УДК 004.942

Е. С. ЯШИНА, А. А. БЕРЕЖНАЯ

Национальный аэрокосмический университет им. Н. Е. Жуковского «ХАИ», Украина

КАЧЕСТВЕННЫЙ И КОЛИЧЕСТВЕННЫЙ АНАЛИЗ РИСКОВ В IT – ПРОЕКТАХ

Рассмотрены вопросы анализа и управления рисками проектов при разработке программных продуктов. Систематизирован терминологический аппарат и раскрыты основополагающие подходы к анализу и управлению рисками. Предлагается подход к качественной и количественной оценкам совокупного риска проекта, основанном на внедрении существующих подходов к управлению рисками. Полученные данные могут служить основой для регламентирования действий риск – менеджеров и позволяют прогнозировать наиболее вероятные сроки завершения проекта с учетом совокупности всех рисков проекта.

Ключевые слова: *управление рисками, риск, программный проект, неопределенность, информационные технологии.*

Введение

В силу специфики отрасли, производство программных проектов остается, и будет оставаться производством с высоким уровнем рисков. Если задуматься, то все, что мы делаем, управляя проектом разработки программного обеспечения (ПО), направлено на борьбу с рисками не уложиться в срок, перерасходовать ресурсы, разработать не тот продукт, который требуется.

В связи с постоянно возрастающей сложностью программных проектов, чрезвычайно трудно бороться с рисками без использования специальных программных приложений (систем управления рисками). В настоящее время на смену интуитивному планированию приходит строгий анализ и расчет. По данным исследовательской группы IDC за 2011 год, погрешность оценки ресурсов ПО – проектов составляет 25% в 75% случаев [1]. Реализация ПО – проектов в общем случае осуществляется в условиях неопределенности, обусловленной экономическими, техническими, юридическими факторами, а также существующими ресурсными и временными ограничениями. Кроме того, процесс проектирования и программирования практически не поддается жесткому нормированию, поскольку в общем случае имеет творческий, исследовательский характер. В связи с этим большая часть ПО – проектов не достигает изначально поставленных целей.

Понятия «оценка рисков» (Risk Assessment) и «управление рисками» (Risk Management) появились сравнительно недавно и сегодня вызывают постоянный интерес специалистов в области обеспечения непрерывности бизнеса (Business Continuity) и сетевой безопасности (Network Security) [2]. Примерно с 1995 года в ряде высокотехнологичных стран мира, главным образом в США, Великобритании, Германии и Канаде, проводятся ежегодные слушания специально созданных комитетов и комиссий по вопросам управления информационными рисками. Подготовлено более десятка различных стандартов и спецификаций, детально регламентирующих процедуры управления информационными рисками, среди которых наибольшую известность приобрели международные спецификации и стандарты ISO 17799-2002 (BS 7799), GAO и FISCAM, SCIP, NIST, SAS 78/94 и COBIT [3].

Постановка задачи исследования

Основными методологиями управления IT-рисками являются CORAS, OCTAVE и CRAMM. Однако они и им подобные имеют множество недостатков: отсутствуют методы количественной оценки рисков и четкие инструкции по мониторингу их состояния, нет подробных рекомендаций по проведению повторных оценок рисков. Используемые в настоящее время стандарты в области защиты информации рассматривают анализ и управление информационными рисками, однако не отражают ряд важных деталей, которые необходимо учитывать при разработке практических методик управления рисками.

В качестве методик управления рисками чаще всего коллективы разработчиков используют PMBoK и MSF, определяющие основные этапы жизненного цикла управления рисками: планирование управления рисками, идентификация, анализ рисков, планирование реагирования на риски, мониторинг, извлечение уроков.

В данной работе под риском понимается возможность возникновения неблагоприятной ситуации или неудачного исхода производственно-хозяйственной или какой-либо другой деятельности.

Планирование управления рисками - процесс, в рамках которого выясняется, каким образом будет осуществляться весь комплекс мер, связанных с анализом рисков, кто именно будет вовлечен в этот процесс, когда именно должны запускаться процедуры управления рисками и как часто.

При идентификации рисков важно обратить самое серьезное внимание на все допущения и предположения в проекте. Для наиболее полной идентификации рисков разработано несколько методов, которые по-разному сочетаются в реальной практике идентификации рисков. На сегодняшний день хорошо зарекомендовали себя методы – сравнение со списком рисков и списком категорий рисков; анализ рисков предыдущих проектов; мозговой штурм; интервью с экспертами.

С точки зрения методологии управления рисками важным и наиболее сложным этапом является анализ рисков. При этом, если методы качественного анализа широко известны и применяемы, то методы количественного анализа еще недостаточно распространены. Качественный анализ рисков применяется на начальных этапах управления рисками, методы качественного анализа сравнительно легко подстраиваются под параметры проекта и дают возможность получить грубую оценку совокупного риска проекта. Методы количественного анализа обычно требуют наличия информации о рисках, накопленной при помощи качественного анализа, и при корректной подстройке параметров дают более точные результаты. Среди методов количественного анализа можно отметить анализ чувствительности, анализ сценариев, метод достоверных эквивалентов, метод Монте-Карло, метод исторических симуляций, деревья событий, деревья отказов, логико-вероятностные методы, эвристические методы количественного анализа.

Качественная оценка рисков проводится с помощью оценки таких параметров риска, как вероятность возникновения и ожидаемая величина потерь.

При оценке риска наиболее часто используются экспертная оценка параметров риска и ее отображение в виде карты рисков (матрица вероятности и последствий). На одной из осей откладывается вероятность возникновения риска, на другой – угроза риска. Ожидаемая величина – итоговое воздействие риска, которое вычисляется по формуле:

$$R = P \cdot Q,$$

где R – ожидаемая величина риска;

P – вероятность возникновения риска;

Q – угроза.

В зависимости от полученного результата ячейка карты рисков окрашивается в определенный цвет (обычно используются зеленый, желтый и красный). Данный подход позволяет оценивать только каждый риск проекта по отдельности, но не совокупный риск. Для проведения такой оценки используются различные эвристические методы. Например, оценивается время, затрачиваемое на устранение всех рисков, находящихся в красной зоне. Если это время составляет более 20 % от общего времени проекта – статус проекта в красной зоне, если в пределах 10–20 % – в желтой, если менее 10 % – в зеленой зоне [4].

В результате качественного анализа создается более короткий список рисков, определяются критические риски, которые уже будут пропущены через количественный анализ и для которых будут планироваться ответные действия. Кроме того, на стадии качественного анализа принимается решение о судьбе проекта: продолжать проект или закрывать. Также параметры, определенные на этапе качественного анализа (вероятность возникновения риска и ожидаемая величина потерь), являются входными параметрами для количественного анализа.

Для проведения количественного анализа рисков предлагается модель совокупного риска проекта, основанная на методе Монте-Карло, а также метод дерева решений.

Ставится задача нахождения некоторой оценки времени продолжительности работы над проектом (с учетом всех его рисков), то есть необходимо оценить влияние всех рисков проекта на его длительность во времени. Предполагается, что риски никак не взаимодействуют между собой, то есть исключена ситуация, когда один риск влияет на воздействие другого на проект.

Качественные методы управления рисками

Качественные методики управления рисками приняты на вооружение в технологически развитых странах многочисленной армией внутренних и внешних IT-аудиторов. Эти методики достаточно популярны и относительно просты и разработаны, как правило, на основе требований международного стандарта ISO 17799-2002 [5], история развития которого началась в 1993 году, когда Министерство торговли Великобритании опубликовало пособие, посвященное практическим аспектам обеспечения информационной безопасности (ИБ). Пособие оказалось настолько удачным, что его стали использовать администраторы безопасности многих органи-

заций. Позже доработанная версия этого пособия была принята в качестве британского стандарта BS7799 «Практические правила управления информационной безопасностью» (1995). Сегодня это наиболее распространенный стандарт во всем мире среди организаций и предприятий, которые используют подобные стандарты на добровольной основе.

Количественный метод анализа совокупного риска проекта

Опишем случай двух невзаимодействующих рисков. Рассмотрим каждый риск отдельно, полагая, что у проекта существует только данный риск. Положим, что случайная величина X_1 – это длительность проекта в случае возникновения данного риска. Будем считать, что X_1 – случайная величина непрерывного типа, то есть у нее, помимо функции распределения, также существует функция плотности распределения. Зная распределение X_1, можно получить всю необходимую информацию о возможных значениях длительности проекта в случае возникновения только этого риска. В реальных проектах параметры распределения X_1 обычно неизвестны. Более того, в различных проектах они тоже различны (в силу специфики организации работы, опыта разработчиков).

Проблема нахождения вида распределения и его параметров может быть решена, если предположить, что существуют некоторые статистические данные о подобного рода рисках, которые проявили себя во время разработки предыдущих проектов, например: какая была длительность проекта в большинстве случаев из-за этого риска, максимальная длительность, минимальная длительность. Если такие данные есть, то в качестве параметров распределения случайной величины X_1 можно использовать именно эти параметры. Далее будем полагать, что такие параметры известны.

Пусть b, mp, w – минимальная (при отсутствии рисков), наиболее вероятная и максимальная длительности проекта в случае возникновения только этого риска.

Наиболее распространённый подход к моделированию неопределённости основан на использовании теории вероятностей. При этом предполагают, что параметры работ проекта распределены по известному закону. Однако на практике это не всегда так. Часто известен лишь доверительный интервал, в котором могут быть распределены значения параметров и имеются лишь предположения относительно того, к какому классу может принадлежать данный закон распределения. Однако при большом числе работ в проекте индивидуальные законы распределения параметров работ не имеют существенного значения. Это явление выражено в принципе инвариантности.

Принцип инвариантности: в сложных системах показатели, характеризующие поведение системы в целом (макрохарактеристики), являясь функциями большого числа случайных характеристик микроэлементов системы, весьма нежестко зависят от значений последних. Иными словами, распределение макрохарактеристик остается практически неизменным при изменении распределений микрохарактеристик в довольно широких пределах [6].

В системах Управления Проектами (УП), учитывающих фактор неопределённости, часто предполагают, что время выполнения отдельных работ проекта является случайной величиной, распределённой по одному и тому же закону для всех работ, но с разными параметрами. Однако при таком подходе почти всем работам приписывают одинаковую степень неопределённости, что не всегда соответствует реальной ситуации.

При моделировании выполнения проекта в условиях неопределённости для установления продолжительности и стоимости отдельных работ наиболее часто используют перечисленные ниже вероятностные законы распределения (ЗР).

1. β – распределение. Такое распределение предложено использовать при рассмотрении метода PERT без строгого теоретического обоснования, а скорее в качестве иллюстрации. Тем не менее, во многом благодаря авторитету создателей метода, β-распределение получило широкое распространение в практике УП. Статистические исследования подтверждают, что в большинстве случаев параметры работ достаточно хорошо согласуются с β-распределением.

2. Нормальное распределение (распределение Гаусса). Симметричное распределение происходит в случае, когда параметры работ подвержены воздействию большого числа случайных факторов примерно одинаковой степени влияния.

Нормальное распределение часто используют в различных статистических методах, что удобно, если параметры работ определяют на основе статистических данных.

3. Логарифмически нормальное распределение.

При симметричном распределении с острым пиком значения в меньшей степени сосредоточены вокруг математического ожидания, чем при обычном нормальном законе.

4. Равномерное распределение. Все значения в интервале равновероятны. Равномерное распределение часто используют в случаях, когда известны

только границы распределения, а точный закон не известен. Следует помнить, что предположение о равномерности распределения далеко не всегда соответствует действительности и может привести к большим погрешностям при анализе.

В качестве исходного неизвестного распределения, используя принцип инвариантности, предлагается использовать треугольное распределение, основанное на данных трех параметров (рис. 1).

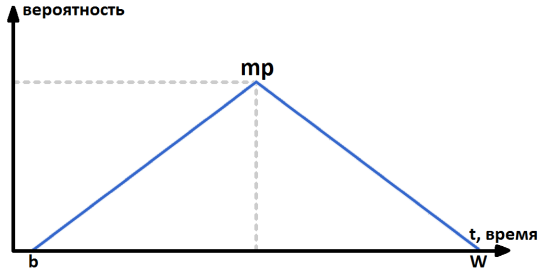

Рис. 1. Треугольное распределение

Треугольное распределение достаточно часто используется в процессе моделирования случайных явлений при отсутствии достаточных данных, позволяющих сформулировать гипотезу об ином распределении. Точное аналитическое выражение для функции плотности треугольного распределения может быть рассчитано на основе трех известных параметров и условия нормирования.

Таким образом, выражение для функции плотности треугольного распределения в терминах введенных ранее параметров b, mp, w имеет вид

$$f(x)=\begin{cases} 0,\ x \ge w \text{ or } x \le b, \\ \dfrac{2(x-b)}{(mp-b)(w-b)},\ b < x \le mp, \\ -\dfrac{2(x-w)}{(w-mp)(w-b)},\ mp < x \le w. \end{cases}$$

Выражение для функции распределения имеет вид

$$F(x)=\begin{cases} 0,\ x \le b, \\ \dfrac{(x-b)^2}{(mp-b)(w-b)},\ b < x \le mp, \\ \dfrac{mp-b}{w-b}+\dfrac{(x-mp)}{(w-mp)(w-b)},\ mp < x \le w, \\ 1,\ x \ge w. \end{cases}$$

Если у проекта только один риск и при этом за основу взята модель, описанная выше, то совокупный риск будет иметь треугольное распределение. Если рисков больше, ситуация совершенно иная.

Для перехода к модели с n рисками следует принять предположение о том, что за каждый риск отвечает определенная группа людей. Таким образом, идет одновременная работа по каждому из рисков. Данное предположение позволяет сделать вывод, что в качестве случайной величины Z, соответствующей суммарной длительности проекта, может быть взята случайная величина, равная $\max(X_1, X_2, \ldots, X_n)$, то есть итоговая длительность проекта будет равна максимальной из длительностей по всем рискам. Таким образом, итоговая задача построения совокупного риска проекта свелась к следующей задаче теории вероятностей.

Пусть $X_1, X_2, \ldots, X_n$ – независимые случайные величины, имеющие плотности распределения f1(x), f2(x), …, fn(x). Необходимо найти функцию распределения и функцию плотности распределения случайной величины $Z = \max(X_1, X_2, \ldots, X_n)$.

Используя определение функции распределения из теории вероятностей, можно легко получить функцию распределения случайной величины Z. Функцией распределения данной величины будет функция

$$F(z)=\prod_{i=1}^{n} F_i(z),$$

где $F_i(z)$ – функция распределения i-го риска (имеет вид, описанный выше). Функция плотности распределения

$$f(z)=\sum_{j=1}^{n}(f_j(z)/F_j(z))\prod_{i=1}^{n} F_i(z),$$

где $f_j(z)$ – функция плотности распределения j-го риска.

График полученной функции распределения назовем диаграммой совокупного риска проекта, по которой можно сделать заключение о готовности проекта к заданной дате (рис. 2).

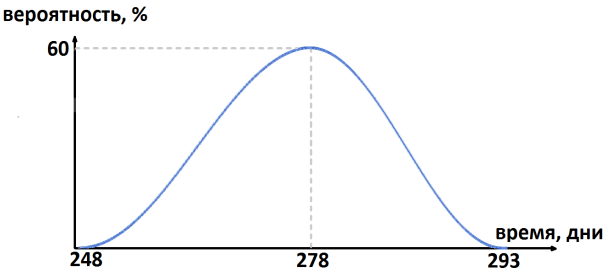

Рис. 2. Диаграмма совокупного риска проекта

Из графика видно, что минимальная длительность рассматриваемого проекта с учетом рисков составляет – 248 часов, наиболее вероятная длительность проекта с учетом рисков составляет – 278

часов, а максимальная длительность проекта с учетом рисков составляет – 293 часа.

Заключение

Таким образом, в данной статье рассмотрен процесс анализа и управления рисками в IT – проектах.

Рассмотрены способы идентификации рисков.

Построена модель количественного анализа рисков с использованием различных методов распределения. Достоинством предложенной модели является точность предсказания длительности проекта при корректной оценке исходных параметров риска, а недостатком – предположение о независимости и одновременности рисков, что не всегда верно.

Предложенная модель может лечь в основу метода управления рисками, что позволит сократить случаи возникновения непредвиденных рисков в проектах разработки и тестирования ПО.

Литература

1. Грей, К. Ф. Управление проектами: практическое руководство [Текст] / К.Ф. Грей, Э.У. Ларсон. – М. : Дело и сервис, 2012. – 579 с.

2. Товс, А. С. Управление проектами: стандарты, методы, опыт [Текст] / А. С. Товс, Г. Л. Ципес. – М. : ЗАО «Олимп-Бизнес», 2003. – 240 с.

3. Орлов, А. И. Менеджмент [Текст] / А. И. Орлов. – М. : Изумруд, 2003. – 298 с.

4. Шарова, Е. С. Управление IT-проектами. [Текст] / Е. С. Шарова – М. : Конференция «СКУПИТ 2006», 2006. – 125 с.

5. Боровкова, В. А. Управление рисками в торговле [Текст] / В. А. Боровкова. – СПб. : Питер, 2004. – 288 с.

6. Борисов, Ю. С. Нейросетевые методы обработки информации и средства их программно-аппаратной поддержки [Текст] / Ю. С. Борисов, В. О. Кашкаров, С. Ю. Сорокин. – СПб. : Питер, 1997. – 215 с.

Поступила в редакцию 05.02.2014, рассмотрена на редколлегии 12.02.2014

Рецензент: д-р техн. наук, проф., зав. каф. инженерии программного обеспечения И. Б. Туркин, Национальный аэрокосмический университет им. Н. Е.Жуковского «Харьковский авиационный институт», Харьков.

ЯКІСНИЙ ТА КІЛЬКІСНИЙ АНАЛІЗ РИЗИКІВ В IT - ПРОЕКТАХ

О. С. Яшина, А. О. Бережна

Розглянуто питання аналізу та управління ризиками проектів при розробці програмних продуктів. Систематизовано термінологічний апарат і розкрито основоположні підходи до аналізу та управління ризиками. Пропонується підхід до якісної та кількісної оцінок сукупного ризику проекту, який засновано на впровадженні існуючих підходів до управління ризиками. Отримані дані можуть служити основою для регламентування дій ризик - менеджерів і дозволяють прогнозувати найбільш вірогідні терміни завершення проекту з урахуванням сукупності всіх ризиків проекту.

Ключові слова: управління ризиками, ризик, програмний проект, невизначеність, інформаційні технології.

QUALITATIVE AND QUANTITATIVE ANALYSIS RISKS IN IT - PROJECTS

O. S. Yashina, A. O. Berezhna

The problems of analysis and risk management projects with software development. Systematized and terminological apparatus disclosed fundamental approaches to the analysis and risk management. An approach to the quantitative and qualitative assessment of the overall risk of the project, based on implementation of existing approaches to risk management. The data obtained can serve as a basis for regulatory action risk - and allow managers to predict the most likely time frame for completion of the project taking into account the totality of the project risks.

Key words: risk management, risk, software project uncertainty, information technology.

Яшина Елена Сергеевна – канд. техн. наук, доцент, доцент каф. информационных управляющих систем, Национальный аэрокосмический университет им. Н. Е. Жуковского «Харьковский авиационный институт», Харьков, Украина.

Бережная Алина Александровна – магистрант каф. информационных управляющих систем, Национальный аэрокосмический университет им. Н. Е. Жуковского «Харьковский авиационный институт», Харьков, Украина, e-mail: allieberezhnaya@gmail.com.