1.2.5	Намеренное нанесение ущерба материальным активам организации

1	2	3	4	5	6
1	Внутреннее мошенничество	1.2	Кражи и мошенничества (преднамеренные действия с участием сотрудников)	1.2.6	Использования сотрудником материальных активов организации в личных целях
				1.2.7	Завышение сотрудником понесенных расходов
				1.2.8	Намеренное и необоснованное увеличение сотрудником объемов проводимых операций в целях извлечения личной выгоды
				1.2.9	Прочее
2	Внешнее мошенничество	2.1	Кража и мошенничество	2.1.1	Ограбление, кражи, хищения активов организации
				2.1.2	Прием фальшивых денежных средств
				2.1.3	Проведение операций на основании представленных поддельных документов
				2.1.4	Вандализм, нанесение внешними лицами ущерба имуществу организации
				2.1.5	Прочее
		2.2	Нарушение безопасности информационных систем	2.2.1	Взлом компьютерных систем
				2.2.2	Спам
				2.2.3	Вирусы и прочие вредоносные программы
2.2.4	Прочее				
3	Нарушения, связанные с безопасностью и охраной труда, окружающей средой	3.1	Безопасность и охрана труда	3.1.1	Нарушение внутренних норм безопасности и охраны труда

1	2	3	4	5	6
3	Нарушения, связанные с безопасностью и охраной труда, окружающей средой	3.1	Безопасность и охрана труда	3.1.2	Причинение ущерба здоровью работников
				3.1.3	Прочее
		3.2	Окружающая среда	3.2.1	Нарушение внутренних норм охраны окружающей среды
				3.2.2	Прочее
4	Ущерб, нанесенный материальным активам	4.1	Ущерб в результате событий стихийного характера и прочих внешних событий, досрочного списания (выбытия) материальных активов по причинам событий стихийного характера	4.1.1	Пожар
				4.1.2	Стихийные бедствия
				4.1.3	Военные действия
				4.1.4	Террористические действия
				4.1.5	Технологические катастрофы
				4.1.6	Прочее
5	Нарушение деятельности или функционирования систем	5.1	Сбой в работе IT-систем	5.1.1	Сбой в работе сетевого оборудования
				5.1.2	Сбой в работе программного обеспечения
				5.1.3	Сбой в работе компьютерного оборудования
				5.1.4	Сбой в работе средств связи и телекоммуникаций
				5.1.5	Сбой в работе технических систем обеспечения работы зданий, сооружений
				5.1.6	Прочее
		5.2	Недостатки инфраструктуры	5.2.1	Сбой в работе систем водоснабжения, пожаротушения и/или отопительных систем
				5.2.2	Сбой в работе систем электроснабжения

1	2	3	4	5	6
5	Нарушение деятельности или функционирования систем	5.2	Недостатки инфраструктуры	5.2.3	Сбой работы транспорта
				5.2.4	Сбой телекоммуникаций по внешним причинам
				5.2.5	Затопление водой из систем водоснабжения, пожаротушения
				5.2.6	Прочее
	Нарушение деятельности или функционирования систем	5.3	Оборудование	5.3.1	Сбой в работе оборудования профильных видов деятельности
				5.3.2	Сбой в работе оборудования непрофильных видов деятельности
5.3.3				Прочее	
6	Нарушения или ошибки, связанные с выполнением операций и вследствие отношений с поставщиками	6.1	Подготовка, проведение и сопровождение операций	6.1.1	Неисполнение договорных обязательств перед контрагентами (вследствие несовершенства организации проведения операций)
				6.1.2	Техническое нарушение лимитов сделок с контрагентами (по причине несовершенства организации проведения операций)
				6.1.3	Ненамеренная недостача / просчет при проведении операций с наличными ценностями
				6.1.4	Нарушение сроков исполнения договорных обязательств перед контрагентами (по вине работников)

1	2	3	4	5	6
6	Нарушения или ошибки, связанные с выполнением операций, и вследствие отношений с поставщиками	6.1	Подготовка, проведение и сопровождение операций	6.1.5	Непреднамеренное нарушение лимита сделок с контрагентами (по вине сотрудника)
				6.1.6	Нанесения ущерба чужому имуществу
				6.1.7	Нарушение сотрудником установленных сроков исполнения поручения/ должностных обязанностей
				6.1.8	Ошибочная интерпретация сотрудником полученного поручения
				6.1.9	Ошибки сотрудника при вводе/ обработке данных
				6.1.10	Прочее
		6.2	Договоры и документация	6.2.1	Неполнота заполнения документов, предназначенных для проведения операций
				6.2.2	Утеря документов
				6.2.3	Прочее
		6.3	Поставщики и аутсорсинг	6.3.1	Неисполнение организацией своих обязательств по причине банкротства поставщика товаров / услуг
				6.3.2	Несоответствие договора с поставщиком товаров / услуг потребностям организации
				6.3.3	Прочее