

УДК 654.07.012.12

Методологические аспекты и инструментальная среда моделирования операционного риска в телекоммуникационных компаниях¹

В.С. Канев, Ю.В. Шевцова

Предлагаются подходы к созданию системы управления операционным риском в телекоммуникационных компаниях с применением байесовых технологий.

Ключевые слова: операционный риск, байесовы сети, диаграммы влияния, карта рисков.

*Но дальновидный риска не боится
И в безграничность верит без границы.
И.В. Гёте. Фауст*

1. Введение

В последние годы среди компаний нефинансового сектора наблюдается значительный рост интереса к вопросам внедрения в корпоративную среду комплексной системы управления рисками, по оценке экспертов Integrated Services Group, среди них лидирующее положение занимают именно телекоммуникационные компании [12]. Крупнейшие зарубежные операторы: British Telecom, France Telecom, Deutsche Telecom, Telecom Italia – добились существенных успехов в этой области. Среди российских телекоммуникационных компаний наиболее масштабным видится проект по созданию системы управления операционными рисками в ОАО «Сибирьтелеком» и ОАО «ЮТК» [9, 10, 11]. Эта тенденция обусловлена рядом причин, важнейшие из которых следующие:

- осознание топ-менеджментом компаний необходимости перехода к новым методам управления и повышения качества управления;
- ужесточение требований регуляторов рынка ценных бумаг в части эффективности системы контроля и управления рисками;
- повышение рискованности на рынке предоставления услуг связи;
- увеличение непредвиденных расходов телекоммуникационных компаний [16].

Однако, несмотря на серьезные практические реализации и теоретические исследования, операционный риск остаётся наименее теоретически формализованной областью современного риск-менеджмента: начиная от отсутствия единства в понимании его типологических особенностей, заканчивая методологическими трудностями количественной оценки уровня операционного риска.

Мы ранее [2] рассматривали вопросы системного управления рисками в телекоммуникациях, где подробнее освещалось состояние проблемы, используемые методы, модели и имеющиеся в поле нашего зрения отечественные и зарубежные подходы, реализации при управле-

¹ Работа выполнена при поддержке гранта Фонда фундаментальных и прикладных исследований СибГУТИ.

нии рисками. Эта работа, как и её настоящее продолжение, являются функциональными элементами, разрабатываемыми нами для системы моделей регионального инфокоммуникационного комплекса [7].

Данная работа имеет своей *целью* уточнение некоторых методологических аспектов и инструментальной среды операционного риск-менеджмента. Достижению этой цели способствует решение следующих *задач*:

- уточнение определения операционного риска применительно к моделированию операционных потерь;
- анализ особенностей моделирования событий операционного риска с помощью байесовых сетей и их продолжения – диаграмм влияния;
- разработка подходов к автоматизации процесса управления операционными рисками на основе адекватной инструментальной среды.

Далее в работе приняты следующие сокращения:

БС – байесова сеть;

ДВ – диаграмма влияния;

ОРС – операционное рисковое событие;

И – источник возникновения операционного рискового события;

П – последствие реализации операционного рискового события;

М – мероприятие по снижению вероятности реализации источника возникновения операционного рискового события;

ЛПР – лицо, принимающее решение.

2. Определение операционного риска

В настоящее время стандартным определением операционного риска среди профессиональных риск-менеджеров является определение, предложенное в рамках Базельского соглашения по капиталу 2004 г.², согласно которому под *операционным риском* понимается *риск потерь³, связанных с неадекватными или неудачными внутренними процессами, системами или действиями людей, либо с внешними событиями* [3, 17, 19].

Помимо указанного, в экономической литературе применяются и другие определения операционного риска, отличающиеся друг от друга, в основном, степенью детализации [3, 17]. Важно заметить, что в некоторых⁴ отечественных источниках по управлению рисками термин «операционный риск» непосредственно вообще не употребляется. В них данный тип риска рассматривается через его источники: природный, экологический, социальный, транспортный риски, риск персонала и др. – каждый из которых определяется как отдельный тип риска, что приводит к искажению понимания природы операционного риска и его идентификации [5].

Здесь важно заметить, что, являясь относительно молодой областью знаний, риск-менеджмент ещё не имеет общепринятых, концептуально полных, универсальных методических подходов и практических приёмов по его реализации.

На наш взгляд, принципиально важным, с точки зрения лучшего понимания сущности операционного риска как экономической категории, является выявление его типологических признаков, т.е. таких особенностей, которые позволяют однозначно или близко к этому отнести конкретное рисковое событие именно к инциденту операционного риска.

² Базельский комитет по банковскому надзору – комитет, созданный центральными банками и надзорными органами стран G-10 с целью сближения национальных систем регулирования и повышения устойчивости банковских систем.

³ Следует заметить, что первоначально (2001 г.) Базельский комитет определял операционный риск как «риск прямых потерь...», в дальнейшем определение «прямых» было изъято. Это подразумевает, что при управлении операционным риском следует учитывать как прямые, так и косвенные потери.

⁴ За исключением литературы, посвящённой управлению рисками в компаниях финансового сектора.

В этой связи полезным видится подход, предложенный М.А.Бухтиным [3]. Автор в основу выделения из всего многообразия рисков однородных типов положил выявление объекта риска⁵, на котором они реализуются. М.А.Бухтин идентифицирует три основных объекта риска:

- финансовые инструменты и генерируемые ими денежные потоки;
- бизнес-процессы (операционные процессы) и отдельные операции;
- бизнес-стратегии, цели и репутация.

В соответствии с категоризацией объектов риска выделяют следующие типы риска: финансовые, операционные и стратегические риски. Таким образом, важным типологическим признаком операционного риска является то, что *операционные рискованные события возникают на объектах риска, являющихся бизнес-процессами или отдельными бизнес-операциями*.

Также целесообразным при выделении перечисленных выше типов риска видится подход, основанный на различии в последствиях их реализации. Так, управление стратегическими и финансовыми рисками даёт возможность увеличить доходы организации (это – риск-шанс), в то время как управление операционными рисками позволяет снизить потери (это – риск-угроза) (рис. 1) [17].



Рис. 1. Последствия реализации различных типов риска

Важно понимать, что *реализация операционного рискованного события может сопровождаться только потерями* (или повышением возможности их получения). Это обстоятельство также является типологической особенностью операционного риска.

Итак, мы предлагаем следующее уточнённое определение операционного риска: *операционный риск – это риск потерь, вызванных:*

– *нарушением регламента процедуры выполнения внутреннего бизнес-процесса компании, источниками которого могут быть:*

- а) системы,
- б) персонал,
- в) внешние события;

– *неадекватностью (методической ошибочностью) процедуры выполнения внутреннего бизнес-процесса компании.*

Данное определение согласуется с общим принципом стандартов качества управления (ISO9000-2000): процессным подходом – согласно которому риск любого типа следует представлять в виде причинно-следственной модели, включающей в себя следующие компоненты: объект, источник, событие и его последствие (рис. 2).

В соответствии с предлагаемым определением операционного риска:

- *объектами операционного риска* являются внутренние бизнес-процессы компании;
- *источниками операционного риска*, т.е. причинами возникновения событий операционного риска, являются как внутренняя среда: системы, персонал, ошибки в технологии реализации внутреннего бизнес-процесса – так и внешняя;

⁵ Объект риска – любой финансовый инструмент, процесс, вид деятельности или операции, при исполнении которых может произойти ухудшение финансового состояния компании, потеря стоимости актива, увеличение стоимости обязательств, получение убытков или ухудшение технологий управления компанией [3].

- *операционным рисковым событием* или *событием операционного риска* (инцидентом) является нарушение процедуры выполнения внутреннего бизнес-процесса;
- *последствиями* реализации операционного рискового события являются прямые и/или косвенные операционные потери.

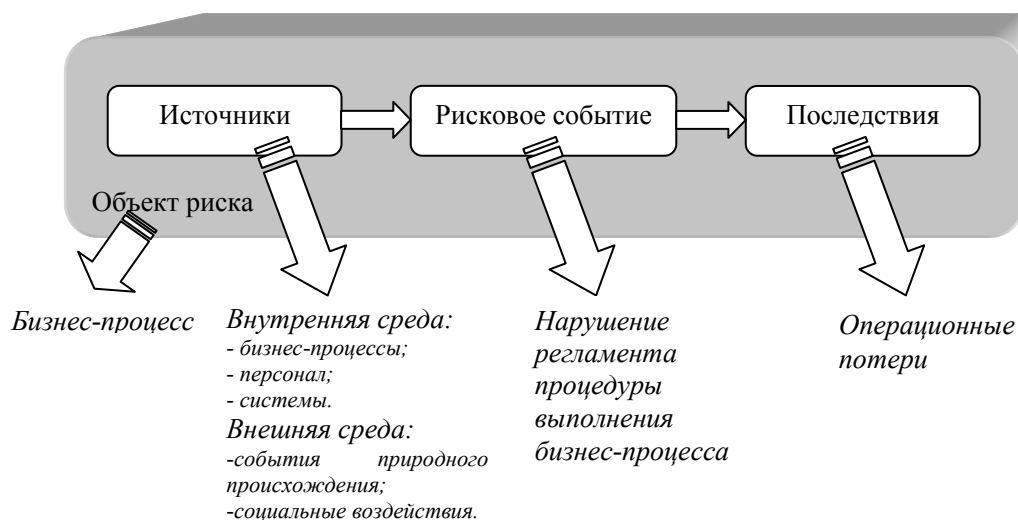


Рис. 2. Причинно-следственная модель операционного риска

3. Моделирование событий операционного риска с помощью байесовых технологий

3.1 Задание причинно-следственных схем событий операционного риска в виде байесовых модельных конструкций

Применение подходов на основе объективных вероятностей и методов формального статистического анализа (например, оценка параметров функции распределения потерь, методология VaR) для оценки операционных потерь крайне ограничено. Вероятностно-статистические методы могут применяться только для тех источников операционного риска, которые имеют характер массового проявления (например, для технологических сбоев, по которым возможно получить и аккумулировать статистику).

В большинстве же случаев количественное измерение параметров операционного риска, т.е. вероятности и существенности его последствий, затруднено или даже невозможно. Это обстоятельство обусловлено, прежде всего, тем, что подходы на основании объективных вероятностей предъявляют жёсткие требования к объёму исторических данных, необходимых для построения эмпирических функций распределения потерь. В настоящее время существенное большинство российских компаний, в том числе и телекоммуникационных, не имеют «богатых» баз релевантных данных об инцидентах реализации операционного риска.

Кроме того, вероятностная природа некоторых событий операционного риска крайне сложна. Так, совершенно ясно, что такие источники возникновения операционных потерь, как землетрясение, наводнение, террористический акт, потеря ключевого сотрудника, являются уникальными событиями, к которым не может быть применимо исчисление объективных вероятностей.

В таком положении полезным и продуктивным представляется подход на основании субъективной вероятности. *Субъективная вероятность* (условная, байесова) оценивается субъектом (экспертом) на основании индивидуального опыта, интуиции, знаний и *показывает меру*

доверия, степень убеждённости субъекта в вероятности данного события, поэтому субъективную вероятность можно приписать любым, даже уникальным событиям.

Если отдавать приоритет интеллектуальной комфортности и наибольшему методологическому совершенству, конечно, следует оперировать только объективными вероятностями, убедившись предварительно в выполнении, по крайней мере, свойства статистической устойчивости.

Однако при решении практических задач, когда не всегда и не везде это (свойство статистической устойчивости результатов экспериментов) выполнимо, нельзя пренебрегать зачастую имеющимся доброкачественным экспертным материалом, следствием которого и являются субъективные вероятности – основа построения байесовской сети. Байесовские сети – формальное представление для неопределённых, не точных знаний [21] и играют роль, примерно аналогичную той, которую выполняет пропозициональная логика применительно к определённым знаниям.

Наш методический выбор стимулирует ещё и осознание достижения возможности на этом пути автоматизировать технику и технологию совершенствования логического вывода при инжиниринге бизнес-процессов с вновь поступающей информацией (эксперты, рискованные прецеденты) о потенциальных операционных потерях. На этом пути в сфере высоких технологий уже имеются впечатляющие реализации. Так, одними из наиболее широко используемых систем на основе байесовских сетей оказались модули диагностики и восстановления (например, модуль Printer Wizard) в операционной системе Microsoft Windows и Office Assistant в пакете Microsoft Office [27].

Изложенные выше обстоятельства позволяют надеяться на то, что наиболее плодотворным подходом при моделировании операционных рискованных событий является применение байесовых технологий (уже достаточно тщательно разработанного направления формального представления неопределённых знаний). Данное утверждение основано на следующих выводах:

1. Как отмечено ранее, количественные характеристики некоторых событий операционного риска можно оценить преимущественно субъективно. Использование субъективных вероятностей в байесовых сетях (БС) является единственной альтернативой, если необходим учёт априорных мнений экспертов о возможности наступления события, к которому неприменимо понятие повторяемости, а также невозможно его описание в терминах совокупности элементарных событий. При этом в БС могут сочетаться эмпирические частоты появления различных состояний компонент операционного риска (т.е. события и его источники), теоретические представления об их математических вероятностях и субъективные оценки. Кроме этого, как замечено выше, последствиями реализации операционного рискованного события могут являться как прямые потери, так и косвенные. Возможность интегрирования данных количественного и качественного характера является существенным преимуществом БС.

2. БС дают возможность представлять исследуемый объект в виде системы причинно-следственных отношений с содержательной интерпретацией каждой переменной в терминах рассматриваемой проблемной области. Это позволяет моделировать зависимости между компонентами операционного риска (рис. 2), что способствует:

- учёту кумулятивных эффектов при воздействии на объект риска нескольких источников одновременно;
- системному представлению операционного риска;
- логической интерпретации результатов вероятностного вывода в сети.

3. Как замечено ранее, объектом операционного риска являются внутренние бизнес-процессы. В настоящее время для компаний характерно постоянное расширение перечня выполняемых бизнес-процессов, направлений деятельности, появление принципиально новых бизнес-функций. Всё это обуславливает динамичность *операционного рискованного профиля*⁶

⁶ В общем случае под рискованным профилем понимается совокупность оценённых рисков компании на определённый период [5].

и, соответственно, необходимость корректировки используемых модельных конструкций с учётом новой информации, что может быть легко реализовано именно в БС.

Бейесова сеть (Bayesian network, Bayes net, causal probabilistic network, Bayesian belief network, belief network) – это графовая модель описания отношений между переменными в проблемной области. Так, пусть некоторая проблемная область U состоит из множества переменных $U = \{x_1, \dots, x_n\}$, тогда БС данной проблемной области представляет собой множество локальных распределений условных вероятностей $P(x_i | x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_n)$ и множество утверждений об отношениях условной независимости переменных, которые позволяют генерировать ациклический направленный граф, представляющий её структуру. Каждая переменная БС может принимать множество взаимоисключающих состояний, каждое из которых соответствует определённому событию, вместе составляющих полную группу. Переменные проблемной области в БС выражаются в виде узлов (вершин), а условные вероятностные зависимости – в виде направленных дуг (рёбер). По сути, БС являются способом представления экспертных знаний в условиях неопределённости.

БС позволяют осуществлять т.н. логический (или вероятностный) вывод, т.е. вычислять апостериорные вероятностные распределения переменных на основании априорных глобальных совместных распределений, генерируемых из совокупности априорных локальных распределений. Математическим основанием такого вычисления служит *теорема Т.Бейеса*:

$$P(x_i | x_j, \dots, x_k) = \frac{P(x_i, x_j, \dots, x_k)}{P(x_j, \dots, x_k)}, \quad (1)$$

где $P(x_i | x_j, \dots, x_k)$ – апостериорное локальное вероятностное распределение;
 $P(x_i, x_j, \dots, x_k)$ и $P(x_j, \dots, x_k)$ – априорные глобальные вероятностные распределения.

Бейесовы технологии могут использоваться при принятии решений в условиях неопределённости. Согласно теории принятия решений, ситуация принятия решения содержит три компоненты:

- что ЛПР может сделать (альтернативы решения);
- что ЛПР знает (его доверие);
- что ЛПР хочет получить (его предпочтения).

Эти составляющие могут быть смоделированы с помощью разновидности БС – диаграмм влияния (ДВ) [23].

Диаграмма влияния (influence diagram) представляет собой графовую модель представления экспертных знаний, служащую для обоснования принимаемых решений в условиях неопределённости. ДВ, как и БС, содержит узлы, представляющие переменные проблемной области, которые отражают доверие ЛПР (субъективные вероятности)⁷. Однако, помимо случайных узлов, ДВ также содержат узлы решения, представляющие множество взаимоисключающих альтернатив решения; и узлы полезности, моделирующие предпочтения ЛПР, т.е. полезность каждой альтернативы решения (рис. 3).

Дуги, представляющие условные вероятностные зависимости переменных БС, называются существенными (relevance). ДВ, кроме существенных, также содержат информационные дуги, показывающие, какая информация известна ЛПР в момент принятия решения. Если состояние случайного узла ДВ оказывает влияние на принятие ЛПР решения, то в ДВ необходимо добавить связь от данного случайного узла к узлу решения.

⁷ Данные переменные называются случайными узлами или узлами состояний.

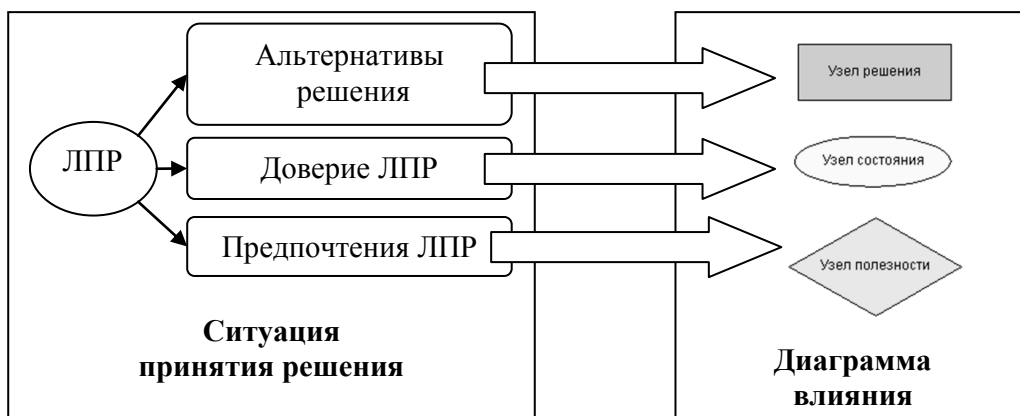


Рис. 3. Моделирование ситуации принятия решения с помощью диаграммы влияния

Таким образом, порядок следования случайных узлов и узлов решения в ДВ должен быть следующим:

$$I_0, D_1, I_1, D_2, \dots, D_n, I_n \quad (2)$$

где I_{i-1} – набор случайных узлов, состояние которых известно до принятия решения D_i , $\forall i = \overline{1, n}$;

I_n – набор случайных узлов, состояние которых станет известно после принятия решения D_n .

Следует заключить, что ДВ – это инструмент нахождения оптимальной альтернативы решения, которая наиболее выгодна (полезна) в условиях предоставленной информации исходя из принципа максимизации ожидаемой полезности.

Процесс моделирования проблемной области с помощью байесовых технологий может быть обобщённо представлен в виде последовательности действий, отражённых на рис. 4.



Рис. 4. Схема процесса моделирования проблемной области с помощью байесовых технологий

Применительно к процессу управления рисками первый этап представленной схемы соответствует процедуре идентификации рисков; второй – их анализу; третий – оценке (рис. 12).

Этап 1

При моделировании операционного риска в качестве переменных следует рассматривать его компоненты, а именно: источники, операционное рисковое событие, последствия его реализации (рис. 2). Данные переменные могут принимать два взаимоисключающих состояния: «да=1» и «нет=0» – и, соответственно, являются булевыми.

Для идентификации операционного риска первоначально необходимо определить объекты, на которых реализуются операционные рисковые события. Как отмечено ранее, объектами операционного риска являются бизнес-процессы компании. К настоящему моменту международной организацией TeleManagement Forum разработана универсальная модель бизнес-процессов телекоммуникационных компаний, поддерживаемая Международным телекоммуникационным союзом (ITU) [13, 15]. Расширенная карта процессов телекоммуникационной отрасли (enhanced Telecom Operations Map), представленная на рис. 5, может служить основой для разработки индивидуальной модели бизнес-процессов компании.

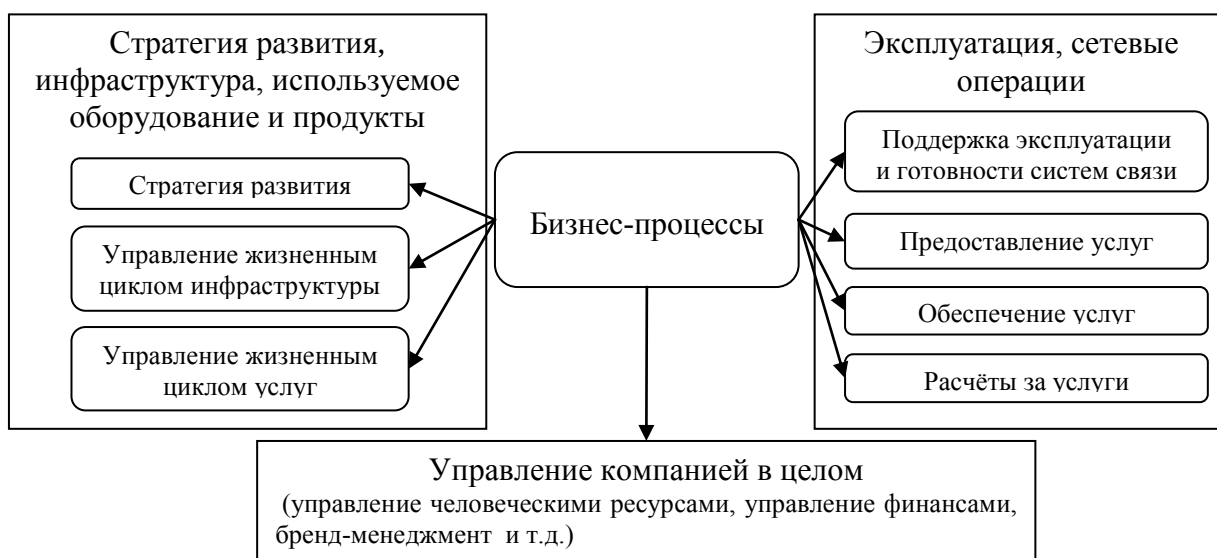


Рис. 5. Расширенная карта процессов телекоммуникационной отрасли [15]

Для того чтобы выявить возможные события операционного риска на конкретном бизнес-процессе, необходимо определить, какие неблагоприятные события могут произойти при его выполнении. В качестве операционных рисковых событий, характерных для бизнес-процессов телекоммуникационных компаний, можно привести:

- простои каналов и трактов;
- нарушение плана строительства объектов связи;
- ошибки при выставлении счетов пользователям;
- ошибки при взаиморасчётах с операторами.

Для того чтобы выявить источники конкретного операционного рискового события, необходимо определить причины его возникновения. В качестве источников операционных рисковых событий, характерных для бизнес-процессов телекоммуникационных компаний, можно привести:

- отказы станционного оборудования из-за нарушений правил технической эксплуатации;
- повреждения линейно-кабельных сооружений из-за нарушений правил технической эксплуатации;

- повреждения линейно-кабельных сооружений из-за действий сторонних организаций;
- повреждения линейно-кабельных сооружений из-за действий природного характера: мерзлотные явления, удары молнии, затопления, подвижки грунта, пожары, ураганы и т.д.;
- отказы электропитающих устройств;
- сбои информационных систем.

Для того чтобы выявить последствия реализации конкретного операционного рисковогго события, необходимо определить потери, к которым оно может привести. В качестве последствий операционных рисковогго событий, характерных для бизнес-процессов телекоммуникационных компаний, можно привести:

- недополученные доходы из-за простоев каналов;
- недополученные доходы из-за незаконной передачи трафика по сетям компании;
- затраты на ремонт и восстановление работы повреждённого участка сети;
- затраты на ремонт и восстановление работы оборудования связи;
- затраты на восстановление потерянных данных;
- штрафы за нанесение экологического ущерба при строительстве сетей.

Следует иметь в виду, что для одного и того же бизнес-процесса могут быть характерны несколько событий операционного риска; а также то, что каждое событие операционного риска может иметь как несколько источников возникновения, так и несколько последствий его реализации (рис. 6).

Разумно полагать, что идентификация операционного риска на конкретном бизнес-процессе может быть реализована только экспертно на основании суждений владельцев данного бизнес-процесса. Это обстоятельство объясняется тем, что только специалисты, облагающие глубокими знаниями о процедурах выполнения внутренних бизнес-процессов, способны идентифицировать возможные операционные рисковогго события на определённом бизнес-процессе, выявить их источники и последствия. Риск-менеджеры (специалисты службы внутреннего контроля, внутреннего аудита) должны осуществлять организационно-методическую и консультационную поддержку процесса идентификации.

Полезной, с точки зрения осуществления анализа информации, полученной при идентификации от владельцев бизнес-процессов, видится разработка риск-менеджерами на её основании классификационной модели операционного риска. *Классификационная модель операционного риска* компании должна включать в себя однородные группы:

- типов объектов операционных рисковогго событий;
- типов операционных рисковогго событий;
- типов источников возникновения операционных рисковогго событий;
- типов последствий реализации операционных рисковогго событий (рис. 6).

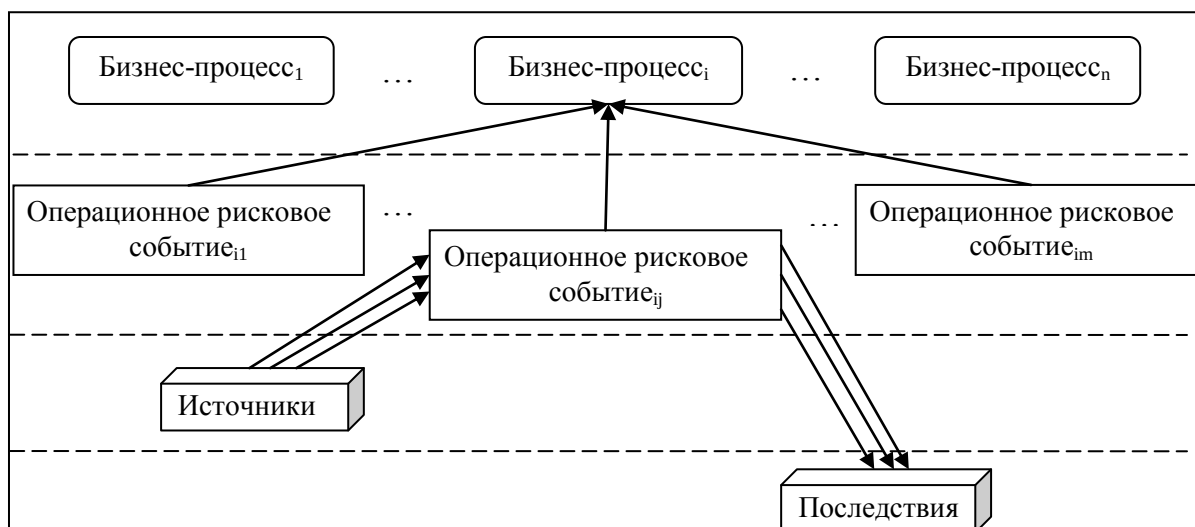


Рис. 6. Структура классификационной модели операционного риска

Этап 2

Данный этап подразумевает консолидацию, обработку и преобразование риск-менеджерами информации, полученной на предыдущем этапе, путём построения топологии (т.е. структуры) ДВ, моделирующих причинно-следственные схемы идентифицированных событий операционного риска (рис. 7). При этом, применяя инструментарий ДВ, следует представлять:

- источники возникновения события операционного риска в качестве случайных узлов;
- событие операционного риска в качестве случайного узла;
- последствия реализации события операционного риска в качестве узлов полезности.

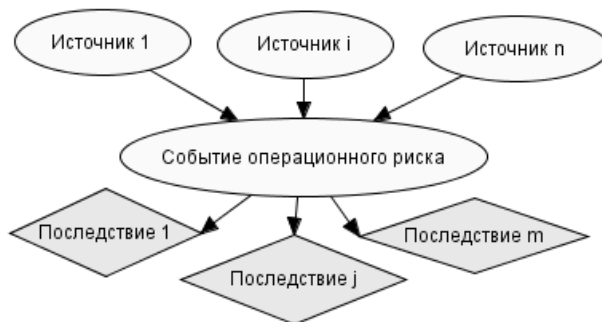


Рис. 7. Диаграмма влияния, моделирующая причинно-следственную схему события операционного риска

Этап 3

Разработанную на предыдущем этапе структурную модель ДВ необходимо наполнить количественными данными, т.е. совокупностью таблиц условных вероятностей для случайных узлов и таблиц полезности для узлов полезности. Для рассматриваемого случая (рис. 7) должны быть определены:

- безусловные⁸ вероятности состояний узлов, представляющих источники возникновения операционного рискованного события (И): $P(I_i = l)$, $i = \overline{1, n}$; $l = 0, 1$;
- условные вероятности состояний узла, представляющего операционное рискованное событие (ОРС): $P(ОРС = k | I_1 = l, \dots, I_n = s)$, $k, l, s = 0, 1$;
- величина потерь при реализации операционного рискованного события (П), по сути, антиполезность: $U(P_j | ОРС = 1)$, $j = \overline{1, m}$. Важно заметить, что $U(P_j | ОРС = 0) = 0$, $j = \overline{1, m}$, так как в случае нереализации операционного рискованного события компания не несёт операционные потери.

В настоящее время разработаны алгоритмы, позволяющие определять распределения вероятностей нахождения переменных, соответствующих узлам БС или ДВ, в определённом состоянии из эмпирических данных (например, алгоритм ЕМ) [18]. Однако применение любого алгоритма обучения предполагает наличие большого объёма обучающих данных, что в случае операционного риска, как неоднократно отмечалось ранее, пока не представляется возможным.

Поэтому на начальных этапах разработки и внедрения системы оценки операционного риска, пока не будет собран достаточный объём исторических данных о фактических операционных потерях, видятся полезными следующие процедуры получения информации.

Вероятности реализации источников операционного рискованного события могут быть оценены как экспертно (владельцами бизнес-процессов и владельцами ресурсов), так и с помощью методов формального анализа. Так, например, теория надёжности может быть применена для оценки вероятности технологических сбоев; теория массового обслуживания – для оценки вероятности ухудшения качества обслуживания потребителей в связи с занятостью каналов

⁸ так как данные узлы не имеют предшествующих узлов

связи и т.д. Однако важно при этом осуществлять поправку полученных значений с учётом состояния внутренней и внешней среды данной конкретной организации.

Условные вероятности реализации операционного рисковогго события в зависимости от комбинации состояний источников его возникновения, на наш взгляд, следует оценивать экспертным путём (владельцами бизнес-процессов), так как они существенным образом зависят от индивидуальных особенностей организации: эффективности системы внутреннего контроля, психологического климата в коллективе, эффективности системы внутренней безопасности и т.д. Важно обратить внимание на то, что возможность учёта в ДВ совместного влияния состояний узлов-предков на состояние узлов-потомков позволяет моделировать кумулятивные эффекты или концентрацию источников операционного рисковогго события, увеличивающих вероятность его возникновения (как правило, это нелинейный рост).

Величина потерь, которыми сопровождается реализация операционного рисковогго события, может быть определена или из предыдущих прецедентов, или экспертно (владельцами бизнес-процессов), в случае если данное событие крайне редкое.

Риск-менеджеры должны осуществлять организационно-методическую и консультационную поддержку процесса оценки количественных характеристик компонент операционного риска, а также интегрировать полученную информацию в разработанные структурные модели ДВ.

3.2 Аналитические возможности бейесовых технологий в операционном риск-менеджменте

Результатом выполнения перечисленной выше последовательности действий должна стать модель причинно-следственной схемы конкретного операционного рисковогго события на конкретном объекте риска (внутреннем бизнес-процессе), представленная в виде ДВ.

Разработанные ДВ дают широкие аналитические возможности, основанные на применении методов теории вероятностей и теории принятия решений.

Универсальным и уже стандартно используемым графическим инструментом анализа риска любого типа является т.н. *карта рисков* [5, 6]. Как правило, карта рисков представляет собой графическое описание перечня рисков по двум категориям: вероятность (частота возникновения) и существенность (величина последствий) (рис. 8).

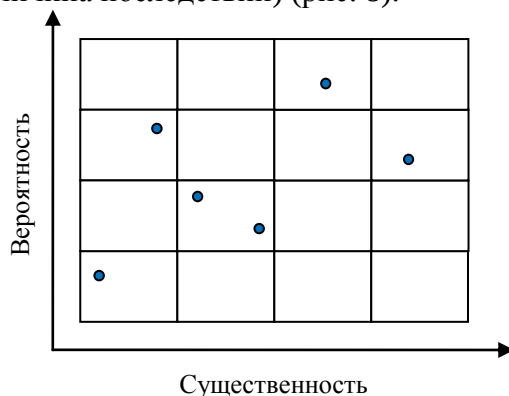


Рис. 8. Карта рисков

Применительно к целям операционного риск-менеджмента карта рисков может быть построена по количественным характеристикам каждого идентифицированного операционного рисковогго события, а именно по:

- вероятности его возникновения, вычисляемой по формуле полной вероятности [4]:

$$P(OPC = 1) = \sum_{l,s} P(OPC = 1 | I_1 = l, \dots, I_n = s) \times P(I_1 = l) \times \dots \times P(I_n = s), \quad l, s = 0, 1; \quad (3)$$

– величине потерь при его реализации

$$U(\Pi) = \sum_{j=1}^m U(\Pi_j | OPC = 1). \quad (4)$$

Основной целью картографирования риска любого типа выступает их ранжирование по уровню значимости с целью выделения наиболее критичных категорий. С точки зрения операционного риск-менеджмента, значимость операционного рисковог события определяется ожидаемой величиной потерь при его реализации, вычисляемой следующим образом:

$$EU(\Pi) = \sum_{k=0}^1 \sum_{j=1}^m U(\Pi_j | OPC = k) \times P(OPC = k), \quad (5)$$

$$P(OPC = k) = \sum_{l,s} P(OPC = k | I_1 = l, \dots, I_n = s) \times P(I_1 = l) \times \dots \times P(I_n = s), \quad k, l, s = 0, 1. \quad (6)$$

Карты по операционным рисковым событиям могут быть построены как для компании в целом, так и для её отдельных подразделений и бизнес-процессов. Важно заметить, что возможности байесовых технологий позволяют также получать данные, необходимые для построения карт по операционным рисковым событиям для групп источников их возникновения, а именно:

– вероятность возникновения данного операционного рисковог события с учётом вероятности состояний узла, представляющего его i -ый источник, вычисляемая исходя из формулы Байеса следующим образом:

$$P(OPC = 1 | I_1 = 0, \dots, I_{i-1} = 0, I_{i+1} = 0, \dots, I_n = 0) = \frac{P(OPC = 1, I_1 = 0, \dots, I_{i-1} = 0, I_{i+1} = 0, \dots, I_n = 0)}{P(I_1 = 0, \dots, I_{i-1} = 0, I_{i+1} = 0, \dots, I_n = 0)}, \quad i = \overline{1, n}. \quad (7)$$

Совместная вероятность комбинации состояний узлов $OPC = 1, I_1 = 0, \dots, I_{i-1} = 0, I_{i+1} = 0, \dots, I_n = 0, i = \overline{1, n}$ ($P(OPC = 1, I_1 = 0, \dots, I_{i-1} = 0, I_{i+1} = 0, \dots, I_n = 0)$) и $I_1 = 0, \dots, I_{i-1} = 0, I_{i+1} = 0, \dots, I_n = 0, i = \overline{1, n}$ ($P(I_1 = 0, \dots, I_{i-1} = 0, I_{i+1} = 0, \dots, I_n = 0)$) вычисляется исходя из теоремы умножения вероятностей [4] и отношений условной независимости переменных:

$$P(OPC = 1, I_1 = 0, \dots, I_{i-1} = 0, I_{i+1} = 0, \dots, I_n = 0) = \sum_{l=0}^1 P(OPC = 1 | I_1 = 0, \dots, I_i = l, \dots, I_n = 0) \times P(I_1 = 0) \times \dots \times P(I_i = l) \times \dots \times P(I_n = 0), \quad i = \overline{1, n}, \quad (8)$$

$$P(I_1 = 0, \dots, I_{i-1} = 0, I_{i+1} = 0, \dots, I_n = 0) = P(I_1 = 0) \times \dots \times P(I_{i-1} = 0) \times P(I_{i+1} = 0) \times \dots \times P(I_n = 0), \quad i = \overline{1, n}, \quad (9)$$

– величину потерь при реализации данного операционного рисковог события (формула 4).

Также важным практическим преимуществом байесовых технологий является то, что они позволяют уточнять распределения вероятностей переменных на основании наблюдаемых (даже неполных) данных. В байесовой терминологии этот процесс называется *адаптацией сети* [18, 21].

Предположим, что получено свидетельство⁹ о том, что произошло операционное рисковое событие (отчёт о факте его реализации, см. раздел 4), однако источник его возникновения не установлен. Тогда локальная вероятность нахождения узла, представляющего в ДВ данное операционное рисковое событие, в k -ом состоянии по всем комбинациям состояний узлов-предков (источников) находится по формуле 10:

$$P^*(\text{ОРС} = k | I_1 = l, \dots, I_n = s) = \frac{N^*(\text{ОРС} = k | I_1 = l, \dots, I_n = s)}{\sum_{k=0}^1 N^*(\text{ОРС} = k | I_1 = l, \dots, I_n = s)}, \quad k, l, s = 0, 1, \quad (10)$$

где $N^*(\text{ОРС} = k | I_1 = l, \dots, I_n = s)$ – количество наблюдений k -го состояния узла ОРС по комбинациям состояний узлов I_i , с учётом полученного свидетельства.

$$\begin{aligned} N^*(\text{ОРС} = k | I_1 = l, \dots, I_n = s) \\ = N(\text{ОРС} = k | I_1 = l, \dots, I_n = s) + N_{ad}(\text{ОРС} = k) \\ \times P(I_1 = l, \dots, I_n = s | \text{ОРС} = k), \quad k, l, s = 0, 1, \end{aligned} \quad (11)$$

где $N(\text{ОРС} = k | I_1 = l, \dots, I_n = s)$ – количество наблюдений k -го состояния узла ОРС по комбинациям состояний узлов I_i до того, как получено свидетельство;

$N_{ad}(\text{ОРС} = k)$ – количество новых наблюдений k -го состояния узла ОРС (свидетельство);

$P(I_1 = l, \dots, I_n = s | \text{ОРС} = k)$ – совместная вероятность комбинации состояний узлов $I_1 = l, \dots, I_n = s$ при условии, что узел ОРС находится в k -ом состоянии.

Исходя из условий рассматриваемой ситуации, $N_{ad}(\text{ОРС} = 1) = 1$, тогда

для $k = 0$

$$\begin{aligned} N^*(\text{ОРС} = 0 | I_1 = l, \dots, I_n = s) \\ = N(\text{ОРС} = 0 | I_1 = l, \dots, I_n = s) + N_{ad}(\text{ОРС} = 0) \\ \times P(I_1 = l, \dots, I_n = s | \text{ОРС} = 0) = N(\text{ОРС} = 0 | I_1 = l, \dots, I_n = s), \\ l, s = 0, 1, \end{aligned} \quad (12)$$

для $k = 1$

$$\begin{aligned} N^*(\text{ОРС} = 1 | I_1 = l, \dots, I_n = s) \\ = N(\text{ОРС} = 1 | I_1 = l, \dots, I_n = s) + N_{ad}(\text{ОРС} = 1) \\ \times P(I_1 = l, \dots, I_n = s | \text{ОРС} = 1) \\ = N(\text{ОРС} = 1 | I_1 = l, \dots, I_n = s) + P(I_1 = l, \dots, I_n = s | \text{ОРС} = 1), \\ l, s = 0, 1. \end{aligned} \quad (13)$$

Если оценивание распределений вероятностей в ДВ проводилось не по фактическим данным, а на основании субъективных экспертных оценок и при этом нет достаточной уверенности в их существенности, то стоит задать $N(\text{ОРС} = k | I_1 = l, \dots, I_n = s)$, $k, l, s = 0, 1$, незначительным (например, равным 10).

Совместная вероятность комбинации состояний узлов $I_1 = l, \dots, I_n = s$;

⁹ Термин свидетельство (evidence) в бейесовой методологии обозначает получение наблюдения о состоянии переменной.

$l, s = 0, 1$, при условии, что узел ОРС находится в k -ом состоянии, т.е. апостериорная вероятность $(P(I_1 = l, \dots, I_n = s | OPC = k), k, l, s = 0, 1,)$, определяется исходя из формулы Байеса (формула 1) следующим образом:

$$P(I_1 = l, \dots, I_n = s | OPC = 1) = \frac{P(I_1 = l, \dots, I_n = s, OPC = 1)}{P(OPC = 1)}, \quad l, s = 0, 1. \quad (14)$$

Априорная совместная вероятность комбинации состояний узлов $I_1 = l, \dots, I_n = s, OPC = 1; l, s = 0, 1, (P(I_1 = l, \dots, I_n = s, OPC = 1))$ вычисляется исходя из теоремы умножения вероятностей [4] и отношений условной независимости переменных:

$$P(I_1 = l, \dots, I_n = s, OPC = 1) = P(OPC = 1 | I_1 = l, \dots, I_n = s) \times P(I_1 = l) \times \dots \times P(I_n = s), \quad l, s = 0, 1. \quad (15)$$

Полученное наблюдение $(N_{ad}(OPC = 1) = 1)$ изменит не только локальное распределение вероятностей состояний узла ОРС (формула 10), но и распределение вероятностей состояний узлов $I_i, i = \overrightarrow{1, n}$, (формула 16) вследствие того, что они становятся d-связанными как предки конкретизированного¹⁰ узла в конвергентном соединении [26].

$$P^*(I_i = k) = \frac{N^*(I_i = k)}{\sum_{k=0}^1 N^*(I_i = k)}, \quad i = \overrightarrow{1, n}; k = 0, 1. \quad (16)$$

Формулы 17 – 19 аналогичны формулам 12 – 15.

$$N^*(I_i = k) = N(I_i = k) + N_{ad}(OPC = 1) \times P(I_i = k | OPC = 1), \quad i = \overrightarrow{1, n}; k = 0, 1, \quad (17)$$

$$P(I_i = k | OPC = 1) = \frac{P(I_i = k, OPC = 1)}{P(OPC = 1)}, \quad i = \overrightarrow{1, n}; k = 0, 1, \quad (18)$$

$$\begin{aligned} P(I_i = k, OPC = 1) &= \sum_{l, s} P(OPC = 1 | I_1 = l, \dots, I_n = s) \times P(I_1 = l) \times \dots \times P(I_i = k) \times \dots \\ &\times P(I_n = s), \quad i = \overrightarrow{1, n}; k, l, s = 0, 1, \end{aligned} \quad (19)$$

Ясно, что основной оперативной целью управления операционным риском является снижение ожидаемых операционных потерь до приемлемого для компании уровня. Уровень «приемлемости» определяется (как и во всех других аспектах управления) соотношением затраты/результаты. Снижение уровня ожидаемых операционных потерь возможно путём осуществления управленческих воздействий на источники возникновения операционных рисков событий, точнее, на вероятность их реализации. Так, для такого источника возникновения событий операционного риска, как повреждение линейно-кабельных сооружений, в качестве мероприятий по снижению вероятности его реализации можно привести:

- проведение ремонтно-профилактических работ;
- проведение капитального ремонта;
- выноска кабеля из опасных зон (зон застройки и разрушений);
- защита кабеля от электрохимической коррозии, ударов молний и др.;
- проведение просветительской работы среди населения и т.д.

¹⁰ Узел БС или ДВ считается конкретизированным, если его состояние становится известно.

Результат осуществления управленческих воздействий на источники возникновения событий операционного риска может быть отражён графически с помощью карты риска в виде миграции «точек риска» в наименее критичные зоны¹¹ (рис. 9).

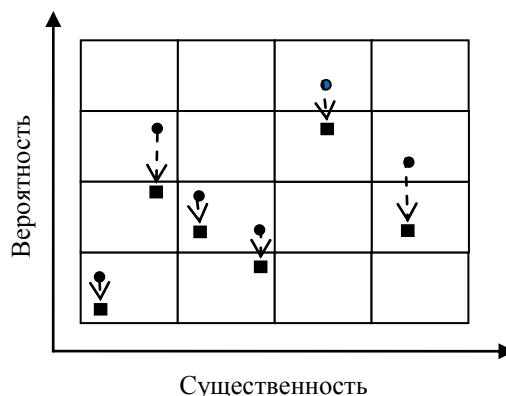


Рис. 9 Карта рисков

Как замечено ранее, ДВ позволяют найти оптимальную стратегию в ситуации принятия решения, поэтому чтобы определить эффективность применения того или иного мероприятия по снижению вероятности реализации источников возникновения операционного рисков события, достаточно в моделирующую его ДВ (рис. 7) ввести узел решения, соответствующий данному мероприятию, и узел полезности, отражающий стоимость его реализации (рис. 10).



Рис. 10. Диаграмма влияния, моделирующая ситуацию осуществления управленческого воздействия на источник события операционного риска

Переменная, представляющая мероприятие по снижению вероятности реализации источников возникновения операционного рисков события (M_i), также является булевой, так как может принимать два взаимоисключающих состояния: «да, осуществлять=1» и «нет, не осуществлять=0».

Введение в ДВ узла решения, соответствующего переменной M_i , $i = \overline{1, n}$, приводит к необходимости задания:

– вероятности состояний узла I_i , $i = \overline{1, n}$: $P(I_i = s | M_i = g)$, $i = \overline{1, n}$; $g, s = 0, 1$. Ясно, что для $g = 0$ вероятности $P(I_i = s | M_i = 0)$, $i = \overline{1, n}$; $s = 0, 1$, соответствуют их прежним значениям (т.е. до добавления в ДВ узла решения M_i , $i = \overline{1, n}$ (рис. 7)), а вероятности $P(I_i = s | M_i = 1)$, $i = \overline{1, n}$; $s = 0, 1$, отражают снижение вероятности реализации i -го источника возникновения операционного рисков события при воздействии на него мероприятия M_i , $i =$

¹¹ Расчёт вероятности реализации события операционного риска, при условии осуществления мероприятий по снижению вероятности возникновения его источников, осуществляется по формуле 24.

$\overrightarrow{1, n};$

– стоимости реализации мероприятия M_i в виде $U(C_i|M_i = 1), i = \overrightarrow{1, n}$, тогда как $U(C_i|M_i = 0) = 0$.

Следует заметить, что разработка мероприятий по снижению вероятности реализации источников возникновения событий операционного риска, а также оценка их количественных характеристик требуют совместной работы владельцев бизнес-процессов, владельцев ресурсов и риск-менеджеров.

Итак, осуществление мероприятия $M_i, i = \overrightarrow{1, n}$, целесообразно, если выполняется следующее неравенство:

$$|U(C_i|M_i = 1)| < EU(\Pi|M_i = 1) - EU(\Pi|M_i = 0), \quad i = \overrightarrow{1, n}, \quad (20)$$

где $U(C_i|M_i = 1)$ – стоимость реализации мероприятия M_i ;

$EU(\Pi|M_i = 1)$ – ожидаемые операционные потери при условии, что узел M_i находится в состоянии 1;

$EU(\Pi|M_i = 0)$ – ожидаемые операционные потери при условии, что узел M_i находится в состоянии 0.

Правая часть неравенства 20 отражает сокращение операционных потерь за счет снижения вероятности реализации источника $I_i, i = \overrightarrow{1, n}$, операционного рисковог события, вызванного осуществлением мероприятия $M_i, i = \overrightarrow{1, n}$.

Иначе говоря, исходя из основного принципа теории принятия решений: максимизации ожидаемой полезности – оптимальная альтернатива (состояние) в узле решения $M_i, i = \overrightarrow{1, n}$, определяется по формуле 21:

$$g^* = g | \max(EU(M_i = g)), \quad i = \overrightarrow{1, n}; g = 0, 1, \quad (21)$$

где $EU(M_i = g)$ – ожидаемая полезность при нахождении узла M_i в состоянии g .

$$EU(M_i = g) = U(C_i|M_i = g) + EU(\Pi|M_i = g), \quad i = \overrightarrow{1, n}; g = 0, 1, \quad (22)$$

где $U(C_i|M_i = g)$ – стоимость нахождения узла M_i в состоянии g ;

$EU(\Pi|M_i = g)$ – ожидаемые операционные потери при условии, что узел M_i находится в состоянии g .

Ожидаемые операционные потери при условии, что узел $M_i, i = \overrightarrow{1, n}$ находится в состоянии g , определяются, исходя из формулы 5, следующим образом:

$$EU(\Pi|M_i = g) = \sum_{k=0}^1 \sum_{j=1}^m U(\Pi_j | OPC = k) \times P(OPC = k | M_i = g), \quad i = \overrightarrow{1, n}; g = 0, 1. \quad (23)$$

Вероятность нахождения узла ОРС в k -ом состоянии при условии, что узел $M_i, i = \overrightarrow{1, n}$, находится в состоянии g ($P(ОРС = k | M_i = g), i = \overrightarrow{1, n}; k, g = 0, 1$), вычисляется по редуцированной формуле полной вероятности:

$$\begin{aligned} P(ОРС = k | M_i = g) &= \sum_{l, s, t} P(ОРС = k | I_1 = l, \dots, I_i = s, \dots, I_n = t) \times P(I_1 = l) \times \dots \\ &\times P(I_i = s | M_i = g) \times \dots \times P(I_n = t), \quad i = \overrightarrow{1, n}; \quad g, k, l, s, t = 0, 1. \end{aligned} \quad (24)$$

Стоит заметить, что так как для $g = 0 \quad U(C_i | M_i = 0) = 0, i = \overrightarrow{1, n}$, и $P(I_i = s | M_i = 0) = P^*(I_i = s), i = \overrightarrow{1, n}; s = 0, 1$, где $P^*(I_i = s)$ – вероятность нахождения узла I_i в состоянии s , заданная для ДВ, не включающей узел решения M_i (рис. 7), то

$$EU(M_i = 0) = EU^*(\Pi), \quad i = \overrightarrow{1, n}, \quad (25)$$

где $EU^*(\Pi)$ – ожидаемые операционные потери, соответствующие ДВ, не включающей узел решения M_i .

Таким образом, обобщая изложенное, можно заключить, что моделирование причинно-следственной схемы операционного рискованного события в виде ДВ даёт возможность определять:

- полную вероятность реализации операционного рискованного события с учётом вероятностей состояний его источников и их взаимовлияния;
- ожидаемую величину операционных потерь с учётом полной вероятности реализации операционного рискованного события;
- любые априорные вероятностные распределения компонент причинно-следственной схемы операционного рискованного события на основании апостериорной информации, в том числе позволяет осуществлять адаптацию их локальных вероятностных распределений;
- целесообразность осуществления мероприятия по снижению вероятности реализации источников возникновения операционного рискованного события путём сопоставления его стоимости и величины снижения ожидаемых операционных потерь в результате его проведения.

4. Подходы к автоматизации процесса управления операционным риском

Построение робастных модельных конструкций событий операционного риска, имеющих предсказательную силу, возможно только на репрезентативном объёме исторических данных. В этой связи, важной видится постановка процесса управления операционным риском на непрерывную системную основу. Для этого, главным образом, необходимы разработка и внедрение комплексной информационно-аналитической среды, в рамках которой должны осуществляться все процедуры управления операционным риском.

Любой управленческий процесс представляет собой процесс управления информацией (рис. 11).

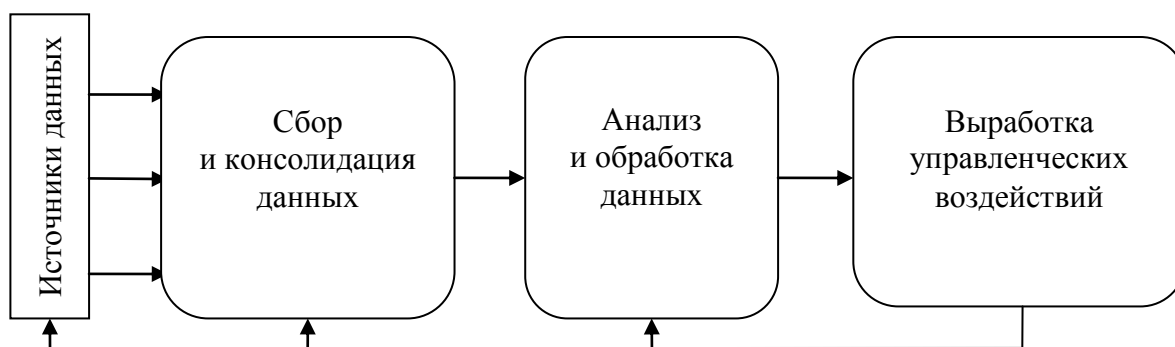


Рис. 11. Обобщённая схема управленческого процесса

Как и во всех других методологических аспектах риск-менеджмента, общепринятого формата управления риском пока не разработано. Обобщённое определение понятия «*управление риском*», которое отражает состав работ, признаваемый всеми специалистами, сводится к следующему – это процесс идентификации и оценки уровня риска с последующим выбором образа действия (рис. 12).

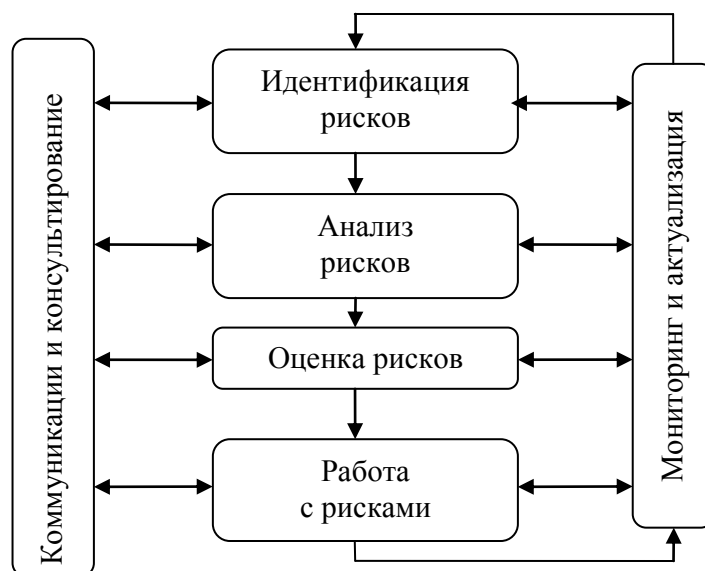


Рис. 12. Схема процесса управления рисками по австралийско-новозеландскому стандарту [5]

Сопоставление схем, представленных на рис. 11 и 12, показывает, что этап «Коммуникации и консультирования» (рис. 12) соответствует этапу «Сбор и консолидация данных» (рис. 11); этапы «Идентификация рисков», «Анализ рисков», «Оценка рисков» (рис. 12) – этапу «Анализ и обработка данных» (рис. 11); этап «Работа с рисками» (рис. 12) – этапу «Выработка управленческих воздействий» (рис. 11); этап «Мониторинг и актуализация» (рис. 12) – обратной связи в схеме (рис. 11).

Далее описываются процедуры, позволяющие придать процессу управления операционным риском комплексный непрерывный характер с учётом того, что в компании проведена первоначальная диагностика операционного рискованного профиля, т.е. построены в эскизном варианте причинно-следственные схемы событий операционного риска и заданы в виде ДВ (см. раздел 3).

Идентификация операционного риска

Идентификация событий операционного риска на внутренних бизнес-процессах компании должна иметь непрерывный характер. Это объясняется как тем, что процедуры выполнения существующих бизнес-процессов регулярно корректируются вследствие изменения технических, организационных, методических и др. условий их выполнения; так и тем, что перечень бизнес-процессов компании постоянно расширяется в связи с внедрением новых направлений деятельности. По сути, процедура идентификации операционного риска представляет собой выявление новых или ранее неучтённых:

- событий операционного риска, которые могут возникнуть на данном объекте риска (т.е. бизнес-процессе);
- источников возникновения данных событий;
- возможных последствий реализации данных событий.

Для этого владельцы бизнес-процессов должны с определённой периодичностью (оптимальным периодом мониторинга видится один год¹²) анализировать «свои» бизнес-процессы и доводить в установленной форме до сведения риск-менеджеров выявленные на них новые уязвимости к операционному риску.

Анализ операционного риска

Информация, полученная от владельцев-бизнес-процессов на этапе идентификации операционного риска, должна быть соответствующим образом агрегирована и систематизирована риск-менеджерами. Содержательно этап анализа операционного риска подразумевает:

- совершенствование классификационной модели операционного риска компании путём добавления новых или уточнения существующих классификационных групп объектов операционного риска (бизнес-процессов или отдельных бизнес-операций), событий операционного риска, источников их возникновения и последствий их реализации и др. (рис. 6);
- разработку новых (вновь выявленных) или актуализацию существующих моделей причинно-следственных схем событий операционного риска и их преобразование в ДВ (см. раздел 3).

Оценка операционного риска

В рамках данного этапа принципиальной видится организация непрерывного процесса регистрации случаев реализации событий операционного риска на всех объектах риска путём предоставления в оперативном режиме соответствующих отчётов в отдел по управлению рисками. Отчёты о фактах реализации событий операционного риска следует составлять в специализированной форме, которая как минимум должна содержать следующие поля:

- дата реализации события;
- подразделение, должность лица, выявившего событие;
- описание события;
- описание бизнес-процесса, на котором произошло событие;
- владелец данного бизнес-процесса;
- описание источников, вызвавших событие;
- описание последствий реализации события.

Полнота заполнения перечисленных элементов определяется наличием информации, а также уровнем корпоративной культуры операционного риск-менеджмента в компании (в смысле понимания его базовых методических аспектов всем менеджментом). При этом следует заметить, что при составлении отчётов сотрудники могут заполнять его, как руководствуясь разработанной классификационной моделью операционного риска (рис. 6), так и в свободной форме, если категоризация вызывает затруднения. На основе этого описания риск-

¹² В случае разработки нового бизнес-процесса его внедрение должно предваряться подобным анализом.

менеджеры должны самостоятельно провести категоризацию всех компонент данного события операционного риска.

Отчёты о фактах реализации событий операционного риска позволяют риск-менеджерам:

- совершенствовать классификационную модель операционного риска в случае выявления компонент причинно-следственной схемы событий операционного риска, которых нельзя отнести к существующим классификационным группам (рис. 6);
- актуализировать ДВ, моделирующие причинно-следственные схемы событий операционного риска, в случае выявления их новых компонент; или разрабатывать ДВ для вновь выявленных событий операционного риска (см. раздел 3)¹³;
- проводить уточнение локальных вероятностных распределений компонент причинно-следственной схем событий операционного риска на основании описанной в разделе 3 процедуры адаптации сети.

Основным выходом данного этапа должна служить консолидированная аналитическая отчётность по различным направлениям, например, ожидаемые операционные потери:

- по классификационным группам объектов риска (бизнес-процессам);
- по подразделениям компании;
- по классификационным группам событий операционного риска;
- по классификационным группам источников возникновения событий операционного риска.

Ясно, что описанные выше процедуры процесса управления операционным риском требуют обработки и анализа значительных объёмов информации, поэтому принципиально важным видится создание единого автоматизированного *хранилища информации по операционному риску* (рис. 13).

Для создания полноценной информационно-аналитической среды системы управления операционным риском полезно анализировать не только внутреннюю информацию, но и информацию о случаях реализации событий операционного риска в аналогичных компаниях. Разумно полагать, что уровень отсекаемых внешних данных должен быть достаточно высок, в том смысле, что во внимание необходимо принимать только те события, которые сопровождались существенными последствиями, например, остановки информационных систем; крупные аварии и повреждения сети, станционного оборудования; получение работниками травм на рабочем месте и т.д.

Стоит заметить, что крупные российские телекоммуникационные компании имеют филиальную структуру (МРК ОАО «Связьинвест», ОАО «Ростелеком», ОАО «МТТ» и др.), что даёт им широкие возможности для получения качественной высоко детализированной информации о случаях понесения значительных операционных потерь в других филиалах Общества.

В базу данных, содержащую внешнюю информацию, помимо реквизитов данных, составляющую внутреннюю базу, должны быть дополнительно включены:

- источники получения информации;
- основные характеристики компании, в которой произошло рассматриваемое событие операционного риска;
- коэффициенты сопоставления и т.д.

¹³ Первые два комплекса работ на данном этапе аналогичны комплексу работ на этапе «Анализ операционного риска». Различие состоит в том, что на этапе «Анализ операционного риска» входная информация поступает от владельцев бизнес-процессов с установленной периодичностью, определяемой периодом мониторинга процедур выполнения бизнес-процессов, или каждый раз при внедрении нового бизнес-процесса, т.е. эта информация фиксирует потенциальные уязвимости к операционному риску. Тогда как на этапе «Оценка операционного риска», информация поступает в оперативном режиме и фиксирует случаи реализации событий операционного риска.

Работа с рисками

Данный этап в рамках базы внутренних данных подразумевает разработку мероприятий по снижению вероятности реализации источников возникновения событий операционного риска и оценку целесообразности их осуществления. Процедуры реализации данных работ описаны в разделе 3, здесь остаётся добавить только то, что они должны осуществляться на регулярной основе с учётом:

- выявления новых источников возникновения событий операционного риска;
- актуализации мероприятий по снижению вероятности реализации источников возникновения событий операционного риска;
- изменения стоимостных характеристик мероприятий и т.д.

Формирование базы внешних данных важно, главным образом, с точки зрения выявления источников возникновения крупных операционных потерь в телекоммуникационных компаниях, что позволит выработать систему превентивных мер по их локализации, а в случае, если эти источники полностью устранить невозможно, организовать постоянный мониторинг их состояния; а также разработать систему оперативных действий в случае реализации подобных операционных событий в данной компании. Это подразумевает разработку т.н. *плана обеспечения непрерывности деятельности* (business recovery plan) [5], который должен, как минимум, описывать:

- состав операционных событий, для борьбы с последствиями которых разработан план;
- ключевые ценности (активы, бизнес-процессы, персонал), которые должны находиться под постоянным контролем;
- превентивные меры, направленные на снижение вероятности реализации источников возникновения данных операционных событий;
- симптомы, указывающие на повышение вероятности возникновения данных операционных событий;
- оперативные действия (в т.ч. их порядок, распределение ответственности, состав ресурсов) в случае реализации данных операционных событий.

Коммуникации и консультирование, мониторинг и актуализация

Данные процедуры отражают факт того, что процесс оперативного управления операционным риском требует совместной работы риск-менеджеров, владельцев бизнес-процессов и владельцев ресурсов, которая должна носить непрерывный системный характер.

Таким образом, исходя из предлагаемой системы организации процесса управления операционным риском, функциями владельцев бизнес-процессов и владельцев ресурсов являются:

- осуществление мониторинга существующих бизнес-процессов в соответствии с установленным периодом на предмет выявления новых потенциальных (или корректировки уже установленных) событий операционного риска, источников их возникновения, последствий их реализации и оценки их количественных характеристик;
- выявление потенциальных событий операционного риска, источников их возникновения и последствий реализации на вновь вводимых бизнес-процессах и оценка их количественных характеристик;
- участие в разработке мероприятий по снижению вероятности реализации источников возникновения событий операционного риска и корректировка их (источников) вероятностных распределений;
- регистрация случаев реализации событий операционного риска;
- предоставление в отдел по управлению рисками отчётов по всем перечисленным выше видам работ.

В свою очередь, в функции риск-менеджеров входят:

- координирование, консультирование и методическое обеспечение (разработка методик выявления и оценки компонент операционного риска, классификационной модели операционного риска, форм отчётности и др.) всех работ, выполняемых владельцами бизнес-процессов и владельцами ресурсов в рамках процесса управления операционным риском;
- сбор, консолидация, хранение внутренней информации (от владельцев бизнес-процессов, владельцев ресурсов, др. специалистов) и её анализ, а именно:
 - совершенствование классификационной модели операционного риска (рис. 6);
 - разработка и актуализация причинно-следственных схем событий операционного риска;
 - участие в разработке мероприятий по снижению вероятности реализации источников возникновения событий операционного риска;
 - моделирование причинно-следственных схем событий операционного риска в виде ДВ (рис. 7);
 - оценка целесообразности применения разработанных мероприятий (рис. 10);
 - формирование аналитической отчётности по различным направлениям;
- сбор, консолидация, хранение внешней информации (об аналогичных телекоммуникационных компаниях), её анализ и разработка на его основании плана обеспечения непрерывности деятельности.

В заключение следует добавить, что в настоящее время на рынке программного обеспечения уже представлены продукты, позволяющие автоматизировать некоторые процедуры управления операционным риском, например, зарубежные системы OpVar (разработчик – PricewaterhouseCoopers), RiskOps (разработчик – NetRisk) [1]; отечественная система «Контур Корпорация. Операционные риски» (разработчик – «Зирван. Информационные технологии и консалтинг») [8]. Однако данные программно-методические решения предназначены для управления операционным риском в банках и финансово-промышленных группах, поэтому нуждаются в определённой адаптации под особенности телекоммуникационных компаний (это задача следующего этапа исследований и в настоящей работе мы не претендуем на её решение).

Среди программных продуктов, позволяющих осуществлять моделирование проблемных областей с использованием бейесовых технологий, наиболее известны: Bayesware discoverer, Hugin, Netica [14, 24]. Они являются универсальными и потому могут применяться в компаниях любой отрасли (в сфере их применения), в том числе и в отрасли инфокоммуникационных услуг. Отработка конкретных практических навыков и тем более получения значимых результатов требует консолидированных усилий разработчиков научно-методических вопросов и заинтересованно действующего инфокоммуникационного бизнеса.

Литература

1. Балашова Н. Управление операционным риском: анализ современных тенденций // Рынок ценных бумаг. 2001. №7. С.68-70.
2. Бунцев И.А., Канев В.С. Системное управление рисками в телекоммуникациях (состояние проблемы, методы, модели, реализации)//Вестник СибГУТИ. 2009. № 1. С.26-51.
3. Бухтин М.А. Риск-менеджмент в кредитной организации: методология, практика, регламентирование. Книга 1. Методика и практика работы подразделений риск-менеджмента. Методическое пособие. М.: Издательский дом «Реквизит», 2008. 448с.
4. Вентцель Е. С. Теория вероятностей. М.: Наука, 1969. 576с.
5. Вяткин В.Н., Гамза В.А. Управление рисками фирмы: программа интегративного риск-менеджмента. М.: Финансы и статистика, 2006. 400с.

6. Зинкевич В., Черкашенко В. Карта рисков – эффективный инструмент управления. [Электронный ресурс]. URL: <http://www.franklin-grant.ru/ru/reviews/review7.shtml> (дата обращения: 12.01.2010).
7. Канев В.С. Методологические и методические вопросы построения системы моделей регионального инфокоммуникационного комплекса // Вестник СибГУТИ. 2009. № 1. С.3-25.
8. Контур Корпорация. Операционные риски. [Электронный ресурс]. URL: http://www.csbi-zirvan.ru/catalog/element.php?ELEMENT_ID=1128&ID=206 (дата обращения: 12.01.2010).
9. Круглый стол: Учимся управлять рисками // Связьинвест. 2005. №6. С.12.
10. Кто не рискует, тот... не умеет управлять рисками // Связьинвест. 2005. №5. С.13.
11. Никифоров А.В. Управление рисками – важный элемент эффективной системы управления телекоммуникационных компаний // Мобильные системы. 2006. №10. С.42-45.
12. Мировые тенденции развития риск-менеджмента. Создание комплексной системы управления рисками. [Электронный ресурс]. URL: <http://www.isgr.ru/ru/about/press/news/index.php?id4=70> (дата обращения: 12.01.2010).
13. Модели бизнес-процессов телекоммуникационной отрасли. [Электронный ресурс]. URL: <http://www.finexpert.ru/content.asp?ID=758&mID=65&mode=w> (дата обращения: 12.01.2010).
14. Терехов С.А. Введение в Бейесовы сети // Научная сессия МИФИ-2003. V Всероссийская научно-техническая конференция «Нейроинформатика-2003»: Лекции по нейроинформатике. Часть 1. М.: МИФИ, 2003. С.149-187.
15. Чаадаев В.К. Бизнес-процессы в компаниях связи. М.: Эко-Трендз, 2004. 176с.
16. Шевцова Ю.В. Методические подходы и практические приёмы операционного риск-менеджмента в компаниях телекоммуникационного сектора // Вестник СибГУТИ. 2009. №1. С.52-67.
17. Энциклопедия финансового риск-менеджмента / под ред. А.А. Лобанова, А.В. Чугунова. -2-е изд., перераб. и доп. М.: Альпина Бизнес Букс, 2005. 878с.
18. Heckerman D. A tutorial on learning with Bayesian Networks. – Microsoft Tech. Report – MSR-TR-95-06, 1995.
19. International Convergence of Capital Measurement and Capital Standards / A Revised Framework. Basel Committee on Banking Supervision. Basel, 2004.
20. Jensen F. V. Bayesian Networks and Decision Graphs, Springer. 2001.
21. Jensen F. V., Lauritzen S. L. & Olesen K. G. Bayesian updating in causal probabilistic networks by local computations. Computational Statistics Quarterly, 4. 1990. P. 269-282.
22. Lauritzen S. L. & Spiegelhalter D. J. Local computations with probabilities on graphical structures and their application to expert systems. Journal of the Royal Statistical Society, Series B (Methodological). 1988. P. 157-224.
23. Matheson J. Using Influence diagrams to value information and control. Influence Diagrams, Belief Networks and Decision Analysis. 1990.
24. Olesen K. G., Lauritzen S. L. & Jensen F. V. Hugin: a system creating adaptive causal probabilistic networks. Proceedings of the Eighth Conference on Uncertainty in Artificial Intelligence, Stanford, California. 1992.
25. Pearl J. Causality: Models, Reasoning, and Inference. Cambridge University Press, UK. 2000.
26. Pearl J. Probabilistic Reasoning in Intelligent Systems. Morgan Kaufmann, San Mateo, California. 1988.
27. Horvitz E. J., Breese J. S., Heckerman D., and Hovel D. 1998, The Lumiere project: Bayesian user modeling for inferring the goals and needs of software users. In Uncertainty in Artificial Intelligence: Proceedings of the Fourteenth Conference, p. 256-265, Madison, Wisconsin. Morgan Kaufmann.

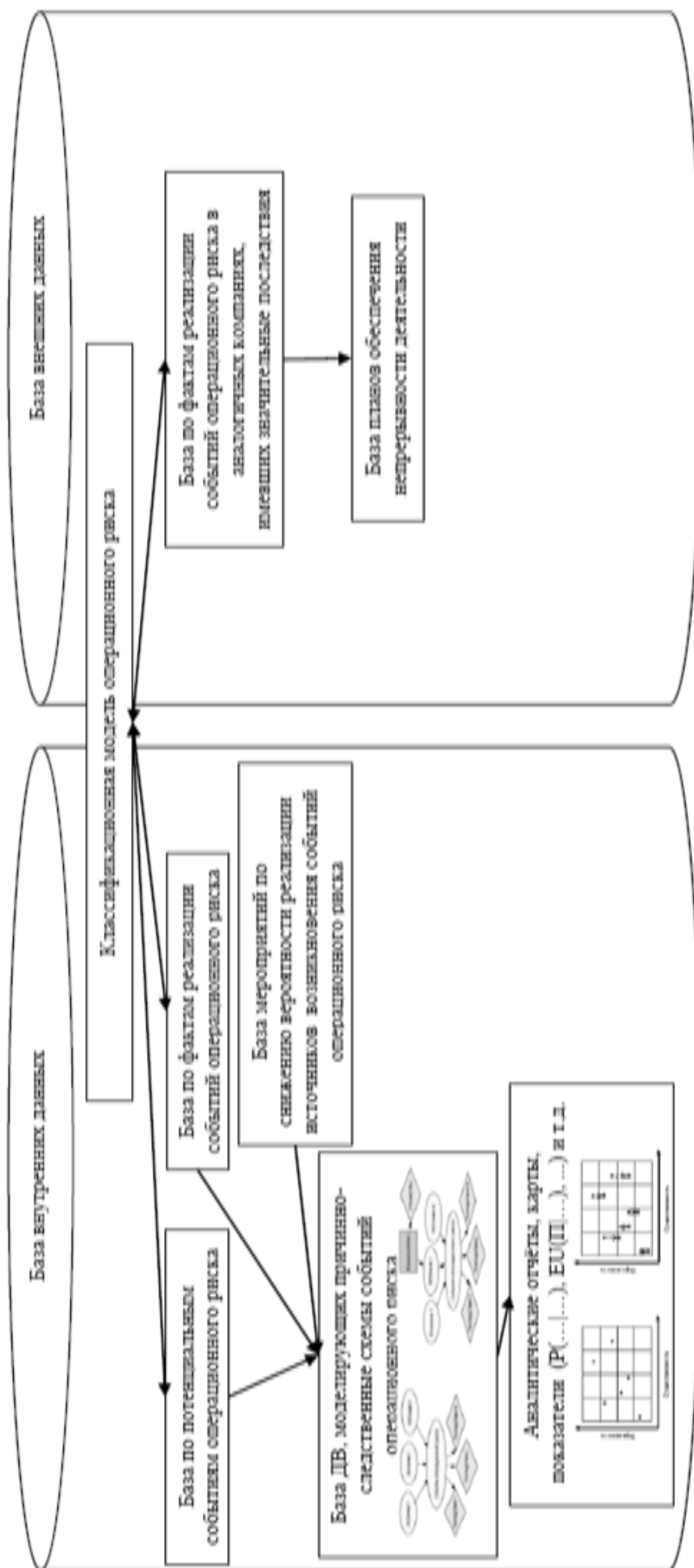


Рис. 13. Структура хранения информации по операционному риску

Канев Валерий Семёнович

д.т.н., к.ф.-м.н., профессор, завкафедрой математического моделирования бизнес-процессов СибГУТИ

тел: (383)269-82-77, e-mail: kanev@ngs.ru

Шевцова Юлия Владимировна

аспирант, ассистент кафедры математического моделирования бизнес-процессов СибГУТИ

тел: (383)269-82-78, 8 923 249 15 97, e-mail: shevcova_yuliya@mail.ru

Methodological aspects and system of tools for modeling of operational risk in telecommunication companies

V. Kanev, Yu. Shevtsova

Approaches to organization of operational risk-management system in telecommunication companies by using Bayes technologies are offered.

Keywords: operational risk, Bayes networks, influence diagrams, risks-map.