



Потапов И. В.

ПРОБЛЕМАТИКА В ОБЛАСТИ НАДЕЖНОСТИ ПРОГРАММНЫХ СИСТЕМ

В рамках методологии системного анализа в области изучения надежности программных систем рассматриваются основные проблемы, задачи и способы их решения. Представлены мнения о решении проблем надежности программных систем. Рассматриваемые проблемы упорядочены и систематизированы.

Ключевые слова: надежность, программное средство, программная система.

Введение

Уже в конце прошлого века наметилась тенденция к существенному перераспределению мирового рынка информационных технологий в пользу программного обеспечения (ПО). Сейчас средства вычислительной техники используются повсеместно. Это обуславливает интерес пользователей и разработчиков программных систем (ПС) к созданию качественной программной продукции, отвечающей требованиям современных мировых стандартов. Не останавливаясь подробно на общих вопросах, отметим одну важную особенность: в тех случаях, когда к функционированию систем с использованием вычислительной техники предъявляются повышенные требования по качеству, часто подразумевают такие свойства как надежность и безопасность ПО. В данной работе речь пойдет именно о надежности, как она понимается в технике, а не о других свойствах, характеризующих близкими по смыслу понятиями — «точность», «достоверность», «правдоподобие» и т. п.

В технологии разработки ПС при описании, изучении и проектировании широко используется методология системного анализа. Изучение надежности ПС тоже может опираться на эту методологию. Одной из важнейших стадий системного анализа является формирование проблематики [1]. В данной работе делается попытка обобщения проблем и задач пользователей и разработчиков надежного ПО. Формат журнальной публикации требует некоторого преобразования информации, получаемой при формировании проблематики, представленной в исходном виде «клубком» проблем. Можно рассматривать это преобразование как некоторую адаптацию исходного набора данных, сообщаемых заинтересованными сторонами. В литературе по системному анализу рекомендуется проводить упорядочение, классификацию и структурирование проблематики, что отчасти сделано в данной работе. В качестве цитируемых печатных источников выбраны основополагающие работы, отражающие важные идеи и тенденции, характерные для проблематики в области надежности ПС. Многие проблемы и задачи, возникающие перед современными исследователями, разработчиками и пользователями, являются фундаментальными в данной области знаний, поэтому цитируемые авторы и их публикации, включая самые ранние, вполне могут рассматриваться в качестве источников формирования основ проблематики. В качестве дополнительной цели данной работы можно указать

необходимость систематизации и анализа публикаций в области надежности программных систем.

Формирование проблематики

Специалисты часто указывают на то, что программные системы (например, в работе [2] — комплексы программ) являются сложными в том смысле, который вкладывают в это понятие исследователи в области теории систем и системного анализа. Это во многом определяет базовые проблемы и задачи разработки надежных ПС, среди которых основное внимание уделяется проектированию, отладке программ и диагностированию программных ошибок, контролю правильности функционирования отдельных компонентов и всей системы в целом. В [3] сложность считается одним из важнейших условий, определяющих ненадежность ПС. В работе [4] указывается на взаимосвязь сложности и качества ПО, управление которыми дополняет проблематику надежности. Согласно мнению авторов книги [5] проблематика теории надежности ПО опирается на вопросы, связанные с изучением работоспособности сложных ПС.

Важную часть проблематики надежности ПС составляют вопросы изучения ошибок в программах [3, 5, 6], поскольку их наличие — одна из главных причин появления отказов в работе ПС. Само определение терминов «ошибка» и «отказ» ПС является отдельной проблемой.

В [2] проанализированы понятия корректности программ и программных ошибок. В проблематику может включаться разработка методики оценки корректности и отсутствия ошибок. При этом самостоятельными проблемами являются точное определение понятия ошибки для достоверного выявления наличия и причин их появления и разработка методов их обнаружения, поскольку наличие ошибок во многом определяется ожиданиями пользователей и не всегда точно формализуется [2, 3, 7]. Учет пользовательских ожиданий в проектировании ПС [3] вполне может рассматриваться как заметная часть проблематики надежности. В этой же книге много внимания уделено той части проблематики, которая связана с появлением ошибок в программах и проявлением их в виде отказов ПС. В [2] указывается на важность задач классификации, выявления характеристик и анализа статистики ошибок, статистического определения полного числа ошибок в программе. Эта проблема и некоторые подходы к ее решению обсуждаются в работах [8, 9], авторы которых делятся своим опытом по разработке методологии и практическому выполнению классификации и статистической обработки программных ошибок. При этом значимыми проблемами являются организация сбора данных для изучения и классификация ошибок [7, 9].

Эту часть проблематики можно дополнить вопросами изучения структуры текстов программ для получения статистических характеристик, по которым можно по-

пытаться сделать выводы о тех или иных свойствах ПС, в том числе о надежности [4]. Можно предполагать, что применение подходящих методик составления структурных моделей позволит получать сведения о закономерностях в появлении программных ошибок.

Важной частью проблематики, определяющей применение традиционных подходов теории надежности, является выявление того, что является случайной величиной, случайным процессом и т. д. Здесь важно, что программные ошибки сами по себе не являются случайными величинами. Специалисты указывают на то, что случайными событиями являются проявления ошибок при функционировании ПС [2, 8, 10, 11]. Случайность объясняется тем, что для проявления ошибки необходимо возникновение соответствующей ситуации — комбинации некоторого состояния системы и входного воздействия. Поскольку эти комбинации достаточно редки и плохо предсказуемы, появляются основания для рассмотрения момента проявления программной ошибки в качестве случайной величины. Иными словами, в рамках проблематики надежности ПС возможно рассмотрение характеристик потоков входных воздействий.

В проблематике ошибок содержатся и вопросы, возникающие в связи с необходимостью уменьшения числа ошибок проектирования ПС [2, 10]. В работе [8] подчеркивается необходимость предупреждения ошибок и контроля надежности в ходе проектирования, создания и внесения изменений в ПС, а в ходе эксплуатации — применения специальных систем защиты от нарушений функционирования. В [7] сформулированы и детализированы проблемы обоснования требований к надежности ПС и организации проектирования систем с требуемой надежностью. Там же приведена подробная классификация факторов, определяющих проблематику в области надежности ПС.

Важное место в проблематике надежности занимает совокупность вопросов функциональной безопасности ПС, изучаемых схожими методами. Одно из основных отличий, требующее терминологического разделения этих понятий, состоит в том, что при анализе функционирования ПС рассматриваются не все отказы, как это принято в теории надежности, а только те, что приводят к последствиям, отражающимся на безопасности [10]. О надежности ПО, измеряемой потерями, которые несет пользователь из-за ошибок в проектировании и функционировании систем, говорится в [7]. Там же определена важная часть проблематики надежности — необходимость учета особенностей эксплуатации ПС.

Одной из центральных проблем в области надежности ПС является существенное отличие компьютерной программы от технического устройства. Требования по надежности формируются специалистами, ориентирующимися на традиционные понятия теории надежности и действующий стандарт, разработанный для технических систем. Между тем, программные системы отличаются от технических настолько значимо, что традиционные подходы могут оказываться либо вовсе неприменимы,

либо могут применяться ограниченно. Например, в [8] прямо говорится о том, что изучение надежности ПС должно быть преимущественно ориентировано на системы реального времени и там же отмечается невозможность расчета надежности ПС обычными методами (данное высказывание несколько смягчается в том смысле, что обычные подходы ограничено применимы только для систем реального времени). Трудности аналитических расчетов надежности и функциональной безопасности ПС отмечены также и в [10]. Это позволяет дополнить проблематику, указав необходимость в определении соответствующих терминов, показателей надежности и подходов к аналитическим, статистическим и экспериментальным исследованиям надежности ПС. При этом необходимо точно представлять отличия ПС от других технических систем с точки зрения надежности. Они достаточно объемно сформулированы в нескольких основополагающих работах, среди которых можно отметить [3, 5, 8, 10, 12–14]. Эти отличия во многом определяют и дополняют соответствующие компоненты проблематики: необходимо разрабатывать специальные подходы к исследованию надежности ПС, уделять особое внимание стадии проектирования, четко определить терминологию и критерии применения терминов. Например, большое значение [3, 5, 12] имеет определение понятий «ошибка», «надежность» и т. д.

В [2, 10] рассматриваются две разновидности программных систем, первая из которых характеризуется тем, что исполнители могут уделять меньше внимания вопросам надежности, поскольку качество этих ПС имеет значение в основном только для самих разработчиков. Автор указывает на то, что вопросы надежности приобретают смысл в основном для ПС второго типа, более похожих на другие промышленно выпускаемые продукты.

В [2, 8, 10] обсуждается использование показателей надежности технических систем. В качестве пригодных для анализа ПС предложено рассматривать наработку на отказ и коэффициент готовности. Классификация моделей, предназначенных для расчета показателей надежности ПС, вместе с обсуждением соответствующей проблематики приводится в [5]. Например, известна проблема определения показателей надежности ПС, поскольку некоторые важные характеристики качества (число программных ошибок и т. п.) не вполне годятся для оценки надежности. Дополняет эту часть проблематики необходимость учета особенностей, отличающих программы от других технических изделий. В работе [12], например, рассматриваются некоторые показатели надежности, учитывающие специфику отказов ПС.

Существуют разные подходы к оценке надежности ПО в составе информационных систем [7, 14]. С одной стороны, ПО является чрезвычайно важным компонентом и его надежность необходимо оценивать самостоятельно. С другой стороны, при рассмотрении информационных систем предполагается, что отказы вычислительной техники и ПО взаимозависимы, то

есть надежность таких систем должна оцениваться комплексно.

Отказы ПС могут возникать при появлении данных, которые не были учтены при отладке и тестировании [2, 6]. Существует проблема регистрации отказов в ходе испытаний ПС на надежность, поскольку они сравнительно редко проявляются, проведение экспериментов над ПО является сравнительно трудоемкой задачей, а стоимость таких экспериментальных исследований, особенно при изучении функциональной безопасности, может быть достаточно высокой [7, 8, 10].

Может возникнуть необходимость в решении задачи классификации отказов и сбоев по длительности восстановления, поскольку от этого зависит фиксация нарушения работоспособности ПС. Для повышения надежности важно правильно организовать процедуру восстановления системы после отказов. В некоторых случаях, с учетом соответствующих временных показателей, восстановление позволяет преобразовывать отказы в менее значительные по своим последствиям сбои — данные идеи и терминология характерны для [2, 10]. В этих же работах помимо классификации отказов и сбоев уточняется и детализируется проблематика по вопросам восстановления ПС и использованию для этих целей различных видов избыточности.

Проблематика целесообразности введения и соответствующего использования избыточности в программы, данные и процессы функционирования ПС обсуждается многими авторами, например [2, 4, 13]. Как правило, смысловое наполнение терминов в этом вопросе вполне соответствует традиционному для теории надежности. В основном рассматриваются программная (алгоритмическая), информационная и временная избыточности. В этом контексте появляются традиционные вопросы о постановке оптимизационных задач [2], то есть проблематика дополняется базовой проблемой оптимизации использования избыточных ресурсов. При этом, однако, не вполне ясно как количественно оценивать уровень надежности ПС при соответствующих затратах. На основе [4] можно предложить рассматривать эту проблему совместно с группой вопросов о сборе и анализе статистической информации. С другой стороны дополняет эту часть проблематики мнение о недостаточной эффективности введения избыточности и резервирования [13].

В книге [14] и цитируемых в ней работах при рассмотрении вопросов о классификации и причинах появления программных ошибок, что само по себе является частью проблематики надежности ПС, затрагивается еще одна важная тема — влияние человеческого фактора на надежность ПС, точнее, проблема оценки этого влияния и свойств программиста (или коллектива программистов). Некоторые аспекты данной области проблематики также обсуждаются в работах [3, 5, 9, 12, 15].

Особое значение в проблематике надежности ПС приобретает необходимость построения моделей исследуемых систем и процессов ввиду их сложности. Существенную роль играют допущения [2], в рамках которых

строятся математические модели. Важно, что время, как параметр математических моделей, не имеет того значения, которое присуще исследованиям надежности других технических систем [5], за исключением, возможно, ПС реального времени [2, 8, 10]. В качестве недостатков, дополняющих проблематику моделей надежности ПС, в [8] отмечено, что модели прогнозирования надежности, построенные с применением классических подходов, могут оказаться пригодны только в условиях большого числа отказов, а попытки их применения к хорошо отлаженным и высоконадежным ПС не дают приемлемых результатов. В литературе приведено описание большого числа разработанных для исследования надежности ПО математических моделей, классифицируемых по различным основаниям [6, 11, 13].

Важную часть проблематики надежности составляют смежные вопросы качества ПС. Действующие в настоящее время стандарты в этой области, определяющие надежность как одну из характеристик качества, могут считаться устаревшими. Специалисты обращаются к более современным редакциям международных стандартов или аккуратно обходят эти вопросы стороной. В любом случае вопросы качества — это тема для отдельной работы. Поскольку здесь задача анализа качества не является основной, далее коротко будут отмечены несколько более общих вопросов, которые могут быть важны для дальнейших исследований.

Надежность рассматривается специалистами как одна из характеристик качества ПС [8, 10, 14]. Проблематика качества, как и проблематика надежности, может включать вопросы, связанные с определением показателей качества и соответствующим управлением. В [4] с качеством ПС связывается ряд вопросов, касающихся сложности их структуры. Рассматриваются специальные показатели сложности ПС и отдельных компонентов. В [9] к проблематике надежности добавляется задача анализа структурных особенностей программ. Проблема оценки сложности ПС и взаимосвязи сложности с надежностью описана в [5], где, в частности, указывается на зависимость ошибок не от объемов программного кода, а от структуры ПС, исключается возможность обобщения результатов исследования ошибок, в том числе и при сохранении постоянных условий разработки, и предполагается индивидуальный подход в этом вопросе к каждой вновь создаваемой ПС. В [14] определение качества связывается с полезностью программ, что согласуется с той вышеописанной частью проблематики надежности и качества ПС, в которой рассматриваются программные ошибки и отказы функционирования в контексте пользовательских ожиданий.

Заканчивая формирование проблематики, необходимо вернуться к вышеупомянутому вопросу совершенствования стандартов в области надежности и качества ПС [8, 10]. Возможно, решение данных проблем находится в одной плоскости с общими проблемами стандарта в области надежности, описанными в [16]. Важнейшими проблемами для надежности программных систем яв-

ляются стандартизация терминологии [10] (особенно в отношении базовых понятий — отказа, работоспособного состояния ПС и т. д.), формализация показателей надежности и качества, совершенствование технологии создания и сопровождения. Вопросы стандартов здесь подробно рассматриваться не будут, поскольку это большая тема для отдельной работы.

Обсуждение и выводы

Формирование проблематики — это только начало в анализе проблемной области. На данной стадии еще рано делать окончательные выводы и принимать решения, но можно сделать некоторые предположения относительно дальнейшего направления усилий исследователей, работающих в этой области знаний.

Например, можно утверждать, что для комплексного изучения и решения перечисленных проблем необходимо применять системноаналитические методы. Это высказывание имеет следующие основания. Во-первых, отмечаются сложности в применении традиционных формальных методов, что вызвано очевидными трудностями формализации рассматриваемых процессов, громоздкостью описания объектов, многокритериальностью задач принятия решений и т. д. Во-вторых, частные задачи, полученные в результате декомпозиции общей проблемы, характеризуются меньшей неопределенностью и, вероятно, могут быть решаемы с учетом необходимости их дальнейшего объединения для получения общесистемных результатов.

Можно отметить, что выполненные здесь в простейшем виде классификация и упорядочение проблем не являются единственными. Практика системноаналитического исследования предполагает рассмотрение различных способов переработки проблематики. Возможно, один из вариантов лучше других позволит приблизиться к вышеописанному подходу в получении комплексного решения.

Рассмотрение почти каждой отдельной из перечисленных в данной работе проблем может привести к пессимистическим выводам о том, что универсального решения не существует. Это становится ясно, например, в тот момент, когда возникает необходимость принять решение об исследовании надежности ПО как составной части программно-аппаратных комплексов или как самостоятельного объекта. Аналогично затруднено принятие решений и по многим другим ключевым вопросам. Вероятно, улучшение в данном вопросе может быть достигнуто через развитие самостоятельной теории надежности ПС при рассмотрении всего комплекса проблем методами системного анализа.

Еще одним возможным направлением в решении проблем надежности является изучение качества ПС. С одной стороны, качество характеризуется через показатели надежности, а с другой — надежное функционирование возможно только в случае достижения высокого качества проектирования, реализации и сопровождения

ПС. Особое внимание исследователей должно быть уделено вопросам, связанным с учетом человеческого фактора, поскольку разработка ПС — это трудно формализуемый творческий процесс.

Обобщая вышеизложенное, отметим, что в данной области исследования, возможно, необходимо разрабатывать самостоятельную теорию, а не опираться на традиционную теорию надежности технических систем. Это обусловлено спецификой ПС, усложняющей изучение их надежности через рассмотрение надежности отдельных компонентов. Здесь же добавим, что методология системного анализа предполагает участие в изучении и решении поставленных задач специалистов из разных областей знаний. Этому способствует появление печатных работ, в том числе обобщающих, направленных на систематизацию знаний, стимулирующих дальнейшее продвижение в данном исследовании. Возможно, в этом направлении может быть найден подход к решению упомянутых в [17] на стр. 4 инженерных задач.

Литература

1. **Перегудов Ф.И., Тарасенко Ф.П.** Основы системного анализа : 3-е изд. Томск: Изд-во НТЛ, 2001. 396 с.
2. **Липаев В.В.** Проектирование программных средств: М.: Высш. шк., 1990. 303 с.
3. **Майерс Г.** Надежность программного обеспечения: пер. с англ. М.: «Мир», 1980. 360 с.
4. **Штрик А.А., Осовецкий Л.Г., Мессих И.Г.** Структурное проектирование надежных программ встроенных ЭВМ. Л.: Машиностроение. Ленингр. отд-ние, 1989. 296 с.
5. **Пальчун Б.П., Юсупов Р.М.** Оценка надежности программного обеспечения. СПб.: Наука, 1994. 84 с.
6. **Полонников Р.И., Никандров А.В.** Методы оценки показателей надежности программного обеспечения. СПб.: Политехника, 1992. 78 с.
7. **Шураков В.В.** Надежность программного обеспечения систем обработки данных : 2-е изд., перераб. и доп. М.: Финансы и статистика, 1987. 272 с.
8. **Липаев В.В.** Надежность программных средств. М.: СИНТЕГ, 1998. 232 с.
9. **Тейер Т., Липов М., Нельсон Э.** Надежность программного обеспечения : пер. с англ. М.: Мир, 1981. 323 с.
10. **Липаев В.В.** Надежность и функциональная безопасность комплексов программ реального времени. М.: ЗАО «Светлица», 2013. 192 с.
11. **Черкесов Г.Н.** Надежность аппаратно-программных комплексов : СПб.: Питер, 2005. 480 с.
12. **Карповский Е.Я., Чижов С.А.** Надежность программной продукции. К.: Тэхника, 1990. 160 с.
13. **Смагин В.А., Дорохов А.Н.** Основы теории надежности программного обеспечения : СПб.: Балт. гос. техн. ун-т., 2009. 304 с.
14. **Шубинский И.Б.** Функциональная надежность информационных систем. Методы анализа. М.: ООО «Журнал «Надежность», 2012. 296 с.
15. **Абрамова Н.А.** О некоторых мифах в оценке качества программного обеспечения // Надежность. 2004. № 1. С. 38–63.
16. **Нетес В.А., Тарасьев Ю.И., Шпер В.Л.** Актуальные вопросы стандартизации терминологии в области надежности // Надежность. 2014. № 2. С. 116–119.
17. **Ушаков И.А., Шубинский И.Б.** Насущные проблемы инженерной надежности (Кто мы? Откуда мы? Куда мы идем?) // Надежность. 2012. № 1. С. 3–4.