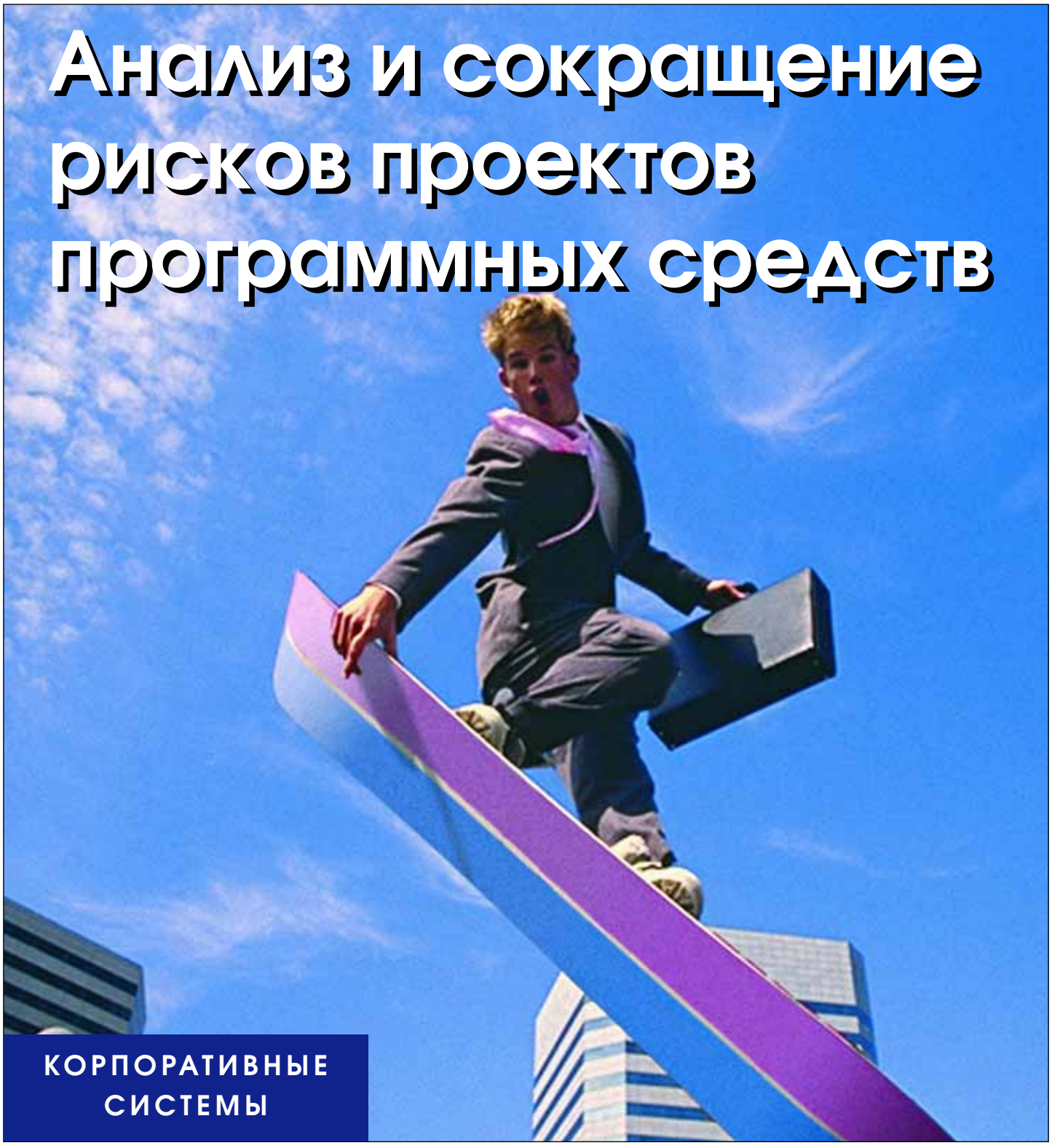
Jet Info

ИНФОРМАЦИОННЫЙ БЮЛЛЕТЕНЬ № 1 (140)/2005

Анализ и сокращение рисков проектов программных средств



КОРПОРАТИВНЫЕ СИСТЕМЫ

Анализ и сокращение рисков проектов программных средств

В.В. Липаев, профессор, доктор технических наук

СОДЕРЖАНИЕ

Введение

Оценки качества в жизненном цикле программных средств (ПС) могут проводиться с **двух позиций**: с **позиции положительной** эффективности использования и непосредственной адекватности их характеристик назначению, целям создания и применения, а также с **негативной позиции** возможного при этом ущерба — риска от использования и реализации жизненного цикла ПС или системы. В жизненном цикле ПС не всегда удается достигнуть требуемого положительного эффекта и может проявляться некоторый ущерб — риск в создаваемых системах, программных продуктах и их характеристиках. **Характеристики качества и риски объектов и процессов обычно тесно связаны**, на них влияют подобные факторы, которые с разных сторон отражаются в свойствах систем или комплексов программ. Характеристики качества преимущественно отражают особенности и положительный эффект от применения системы или ПС, и основная задача проекта состоит в обеспечении его высоких значений качества. Риски характеризуют возможные негативные последствия или ущерб при функционировании ПС и системы, и задача разработчиков сводится к сокращению и ликвидации рисков. Повышению качества проекта обычно сопутствует снижение его рисков и наоборот, сокращение рисков способствует улучшению характеристик качества. Поэтому методы и системы управления качеством в жизненном цикле ПС близки к методам анализа и сокращения рисков проектов комплексов про-

грамм, они должны их дополнять и совместно способствовать совершенствованию программных продуктов и систем на их основе.

К **понятию риски** относятся негативные события и их величины, отражающие потери, убытки или ущерб от процессов или продуктов, вызванные дефектами при проектировании требований, недостатками обоснования проектов ПС, а также при последующих этапах разработки, реализации и всего жизненного цикла комплексов программ. Риски проявляются, как **негативные последствия функционирования или нарушение безопасности применения ПС**, в результате **отклонения характеристик объектов или процессов** от заданных требований заказчика (согласованных с разработчиками), которые способны вызвать ущерб системе, внешней среде или пользователю.

Проблема исследования и сокращения рисков функционирования ПС и систем в процессе разработки и жизненного цикла возникла и развивается вследствие возрастания разнообразия, сложности и ответственности задач их использования. Причинами возникновения и проявления рисков могут быть: **злоумышленные, активные воздействия заинтересованных лиц** или **случайные негативные проявления дефектов** внешней среды, системы, действий разработчиков или пользователей. В первом случае риски могут быть обусловлены искажениями программ и информационных ресурсов и их уязвимостью от предумышленных, внешних воздействий (атак) с целью незаконного использования или изменения информации и программ, которые по своему содержанию предназначены для применения ограниченным кругом лиц. При этом подразумевается наличие лиц, заинтересованных в доступе к конфиденциальной или полезной информации в системах, с целью ее использования или разрушения, способных привести к значительному или катастрофическому ухудшению требуемых характеристик функционирования системы. Для решения этой проблемы созданы и активно развиваются методы, средства и стандарты обеспечения информационной безопасности и защиты программ и данных от предумышленных негативных внешних воздействий. Факторы безопасности и риски, характерные для сложных информационных систем — целостность, доступность и конфиденциальность информационных ресурсов, а также ряд типовых процедур систем защиты — криптографическая поддержка, идентификация и аутентификация, обеспечение защиты и сохранности данных пользователей при предумышленных атаках из внешней среды, **далее не рассматриваются.**

Риски при случайных, негативных воздействиях дефектов и отсутствии злоумышленного влияния на системы, ПС или информацию баз данных существенно отличаются от предшествующих задач. Эти риски объектов и систем зависят от отказовых ситуаций, отражающихся на работоспособности и безопасности реализации их основных функций, причинами которых могут быть дефекты и аномалии в аппаратуре, программах, данных или вычислительных процессах. При этом существенно искажается процесс функционирования систем, что может наносить значительный ущерб при их применении. Основными источниками отказовых ситуаций могут быть некорректные исходные требования при проектировании, сбои и отказы в аппаратуре, дефекты или ошибки в программах и данных функциональных задач, проявляющиеся при их исполнении в соответствии с назначением. В реальных сложных системах возможны катастрофические последствия и отказы функционирования с большим ущербом, при отсутствии воздействия от лиц, заинтересованных в нарушениях работоспособности систем и ПС. Вредные последствия таких отказов в ряде областей применения систем могут превышать по результатам, последствия злоумышленных воздействий, имеют свою природу, особенности и характеристики. Поэтому они требуют самостоятельного изучения и адекватных методов и средств сокращения рисков, которые рассматриваются ниже.

Проблемы анализа и оценки рисков ПС могут рассматриваться с **промышленной и практической точек зрения**. Промышленная позиция подразумевает, что управление рисками ПС является инженерной дисциплиной, комплексы программ всегда содержат риски, которые априори невозможно достоверно предсказать и контролировать, но они иногда катастрофически отражаются на качестве функционирования систем или внешней среды. Практическая точка зрения предполагает, что: существует недостаточное понимание заказчиками, разработчиками и пользователями значения и **необходимости анализа и сокращения рисков** в жизненном цикле сложных ПС, недостаточно используются технологические дисциплины и инструментальные средства для управления и уменьшения рисков при создании и применении ПС.

Деловой или присущий проекту ПС риск состоит в проявлении ущерба в связи с деловой деятельностью при его реализации и применении. Примерами подобных потерь служат непо-

средственная утрата или катастрофическое искажение системы и материального имущества, значительные потери последствий деятельности отдельного лица или коллектива, персональный ущерб для человека или появление юридической ответственности за негативные результаты проекта. Непосредственный ущерб имуществу включает потери от дефектов, аварий и хищения ценностей, затраты на его страхование. **Юридическая ответственность** предполагает защиту от неправомерных правовых действий в случае возникновения дефектов в ходе проектирования, разработки или при нарушениях технологии выполнения проекта.

Рассматриваемые риски могут быть обусловлены нарушениями технологий или ограничений при использовании ресурсов, выделенных на разработку ПС. Результирующий ущерб в совокупности зависит от величины и вероятности проявления каждого негативного последствия. Этот ущерб – риск характеризуется **разнообразными метриками**, зависящими от их специфики и объектов анализа, и в некоторых случаях может измеряться прямыми материальными, информационными, функциональными потерями применяемых ПС или систем. Одним из косвенных методов определения величины риска может быть **оценка совокупных затрат**, необходимых для ликвидации негативных последствий, проявившихся в результате конкретного рискового события в ПС, системе или внешней среде. Более точные и сложные методы оценивания величины ущерба при проявлении рисковых событий базируются на статистических исследованиях вероятностей угроз проявления рисков, оценках при этом уязвимости объектов и величин возможной совокупности отрицательных последствий для применения конкретных ПС и систем.

В жизненном цикле программных средств при исследовании выделены **три крупных класса ущерба – рисков**:

- искажения или не полная реализация требуемого назначения, функций или взаимодействия ПС с компонентами системы или внешней среды – недостатки и дефекты **функциональной пригодности**;
- недостаточные и не соответствующие требованиям, реализации **конструктивных характеристик** качества ПС при его функционировании и применении по прямому назначению;
- нарушения ограничений на использование **экономических, временных или технических ресурсов** при создании и применении ПС.

Анализ и оценка рисков ПС должны начинаться с исследования понятий, требований и функций, **способствующих одобрению и эффективному применению** конкретного программного продукта. При этом должны быть определены требования к характеристикам ПС и оценки влияния возможного ущерба при их нарушении. Исследования процессов разработки проектов ПС показали, что во многих случаях стоимость и длительность их реализации значительно превышали предполагаемые, а характеристики качества не соответствовали требуемым, что наносило ущерб заказчикам, пользователям и разработчикам. Эти потери – ущерб проектов могли бы быть значительно уменьшены своевременным анализом, прогнозированием и сокращением рисков возможного нарушения требований контрактов, технических заданий и спецификаций на характеристики, выделяемые ресурсы и технологию создания конкретных комплексов программ.

Управления рисками предполагает необходимость ясного понимания внутренних и внешних причин, влияющих на качество проекта ПС, которые могут привести к его провалу или большому ущербу. В результате анализа следует создавать план измерения и отслеживания изменения рисков в жизненном цикле ПС, который должен регулярно просматриваться и корректироваться. Главной целью управления рисками является обнаружение, идентификация и контроль за редко встречающимися ситуациями и факторами, которые приводят к негативным – рисковым результатам проекта. Это должно отражаться на применении регламентированных процессов, в которых факторы и угрозы рисков систематически идентифицируются, оцениваются и сокращаются.

Для снижения возможного ущерба – рисков применяются **анализ, оценка и мониторинг рисков,** а также **различные контрмеры**. Контрмеры могут устранять первичные **причины – угрозы**, вызвавшие появление итоговых регистрируемых рисков, или уменьшать **уязвимость** в некоторых критических ситуациях реализации или применения компонентов ПС, систем или внешней среды и предотвращать проявление рисков. В некоторых ситуациях контрмеры могут воздействовать непосредственно на **результаты проявления рисков** без устранения их первичных причин. Уменьшение рисков должно производиться путем максимального приближения проекта к требованиям заказчика и к ограничениям выделенных ресурсов или путем снижения этих требований и увеличения заказчи-

ком ресурсов на проект ПС. В проектах крупных систем, использующих комплексы программ, риски могут быть обусловлены дефектами функциональных характеристик самих ПС, компонентов и их жизненного цикла, а также недостатками систем и внешней среды, в которой они используются. Основной ущерб от рисков ПС проявляется в последствиях их применения — **в дефектах и недостатках функционирования систем и внешней среды**. Поэтому анализ рисков ПС должен быть тесно связан с исследованием возможности их проявления в системах, где они используются.

Риски ПС могут проявляться в процессах проектирования, разработки и сопровождения при изменении и развитии комплексов программ и при применении готового программного продукта по прямому назначению. Это приводит к необходимости анализа рисков ПС в различных условиях, различающихся: источниками и причинами угроз появления рисков; вероятностью проявления и величиной последствий рисков; возможными контрмерами для сокращения рисков. Оценка и измерение рисков во многих случаях характеризуется значительной неопределенностью и применением качественных метрик. При анализе и управлении рисками рекомендуется выделять наиболее характерные этапы ЖЦ ПС: обоснование концепции проекта ПС; разработку требований спецификаций; проектирование; кодирование; тестирование; документирование и сопровождение.

Последующее изложение ориентировано на коллективную, групповую работу «команд» специалистов над **средними и крупными программными проектами**. Для гарантирования высокого качества и допустимых рисков комплексов программ целесообразно выделять специалистов — экспертов, ответственных за соблюдение промышленной технологии создания и совершенствования программ, за измерение и контроль характеристик качества и за сокращение рисков ПС в целом и их компонентов. Для систематической, координированной борьбы с рисками проектов ПС необходимо учить специалистов анализу и оцениванию конкретных факторов, влияющих на риски проектирования и функционирования программных продуктов со стороны реально существующих опасностей — угроз и потенциально возможных дефектов в программах и данных.

Глава 1. Модели и стандарты управления рисками проектов программных средств

1.1. Основные модели управления рисками проектов программных средств

Разработано **несколько моделей и стандартов для анализа и сокращения рисков в жизненном цикле программных средств**, обзор которых представлен ниже [6, 7, 9, 11, 12, 13]. Каждая из этих моделей имеет свои особенности, обусловленные свойствами и характеристиками объектов разработки — комплексов программ, а также систем и внешней среды, в которых они применяются. Модели отличаются спецификой интересов и квалификации их авторов и охватывают широкий спектр реальных ситуаций проектирования ПС, в которых необходимо сокращение или исключение рисков проектов. В приводимых вариантах внимание акцентируется на процессах анализа и уменьшения рисков, однако практически отсутствуют оценки реальных значений рисков, которые могут быть достигнуты при предлагаемых методах и стратегиях. Решение этой задачи сильно зависит от параметров и характеристик реальных проектов ПС и вряд ли может конструктивно решаться в общем виде. Приведенный набор моделей и стандартов и их фрагменты целесообразно обобщать и использовать разработчикам и заказчикам сложных ПС высокого качества для формирования собственных руководящих документов предприятия при необходимости обеспечения минимальных рисков в жизненном цикле конкретных программных продуктов. Для облегчения разработки таких документов в главе 2 представлена Концепция анализа и управления рисками проектов ПС, которая поддержана детализирующими материалами последующих глав.

Институт программного инжиниринга (SEI) [9, 11] разработал модель оценки рисков при разработке комплексов программ**.** Рассматриваемая **первая модель** обеспечивает рисковую информацию и получение откликов на нее как внутри, так и вне проекта. **Подготовку процессов управления рисками** проекта комплекса программ **SEI** рекомендуется проводить в следующей последовательности:

- **согласование целей** проекта и управления рисками ПС — разработка и заключение договора с группой экспертов на проведение оценок и анализа рисков, а также на разработку концепции управления рисками проекта;
- **планирование и координация работ** по оценке рисков проекта — выделение группы экспертов для управления рисками в жизненном цикле ПС, интервьюирование специалистов-разработчиков проекта ПС с целью выявления рисков в результатах их деятельности;
- **оценка рисков** — обнаружение, спецификация и оценивание влияния рисков на проект, разработка рекомендаций по управлению рисками проекта ПС;
- **подготовка к устранению рисков** — разработка стратегии и комплекса мероприятий по сокращению или исключению рисков, подготовка отчета с рекомендациями для руководства проекта по анализу и управлению рисками;
- **разработка плана управления рисками** — методы, процессы, этапы работ, инструменты, организация и распределение ответственности за управление, а также за обеспечение допустимого уровня рисков проекта ПС.

План управления и сокращения рисков в модели **SEI** рекомендуется выполнять итерационно по основным крупным этапам жизненного цикла проекта ПС. На рис. 1 эта модель представлена из **следующих компонентов:**

- **идентификация рисков** — поиск и локализация источников-причин угроз проявления рисков до того, как они превратятся в дефекты, определение ситуаций и условий возникновения риска, идентификация и регистрация потенциальных рисковых событий и спецификаций содержания угроз риска;
- **анализ рисков** — преобразование и классификация исходной информации, определяющей возможность принятия решений, на которые влияет риск, определение приоритетов, качественных и количественных характеристик риска, вероятностных значений для благоприятных и неблагоприятных последствий, значений, позволяющих игнорировать определенные события, и неблагоприятные обстоятельства, которые не следует допускать;
- **планирование откликов и контрмер** — преобразование информации, на которую влияет риск, в решения и действия по снижению влияния риска (как в настоящем, так и в будущем), реализация этих действий на практике, управление рисками и планирование случайностей, идентификация результатов, выраженных в изменении требований или ресурсов проекта, определение методики снижения влияния рисков с использованием оговоренных в контракте средств;
- **отслеживание** — учет и обобщение значений индикаторов риска и действий по снижению его влияния, контроль и корректировка отклонений от планов по снижению риска, разработка планов корректирующих мероприятий и просмотр результатов внедрения контрмер как части общего плана управления рисками;
- **контроль состояния и управление** уровнем риска программного средства — регистрация и обобщение данных о реальных, интегральных рисках, подготовка и реализация планов дальнейшего снижения и ликвидации рисков проекта ПС.

Идентификацию рисков рекомендуется выполнять с помощью методик контрольных списков (шаблонов рисков), анализа принимаемых решений и устранения проблем. Риски проявляются вследствие неопределенности или же недостаточного объема знаний, касающихся всех возможных будущих событий в жизненном цикле и при функционировании ПС. Эти события можно разделить на благоприятные и неблагоприятные для создания и применения ПС в будущем. План разработки программного проекта представляет собой подготовленный **прогноз** запланированных событий. На протяжении жизненного цикла проекта может происходить большое число событий, не внесенных в этот план, состав которых необходимо минимизировать. Менеджер проекта имеет дело с **рисками, которые можно классифицировать** следующим образом [9]:

Известное в известном — риски известны разработчикам проекта, определены категории риска, а также реальные оценки величины и последствий конкретных рисков для данного проекта. Например, если отсутствует достаточно квалифицированный исполнитель для крупного раздела проекта, проявляющийся в этом случае риск относится к известному типу, а относительно его наличия в данном проекте также можно сделать определенные выводы.

Известное в неизвестном — риски известны команде разработчиков проектов, знакома

категория риска, но неизвестны возможные ситуации его реального проявления и возможная величина последствий для данного проекта. Например, отсутствие достаточного взаимодействия с конечным пользователем приводит к риску, связанному с корректностью формулировки и идентификации требований. Если для данного проекта неизвестно, будет ли обеспечен доступ к конечному пользователю, речь идет об известных типах рисков. Однако неизвестно, существует ли вообще этот риск и его значение для данного проекта ПС.

Неизвестное в неизвестном — риски могут быть известны разработчикам проекта, знакома категория риска, но неизвестны его реальные перспективы для данного проекта ПС. Подобное проявляется в том случае, если проект использует специфическое технологическое решение, которое формулируется в требованиях контракта для данного проекта. При отсутствии опыта работы с инструментом, менеджер проекта не может знать всех потенциальных рисков, которые может повлечь за собой его применение.

Если проекты разрабатываются с учетом новой предметной области или же применяется новая методика, мало известная команде разработчиков проекта, рекомендуется обращаться к анализу принимаемых решений и к процедуре устранения проблем. С помощью этих инструментов команда разработчиков сможет более четко представлять особенности предметной области, с учетом которой разрабатывается программное средство, и сосредоточить внимание на особенностях общего плана уже определенных классов риска.

Анализ идентифицированных рисков может выполняться с использованием моделирования производительности и размеров стоимости, анализа сетевых возможностей (принимаемых решений и факторов, влияющих на качество). Моделирование производительности и затрат ресурсов позволяет менеджеру проекта на основе переменных, отражающих особенности производительности и размеры затрат, формировать сценарии по принципу «что, если». Значения этих переменных оцениваются на основе представлений, присущих изначально предметной области, где исследуется данная проблема. Можно добавить усовершенствованные статистические методики типа метода Монте-Карло, что позволит в дальнейшем проводить дополнительный анализ. Анализ качественных факторов, а также выбор решений позволяет команде разработчиков проекта получить расширенные представления об информации проекта, которая разрабатывается в процессе анализа проблемы при выполнении идентификации рисков.

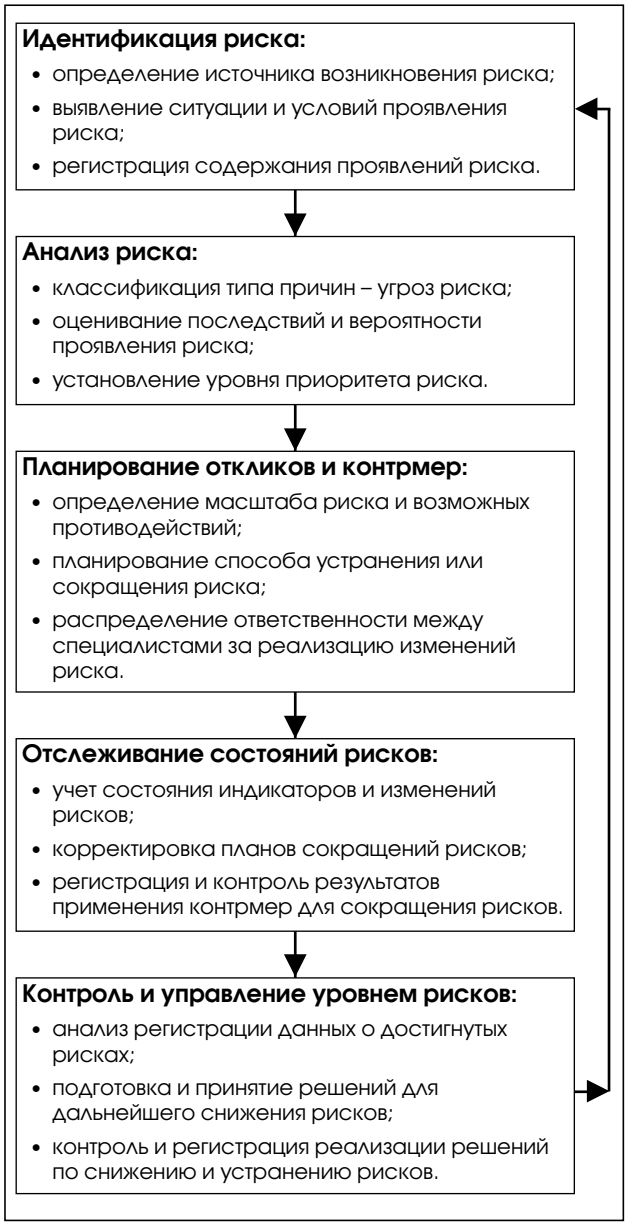


Рис. 1.

После идентификации и анализа рисков следует определить относительный потенциал их проявления и степень влияния на проект — угрозу риска. **Уточнение приоритетов рисков** позволяет команде разработчиков проекта обратить внимание на некоторые критические факторы риска. Именно они наиболее опасны и могут послужить причиной возникновения отказов при выполнении проекта. Для каждого риска, имеющего высокий уровень угрозы — приоритета, должна проводиться оценка его вероятности, определение количественных показателей, характеризующих проявление и последствия ри-

ска. Сначала должна вычисляться вероятность текущего проявления риска, а затем определяться это же значение после выполнения действий по снижению риска. Определяется стоимость затраченных ресурсов по выполнению действий, направленных на снижение риска. Вычитая коэффициент, полученный после выполнения действий по снижению риска, из значения, вычисленного до выполнения этих действий, следует разделить полученный результат на затраты, понесенные на этапе снижения риска. Таким образом, получится мера для оценивания эффекта изменения рисков при относительных затратах. Редукция составного риска представляет собой разложение многофакторных рисков на однофакторные компоненты, что позволяет оценивать приоритеты среди рисков.

Управление рисками включает планирование менеджмента рисков, определение состояния и мониторинг рисков. Наряду с оцениванием рисков эти компоненты должны поддерживаться наборами инструментов и методик. Во время планирования менеджмента рисков используются инструменты по получению информации и методики, позволяющие избежать проявления рисков. Также применяется передача, редукция элементов и интеграция планирования. Производится подписание контрактов с консультантами-экспертами по основополагающим вопросам, получение информации из баз данных, содержащих интересующие вопросы, а также оказание исследовательских услуг.

Меры, позволяющие **избежать проявления рисков**, содержат возможности по реструктуризации и изменению характеристик качества проекта и продукта, которые помогают не допустить проявления определенного риска. Передача комплекса программ заказчику или пользователю обычно предполагает **заключение страхового договора**, покрывающего издержки возможных рисков. Происходит передача ответственности для части или всего проекта, с учетом возможного изначально риска, другой организации.

Планирование элементов риска и **интегрирование плана исследования рисков** реализуются одновременно при структурировании проекта. При интегрировании плана риски рассматриваются его отдельные элементы, которые затем объединяются в обобщающем проекте. Путем разложения риска на части можно адресовать ответственность отдельным специалистам и определять каждый элемент риска.

Определение и оценки риска рекомендуется выполнять с помощью прототипов, имитаций, анализа показателей производительности и привлечения экспертов. Поэтому в **моделях риска должна прослеживаться явная связь с виртуальной моделью процессов разработки и всего жизненного цикла ПС**. Прототипы, имитации и показатели производительности обычно предполагают дополнительные инструменты и возможности. Эти инструменты играют большую роль при уменьшении и снижении рисков. Однако эти инструменты требуют инвестиций и для реализации предоставляемых преимуществ необходима определенная тренировка и обучение.

В ряде публикаций активно рекомендуется **вторая модель управления рисками**, представленная на рис. 2 [11], по существу близкая к предыдущей модели. В отличие от первой модели **(SEI)**, в ней структура содержит шесть этапов, содержание которых охватывает те же процессы, подробно отраженные на рисунке модели. В описании выделены две основные проблемы управления рисками сложных программных проектов: **проблема менеджмента проектов** и **проблема теории управления** проектом. В этой модели выделены **десять компонентов** — наиболее важных причин при управлении рисками проектов сложных комплексов программ, для которых рекомендуются процедуры их сокращения:

- недостаточное количество и квалификация коллектива специалистов;
- нереальная оценка требуемого времени реализации проекта и выделяемого бюджета;
- дефекты и неопределенности при разработке требований и основных функций комплекса программ;
- дефекты и ошибки при разработке пользовательского интерфейса и связей компонентов ПС;
- нарушения базовых (золотых) основ процессов разработки и жестких требований, отсутствие прототипов, анализа и проектирования затрат;
- непрерывное изменение требований, информационных связей, расширение функций проекта ПС;
- недостатки компонентов внешнего обслуживания и контроля, анализа совместимости компонентов, рекомендаций и применения связей;
- недостатки средств внешних преобразований и взаимодействия компонентов, компетентного проектирования или прототипирования;
- дефекты при обеспечении процессов реального времени, моделировании прототипов, настройки инструментов разработки и контроля;

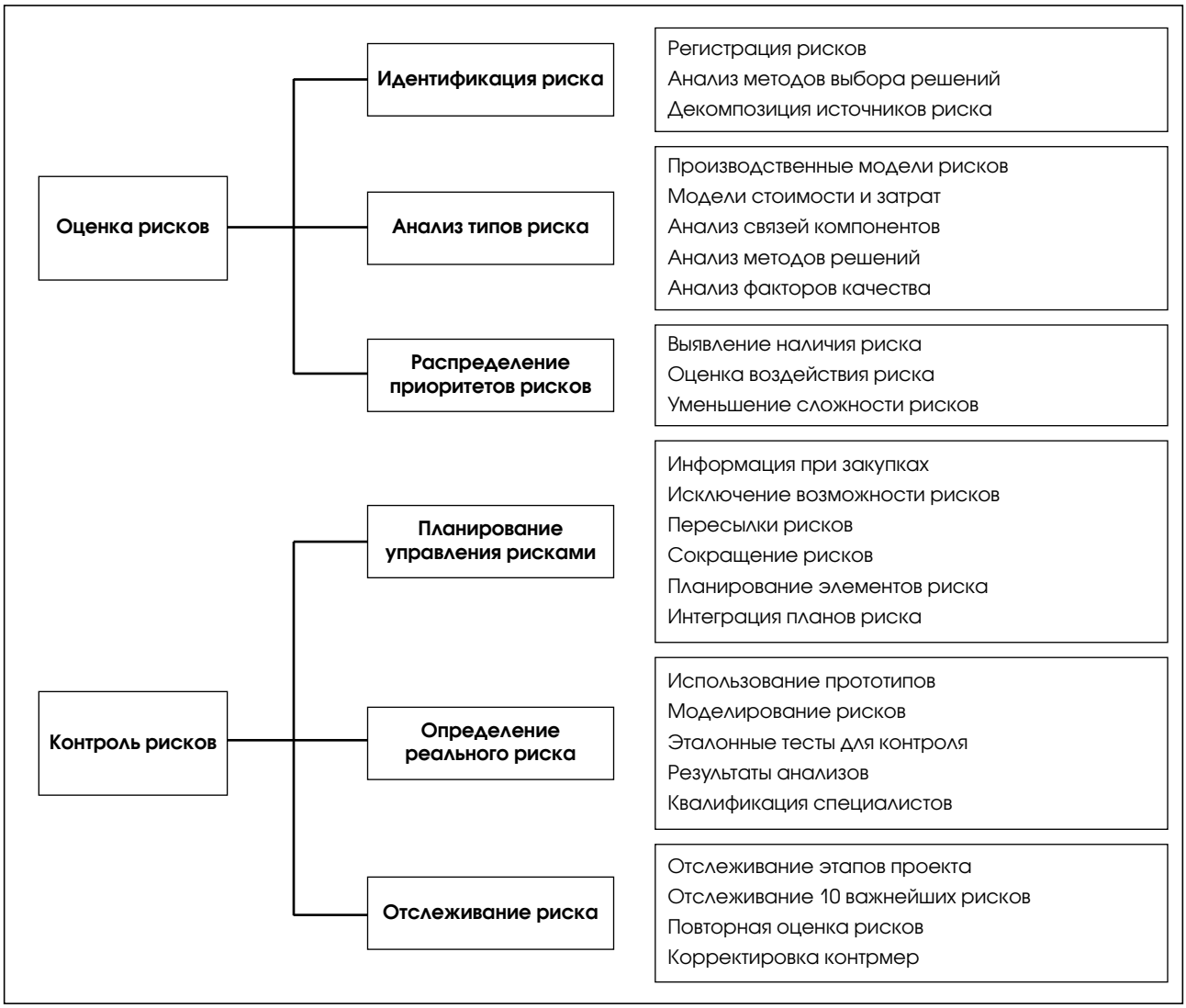


Рис. 2.

- дефекты контроля вычислительной техники и отказы функционирования компьютеров и системы.

В [9] предлагается **третья модель управления рисками** с использованием **12 категорий потенциального риска** для определенного 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 и атрибутов которых представлено в обширной таблице. План управления проектными рисками для конкретного ПС рекомендуется **моделировать категориями**:

1. **Задачи и цели.** Каждый одобренный проект ПС должен занимать соответствующее место среди целей и задач предприятия. Те проекты, которые не соответствуют реальным целям организации, создают напряжение, влияющее на все проекты. Например, потребуем, чтобы существовала организация, в задачи которой входила бы разработка ПС для внутреннего корпоративного производства, а цель состоит в создании наиболее эффективного, заказного программного обеспечения для предприятий организации. Если предприятие приступит к выполнению проекта по созданию пакета ПС общей направленности и на коммерческой основе, то это может быть рискованным мероприятием, противоречащим текущим задачам, квалификации и целям организации.
2. **Организационный менеджмент**. Каждый из выбранных проектов должен вписываться в текущую или планируемую организационную структуру. Если организация не облада-

ет подобной структурой или же она еще не создана, трудно рассчитывать на успешную реализацию программного проекта. Примером подобных рискованных формирований являются торговые организации, прекращающие разработку проектов без дотаций со стороны исполняющих организаций. Проект перебрасывается на другое предприятие по разработке, поскольку нет подходящей команды и отсутствует процесс формирования необходимого типа системы.

3. **Заказчик**. Все проекты должны иметь постоянную обратную связь с заказчиком. Проект разработки ПС требует обширных исходных данных, которые могут представить заказчики и конечные пользователи. Без подобных данных самый удачный процесс разработки приведет к формированию только отлично функционирующей системы, не отвечающей реальным запросам конечных пользователей. Скрытый здесь риск состоит в привлечении в команду неопытных сотрудников, не обладающих адекватным опытом по разрешению проблем, связанных с конкретной предметной областью. Такие сотрудники не смогут удовлетворять требуемые технические запросы заказчика и разработчиков ПС.
4. **Бюджет/стоимость**. Именно данная категория обычно привлекает наиболее пристальное внимание и оказывает влияние на все другие категории рисков. Менеджеры проектов сосредотачивают внимание на бюджете и объемах затрат, поскольку именно эти рычаги позволяют задействовать широкий спектр возможностей, приводящих проект к успешному завершению. Для уменьшения риска, относящегося к этой категории, следует четко представлять размеры проекта, располагать достоверной предысторией о работе над подобными проектами, а также иметь достаточно полное представление о внешних влияниях, например, о технологии.
5. **График**. Большой риск состоит в том, что команде разработчиков навязываются слишком тесные временные рамки графика работ. Если разработчики не могут оказывать влияния на формирование графика и даты ключевых этапов проекта, велика вероятность того, что график выполняться не будет. Команды разработчиков ПС должны принимать участие в разработке проектных графиков и иметь возможность вносить туда изменения.
6. **Содержание проекта**. Все проекты генерируют те или иные особенности, которые дополняют проект и образуют промежуточные продукты. Одним из основных компонентов является документация, содержащая требования, сведения о проектировании, о целевой системе и внешней среде. Если эта информация отсутствует, могут появиться ошибки, либо резко и непредсказуемо возрастет риск потери сведений, содержащихся в проекте. Также может нарушиться график или существенно пострадает содержимое продукта.
7. **Выполнение**. Эти факторы риска относятся к особому периоду, когда наступает момент практических испытаний разработанной системы и ПС. Однако именно эти факторы риска являются ключевыми для критерия по разработке программного продукта. Некоторые из основных областей риска относятся к функционированию системы во время тестирования. Критическое значение имеет доступная возможность полного тестирования всех модулей и их интерфейсов. Неадекватное тестирование ведет к отказам при выполнении проекта и соответствующим рискам.
8. **Управление проектом**. Эта категория относится как к процессу управления проектом, так и к компетенции менеджера проекта. Риск существует не только из-за недостатков, неадекватной трактовки, процессов менеджмента, но может быть также следствием предыдущего опыта работы менеджера проекта. Менеджеры проектов должны иметь опыт работы с определенной предметной областью и иметь представления о процессах проектного менеджмента в жизненном цикле ПС.
9. **Процессы разработки**. Эта категория фокусируется на тех процессах, которые уменьшают общий риск и улучшают качество производимого продукта. К процессам разработки не относятся специфические инструменты, такие как языки программирования, построители или генераторы кода. Рассматриваемые процессы фокусируются на процессах конфигурационного менеджмента, практиках и методах обеспечения качества и на анализе альтернатив.
10. **Среда разработки**. Данная категория сосредоточена на физической среде возможностей, аппаратных платформах и инструментах по разработке программного продукта. Риск возникает не только из-за недостатка

адекватных инструментов, но и вследствие отсутствия адекватных возможностей их использования. Если команда не подобрана специально для решения конкретной задачи, отсутствует адекватное пространство для выработки соглашений, пространство для поддержки интервью с заказчиком и рабочие комнаты, риск существенно возрастает.

11. **Персонал**. Эта категория является единственной, где существенное уменьшение риска достигается за счет набора опытной и высокопроизводительной команды разработчиков ПС. Разработчики, обладающие высокой рабочей эффективностью, могут в 10 и даже в 25 раз продуктивнее работать, чем обычная команда. Неуверенность в возможностях команды или в опытности ее членов в сочетании с некоторыми особенностями предметных областей, способствует фиксации консервативного подхода к факторам риска из этой категории.
12. **Поддержка**. Эта заключительная категория позволяет количественно оценивать риск, связанный с ПС, после поставки программного продукта. Команда разработчиков проекта часто несет ответственность за поддержку программного продукта в течение определенного периода после его поставки. Если же это не так, а неопытные пользователи пытаются фиксировать и исправлять ошибки в ПС, проектный риск существенно возрастает. Инструменты, применяемые для разработки, должны быть доступны и на этапе поддержки. Поддержка поставщика после выпуска продукта характеризуется наличием риска выпуска, если отсутствует план или бюджет для реализации инструментария непрерывной поддержки.

В [9] выделены **десять наиболее важных факторов и откликов** — рекомендаций на проявления рисков проектов ПС, которые частично перекликаются с десятью рекомендациями в предыдущей модели:

- слишком мало экспертов для анализа и управления рисками — следует уточнить условия контракта;
- плотный график разработки проекта — необходимо выполнить дополнительные оценки и уточнить разработчику график совместно с заказчиком;
- недостаточно эффективная функция отчетности о рисках — руководителю проекта следует провести экспертную оценку документирования с заказчиком;
- слишком разнообразный интерфейс — экспертная оценка руководителем проекта совместно с заказчиком;
- новые требования — необходима экспертная оценка затрат менеджером проекта;
- угроза неоправданных усовершенствований (позолоты) — руководителю проекта следует придерживаться утвержденных требований заказчика;
- просчеты в достижимом качестве — использовать возможность обратиться ко второму поставщику для анализа и дополнительных работ;
- нестабильность в замкнутости текстов программ — необходимо исследовать применение и расположение скобок программистами;
- проблемы со временем исполнения ПС — проводить имитацию тестов и тестирование в течение всего проекта;
- новые технологические риски — экспертная оценка нового инструментария с ответственным по научной части и руководителем проекта.

Рекомендуется **разработка плана управления рисками**, состоящего из пяти этапов. 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 скомпоновать в процессе идентификации потенциальных угроз и рисков, введения их категорий и установления приоритетов.

Этап 1. Используя описанные категории рисков, рекомендуется создать таблицу категорий. Команда разработчиков может воспользоваться этой таблицей для обзора категорий рисков данного проекта. Также команда должна сформировать информацию о наборе факторов и угроз для изучения. Таблица категорий рисков должна содержать сведения о том, какие факторы рисков более реальны и насколько они очевидны. Если предприятие располагает методами работы с этими факторами, можно сравнить их рейтинги в данном проекте с рейтингами в проектах, которые разрабатывались ранее. Можно использовать подход, основанный на всеобъемлющем рейтинге, или фиксировать внимание на определенном количестве наибольших рисков или же комбинировать количество рисков и степень их влияния, прогнозируя успех или неудачу проекта. Данная таблица является отправной точкой при идентификации определенных рисков в каждом проекте.

Этап 2. Ранжируются риски, связанные с выполнением проекта, по категориям:

- факторы риска и области — для каждой категории в столбце перечисляются факторы и угрозы категории риска;
- выделяется низкая очевидность рисков — этот столбец характеризует факторы относительно невысокой вероятности и малых последствий риска для проекта;
- средняя очевидность рисков — столбец характеризует факторы, имеющие среднюю вероятность, и последствия рисков для проекта;
- высокая очевидность рисков — выделяются факторы, когда вероятность и негативные последствия риска для проекта достаточно велики;
- определение рейтинга — выделение уровня интегрального риска, допустимого для данного проекта;
- комментарии — поддерживается информация об особенностях проекта, которая позволяет соблюдать выбранный рейтинг.

В некоторых случаях очевидное проявление риска одной категории может характеризоваться как высокое, а другой — как низкое. В [9] приведена таблица факторов риска и категорий, для которых очевидность риска характеризуется соответственно как низкая, средняя или высокая. Данная таблица может служить шаблоном, используемым в качестве отправной точки для разработки проекта программного продукта. Категории, факторы и очевидность рисков можно обновлять для любого проекта в пределах рассматриваемой схемы.

Этап 3. Выполняется сортировка таблицы рисков, располагая их 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. Именно они и будут ключевыми. Идентифицируются средства для контроля каждого ключевого риска, устанавливается ответственность за его сокращение и дата выполнения. Интегрируются ключевые риски в план проекта, и уточняется их влияние на график и размер затрат.

Этап 4. Устанавливается формат отчета для каждого регулярного риска. Этот отчет рекомендуется заслушивать на еженедельных встречах коллектива специалистов, где рассматривается состояние проекта. Показывается состояние наибольших десяти рисков, изменения в ранжировании для каждого риска за последнюю неделю. Отображается отчет откликов-контрмер о рисках и об их изменениях.

Этап 5. На заключительном этапе следует удостовериться, что управление и сокращение рисков является непрерывным процессом в рамках жизненного цикла проекта ПС. Отслеживание и контроль рисков, включенных в список, должны выполняться на регулярной основе. Менеджер проекта и все члены команды должны обращать внимание на поведение идентифицированных рисков, а также контролировать процессы их определения. Новые риски должны идентифицироваться, прежде всего, для них определяются приоритеты, которые затем добавляются в план управления рисками. Риски с высоким приоритетом следует обрабатывать в соответствии с общим планом проекта ПС.

В [13] предложена и детально рассмотрена **четвертая модель анализа рисков программных средств**, базирующаяся на: крупных элементах, факторах и свойствах — метриках рисков, к каждому из которых приводится краткое описание их содержания (см. рис. 3). Компоненты анализа рисков иллюстрируются таблицами связей и взаимодействия. В **элементы рисков** включены взаимосвязанные технические, стоимостные и плановые риски.

Технические риски определяются требованиями и особенностями объекта — программного средства и включают:

- функциональные характеристики;
- характеристики качества;
- надежность;
- применимость;
- временную производительность;
- сопровождаемость;
- повторное использование компонентов.

Стоимостные риски составляют:

- ограничения суммарного бюджета;
- недоступная, фиксированная или варьируемая стоимость проекта ПС;
- степень реализма при оценивании затрат на проект ПС.

Плановые риски включают:

- свойства и возможности гибкости изменения планов;
- возможности нарушения установленных вех — сроков этапов;
- реализм планов и этапов жизненного цикла.

Кроме того, выделены **риски процессов и процедур управления** проектом, которые мож-

Рис. 3.

но отнести к основным перечисленным элементам рисков:

- риски идентификации;
- риски стратегии и планирования проекта;
- риски оценок;
- допустимые результирующие риски при сокращении или устранении угроз;
- риски документирования;
- риски прогнозирования развития и совершенствования проекта.

Для выделенных групп элементов риска в [13] представлены подробные таблицы, в которых отражено взаимодействие между **факторами риска**. Для каждого фактора рекомендуется оценивать тип, характеристики и природу последствий рисков, расшифровано содержание от пяти до двенадцати **свойств – метрик риска**. Факторы и метрики рисков связаны десятью таблицами, в которых выделены и отмечены свойства проектов ПС, рекомендуемые для учета при анализе рисков. В качестве **факторов, определяющих риски** выделены:

- **организация проекта** ПС – риски управления, действий и квалификации менеджеров при создании комплексов программ (8 свойств);
- **оценки характеристик управления** проектом ПС (7 свойств);
- **мониторинг управления** проектом ПС (7 свойств);
- **уровень методологии** управления разработкой проекта ПС (7 свойств);
- **уровень и свойства инструментальных средств** разработки проекта ПС (9 свойств);
- **риски культуры** – современности и качества методов разработки проекта ПС (11 свойств);
- **широта применения** – перспективы используемости программного продукта (6 свойств);
- **корректность** – степень соответствия программного продукта требованиям спецификаций заказчика (9 свойств);
- **надежность** функционирования программного продукта (12 свойств);

- необходимый **уровень и количество специалистов** для реализации проекта (5 свойств).

В заключение рассмотрены фазы и рекомендации применения изложенной модели по традиционным этапам жизненного цикла сложных ПС, а также примеры анализа угроз рисков и интерпретации результатов управления для некоторых вариантов проектов комплексов программ.

1.2. Стандартизация управления рисками программных средств

Общие методы анализа рисков в сложных системах регламентированы стандартом **ГОСТ Р 51901** — 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 и разработке проектов комплексов программ. Ниже представлены основные концепции и сокращенное содержание этого стандарта, адаптированные для возможности применения его положений при анализе рисков проектов программных средств. Для повышения эффективности управления проектами рекомендуется проводить **анализ риска, включающий**:

- идентификацию риска и определение методов решения связанных с ним проблем;
- использование объективной информации при принятии решений для сокращения рисков;
- удовлетворение регламентированных требований заказчика к допустимому риску.

Применяемый **метод анализа риска** должен быть:

- научно обоснованным и соответствовать функциям, характеристикам и сложности исследуемой системы;
- давать результаты в форме, обеспечивающей понимание природы угроз, свойств риска и способов его контроля;
- типовым и обладать свойствами, обеспечивающими прослеживаемость, повторяемость и контролируемость результатов анализа.

Должно быть представлено обоснование по выбору метода с точки зрения его пригодности для анализа конкретной системы. Как только принято решение о проведении анализа риска, должны быть определены цели и область применения метода. Результаты анализа риска могут использоваться специалистом, принимающим решение при оценке допустимости риска, а также при выборе между потенциальными мерами по снижению или устранению риска. С точки зрения специалистов-разработчиков систем, принимающих решения, к основным **достоинствам изложенных ниже методов анализа риска** относятся:

- систематическая идентификация потенциальных опасностей, угроз;
- систематическая идентификация возможных видов отказов системы;
- количественные оценки или ранжирование рисков;
- оценка надежности возможных контрмер и модификаций системы для снижения риска и достижения предпочтительных уровней ее качества;
- 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.

Все эти факторы играют важную роль в эффективном управлении рисками независимо от того, какие задачи рассматриваются (охрана здоровья, безопасность, предотвращение экономических потерь, обеспечение выполнения требований заказчика программных средств). **Общей задачей анализа риска** является обоснование и подготовка решений, касающихся сокращения рисков. Эти решения могут приниматься как часть более крупного процесса управления рисками системы, посредством сопоставления результатов анализа риска компонентов с критериями допустимого риска системы в целом.

Применение анализа риска рассматривается на двух стадиях жизненного цикла опасных систем. **Стадия проектирования**:

- выявление главных источников угроз риска и предполагаемых факторов, существенно влияющих на риск;
- предоставление исходных данных для оценки качества системы в целом;

- определение и оценка эффективности возможных мер обеспечения безопасности, закладываемых в систему;
- предоставление исходных данных для оценки потенциально опасных действий, оборудования или систем;
- обеспечение соответствующей информацией при проведении опытно-конструкторских работ, ориентированных на нормальные и чрезвычайные условия;
- оценка риска с учетом регламентов и других требований поддержки применения;
- оценка альтернативных, конструктивных решений.

Стадии изготовления, эксплуатации и технического обслуживания:

- контроль и оценка данных эксплуатации с целью сопоставления фактических показателей работы с соответствующими требованиями;
- обеспечение исходными данными процессов разработки, методик эксплуатации, технического обслуживания, контроля и действий в чрезвычайных ситуациях;
- корректировка информации об основных источниках угроз, риска и влияющих факторах;
- предоставление информации по значимости риска для принятия оперативных решений для его сокращения;
- определение влияния на риски изменений в организационной структуре, производстве, процедурах эксплуатации и компонентах системы;
- подготовка персонала к применению системы.

Процесс анализа риска для повышения эффективности и объективности анализа и обеспечения сопоставимости с другими результатами рекомендуется осуществлять в соответствии со следующими этапами:

- определение области применения системы;
- идентификация опасностей, угроз и предварительная оценка возможных последствий;
- оценка возможных величин риска;
- проверка достоверности результатов анализа;
- документальное обоснование результатов анализа;
- корректировка результатов анализа с учетом последних данных.

Важным требованием является достоверное знание разработчиками анализируемой системы и используемых методов анализа. В том случае, если имеются результаты анализа риска для аналогичной системы, они могут быть использованы в качестве справочного материала или прототипа. При этом необходимо доказать, что процессы являются подобными и что изменения не вносят существенных различий в результаты. Выводы должны основываться на систематической оценке изменений и на том, каким образом они могут влиять на существующие опасности. Многие системы слишком сложны для работы одного человека, поэтому для выполнения анализа может требоваться группа аналитиков. Отдельное лицо или рабочая группа должны быть ознакомлены с методами, используемыми для анализа риска, и должны располагать достаточными знаниями о рассматриваемом предмете и системе. Заключение специалистов рабочей группы должно быть документально зафиксировано.

Для выработки плана исследований **область применения анализа риска** должна быть определена и документально установлена. Она должна включать в себя следующие этапы:

- описание оснований и/или проблем, повлекших необходимость анализа риска, которое включает: формулировку задач анализа риска, основанных на идентифицированных потенциальных опасностях, угрозах; определение критериев работоспособности и отказа системы;
- описание исследуемой системы — определение границ и областей интерфейса со смежными системами; описание условий окружающей среды; выделение видов информации, превышающих допустимые границы; определение рабочих условий и состояний системы, на которые распространяется анализ риска и соответствующие ограничения;
- установление источников, предоставляющих подробную информацию о всех технических, связанных с окружающей средой, правовых, организационных и человеческих факторах, имеющих отношение к анализируемым действиям и проблеме; в частности, должны быть описаны обстоятельства, касающиеся безопасности;
- описание используемых предположений и ограничивающих условий при проведении анализа рисков;
- формулировка решений, которые могут быть приняты, описание требуемых выходных данных, полученных по результатам исследований и от лиц, принимающих решения.

Идентификация опасностей и предварительная оценка последствий, являющихся причиной риска, а также путей, по которым эти опасности могут реализовываться. Известные опасности, угрозы (возможно, имевшие место при предыдущих авариях) должны быть четко и точно определены. Для идентификации опасностей, не учитываемых ранее при проведении анализа, должны применяться формальные методы. Предварительную оценку значения идентифицированных опасностей необходимо выполнять, основываясь на изучении их основных причин и анализе последствий. Предварительная оценка значения идентифицированных опасностей определяет выбор последующих действий:

- принятие немедленных мер с целью исключения или уменьшения опасностей;
- прекращение анализа, поскольку опасности или их последствия являются несущественными;
- переход к оцениванию риска.

В **процессе оценки величины риска** для выбора критического уровня допустимых рисков должны исследоваться начальные события или обстоятельства, последовательность потенциально опасных событий, любые смягчающие факторы и характеристики, а также природа и частота возможных негативных последствий идентифицированных опасностей. Эти критерии и меры должны распространяться на риски для людей, имущества и окружающей среды и должны включать значения неопределенностей оценок.

Методы, используемые для оценки величины риска, обычно являются количественными, несмотря на то, что степень детализации при подготовке исходной информации зависит от конкретного применения. Однако полный количественный анализ не всегда возможен из-за недостатка информации о системе или деятельности, подвергающейся анализу, отсутствия или недостатка данных об отказах, влиянии человеческого фактора. При таких обстоятельствах может оказаться эффективным сравнительное количественное или качественное ранжирование риска специалистами, хорошо информированными в данной области и системах. В тех случаях, когда проводится качественное ранжирование, необходимо иметь четкое разъяснение всех используемых терминов и должно быть зафиксировано обоснование всех классификаций частот и последствий. В том случае, когда проводится полная количественная оценка величины риска, необходимо учитывать, что расчетные значения риска представляют собой оценки и следует позаботиться о том, чтобы их точность соответствовала точности используемых исходных данных и аналитических методов.

Элементы процесса оценки величины риска являются общими для всех видов опасности. Прежде всего, анализируются возможные причины опасности с целью определения частоты ее возникновения, продолжительности, а также характера. В процессе анализа может возникнуть необходимость определения оценки вероятности опасности, вызывающей негативные последствия, и проведения анализов последовательности обуславливающих событий.

Анализ частот используется для оценки вероятности каждого негативного события, проявившегося на стадии идентификации опасностей, угроз. Для оценки частот происходящих событий обычно применяются следующие три метода:

- использование имеющихся статистических данных (предысторий);
- получение частот негативных событий на основе аналитических или имитационных методов;
- использование мнений экспертов.

Данные эксплуатации используются с целью определения частоты, с которой негативные события происходили в прошлом, и, исходя из этого, прогнозирование частоты, с которой они могут произойти в будущем. В том случае, когда статистические данные недоступны или не соответствуют требованиям к системе, можно получать частоты событий посредством анализа структуры и содержания системы и ее аварийных состояний. При проведении анализа частот могут использоваться методы имитационного моделирования отказов. Существует ряд методов для сопоставления экспертного мнения, которые исключают двусмысленность оценок, помогают при постановке соответствующих вопросов [1, 8, 9].

Анализ последствий используется для оценки вероятного воздействия, которое вызывается нежелательным событием. Анализ последствий должен:

- основываться на выбранных негативных событиях;
- описывать и оценивать любые последствия, являющиеся результатом негативных событий;
- учитывать существующие меры, направленные на смягчение последствий, наряду со

всеми соответствующими условиями, оказывающими влияние на последствия;
- устанавливать критерии, используемые для полной идентификации последствий;
- рассматривать и учитывать как немедленные последствия, так и те, которые могут проявиться по прошествии определенного периода времени, если это не противоречит сфере распространения исследований;
- рассматривать и учитывать вторичные последствия, распространяющиеся на смежные компоненты и системы.

Анализ последствий должен предусматривать определение результатов и ущерба в случае наступления негативных событий. Модели последствий требуются для прогнозирования размеров аварий, катастроф и других негативных явлений в различных анализируемых системах. Знание механизмов происходящих с ними последующих процессов **должно давать возможность прогнозировать соответствующие негативные процессы** заранее. Разработан ряд методов оценки такого рода явлений, диапазон которых простирается от упрощенных аналитических подходов до очень сложных компьютерных моделей.

Риск должен выражаться в достаточно **подходящих показателях**. Наиболее часто используемыми результатами являются:
- 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.

Необходимо установить, отражает ли полученная оценка риска уровень общего риска в системе или является лишь его частью. При расчете риска необходимо учитывать как продолжительность нежелательного события, так и вероятность того, что система будет подвергаться его воздействию. Данные, используемые для расчета уровней риска, должны соответствовать конкретному виду применения. Такого рода данные, по возможности, должны основываться на конкретных анализируемых обстоятельствах. Если таковые отсутствуют, должны использоваться данные общего характера, являющиеся характерными и представительными для данной ситуации, либо должна применяться пользующаяся доверием экспертная оценка. Данные должны собираться и группироваться в такой форме, которая способствовала бы удобному ее использованию при анализе риска.

Существует **множество неопределенностей**, связанных с оценкой риска. Понимание неопределенностей и вызывающих их причин необходимо для эффективной интерпретации значений риска. Анализ неопределенностей должен предусматривать определение изменений и неточностей в результатах моделирования, которые являются следствием отклонения параметров и предположений, применяемых при построении модели. Областью, тесно связанной с анализом неопределенностей, является **анализ чувствительности**. Анализ подразумевает определение изменений в реакции модели на отклонения отдельных параметров модели. Оценка неопределенности состоит из преобразования неопределенности критических параметров модели в неопределенность результатов в соответствии с моделью риска. Это относится как к неопределенностям данных, так и к неопределенностям модели. Должны быть определены те параметры, к которым чувствителен анализ.

Проверка результатов анализа должна осуществляться 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.

Отчет об анализе риска документально обосновывает процесс анализа и должен включать в себя либо план анализа риска, либо ссылки на него и результаты оценки опасностей. Техническая информация, представленная в отчете, является важной частью процесса анализа риска. В отчете должны быть разъяснены преимущества и ограничения используемых критериев риска. Пояснения относительно неопреде-

ленностей, соответствующих риску, должны быть изложены на языке, понятном предполагаемому заказчику или пользователю. В отчете должна быть отражена следующая информация:

- краткое изложение анализа рисков;
- выводы;
- цели и область применения анализа;
- ограничения, допущения и обоснование предложений по сокращению рисков;
- описание соответствующих частей системы;
- методология анализа рисков;
- результаты идентификации опасностей;
- используемые модели, в том числе допущения и их обоснования;
- использованные данные и их источники;
- результаты оценки величины риска;
- анализ чувствительности и неопределенности;
- рассмотрение и обсуждение результатов и предложений по сокращению или исключению рисков.

Если анализ риска используется для обеспечения непрерывного процесса управления риском, его необходимо выполнять и документировать таким образом, чтобы он мог поэтапно корректироваться на протяжении всего жизненного цикла системы. Анализ должен обновляться по мере поступления новой информации и в соответствии с потребностями процесса управления.

В стандарте содержится обширное справочное Приложение А – Методы проведения анализа рисков, которое ориентировано на аппаратные технологические системы и в отличие от основного содержания стандарта, вряд ли полезно для анализа рисков ЖЦ проектов комплексов программ.

Управление рисками в 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, которые 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 ПС [3, 6]. В результате такого стандартизированного процесса, менеджером по управлению рисками должны быть определены: возможные источники рисков в исходных требованиях к проекту, а также к характеристикам качества; проанализированы и определены сбалансированные приоритеты сокращения рисков. На этом основании должны выделяться ресурсы на сокращение рисков; определены рациональные стратегии управления, методы и средства уменьшения рисков в ЖЦ ПС; сокращены до допустимых пределов риски характеристик качества ПС. Поэтапное, иерархическое снижение интегрального риска проекта ПС при использовании выбранной стратегии может потребовать ее корректировки в зависимости от достигаемого эффекта и требуемых затрат на сокращение определенных рисков. Для решения этих задач **стандартом рекомендуются последовательные процедуры**:

- выявление и идентификация относящихся к проекту рисков как в исходном состоянии и требованиях к проекту, так и на последовательных этапах его выполнения: по характеристикам качества, графикам, трудоемкости, ресурсам и техническим рискам;
- анализ вероятности проявления, причин, взаимозависимости видов и последствий рисков, чтобы сбалансировать и распределить их приоритеты, на основании которых будут отводиться ресурсы на различные контрмеры для снижения этих рисков;
- определение целесообразной стратегии и области управления каждым видом риска или их наборами в проекте, в соответствии с политикой на предприятии, а также со степенью влияния, вероятностью и типами рисков, которые должны выявляться и которыми следует управлять;
- для каждого вида риска (или набора рисков) определение метрики, отражающей изменения в состоянии рисков в зависимости от деятельности по их устранению, которые должны характеризовать изменения в вероятности проявления, последствиях и временных диапазонах проявления рисков;
- реализация разработанной стратегии управления рисками, аттестация результатов и успешности стратегии в контрольных точках жизненного цикла проекта ПС;
- если не достигнут ожидаемый успех деятельности по изменению или устранению последствий рисков, применение мер для коррекции или сокращения влияния наибольших рисков, которые, в частности, могут включать разработку и реализацию новых откорректированных требований к ПС

или изменение существующих стратегий и ресурсов для устранения рисков.

Изложенная в стандарте методология оценивания и сбалансированного снижения рисков проектов сложных комплексов программ встречается со значительными трудностями при стремлении ее применить полностью к комплексной оптимизации рисков обеспечения качества и ограничений ресурсов проектов. Выше предполагалось, что требуемые и реализуемые значения характеристик ПС и ресурсов характеризуются относительными величинами — приоритетами, которые оцениваются квалифицированными экспертами [3, 4]. Такие оценки субъективны и не всегда способны отразить реальные физические параметры и их взаимосвязь, которые в конкретном проекте способны снизить его интегральный риск до допустимого предела. Поэтому на практике при анализе рисков целесообразно его сузить путем выделения важнейших факторов. Особое внимание в стандарте обращается на анализ рисков при усовершенствовании (сопровождении) и конфигурационном управлении версиями комплексов программ. Анализ и сокращение рисков на этих этапах связаны с необходимостью четкой формулировки требований заказчика, с проблемами организации скоординированных изменений программ в определенные сроки, со сложностью и неопределенностью объемов финансирования и привлечения квалифицированных специалистов, достаточно компетентных в конкретном проекте.

В [7] 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. Предлагается решать проблемы информационной безопасности с учетом уровня зрелости технологий предприятий, создающих информационные системы. Выделены и описаны пять уровней зрелости, различающиеся степенью организации и регламентирования процессов анализа и управления рисками систем информационной безопасности. В **подробной концепции** внимание акцентируется на возможных рисках нарушения информационных ресурсов ИС при наличии предумышленного, негативного воздействия на их безопасность из внешней среды. Поэтому, 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.

Значительное внимание в [7] уделено систематизации и анализу основных терминов, **относящихся к рассматриваемой области управления рисками**, которые позволяют уточнять содержание представленной концепции. Из разных документов для каждого термина приводится свыше пяти (до пятнадцати) определений, из которых в Приложении 1 выделены, скомпонованы и отредактированы наиболее представительные. Эти определения терминов полезно использовать с учетом особенностей рассматриваемых систем.

В [7] изложен обзор инструментальных средств для автоматизированного анализа и управления рисками в рассматриваемом классе систем и задач. При этом отмечается, что наибольшие трудности представляют разработка корректных процедур измерения величины рисков, методов учета наборов различных факторов, влияющих на риски, и оценок эффективности комплексов контрмер, способных сокращать интегральные риски до допустимых пределов.

Глава 2. Концепция анализа и сокращения рисков проектов сложных программных средств

В предыдущей главе представлен ряд моделей и стандартов, касающихся методов анализа и управления рисками проектов ПС. В этих документах имеется много общего, однако отсутствует целостная методология и концепция анализа и управления для сокращения рисков в жизненном цикле сложных комплексов программ. Ниже эти модели и стандарты, частично, использованы и переработаны с целью систематизирования и подготовки совокупности упорядоченных процессов, обеспечения высокого качества ПС путем исследования и уменьшения рисков в их жизненном цикле. Представленная **концепция анализа и сокращения рисков, ориентирована на обеспечение высокого качества проектов крупномасштабных комплексов программ путем минимизации рисков**. Подобные процессы должны сопутствовать основным этапам разработки и обеспечения ЖЦ сложных программных средств в соответствии с международными стандартами, а также графиками систем обеспечения качества ПС [3]. Особенности предлагаемой концепции состоят в следующем:

- анализ рисков рекомендуется начинать с подготовки детальных исходных требований и характеристик проекта ПС, системы и внешней среды, для которых должны отсутствовать риски функционирования и применения;
- для управления рисками и их сокращения в рассматриваемых проектах рекомендуется выделять три класса рисков: функциональной пригодности ПС, конструктивных характеристик качества и нарушения ограничений ресурсов при реализации процессов ЖЦ ПС;
- в каждом классе предлагается выделять несколько категорий наиболее важных рисков, которые упорядочивать по степени опасности, угрозы для проекта, обусловленных дефектами и/или недостаточным качеством разработки и жизненного цикла ПС;
- контрмеры для сокращения рисков рекомендуется анализировать и применять последовательно, начиная с ликвидации исходных причин — угроз, затем проводить анализ и уменьшение уязвимости компонентов и ПС в целом, а при недостаточности этих контрмер воздействовать непосредственно на уменьшение итогового ущерба — риска в жизненном цикле ПС и системы;
- процессы устранения рисков должны завершаться процедурами мониторинга, сопровождения и конфигурационного управления версиями комплексов программ высокого качества с минимальными допустимыми рисками.

Итоговые положения этой концепции ниже отражены перечнем этапов работ и процедур, которые рекомендуется выполнять при поддержке базовых работ жизненного цикла проектов сложных программных средств, и могут служить основой для разработки соответствующих графиков работ при управлении и минимизации рисков проектов сложных ПС (рис. 4). Перечисленные для каждого этапа процедуры комментируются особенностями их реализации.

Этап 1. Подготовка исходных данных для анализа и управления рисками проекта программного средства включает**:**

- описание назначения исследуемой системы, условий и характеристик внешней среды применения, структуры и функций системы и программного средства;
- определение целей, назначения и функций проекта программного средства в жизненном цикле системы и внешней среды, проблем анализа и сокращения рисков;
- разработку предварительных требований к функциональной пригодности и конструктивным характеристикам жизненного цикла проекта ПС, определение состояний системы, на которые распространяется анализ рисков и соответствующие ограничения;
- формирование группы специалистов — экспертов для анализа и управления рисками проекта ПС на всем жизненном цикле.

Должны быть установлены источники, способные предоставить подробную информацию обо всех технических, связанных с окружающей средой, правовых, организационных и человеческих факторах, имеющих отношение к анализируемой проблеме и системе; описание предположений и ограничивающих условий, допустимых при проведении анализа рисков. Следует сформулировать ожидаемые решения, которые могут быть приняты, структура и описа-

Подготовка исходных данных:

- описание системы, внешней среды и программного средства;
- определение целей, назначения и функций проекта программного средства и системы;
- разработка предварительных требований к функциональной пригодности и конструктивным характеристикам проекта ПС;
- формирование группы экспертов для анализа угроз и управления рисками.

Выделение, идентификация, анализ угроз и рисков программного средства:

- выделение источников и угроз нарушения требований и ограничений ресурсов, определение критериев работоспособности проекта ПС;
- отбор и идентификация основных угроз и рисков проекта ПС;
- анализ причин, выделение категорий угроз и возможных последствий проявления рисков функциональной пригодности проекта ПС;
- анализ причин, выделение категорий угроз и возможных последствий проявления рисков конструктивных характеристик проекта ПС;
- анализ причин, выделение категорий угроз и возможных последствий рисков ограничения доступных ресурсов проекта ПС.

Оценивание опасности угроз и рисков и выбор контрмер для их сокращения:

- оценивание возможных последствий, уровней потенциальных опасностей угроз и приоритетов категории рисков проекта ПС;
- выделение и упорядочение группы наиболее опасных, высокоприоритетных рисков проекта ПС;
- планирование методов и ресурсов реализации контрмер для сокращения опасных, приоритетных рисков проекта ПС;
- распределение ресурсов на контрмеры для сбалансированного сокращения интегрального риска проекта ПС;
- распределение ответственности специалистов за реализацию сокращения опасных рисков проекта ПС.

Сокращение или ликвидация опасных рисков проекта ПС:

- реализация контрмер для сокращения интегрального риска и составление отчетов о состоянии проекта;
- корректировка требований к функциональной пригодности, конструктивным характеристикам и ограничениям ресурсов проекта ПС;
- регистрация результатов сокращения интегрального риска на очередном этапе проекта ПС.

Контроль, регистрация, мониторинг и утверждение допустимого интегрального риска проекта ПС:

- контроль, отслеживание и мониторинг реализации сокращения интегрального риска по этапам проекта ПС;
- мониторинг состояния проекта и интегрального риска по этапам жизненного цикла ПС и системы;
- документирование и утверждение допустимого интегрального риска по этапам жизненного цикла проекта ПС и системы;
- оформление итогового отчета по результатам сокращения рисков ПС.

Рис. 4.

ние предполагаемых данных по результатам исследований и от лиц, принимающих решения. Исходные данные проекта программного средства новой или модернизированной системы должны содержать достаточно полные требования к функциям и характеристикам качества комплекса программ, описание и графическое представление его архитектуры, базы данных и взаимодействия компонентов, предполагаемую модель жизненного цикла, предварительные планы последующих этапов и работ. Кроме того, в них должны входить проекты технического задания и контракта на детальное проектирование и весь жизненный цикл ПС [2, 9, 15].

В исходных данных должны определяться состав и структура технологических и эксплуатационных документов для поддержки всего ЖЦ ПС. Эти документы должны обеспечивать реализацию процессов жизненного цикла ПС, планирования и управления, регистрировать выполнение требуемых действий. Для этого следует подготовить требования к документации и

обеспечить их реализацию, которая должна быть однозначной — написана в стандартизированных терминах, уточняемых, если необходимо, соответствующими комментариями.

Необходимым требованием к специалистам для применения анализа и управления рисками должно быть **достоверное знание целей и структуры комплекса программ, исследуемой системы и внешней среды**, а также доступных и используемых методов анализа. Область применения методов и процессов анализа и сокращения рисков должна быть определена и документально зафиксирована. Для этого следует составить описание оснований и/или проблем, определивших целесообразность проведения исследования рисков. Оно должно включать: описание области применения исследуемой системы; формулировку целей и задач анализа риска, основанную на идентифицированных потенциальных опасностях и угрозах; определение критериев работоспособности и отказа системы; определение границ и областей интерфейса со смежными системами; описание условий и характеристик окружающей среды.

Должна быть выполнена первичная идентификация возможных опасностей, угроз и предварительная оценка возможных их последствий, являющихся причиной рисков, а также процессов, по которым эти опасности могут реализовываться. Известные потенциальные опасности должны быть четко и точно определены и описаны. Предварительную оценку значения идентифицированных опасностей — угроз необходимо выполнять, основываясь на анализе последствий рисков и изучении их основных причин у аналогичных проектов. В результате следует выбрать решения: принятие немедленных мер с целью исключения или уменьшения некоторых угроз; прекращение анализа, поскольку определенные опасности или их последствия являются несущественными; переход к детальному исследованию, оцениванию и сокращению конкретного риска.

Программные средства для обработки информации обычно входят компонентами в системы более высокого уровня и полностью зависят от внешней среды и функций системы, в которой они используются. С этой точки зрения, **требования к характеристикам комплексов программ определяются назначением и функциями системы и внешней среды**, для которых они предназначены. Описания назначения, функций и требований к характеристикам системы, внешней среды и комплекса программ являются исходными данными трех взаимосвязанных технологических процессов (рис. 5):

- базовых, регламентированных **технологических процессов и инструментария** для их автоматизации, обеспечивающих проектирование, разработку и весь жизненный цикл проектов сложных программных средств;
- методов, средств и процессов обеспечения требуемых характеристик комплекса программ на основе **системы автоматизации контроля качества** процессов и продуктов в жизненном цикле ПС;
- процессов и системы автоматизированного **анализа, управления и сокращения рисков** ПС при создании и применении комплексов программ и систем в заданной внешней среде.

Для обеспечения высокого качества программного продукта этапы и работы управления качеством, а также процессы анализа и сокращения рисков целесообразно **выделять из основного жизненного цикла проекта ПС** и поручать отдельным группам специалистов — экспертов. Прогнозы и анализ вариантов технологических процессов проектирования ПС, их технико-экономических показателей и характеристик объекта разработки являются основой для выбора, планирования и последующего системного анализа всего ЖЦ ПС. Достоверность планов и прогнозов определяется точностью сведений об объекте разработки, характеристиках технологической среды и прототипов, принятых за основу при планировании. Таким образом, производится обоснование проекта, определяются приближенные значения трудоемкости и длительности всей разработки ПС, а также число необходимых специалистов, что позволяет оценить предварительный укрупненный план создания ПС в заданных условиях, ресурсах и сроках [1, 5, 15].

Проведенные таким образом оценки проекта ПС позволяют осуществить **предварительный выбор основных технологических методов и инструментальных средств** для проведения последующего детального и рабочего проектирования и реализации всего ЖЦ ПС. Кроме того, должна подготавливаться адаптация средств автоматизации, применительно к особенностям объекта и среды проектирования. Интегрированные инструментальные средства служат для формализации знаний заказчика на этапе проведения обследования, анализа и подготовки требований технического задания, а также для проектирования концептуальной и логической структур комплексов программ и баз данных.

При обосновании и реализации жизненного цикла комплексов программ, анализ и уп-

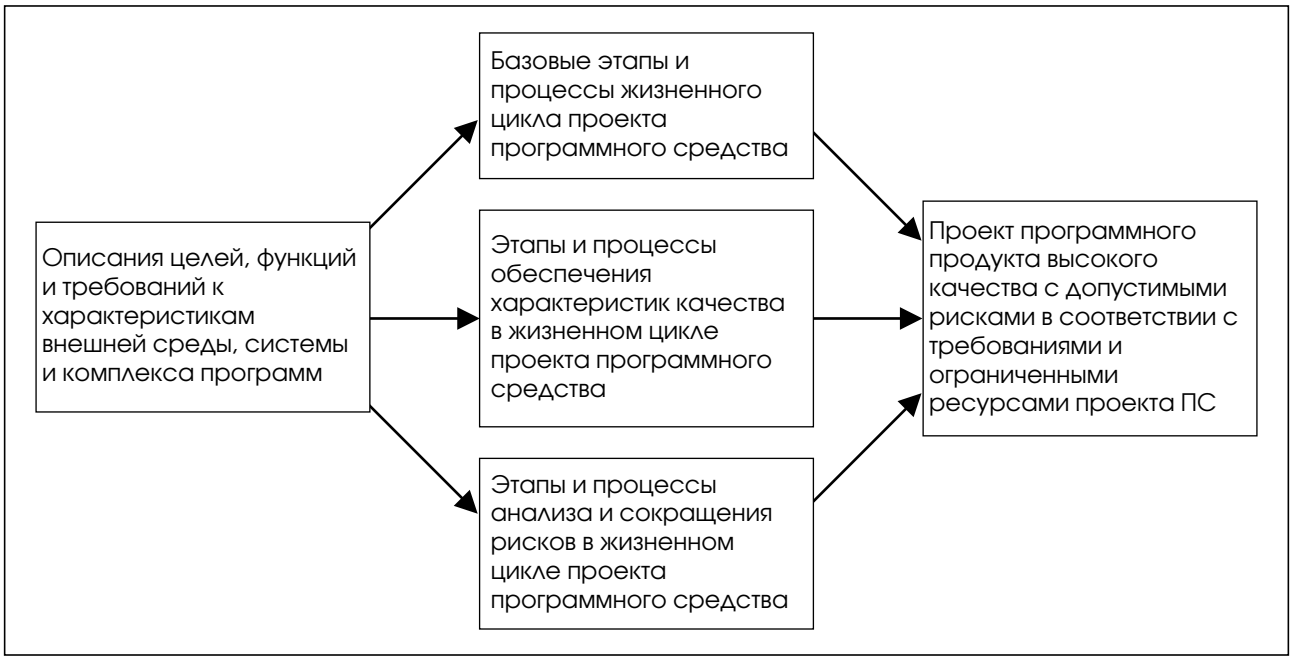


Рис. 5.

равление их рисками должны являться частью общей **проблемы обеспечения высокого качества проекта, предотвращения и сокращения рисков в системе и внешней среде**. Эти процессы состоят в выявлении возможных негативных отклонений характеристик комплекса программ и систем от требований контракта, технического задания и спецификаций, а также в создании базы для принятия мер по минимизации таких отклонений, с учетом ограниченных ресурсов на их реализацию и других факторов. При этом для каждого класса и категории рисков ПС следует определять характеристики, позволяющие контролировать их состояние и/или величину, а также отражение их последствий на риски характеристик и дефекты функционирования системы и объектов внешней среды. Для этого, при оценивании рисков ПС, их необходимо трансформировать в величины получающихся рисков для систем и среды, которые являются важнейшими и определяющими при применении комплексов программ (рис. 6).

Этап 2. Выделение, идентификация и анализ рисков в жизненном цикле программного средства включает**:**

- выделение возможных источников нарушения требований и ограничений ресурсов в жизненном цикле проекта ПС, определение критериев работоспособности и/или отказа системы;
- выделение, отбор и идентификация основных классов рисков в жизненном цикле проекта ПС, описание используемых предположений и ограничивающих условий при проведении анализа рисков;
- идентификацию и анализ причин, выделение категорий и возможных последствий проявления рисков функциональной пригодности проекта ПС;
- идентификацию и анализ причин, выделение категорий и возможных последствий проявления рисков конструктивных характеристик проекта ПС;
- идентификацию и анализ причин, выделение категорий и возможных последствий рисков нарушения ограничений доступных ресурсов для проекта ПС.

Основное содержание, размер и требуемое качество создаваемых ПС практически всегда определяют затраты и риски, связанные с их непосредственной разработкой. Влияние этой части затрат определяется наиболее сложным творческим процессом создания программ, который зависит от многих факторов. Накопленный опыт создания ПС и обобщение проведенных исследований позволили в [1, 3, 9, 10] выделить четыре основные **группы факторов**, влияющих на оценки затрат и рисков проектов при непосредственной разработке программ:

- факторы, отражающие особенности создаваемого комплекса программ **как объекта**

Рис. 6.

разработки, и требования к его функциональным характеристикам и качеству;

- факторы, определяющие **организацию процесса** разработки комплексов программ и его обеспечение квалифицированными специалистами;
- факторы, характеризующие **технологическую среду** и оснащенность инструментальными средствами автоматизации процесса разработки комплекса программ;
- факторы, отражающие оснащенность процесса создания ПС **аппаратурными вычислительными средствами**, на которых реализуются комплексы программ и базируются инструментальные системы автоматизации разработки.

В представленных четырех группах распределены факторы, которые наиболее важны при анализе рисков проектов ПС. В то же время имеющийся опыт показывает, что обычно отсутствуют отдельные, предсказуемые факторы или методы, способные изменять на порядок или более основные риски процесса разработки программ. Риски в ЖЦ ПС могут быть обусловлены **недостатками или непредумышленными, негативными действиями различных лиц**, участвующих в создании или применении системы и программного продукта. (Злоумышленные, враждебные действия заинтересованных лиц и защиты от них, при анализе и сокращении рисков ПС ниже не рассматриваются). Основными источниками непредумышленных рисков ПС, которые могут приводить к ущербу при их разработке и применении, являются:

- **заказчики,** определяющие назначение и функций системы и программного продукта, которые могут задавать некорректные или нереализуемые разработчиками требования к ним, а также ограничивают выделенные и доступные для проекта ПС бюджет, ресурсы, технологию и инструментальные средства;
- **разработчики** проекта системы и ПС, а также специалисты, обеспечивающие реализацию его ЖЦ, которые могут допускать дефекты и ошибки при обосновании проекта, не выполнять согласованные с заказчиком требования к характеристикам и качеству комплекса программ, а также превышать допустимое использование ресурсов, что может отражаться на проявлении и последствиях рисков на различных технологических этапах ЖЦ ПС и системы;
- **менеджеры и эксперты управления рисками** – координаторы взаимодействия заказчиков и разработчиков, которые уполномочены принимать решения о необходимости их снижения путем применения необходимых контрмер, а также о допустимости применения системы и/или ПС с прогнозируемыми или достигнутыми, конкретными уровнями рисков.

Косвенными источниками и причинами рисков функционирования ПС могут быть также **пользователи**, некомпетентно применяющие систему или программный продукт с отклонениями от требований документации по функциональной пригодности или с недопустимым использованием ресурсов при эксплуатации ПС.

Управление рисками, связанными с результатами разработки и применения ПС, должно представлять собой формализованный процесс, позволяющий **систематически идентифицировать, оценивать и смягчать факторы, угрозы и величину последствий возможных рисков**. В процессе управления проектом основное вни-

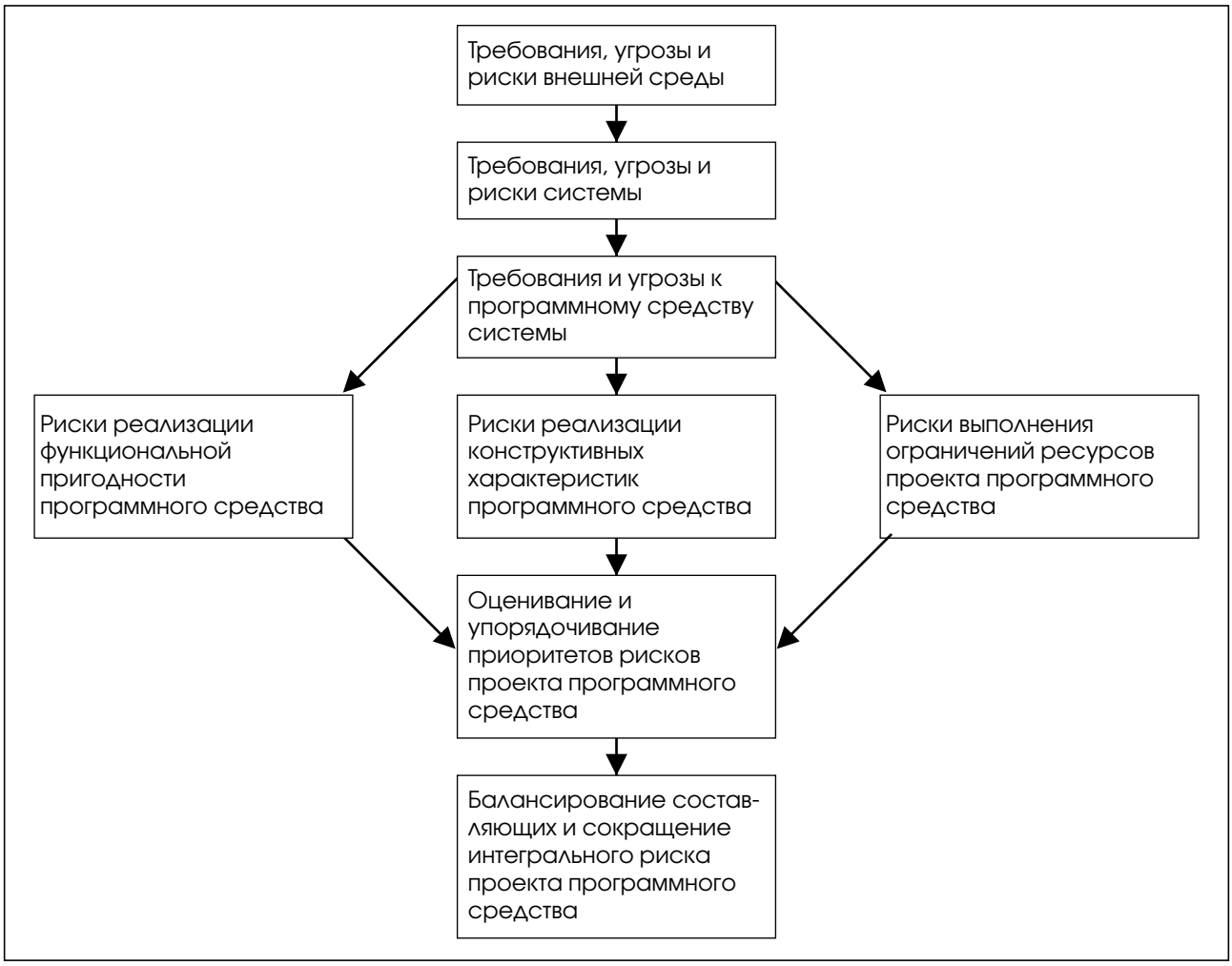


Рис. 7.

мание должно уделяться идентификации угроз и рисков в проекте, имеющих как внешние, так и внутренние причины, их количественную оценку, разработку откликов и контрмер для сокращения рисков и контроль реализации откликов. Риски при разработке и применении программного продукта могут негативно влиять на проект (в том числе на качество) всей системы. Это влияние может приводить к ухудшению (рис. 7) [4]:

- **функциональной пригодности,** назначения, состава и характеристик основных, функциональных задач, решаемых системой и ПС;
- **конструктивных характеристик** конечного программного продукта и результатов его применения для целей использования системы;
- **к нарушению ограничений доступных и используемых ресурсов**, к превышению допустимых затрат, нарушению сроков или же к полному срыву возможности реализации проекта ПС и системы в заданных ограниченных условиях.

Эти три базовые группы характеристик проектов систем и ПС тесно связаны между собой и определяют соответствующие классы рисков. Изменение каждого из них может влиять на другие риски. Риски функциональной пригодности имеют доминирующее значение и изменения двух других классов рисков обычно должны быть, в первую очередь, подчинены сокращению рисков функционирования системы и комплекса программ. Поэтому анализ рисков и возможных угроз целесообразно проводить систематизировано, начиная с рисков функциональной пригодности ПС. Ущерб, вследствие ошибок функциональных требований к проекту программного средства может проявляться двумя видами рисков: недостатками достигнутых **характеристик** ПС и рисков от нарушения огра-

ниченности доступных и используемых **ресурсов** в последующем жизненном цикле ПС.

В жизненном цикле ПС **важнейшим риском** является ущерб при невыполнении комплексом программ, формализованных в требованиях заказчика, назначения и функций главной характеристики качества — **функциональной пригодности** (рис. 8). Характеристики, определяющие функциональную пригодность сложных ПС, требуют для реализации каждой из них различных видов ресурсов и величин затрат. Все виды рисков процессов и продуктов ЖЦ ПС должны учитывать, прежде всего, их степень влияния на этот основной вид риска. Предъявление заказчиком необоснованных требований к функциональной пригодности, проявления в них конфликтов и внутренних противоречий в содержании функций и компонентов, при реально доступных ресурсах и возможных условиях внешней среды применения ПС, могут вызывать наиболее существенный ущерб в ЖЦ. В зависимости от назначения, функций, критичности и требований к системе и ПС может потребоваться либо полная ликвидация определенных или всех видов рисков, либо сокращение некоторых из них до допустимых пределов, либо игнорирование некоторых и сохранения на достигнутом уровне ущерба вследствие нарушения требований заказчика.

Риски реализации функциональной пригодности программного средства:

- цели проекта программного средства;
- назначения программного средства;
- функций программного средства;
- масштаба - размера программного средства;
- сложности программного средства;
- архитектуры программного средства.

Риски реализации конструктивных характеристик программного средства:

- корректности программ;
- способности компонентов к взаимодействию;
- защищенности – безопасности программного средства;
- надежности – готовности программного средства;
- временной эффективности функционирования программного средства;
- практичности – изучаемости программного средства;
- сопровождаемости – изменяемости версий программного средства;
- мобильности – переносимости программного средства.

Риски выполнения ограничений доступных ресурсов проекта программного средства:

- экономических и трудовых затрат на реализацию проекта программного средства;
- плановых и временных ресурсов на реализацию проекта программного средства;
- квалификации коллектива специалистов проекта программного средства;
- технических, вычислительных ресурсов для реализации и функционирования программного средства;
- технологических – инструментальных ресурсов на обеспечение жизненного цикла программного средства.

Рис. 8.

Цель и назначение ПС детализируются и формализуются в **требованиях к функциям** компонентов и всего комплекса программ, способного реализовать декларированные цели при отсутствии или с допустимыми рисками:

- соответствие комплекса программ функциям системы;
- соответствие автоматизируемых функций и комплексов задач назначению ЖЦ ПС;
- общие технические требования к реализации функций, компонентов и задач ПС.

Адекватность и полнота отражения требуемыми функциями, сформулированного назначения ПС, является характеристикой, определяющей потенциальную возможность реализации его функциональной пригодности в целом. Прослеживание детализации и покрытия целей, требованиями к функциям компонентов сверху вниз (начиная от целей ПС и системы), а также конкретизация и корректировка целей снизу вверх от потенциально реализуемых функций должны обеспечивать адекватность и качество этой части декларируемой основы функциональной пригодности [2, 8].

Функции ПС реализуются в определенной аппаратной, операционной и пользовательской внешней среде системы, характеристики которых существенно влияют на функциональную пригодность. Для выполнения требуемых функций комплекса программ необходима **адекватная исходная информация от объектов внешней среды**, содержание которой должно полностью обеспечивать реализацию декларированных функций. Полнота формализации номенклатуры, структуры и качества входной информации для выполнения требуемых функций является одной из важных составляющих при определении

функциональной пригодности ПС и сокращения рисков в соответствующей внешней среде.

Цель и функции ПС реализуются тогда, когда **выходная информация** достигает потребителей — объектов или операторов-пользователей, с требуемым содержанием и качеством, достаточным для обеспечения их эффективного применения. Степень покрытия всей выходной информацией: целей, назначения и функций ПС для пользователей, следует рассматривать как **основную меру рисков функциональной пригодности**. Прослеживание и оценивание адекватности и полноты состава выходной информации снизу вверх к назначению ПС должны завершать выбор базовых характеристик функциональной пригодности, независимо от сферы применения системы.

При начальном формировании требований к функциональной пригодности комплекса программ практически невозможно достоверно предусмотреть сбалансированное выделение каждого вида ресурса для полной реализации каждой требуемой характеристики. Кроме того, требования заказчика к функциям всегда субъективны и не стабильны, что также отражается на изменении рисков при разработке и модификациях ПС [2, 8, 9]. При этом некоторые характеристики в реальном проекте ПС могут приобретать значения более высокие, чем действительно требуются, на что нерационально расходуются ресурсы, а другие — не удовлетворять требованиям контракта и технического задания. Для разрешения этого противоречия основное значение имеет деятельность менеджера рисков, который должен быть способен прогнозировать, проводить поэтапный анализ, контроль, оценивание и мониторинг возможных и реальных отклонений от требуемых характеристик и используемых ресурсов, **управление контрмерами и последовательное изменение их для сокращения и минимизации интегрального риска** всей системы.

Анализ и сокращение рисков конструктивных характеристик сложных ПС должен сопровождать весь их жизненный цикл (см. рис. 8, перечень в соответствии со стандартом **ISO 9126**). Для этого необходимо контролировать области возможного возникновения рисков, оценивать вероятности их проявления, виды и степень влияния угроз, которые следует минимизировать как можно раньше по мере их возникновения и обнаружения в процессах жизненного цикла ПС. Основной эффект по снижению рисков конструктивных характеристик должен достигаться на начальных этапах разработки, когда возможно предотвращение или сокращение многих из них с минимальными затратами времени и других ресурсов. Для этого в **технологическом процессе разработки** необходимо использовать **методы, которые включают**:

- определение ценности (приоритета) и выделение каждой требуемой конструктивной характеристики для реализации необходимой функциональной пригодности системы и ПС;
- систематизацию, документирование и оценивание эффективности доступных методов, средств и ресурсов контрмер для сокращения рисков функциональной пригодности и выделенных конструктивных характеристик ПС;
- определение приоритетов конструктивных характеристик качества, компонентов и этапов ЖЦ проекта ПС, которые имеют потенциальные технические, стоимостные или плановые риски;
- оценивание вероятности каждого вида угроз конструктивной характеристики качества, потенциальной величины и вероятности их возможного негативного воздействия на каждую характеристику функциональной пригодности системы и ПС;
- оценивание уязвимости и последствий дефектов каждой конструктивной характеристики и затрат ресурсов для восстановления требуемой функциональной пригодности системы и ПС при проявлении рисков;
- планирование и разработку решений по контрмерам для обеспечения допустимого уровня интегрального риска функциональной пригодности и конструктивных характеристик системы, в том числе возможно за счет изменения требований к системе и ПС и доступных ресурсов;
- оценку вероятностей сокращения рисков конструктивных характеристик качества до допустимых пределов при реализации процессов разработки и всего ЖЦ программного средства с учетом доступных ресурсов.

Улучшение каждой **конструктивной характеристики качества** требует затрат ресурсов, которые в той или иной степени должны отражаться на основной характеристике ПС — на функциональной пригодности. Эти конструктивные характеристики имеют значение для проекта постольку, поскольку они обеспечивают требуемое качество реализации основного назначения и функций ПС. При выборе конкретных мер допустимых, конструктивных характеристик следует учитывать возможные за-

траты ресурсов на их достижение и на результирующее повышение функциональной пригодности, желательно, в сопоставимых экономических единицах, в тех же мерах и масштабах. Такое качественное сравнение эффекта и затрат, даже приблизительно, позволяет избегать многих нерентабельных завышений требований к отдельным конструктивным характеристикам, которые не достаточно отражаются на адекватном улучшении функций ПС. Поэтому для каждого проекта необходимо ранжировать характеристики (приоритеты) и выделять, прежде всего, те, которые могут в наибольшей степени улучшить функциональную пригодность для конкретных целей.

Решение этих задач должно быть направлено на обеспечение высокой функциональной пригодности ПС **путем сбалансированного улучшения остальных, конструктивных характеристик в условиях ограниченных ресурсов на ЖЦ**. Для этого в процессе системного анализа при подготовке технического задания и требований спецификаций значения и риски конструктивных характеристик должны выбираться с учетом опасности их влияния на функциональную пригодность. С позиции опасности угроз и возможного риска целесообразно выделять конструктивные характеристики объективно опасные, возможно опасные при определенных условиях и допустимые для игнорирования. Излишне высокие требования к отдельным конструктивным характеристикам качества, требующие для реализации больших дополнительных трудовых и вычислительных ресурсов, целесообразно снижать, если они слабо влияют на основные, функциональные характеристики ПС.

Для управления рисками с целью минимизации и выделения наиболее опасных из них необходимо сопоставлять вероятности (частости) и последствия проявления, как рисков функциональных характеристик комплекса программ, так и рисков ресурсов. Для каждого проекта ПС эти виды рисков могут различно влиять на **интегральный ущерб** – риск в ЖЦ ПС, отражающийся общим риском системы. Применяемые методы оценивания и анализа величин и вероятности рисков должны позволять определять приоритеты видов рисков с целью выделения соответствующей доли **ресурсов на контрмеры** для сбалансированного сокращения негативных последствий различных видов рисков.

Риски ограничений доступных и используемых ресурсов в ЖЦ ПС могут включать (см. рис. 8):

- экономические риски – превышение разработчиком обоснованных, допустимых по контракту размеров стоимости, трудоемкости и эксплуатационных затрат на программные компоненты и ПС в целом, которые могут также отражаться на их функциональной пригодности и других характеристиках качества;
- плановые риски – нарушение разработчиком допустимых временных затрат в графиках работ, сроков реализации этапов и проекта в целом, а также распределений задач по подрядчикам, подразделениям и специалистам, что может также увеличивать риски характеристик ПС;
- кадровые риски – недостаточная квалификация специалистов, отражающаяся на качестве разработки, совершенствования и/или применения ПС;
- технические риски – недостаточность вычислительных ресурсов, несогласованность ресурсов внутренней и внешней среды для реализации основных функций ПС, что может иметь как самостоятельное значение, так и влияние на их риски;
- технологические риски – недостаточное качество инструментария для автоматизации всего ЖЦ ПС и технологических процессов, предназначенных для обеспечения гарантированного сокращения рисков конечного программного продукта.

Последствия ошибок использования доступных ресурсов и технико-экономического обоснования проекта определяют значительную долю различных рисков ПС, могут катастрофически отражаться на всех этапах разработки и даже полностью определять реализуемость проекта. Прямые риски, обусловленные ошибками заданных экономических характеристик, могут причинить ущерб заказчику при **завышении стоимости проекта** относительно реально необходимой или ущерб разработчикам, если **стоимость оценена недостаточной** для его успешной реализации. Эти риски могут уменьшаться при последовательном уточнении размера ПС на этапах формирования требований, предварительного и детального проектирования, однако они не полностью учитывают реальное влияние ограничений ресурсов на процессы и риски разработки и конечного программного продукта. Поэтому риски нарушения ограничений доступных ресурсов проекта ПС целесообразно оценивать по их последующему отражению на степень возможной реализации требований заказ-

чика в конечном программном продукте. По мере уточнения размера — масштаба и развития проекта комплекса программ эти риски уменьшаются, однако обычно их влияние остается существенным в процессе всего жизненного цикла ПС.

Этап 3. Оценивание опасности рисков и выбор эффективных контрмер для их сокращения включает:

- оценивание возможных последствий, уровней потенциальных опасностей и приоритетов каждого класса и категории рисков проекта ПС;
- выделение и упорядочение ограниченной группы наиболее опасных, высокоприоритетных рисков проекта ПС;
- планирование методов и необходимых ресурсов реализации эффективных контрмер для сокращения каждой категории опасных, приоритетных рисков проекта ПС;
- анализ, определение стратегии и распределение ресурсов на контрмеры для сбалансированного сокращения интегрального риска проекта ПС с учетом приоритетов опасных рисков;
- распределение ответственности специалистов за реализацию сокращения конкретных опасных рисков проекта ПС.

Для учета влияния рисков на функциональную пригодность и другие характеристики ПС, а также для выбора контрмер целесообразно ранжировать риски **относительными величинами – приоритетами.** Величины и вероятности проявления этих рисков, а также ресурсы контрмер для их сокращения, желательно оценивать соизмеримыми экономическими, стоимостными категориями, или унифицированными относительными количественными величинами — приоритетами (например, по шкале от 1 до 10), или качественными показателями (катастрофический, критический, допустимый — высокий, средний, низкий). Подобные рейтинги рисков с оценкой их вероятностей и последствий особенно необходимы для оценивания, сбалансированного прогнозирования и последовательной минимизации интегральных рисков и **мониторинга различных контрмер** в проектах ПС. Интегральный риск проекта можно оценивать как результат обобщения всех видов рисков с учетом их относительного влияния на функциональную пригодность и другие важнейшие характеристики системы и ПС. Такой риск может оцениваться, например, суммой приоритетов рисков характеристик ПС, а также суммой приоритетов рисков из-за ограниченности ресурсов проекта. Такие, даже экспертные, качественные оценки позволяют прогнозировать и выявлять наиболее крупные и опасные риски, их долю в интегральном риске проекта ПС и системы, а также рентабельность контрмер для их снижения [14].

Для **выбора критического уровня допустимых рисков** необходимо исследовать возможные начальные события и особенности системы, последовательность потенциально опасных событий, любые смягчающие факторы и характеристики, а также природу и частоту возможных негативных последствий идентифицированных угроз в ПС и в системе. Методы, используемые для оценки величины риска, обычно являются количественными, несмотря на то, что степень детализации при подготовке исходной информации зависит от конкретного применения. Однако полный, количественный анализ не всегда возможен, вследствие недостатка информации о системе, подвергающейся анализу, отсутствия или недостатка данных о характеристиках возможных отказов, влиянии человеческого фактора. При этом для сбалансированного снижения интегрального риска, может оказаться эффективным сравнительное, количественное или качественное ранжирование рисков (присвоение им приоритетов) специалистами, хорошо информированными в данной области систем.

Используя **планы управления проектом ПС и рисками**, менеджер должен осуществлять распределение ресурсов контрмер, направленных на преодоление негативных случайностей. На начальных этапах жизненного цикла разработки ПС, инвестиции в проект постепенно растут вплоть до формулирования конкретных требований. Наряду с разработкой требований, исследование концепции ПС и системы представляют первые этапы жизненного цикла. В течение этих этапов планирование проекта оказывает наибольшее влияние на контрмеры управления и сокращения рисков. Для обеспечения требуемого качества ПС необходима **организация контрмер** в процессе управления рисками. Задача менеджера рисков состоит в выявлении и идентификации источников рисков, противоречий требований характеристик и ресурсов для их реализации и в предложении заказчику и разработчикам **рациональных и возможных контрмер**, обеспечивающих сокращение рисков до допустимых пределов. Контрмеры для сокращения рисков можно разделить на три типа:

- сокращение или исключение **первичных причин – угроз**, дефектов и ошибок в компонентах и комплексе программ, обусловленных недостатками их проектирования, разработки или модификации, отражающихся на рисках функциональной пригодности или характеристик ПС;
- сокращение или ликвидация **уязвимости** компонентов программ и данных при воздействии на них угроз, дефектов и ошибок, путем введения в ПС средств защиты для блокирования их возможного негативного воздействия на риски функционирования и применения комплекса программ;
- непосредственное изменение и сокращение последствий **проявления рисков** функциональной пригодности и характеристик ПС, путем их оперативного обнаружения и ликвидации ущерба при сохранении (возможно) вызывающих их первичных источников и причин.

Для выработки плана анализа рисков и применения контрмер при их сокращении должна быть определена и документально установлена **методика применения последовательного анализа угроз, уязвимостей и изменения проявления рисков.** Если менеджеры проекта имеют достаточно большой опыт работы, а процессы развития проекта регламентированы и ведут себя предсказуемо, количество дефектов и угроз последовательно убывает и степень риска в ЖЦ проекта ПС должна уменьшаться. Последние этапы – эксплуатация и сопровождение обычно отличаются наименьшими значениями остаточного риска, связанными с внутренними дефектами и угрозами вследствие разработки ПС.

После того как менеджеры проекта идентифицируют риски в жизненном цикле разработки ПС, а также уточнят тактику итераций применения контрмер по сокращению их влияния, возникает необходимость в **идентификации уровня допустимости остаточного риска**. В зависимости от требований к характеристикам ПС, уровни допустимости рисков и контрмер могут варьироваться от качественных оценок до итерационных действий, предполагающих использование альтернативных подходов и дополнительных, последовательных разработок контрмер для более полного сокращения рисков.

Этап 4. Сокращение и ликвидация опасных рисков проекта программного средства включает:

- реализацию выбранных контрмер для сокращения последствий интегрального риска путем снижения или исключения проявления наиболее опасных категорий рисков проекта ПС и составление поэтапных отчетов о состоянии проекта;
- корректировку при необходимости требований к функциональной пригодности, конструктивным характеристикам и ограничениям ресурсов для обеспечения допустимого интегрального риска проекта ПС;
- обобщение и регистрация результатов сокращения интегрального риска на очередном этапе проекта ПС.

После предварительного проектирования первичные дефекты – угрозы отходят на второй план и определяющими становятся непосредственные риски функций и конструктивных характеристик комплекса программ. На эти риски непосредственно влияют соответствующие им выделенные ресурсы для разработки и всего жизненного цикла ПС, от которых зависят возможные контрмеры для их снижения. Совместное влияние на реализацию требований заказчика к проекту ПС, рисков характеристик программ и ресурсов для их реализации должно быть **сбалансировано контрмерами допустимого изменения** тех и других видов рисков. В крайнем случае, если интегральный риск остается недопустимо большим, возможна, по согласованию с заказчиком, **корректировка требований или выделяемых ресурсов** (рис. 9).

На этапах предварительного проектирования ПС заказчик совместно с разработчиком подготавливают исходные требования к характеристикам проекта комплекса программ и ограничения для ресурсов, которые могут быть использованы для его реализации и применения. Эти требования и ограничения могут не полностью выполняться на последующих этапах ЖЦ ПС, что приводит к ущербу у заказчиков и пользователей. Причинами такого ущерба могут быть ошибки, а также завышенные заказчиком требования к характеристикам ПС, которые не могут быть реализованы при выделенных ресурсах, или недостаточное качество технологии и квалификация специалистов – разработчиков, исполняющих проект.

Для сокращения интегрального риска до допустимого значения возможно изменение требований к функциональным и конструктивным характеристикам и/или к используемым ресурсам в технологических процессах ЖЦ ПС.

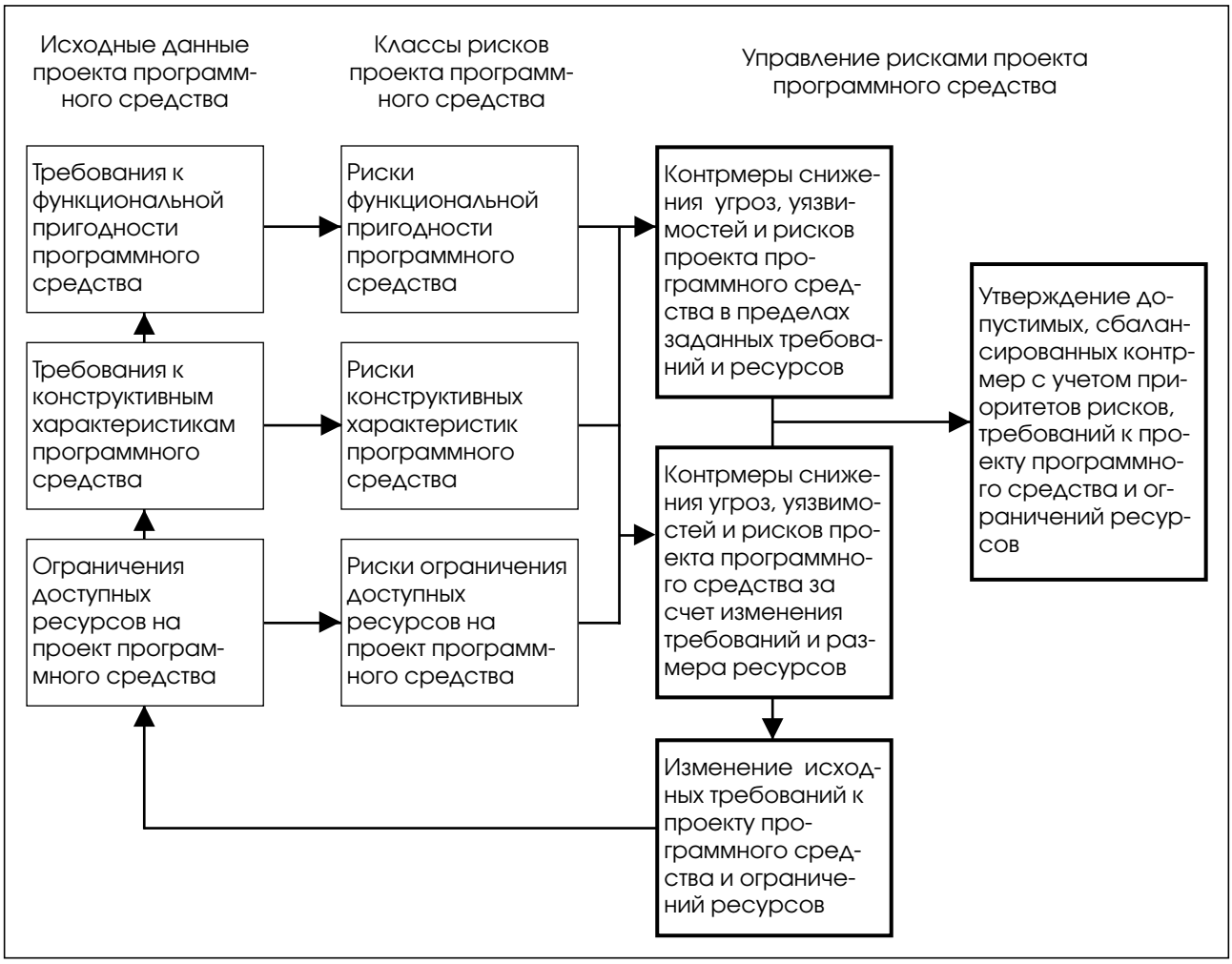


Рис. 9.

При этом для обеспечения требуемой функциональной пригодности и минимального интегрального риска разработчиками возможно применение **первой стратегии контрмер сокращения рисков** (см. рис. 9):

- изменение соотношения между отдельными, достигаемыми функциональными и конструктивными характеристиками ПС в пределах согласованных требований, зафиксированных в техническом задании и спецификациях;
- изменение соотношения между используемыми ресурсами в пределах, заданных исходными ограничениями на их применение.

Таким образом, при управлении контрмерами рисков по первой стратегии необходимо обеспечить соответствие достигнутых функциональных и конструктивных характеристик требованиям, которые были первоначально установлены в процессе их разработки. Для этого могут быть перераспределены имеющиеся ресурсы с целью реализации требуемых отдельных характеристик, и тем самым, в частности, уменьшены риски, с наибольшими значениями или ограничены их последствия. Однако если при первой стратегии не обеспечивается допустимый минимальный интегральный риск и требуемая функциональная пригодность, то **по согласованию с заказчиком, разработчиками** может применяться **вторая стратегия контрмер сокращения рисков** (см. рис. 9):

- пересмотр и изменение исходных требований к совокупности функциональных и конструктивных характеристик проекта ПС и уменьшение за счет этого результирующих значений рисков;
- пересмотр и изменение некоторых ограничений требуемых и используемых ресурсов и технологии обеспечения жизненного цикла ПС для получения допустимых рисков.

При этой стратегии эффект может быть достигнут пересмотром и снижением требований к характеристикам ПС, имеющим наибольшие риски или увеличением отдельных доступных ресурсов и совершенствованием технологии, отражающихся на необходимом сокращении этих рисков. Если интегральные риски обусловлены недостаточной величиной одного из видов ресурса, то приходится перераспределять доступные ресурсы или искать заказчику способы увеличения некоторого критического ресурса. В результате изменения характеристик ПС и ресурсов, выделяемых на этапы их жизненного цикла, должны достигаться сбалансированные значения их рисков и минимизироваться интегральный риск комплекса программ и системы. В соответствие с их значениями следует откорректировать и утвердить обновленные, экономически и функционально оправданные, требования к характеристикам, используемым ресурсам и технологии проекта ПС. При обеих стратегиях **наиболее стабильными должны быть требования к функциональной пригодности комплекса программ**, изменения которых допустимы при исчерпании возможностей сокращения интегральных рисков за счет изменения конструктивных характеристик качества, используемых ресурсов и других контрмер.

Риски должны анализироваться **итерационно на всех крупных этапах жизненного цикла ПС**, определяться их приоритеты с учетом графика работ, причем текущий список наибольших рисков следует выделять и оглашать на собрании специалистов, на котором рассматривается текущее состояние проекта ПС. Умение оценивать и обрабатывать риски является основным в деятельности любого менеджера проекта программного продукта. Для менеджеров проектов ПС эти навыки представляются важнейшими, поскольку упущения в этой сфере могут катастрофически влиять и блокировать усилия, направленные на успешное выполнение проекта всей системы, использующей ПС. Следует учитывать, что программные проекты постоянно усложняются, развиваются и модифицируются, вследствие чего весьма затруднительно рассматривать продукт как единое стабильное целое.

В некоторых случаях процессы анализа и сокращения рисков могут быть значительно упрощены [14]. Для этого целесообразно выделять и контролировать только отдельные (2 — 3), наибольшие по величине последствий и по вероятности проявления риски отклонения от требований и минимизировать возможный в результате ущерб для функциональной пригодности в ЖЦ системы и ПС. Подобный упрощенный анализ полезен на начальных этапах проектирования систем и может давать значительный экономический эффект для последующего совершенствования всего ЖЦ проектов ПС.

В процессах устранения рисков сложных ПС может участвовать большое число специалистов различных направлений и квалификации, которые, при необходимости, могут объединяться в **службу сопровождения и управления конфигурацией ПС** [3, 9, 15] (см. стандарт **ISO 15846** — Процессы жизненного цикла программных средств. Конфигурационное управление программными средствами). Структура такой службы зависит от сложности и фазы развития проекта, от структуры фирмы, от ее взаимодействия с заказчиком и субподрядчиками и от ряда других факторов. При организации сложного проекта следует идентифицировать инстанцию, уполномоченную утверждать изменения ПС. Необходимо установить **полномочия специалистов** для санкционирования и выполнения изменений рисков и контрмер на каждом уровне проекта ПС: последовательность работ, которые необходимо выполнить для того, чтобы запросить разрешение на изменение; обработать запрос на изменение, проследить изменение, распределять изменения и сопровождать предыдущие версии.

Основной задачей управления конфигурацией ПС является документальное оформление и обеспечение полной наглядности выполняемых изменений, текущей конфигурации программ и данных и степени выполнения требований к их функциональной пригодности и конструктивным характеристикам при сокращении рисков. Другая задача заключается в том, чтобы все лица, работающие над проектом, в любой момент его жизненного цикла использовали достоверную и точную информацию о всех единицах конфигурации проекта и их взаимодействии. Изменения конфигурации ПС и его компонентов при сокращении рисков должны планироваться и предусматривать действия с четкими разделами:

- **почему** и с какой целью производится корректировка программ или данных;
- **кто** персонально выполняет, оценивает риски и контрмеры, санкционирует и утверждает проведение изменений ПС или компонентов;
- **какие** действия и процедуры должны быть выполнены для реализации изменений конфигурации ПС;

- **когда** по срокам и в координации с какими другими процедурами ЖЦ следует реализовать определенную корректировку конфигурации ПС;
- **как** и с использованием каких методов, средств и ресурсов должны быть выполнены запланированные изменения ПС и компонентов.

Приоритет результатов выполнения контрмер и каждого предлагаемого изменения рисков программ и данных целесообразно оценивать по следующим критериям:

- насколько данное изменение риска может улучшить эксплуатационные характеристики и функциональную пригодность ПС в целом;
- каковы затраты на выполнение корректировок ПС при создании новой версии и их распространение пользователям вследствие изменения рисков;
- какова срочность извещения пользователя о разработанной корректировке и целесообразно ли ее распространять до подготовки очередной базовой версии ПС;
- для какого числа пользователей может быть полезно данное изменение риска;
- как данное изменение риска отразится на эксплуатации пользователями предыдущих версий ПС;
- насколько подготовка и внедрение данного изменения ПС может отразиться на сроках создания очередной версии.

При выделении реализуемых изменений рисков приходится решать оптимизационную задачу по оценке и сопоставлению ущерба от того, что изменение не проведено и не повышается качество функционирования ПС, по сравнению с затратами ресурсов на проведение изменений и возможным риском — ущербом, если они содержат дефекты. Селекция проводимых изменений в версиях сложных ПС требует формализации этого процесса и документирования предполагаемых и утвержденных изменений рисков и контрмер.

Этап 5. Контроль, мониторинг и утверждение допустимого интегрального риска программного средства включает:

- контроль, отслеживание и мониторинг реализации сокращения интегрального риска по этапам жизненного цикла проекта ПС;
- мониторинг состояния проекта комплекса программ и утверждение интегрального риска по этапам жизненного цикла ПС и системы;
- документирование и утверждение допустимого интегрального риска по этапам жизненного цикла проекта ПС и системы;
- оформление итогового отчета по результатам анализа и сокращения рисков ПС и системы.

Перечисленные процессы этого этапа являются достаточно типовыми для контроля, мониторинга и утверждения значений любых измеряемых характеристик ПС, и в том числе при регистрации изменений рисков. Они регламентируются общими стандартами жизненного цикла ПС, в частности, **ISO 12207** и **ISO 15504**. В каждом конкретном проекте в зависимости от его особенностей они могут детализироваться и уточняться в технологических инструкциях и руководствах для менеджеров и экспертов по анализу и управлению рисками.

Для **обеспечения процесса контроля, регистрации и мониторинга изменений рисков** (см. стандарт **ISO 14764** — Сопровождение программных средств) специалисты должны разработать, документально оформить и поэтапно выполнять план корректировок программ и данных в результате контрмер и сокращения рисков. На основе проведенного анализа персонал сопровождения должен разработать варианты реализации изменений и документально оформить: сообщение о каждом дефекте или проявлении риска; результаты анализа рисков и варианты реализации контрмер, оценку последствий рисков и их влияния на функциональную пригодность ПС. Персонал сопровождения должен провести анализ и определить, какие документы, программные модули или их версии требуют корректировок, получить подтверждение того, что каждое вносимое изменение удовлетворяет требованиям к ПС, установленным в договоре.

Для конкретного проекта должны быть определены и зафиксированы **правила управления конфигурацией и утверждения интегрального риска версий ПС**, применения административных и технологических процедур их мониторинга на всем протяжении жизненного цикла программного средства для:

- идентификации, определения и регистрации конфигурации и изменений программного средства в системе;
- управления конфигурацией, модификацией и выпуском версий программных продуктов с результатами сокращений интегрального риска;
- фиксирования конфигурации и сообщений о состоянии версий программных средств и

их компонентов после утверждения интегрального риска;
- управления и контролирования хранения, обращения и поставок версий программных средств после реализации контрмер и достижения допустимого риска.

Документирование и утверждение допустимого интегрального риска и выполненных изменений ПС значительно влияет на достигаемую функциональную пригодность сложных комплексов программ. Организация документирования должна определять стратегию, стандарты, процедуры, распределение ресурсов и планы создания, изменения и применения документов на программы и данные. Для этого в общем случае должны быть выделены **специалисты**, которые должны планировать, утверждать, выпускать, распространять и сопровождать комплекты утвержденных документов на ПС. Они должны стимулировать разработчиков программных средств, осуществлять непрерывное, регламентированное документирование процессов и результатов своей деятельности, а также контролировать полноту и качество утвержденных отчетных документов. Структура документации и формы отдельных документов, используемых для конфигурационного управления и регистрации сокращения рисков программ, должны позволять:
- точно документально описывать и идентифицировать каждую утвержденную версию программных компонентов и ПС в целом в любое время на всем протяжении их жизненного цикла;
- надежно учитывать и регистрировать все подготовленные и утвержденные контрмеры и корректировки рисков в версиях ПС;
- снабжать руководителей проекта обобщенной и детальной информацией для принятия решений на изменения рисков программ, а также для контроля выполнения принятых контрмер;
- обеспечивать заказчиков и пользователей объективными сведениями о наиболее существенных контрмерах, изменениях рисков, корректировках программ и о новых версиях ПС.

Методика оформления итоговых отчетов о выявленных дефектах, устраненных рисках и предложениях по корректировке версий ПС должна содержать рекомендации испытателям и пользователям по выявлению, регистрации и формализации условий проявления и содержания обнаруженных дефектов испытываемых и/или эксплуатируемых версий ПС. Методика должна включаться в состав эксплуатационной документации и передаваться каждому пользователю версии ПС. В методике следует стимулировать специалистов-пользователей, анализировать, подготавливать и представлять заказчику и разработчикам рекомендации по сокращению рисков, совершенствованию качества и развитию основных функций поставляемых версий ПС.

При применении методики анализа и сокращения рисков в жизненном цикле программных средств следует учитывать, что вследствие недостаточной квалификации специалистов возможны дополнительные (ложные) обнаружения рисков, обусловленных дефектами, ошибками или некорректным выполнением технологических процедур при управлении рисками. Эти риски не зависят непосредственно от характеристик ПС и внешней среды, однако могут провоцировать нерентабельную деятельность разработчиков по их выявлению, анализу и устранению. Такие проявления рисков могут быть обусловлены:
- дефектами и ошибками экспертов при идентификации характеристик вероятности и возможных последствий реальных рисков;
- субъективными ошибками оценивания степени опасности (завышения или занижения) угроз и уязвимости компонентов ПС и системы, а также необходимых контрмер для сокращения рисков;
- излишним оптимизмом руководителей и экспертов при оценивании достигнутого сокращения или устранения угроз и рисков;
- дефектами пользовательской документации технологических процессов и инструментов для анализа и сокращения рисков.

Приложение 1.

Термины и определения

Риск — негативные события и их величины, отражающие потери, убытки или ущерб от процессов или продуктов, вызванные реализацией угрозы при наличии уязвимости и определенных обстоятельств или событий, приводящих к реализации угрозы при недостатках обоснования, проектирования, разработки и всего жизненного цикла комплексов программ. Риски проявляются, как негативные последствия функционирования и применения ПС, в результате отклонения характеристик объектов или процессов от заданных требований заказчика, согласованных с разработчиками, которые способны причинить ущерб системе, внешней среде или пользователю.

Объекты оценки рисков — программные средства, компоненты системы, результаты ее работы или вся система в целом, включая администратора, пользовательскую документацию и руководства, которые рассматривается на предмет оценки качества, защищенности и безопасности.

Анализ рисков — процесс определения источников и количественной оценки риска, угроз, уязвимостей, возможного ущерба, а также контрмер для его уменьшения. Процесс идентификации рисков, определение их величины и выделение областей, требующих защиты или контрмер, часть процессов управления рисками, систематический процесс и мониторинг оценки величины рисков, обеспечивающий базу для оценивания мероприятий по снижению риска. Формальное описание событий, ущерб от которых может произойти и иметь отношение к проекту.

Оценка риска — процесс идентификации программных и информационных ресурсов системы и угроз этим ресурсам, возможных потерь, основанный на оценке частоты возникновения рисковых событий и возможном при этом размере ущерба. Изучение угроз, уязвимостей, вероятности возможных потерь и возможной эффективности контрмер, позволяющих минимизировать возможные потери. Процесс оценки должен описываться по общедоступной методике для сравнения оцененного риска с определенными критериями с целью определения значимости риска для его обработки и сокращения, оценивания и присвоения значений вероятности и величины последствий риска.

Управление рисками — процесс идентификации, управления, устранения или уменьшения вероятности событий, которые могут негативно воздействовать на ПС, систему и внешнюю среду, действия, осуществляемые для выполнения решений по мониторингу и сокращению рисков. Процесс включает анализ риска, анализ стоимости/эффективности контрмер, выбор, построение и испытание подсистемы обеспечения безопасности, исследование всех аспектов рисков системы. Цель процедуры управления риском состоит в том, чтобы уменьшить риски до уровней, одобренных лицом, уполномоченным утверждать допустимые риски.

Угроза — обстоятельства, дефекты или события, которые потенциально могут причинить ущерб ПС или системе в форме разрушения, раскрытия, модификации данных или отказа в обслуживании. Потенциальная причина нежелательного инцидента, который может заканчиваться причинением ущерба ПС, системе или внешней среде. Способности, намерения и методы атаки заинтересованных лиц, имеющих возможность воспользоваться совокупностью обстоятельств, позволяющих использовать имеющийся потенциал для причинения ущерба.

Уязвимость — пробел (слабость) в процедурах защиты, проектировании, реализации ПС и системы, внутренней системе управления, который может способствовать нарушению политики обеспечения качества и сокращения рисков. Успех угрозы зависит от степени уязвимости, потенциала угрозы (атаки) и эффективности используемых контрмер. Уязвимость — существование дефектов построения ПС и системы, которые могут вести к неожиданному, нежелательному событию, компрометирующему систему безопасности или функции ПС, могут приводить к реализации угроз и проявлению ущерба — риска или к нарушениям в критически важном процессе.

Анализ уязвимости — систематически проводимая экспертиза качества и пробелов ПС и системы, позволяющая идентифицировать погрешности в их построении, собирать исходные данные, чтобы оценивать эффективность предложенных контрмер защиты и подтверждать адекватность таких мер после их реализации.

Менеджмент риска — скоординированные действия по руководству и управлению организацией сокращения рисков включает оценку рисков, обработку рисков, принятие и утверждение допустимых рисков.

Работоспособное состояние — состояние, при котором значения всех параметров, характеризующих способность выполнять заданные функции, соответствуют требованиям нормативно-технической и/или конструкторской и проектной документации.

Неработоспособное состояние — состояние, при котором значение хотя бы одного параметра, характеризующего способность выполнять заданные функции, не соответствует требованиям нормативно-технической и/или конструкторской и проектной документации.

Отказовая ситуация — скрытый отказ, не обнаруживаемый визуально или штатными методами, средствами контроля и диагностирования, но выявляемый средствами автоматизированного рестарта, а также при проведении технического обслуживания, который потенциально может превратиться в отказ.

Отказ — негативное событие, заключающееся в нарушении работоспособного состояния ПС, системы или внешней среды, или защитного состояния с большим ущербом.

Литература

1. Кантор М. Управление программными проектами. Практическое руководство по разработке успешного программного обеспечения. Пер. с англ. — М.: Вильямс. 2002.
2. Леффингуэлл Д., Уидриг Д. Принципы работы с требованиями к программному обеспечению. Унифицированный подход. Пер. с англ. — М.: Вильямс. 2002.
3. Липаев В.В. Методы обеспечение качества крупномасштабных программных средств. — М.: РФФИ. СИНТЕГ. 2003.
4. Липаев В.В. Функциональная безопасность программных средств. — М.: СИНТЕГ. 2004.
5. Нупур Д., Хамфри У., Редвайн С., Цибульски Г., Макгро Г. Процессы разработки безопасного программного обеспечения. Открытые системы. № 08. 2004.
6. Оценка и аттестация зрелости процессов создания и сопровождения программных средств и информационных систем (ISO/IEC TR 15504 — CMM). — М.: Книга и бизнес. 2001.
7. Симонов С. Технологии и инструментарий для управления рисками. Jet Info. № 2. 2003.
8. Тэллес М., Хсих Ю. Наука отладки. — М.: Кудиц-образ. 2003.
9. Фатрелл Р. Т., Шафер Д. Ф., Шафер Л. И. Управление программными проектами: достижение оптимального качества при минимальных затратах. Пер. с англ. — М.: Вильямс. 2003.
10. Boehm B.W. et al. Software cost estimation with COCOMO II. Prentice Hall PTR. New Jersey. 2000.
11. Boehm B.W. Software risk management. IEEE Computer Society Press. Washington. 1989.
12. Charett R. Software engineering risk analysis and management. N.Y.: McGraw — Hill. 1989.
13. Karolak D. W. Software engineering risk management. IEEE Computer Society Press. Washington. 1996.
14. Microsoft Solutions Framework. Пер. с англ. Решения Microsoft 99, Выпуск 7.
15. Sommerville I. Software engineering. Lancaster University. Pearson Education Limited. 2001.

Jet Info
ИНФОРМАЦИОННЫЙ БЮЛЛЕТЕНЬ
Издается с 1995 года
Издатель: компания Джет Инфо Паблишер

Главный редактор: Дмитриев В.Ю. *(vlad@jet.msk.su)*
Россия, 127015, Москва, Б. Новодмитровская, 14/1
тел. (095) 411 76 01
факс (095) 411 76 02
email: JetInfo@jet.msk.su http://www.jetinfo.ru

Подписной индекс по каталогу Роспечати 32555