**УДК 681.324**

# НАДЕЖНОСТЬ И БЕЗОПАСНОСТЬ СЛОЖНЫХ ПРОЕКТОВ И ТЕХНОЛОГИИ СНИЖЕНИЯ РИСКОВ

д.т.н., проф. В.С. Харченко, к.т.н. Н.К.Байда, В.В.Скляр

Анализируется проблема надежности и безопасности сложных проектов. Определяется понятие проекта как композиции процесса и продукта. Уточняются свойства надежности и безопасности уникальных проектов через свойства процессов и продуктов. Анализируются понятия риска и функции управления риском как основы обеспечения надежности и безопасности проектов. Обосновывается целесообразность использования многоверсионных технологий в управлении и реализации проектов.

***Введение.*** Анализ крупнейших аварий и катастроф последних десятилетий показывает, что более 60% из них носят технический характер, т.е. связаны либо с различными отказами и неисправностями технических систем, либо с нарушением их функционирования или разрушением вследствие ошибочных действий персонала, экстремальных факторов внешней среды, других непредвиденных причин, которые возникли при их испытаниях и эксплуатации [1].

Понятно, что размеры ущерба из-за таких аварий зависят от степени сложности систем, от числа людей, участвующих в их использовании и масштабов применения в целом, опыта разработки и эксплуатации данных систем и много другого. Системы, аварии которых могут вызвать многочисленные человеческие жертвы, большие экономические потери, представлять угрозу для обороны и безопасности государства, получили название *систем или комплексов критического применения* (СКП) (systems of critical applications). К числу СКП относятся: аэрокосмические (авиационные, ракетные и ракетно - космические) комплексы; транспортные (железнодорожные, морские, газо- и нефтепроводные) комплексы; энергетические комплексы (АЭС, гидро- и теплоэлектростанции, специальные энергетические установки); химические производства и крупные захоронения отходов вредных производств и др.

Отличительной чертой многих, наиболее сложных и ответственных СКП является то, что они создаются по уникальным проектам. Для таких проектов характерны следующие особенности [2,3]: *во-первых*, огромные затраты времени и средств на разработку; *во-вторых*, необходимость привлечения высококвалифицированных специалистов из различных областей науки и техники; *в-третьих*, отсутствие широкого и детального опыта создания СКП данного типа (использование опыта разработки «близких» си-

стем требует тщательного и критического анализа); *в-четвертых*, исключительная важность организации управления уникальными проектами и передачи опыта управления рисками на всех этапах жизненного цикла.

*Цель статьи* - анализ проблем надежности и безопасности СКП как сложных проектов и технологий снижения проектных рисков.

***1. Надежность и безопасность проектов как композиции процессов и продуктов.*** Ключевой проблемой разработки уникальных проектов, связанных с созданием, модернизацией и эксплуатацией СКП независимо от их типа, является проблема обеспечения надежности и безопасности.

Следует подчеркнуть, что традиционно требования к надежности и безопасности связывались, прежде всего, с самими системами или их элементами. Другими словами, если провести декомпозицию проекта СКП на две составляющие, условно именуемые **продуктом**, т.е. результатом реализации этого проекта – собственно технической системой, и **процессом**, т.е. системой мер и последовательностью действий, направленных на создание продукта, то свойства надежности и безопасности определялись, анализировались и вычислялись по отношению к продукту проектирования. При этом под надежностью продукта понималось свойство сохранять во времени и установленных пределах значения всех параметров, определяющих его способности выполнять заданные функции в заданных условиях эксплуатации, технического обслуживания и ремонта. Безопасность продуктов проектирования квалифицировалось как свойство исключать или минимизировать вероятность ситуации, приводящей к опасному воздействию на окружающую среду, персонал или другие системы (продукты). Естественно, что надежность и безопасность продуктов проявляются и оцениваются на этапе их применения по назначению, который является только одной из составляющих жизненного цикла СКП. В то же время очевидно, что эти свойства полностью закладываются и в большей степени реализуются на более ранних этапах цикла.

Другими словами, в равной степени следует говорить как о надежности и безопасности продуктов, так и о надежности и безопасности процессов. При этом под надежностью и безопасностью процессов можно понимать их свойства, обеспечивающие создание продуктов с заданным уровнем качества, в том числе надежности и безопасности соответственно. В то же время и надежность, и безопасность процессов могут рассматриваться как самостоятельные свойства, характеризующие процесс как автономный продукт разработки. Следовательно, говоря о сложных проектах СКП, необходимо анализировать и оценивать их надежность и безопасность как комплексное свойство, определяемое надежностью и безопасностью процессов и продуктов проектирования.

***2. Управляющие и вычислительные системы СКП и их влияние на надежность и безопасность проектов.*** Неотъемлемой и важнейшей частью любой СКП являются управляющие и вычислительные системы (УВС). УВС выступают в роли как объекта, так и средства проектирования СКП, как объекта, так и средства управления уникальными проектами. УВС являются иде-

альным примером того, что надежность и безопасность проекта зависит от уровня этих свойств его составляющих – процесса и продукта. Действительно, УВС представляет собой сложную систему , состоящую из двух неразрывно связанных и взаимодействующих компонент - аппаратной и программной. Если для аппаратной компоненты надежность и безопасность в большей степени определяются ее свойствами как свойствами продукта, то надежность и безопасность программной компоненты в максимальной степени зависит от процесса проектирования (включая, естественно, этап тестирования), так как от этого процесса зависит остаточный уровень дефектов, степень устойчивости программных средств к различным возмущающим факторам при функционировании УВС [4].

Таким образом, обеспечение требуемого уровня надежности и безопасности СКП, представляющих уникальные проекты, возможно только на основе комплексного рассмотрения двух составляющих таких процессов. Вторая компонента может рассматриваться как самостоятельная составляющая, требующая разработки и внедрения специальных технологий снижения рисков создания ненадежного и небезопасного продукта. Соотношение свойств компонент проектов и УВС иллюстрируется рис.1, где штриховкой выделены превалирующие пары их составляющих.

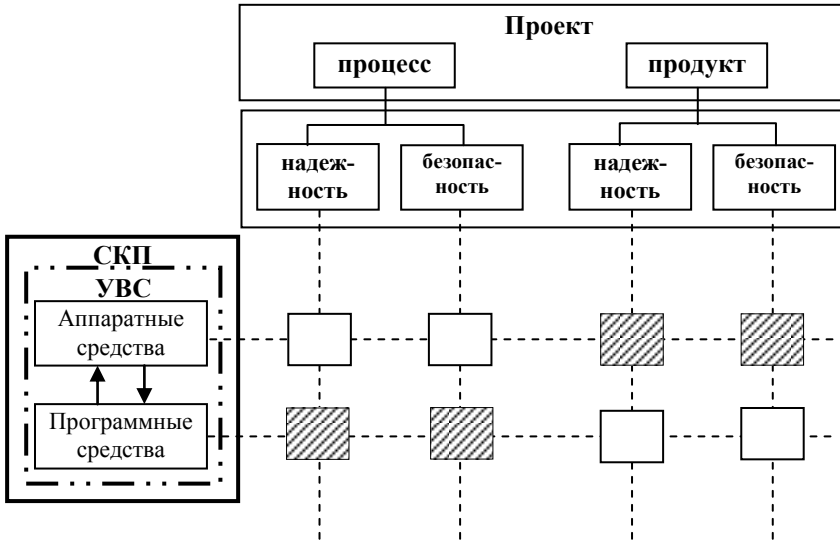


Рис. 1. Соотношение свойств проектов и УВС компонент

***3. Управление рисками как путь повышения надежности и безопасности сложных проектов.*** Двойственным по отношению к понятию надежности и безопасности проектов является понятие риска. Риск определяется как произведение вероятности возникновения возможного ущерба и ожидаемого объема ущерба [2].

Следует подчеркнуть, что функция управления рисками является одной из основных функций управления проектами. В соответствии с определенной в мировой практике терминологией, отраженной в стандарте “Project Management Body of Knowledge” , изданном в США Институтом проектного менеджмента – одной из ведущих мировых профессиональных ассоциаций, среди функций управления проектами (координации проекта, содержания проекта, временного планирования, управления стоимостью проекта, управления качеством, управления человеческими ресурсами, управления коммуникацией и управления контрактами и закупками) выделяется функция управления рисками (Project Risk Management). Она определяется как функция идентификации и квалификации риска и выполнения противорисковых мероприятий.

Проектные риски классифицируются на технико-технологические, маркетинговые, финансовые, риски участников проекта, социальные, юридические, политические, экологические, строительные, риски обстоятельств непреодолимой силы, или форс-мажор, специфические риски. Технико-технологические риски применительно к проектам УВС СКП, обусловлены, прежде всего, ненадежностью процессов и продуктов разработки – аппаратных и программных средств таких систем. При этом функция управления рисками реализуется путем разработки и выбора как конкретных архитектурных решений, так и технологий проектирования, минимизирующих вероятности отказов, переводящих систему в критическое (опасное) или некритическое (защищенное) состояние. Поскольку в некоторых типах СКП УВС выполняют функции систем безопасности (это касается, например, бортовых УВС ракетных комплексов, систем аварийной защиты АЭС), то при оценке безопасности таких проектов учитываются только надежностные характеристики УВС.

***4. Анализ технологий снижения проектных рисков.*** В настоящее время разработано большое число методов, позволяющих уменьшить технико-технологические риски на различных этапах реализации проектов [2,5,6]. К ним относятся методы, основанные на построении и *анализе деревьев отказов* (Fault Tree Analysis – FTA-технология), *анализе и видов и последствий отказов* (Failure Modes and Effects Critical Analysis – FMECA-технология) и др. Большинство этих технологий ориентировано, прежде всего, на решение задач анализа надежности и безопасности проектов, основываясь на результатах которых предусматриваются и реализуются мероприятия по снижению рисков. Другими словами, их использование направлено на все более глубокий и всесторонний поиск причин, увеличивающих риски. Очевидно, что с усложнением СКП, их ядра УВС такой подход, который можно назвать концепцией **“направленного движения к идеальному проекту**” (НДИП), вызывает и неадекватный резкий рост временных и материальных затрат и не позволяет выявить все эти причины. Такая ситуация особенно характерна для программных средств УВС, поскольку полное выявление и устранение дефектов связано со значительным увеличением

времени и стоимости тестирования и отладки и практически не реализуемо. Выход из сложившейся ситуации может быть найден, учитывая следующие обстоятельства.

1. Практически на всех этапах жизненного цикла проекта разработчики имеют дело с несколькими вариантами (альтернативами, версиями) решения одной и той же задачи. Так обстоит дело: *при разработке концепции проекта*, когда предлагаются и анализируются различные подходы к его осуществлению; *при решении конкретных задач проектирования*, когда генерируется несколько конкурентоспособных вариантов, которые ранжируются по сформулированным критериям с учетом целевых функций и ограничений; *при независимой верификации проектов* (например, программного обеспечения) важных для безопасности систем, которая проводится административно или финансово - независимыми организациями с целью минимизации числа остаточных дефектов; *при экспертизе принимаемых решений*, когда несколько экспертов (групп экспертов) проводит их анализ, на основе которого делаются оценки проекта (его вариантов) и осуществляется его окончательный выбор.

2. Для уникальных проектов (даже с учетом их большой стоимости громоздкости) практикуется создание нескольких альтернативных вариантов отдельных подсистем (субпроектов), анализ которых позволяет выбрать предпочтительный вариант (варианты).

3. Генерация нескольких вариантов решения задач на различных этапах жизненного цикла проекта позволяет не только найти лучший по некоторому критерию вариант, но и доработать его с учетом выявленных при “перекрестном” (межвариантном) анализе дефектов, относящихся к одной или нескольким версиям.

4. При разработке и реализации наиболее ответственных и важных для безопасности систем уже многие годы реализуется принцип разнообразия и многоуровневой защиты от отказов. В атомной энергетике он получил название “Defence-in-Deep and Diversity” (DinD&D) – защита в глубину и диверсность (разнообразие) [7,8 ]. Этот принцип предполагает не только генерацию и анализ нескольких вариантов построения системы или наиболее важных ее подсистем, но и реализацию этих вариантов (их полного или сокращенного по определенным критериям множества) в окончательном проекте. Можно провести большое число примеров, где этот принцип реализуется [3,9]: *системы аварийной защиты* реакторов АЭС, состоящие из нескольких независимых и реализованных на разных физических принципах подсистем; *системы управления* многих типов летательных аппаратов, которые имеют несколько измерительных каналов от грубых (с высокой безотказностью) и точных (менее надежных) датчиков, дублирующих друг друга; *ручные и автоматические каналы* управления и контроля в бортовой и наземной аппаратуре различного назначения и т.д.

Таким образом, следует говорить о том, что одним из возможных и естественных путей обеспечения и повышения уровня надежности и без-

опасности проектов является использование технологий, которые можно назвать **многоверсионными** (многоальтернативными, многовариантными и т.д.). [8-10]. Суть таких технологий заключается в том, что при управлении и реализации проекта:

а) формируется (генерируется, синтезируется) несколько вариантов – версий решения той или иной проектной задачи;

б) по определенному критерию и соответствующим методам осуществляется выбор нескольких (двух и более) версий;

в) при необходимости выполняется их доработка и тиражирование;

г) определяется порядок использования полученных версий на последующих этапах жизненного цикла проекта.

Тогда многоверсионными проектом и системой можно называть такой проект и систему, которые разрабатываются и реализуются с использованием многоверсионных технологий. Формализованное описание этих понятий дано в [3,4]. Многоверсионные технологии управления и реализации проектов основываются на концепции "**реальной оценки достижимости характеристик и использования избыточности проекта**" (РОИП).

***Выводы.*** Проект СКП (как и любой другой проект) представляет собой композицию двух элементов – процесса и продукта. Процесс – это система действий, направленных на создание продукта – материального результата реализации проекта. Исходя из этого целесообразно рассматривать понятия надежности и безопасности проектов через свойства надежности и безопасности процессов и продуктов. Для СКП в целом и УВС, состоящих из аппаратных и программных средств, исключительно важным с точки зрения надежности и безопасности проекта является *анализ и оценка свойств процесса проектирования*.

Обеспечение надежности и безопасности проекта в целом может быть осуществлено, прежде всего, посредством реализации функции управления рисками. Эту функцию следует рассматривать как совокупность взаимосвязанных организационных и технических мер, направленных на снижение вероятности выхода результатов проекта за пределы допустимой области и минимизации ущерба, который может иметь место вследствие его реализации, в том числе из-за неблагоприятных и непредусмотренных внешних воздействий. Разработка *эффективных методов и средств реализации функции управления проектными рисками* представляет собой сложную самостоятельную задачу.

Известные подходы и технологии, направленные на повышение надежности и безопасности проектов, как правило, ориентированы на расширение спектра и углубление анализа причин, увеличивающих риски [1,2,11]. Они могут быть объединены единой концепцией НДИП, реализация которой требует постоянного и не всегда эффективного роста временных затрат на повышение надежности и безопасности при разработке и тестировании проекта. Альтернативный подход базируется на концепции реальной оценки достижимых характеристик надежности и безопасности проекта, введении и

сохранении избыточности, позволяющей парировать его дефекты – концепции РОИП. Эта концепция реализуется на основе *многоверсионных технологий, предполагающих параллельное использование нескольких альтернативных версий* (субпроектов и подсистем) на различных этапах жизненного цикла.

## ЛИТЕРАТУРА


1. P. Kafka, How safe is enough? – An unresolved issue for all technologies // Proceeding of 10th European Conference on Safety and Reliability, – Munich, Germany, 13-17 September, 1999. – P.385 - 390.

2. Згуровський М.З., Коваленко І.І., К. Кондрак, Е. Кондрак. Інформаційний підхід до аналізу та управління проектними ризиками // Проблеми управління та інформатики. – 2000.– №4. – С. 149 - 156.

3. Харченко В.С. Многоверсионные цифровые системы, важные для безопасности: анализ и перспективы // Модели и системы. – 1999. – № 1. – С. 62 - 69.

4. Харченко В.С. , Литвиненко В.Г. Применение концепции многоальтернативного проектирования для построения высоконадежных и безопасных систем // Приборы и системы управления. – 1993. – №6. – С. 18 - 11.

5. IEC 1025 - 1990 Std. Fault Tree Analysis (FTA). – 39 p.

6. IEC 812 - 1985 Std. Failure Mode and Effects Analysis (FMEA). – 41 p.

7. Бегун В.В., Горбунов О.В., Каденко И.Н. и др. Вероятностный анализ безопасности атомных станций. – К.: Мин. образования и науки. – 2000. – 568 с.

8. Kharchenko V.S. The Probabilistic Assessment of Surviability and Safety of an Unmanned Control Systems with Multistage Degradation by Use of QD-diagrams // Proceedings of 5th International Conference Probabilistic Safety Assessment and Menegement, Osaka, Japan, November, 27 Desember, 1, 2000. – P. 345 - 351.

9. Littlewood B., Strigini L. A Discussion of Practices for Enhancing Diversity in Software Designs // Technical report LS_DI_TR-04, version 1.1d, 23 November, 2000. – 58 p.

10. Vilkomir S.A., Kharchenko V.S. Metology of the Review of Sofrware for Safety Impotant Systems // Proceedings of 10th European Conference on Safety and Reliability, Munich - Garshing, 13 - 17 September, 1999. – P. 593 - 596.

11. Фоменко О.Н. Управление реализуемостью проектов ракетно-космической техники путем стандартизации и унификации // Системи обробки інформації. – Харків: НАНУ,ПАНМ, ХВУ. – 1995. – С. 186 - 189.


*Поступила в редколлегию 28.02.2001*