УДК 004.052

Элементы системного анализа в изучении надежности

программных средств

*И.В. Потапов*

Омский государственный технический университет, г. Омск, Россия

*Аннотация* – В данной работе изучаются общие вопросы теории надежности программных средств. Применяется методология прикладного системного анализа. Эта методология ориентирована на решение сложных проблем, трудно поддающихся формализации. Надежность программных средств рассматривается в контексте общей теории надежности информационно-вычислительных систем.

*Ключевые слова*: Надежность программ, надежность программных средств

Данная работа является продолжением начатого в [1] системно-аналитического описания в области надежности программных средств (ПС). Изучение и решение задач в указанной области знаний затруднены ее сложностью и громоздкостью. Многие вопросы, составляющие проблематику [1], не подаются формальному описанию. Затруднения возникают и при теоретическом, и при практическом, или инженерном, анализе. В этой связи одним из возможных средств преодоления трудностей может оказаться применение методологии прикладного системного анализа. Здесь применяется методология томской школы системного анализа [2]. Предполагается выполнение нескольких взаимозависимых шагов для достижения общей цели. В качестве цели системного анализа рассматривается проектирование улучшающего вмешательства для преобразования проблемосодержащей системы. Данная методология полезна и в том случае, когда улучшающее вмешательство не предполагается, поскольку позволяет всесторонне изучить проблему, переформулировать ее разными способами и по-новому взглянуть на решение ключевых задач.

Здесь будут рассмотрены две составляющие общего системно-аналитического подхода. Будут сформированы множество целей и дано описание проблемосодержащей системы, как оно видится с различных точек зрения. Сразу необходимо отметить, что формат печатной работы предполагает некоторое преобразование результатов к виду, удобному для восприятия. Громоздкость словесного описания приводит к необходимости сокращения изложения и, что наиболее существенно, к выполнению некоторого упорядочения и структуризации результатов. Хотя упорядочение и структуризация всех промежуточных результатов являются важными составляющими системно-аналитической практики, их выполнение существенно зависит от текущих взглядов исследователей и применяемых ими моделей. Это в принципе означает возможность различного упорядочения результатов анализа.

В данной работе описывается только свойство надежности ПС. Существуют несколько близких и взаимосвязанных свойств — точность, безопасность и т.п. Эти свойства очень важны и могут быть рассмотрены обособленно. Они могут быть рассмотрены и в комплексе с надежностью, поскольку, по мнению некоторых специалистов, являются атрибутами надежности.

При формировании множества целей всегда возникает трудность с определением целей на разных уровнях иерархии. В данном случае попробуем сформулировать базовые цели как результат декомпозиции по фундаментальной модели научного знания. Станем различать глобальную цель формирования абстрактной теории надежности ПС и отдельно — формирование прикладной теории надежности ПС. Эти две цели находятся на вершине иерархии. Далее сформулируем подцели, но при этом станем учитывать, что между ними существуют сложные взаимосвязи. Поэтому построение дерева целей не прояснит, а наоборот, скорее усложнит представление. Здесь можно обнаружить «клубок» целей, который по сложности структуры напоминает проблематику.

Важной целью, во многом пересекающейся с остальными, является изучение появления ошибок в программах. Ошибки являются фактором, вызывающим отказы. Точнее, к отказам приводит появление определенных состояний программы и входных воздействий, которые приводят к выполнению участка программы, содержащего ошибку. Здесь можно сформулировать ряд подцелей со сложными взаимосвязями. К ним относятся цели создания методов прогнозирования, игнорирования, количественного подсчета программных ошибок и т. п., формирование моделей для их изучения. Отметим, что в литературе можно найти большое количество различных моделей для исследования ошибок. Но все они довольно специфические и не всегда дают приемлемые результаты. Как правило, это модели структурные. Интерес представляют подходы к изучению динамики появления ошибок, которые, по-видимому, могут быть сформулированы в рамках инженерной психологии.

Отметим важную цель — построение моделей функционирования ПС для изучения проявления ошибок и превращения их в отказы. Вопросы построения моделей составляют важную часть проблематики в области надежности ПС. Однако здесь имеются существенные трудности. Они во многом связаны с тем, что традиционно в теории надежности строятся вероятностные модели, а программы вполне четко определены и программные ошибки не являются случайными явлениями. Поэтому в множество целей можно добавить и необходимость определения того, что является случайной величиной, случайным процессом и т. п. Отметим, что эта цель по существу нужна только для встраивания расчетов надежности ПС в стандартную схему, оперирующую вероятностными и временными показателями. Известны подходы к изучению структуры текстов, в рамках которых возможно построение моделей другого вида.

Центральными проблемами в теории надежности ПС являются отличия этих объектов исследования от других технических систем. Отличия настолько существенные, что вместо применения известных в теории надежности приемов, моделей и показателей необходимо разрабатывать новые, отражающие специфику отказов программ. Это тоже цель. Отметим еще одну, не менее важную. Особенности ПС требуют уточнения терминологии надежности и рассмотрения специфических моделей и показателей. Некоторые из этих вопросов находят отражение в работе [3] и ряде других. Важной целью является переработка существующих стандартов в области надежности, поскольку действующий в настоящее время ГОСТ 27.002–89 [4] не учитывает специфику надежности информационно-вычислительных систем (ИВС), сделавших за время, прошедшее с момента введения данного стандарта, заметный скачек в развитии, и специфику надежности программных средств этих систем.

В работах по надежности ПС большое значение играет тот факт, что сами по себе программы не отказывают. Они исполняются в информационно-вычислительной системе. С другой стороны, ИВС функционируют под управлением программ. Некоторые специалисты полагают, что при описании и расчетах надежности ИВС можно рассматривать ПС как отдельную систему. Другие авторы научных работ указывают на необходимость рассмотрения работы ИВС в целом, т. е. описывать их надежность комплексно. Отсюда возможна формулировка цели, состоящей в определении возможности описания и расчета надежности ПС как самостоятельного компонента ИВС.

Следующими шагами в анализе должны стать структуризация, упорядочение сформулированных целей, уточнение их взаимосвязей и подробностей. При этом возможно формулирование новых целей и подцелей и даже пересмотр уже определенных. Эти вопросы выходят за рамки данной работы. Важнее перейти к очередной задаче системного анализа, состоящей в описании проблемосодержащей и проблеморазрешающей систем с использованием различных точек зрения, определяемых сторонами, заинтересованными в решении проблем.

Кратко задача ставится следующим образом [2]. В результате системного анализа выявляются стороны, формирующие проблематику и заинтересованные в проектировании улучшающих вмешательств, помогающих решить проблемы. Для выполнения проектирования улучшающих вмешательств надо определить терминологию для описания систем в терминах, применяемых различными специалистами. Проблематика надежности ПС подробно рассмотрена в [1]. Далее будут отмечены результаты рассмотрения данной проблематики с наиболее важных, определенных в [1], точек зрения. Разумеется, возможны и другие. Практика системного анализа основывается на построении первичных моделей, по которым выполняется дальнейшая работа. Каждый может предложить свои модели, дополняющие или меняющие приведенные здесь результаты.

В данной работе рассматривается проблематика надежности программ с точек зрения специалистов в общей теории надежности технических систем, теории надежности ИВС и в области качества ПС. Как указано выше, этот перечень не претендует на полноту и может быть модифицирован тем или иным образом. Для примера далее будут приведены определения свойства надежности программ, используемые в этих областях знаний.

Ясно, что ПС являются специфическим объектом, с определенными особенностями, затрудняющими традиционные подходы, применяемые в области общей теории надежности технических систем. Однако, в настоящий момент продолжают действовать ГОСТ 27.002–89 [4] и ряд других стандартов, хотя многие из них давно требуют пересмотра и уточнения. Эти стандарты и многие литературные источники в области классической надежности не рассматривают специфику ПС, но они обязательно должны быть учтены. Стандарт [4] определяет надежность как «свойство объекта сохранять во времени в установленных пределах значения всех параметров, характеризующих способность выполнять требуемые функции в заданных режимах и условиях применения, технического обслуживания, хранения и транспортирования».

Отметим здесь книгу [3], в которой подробно обосновывается необходимость рассмотрения надежности информационных систем и программ с учетом специфики их создания и функционирования. Добавим, что классические термины и показатели общей теории надежности могут быть применены для некоторых видов ПС, но не для всех.

Дискуссия о необходимости обновления стандартов в области терминологии во многом основывается на появлении новых объектов анализа надежности. В частности, этому способствуют успехи в области компьютерных наук. Отдельные авторы давно отмечают необходимость пересмотра базовой терминологии надежности специально для информационно-вычислительной техники. Это во многом продиктовано и необходимостью учитывать терминологические особенности международных стандартов и научных публикаций. Фундаментальной проработке этих вопросов посвящена работа [5] и ряд предшествующих ей. Эти работы призваны однозначно определить терминологию и фундаментальные представления в области общей теории надежности ИВС. Поскольку в них предложен общий подход, возможно применение этих результатов и при рассмотрении надежности ПС как важнейшей части ИВС. Надежность в [5] определена как способность системы предоставлять обслуживание, которому можно доверять.

Еще одним важным компонентом в наборе для описания надежности функционирования программ является подход, основанный на проработке проблематики качества ПС. Действительно, стандарты в области качества ПС оперируют терминами надежности, поскольку рассматривают ее как элемент качества. Например, стандарты [6–8] рассматривают надежность как характеристику качества программ. Эти документы предлагают описывать надежность комплексом атрибутов, включающим свойства восстанавливаемости, устойчивости к ошибкам, устойчивости функционирования и др. К сожалению, эти стандарты, хотя и продолжают действовать, но уже давно считаются устаревшими. Тем не менее, они предоставляют набор терминов, пригодных для описания надежности ПС. Отметим здесь формулировки для свойства надежности. В стандарте [6] определения надежности нет, в [7] – это набор атрибутов, относящихся к способности программного обеспечения «сохранять свой уровень качества функционирования при установленных условиях за установленный период времени», а в [8] — совокупность свойств, характеризующая «способность программного средства сохранять заданный уровень пригодности в заданных условиях в течение заданного интервала времени» (уровень пригодности в [8] понимается как «степень удовлетворения потребностей, представленная посредством конкретного набора значений характеристик качества программного средства»).

Ясно, что выбор способов описания проблемной области производится по традиционным критериям минимальности и достаточности. Набор из трех перечисленных компонентов удовлетворяет условию минимальности, но, возможно, не отвечает требованию достаточности. Это объясняется широтой проблематики [1]. Часть вопросов могут потребовать расширения представленного здесь набора. Например, вопросы человеко-машинного взаимодействия и др.

Завершая данную работу, необходимо отметить, что возможны декомпозиции проблематики по различным моделям. Одним из возможных направлений в этом является декомпозиция по видам программной продукции. Ясно, что различные виды ПС могут быть по-разному описаны с точки зрения их надежности. Это объясняется различиями в сложности, функциональности, управлении ИВС, функционировании во времени, местом в иерархии информационных взаимодействий и т. д. Это задача на будущее.

Библиографический список

1. Потапов, И. В. Проблематика в области надежности программных систем / И. В. Потапов // Надежность. – 2015. – № 1 (52). – С. 53–57.
2. Перегудов, Ф. И. Основы системного анализа : 3-е изд. / Ф. И. Перегудов, Ф. П. Тарасенко. – Томск: Изд-во НТЛ, 2001. – 396 с.
3. Шубинский, И. Б. Функциональная надежность информационных систем. Методы анализа. / И. Б. Шубинский. – М. : ООО «Журнал «Надежность», 2012. – 296 с.
4. ГОСТ 27.002–89. Надежность в технике. Основные понятия. Термины и определения. – введ. 01.07.90. – М. : Издательство стандартов, 1989 г. – 24 с.
5. Basic Concepts and Taxonomy of Dependable and Secure Computing / A. Avizienis [et al.] // ISR Technical report TR 2004–47. – 2004. – P. 37.
6. ГОСТ 28195–89. Оценка качества программных средств. Общие положения. – введ. 01.07.90. – М. : Издательство стандартов, 1989. – 10 с.
7. ГОСТ Р ИСО/МЭК 9126–93. Информационная технология. Оценка программной продукции. Характеристики качества и руководства по их применению. – введ. 01.07.94. – М. : Издательство стандартов, 1994. – 10 с.
8. ГОСТ 28806–90. Качество программных средств. Термины и определения. – введ. 01.01.92. – М. : Издательство стандартов, 1991. – 8 с.