УДК 681.518

И.В. Груздо

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

ПОВЫШЕНИЕ КАЧЕСТВА ПРОГРАММНОГО ПРОЕКТА ЗА СЧЕТ УПРАВЛЕНИЯ РИСКАМИ

Статья посвящена проблемам применения стандартных методик и технологий анализа рисков для оценки качества выполнения программных проектов.

Ключевые слова: *программный проект, управление рисками.*

Введение

Актуальной проблемой при разработке программных проектов является эффективное управление проектом и повышение качества разрабатываемого программного продукта за счет применения специальных методов планирования, уменьшения рисков и оценивания трудоемкости программных проектов.

Основным фактором эффективного управления в настоящее время считается способность гибко изменять методы планирования, что не всегда приводит к уменьшению рисков в программном проекте, а, наоборот, к возникновению новых, в результате чего и снижается качество самого программного продукта.

Решение проектных задач управления в условиях неопределенности порождает риски выхода из бюджета и расписания, что ставит под угрозу достижимость целей проекта, поэтому, процессы управления рисками являются наиболее важной компонентой процессов принятия решений и управления проектами, позволяют максимизировать положительные и минимизировать отрицательные последствия наступления рисковых событий [1].

Проблемам моделирования, проектирования, повышения качества программных средств посвящено достаточно много научных работ. Среди них можно выделить наиболее известные работы отечественных и зарубежных ученых: В.В. Липаева, А.М. Вендерова, Г.Н. Калянова С.А. Орлова, Е.З. Зиндера, Д.Л. Шумейко, В. Михеева, G. Booch, E. Yourdon, I Jacobson, D.Longstreet, B. Boem, R. Ganter, K.Clark, Jongmoon Baik, и др.

Таким образом, **целью статьи** является изложение подходов управления рисками, для повышения качества программного проекта.

Понятие качества программного проекта

В связи с выходом Украины на международный рынок программных проектов, где традиционно существует жесткая конкуренция на рынке, первоочередная задача, которую приходится решать разработчикам, состоит в повышении качества разрабатываемого программного продукта.

Практика разработки современных информационных средств, показала самыми критичными этапами реализации подобных проектов, являются те этапы в которых недостаточное качество программы, ошибки данных могут стать причиной нанесения ущерба, что вызывает серьезные последствия при этом положительный эффект от их использования сводится к нулю.

В то же время многие программные продукты не способны выполнять требуемые функциональные задачи, поскольку заказчик изначально не всегда может четко определить требуемые значения показателей качества, что приводит к возникновению конфликтов между разработчиком и заказчиком. Это происходит в связи с разным пониманием (трактовкой) одного и того же показателя определяющего качество.

На протяжении последних лет было создано много международных стандартов, которые регламентируют процессы и продукты жизненного цикла программных средств. Среди них наиболее распространены:

– ISO/IEC 12207(ISO – International Organization of Standardization – Международная организация по стандартизации, IEC – International Electrotechnical Commission – Международная комиссия по электротехнике) – он предназначен для определения структуры жизненного цикла, содержит процессы, действия, и задачи, которые должны быть выполнены во время создания программного обеспечения [2, 3];

– ISO 9126:1991(ГОСТ Р ИСО/МЭК 1926-93) – «Информационная технология. Оценка программного продукта. Характеристика качества и руководство по их применению» [4];

– ГОСТ Р ИСО МЭК ТО 12182-2002 – Классификация программных средств;

– ГОСТ 28195-99 – Оценка качества программных средств. Общие положения [5];

– ISO 9001:2000 – Система менеджмента (административного управления) качества. Требования.

Дополнение к нему является стандарт ISO 90003:2004 – Руководство по организации применения стандарта ISO 9001:2000 для программных средств [5 – 8];

– ISO 15288:2002 – Системная инженерия. Процессы жизненного цикла системы [2];

– ISO 15504:1-9:1998 – Оценка и аттестация зрелости процессов жизненного цикла программных средств [2, 5];

– IEEE 610.12-1990 – Стандартный глоссарий терминологии разработки программного обеспечения Института Инженеров электрической аппаратуры;

– ANSI PMI PMBOK 2004 – Основные участники проекта (Руководитель, спонсор и заказчик проекта). Заинтересованные стороны в проекте (Project Stakeholders) и отношения между ними. Баланс интересов сторон. Исполнение проектов в различных организационных структурах компаний;

– AS/NZS4360:2004 – оценка риска. Стандарт, касающийся оценки риска [3];

– HB436:2004 – указания по оценке риска [3].

В перечисленных выше стандартах определение качества дается в различных аспектах, в следствие чего отсутствует единое определение качества. Кроме того, существует много подходов к обеспечению качества.

В соответствии со стандартом ISO [9] качество – это полнота свойств и характеристик продукта, процесса или услуги, которые обеспечивают способность удовлетворять заявленным или подразумеваемым потребностям.

Вместе с тем, по стандарту IEEE [9] качество программного обеспечения - это степень, в которой оно обладает требуемой комбинацией свойств.

Одними из первых моделей качества стали стандарты. По ним модель характеристик качества включает несколько видов атрибутов [10]:

- внутренние атрибуты качества (требования к качеству кода и внутренней архитектуре);
- внешние атрибуты качества (требования к функциональным возможностям и т.д.);
- атрибуты «качества в использовании» (данные атрибуты качества относятся не только к ПС, а ко всей информационной системе, они характеризуют эффект для пользователя от использования ПС в разных контекстах использования).

Исходя из вышесказанного на рис. 1, приведена модель характеристик качества в аспекте жизненного цикла программных проектов.

Рисунок 2 показывает различные подходы к качеству программ использованием метрик определенных стандартами средств. При этом в процессе верификации происходит преобразование требований пользователя к качеству в требования к внешнему качеству, а затем в требования к внутреннему качеству. Процессы реализации требований к внутреннему качеству должны обеспечивать внешнее качество, а последнее — воплощаться в качество для пользователей.

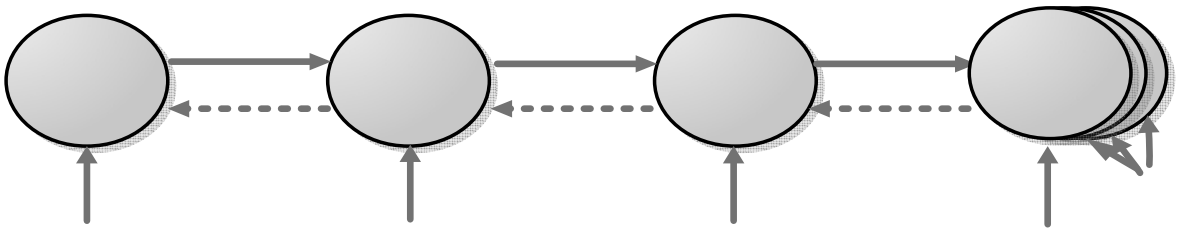

Рис. 1. Качество в жизненном цикле программных проектов [10]

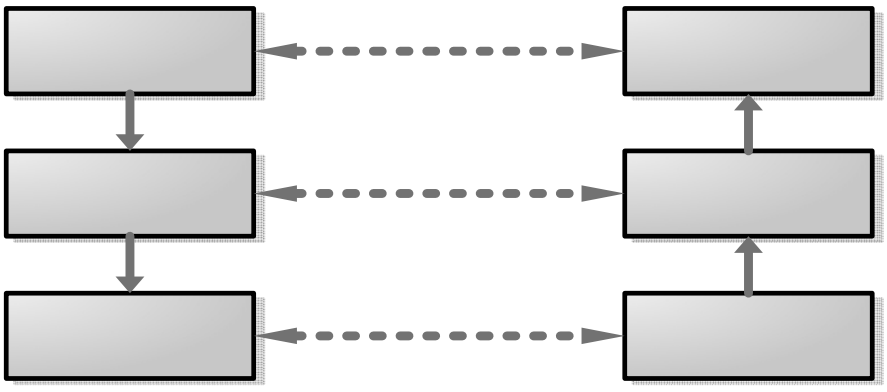

Рис. 2. Различные подходы к качеству ПП и соответствующим метрикам качества

Риски программных проектов: определение и классификация

Риск проекта (project risk) – всякое событие или условие, которое может оказать позитивное либо негативное влияние на итоги проекта [12].

Риск – возможность возникновения некоторой угрозы, связанной с текущей деятельностью компании. Также риск – это комбинация вероятности события и его последствий (ISO/IEC 27001:2005). Риск отражает возможные прямые или косвенные финансовые потери.

Разновидностью риска является информационный риск как возможность наступления случайного события, приводящего к нарушению функционирования и снижению качества информации в информационной системе предприятия, а так же к неправильному использованию или распространению информации во внешней среде, в результате которых наносится ущерб предприятию [11].

Риск имеет три основных атрибута: случай, вероятность и воздействие [13].

Случай. Необходимо определять, в каких ситуациях может возникнуть риск. Чтобы оценить вероятность возникновения риска, необходимо понять его природу.

Вероятность возникновения риска. Обычно, вероятность измеряется в количественных показателях. Однако, в рамках управления проектами, вероятность возникновения риска может быть оценена как в количественных, так и в качественных показателях. Как правило, в управлении рисками ведется вероятностная оценка события в пределах от 0 – 100%.

Воздействие риска. Воздействие – измерение того, насколько тяжелы будут последствия, в случае, если риск произойдет. Для облегчения анализа управления рисками, принято воздействие риска рассматривать с позиции влияния риска на стоимость, качество и продолжительность выполнения работ.

К примеру, риск потери высококвалифицированного программиста в проекте по разработке программного обеспечения, затрагивает проект с позиции стоимости, качества и продолжительности работ.

Произведение вероятности и воздействия определяет важность риска – его ценность – показатель, который может использоваться в процессе принятия решения и как проектный механизм контроля. Важность риска – полезный проектный индикатор, активно используемый в управлении проектами.

В соответствии с подходом, изложенным в работе [14] риски делятся на:

– “Известные ”– те, которые определены, оценены, для которых возможно планирование;

– “Неизвестные” – те, которые не идентифицированы и не могут быть спрогнозированы.

Хотя специфические риски и условия их возникновения не определены, менеджеры проекта знают, исходя из прошлого опыта, что большую часть рисков можно предвидеть.

Кроме того, в соответствии с [14] выделены три основные группы рисков:

- риск проектирования;
- технический риск;
- бизнес-риск (деловой риск).

Классификационным способом для рисков может служить так же последствия наступления риска. В связи с этим риски подразделяются на три категории [15]:

– допустимый риск – это риск решения, в результате неосуществления которого предприятию грозит потеря прибыли; в пределах этой зоны предпринимательская деятельность сохраняет свою экономическую целесообразность, т.е. потери имеют место, но они не превышают размер ожидаемой прибыли;

– критический риск – это риск, при котором предприятию грозит потеря выручки; иначе говоря, зона критического риска характеризуется опасностью потерь, которые заведомо превышают ожидаемую прибыль и в крайнем случае могут привести к потере всех средств, вложенных предприятием в проект;

– катастрофический риск – риск, при котором возникает неплатежеспособность предприятия; потери могут достигнуть величины, равной имущественному состоянию предприятия. Также к этой группе относят любой риск, связанный с прямой опасностью для жизни людей или возникновением экологических катастроф.

Существует множество классификаций общих рисков проектов по разработке программного обеспечения. Хорошо известны и часто используются Barry Boehm, Caper Jones, и SEI Software Risk Taxonomy, описывающие источники таких рисков.

С учетом особенностей, присущих процессам разработки и реализации, целесообразно использовать комплексный подход к классификации рисков в программных проектах, который дает возможность наиболее точно определить перечень угроз и последствий их возникновения.

Проблема идентификации рисков программных проектов

Риски отличаются от проблем и трудностей, так как они имеют отношение к будущим, потенциально возможным негативным результатам и убыткам. Проблемы же и трудности представляют собой нечто, имеющее место в настоящее время. Риски могут стать проблемами, если ими эффективно не управлять. В рамках MSF(Microsoft Solutions Framework) управление рисками рассматривается как процесс их выявления, анализа и эффективной превентивной работы над ними. Эффективный процесс выявления и управления рисками помогает достичь разумных компромиссов между упомянутыми опасностями и открывающимися возможностями.

Проекты в области информационных технологий (IT) обладают специфическими характеристиками, в силу которых эффективное управление рисками становится жизненно важным для их успеха.

Рыночная конкуренция, эволюция технических стандартов, равно как и другие факторы, могут заставить работающую над проектом группу модифицировать принятые планы и решения в середине проекта. Изменяющиеся требования пользователей, новый инструментарий и новые технологии, растущие угрозы для информационной безопасности, текучесть кадров – все это дополнительные факторы, способные повлечь за собой изменения в IT-проекте и заставить проектную группу принимать решения в условиях неопределенности (риска) [16].

Целью фазы выявления рисков является создание проектной группой списка имеющихся рисков проекта. Этот список должен в максимально-возможной степени охватывать все факторы, влияющие на проект [17].

Исходными данными фазы выявления рисков являются имеющиеся знания как об общих, так и о специфических для данного проекта рисках, связанных с бизнесом, технологиями, организациями и внешними условиями. Дополнительные факторы, которым должно быть уделено внимание: имеющийся у команды опыт, применяемые внутри организации подходы к рискам, выраженные в виде правил и инструкций, а также вся информация о проекте, известная на данный момент, включая его историю и текущее положение дел.

В процессе выявления рисков проектная группа старается четко сформулировать и перечислить все имеющиеся в проекте риски. На начальной стадии проекта может быть организован семинар или мозговой штурм с целью выявления рисков, возникающих в новых условиях. Как минимум, в результате процесса выявления рисков должны быть получены их четкие, однозначные и согласованные формулировки, представленные в виде списка рисков [17].

Эффективное управление рисками не может быть сведено к простому реагированию на возникающие проблемы. Проектная группа должна работать над заблаговременным выявлением рисков и создавать стратегии и планы по управлению ими. Должны быть разработаны планы по решению проблем в случае их возникновения. Предвосхищение потенциальных проблем и заблаговременная подготовка четко составленных планов по борьбе с ними сокращает временные затраты в критических ситуациях. Такая деятельность способна ограничить негативный эффект, создаваемый этими проблемами, и даже помочь извлечь из них некоторую пользу.

Определяющими характеристиками превентивного управления рисками являются профилактика рисков (risk mitigation) и сокращение их негативного воздействия. Профилактика может проводиться по отношению к одному специфическому риску и иметь своей целью воздействие на его непосредственную причину. Но она может также относиться к исходной первопричине риска, равно как и к любому звену цепи причинно-следственных связей, порождающей риск. Лучшее время для профилактических мер – ранние этапы работы над проектом, когда проектная группа все еще может оказать своевременное влияние на его результат.

Для предприятия особенно важны обнаружение и ликвидация первопричин рисков, так как соответствующие корректирующие шаги могут дать весьма ощутимый позитивный эффект, выходящий за пределы одного отдельно взятого проекта.

Обоснование выбора метода управления рисками программного проекта

Методика управления рисками подразумевает несколько способов действий.

Риск может быть:

– принят (assumption), т.е. пользователь согласен на риск и связанные с ним потери, поэтому работа информационной системы продолжается в обычном режиме;

– снижен (mitigation) – с целью уменьшения величины риска будут приняты определенные меры;

– передан (transference) – компенсацию потенциального ущерба возложат на страховую компанию, либо риск трансформируют в другой риск - с более низким значением – путем внедрения специальных механизмов.

Некоторые методики дополнительно предусматривают еще один способ управления – "упразднение" (avoidance). Он подразумевает принятие мер по ликвидации источника риска. При низких значениях риска данный метод трансформируется в метод снижения риска (mitigation).

В настоящее время существует много общепринятых методов управления рисками. Большинство из них, безусловно, эффективны в применении, но требует специальных разработок и материальных затрат, которые могут покрыть выгоды от применения. Поэтому необходимо четко представлять, что ожидается от управления рисками и как данная технология вписывается в процесс управления рисками.

Механизм управления рисками проекта – совокупность состояний и процессов, из которых складывается управление рисками, и основными составляющими которого являются: система управления рисками, цель и задачи управления рисками, принципы управления рисками, функции управления рисками, методы управления рисками, культура и стиль управления рисками

Применение специальных методов управления рисками позволяет решить основные задачи выявления возможных негативных ситуаций, оценки вероятности их наступления и величины последствий от их проявления. Однако существование большого количества различных методов управления рисками усложняет выполнение поставленных задач.

Наряду с существованием методов, реализованных в виде специального программного обеспечения, в настоящее время существует ряд простых методов управления рисками. Они представлены в табл. 1.

Таблица 1

Классификация методов управления рисками

Группа	Метод	Краткое описание
Методы получения информации	Оценка рисков независимыми экспертами	Методы интервьюирования и/или анкетирования опытных специалистов по управлению рисками, которые выступают в роли экспертов и не являются участниками реализации оцениваемых ИСП.
Методы прогнозирования	Имитационное моделирование	Моделирование и анализ неопределённости в оценках основных показателей проекта (денежные и временные затраты).
Творческие методы	"Мозговая атака"	Дискуссии, на которых специалистами по управлению рисками с использованием методических пособий обсуждаются все аспекты данного механизма, и осуществляются планирование, идентификация рисков, оценка рисков, обработка рисков, контроль и документирование.
Методы анализа	Контрольные списки источников рисков	Структурированные списки источников рисков, в основе которых лежит историческая информация об инцидентах, произошедших при реализации предыдущих ИСП.
Методы оценки	Калькуляция вероятных потерь	Методы, основанные на расчёте математического ожидания убытка для каждого риска в отдельности и по проекту в целом.

В настоящее время на практике широко используется достаточно много методов оценки и управления рисками программных проектов. Одним из таких методов является OCTAVE, разработанный в университете Карнеги-Мелон для внутреннего применения в организации. OCTAVE – Оценка критичных угроз, активов и уязвимостей (Operationally Critical Threat, Asset, and Vulnerability Evaluation) имеет ряд модификаций, рассчитанных на организации разного размера и области деятельности. Сущность этого метода заключается в том, что для оценки рисков используется последовательность соответствующим образом организованных внутренних семинаров (workshops). Оценка рисков осуществляется в три этапа, которым предшествует набор подготовительных мероприятий, включающих в себя согласования графика семинаров, назначения ролей, планирование, координация действий участников проектной группы [18].

Метод оценки рисков CRAMM (the UK Goverment Risk Analysis and Managment Method) разработан, по заказу британского правительства. В CRAMM основной способ оценки рисков – это тщательно спланированные интервью, в которых используются подробнейшие опросники. CRAMM используется в тысячах организаций по всему миру.

В отличие от метода OCTAVE, в CRAMM используется несколько иная последовательность действий и методы определения величины рисков. Сначала определяется целесообразность оценки рисков вообще и если информационная система организации недостаточно критична, то к ней применятся стандартный набор механизмов контроля описанный в международных стандартах и содержащихся в базе знаний CRAMM [18].

На основе требований ISO 17999 к качественным методикам управления рисками относятся методики COBRA (Consultative Objective and Bi-Functional Risk Analysis) и RA Software Tool.

Во второй половине 90х годов компания C & A Systems Security Ltd. разработала одноименные методику и соответствующий инструментарий для анализа и управления информационными рисками под названием COBRA. Эта методика позволяет выполнить в автоматизированном режиме простейший вариант оценивания информационных рисков любой компании. Для этого предлагается использовать специальные электронные базы знаний и процедуры логического вывода, ориентированные на требования ISO 17799. Существенно, что при желании перечень учитываемых требований можно дополнить различными требованиями отечественных нормативно-регулирующих органов, например, требованиями руководящих документов [19].

Методика COBRA представляет требования стандарта ISO 17799 в виде тематических вопросников (check list's), на которые следует ответить в ходе оценки рисков информационных активов и электронных бизнестранзакций компании. Далее введенные ответы автоматически обрабатываются, и с помощью соответствующих правил логического вывода формируется итоговый отчет с текущими оценками информационных рисков компании и рекомендациями по их управлению [19].

Методика и одноименное инструментальное средство RA Software Tool основаны на требованиях международных стандартов ISO 17999 и ISO 13335 (части 3 и 4), а также на требованиях некоторых руководств Британского национального института стандартов (BSI), например, PD 3002 (Руководство по оценке и управлению рисками), PD 3003 (Оценка готовности компании к аудиту в соответствии с BS 7799), PD 3005 (Руководство по выбору системы защиты) и пр. Эта методика позволяет выполнять оценку информационных рисков (модули 4 и 5) в соответствии с требованиями ISO 17799, а при желании в соответствии с более детальными спецификациями руководства PD 3002 Британского института стандартов [19].

Приведенные выше соображения позволяют утверждать, что метод CRAMM наиболее пригоден для управления рисками в программных проектах. Однако при использовании данного метода требуется: специальная подготовка и высокая квалификация аудитора; метод CRAMM больше подходит для аудита уже существующих ИС (информационных систем), находящихся на стадии эксплуатации, нежели для ИС, находящихся на стадии разработки; аудит по методу CRAMM - процесс достаточно трудоемкий и может потребовать несколько месяцев непрерывной работы аудитора.

Выводы

1. На данном этапе актуальной является проблема стандартизации качества и рисков в программной инженерии, поскольку определение качества программных проектов, содержащиеся в большинстве стандартов, не гармонизировано.

2. Качество программного проекта – это комплексное понятие, которое включает в себя внутренние атрибуты качества, внешние атрибуты качества, атрибуты «качества в использовании», что влечет за собой необходимость комплексного использования методик.

3. При решении задач идентификации рисков программных проектов основной фазой является фаза профилактики рисков и, следовательно, сокращение их негативного воздействия.

4. Для классификации методов управления рисками рациональной является классификация, основанная на группировке методов.

Список литературы

1. Гордиевский М.Д. Управление рисками в высокотехнологичных проектах: состояние и подходы управления / М.Д. Гордиевский, А.А. Поляков // Методи та засоби програмної інженерії. – 2008. – 1. – С. 311-319.

2. Международные стандарты ИСО серии 9000 и 10000 на системы качества: версии 1994 г. – М.: Изд-во стандартов, 1995. – 120 с.

3. Общая информация управления риском. – [Электронный ресурс]. – Режим доступа к документу: http://www.rmanage.ru:80. – Заголовок с экрана.

4. Липаев В. Оценка качества программных средств / В. Липаев // ИСП РАН "Сетевой журнал". – 2002. – № 3. – С. 37-41.

5. Оценка факторов, влияющих на качество программных продуктов // LAN. – 2007. – 10. – С. 67-71.

6. Терехов А.А. Современные модели качества программного обеспечения / А.А.Терехов, В. Туньон // Россия. – 1999. – № 12. – С. 12-14.

7. Стандартам серии ISO 9000. – [Электронный ресурс]. – Режим доступа к документу: http://www.iso9000.ru/. – Заголовок с экрана.

8. Панкратов С. Основы качества программного обеспечения (Software Quality Fundamentals) / С. Панкратов. – Май 2007. – [Электронный ресурс]. – Режим доступа к статье: http://it4business.ru:80/lib/74/print/. – Заголовок с экрана.

9. Карпенко С.Н. Метрики качества программного проекта / С.Н. Карпенко. – Нижний Новгород, 2003. – 240 с.

10. Полаженко С. Оценка характеристик безопасности в рамках процесса оценки качества программных средств в соответствии с международными стандартами ISO/IEC / С. Полаженко. – [Электронный ресурс]. – Режим доступа к статье: http://www.securitylab.ru/. – Заголовок с экрана.

11. Парадигмы управления рисками. – [Электронный ресурс]. – Режим доступа к документу: www.fa-kit.ru. – Заголовок с экрана.

12. Грекул В.И. Управление внедрением информационных систем / В.И. Грекул // Бизнес-информатика. – Нижний Новгород, 2006. – 152 с.

13. Адамова Н. Принятие проектных решений через управление рисками / Н. Адамова. – [Электронный ресурс]. – Режим доступа к статье: www.projectmanagement.ru. – Заголовок с экрана.

14. Симонов С. Методология и технология анализа рисков / С. Симонов. – [Электронный ресурс]. –- Режим доступа к документу: http://www.usp-compulink.ru. – Заголовок с экрана.

15. Стенли Соммерсби. Классификация рисков: принципы и критерии / Стенли Соммерсби. – 7.2007. – [Электронный ресурс]. – Режим доступа к документу: http://www.djoen.ru/. – Заголовок с экрана.

16. Microsoft Solutions Framework: Основное руководство. – Нижний Новгород, 2006. – 268 с.

17. Технологии программирования. – Нижний Новгород, 2006. – 240 с.

18. Астахов А. Как управлять рисками информационной безопасности? / А. Астахов // CISA. – ноябрь 2006. – С. 121-124.

19. Петренко С. Методики и технологии управления информационными рисками / С. Петренко, С. Симонов // &laquoIT Manager. – 2003. – № 3. – С. 57-61.

Поступила в редколлегию 19.12.2008

Рецензент: д-р техн. наук, проф. В.П. Авраменко, Харьковский национальный университет радиоэлектроники, Харьков.

ПІДВИЩЕННЯ ЯКОСТІ ПРОГРАМНОГО ПРОЕКТУ ЗА РАХУНОК УПРАВЛІННЯ РИЗИКАМИ

І.В. Груздо

Стаття присвячена проблемам застосування стандартних методів і технологій аналізу ризиків для оцінки якості виконання програмних проектів.

Ключові слова: *програмний проект, управління ризиками.*

UPGRADING PROGRAMMATIC PROJECT DUE TO A MANAGEMENT RISKS

I.V. Gruzdo

This article is devoted to the problems of using some standard methods and technologies of risks analysis to estimate the quality of programming projects.

Keywords: *programmatic project, management risks.*