УДК 621.321

О.Н. ОДАРУЩЕНКО, Ю.Л. ПОНОЧОВНЫЙ, Е.Б. ОДАРУЩЕНКО

Полтавский военный институт связи, Украина

ТЕРМИНОЛОГИЧЕСКИЕ АСПЕКТЫ ТЕОРИИ НАДЕЖНОСТИ ПРОГРАММНЫХ СРЕДСТВ

Рассмотрены основные термины дефектологии современных программных средств. Определены причины отсутствия единого подхода к терминологическим аспектам теории надежности ПС, расширена классификация дефектов ПС, а также уточнены причинно-следственные связи возникновения отказов ПС.

дефектология, дефект, ошибка, сбой, отказ, классификация дефектов, причинно-следственная связь отказов ПС

Введение

На современном этапе научно-технического прогресса (НТП) остается актуальной задача обеспечения надежности сложных систем и их элементов, в частности, программных средств (ПС). Для решения задач обеспечения надежности ПС созданы такие консорциумы, как High Dependability Computing Consortium, Sustainable Computing Consortium, Dynamic Assembly for System Adaptability, Dependability and Assurance [1]. В рабочих проектах данных организаций предусмотрено создание моделей ПС, в которых надежность ПС количественно оценивается как функция от некоторого множества переменных. В качестве переменных выступают различные параметры ПС и внешней среды, наиболее характерными из которых являются ансамбли дефектов ПС (переменные, описывающие количество определенных видов дефектов). Очевидно, что в условиях наличия различных видов дефектов ПС необходимо уточнить их определение в рамках дефектологии ПС. При этом под дефектологией ПС понимается раздел теории надежности ПС, в котором исследуются причинно-следственные связи возникновения и проявления дефектов ПС различных видов.

1. Формулирование проблемы

Анализ литературных источников [2–9] указывает на существенное несоответствие терминов и подходов разных авторов. Не проводился хронологический анализ причинно-следственных связей возникновения отказа в ПС. В связи с этим целью статьи является исследование терминологических аспектов теории надежности ПС и уточнение ряда базовых понятий.

Для этого необходимо:

1. Провести анализ подходов различных авторов и раскрыть причины расхождения мнений различных исследователей.
2. Уточнить основные термины дефектологии ПС – дефект, ошибка, отказ.
3. Уточнить причинно-следственные связи возникновения отказов ПС.
4. Расширить классификацию дефектов применительно к современным ПС.

2. Анализ существующих подходов

Дефектология ПС является сравнительно молодым разделом теории надежности ПС. Ее элементы рассматриваются в работах [3–8], но лишь в последних исследованиях, например в [9], просматривается целостная информация относительно этого вопроса. Анализ источников показывает близкое сходство понятий дефектологий ПС и физических систем (последние достаточно хорошо описаны в [2]), что вполне логично – теория надежности физических систем является полной и структурированной нау-

кой, чего, к сожалению, нельзя сказать о теории надежности ПС. Поэтому представленный ниже хронологический анализ литературных источников начат с рассмотрения вопросов дефектологии физических систем.

Под **дефектом** понимается каждое отдельное несоответствие объекта установленным требованиям нормативно-технической и (или) конструкторской документации (НТД и КД), снижающее его уровень надежности [2]. Следует отметить, что дефект рассматривается как возможная причина возникновения отказа, но наличие дефекта не означает, что отказ произошел. Под **отказом** понимается событие, заключающееся в нарушении работоспособного состояния системы. Отказу может предшествовать **повреждение** – событие, заключающееся в нарушении исправного состояния объекта при сохранении работоспособного состояния.

На рис. 1 изображена причинно-следственная связь возникновения отказа в физических системах [2].

Рис. 1. Причинно-следственная связь возникновения отказа в физических системах

Обычно дефекты классифицируются по признаку стадии происхождения так:

– дефекты (ошибки) проектирования;
– дефекты изготовления (производственные);
– дефекты эксплуатации.

На рис. 2 изображены причинно-следственные связи возникновения отказа в ПС, построенные на основе анализа литературных источников [3–8].

На начальном этапе развития теории надежности ПС понятие дефект ПС употреблялось в технической литературе довольно редко. Так, Г. Майерс [3], которого считают основоположником теории надежности ПС, дал следующие определения: «В программном обеспечении (ПО) имеется **ошибка**, если оно не выполняет того, что пользователю разумно ожидать от него; **отказ** ПО – это проявление ошибки в нем». Эстафету подхватили наши ученые, и в работе [5] под **ошибкой** понимается изъян программы, приводящий к отказу, а **отказ** – это отклонение характеристик процесса функционирования за допустимые пределы.

Определение дефекта ПС упоминается в [6], где «**дефект** – это такая вариация структуры ветви вычислительного пути (другое месторасположение оператора, его замена или его отсутствие), которая приводит к неправильности вычислений при задании вектора входных величин на соответствующей дефектной входной области $\{X\}$; дефект является следствием чьих-либо ошибочных действий». В данном источнике уже просматриваются элементы дефектологического анализа ПС. В частности, указывается, что отказы ПС обусловлены только наличием дефектов в ПС. **Ошибка** определяется как результат какого-либо процесса (функционирования некоторой системы). Указывается некорректность определения ошибки ПС как единственной причины их отказов и обосновывается многозвенность причинно-следственной связи возникновения дефектов ПС «… – ошибка – дефект – ошибка – …».

Исследования, представленные в [6], совпадают в какой-то мере с результатами, приведенными в [4]. В этом источнике под **ошибкой** понимается причина, обуславливающая **дефект** программы, который проявляется в **отказах** программы в процессе ее внедрения. Однако в этом источнике отмечается схожесть терминов «ошибка» и «**проблема**» – ситуация, когда пользователь зафиксировал какие-либо отклонения от ожидаемых результатов функционирования ПС.

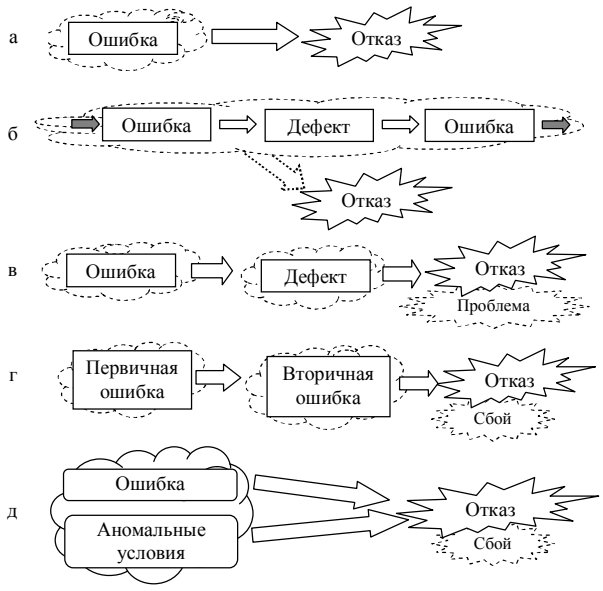


Рис. 2. Причинно-следственные связи возникновения отказов ПС из источников: а – [3,5]; б – [6]; в – [4]; г – [7]; д – [8]

В пособии [7] авторы возвращаются к концепции использования термина «ошибка ПС». Здесь **ошибка** – это неправильность, погрешность или непреднамеренное искажение объекта или процесса. Причинно-следственная связь возникновения отказа включает в себя *первичные ошибки* – искажения в тексте программы, требующие корректирования, и *вторичные ошибки* – искажения выходных результатов выполнения программ. Под **отказом** понимается: отклонение результатов выполнения настроенных программ; нарушение кодов записи программ в памяти команд; стирание или искажение данных в оперативной или дисковой памяти; нарушение нормального хода вычислительного процесса. Проявлением вторичной ошибки может быть **сбой** – самоустраняющийся отказ, не требующий внешнего вмешательства для замены отказавших компонент ПС. В этой работе рассматривается три класса ошибок: программные, алгоритмические и системные.

В [8], как в официальном документе, употребляются следующие определения: **отказ** – это событие, заключающееся в проявлении неработоспособности ПС; **ошибка** – запись элемента программы, или программной документации, исполнение которой приводит (или может привести) к непредвиденной ситуации. В этом документе также употребляется термин **аномальные условия** – сбои и отказы технических средств, ошибки операторов и ошибки в исходных данных.

Хотелось бы отметить тенденцию увеличения количества звеньев связи по мере увеличения сложности ПС, в частности, трехзвенные связи характерны для модульных ПС (рис. 2, б – д).

Наконец, в [9] приведено достаточно полное описание дефектологии ПС. Здесь **дефект** – это явная или гипотетическая причина **отказов** системы, то есть отклонений от результатов корректного обслуживания пользователей ПС. Там же предложена причинно-следственная связь возникновения отказов ПС, которая является многозвенной, что характерно для современных многокомпонентных ПС (рис. 3).

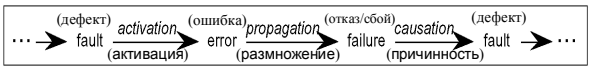


Рис. 3. Причинно-следственная связь возникновения отказов ПС

В этом же источнике представлена обширная классификация дефектов ПС, показанная на рис. 4.

Кроме указанных на рис. 4 в статье упоминаются еще три признака классификации:

- по видам отказов, обусловленных дефектами (например, отказы, терпимые пользователем, и «византийские» отказы);
- по возможности проследить весь ансамбль причин, при котором проявился дефект (жесткие, или уловимые дефекты и мягкие, или неуловимые дефекты);
- по количеству причин в ансамбле, при котором проявился дефект (простые и множественные дефекты, последние, в свою очередь, рассматриваются как независимые или связанные).

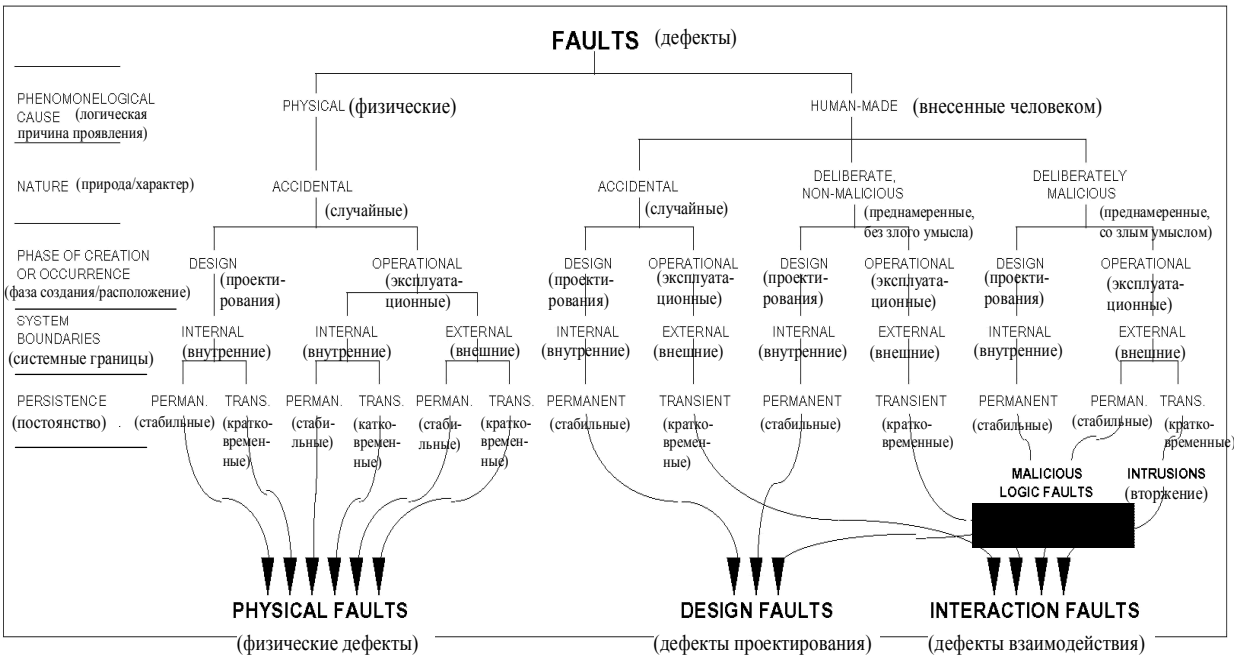


Рис. 4. Классификация дефектов ПС

3. Уточнение терминов

Что же является причиной отказа ПС – ошибка или дефект? Решение данного вопроса подобно нахождению ответов на философские парадоксы «Кто виноват и что делать?» и «Что было раньше – курица или яйцо?». Очевидно, что придется вспомнить некоторые философские категории, как указывалось в [6]. Как уже упоминалось ранее, рост сложности ПС обусловил увеличение количества звеньев в причинно-следственной связи возникновения отказа ПС; отсюда вытекает первая причина разногласий исследователей – они рассматривали ПС различного уровня сложности. Второй причиной разногласий является огромное разнообразие ПС, располагающихся на разных уровнях программной иерархии: операционные системы, драйвера, программы-приложения, компиляторы, загружаемые библиотеки и др. Свою лепту внесли и переводчики: с английского термин "fault" переводится и как дефект, и как ошибка, поэтому, чтобы подчеркнуть отличие ПС от физических систем, в дефектологии ПС часто употребляется термин «ошибка». Такой перевод, например, характерен для [8]. Но следует отметить, что в [9] для обозначения ошибки ПС используется термин "error".

Переход на современные подходы к оценке качества сложных систем, когда критерием отказа в первую очередь является не нарушение требований НТД и КД, а оценка пользователя, вносит свои коррективы при определении терминов дефектологии ПС. С учетом этих тенденций, а также принимая во внимание замечания, указанные в [6], предлагается следующее определение: **дефект ПС** – это всякое искажение программного кода, включая и отсутствие отдельных его участков (обусловленное недоработками проектной документации), которое приводит к невыполнению ПС всего перечня функций, ожидаемых пользователем. При этом дефект является статической характеристикой ПС – он присутствует в программном коде, даже когда программа не запущена.

Напротив, ошибка является результатом действия, функционирования ПС, его динамической характеристикой. Предлагается следующее определение: **ошибка ПС** – это проявление выполнения дефектного участка программного кода. Ошибка занимает промежуточное значение между дефектом и

отказом. **Отказ ПС** – это событие нарушения работоспособного состояния ПС, основным критерием которого является оценка пользователя. Иными словами, отказ заключается в проявлении события, когда пользователь зафиксировал факт отклонения характеристик функционирования ПС от их корректных значений. **Сбой** является самоустраняющимся отказом, не влияющим на работоспособность ПС.

Возникает вопрос, а что же происходит, если пользователь по какой-либо причине не заметил отклонений от корректного функционирования ПС (например, он отвлекся в момент проявления дефекта, или отказал удаленный компонент распределенного ПС)? В некоторых источниках в таких случаях говорят о скрытом отказе, однако авторы статьи на основе анализа причинно-следственных связей предлагают считать данную ситуацию проявлением ошибки ПС. При таком подходе хорошо объясняется связь «ошибка – дефект» на рис. 2, б, в.

4. Причинно-следственные связи отказов ПС

Концептуальный подход пользовательского критерия оценки работоспособного состояния ПС поддерживает (в отличие от [8]) только одну причину отказов – наличие дефектов ПС. Поэтому причинно-следственная связь возникновения отказа ПС модифицирована, как показано на рис. 5.

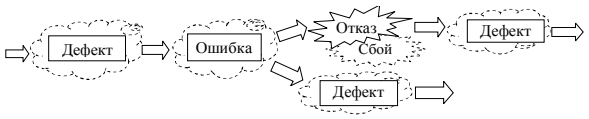


Рис. 5. Модифицированная причинно-следственная связь возникновения отказов ПС

Вышеприведенные сведения возможно объединить в табл. 1.

5. Классификация дефектов

Из предложенного определения дефектов ПС вытекает глобальный признак классификации дефектов – по типу кодового представления. По этому признаку дефекты ПС можно разделить на два класса:

– дефекты, связанные с искажениями программного кода, не изменяющими его объем;
– дефекты, связанные с отсутствием отдельных элементов программного кода (блоков, модулей, подпрограмм и др.).

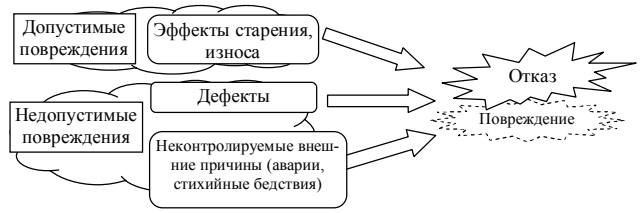
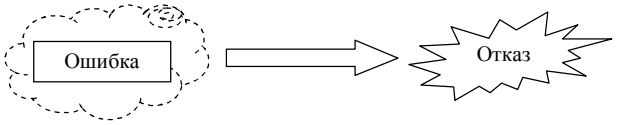
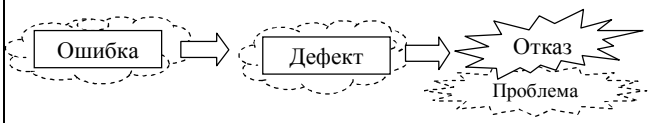
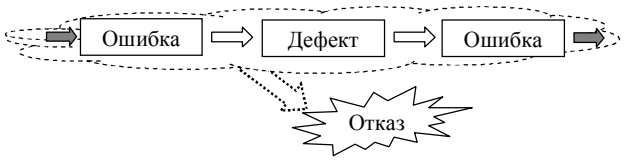
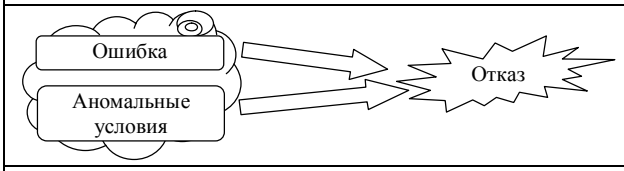
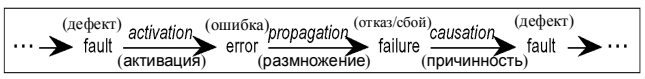
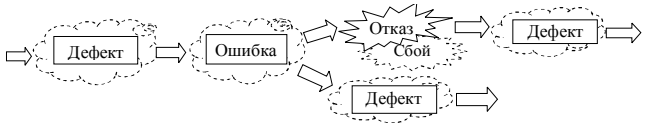
Относительно дефектоскопии физических систем второй класс дефектов описывает вторую причину проявления отказов при недопустимых повреждениях: отказы ПС происходят потому, что в программном коде изначально не предусмотрены «элементы защиты» (обработчики исключительных ситуаций, мониторинговые подпрограммы и др.), реагирующие на неконтролируемые внешние воздействия – аномальные условия.

Очевидно, что в отличие от физических систем [2] ПС не подвержены эффектам старения и износа, поэтому в причинно-следственной связи возникновения отказов ПС отсутствует звено – аналог допустимых повреждений физических систем. Однако следует отметить, что для ПС характерно явление «морального» старения, связанное с постоянным ростом требований пользователей, обуславливающих высокую динамичность программной инженерии и, как следствие, постоянное изменение внешних условий применения ПС. На лицо эффект старения НТД – на момент создания ПС внешние условия отличались от условий, действующих на момент внедрения ПС. Устранить данный эффект позволяют кольцевые стратегии разработки ПС (например стратегия Гради-Буча) и стратегии сопровождения ПС.

Так как современные ПС являются объектными, взаимосвязанными и параллельными, то эти свойства можно использовать как признак классификации дефектов.

Таблица 1

Хронологическая последовательность причинно-следственных связей возникновения отказов

Причинно-следственная связь возникновения отказов	*Объект теории надежности*	*Количество звеньев в связи*	*Ключевые термины теории надежности*	*Год появления*
	Физические системы (аппаратная компонента)	1	Эффекты старения, дефект, повреждение, отказ	1950-е
	Немодульные ПС	1	Ошибка, отказ	1960-е
	Многомодульные ПС	2	Дефект, ошибка, проблема, отказ	1970-е
	Многомодульные ПС	≥ 2	Дефект, ошибка, отказ	1980-е
	Многомодульные ПС	1	Аномальные условия, ошибка, сбой, отказ	1994
	Многомодульные ПС	≥ 2	Дефект, ошибка, отказ	1999
	Многомодульные ПС	2	Ошибка, сбой, отказ	2003
Гармонизированный вариант				
	Многомодульные ПС	≥ 2	Дефект, ошибка, сбой, отказ	2004

Следует различать:

- дефекты объектов ПС (искажения в программном коде объектов, отсутствие определенных классов объектов);
- дефекты взаимосвязи (обработка набора входных данных неверным методом);
- дефекты параллельности или реактивности (несвоевременная обработка набора входных данных, поступление большого количества входных данных одновременно).

Заключение

В данной статье рассмотрены терминологические вопросы сравнительно молодого раздела теории надежности ПС – дефектологии ПС. На основе хронологического анализа выявлены причины отсутствия единого подхода к основным терминам дефектологии и предпринята попытка обобщить существующие подходы. Предложены уточнения определений дефекта, ошибки и отказа ПС, позволяющие гармонизировать подход различных авторов к данному вопросу. Уточнено место дефекта и ошибки ПС в причинно-следственной связи возникновения отказов ПС. На основе полученных данных планируется построение ряда новых моделей надежности современных ПС, которые будут учитывать взаимосвязи дефектов ПС с вызывающими их проявление воздействиями внешней среды.

Литература

1. Тибоди П.П. Чтобы программы стали лучше. Журнал "Открытые системы", #03, 2003 год // Издательство "Открытые системы" (http://www.osp.ru/) Постоянный адрес статьи: http://www.osp.ru/os/2003/03/011.htm.

2. Рыжкин А.А., Слюсарь Б.Н., Шучев К.Г. Основы теории надежности: Учеб. пособие. – Ростов н/Д.: Издат. центр ДГТУ, 2002. – 182 с.

3. Майерс Г. Надежность программного обеспечения. – М.: Мир, 1980. – 360 с.

4. Тейер Т., Липов М., Нельсон Э. Надежность программного обеспечения. Анализ крупномасштабных разработок. – М.: Мир, 1981. – 323 с.

5. Арсеньев Ю.Н., Журавлев В.М. Проектирование систем логического управления на микропроцессорных средствах: Учеб. пособие для вузов по спец. "Вычисл. машины, комплексы, системы и сети". – М.: Высш. шк., 1991. – 319 с.

6. Пальчун Б.П., Юсупов Р.М. Оценка надежности программного обеспечения. – СПб: Наука, 1994. – 84 с.

7. Проектування автоматизованих систем управління: Навч. посібник / Гаманєк В.О., Ільяшов О.А., Кисельов І.М.; Під ред. Б.П. Шохіна. – К.: ВІТІ НТУУ "КПІ", 2003. – 157 с.

8. ДСТУ 2850-94. Програмні засоби ЕОМ. Показники і методи оцінювання якості. Введ. 01.01.96. – К.: Держстандарт України, 1995. – 20 с.

9. Avizienis A., Laprie J.-C., Randell B. Fundamental Concepts of Dependability. Newcastle University Report no. CS-TR-739.

Поступила в редакцию 16.04.04

Рецензент: д-р техн. наук, проф. В.С. Харченко, Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ», г. Харьков