

Абрамова Н.А., Коврига С.В., Макаренко Д.И.

ПРИНЦИПЫ УПРАВЛЕНИЯ КАЧЕСТВОМ ПРОЕКТИРОВАНИЯ СЛОЖНЫХ ПРОГРАММНО- ТЕХНИЧЕСКИХ КОМПЛЕКСОВ С УЧЕТОМ ОЦЕНКИ РИСКОВ ОШИБОК ЧЕЛОВЕКА

Для снижения влияния человеческих факторов при проектировании программно-технических комплексов, связанных с безопасностью, на риски возникновения опасных ситуаций в ходе их эксплуатации, предложены некоторые новые принципы, направленные на повышение качества проектирования таких комплексов. Представленные результаты основаны, с одной стороны, на психологических и междисциплинарных исследованиях, а с другой, – на анализе практики проектирования сложных программно-технических комплексов в атомной энергетике.

Ключевые слова: потенциально опасный объект, безопасность, программно-технический комплекс, достоверность, риски из-за человеческого фактора, управление качеством проектирования.

Введение

Сегодня имеет место существенное усложнение потенциально опасных объектов, для которых создаются методы и системы управления или поддержки принятия решений на основе формальных методов. В понятие сложности объектов (систем, комплексов), наряду с более традиционными признаками (такими как количественная сложность, структурная сложность, сложность математических моделей – «organized complexity»), включается человеческий аспект сложности, когда интеллектуально сложным этапом решения задач управления и обеспечения безопасности является первичная структуризация и формализация знаний о проектируемых объектах и предъявляемых к ним требованиях.

В силу неизбежного участия людей, применяемые методы структуризации и формализации знаний при проектировании сложных объектов в принципе не могут обеспечить достоверности конечных результатов. Другими словами, они являются рискованными в отношении достоверности результатов¹. Таким образом, поиск решений проблемы рисков, обусловленных человеческим фактором, должен охватывать не только сами объекты, но и процесс их создания, в котором также

¹ Здесь достоверность понимается в широком смысле, как возможность полагаться на результаты применения таких методов.

участвуют люди. Это означает, что человеческие факторы риска могут быть связаны не только с людьми, участвующими в процессе управления объектом, но и с разработчиками методов и систем управления и информационных технологий, и учеными, которые теоретически обосновывают методы управления.

Целью данной работы является разработка подходов и принципов управления качеством проектирования сложных программно-технических комплексов (ПТК), связанных с безопасностью, для снижения влияния человеческих факторов при проектировании таких ПТК на риски возникновения опасных ситуаций в ходе их эксплуатации.

Серьезным свидетельством практической значимости рассматриваемых рисков при решении задач управления сложными объектами являются экспериментальные исследования мышления субъекта управления в сложных проблемных ситуациях и анализ причин мыслительных ошибок, порождаемых в ходе их разрешения [1].

В статье представлена типология рисков по характеру их влияния на безопасность потенциально опасного объекта при эксплуатации ПТК, предложены некоторые новые принципы и подходы, направленные на повышение качества проектирования ПТК. Представленные результаты основаны, с одной стороны, на психологических и междисциплинарных исследованиях, а с другой, – на анализе практики проектирования сложных ПТК для АЭС.

1. Разнообразие косвенных источников риска возникновения опасных ситуаций в ходе эксплуатации программно-технических комплексов, связанных с безопасностью

С целью выявления и систематизации человеческих факторов и механизмов риска, (1) действующих в жизненном цикле создания, внедрения и применения ПТК и (2) практически значимых для управления качеством, проведен выборочный анализ практики проектирования сложных ПТК, связанных с безопасностью (применительно к АЭС).

Изучение практической деятельности по обеспечению качества ПТК для потенциально опасных объектов показывает, что в условиях возрастающей интеллектуальной сложности ПТК традиционный подход к обеспечению качества не охватывает широкого спектра разнородных косвенных рисков для безопасности, действующих на практике и не поддающихся количественной оценке. Прежде всего, это относится к рискам из-за человеческого фактора в ходе проектирования и испытаний ПТК. При этом в качестве традиционного подхода к обеспечению качества ПТК, связанных с безопасностью, рассматривается поэтапная верификация и валидация вкупе с организационными методами и ограниченным применением формальных методов, возможности которых в условиях возрастающей сложности ПТК существенно ограничены.

Выделены следующие типы рисков по характеру их влияния на безопасность потенциально опасного объекта при эксплуатации ПТК:

- риски, явно связанные с безопасностью при эксплуатации ПТК (т.е. порождающие риск возникновения опасных ситуаций на объекте),

- косвенные риски, в которых явная связь с опасными ситуациями не прослеживается.

К косвенным рискам относятся:

- технические риски – риски, связанные с принятием технических решений при создании ПТК;

- организационно-управленческие риски, включая риски, связанные
 - с уровнем зрелости производственного процесса создания ПТК в терминах модели зрелости SW-CMM [2];
 - с компетентностью субъектов производственной и управленческой деятельности;
- субъективные риски – риски, связанные с когнитивными и иными особенностями субъектов производственной и управленческой деятельности (согласно современным данным когнитивных наук).

На рис. 1 представлены типовые риски и причинно-следственные связи между этими типами рисков (знак «+» на связи означает положительное влияние («чем больше..., тем больше...»), а знак «-» – отрицательное влияние («чем больше..., тем меньше...»); серые стрелки указывают на другие возможные типы рисков).

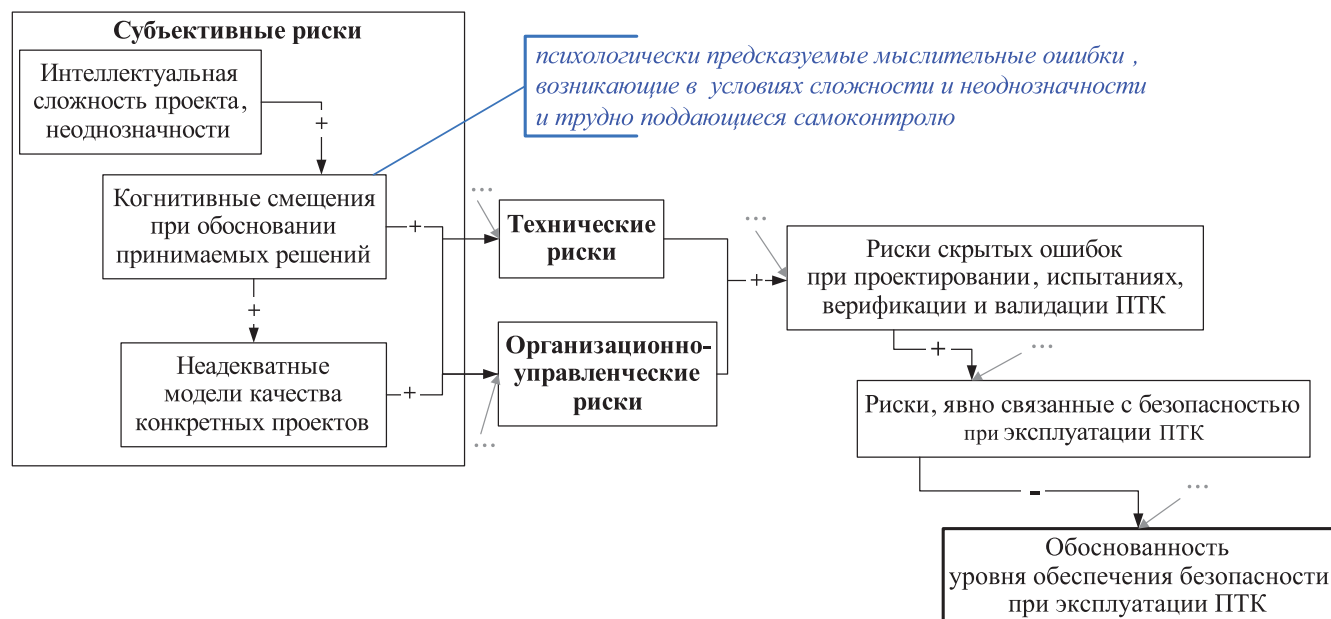


Рис. 1. Риски из-за человеческого фактора при создании ПТК, связанных с безопасностью, и их причинно-следственные связи

В ходе анализа и систематизации рисков по характеру их влияния на безопасность потенциально опасного объекта при эксплуатации ПТК (1) нашла свое подтверждение гипотеза о зависимости рисков из-за человеческого фактора при проектировании ПТК, связанных с безопасностью, от функциональных ролей человека в жизненном цикле ПТК; (2) а также выдвинута и прошла проверку гипотеза о зависимости неадекватных моделей качества конкретных проектов у ответственных исполнителей от известных в психологии факторов риска, называемых когнитивными смещениями (психологически предсказуемых мыслительных ошибок, возникающих в условиях сложности и неоднозначности и трудно поддающихся самоконтролю). К ним относятся стереотипы применения устаревших технологий, систематическая недооценка значимости непривычных требований.

Разнородность выделенных практически значимых рисков при проектировании сложных ПТК, связанных с безопасностью, при существенной роли человеческого фактора в них в сочетании с практической невозможностью достоверной количественной оценки такого рода рисков свидетельствуют о необходимости разработки новых теоретических подходов к решению исследуемой задачи управления качеством проектирования сложных ПТК.

2. Общие принципы косвенного управления качеством программно-технических комплексов, связанных с безопасностью

Известный принцип поэтапной верификации в ходе создания ПТК, связанных с безопасностью, может рассматриваться как принцип косвенного управления качеством таких ПТК. При этом стандартным подходом считается верификация по predetermined критериям качества, которые предъявляются к промежуточным продуктам проектирования, представленным соответствующей документацией.

Для расширения возможности раннего обнаружения косвенных рисков из-за человеческого фактора (по сравнению с типовым подходом к верификации) предложен ряд новых принципов:

- *более широкий охват разнородных косвенных факторов риска и их причинно-следственных связей*, прежде всего человеческих факторов, в ситуациях обнаружения ошибок или рисков неадекватных технических и управленческих решений, с целью повышения эффективности управления качеством ПТК и расширения состава механизмов управления;

- *принцип расширенной верификации*, включая верификацию не только технических решений, но и используемых методов оценки, в том числе моделей качества проектов (в рамках имеющихся суммарных ресурсов);

- *ограниченное применение формальных методов комплексного оценивания*, используемых при управлении качеством проектирования и испытаний ПТК, связанных с безопасностью, во избежание рисков недоверенного оценивания в сочетании с верификацией самих методов оценивания. Обоснованиями принципа ограниченного применения формальных методов комплексного оценивания в сочетании с верификацией самих методов оценивания служат (1) найденные ранее теоретическим анализом и подтвержденные на практике возможности манипулирования оценками качества в условиях невозможности достоверной количественной оценки рисков или иных показателей качества проектирования; (2) найденные риски в самих методах оценивания, которые предлагаются теорией и стандартами для решения задач комплексного оценивания, связанных с безопасностью [3];

- *рефлексивный подход к анализу обоснований* принимаемых технических и управленческих решений, учитывающий не только собственно объективные обоснования принимаемых решений, но и зависимость представлений и оценок ответственных исполнителей от субъективных факторов риска, функциональных ролей и интересов. Обоснованием рефлексивного подхода служит наличие ряда практических ситуаций, в которых выявление необоснованных решений невозможно или затруднительно без учета субъективных факторов (например, ошибочное занижение уровня требований к проектированию ПТК по сравнению с уровнем требований, который мотивирован классом безопасности);

- *экспертная верификация без predetermined критериев* в дополнение к традиционной верификации по predetermined критериям качества. Обоснованиями принципа экспертной верификации без predetermined критериев служат:

- анализ опыта верификации и перекрестных анализов проектных решений соисполнителями конкретного проекта ПТК;

- междисциплинарное исследование психологических механизмов, лежащих в основе экспертной верификации, начиная с таких как «детекторы ошибок» [4], «когнитивный диссонанс» [5].

Для повышения качества процесса обнаружения ошибок и рисков экспертами-верификаторами разработана оригинальная междисциплинарная модель когнитивного процесса экспертной верификации без predetermined критериев. Она сопоставима с широко известной моделью двух когнитивных систем, отражающей внутренние возможности человека к обнаружению ошибок в обоснованиях [6].

2.1. Модель когнитивного процесса экспертной верификации без predetermined критериев

Принципиальное различие традиционной верификации по predetermined критериям от экспертного анализа как метода верификации состоит в том, что в первом случае выбор критерия и выбор (идентификация) верифицируемого фрагмента предшествуют оценке соответствия, тогда как при экспертном анализе некоторый анализируемый материал сразу идентифицируется как несоответствующий тем или иным представлениям эксперта-верификатора. «Сразу» здесь означает, что оценка появляется в результате внутренних, необязательно осознаваемых когнитивных процессов.

Предлагаемая модель экспертной верификации без predetermined критериев опирается на принципиальное свойство – свойство самопроизвольной идентификации (локализации) несоответствий. При этом учитывается, что, как показывают наблюдения, типичны два вида определения несоответствий. В одних случаях идентифицированный экспертом-верификатором фрагмент анализируемого материала (или его свойство) может сразу оцениваться им как несоответствующий некоторому объявляемому (но не выбранному заранее) критерию, требованию. В других случаях оценка дается в самых общих словах типа «некорректно», «так не может быть», «сомнительно», «что-то тут не то», «непонятно», «какая-то странность (или аномалия)».

Далее последующим «самоизвлечением знаний» даются объяснения оценки, так что, в конечном счете, либо выявляется нарушенный критерий соответствия, либо устанавливается необходимость



Рис. 2. Структурная организация обработки экспертного знания с прерываниями при обнаружении ошибок и аномалий

дальнейшего анализа для объяснения идентифицированной странности или аномалии. В последнем случае можно говорить об идентификации рискованного фрагмента или общего свойства.

Объяснение когнитивных процессов, дающих такого рода реакцию эксперта-верификатора, может быть дано с использованием знаний когнитивных наук в таких терминах как «когнитивный диссонанс», «когнитивный контроль», «детектор ошибок», «функциональный орган».

Однако более четкое и целостное представление получается дополнительным привлечением компьютерной метафоры с использованием понятия «системы прерываний» и родственных понятий таких как «источник прерываний», «основной (прерываемый) процесс», «механизм прерываний», «дисциплина обслуживания прерываний» для увязывания. Структурная организация обработки экспертного знания с прерываниями при обнаружении ошибок и аномалий представлена на рис. 2.

Идентификацию несоответствия представляется уместным рассматривать как частный случай проявления когнитивного диссонанса – психологического дискомфорта, который, по теории Л. Фестингера [5], может вызываться противоречием между имеющимся устоявшимся представлением и свежей поступающей информацией, фактами.

Акт идентификации несоответствия может трактоваться как срабатывание «системы прерываний», которая осуществляет когнитивные контроли над знаниями, извлекаемыми экспертом из объекта верификации.

Система прерываний выявляет несоответствия посредством совокупности релевантных детекторов ошибок. Эти детекторы отражают стереотипные, или, по крайней мере, хорошо усвоенные активные знания, относящиеся к сфере анализа. Обнаружение несоответствия тем или иным детектором может приводить к прерыванию основного процесса в соответствии с той или иной «дисциплиной обслуживания прерываний», так что несоответствие, по крайней мере, регистрируется экспертом-верификатором, и, возможно, проводится его первичный анализ (прерывание «обслуживается»). С учетом наблюдений по идентификации рискованных фрагментов предполагается, что детекторы могут обнаруживать не только ошибки, но и рискованные и сомнительные ситуации.

Согласно нейрофизиологическим экспериментам Н.П. Бехтеревой [4], действие механизма, который она назвала «детектором ошибок», происходит через эмоции, которые могут рассматриваться как «механизм прерывания».

Из предложенной модели экспертной верификации с двумя видами знаний, порождающих когнитивный диссонанс, можно сделать довольно нетривиальный вывод. Для срабатывания теоретических знаний в качестве элемента диссонанса у эксперта-верификатора должны сформироваться надлежащие детекторы ошибок или, по крайней мере, детекторы риска, рискованных свойств, способные в силу высокой активности вызвать когнитивный диссонанс и самопроизвольные прерывания основного когнитивного процесса в случае несоответствий.

Анализ практики верификации ПТК, связанных с безопасностью, в области атомной энергетики, показал, что предложенная модель не только обладает сравнительно большими объяснительными возможностями, но и открывает пути для повышения качества процесса обнаружения ошибок и рисков экспертами-верификаторами и для его компьютерной поддержки.

2.2. Модифицированная модель управления качеством программно-технических комплексов, связанных с безопасностью

На основе предлагаемых принципов модифицирована модель управления качеством ПТК, которая включает, в дополнение к традиционной модели управления качеством посредством поэтапной верификации, выделение и оценку в конкретном процессе проектирования, верификации и испытаний ПТК разнородных косвенных факторов риска, действующих в жизненном цикле ПТК и их

причинно-следственных влияний на управление качеством. Обобщенная схема модифицированной модели управления качеством проектирования ПТК, связанных с безопасностью, представлена на рис. 3.

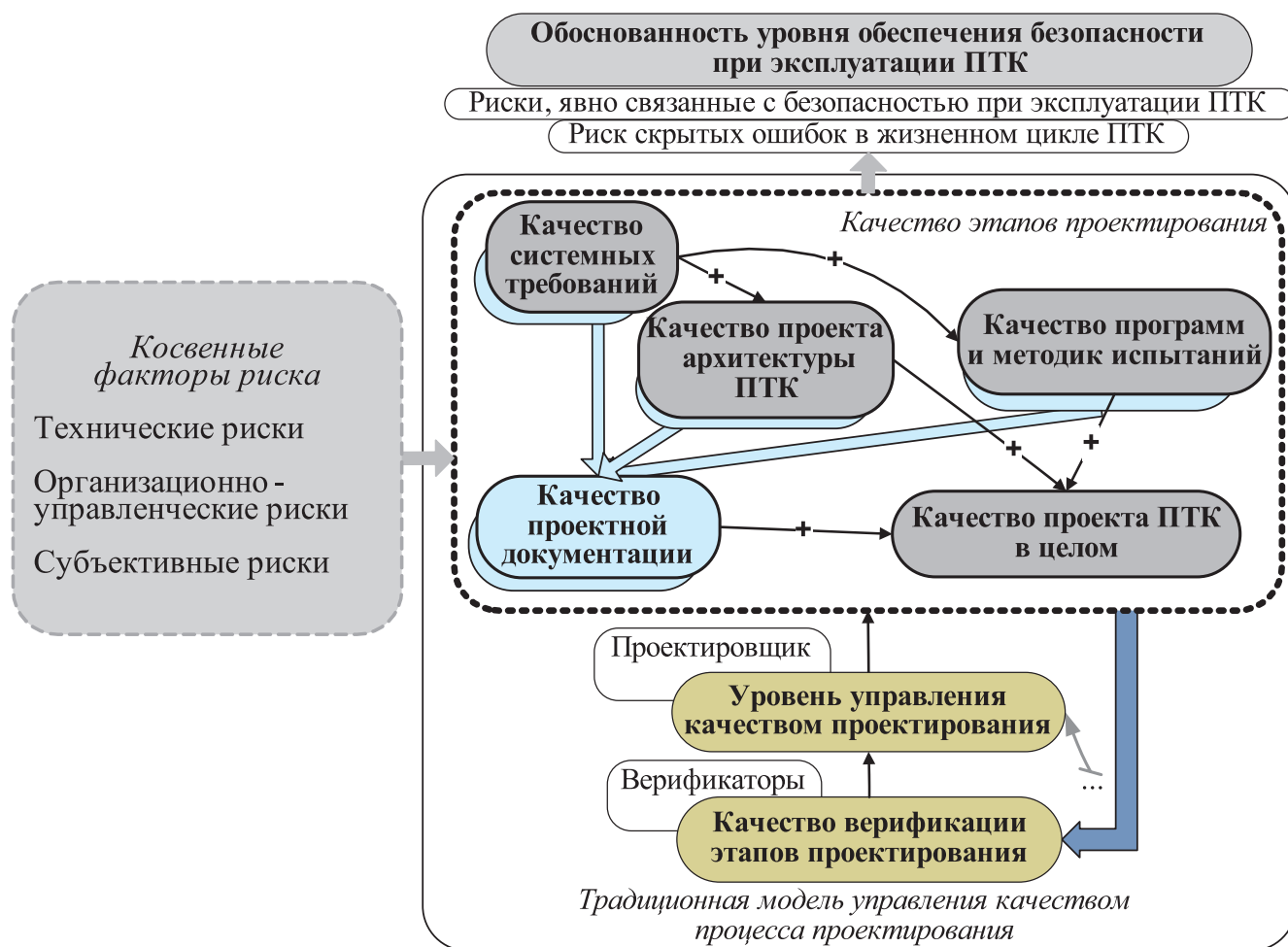


Рис. 3. Обобщенная схема модифицированной модели управления качеством проектирования ПТК, связанных с безопасностью

Предлагаемый подход с расширением традиционной модели управления качеством проектирования в ходе верификации прошел частичную эмпирическую проверку применительно к созданию конкретного ПТК, связанного с безопасностью, для АЭС «Куданкулам». В процессе верификации проекта ПТК был выявлен ряд значимых разнородных факторов риска, выходящих за рамки ошибочных или рискованных технических решений (например, несогласованность системы понятий в неоднородном коллективе участников и руководства международного проекта, сложность (непрозрачность) ролевой структуры взаимоотношений между участниками проекта, недостаточный опыт разработчиков по созданию ПТК, связанных с безопасностью). Это позволило уточнить первоначальную модель управления качеством проекта в виде соответствующей причинно-следственной схемы косвенного влияния найденных факторов на риск скрытых ошибок проектирования, а значит, и на уровень обеспечения безопасности при эксплуатации ПТК. Модифицированная модель позволила выделить дополнительные точки приложения управляющих воздействий по повышению качества проектирования. В том числе была подтверждена целесообразность ее применения для согласования и обоснования различных представлений в условиях сложной ролевой структуры взаимоотношений между участниками международного проекта.

Заключение

Практическая роль предложенных новых принципов косвенного управления качеством ПТК состоит в расширении возможностей управления качеством проектирования таких комплексов благодаря выявлению и учету рисков из-за человеческого фактора при разработке объектов с повышенными требованиями надежности и безопасности функционирования.

Работоспособность модифицированной модели управления качеством ПТК подтверждена в ходе создания конкретного ПТК, связанного с безопасностью, для АЭС «Куданкулам», что обуславливает целесообразность разработки методического обеспечения для внедрения данного подхода в практику управления качеством проектирования потенциально опасных объектов.

Оригинальная междисциплинарная модель когнитивного процесса экспертной верификации открывает возможности:

- для целенаправленного управления процессами обнаружения ошибок и аномалий, не охватываемых традиционным методом поэтапной верификации по predetermined критериям;
- для комплексного развития теоретических и инструментальных средств поддержки экспертного анализа, активизирующих когнитивные ресурсы экспертов-верификаторов на разных этапах проектирования ПТК.

Литература

1. Дёрнер Д. Логика неудачи. Стратегическое мышление в сложных ситуациях. – М.: Смысл, 1997. – 243 с.
2. Paulk M. and others. Capability Maturity Model for Software. (CMU/SEI-93-TR-24). Pittsburgh, Pa.: Software Engineering Institute, Carnegie Mellon University, 1993.
3. Абрамова Н.А. О некоторых мифах в оценке качества программного обеспечения // Надежность, №1, 2004. – С. 38-63.
4. Бехтерева Н.П. Мозг человека. Сверхвозможности и запреты. // Доклад на Всемирном Конгрессе «Итоги тысячелетия». – Санкт-Петербург, 2000.
5. Фестингер Л. Теория когнитивного диссонанса: Пер. с англ. СПб.: Ювента, 1999. – 318 с.
6. Kahneman D., Frederick S. Representativeness revisited: Attribute substitution in intuitive judgment. In T. Gilovich, D. Griffin & D. Kahneman (Eds.), *Heuristics and Biases* Heuristics and biases: The psychology of intuitive judgment (pp. 49-81). New York: Cambridge University Press, 2002.