УДК 51-74 + 004.4'2

М.В. Владимирова, Махмуд Омар Махмуд Хасан

Харьковский национальный университет им. В.Н. Каразина

СИСТЕМНЫЙ ПОДХОД К ПОНЯТИЮ «РИСК» ПРИ РАЗРАБОТКЕ БОЛЬШИХ ПРОГРАММНЫХ КОМПЛЕКСОВ

В статье предложен обзор существующих подходов к вопросам риска при разработке программного обеспечения. Сделан обзор стандартов, а также рассмотрены 4 модели управления рисками в программном обеспечении. На основании приведенного обзора, предложен адаптивный подход к построению моделей для оценки и анализа риска, а также к построению системы принятия решений, основанный на этих моделях.

риск, программный комплекс, системный подход

Введение

Что такое риск? Чаще всего, понятие риск тесно связывают с понятием качества. Если под качеством обычно понимают удовлетворение всех требований заказчика и характеристики качества пытаются улучшать, то риск - это негативные события или величины, отражающие потери, и существующие методики чаще всего сводятся к оценке ущерба и направлены на минимизацию или, если возможно, ликвидацию риска.

Теория риска начала интенсивно развиваться примерно с 50-х годов нашего столетия. Наибольшее число исследований, посвященных анализу риска, принадлежит американским ученым, хотя эта проблема активно изучалась и в западноевропейских странах. С тех пор термин «риск» встречается в большинстве наук. В каждой их них, исходя из специфики науки, есть свои направления исследований риска, его анализа, свои методы оценки.

Чаще всего можно встретить такое определение риска- «риск – это опасность потерь». Такое определение не решает вопроса об измеряемости риска, о его количественной оценке. Начиная с 1990-х гг., с появлением концепции *Value-At-Risk* [1], риск начали определять через *вероятность потерь*. Соответственно, измерение риска было сведено к измерению размера потенциальных потерь. Приведем ряд примеров определений риска, встречающихся в литературе. Согласно ряду авторов, риск – это:

– это вероятность возникновения потерь, убытков, недопоступлений планируемых доходов, прибыли" [2].

– негативные события и их величины, отражающие потери, убытки или ущерб [2].

– наиболее близко к бытовому представлению о риске его определение, принятое в актуарном деле: здесь под риском понимают "гипотетическую возможность наступления ущерба («страхового случая") [11]. Страховые расчеты – исторически первая область науки о риске. В работе [15] сказано: "страхование призвано заменить *определенностью* ту *неопределенность* в экономической стоимости, которая может быть обусловлена будущими потерями".

Говоря о риске, нельзя не упомянуть о тесно связанном с ним понятии неопределенности. Неопределенность предполагает наличие факторов, при которых результаты действий не являются детерминированными, а степень возможного влияния этих факторов на результаты неизвестна [2]. Факторы неопределенности подразделяются на внешние и внутренние. Внешними факторами, например, могут быть: законодательство, реакция рынка на выпускаемую продукцию, действия конкурентов; внутренними факторами могут быть, например, компетентность персонала фирмы, ошибочность определения характеристик проекта и т.д. Согласно работе [8], все неопределенности принято относить к одной из двух групп: *чистые* и *спекулятивные*. В условиях *спекулятивной* неопределенности возможен как выигрыш (увеличение полезности) субъекта, так и проигрыш (потеря полезности). *Чистые* неопределенности связаны только с возможностью потерь.

С точки зрения автора [11], в отличие от неопределенности, риск возникает только в тех ситуациях, когда экономический субъект принимает решения (совершает целенаправленные действия). Будучи неразрывно связанным с принятием решений, риск является *прогностической оценкой* возможности и последствий осуществления действия. Аналогичное понимание риска можно встретить в кибернетике, где неопределенность интерпретируется как неудача (неуспех) в предсказании поведения некоторой системы на базе предполагаемых законов ее поведения и доступной информации о ее начальном состоянии. При этом в условиях неопределенности субъект может осуществить действие, отсрочить его осуществление либо вообще отказаться от выполнения действия.

Классическая концепция взаимосвязи риска и неопределенности была сформулирована в работе Ф. Найта [17]. Согласно этой концепции, риск – это

измеримая неопределенность – экономический субъект может "предвидеть" или "угадать" некоторые параметры (результаты, условия) своего действия в будущем. С точки зрения количественного анализа это означает, что распределение ассоциированной с риском (случайной) величины может быть каким-то образом определено. Соответственно, неопределенность связана с отсутствием какого-либо способа определения распределения и не поддается ни объективному, ни субъективному измерению.

Развитие подходов Ф. Найта в область количественного анализа рисков привело к созданию теории рационального выбора и теории оценки предпочтения состояний (*state preference theory*).

Неопределенность здесь описывается как конечное множество взаимоисключающих состояний $S = \{S1, S2, \ldots, Sn\}$, при этом каждому из состояний Si приписывается его вероятностная оценка P(Si). Реализация конкретного состояния Si полностью определяет значения всех экзогенных переменных (т.е. состояние внешней среды). Субъект, совершающий выбор, способен ранжировать свои предпочтения в зависимости от вероятностных оценок.

Таким образом, риск можно рассматривать как конкретную реализация внешнего по отношению к экономическому субъекту состояния "реального мира" (*real world state*). Неблагоприятный исход которого не достоверен, но и не невозможен: $0 < P(Si) < 1$ (т.к. при $P(Si) = 0$ событие невозможно, при $P(Si) = 1$ событие достоверно).

Наиболее полное, на наш взгляд, определение риска, меры риска и стоимости риска приведено в работе [11].

Риск – это возможное нежелательное событие (или класс возможных нежелательных событий), под действием которого объект управления может перейти в нежелательное состояние (называемое *рисковой ситуацией*). При этом под *реализацией риска* понимается появление события риска и переход объекта управления в нежелательное состояние под влиянием этого события.

Определение риска содержит в себе три ключевых компонента, которые неявно объединены в широко распространенном "бытовом" понимании риска.

Во-первых, риск связан с событиями-причинами.

Во-вторых, события наступают или не наступают – т.е. они не достоверны, а лишь возможны.

В-третьих, сами по себе события ни нежелательны, ни благоприятны – в каждом конкретном случае требуется оценка их последствий для пользователя управляемой системы, т.е. оценка качества состояний, в которые может попасть система в результате реализации:

Мера риска – это, во-первых, мера возможности риска и, во-вторых, мера нежелательности состояния, в которое попадает объект управления при реализации риска [11].

Стоимость риска. Пусть для произвольного состояния x системы сформулировано утверждение (набор признаков) "состояние x нежелательно". Стоимостью риска назовем величину потерь μ для данного состояния x и события риска E: μ(x, E) [11].

Основной материал

Обзор существующих подходов к вопросам риска при разработке программного обеспечения. При разработке программных систем понятие «риск», пожалуй, самое «молодое» понятие по сравнению с понятием риска в других областях. Тем не менее, особенно при разработке больших, сложных систем, систем критического назначения, где ценой последствий рисковых событий может быть в худшем случае, закрытие проекта (что может исчисляться миллионами долларов), или потеря человеческих жизней, риску уделяется большое внимание.

Выделяют три категории риска [13]:

– *риски функциональной пригодности*. Это неверно понятые, неполные или искаженные требования заказчика, их искаженная реализация;

– *риски,* связанные с недостаточными или несоответсвующими требованиям реализации *конструктивных характеристик* качества ПО при его функционировании;

– *риски*, связанные с нарушением ограничений *на использование экономических, временных или технических ресурсов.*

Для снижения возможного ущерба – рисков применяются анализ, оценка и мониторинг рисков. Кроме того, иногда экономически выгодней применять различные профилактические меры, которые смогут либо устранить причины возникновения рисковых событий– угрозы, либо уменьшать последствия, если все-таки рисковое событие произойдет. Риски проявляются как на всех стадиях разработки ПО, так и при эксплуатации готового ПО. И, если при разработке ПО, ущерб от происшедших рисковых событий может привести максимум к закрытию проекта, то ущерб от рисков, происшедших во время эксплуатации системы может привести к авариям или даже катастрофам, т.е. это уже будет проблема безопасности. Таким образом, анализ рисков ПО должен быть тесно связан с исследованием возможности их проявления во внешней среде, где будет эксплуатироваться система.

Обзор стандартов.

Общие методы анализа рисков в сложных системах регламентированы стандартом **ГОСТ Р51901** – «Управление надежностью. Анализ риска технологических систем». Основной задачей стандарта является обоснование решений, касающихся анализа риска реализации проектов и технологий сложных систем. Изложенные в стандарте рекомендации могут быть, в частности, применены при технико-экономическом обосновании, при разра-

ботке ПО, при управлении рисками в других областях (охрана здоровья, безопасность, предотвращение экономических потерь и т.д.).

В стандарте рассматриваются следующие факторы:

• выявление факторов, обуславливающих риск, и слабых звеньев в системе;

• более глубокое понимание назначения, структуры и функционирования системы;

• сопоставление риска исследуемой системы с рисками альтернативных систем или технологий;

• идентификация и сопоставление рисков и их неопределенностей при анализе;

• обеспечение возможности поставарийного расследования и мер по предупреждению аварий;

• возможность выбора контрмер и приемов по обеспечению снижения риска.

Анализ риска при разработке ПО рассматривается на двух стадиях жизненного цикла опасных систем: стадии проектирования и стадии изготовления, эксплуатации и технического обслуживания.

Управление рисками на всем жизненном цикле программных средств регламентировано **международными стандартами: ISO 12207** – «Процессы жизненного цикла программных средств» и **ISO 15504** – «Оценка и аттестация зрелости процессов создания и сопровождения программных средств и информационных систем». Эти стандарты целесообразно использовать при разработке комплексов программ. В стандарте ISO 15504 содержится специальный раздел МАН.4. «Процесс управления рисками», назначением которого является регламентирование и планирование процессов выявления и устранения совокупности различных рисков на протяжении всего жизненного цикла ПО [5, 9]. В результате такого стандартизированного процесса, менеджером по управлению рисками должны быть определены возможные источники рисков в исходных требованиях к проекту, а также возможные источники риска к характеристикам качества разрабатываемого ПО. Риски должны быть проанализированы и определены сбалансированные приоритеты для их сокращения. На основании проведенного анализа должны выделяться ресурсы на сокращение рисков, определятся рациональные стратегии управления, методы и средства уменьшения рисков в ЖЦ ПО. Для решения поставленных задач в стандарте перечислены рекомендуемые последовательные процедуры.

В [3] рассмотрены анализ и процессы управления рисками информационных систем (ИС) с позиции обеспечения информационной безопасности, в соответствии с концепцией **стандарта NIST 800-30** – «Руководство по управлению рисками для систем информационных технологий». В этом стандарте предлагается решать проблемы информационной безопасности с учетом уровня зрелости технологий предприятий, создающих информационные системы. В отличие от предыдущих стандартов, особое внимание в модели анализа и управления рисками уделяется идентификации внешних угроз, выделению потенциальных уязвимостей ИС, анализу возможных последствий и контрмерам для сокращения рисков преднамеренного нарушения безопасности информационных ресурсов. В соответствие с классами угроз рекомендуется выбор и оценка эффективности контрмер для снижения рисков. Риски при функционировании программных средств, обусловленные дефектами при их проектировании, разработке и сопровождении, не учитываются. В этом же стандарте приведен глоссарий терминов, относящихся к области управления рисками. Там же приведен обзор инструментальных средств для автоматизированного анализа и управления рисками в рассматриваемом классе систем и задач.

В стандарте **ESA PSS-05-08** приведена базовая классификация рисков при разработке ПО и даны указания по качественному анализу рисковых ситуаций. Кроме того, там рассмотрены два наиболее простых метода количественного управления рисками – метод построения риск-таблиц и метод построения матриц рисков.

В стандарте **STD-12 v1.0** содержится описание классификации рисков в зависимости от источника угроз, в нем же приведена схема качественного анализа рисков.

Основные модели управления рисками.

Наиболее полный анализ существующих подходов к управлению рисками при разработке ПО, на наш взгляд, приведен в работе [13]. В работах [3 – 8] описаны основные модели управления рисками.

Рассмотрим кратко эти модели.

Институт программного инжиниринга (SEI) [4, 6] разработал модель оценки рисков при разработке программ, основанную на цикле Щухарта-Деминга. которая поддерживает информацию о получении откликов как внутри, так и вне проектов. Модель управления представлена на рис. 1.

Для каждого риска, имеющего высокий уровень угрозы, должна проводится оценка его вероятности, определение количественных показателей, характеризующих проявление и последствия от наступления рискового события. Мера для оценивания эффекта изменения рисков при относительных затратах вычисляется как

$$\mu = \frac{K_2 - K_2}{s},$$

где s – стоимость затраченных ресурсов по выполнению действий, направленных на снижение риска; K_2 – коэффициент, полученный до выполнения действий по снижению риска; K_1 – коэффициент, полученный после выполнения действий по снижению риска.

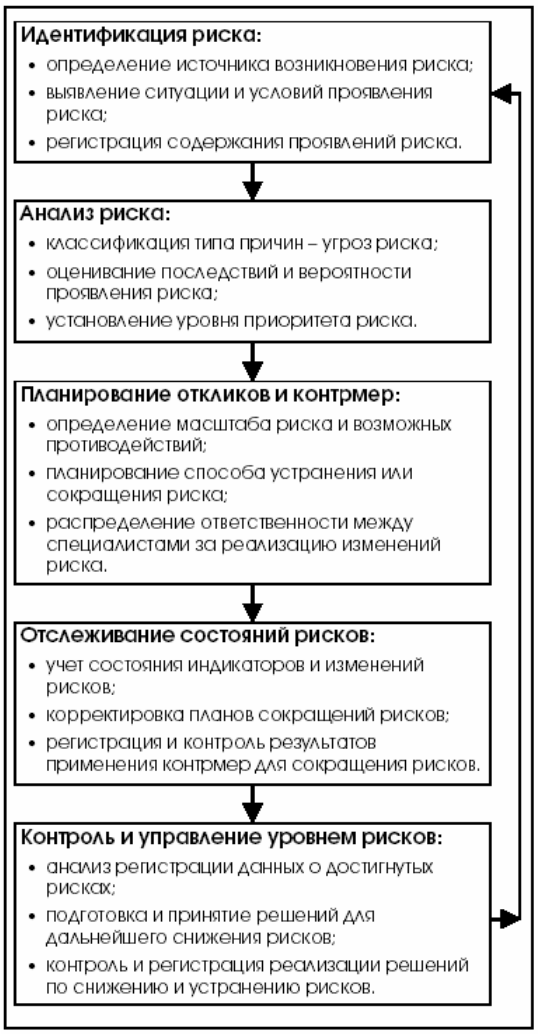

Рис. 1. Модель управления проектными рисками

Интегральный риск представляет собой разложение многофакторных рисков на однофакторные компоненты, что позволяет оценивать приоритеты среди рисков. Путем разложения риска на части можно адресовать ответственность отдельным специалистам и определять каждый элемент риска.

В соответствии с предложенной моделью, управление рисками включает планирование менеджмента рисков, определение состояния и мониторинг рисков. Наряду с оцениванием рисков эти компоненты должны поддерживаться наборами инструментов и методик.

Вторая модель управления рисками – модель проектного риска по Боэму [6] (рис. 2).

В отличие от первой модели (SEI), состоящей из 5 этапов, в этой модели структура содержит шесть этапов, содержание которых охватывает те же процессы. Кроме того, в этой модели выделены десять компонентов – наиболее важных причин при управлении рисками проектов сложного ПО. По каждому из этих компонентов предлагаются рекомендованные процедуры их сокращения.

В [4] предлагается **третья модель управления рисками** с использованием 12 категорий потенциального риска для определенного типа проекта. Для каждой категории детально представлены факторы, влияющие на риски, и рекомендуется проводить их оценки по трем уровням возможного проявления (низкая, средняя, высокая очевидность угрозы риска). Описания содержания, атрибутов и возможных откликов на риск представлены в таблицах [4]. При отсутствии достаточного опыта, эти таблицы можно рассматривать как руководство по анализу ключевых рисков и угроз при разработке ПО. План управления проектными рисками для конкретного ПС рекомендуется моделировать по следующим категориями:

1. Задачи и цели.
2. Организационный менеджмент.
3. Заказчик.
4. Бюджет/стоимость.
5. График.
6. Содержание проекта.
7. Выполнение.
8. Управление проектом
9. Процессы разработки.
10. Среда разработки.
11. Персонал.
12. Поддержка.

Подробное описание категорий и рисков по каждой категории также приведено в [4]. В этой же работе выделены десять наиболее важных факторов риска и откликов на них и предложены рекомендации откликов при наступлении рисковых событий.

Для успешного управления рисками рекомендуется разработка плана, состоящего из пяти этапов.

Этап 1. Используя описанные категории рисков, рекомендуется создать свою таблицу категорий. Таблица категорий рисков должна содержать сведения о том, какие факторы рисков более реальны и насколько они очевидны. Данная таблица является отправной точкой при идентификации определенных рисков в каждом проекте.

Этап 2. Риски, связанные с выполнением проекта, ранжируются по категориям:

• факторы риска и области – для каждой категории в столбце перечисляются факторы и угрозы категории риска;

• выделяется низкая очевидность рисков (относительно невысокая вероятность и малые последствия риска для проекта);

• средняя очевидность рисков (среднюю вероятность, и последствия рисков для проекта);

• высокая очевидность рисков (вероятность и негативные последствия риска для проекта достаточно велики);

• определение рейтинга (выделение уровня интегрального риска, допустимого для данного проекта);

• комментарии (информация об особенностях проекта, которая позволяет соблюдать выбранный рейтинг).

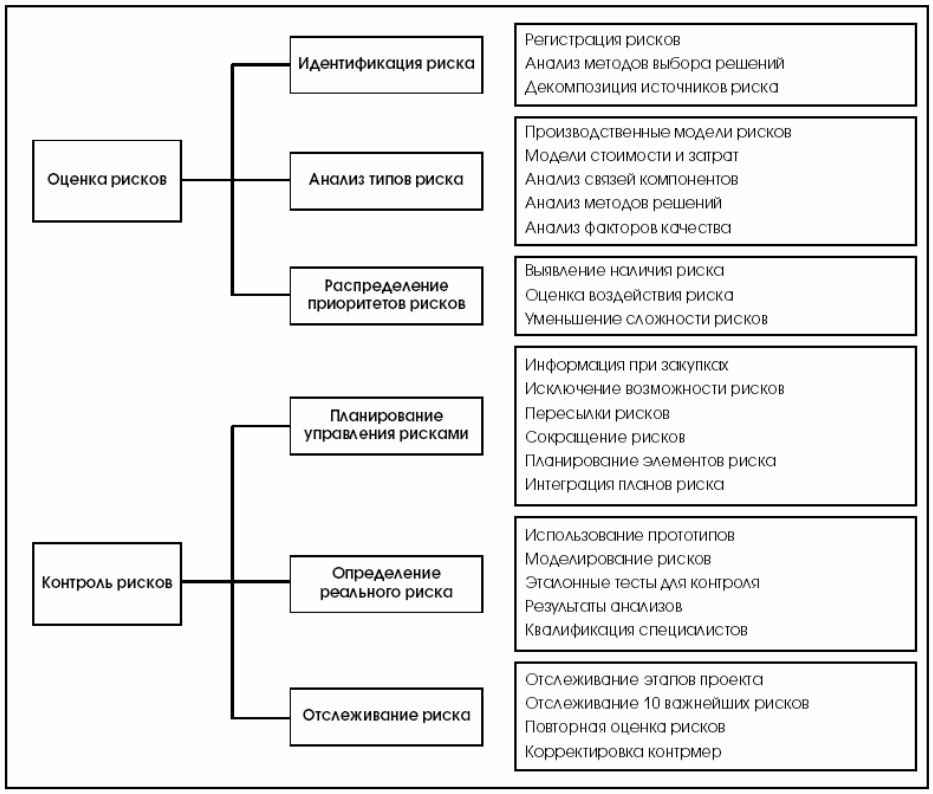

Рис. 2. Модель управления проектными рисками по Боэму

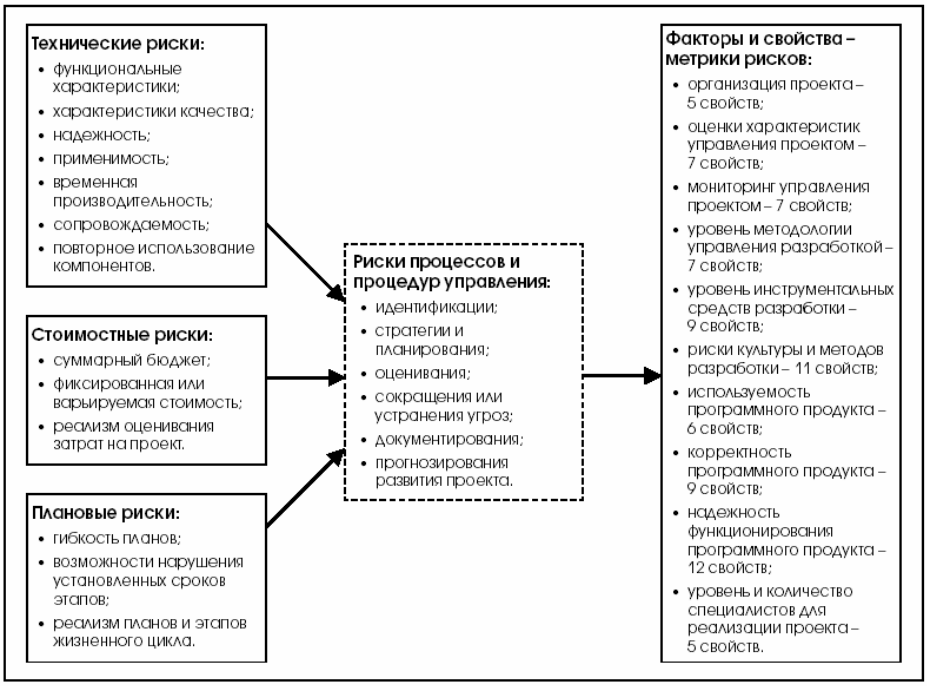

Рис. 3. Модель управления рисками, основанная на крупных элементах

В этом же источнике приведена таблица факторов риска и категорий, для которых очевидность риска характеризуется соответственно как низкая, средняя или высокая.

Этап 3. Выполняется сортировка таблицы рисков (риски располагаются в порядке убывания очевидности и угрозы; сначала перечисляются риски с самой высокой очевидностью). Вычисляется интегральный риск для наибольших десяти рисков, а также для всех рисков, отмеченных как высокие, если их больше десяти.

Этап 4. Устанавливается формат отчета для каждого регулярного риска.

Этап 5. На заключительном этапе следует удостовериться, что управление и сокращение рисков является непрерывным процессом в рамках жизнен-

ного цикла проекта ПС. Отслеживание и контроль рисков, включенных в список, должны выполняться регулярно.

Таким образом, используя предварительное деление на 12 категорий рисков, предлагается выполнить ранжирование и отсортировать риски таким образом, чтобы ими можно было управлять в конкретном проекте. Затем, рассматриваемый план в процессе идентификации потенциальных угроз и рисков уточняется, вводятся (уточняются) категории и устанавливаются (уточняются) приоритеты.

В [8] предложена и детально рассмотрена **четвертая модель анализа рисков,** связанных с разработкой ПО. Эта модель основывается на крупных элементах, факторах и свойствах – метриках рисков, к каждому из которых приводится краткое описание их содержания.

Компоненты анализа рисков иллюстрируются таблицами связей и взаимодействия. В элементы риска включены взаимосвязанные технические, стоимостные и плановые риски.

Различные подходы к математическим моделям оценки риска. Элементы процесса оценки величины риска являются общими для всех видов угроз [13]. Прежде всего анализируются возможные причины угрозы с целью определения частоты ее возникновения, продолжительности, а также характера угрозы.

В процессе анализа может возникнуть необходимость определения оценки вероятности осуществления угрозы, вызывающей негативные последствия, и проведения анализа последовательности событий, смягчающих рисковые ситуации.

Для оценки вероятности каждого негативного события, проявившегося на стадии идентификации угроз, чаще всего проводят анализ частот происходящих событий.

Для оценки частот обычно применяются следующие три метода:

• использование имеющихся статистических данных (предысторий);

• получение частот негативных событий на основе аналитических или имитационных методов;

• использование мнений экспертов.

В работе [1] проверку результатов анализа предлагается осуществлять экспертами, не привлеченными к участию в выполнении проекта. Проверка должна включать в себя следующие этапы:

• проверка соответствия области применения анализа поставленным задачам;

• проверка всех важных допущений при анализе для обеспечения уверенности в том, что они являются правдоподобными в условиях имеющейся информации;

• подтверждение аналитиком правильности использованных методов, моделей и данных;

• проверка результатов анализа на повторяемость с привлечением персонала, не участвующего в выполнении анализа;

• проверка результатов анализа на устойчивость по отношению к различным форматам данных.

В работах [5, 9] представлен ряд методов для сопоставления экспертного мнения, которые исключают двусмысленность оценок, помогают при постановке соответствующих вопросов.

Для оценки риска в других областях чаще всего используются следующие типы математических моделей:

1. Графические методы оценки и сравнения рисков.

2. Частотный подход.

3. Модель риска, основанная на условных вероятностях.

4. Модели относительного риска

5. Модели риска, которые используют функции распределения.

6. Регрессионные модели оценки риска.

Результатом работы этих моделей является количественная характеристика риска, которую, как правило, выражают в следующих показателях:

• диаграммы частоты в зависимости от последствия, либо совокупная стоимость ущерба;

• статистически ожидаемый размер потерь от возникновения аварий, экономических затрат или урона для окружающей среды;

• распределение риска с соответствующим уровнем ущерба, представленное в виде графика и указывающее уровни равного ущерба.

Обзор этих моделей, а также обзор программных инструментов для оценки и анализа рисков не входит в задачи данной статьи. Но хотелось бы подчеркнуть, что в этой области, области количественной оценки и анализа рисков, уже достаточно много наработок. Эти наработки касаются различных предметных областей и некоторые из них могли бы быть адаптированы для оценки риска при разработке ПО.

Риск и система принятия решений. Как видно из предложенного обзора, существующие модели анализа риска при разработке ПО в основном касаются качественного анализа рисковых событий, а все количественные оценки базируются чаще всего на экспертных данных или на знании исторических данных работы над аналогичными или подобными проектами. При этом известно, что влияние человеческого фактора может внести при оценке риска достаточно большую погрешность.

Использование статистических данных (предысторий) также не всегда возможно, поскольку одной из основных характеристик проекта является его уникальность.

Второй характеристикой проекта при разработке ПО является его длительность. Известно, что средний проект разрабатывается до 5 лет, а длительность большого проекта, естественно, больше. В течении этого времени меняются как угрозы внутри самого проекта, так происходит и изменение внешней среды. При этом данные для оценки рисков с течением времени получаются тоже по-разному: где-то известна функция распределения, где-то можно вычислить условные вероятности и т.д. Как правило, для анализа риска используется один инструмент, в котором заложена определенная, но одна, модель. Однако, использование одной модели на протяжении всей работы над проектом также может привести к результатам с большой погрешностью.

Поэтому целью данного исследования является построение *адаптивной* модели принятия решения при разработке ПО с учетом изменения и влияния на проект факторов внешней среды.

Выводы

Разработка ПО является сложной системой со многими видами неопределенности, но все множество проектов можно разбить на такие подмножества, к которым можно применять различные методы принятия решений. В основе этих методов будут использованы те модели оценки риска или их сочетания, которые наиболее адекватны разрабатываемому проекту. Таким образом, основной задачей исследования является построение моделей для оценки и анализа риска, а также адаптация существующих моделей, включая и модели из других предметных областей, под реальные проекты.

Список литературы

1. Финансовый менеджмент / Под. ред. Г.Б. Поляка. – М.: Финансы, ЮНИТИ, 1997. – 340 с.

2. Risk Management – A Practical Guide // J.P. Morgan-Reuters RiskMetrics,LLC, 1998. [Электрон. ресурс]. – Режим доступа: http://www.bis.org.

3. Симонов С. Технологии и инструментарий для управления рисками // Jet Info. – 2003. – № 2. – С. 37-41.

4. Фатрелл Р.Т., Шафер Д.Ф., Шафер Л.И. Управление программными проектами: достижение оптимального качества при минимальных затратах: Пер. с англ. – М.: Вильямс, 2003. – 360 с.

5. Оценка и аттестация зрелости процессов создания и сопровождения программных средств и информационных систем (ISO/IEC TR 15504 – CMM). – М.: Книга и бизнес, 2001. – 320 с.

6. Boehm B.W. Software risk management // IEEE Computer Society Press. – Washington. – 1989. – P. 137-141.

7. Charett R. Software engineering risk analysis and management. – N.Y.: McGraw – Hill, 1989. – 440 p.

8. Karolak D.W. Software engineering risk management // IEEE Computer Society Press. – Washington. – 1996. – P. 121-124.

9. Липаев В.В. Методы обеспечения качества крупномасштабных программных средств. – М.: РФФИ, СИНТЕГ, 2003. – 260 с.

10. Кантор М. Управление программными проектами. Практическое руководство по разработке успешного программного обеспечения: Пер. с англ. – М.: Вильямс, 2002. – 560 с.

11. Бершадский А.В. Исследование и разработка сценарных методов управления рисками: Дисс… канд. физ.-мат. наук, специальность 05.13.18 «Математическое моделирование, численные методы и комплексы программ». – 179 с.

12. Качинський А.Б. Засади системного аналізу безпеки складних систем. – ДП «НВЦ «Євроатлантикінформ», 2006. – 336 с.

13. Липаев В.В. Анализ и сокращение рисков проектов программных средств. – М.: ФиС, 1983. – 360 с.

14. Vaughan E.J. Risk management. – John Wiley. – N.Y., 1997. – 560 p.

15. Ширяев А.Н. Основы стохастической финансовой математики. Т. 1: Факты, модели. – М.: ФАЗИС, 1998. – 336 с.

16. Knight F. Risk, Uncertainty, and Profit. – Boston Houghton Miffin Co, 1921. – 660 p.

17. Найт Ф. Риск, неопределенность и прибыль. – М.: Дело, 2003. – 360 с.

Поступила в редколлегию 17.01.2008

Рецензент: д-р физ.-мат. наук, проф. Г.Н. Жолткевич, Харьковский национальный университет им. В.Н. Каразина, Харьков.

СИСТЕМНИЙ ПІДХІД ДО ПОНЯТТЯ «РИЗИК» ПРИ РОЗРОБЦІ ВЕЛИКИХ ПРОГРАМНИХ КОМПЛЕКСІВ

Владимирова М.В., Махмуд Омар Махмуд Хасан

У статті запропонований огляд існуючих підходів до питань риска при розробці програмного забезпечення. Зроблен огляд стандартів, а також розглянуто чотири моделі управління ризиками в програмному забезпеченні. На підставі приведеного огляду, запропонований адаптивний підхід до побудови моделей для оцінки і аналізу риску, а також до побудови системи ухвалення рішень, заснований на цих моделях.

Ключові слова: *риск, програмний комплекс, системний підхід.*

SYSTEM APPROACH TO THE CONCEPT OF RISK IN SOFTWARE DEVELOPMENT

Vladymyrova M.V., Mahmud Omar Mahmud Hasan

The survey of existing approaches to the software risk management problems as well as the survey of standards is presented in the paper. Four models of risk management are considered. The adaptive approach to the model construction for risk evaluation and analysis and decision support system development is offered.

Keywords: *risk, software development, systems approach.*