УДК 004.89 + 65.011

В.Ф. Мусина

БАЙЕСОВСКИЕ СЕТИ ДОВЕРИЯ КАК ВЕРОЯТНОСТНАЯ ГРАФИЧЕСКАЯ МОДЕЛЬ ДЛЯ ОЦЕНКИ ЭКОНОМИЧЕСКИХ РИСКОВ

Мусина В.Ф. **Байесовские сети доверия как вероятностная графическая модель для оценки экономических рисков.**

Аннотация. Реализация экономических рисков приводит к возникновению нежелательных событий, которые характеризуются возможностью нанесения экономического ущерба предприятию. Стоит задача оценки различных типов экономических рисков, ассоциированных с деятельностью предприятия, и построения систем поддержки принятия решения как на уровне предприятия в целом, так и в различных областях функционирования предприятия. В статье представлено современное состояние применения аппарата байесовских сетей доверия для оценки экономического риска и поддержки принятия решений в условиях неопределенности в контексте риск-менеджмента предприятия. Выделены дисциплины управления операционными рисками и рисками проектов.

Ключевые слова: байесовские сети доверия, экономические риски, управление рисками предприятия, операционные риски, риски управления проектами.

Musina V.F. **Bayesian belief networks as probabilistic graphical model for economical risk assessment.**

Abstract. Realization of economical risks leads to occurrence of adverse effects which result in economic losses in the enterprise. The problem of different types of economical risks associated with the enterprise activities assessment and decision making systems' construction on enterprise level as well as on different levels of enterprise performance comes up. In the paper I provide a state-of-art analysis of Bayesian belief networks use for economical risk assessment and decision making under uncertainty support in the framework of enterprise risk management. The areas of operational risk management and project risk management are singled out.

Keywords: Bayesian belief networks, economical risks, enterprise risk management, operational risks, project risk management.

1. Введение. Риск-менеджмент экономической сфере осуществляется в условиях неопределённости, при которых возможно наступление нежелательных событий, сопряженных с нанесением экономического, морального или другого типа ущерба. Такие события характеризуются риском их реализации. Под экономическими рисками понимаются события, сопряженные с возможностью случайного возникновения нежелательных убытков, измеряемых в денежном эквиваленте [10].

Экономические риски в данной работе рассматриваются в контексте дисциплины управления рисками предприятия. Менеджеры каждого предприятия должны ежедневно принимать решения в рамках процессов функционирования предприятия, такие решения должны соот-

ветствовать цели повышения долгосрочной и краткосрочной ценности предприятия для заинтересованных лиц [23]. При этом менеджеры сталкиваются с изменением конъюнктуры на рынках, действиями конкурентов, сменой предпочтений потребителей, экологическими ограничениями, особенностями законодательства и другими факторами [10, 64]. Оценка рисков является одним из этапов риск-менеджмента предприятия и тесно связана с этапами идентификации и управления риском.

Риски предприятия могут иметь различную природу. Некоторые типы рисков, как например риск негативного влияния человеческого и организационного факторов на деятельность предприятия, невозможно оценить лишь количественными методами [87]. Описание таких типов риска состоит как из качественной информации, описывающей сценарии и ситуации, так из количественной информации, имеющей отношение к характеристикам работы системы [87]. Таким образом, управление рисками предприятия требует системного подхода.

Аппарат байесовских сетей доверия предоставляет возможность объединения экспертной и статистической информации. Байесовские сети доверия, расширенные до диаграмм влияний, могут использоваться в процессе управления рисками предприятия, в том числе при моделировании сценариев развития ситуации. Семантика байесовских сетей доверия позволяет включать в модель зависимости между переменными модели [28]. Кроме того, байесовские сети доверия позволяют интегрировать в модель данные, получаемые на каждом этапе развития проекта, тем самым обеспечивая обратную связь (feedback loop), которая является важной составляющей процедуры управления рисками [41].

Цель данной статьи заключается в анализе современного состояния применения аппарата байесовских сетей доверия для оценки экономического риска и поддержки принятия решений в условиях неопределенности в контексте риск-менеджмента предприятия. Отдельно рассмотрены дисциплины управления операционными рисками и рисками проектов, которые являются составными частями общего риск-менеджмента предприятия.

2. Байесовские сети доверия. Вероятностные графические модели [9, 52] используются для моделирования связей между случайными элементами в некоторой системе в тех случаях, когда в силу сложности системы или неполноты и неточности имеющейся информации о составных её частях невозможно полностью описать совместное вероятностное распределение случайных элементов в системе. Узлы веро-

ятностной графической модели ассоциированы с некоторыми случайными элементами, а графическая структура отвечает предполагаемой или установленной структуре зависимостей случайных элементов.

Графическая структура байесовской сети доверия [7, 8, 48, 52, 71] представляет собой направленный ациклический граф с n вершинами, узлами байесовской сети доверия являются случайные элементы $X_1, X_2 \dots X_n$. Каждый случайный элемент описывается функцией распределения вероятности, а каждый узел сети — тензором условных вероятностей. Например, такие случайные элементы могут отвечать различным типам рисков, которые оказывают влияние на систему. Часто риски не являются независимыми друг от друга, в частности, человеческий фактор может оказывать влияние на вероятность реализации некоторого множества рисков. Для оценки общего риска, которому подвержена система, необходимо учитывать все риски и их взаимосвязи.

Важной особенностью байесовских сетей доверия как вероятностных графических моделей является правило декомпозиции, которое в случае байесовской сети доверия обусловлено свойством d-разделимости [7, 52]. Формально правило декомпозиции выглядит следующим образом:

$$f_0\left(x_1, x_2 \dots x_n\right) = \prod_{i=1}^{n} f_i\left(x_i | \mathrm{pa}\left(X_i\right)\right),$$

где $f_0\left(x_1, x_2 \dots x_n\right)$ — совместное распределение вероятности всех случайных элементов, $f_i\left(x_i | \mathrm{pa}\left(X_i\right)\right)$ — распределение вероятности случайного элемента X_i при условии означивания случайных элементов — родителей узла, соответствующего случайному элементу X_i.

Байесовская сеть доверия может быть построена как на основе экспертных оценок, так и на основе статистических данных. Экспертная информация может использоваться как для установления взаимосвязей между случайными элементами, так и для получения оценок условных вероятностей [82]. Правило декомпозиции позволяет использовать алгоритмы вероятностного вывода [8, 48, 52].

3. Управление рисками предприятия (enterprise risk management). Управление рисками предприятия — это дисциплина, которая включает в себя процессы идентификации, контроля, использования, финансирования и мониторинга рисков любой природы с целью повышения долгосрочной и краткосрочной ценности организации для

заинтересованных лиц [23, 78]. Подразумевается, что управление рисками предприятия представляет собой базу для поддержки принятия стратегически важных решений, которая оказывает влияние на все этапы процесса принятия решений [23]. Дисциплина управления рисками предприятия выделяет следующие типы рисков:

- риски опасных ситуаций, источниками которых являются природные и техногенные катастрофы, нетрудоспособность работников, в том числе связанная с их трудовой деятельностью, преступления в отношении предприятия и его сотрудников, юридические претензии по деятельности предприятия;
- финансовые риски, определяемые с учетом специфики деятельности каждого предприятия и связанные с его финансовой деятельностью. Источниками финансовых рисков могут являться изменения цены (в том числе ставки процента, курса обмена валют и т.д.), изменение ликвидности, кредиты, влияние инфляции и базисные риски;
- операционные риски, связанные с внутренней деятельностью предприятия и включающие риски управления человеческими ресурсами (в т.ч. распределением полномочий), развитием и внедрением продукции, цепями поставок, риски информационных технологий предприятия, риски информационной и деловой отчетности (в т.ч. составление бюджета, планирование, бухгалтерский учет, налогообложение, оценка инвестиционных вложений, пенсионные фонды);
- стратегические риски, включающие репутационные риски, риски конкуренции, ожиданий покупателей, инновативных внедрений, демографические, социо-культурные политические риски.

Различные предприятия могут определять структуру рисков иначе, исходя из конкретного положения на рынке и специфики деятельности, однако необходимо отметить, что дисциплина управления рисками предприятия охватывает все возможные ситуации, реализация которых может тем или иным образом принести ущерб целям (в том числе экономическим) предприятия. Таким образом, меры риска предприятия в целом связаны с мерами эффективности работы.

В основе оценки рисков предприятия лежит построение вероятностного распределения потерь для каждого типа рисков, которое описывает влияние на экономическое состояние предприятия всего возможного спектра реализаций класса рисковых ситуаций, включая маловероятные события [64]. Все риски предприятия рассматриваются

как портфель, формируют *профиль рисков* предприятия, который описывается кумулятивным вероятностным распределением портфеля рисков. Меры риска могут быть направлены как на описание степени платежеспособности предприятия (анализ «хвостов» кумулятивного вероятностного распределения портфеля рисков), так и на описание стабильности функционирования предприятия (анализ средних значений кумулятивного вероятностного распределения портфеля рисков) [64]. Для построения вероятностного распределения потерь каждого типа рисков могут использоваться статистические данные, однако такие данные часто неполны и неточны. Таким образом, важным вкладом в процесс оценки рисков предприятия является экспертная информация, которая может быть использована самостоятельно или же в дополнение к статистическим данным. Таким образом, выделяют [16, 78] два подхода к анализу рисков: статистический, опирающийся лишь на имеющиеся данные, и системный, в рамках которого используется экспертная информация для дополнения имеющихся неполных данных или разбиения предметной области с целью извлечения большего объема данных.

Кроме того, в организациях с повышенной ответственностью (high reliability organizations) [88] реализации связанных с риском ситуаций редки и носят катастрофический характер. Примерами выступают организации, связанные с авиастроением, заводы по обработке ядерных отходов, атомные электростанции. В некоторых случаях учреждения здравоохранения так же относят к организациям с повышенной ответственностью [13, 17, 22]. Менеджмент таких организаций направлен на обеспечение безопасности деятельности (safety), то есть на предупреждение возникновения рисковых ситуаций, а не на борьбу с последствиями реализаций рисков. В организациях с повышенной ответственностью используется системный подход к анализу риска [16].

Методы в рамках системного подхода включают в себя методы количественной оценки риска (quantitative risk assessment) и вероятностной оценки риска (probabilistic risk assessment) [14]. Количественная оценка риска может основываться на различных подходах к представлению неопределенности (аппарат нечеткой логики, теория возможностей). Обзор различных подходов к представлению и обработке неопределенности представлен в работе [5]. Выделяют три этапа количественной оценки риска: определение возможных угроз и опасностей, анализ причин и следствий, описание риска. В работе [16] представлено описание методов в рамках системного подхода к анализу риска,

описаны этапы и основные черты количественной оценки риска. Отмечено, что байесовские сети доверия могут применяться на этапе анализа причин и следствий риска.

Вероятностные графические модели используются для описания независимостей между известными событиями, сценариями развития и интересующими риск-менеджера событиями [87]. Байесовские сети доверия позволяют интегрировать статистические данные и экспертные оценки [20, 87]. Эти свойства байесовских сетей доверия обуславливают их применение для моделирования надежности сложных систем [51, 55, 60], подробный обзор источников представлен в [87].

Человеческий и организационный факторы [16, 85, 87] имеют значительное влияние в тех случаях, когда деятельность предприятия связана с взаимодействием персонала предприятия на различных уровнях его функционирования. Анализ влияния человеческого и организационного фактора на деятельность предприятия складывается, с одной стороны, из качественной информации, описывающей сценарии и ситуации, с другой стороны, из количественной информации, имеющей отношение к характеристикам работы системы [87]. В частности, в работах [56, 58] использован аппарат байесовских сетей доверия для оценки эффективности работы персонала и организационного здоровья предприятия.

К примеру, для координации перевозок морем требуется координированная работа персонала; отмечается, что 70-80% несчастных случаев на воде происходят по вине человека [76, 85]. В подобных случаях байесовские сети доверия могут выступать как графические модели, описывающие как вклад всех участников процесса морской перевозки в общий риск несчастного случая, так и надежность технических систем, использующихся в процессе перевозки. Величина влияния факторов риска в этом случае описывается при помощи условных вероятностей, ассоциированных с каждым узлом сети. Для корректного описания экспертных оценок тензоров условных вероятностей используются нечеткие байесовские сети доверия, опирающиеся на аппарат нечеткой вероятностной меры [30, 34, 58, 76, 79]. Описание аппарата нечетких байесовских сетей с применением его к анализу риска негативного влияния человеческого фактора в области морского судоходства предложено в работах [34, 35].

Риск может восприниматься как бинарная случайная величина и иметь два уровня: риск реализован или не реализован. В работе [20] описан процесс построения байесовской сети доверия на основании данных, содержащих лишь маргинальные вероятности реализации

риска и корреляции между различными типами рисков. В основе предложенного метода лежит решение систем уравнений, которые позволяют вычислить условные вероятности по имеющимся данным.

Риск-менеджмент предприятия предполагает моделирование значительного числа рисков. Хотя процесс построения байесовской сети доверия в этой ситуации достаточно понятен, он часто является трудоемким [45]. В этом случае возможно использование объектно-ориентированных байесовских сетей доверия [53], которые предполагают создание особых подсетей — *классов*, экземпляры класса являются *рисковыми объектами*. В работах [45, 89] описаны примеры применения объектно-ориентированных байесовских сетей доверия в оценке рисков. Работа [89] посвящена разработке модели, сочетающей в себе анализ основополагающей причины (root cause analysis) и поддержку принятия решений при оперировании сложным производственным процессом. Такая модель позволяет интегрировать информацию, получаемую от технического обеспечения производственного процесса (сенсоры, датчики), и экспертные знания оператора процесса. Разработанная модель используется как для определения рисков, связанных с производственным процессом, и принятия решений в процессе производства, так и для оптимизации взаимодействия значительного числа программных комплексов, управляющих производственным процессом.

Важной составной частью риск-менеджмента предприятия является анализ рисков, связанных с его информационной безопасностью [2, 3, 4, 6]. В работах [32, 33] предложен основанный на байесовской сети доверия метод оценки риска, которому подвергается критический ресурс при проведении атаки. Возможные пути развития атаки представлены графом атак, причем каждый профиль нарушителя связан с набором особенностей поведения атакующего. Случайная величина, ассоциированная с каждым узлом сети, определяет, произошло ли событие. В работе [81] описана вероятностная реляционная модель для оценки риска информационной системы.

Байесовские сети доверия могут применяться для анализа конкретных типов экономических рисков. Например, при моделировании доходности портфеля, составленного из некоторых активов, байесовские сети доверия позволяют учитывать корреляций между доходностями активов. Кроме того, байесовские сети доверия позволяют интегрировать исторические данные о доходностях с экспертными мнениями [80].

Моделирование рисков неблагоприятных природных явлений так же включено в дисциплину управления рисками предприятия. Необходимость количественной оценки этого типа риска возникла после серии природных катастроф, оказавших значительное влияние на (экономическую) деятельность компании [23]. Байесовские сети доверия используются в экологическом моделировании [21, 61, 86], моделировании рисков природных угроз [19, 59, 84].

Операционные риски будут рассмотрены подробнее в следующей части статьи.

4. Операционные риски. Термин операционные риски (operational risk) появился в связи с разорением в 1995 году банка Barings, старейшего торгового банка Лондона, вызванным несанкционированными действиями одного из своих сотрудников [74]. Операционные риски имеют особое значение в финансовой и страховой деятельности, и часто тесно связаны с воздействием человеческого фактора.

Общепринятым является определение операционного риска, данное Базельским комитетом по банковскому надзору. Документ Базель II определяет операционный риск [1] как риск убытка в результате неадекватных или ошибочных внутренних процессов, действий сотрудников и систем или внешних событий. Категории типов событий операционного риска, согласно документу, выпущенному Базельским комитетом по банковскому надзору, включают [1]: внутреннее мошенничество (internal fraud); внешнее мошенничество (external fraud); события, связанные с нарушением трудового законодательства и безопасности труда (employment practices and workplace safety); события, связанные с клиентами, продуктами и правилами ведения бизнеса (clients, products, & business practice); ущерб материальным активам (damage to physical assets); прерывание бизнеса и сбои систем (business disruption & systems failures); управление исполнением, доставкой и процессами (execution, delivery, & process management). Однако, как уже отмечалось, каждое предприятие в рамках риск-менеджмента определяет риски, которым подвержена его деятельность, исходя из специфики своей деятельности и положения на рынке. В страховании операционный риск определяется директивой Solvency II [40] и во многом совпадает с определением, данным Базельским комитетом по банковскому надзору [29]. Работа [38] посвящена описанию проблем как математической, так и организационной природы, возникающих при внедрении требований Базельского комитета по банковскому надзору.

Таким образом, под операционными рисками понимаются риски, которые достаточно сложно определить и количественно оценить [23,

54, 78]. В отличие от других типов рисков, операционные риски не несут в себе возможность получения прибыли предприятием [73]. Отмечается, что с математической точки зрения моделирование операционных рисков имеет много общего с актуарными техниками, использующимися в не связанном с жизнью страховании [39, 62, 73].

Одними из стадий риск-менеджмента предприятия являются идентификация (качественное определение) и оценка (количественное определение) риска. Базельским комитетом по банковскому надзору [18] установлены следующие подходы к оценке операционных рисков: подход базового индикатора (BIA, Basic Indicator Approach), стандартизированный подход (TSA, The Standardized Approach) и альтернативный стандартизированный подход (ASA), продвинутые подходы (AMA, Advanced Measurement Approach) [28, 38]. Последний подход [24] предполагает использование статистических данных (как внутренних, так и внешних) и экспертных оценок (моделировании сценариев, определение среды функционирования предприятия). В рамках подхода AMA выделяют три подхода [28] к анализу имеющейся у предприятия информации: актуарный, причинно-следственный и байесовский.

В рамках *актуарного подхода* используются статистические данные для определения частоты реализации риска, которая описывается в терминах вероятности его реализации, и последствий реализации риска, которые в свою очередь связаны с экономическими потерями предприятия [48]. На основании этих данных строится распределение вероятности потерь (loss distribution), которое является объектом дальнейшего исследования, и характеристики которого используются для принятия решений в условиях неопределенности [31, 46]. Пусть компания рассматривает L типов операционных рисков и пусть для каждого типа рисков за определенный промежуток времени n_i событий реализовалось, каждая реализация риска повлекла за собой потери в размере $X_j^i, j = 1..n_i$. Количество событий n_i является реализацией случайной величины, которая определяется частотой реализации риска, каждый объем потерь X_j^i является реализацией случайной величины, описывающей последствия реализации рассматриваемого риска. Тогда операционные потери для каждого типа риска составляют $S_i = \sum_{j=1}^{n_i} X_j^i$. Актуарный подход к анализу распределения потерь накладывает ряд ограничений о независимости: случайные величины, опре-

деляющие частоту реализации риска и потери при реализации, должны быть независимы, все потери являются независимыми и одинаково распределенными случайными величинами [28]. Для моделирования вероятностных распределений редких событий используется аппарат теории экстремальных значений [24]. В работе [66] на основании эмпирических данных проанализированы основные гипотезы о частоте и серьёзности операционных потерь предприятий, учитывая разделение по линиям бизнеса и типам предприятий. В рамках актуарного подхода возможно моделирование зависимости между входящими в модель случайными величинами, для этих целей было предложено [24, 37] использовать аппарат копул [68]. Если известна структура независимостей конкретных операционных рисков предприятия, то возможно использование аппарата копульных байесовских сетей (copula Bayesian network) [36] для получения общего распределения операционных потерь.

Однако часто использование исключительно актуарного подхода к анализу операционных рисков предприятия невозможно, так как имеющиеся статистические данные об операционных потерях являются неполными или неточными [11, 69, 78]. Кроме того, статистические данные зависят от моделей, которые применяются при определении и оценке риска в каждой отдельной организационной единице предприятия; некоторые параметры таких моделей выбираются субъективно [11].

Методы в рамках *причинно-следственного подхода* направлены на установление причинно-следственных связей между операционными потерями и некоторыми событиями, связанными с внутренними процессами предприятия. Характеристики таких событий носят название ключевых показателей риска (key risk indicator). Эти методы достаточно трудны для реализации и не направлены на анализ событий с низкой частотой реализации [28]. Однако ключевые показатели риска могут использоваться в качестве узлов байесовской сети доверия [12] для моделирования риска предприятия, и являться основой для сценарного анализа. В работе [70] представлена модель на основе байесовских сетей доверия, позволяющая идентифицировать показатели организационного риска предприятия.

Байесовский подход предполагает использование байесовских сетей доверия как вероятностно-графической модели оценки операционного риска. Важным свойством байесовских сетей доверия является возможность интегрировать экспертные мнения и статистическую информацию различной природы, что позволяет описывать риски, кото-

рые невозможно описать статистическими методами (риск неблагоприятного воздействия человеческого фактора), и связывать в одной модели операционные риски и рыночные и кредитные риски. Байесовские сети доверия, расширенные до диаграмм влияний, могут использоваться в процессе управления рисками предприятия, в том числе при моделировании сценариев развития ситуации. Кроме того, семантика байесовских сетей доверия позволяет включать в модель зависимости между переменными модели [28]. В работах [11, 12, 29] описаны возможности применения байесовских сетей доверия для моделирования операционных рисков предприятий.

Как уже упоминалось, при моделировании операционных рисков предприятия необходимо учитывать возможные зависимости, как между различными уровнями риска, так и между рисками в различных сферах деятельности предприятия [15, 38]. К примеру, природные катастрофы часто влияют на многие сферы деятельности компании и могут привести к реализации сразу нескольких рисков. Байесовские сети доверия позволяют корректно конструировать распределение операционных потерь в тех случаях, когда реализации рисков зависимы во времени [15] или в случаях, когда частота реализации риска и последствия реализации зависимы [69]. В последнем случае в модель вводится третий тип переменных — переменная, связанная с эффективностью процесса потерь. Тензор условных вероятностей узлов байесовской сети доверия, ассоциированных с этой переменной, оценивается экспертными методами.

5. Управление рисками проектов. Управление рисками проектов направлено на определение, оценку и контроль рисков, которые оказывают влияние на успех проекта [57]. Процесс реализации проекта связан с неопределенностью будущего состояния экономики и развития внутренних процессов предприятия [49, 50, 63]. Кроме того на различных этапах процесса определение успешности проекта может изменяться, хотя основными критериями успешности являются перерасход времени, перерасход денежных средств и качество результатов проекта.

Байесовские сети доверия используются в управлении рисками проектов [25, 27, 57] как диаграммы, отражающие причинно-следственные связи между событиями или диаграммы влияний. Кроме того, байесовские сети доверия позволяют интегрировать в модель данные, получаемые на каждом этапе развития проекта, тем самым обеспечивая обратную связь (feedback loop), которая является важной составляющей процедуры управления рисками [41]. Байесовские сети

доверия могут использоваться для планирования расписания проекта в условиях неопределенности [50].

Типы рисков определяются экспертами в конкретной предметной области; каждый риск численно выражается вероятностью реализации риска и тяжестью потерь, которые он влечет за собой [41, 57]. Как отмечается в [25], основной проблемой применения аппарата байесовских сетей доверия является численная оценка вероятностей ассоциированных с узлами сети. Например, в проектах, посвященных разработке и запуску нового продукта, возникают риски [47], которые специфичны для конкретной ситуации, и потому вероятности реализации рисковых событий не могут быть оценены по статистическим данным [41]. Согласно [25] риски, связанные с внедрением нового продукта, включают в себя риски исследований и разработок, риски производства, риски поставок, риски надежности продукта. Непосредственная оценка таких вероятностей экспертами связана с субъективностью и отклонениями, что в свою очередь влечет сомнения в состоятельности моделей, использующих в своей основе только экспертные знания [57, 65, 83]. В работах [25, 65] описаны и предложены методы, уточняющие экспертные знания для моделей, основанных на байесовских сетях доверия.

Процесс внедрения новых продуктов является основополагающим процессом при разработке программного обеспечения, что обуславливает распространенность основанных на байесовских сетях доверия моделей при управлении рисками проектов в области разработки программного обеспечения [41, 42, 63, 83]. Важным является установление причинно-следственных связей между событиями в процессе разработки программного обеспечения [45, 77]. Действительно, если при тестировании было обнаружено небольшое количество ошибок, означает ли это, что тесты недостаточно чувствительны или же что разработка выполнена качественно? Байесовские сети доверия применяются для количественной оценки качества разрабатываемых программных продуктов (и измерения программных продуктов в целом) [43]. В работе [43] описаны существующие метрики программных продуктов, выделены их недостатки и предложена метрика, в основе которой лежит байесовская сети доверия. Оценка характеристик программных продуктов является субъективной [67] в силу влияния человеческого фактора; использование байесовского статистического вывода позволяет количественно интерпретировать и интегрировать экспертные мнения, что в свою очередь позволяет корректно измерять характеристики программного обеспечения. В работе [44] предложена модель

для предсказания дефектов в программном обеспечении на основе байесовской сети доверия. В работе [45] для решения этой задачи используется аппарат объектно-ориентированной байесовской сети доверия, который позволяет рассматривать полный жизненный цикл проекта. Так же байесовские сети доверия могут применяться для оценки стоимости программного обеспечения на этапе его разработки [26, 72, 75, 83]. Объектно-ориентированные байесовские сети доверия позволяют описывать весь жизненный цикл проекта, определять возможности

Norman Fenton и Martin Neil разработали программный продукт AgenaRisk [90], предназначенный для количественной оценки рисков. В основе модели лежит построение байесовской сети доверия. Программный продукт использовался во многих проектах [91] и применяется как основа для риск-менеджмента в ряде компаний [45].

8. Заключение. Байесовские сети доверия все чаще используются как основа поддержки принятия решений в риск-менеджменте предприятия. Риски, с которыми сталкивается предприятие в процессе функционирования, могут быть зависимыми или же не допускать возможности количественной оценки последствий их реализации [16]. Байесовские сети доверия представляют собой инструмент, позволяющий включать в модель качественную информацию и естественным образом моделировать зависимости между различными рисками. Кроме того, байесовские сети доверия могут быть адаптированы для решения конкретных задач: для представления большого числа рисков предприятия могут использоваться объектно-ориентированные байесовские сети доверия [45, 53, 89], для описания экспертной информации — нечеткие байесовские сети доверия [30, 34, 58, 76, 79].

Байесовские сети доверия используются для количественного описания влияния человеческого и организационного факторов [16, 85, 87], для описания надежности сложных систем [87], при моделировании рисков информационной безопасности системы предприятия [32, 33], финансовых рисков предприятия [80], рисков опасных природных явлений [19, 21, 59, 61, 84, 86], операционных рисков [11, 15, 28, 29, 38], рисков проектов [25, 27, 57].

Литература

1. Базель II. Перевод ЦБ России. URL: http://www.cbr.ru/today/ms/bn/Basel.pdf (дата обращения: 26.02.2013)
2. *Котенко И. В., Юсупов Р. М.* Перспективные направления исследований в области компьютерной безопасности // Защита информации. INSIDE. 2006. №. 2. С. 46-57.
3. *Котенко И.В., Саенко И.Б., Юсупов Р.М.* Аналитический обзор докладов Международной конференции "Математические модели, методы и архитектуры для защи-

ты компьютерных сетей"(MMM-ACNS-2010) // Труды СПИИРАН. 2010. № 13. С. 199–225.
4. *Котенко И.В., Степашкин М.В., Юсупов Р.М.* Математические модели, методы и архитектуры для защиты компьютерных сетей: аналитический обзор перспективных направлений исследований по результатам международного семинара MMM-ACNS-2005 // Труды СПИИРАН. 2006. № 3. Т. 2. С. 11–29.
5. *Суворова А.В.* Подходы к представлению и обработке неопределенности данных и знаний о поведении индивидов // Труды СПИИРАН. 2012. Вып. 23. С. 206–222.
6. *Тулупьева Т.В., Тулупьев А.Л., Пащенко А.Е., Азаров А.А., Степашкин М.В.* Социально-психологические факторы, влияющие на степень уязвимости пользователей автоматизированных информационных систем с точки зрения социоинженерных атак // Труды СПИИРАН. 2010. № 12. С. 200–214.
7. *Тулупьев А. Л., Николенко С. И., Сироткин А. В.* Байесовские сети: логико-вероятностный подход. СПб.: Наука, 2006. 607 с.
8. *Тулупьев А.Л., Сироткин А.В., Николенко С.И.* Байесовские сети доверия: логико-вероятностный вывод в ациклических направленных графах. СПб.: Изд-во С.-Петерб. ун-та, 2009. 400 с.
9. *Фильченков А.А.* Меры истинности и вероятностные графические модели для представления знаний с неопределенностью // Труды СПИИРАН. 2012. №4. С. 254–295.
10. *Чернова Г.В., Кудрявцев А.А.* Управление рисками: Учебное пособие. М.: ТК Велби, Изд-во Проспект, 2003. 160 с.
11. *Alexander C.* Bayesian Methods for Measuring Operational Risk (February 2000). Discussion Papers in Finance 2000-02. URL: http://ssrn.com/abstract=248148 or http://dx.doi.org/10.2139/ssrn.248148 (дата обращения: 26.02.2013)
12. *Alexander C.* Managing operational risks with Bayesian networks // Operational Risk: Regulation, Analysis and Management. 2003. P. 285–294.
13. *Amalberti R, Auroy Y, Berwick D, Barach P.* Improving patient care: Five system barriers to achieving ultrasafe health care // Annals of Internal Medicine. 2005. 142. P. 756–764.
14. *Apostolakis G.E.* How useful is quantitative risk assessment? // Risk Analysis. 2004. Vol. 24, No3. P. 515–520.
15. *Aquaro V., Bardoscia M., Bellotti R., Consiglio A., De Carlo F., Ferri G.* A Bayesian Networks approach to Operational Risk // Physica A: Statistical Mechanics and its Applications. 2010. Vol. 389, No. 8. P. 1721–1728.
16. *Aven T.* Risk analysis //Safety and Risk Modeling and Its Applications. 2011. P. 125–149.
17. *Bagnara S., Parlangeli O., Tartaglia R.* Are hospitals becoming high reliability organizations? // Applied Ergonomics. 2010. 41(5). P. 713–718.
18. Basel Committee on Banking Supervision. Consulting document: operational risk. URL: http://www.bis.org/publ/bcbsca07.pdf // Bank for International Settlements http://www.bis.org (official WEB-site)
19. Bayraktarli Y. Y., Ulfkjaer J., Yazgan U., Faber M. H. On the application of Bayesian probabilistic networks for earthquake risk management [электронный ресурс] URL: http://www.merci.ethz.ch/Publications/bayota.pdf (доступ 01.03.2013) // In 9th international conference on structural safety and reliability, Italy, Rome.
20. *Bonafede C.E., Giudici P.* Bayesian networks for enterprise risk assessment // Physica A: Statistical Mechanics and its Applications. 2007. Vol. 382, issue 1. P. 22–28. Также доступно URL: http://dx.doi.org/10.1016/j.physa.2007.02.065 (дата обращения: 26.02.2013)
21. Borsuk M. E., Stow C. A., Reckhow K. H. A Bayesian network of eutrophication models for synthesis, prediction, and uncertainty analysis // Ecological Modelling. 2004. Vol. 173, No 2. P. 219–239.
22. *Carayon P., Wood K.E.* Patient Safety: The Role of Human Factors and Systems Engineering // Stud Health Technol Inform. 2010. No 153. P. 23–46.

23. Causal Actuarial Society. Overview of Enterprise Risk Management. URL: http://www.casact.org/area/erm/overview.pdf (дата обращения: 26.02.2013)
24. *Chavez-Demoulin V., Embrechts P., Nešlehová J.* Quantitative models for operational risk: extremes, dependence and aggregation // Journal of Banking & Finance. 2006. T. 30, No 10. P. 2635–2658.
25. *Chin K. S., Tang D.W., Yang J.B., Wong S.Y., Wang H.*. Assessing new product development project risk by Bayesian network with a systematic probability generation methodology // Expert Systems with Applications. 2009. Vol. 36. No. 6. P. 9879–9890.
26. *Chulani S., Boehm B., Steece B.* Bayesian analysis of empirical software engineering cost models //Software Engineering, IEEE Transactions on. 1999. Vol. 25, No 4. P. 573–583.
27. *Cooper L.G.* Strategic marketing planning for radically new products // The Journal of Marketing. 2000. P. 1-16.
28. *Cornalba C., Giudici P.* Statistical models for operational risk management // Physica A: Statistical Mechanics and its applications. 2004. Vol. 338, No. 1. P. 166–172.
29. *Cowell R.G., Verrall R.J., Yoon Y.K.* Modeling operational risk with Bayesian networks // Journal of Risk and Insurance. 2007. Vol. 74, No 4. P. 795–827.
30. *Dubois D., Prade H.* Bayesian conditioning in possibility theory // *Fuzzy Sets and Systems*. 1997. 92(2). P. 223–240.
31. *Dutta K., Perry J.* A Tale of Tails: An Empirical Analysis of Loss Distribution Models for Estimating Operational Risk Capital // FRB of Boston. Working Paper No. 06-13. 2006. URL: http://www.bos.frb.org/economic/wp/wp2006/wp0613.htm (дата обращения: 26.02.2013)
32. *Dantu R., Kolan P.* Risk management using behavior based Bayesian networks // Intelligence and Security Informatics. 2005. P. 165-184.
33. *Dantu R., Loper K., Kolan P.* Risk management using behavior based attack graphs // Information Technology: Coding and Computing, 2004. Proceedings. ITCC 2004. International Conference on. IEEE, 2004. Vol. 1. P. 445-449.
34. *Eleye-Datubo A. G., Wall A., Saajedi A., Wang J.* Enabling a powerful marine and offshore decision-support solution through Bayesian network technique // Risk Analysis. 2006. 26(3). P. 695–721.
35. *Eleye-Datubo A. G., Wall A., Wang J.* Marine and Offshore Safety Assessment by Incorporative Risk Modeling in a Fuzzy-Bayesian Network of an Induced Mass Assignment Paradigm // Risk Analysis. 2008. Vol. 28, No. 1. P. 95-112.
36. *Elidan G.* Copula bayesian networks // Advances in Neural Information Processing Systems. 2010. Vol. 23. P. 559–567
37. *Embrechts P., Höing A., Juri A.* Using copulae to bound the Value-at-Risk for functions of dependent risks // Finance and Stochastics. 2003. Vol. 7, No. 2. P. 145–167.
38. *Embrechts P., Hofert M.* Practices and issues in operational risk modeling under Basel II //Lithuanian mathematical journal. 2011. Vol. 51, No. 2. P. 180–193.
39. *Embrechts P., Puccetti G.* Aggregating operational risk across matrix structured loss data // J. Oper. Risk. 2008. Vol. 3, No. 2. P. 29–44.
40. *European Commission et al.* Directive of the European Parliament and of the Council on the taking up and pursuit of the business of insurance and reinsurance (“solvency II”) // Official Journal of the European Union. 2009. L 335, Vol. 52. Также доступно URL: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:335:FULL:EN:PDF
41. *Fan C.F., Yu Y.C.* BBN-based software project risk management // Journal of Systems and Software. 2004. Vol. 73, No 2. P. 193–203.
42. *Fenton N., Krause P., Neil M.* Software measurement: Uncertainty and causal modeling // Software, IEEE. 2002. Vol. 19, No 4. P. 116–122.
43. *Fenton N.E., Neil M.* Software metrics: successes, failures and new directions // Journal of Systems and Software. 1999. Vol. 47, No 2. P. 149–157.

44. *Fenton N. E., Neil M.* A critique of software defect prediction models // Software Engineering, IEEE Transactions on. 1999. Vol. 25, No 5. P. 675–689.
45. *Fenton N., Neil M., Marsh W., Hearty P., Marquez D., Krause P., Mishra R.* Predicting software defects in varying development lifecycles using Bayesian nets //Information and Software Technology. – 2007. – Т. 49. – №. 1. – С. 32-43.
46. *Frachot A., Moudoulaud O., Roncalli T.* Loss Distribution Approach in Practice // The Basel Handbook: A Guide for Financial Practitioners, edited by Micheal Ong, Risk Books, 2004. Available at SSRN: http://ssrn.com/abstract=1032592 (дата обращения: 26.02.2013).
47. *Gidel T., Gautier R., Duchamp R.* Decision-making framework methodology: an original approach to project risk management in new product design / /Journal of Engineering Design. 2005. Vol. 16, No 1. P. 1-23.
48. *Jensen F.V.* Bayesian Networks and Decision Graphs. New York, USA: Springer, 2001. 268 p.
49. *Kayis B., Arndt G., Zhou M., Savci S., Khoo Y.B., Rispler A.* Risk Quantification for New Product Design and Development in a Concurrent Engineering Environment // CIRP Annals – Manufacturing Technology. 2006. Vol. 55, Iss. 1. P. 147–150.
50. *Khodakarami V., Fenton N., Neil M.* Project Scheduling: Improved approach to incorporate uncertainty using Bayesian Networks // Project Management Journal. 2007. Vol. 38, No 2. P. 39–49.
51. *Kohda T., Cui W.* Risk-based reconfiguration of safety monitoring system using dynamic Bayesian network // Reliability Engineering & System Safety. 2007. Vol. 92, No 12. P. 1716–1723.
52. *Koller D., Friedman N.* Probabilistic Graphical Models. Principles and Techniques. Cambridge, Massachusetts, London: MIT Press, 2009. 1231 p.
53. *Koller D., Pfeffer A.* Object-oriented Bayesian networks // Proceedings of the Thirteenth Conference on Uncertainty in Artificial Intelligence. Morgan Kaufmann Publishers Inc., 1997. P. 302-313.
54. *Lamarque E., Karfoul H.* Understanding the Operational Risk Profile of Banks: An Empirical Analysis (June 6, 2012). 29th International Conference of the French Finance Association (AFFI) 2012. URL: http://ssrn.com/abstract=2083638 or http://dx.doi.org/10.2139/ssrn.2083638
55. *Langseth H., Portinale L.* Bayesian networks in reliability // Reliability Engineering and System Safety. 2007. 92(1). P. 92–108.
56. Léger *A., Duval C., Farret R., Weber P., Levrat E., Iung B.* Modeling of human and organizational impacts for system risk analyses // 9th International Probabilistic Safety Assessment and Management Conference, Hong Kong, China. 2008. [Электронный ресурс] URL: http://www.hkarms.org/ASUS_Server/psam9.sytes.netweb_resources_20080518_PSAM9/Parallel_Session/D_Harbour_III/Thu_10-12/D12_1520-1650/Modeling_of_human_and_organizational_impacts_for_system_risk_analyses.pdf (доступ 01.03.2013)
57. *Lee E., Park Y., Shin J.G.* Large engineering project risk management using a Bayesian belief network // Expert Systems with Applications. 2009. Vol. 36. No 3. P. 5880–5887.
58. *Li P. C., Chen G. H., Dai L. C., Zhang L.* A fuzzy Bayesian network approach to improve the quantification of organizational influences in HRA frameworks // Safety Science. 2012. 50(7). P. 1569–1583.
59. *Li L., Wang J., Leung H., Jiang C.* Assessment of catastrophic risk using bayesian network constructed from domain knowledge and spatial data // Risk Analysis. 2010. 30(7). P. 1157–1175.
60. *Mahadevan S., Zhang R., Smith N.* Bayesian networks for system reliability reassessment // Structural Safety. 2001. Vol. 23, No 3. P. 231–251.

61. *McCann R. K., Marcot B. G., Ellis R.* Bayesian belief networks: applications in ecology and natural resource management // Canadian Journal of Forest Research. 2006. Vol. 36, No 12. P. 3053–3062.
62. *McNeil A. J., Frey R., Embrechts P.* Quantitative risk management: concepts, techniques, and tools. Princeton university press, 2005. 538 p.
63. *de Melo A. C. V., Sanchez A. J.* Software maintenance project delays prediction using Bayesian Networks // Expert Systems with Applications. 2008. Vol. 34, No 2. P. 908-919.
64. *Mikes A.* Enterprise risk management in action // London School of Economics Centre for Analysis of Risk and Regulation: Discussion Paper. 2005. No 35. Также доступно URL: http://webfirstlive.lse.ac.uk/researchAndExpertise/units/CARR/pdf/DPs/Disspaper35.pdf
65. *Monti S., Carenini G.* Dealing with the expert inconsistency in probability elicitation // IEEE Transactions on Knowledge and Data Engineering. 2000. 12 (4). P. 499–508.
66. *Moosa I., Li L.* An operational risk profile: the experience of British firms // Applied Economics. 2013. 45:17. P. 2491–2500. Также доступно URL: http://dx.doi.org/10.1080/00036846.2012.667556
67. *Moses J.* Bayesian probability distributions for assessing measurement of subjective software attributes // Information and Software Technology. 2000. Vol. 42, No 8. P. 533–546.
68. *Nelsen R.* B. An introduction to copulas. Springer, 2006. 272 p.
69. *Neil M., Fenton N., Tailor M.* Using Bayesian networks to model expected and unexpected operational losses // Risk Analysis. 2005. Vol. 25, No 4. P. 963–972.
70. Øien K. A framework for the establishment of organizational risk indicators // Reliability Engineering and System Safety. 2001. Vol. 74. P. 147–168.
71. *Pearl J.* Probabilistic Reasoning in Intelligent Systems. NYC: Morgan Kaufmann, 1988. 552 p.
72. *Pendharkar P. C., Subramanian G. H., Rodger J.* A. A probabilistic model for predicting software development effort // Software Engineering, IEEE Transactions on. 2005. Vol. 31, No 7. P. 615–624.
73. *Pfeifer D., Neslehova J.* Modeling and generating dependent risk processes for IRM and DFA // Astin Bulletin. 2004. Vol. 34, No 2. P. 333–360.
74. *Power M.* The invention of operational risk // Review of International Political Economy. 2005. № 12. P. 557–599.
75. *Radlinski L.* A survey of bayesian net models for software development effort prediction // International Journal of Software Engineering and Computing. 2010. Vol. 2, No 2. P. 95–109.
76. *Ren J., Wang J., Jenkinson I.* Fuzzy Bayesian modelling in maritime risk analysis // GERI Annual Research Symposium. 2005.
77. Settas D., Bibi S., Sfetsos Panagiotis, Stamelos, I., Gerogiannis, V. Using Bayesian Belief Networks to Model Software Project Management Antipatterns // Software Engineering Research, Management and Applications, 2006. Fourth International Conference on. 2006. P. 117–124. Также доступно URL: http://doi: 10.1109/SERA.2006.68
78. Sienou A., Lamine E., Karduck A., Pingaud, H. Conceptual model of risk: Towards a risk modelling language. // Web Information Systems Engineering–WISE 2007 Workshops. Springer Berlin/Heidelberg, 2007. P. 118–129.
79. *Sii H. S., Wang J., Eleye-Datubo A. G., Liu J., Yang J. B.* Safety assessment of FPSO turret-mooring system using approximate reasoning and evidential reasoning // Journal of Marine Technology. 2005. 42(2). P. 88–102.
80. Shenoy C., Shenoy P.P. Bayesian network models of portfolio risk and return // Computational Finance. 2000. Vol. 1999. P. 87.
81. *Sommestad T., Ekstedt M., Johnson P.* A probabilistic relational model for security risk analysis // Computers & Security. 2010. Vol. 29, No 6. P. 659–679.

82. *Spiegelhalter D. J., Dawid A. P., Lauritzen S. L., Cowell R. G.* Bayesian Analysis in Expert Systems // Statistical Science. 1993. Vol. 8. No 3. P. 219–247. URL: http://www.jstor.org/stable/2245959
83. *Stamelos I., Angelis L., Dimou P., Sakellaris E.* On the use of Bayesian belief networks for the prediction of software productivity // Information and Software Technology. 2003. Vol. 45, No 1. P. 51-60.
84. *Straub D.* Natural hazards risk assessment using Bayesian networks //Safety and Reliability of Engineering Systems and Structures. 2005. P. 2535–2542.
85. *Trucco P., Cagno E, Ruggeri F., Grande O.* A Bayesian Belief Network modeling of organizational factors in risk analysis: a case study in maritime transportation // Reliability Engineering and System Safety. 2008. No 93. P. 823–834.
86. *Uusitalo L.* Advantages and challenges of Bayesian networks in environmental modelling // Ecological modelling. 2007. Vol. 203, No 3. P. 312–318.
87. *Weber P., Medina-Oliva G., Simon C., Iung B.* Overview on Bayesian networks applications for dependability, risk analysis and maintenance areas // Engineering Applications of Artificial Intelligence. 2012. 25(4). P. 671–682.
88. *Weick K. E., Sutcliffe K. M., Obstfeld D.* Organizing for high reliability: Processes of collective mindfulness // Crisis management. 2008. Vol. 3. P. 81–123.
89. *Weidl G., Madsen A. L., Israelson S.* Applications of object-oriented Bayesian networks for condition monitoring, root cause analysis and decision support on operation of complex continuous processes // Computers & chemical engineering. 2005. Vol. 29, No 9. P. 1996-2009.
90. AgenaRisk [электронный ресурс] URL: http://www.agenarisk.com/ (дата обращения: 01.03.2013)
91. AgenaRisk Case Studies [электронный ресурс] URL: http://www.agenarisk.com/agenarisk/case_studies.shtml (дата обращения: 01.03.2013)

Поддержка исследований. Работа выполнена при финансовой поддержке РФФИ, гранты № 12-01-00945-а, 12-01-31202-мол_а.

Мусина Валерия Фуатовна — младший научный сотрудник лаборатории теоретических и междисциплинарных проблем информатики СПИИРАН, студент магистратуры экономического факультета СПбГУ. Область научных интересов: случайные процессы, вероятностное и статистическое моделирование, биостатистика, вероятностные графические модели. Число научных публикаций — 13. ALT@iias.spb.su, www.tulupyev.spb.ru; СПИИРАН, 14-я линия В.О., д. 39, г. Санкт-Петербург, 199178, РФ; р.т. +7(812)328-3337, факс +7(812)328-4450.

Musina Valeriya Fuatovna — junior research fellow Theoretical and Interdisciplinary Computer Science Laboratory, St. Petersburg Institute for Informatics and Automation of the Russian Academy of Sciences (SPIIRAS), graduate student of Faculty of Economics at Saint Petersburg State University. Research area: stochastic processes, probabilistic and statistic modelling, biostatistics, probabilistic graphical models. Number of publications — 13. ALT@iias.spb.su, www.tulupyev.spb.ru; SPIIRAS, 14-th line V.O., 39, St. Petersburg, 199178, Russia; office phone +7(812)328-3337, fax +7(812)328-4450.

Рекомендовано ТиМПИ СПИИРАН, зав. лаб. А.Л. Тулупьев, д.ф.-м.н., доцент.
Статья поступила в редакцию 23.01.2013.

РЕФЕРАТ

Мусина В.Ф. **Байесовские сети доверия как вероятностная графическая модель для оценки экономических рисков.**

Оценка экономических рисков является одним из этапов риск-менеджмента предприятия и тесно связана с этапами идентификации и управления риском.

Риски, с которыми сталкивается предприятие в процессе своего функционирования, могут иметь различную природу. Некоторые типы рисков, как например риск негативного влияния человеческого и организационного факторов на деятельность предприятия, невозможно оценить лишь количественными методами. Описание таких типов риска состоит как из качественной информации, описывающей сценарии и ситуации, так из количественной информации, имеющей отношение к характеристикам работы системы. Таким образом, управление рисками предприятия требует системного подхода.

Цель данной статьи заключается в анализе современного состояния применения аппарата байесовских сетей доверия для оценки экономического риска и поддержки принятия решений в условиях неопределенности в контексте риск-менеджмента предприятия. Отдельно рассмотрены дисциплины управления операционными рисками и рисками проектов, которые являются составными частями общего риск-менеджмента предприятия.

Байесовские сети доверия представляют собой инструмент, позволяющий включать в модель качественную информацию и естественным образом моделировать зависимости между различными рисками. Кроме того, байесовские сети доверия могут быть адаптированы для решения конкретных задач: для представления большого числа рисков предприятия могут использоваться объектно-ориентированные байесовские сети доверия, для описания экспертной информации — нечеткие байесовские сети доверия.

Байесовские сети доверия используются для количественного описания влияния человеческого и организационного факторов, для описания надежности сложных систем, при моделировании рисков информационной безопасности системы предприятия, финансовых рисков предприятия, рисков опасных природных явлений, операционных рисков, рисков проектов.

SUMMARY

Musina V.F. **Bayesian belief networks as probabilistic graphical model for economical risk assessment.**

Economical risks assessment is one of the stages in risk-management of enterprise and is closely connected to the stages of risk identification and risk control.

Risks associated with the enterprise performance can be of different nature. One cannot assess some types of risks using only quantitative methods, e.g. impact of human and organizational factor on enterprise activities. Such risks are assessed using combinations of qualitative (scenarios and events modeling) and quantitative (system performance characteristics) information. Thereby a system approach to enterprise risk modeling and management is required.

The goal of the paper is state-of-art analysis of Bayesian belief networks use for economical risk assessment and decision making under uncertainty support in the framework of enterprise risk management. The areas of operational risk management and project risk management are singled out.

Bayesian belief networks are a tool that can integrate qualitative and quantitative information in the model and naturally describe dependencies among different types of risks and their components. In addition, Bayesian belief networks can be adapted for the solution of specific problems: object-oriented Bayesian networks can be used for the solution of the modeling of huge amount of enterprise risk problem; fuzzy Bayesian network can be used in systems heavily relied on expert information.

Bayesian belief networks find their application in the areas of qualitative human and organizational factor impact description; for complex system safety modeling; for information security of an enterprise modeling; for enterprise's financial, operational and project management risks assessment; for natural hazards and ecological risk modeling.