УДК 004.052: 004.414.23

Термодинамический подход к моделированию процесса роста надёжности ПС с учётом «вторичных дефектов»

В. О. Мищенко

Харківській національний університет імені В. Н. Каразіна, Україна

В статье на основе термодинамического подхода разработана концепция моделирования процессов роста надёжности программных систем, допускающая появление т.н. вторичных дефектов при исправлениях в системе. Отсутствие таких дефектов в процессе трактуется как свойство зрелости системы, которое означает завершение ею определённого фазового перехода. Обнаружение дефектов и появление новых в процессе исправлений могут воспроизводиться модельным генератором. Можно судить о точности существующих моделей надёжности, учитывающих вторичные дефекты, по их оценкам на основании статистики процесса имитации, подобной статистике реальных проектов.

Ключевые слова: *надёжность программных систем, вторичные дефекты, концепция, термодинамика, фазовый переход, имитационная модель, статистика, верификация.*

У статті на основі термодинамічного підходу розроблено концепцію моделювання процесів росту надійності програмних систем, яка допускає появу т.зв. вторинних дефектів при виправленнях в системі. Відсутність таких дефектів у процесі трактується як властивість зрілості системи, що означає завершення нею певного фазового переходу. Виявлення дефектів і поява нових в процесі виправлень можуть відтворюватися модельним генератором. Можна судити про точність існуючих моделей надійності, що враховують вторинні дефекти, за їхніми оцінками на підставі статистики процесу імітації, подібної статистиці реальних проектів на підставі статистики процесу імітації, подібної статистиці реальних проектів.

Ключові слова: *надійність програмних систем, вторинні дефекти, концепція, термодинаміка, фазовий перехід, імітаційна модель, статистика, верифікація.*

In this paper, the process of software system correction intended to make the system more reliable is considered and this process modeling concept, which allows emergence of so-called secondary defects in course of said correction, is developed based on the thermodynamic approach. The absence of such defects is interpreted as the property of system maturity, which means that certain phase transition is finished. Detection of defects and emergence of new ones in the process of system correction can be simulated with the help of some generator. One can make conclusions about the accuracy of existing probabilistic reliability models from the estimates of the number of secondary errors on the basis of simulation process statistics similar to the statistics of real projects.

Key words: *the reliability of software systems, secondary defects, concept, thermodynamics, phase transitions, simulation model, statistics, verification.*

1 Введение

Проблема адекватной оценки роста надёжности программных систем (ПС) в процессе систематических испытаний с возможным исправлением дефектов всегда вызывала повышенный интерес. Судя по всему, теория таких процессов нашла своё завершение (если не сказать, исчерпала себя) в рамках представлений о таком процессе, в котором новые дефекты не образуются, и который продолжается практически до исчерпания дефектов, первоначально имевшихся в ПС. Последнее время приобрели актуальность постановки задач, в

которых учитывается то обстоятельство, что исправление обнаруженных дефектов (ошибок) в сложной системе, которое повышает её надёжность, одновременно вносит в неё изменения, чреватые некоторым ослаблением этой надёжности. Для математических моделей, которые используют понятие остаточных дефектов (или ошибок), это, по сути, означает, что остаток вычитания из числа остаточных дефектов $N(t)$ числа δN исправленных между моментами t и $t+\Delta t$ дефектов может быть не равен $N(t+\Delta t)$. Если при моделировании процесса следят за динамикой остаточных дефектов, то в выражении для этой величины нужна добавка $\delta_2 N$ - число вторичных дефектов:

$$N(t+\Delta t) = N(t) - \delta N + \delta_2 N\,. \qquad (1)$$

Проблема в том, что наблюдаема только динамика обнаруженных дефектов, но выделить среди них в статистике проектов вторичные дефекты сложно [1].

Наш концептуальный подход состоит в постулировании необходимости отражения в динамических моделях роста надёжности, хотя бы в идеализированной форме, *обстоятельств* ликвидации и воспроизводства дефектов. В связи с этим полезно следить за зрелостью ПС. При её отсутствии дефекты кода не всегда могут быть объективно отделены друг от друга по замеченным проявлениям дефектности. Тогда ликвидация какого-то числа таких проявлений не гарантирует уменьшения числа (нечёткого!) «оставшихся в системе» дефектов на ту же величину даже без новых ошибок. Переход системы в зрелое состояние, в процессе чего одни дефекты уже можно отделить от других, напоминает фазовые переходы в веществах. При этом надёжность, возрастающая вместе с уменьшением дефектности кода, относится к его смыслу, а не к характеристикам архитектуры или объёма. Эти характеристики в процессе исправления дефектов в приобретающей зрелость системе или не меняются вовсе или изменятся слабо. В этом смысле затраты интеллектуальной энергии происходят скрытно, она передаётся «тепловым способом». Речь может идти об интеллектуальном тепле, известном как метрика процесса разработки ПС [2].

2 Известные примеры моделирования эволюции качества ПС с учётом «вторичных дефектов»

В работе [3], нацеленной на инициацию дискуссии по вопросам надёжности ПО, отмечается недостаток новых концепций математического моделирования в терминах дефектов, в том числе, вторичных дефектов:

“Predictive models based on the study of the process of identifying defects allow to foresee of the development of this process over time, and to obtain estimated reliability of the program. ... However, as the experience shows, none of these models can claim to be a universal one, each model "serves" its class of software systems, boundaries between the classes remain very shaky.

If you pay attention to the essence of scientific publications on the theory of software reliability, we can see that in the last twenty years, no fundamentally new ideas in this area have been proposed. … the attempts of mechanical introduction into the existing variable models, designed to take into account the secondary defects, were made. However, according to the authors [здесь в цитируемом тексте ссылка на работу [4]], it is practically impossible to introduce these variables into some models

and for some of them such complicated mathematical expressions are obtained, that their practical application becomes difficult." [3, C.60].

В изложении собственной концепции будем отталкиваться от известных подходов к задаче моделирования с целью прогноза эволюции качества программных систем в процессе их отладки или испытаний с исправлением обнаруженных дефектов. Они предполагают доступность статистики обнаружения дефектов и поддержку режима их исправления, при котором дальнейшему тестированию подвергается исправленная по поводу найденного дефекта система. Вероятностные модели такого процесса, например, рассматриваемые или упоминаемые в монографии [1, С. 13-18, 115-124], хорошо известны. Недавние исследования [4-8] (отраженные в [1]) связаны с тем, что за счёт дополнительной информации (или гипотез) возможно уточнение этих моделей с привлечением понятия вторичных дефектов/ошибок. Каждая из работ этого направления оговаривает класс рассматриваемых программных систем и уточняет этап жизненного цикла, ЖЦ (например, подготовка к эксплуатации, опытная или начальная эксплуатация ИС). В результате классы систем и период применимости моделей не совпадают, но методы всех работ применимы к далеко не пустому общему множеству систем (не только программных!) при сопоставимых условиях процесса обнаружения-исправления дефектов. Далее будем условно говорить о «времени», в котором протекает этот процесс, хотя в каждом конкретном случае эта величина, часто дискретная, понимается по-своему: как число контрольных периодов процесса испытания системы, число транзакций, наработанных в ансамбле одинаковых систем и т.п.

2.1 В работе [4] исследовалась принципиальная возможность учёта эффекта вторичных дефектов на основе существующих вероятностных моделей надёжности (ВМН) программных систем. Оказалось, что из 9 проанализированных моделей и семейств моделей только у 3-х такая перспектива определённо существует и может оказаться практичной в реализации. Однако эти модели после их модификации широкого применения пока не нашли, поскольку математически невозможна однозначная оценка всех их параметров на основании полученных данных о динамике обнаружения дефектов [1]. Впрочем, при наличии оснований для принятия определённых значений некоторыми из параметров, остальные можно определить, включая наиболее интересный с рассматриваемой точки зрения – число обнаруженных дефектов, возникших уже в процессе исправления дефектов, т.е., вторичных дефектов.

2.2 Подход [5] ориентирован на практическое извлечение информации о вторичных дефектах из опытных данных по динамике обнаружения дефектов при том, что эта динамика принимается приближенно имеющей, по крайней мере на каждом характерном этапе, постоянную скорость обнаружения дефектов при том, что они немедленно удалятся. «Во время исправления ошибок новые ошибки не вносятся. Это допущение позволяет создать идеальную модель на этапе эксплуатации УИС, на базе которой возможно построение реальной модели, в которой такое допущение снято» [5, С.207]. Такой шаг к более реалистичной модели был сделан [6] путём дополнения линейного дифференциального уравнения для интенсивности потока исключаемых

первичных дефектов уравнением для потока вносимых вторичных дефектов (подробнее в [1, С.47-58]). Траектории полученной таким образом модельной динамической системы можно рассматривать как возможные трендовые кривые для стохастических процессов, в том числе, при наличии вторичных дефектов.

2.3 Простейший, можно сказать, прикидочный вариант метода оценки наличия и количества вторичных дефектов представлен в [7,8]. Рассматривается ситуация, отмеченная при работе с реальной учётной ИС, когда тренд для кумулятивного числа дефектов можно считать сформировавшимся на начальном этапе процесса (это проверяется сравнением графика изменения кумулятивного числа дефектов с построенной аппроксимирующей кривой экспоненциального закона). Тогда участок (а, более общим образом, нужно полагать, участки), где разность между трендовым прогнозом числа обнаруженных и сразу устранённых дефектов и фактическим их числом положительна, считается бесполезным для анализа (обнаружение дефектов тормозилось какими-то объективными причинами), а участок (участки), для которых эта разность отрицательна, напротив, считается несущим искомую информацию. Эта разность принимается за ожидаемое число внесенных вторичных дефектов, а сумма всех таких разностей – за общее число таких дефектов. Подобная оценка может оказаться слишком грубой, прежде всего потому, что отклонения от трендовой кривой в большинстве случаев носят случайный характер.

2.4 В [9] близкий по идее метод имеет то принципиальное отличие, что учитываются только участки расхождения «тренда» с функцией дефектов на величину оценки, напрашивается сказать, своего математического ожидания. Эту величину, что бы она собой ни представляла, получают на основе правдоподобных предположений для каждого момента умножением квадратичного уклонения тренда от реальных данных по модулю (осреднённого по всей области функции дефектов) на величину обратную времени, прошедшему с начала процесса. Наконец, допускается та эвристика, что на заключительных этапах прогнозируемое число вторичных дефектов, отличное от нуля, игнорируется, если имеются соображения за то, что совершение ошибок при устранении найденных дефектов стало к данному моменту маловероятным.

2.5 Другой усовершенствованный вариант оценки вторичных дефектов основывается на оценке коэффициентов линейной модели второго порядка динамики дефектов (в духе феноменологической термодинамики), о которой шла речь выше в пункте 2.2 [1, С.47]:

$$\begin{aligned} \dot{f}_1 &= -A_1 f_1 - A_2 f_2 \\ \dot{f}_2 &= -A_2 f_1 - A_1 f_2 \end{aligned}, \qquad (1)$$

где f_1 – количество дефектов выходного потока, которые *ещё* находятся в системе в данный момент ($f_1(0) = F_0$ - число всех первичных дефектов);

$(-f_2)$ – количество дефектов входного потока, возникших в процессе и *пока* находящихся в системе без шансов немедленного обнаружения ($f_2(0) = 0$).

В этой модели величины, целочисленные в моменты их контроля, считаются интерполированными для всех промежуточных моментов с тем, чтобы иметь

гладкие функции времени. «Дефекты выходного потока» можно понимать как образно скажем, доступные для обнаружения в любой последующий момент. В начальный момент это все первичные дефекты. «Дефекты входного потока» - это возникшие вторичные, но ещё не «созревшие» для обнаружения дефекты. Смысл первого уравнения в том, что суммарный поток $\dot{f}_1$ слагается из отрицательного потока (убыль за счёт обнаружения дефектов), пропорционального количеству оставшихся первичных и ранее созревших дефектов $(-A_1 f_1)$ и положительного потока созревших $(A_2(-f_2))$, пропорционального числу незрелых. Смысл второго уравнения: суммарный поток $(-\dot{f}_2)$ слагается из положительного потока новых дефектов, пропорционального числу выходящих $(A_2 f_1)$, и отрицательного потока, связанного с созреванием, пропорционального числу незрелых $(-A_1(-f_2))$.

Система (1) легко решается при указанных начальных условиях [1, С.49,52]:

$$f_1 = F_0 \cdot ch(A_2 t) \cdot \exp(-A_1 t), \quad f_2 = -F_0 \cdot sh(A_2 t) \cdot \exp(-A_1 t), \tag{2}$$

и для числа, скажем так, «остаточных» дефектов получается простое выражение:

$$f_{1,2} = f_1 + f_2 = F_0 \cdot \exp\big((A_2 - A_1)t\big). \tag{3}$$

Кумулятивное число обнаруженных дефектов согласно рассматриваемой модели

$$\mu_1(t) = \int_0^t A_1 f_1(\tau) \cdot d\tau = F_0 A_1 \int_0^t f_1(\tau) \cdot d\tau = \frac{F_0 A_1}{2}\left[\frac{e^{(A_2 - A_1)t}}{A_2 - A_1} - \frac{e^{-(A_2 + A_1)t}}{A_2 + A_1}\right]_0^t =$$

$$\frac{F_0 A_1^2}{A_1^2 - A_2^2} - \frac{F_0 A_1}{2}\left(\frac{e^{A_2 t}}{A_1 - A_2} + \frac{e^{-A_2 t}}{A_1 + A_2}\right)e^{-A_1 t} \quad . \tag{4}$$

По известной функции кумулятивного числа фактически *обнаруженных* дефектов $\mu(t)$ предлагается определённым методом последовательных приближений строить приближающую функцию $\mu_1(t)$, определённую выражением для кумулятивного числа обнаруженных дефектов согласно *модели*, что приводит к идентификации параметров A_1, F_0, A_2 [1, С.92-94]. Критерием близости служит среднеквадратичное отклонение трендовой кривой $\mu_1(t)$ от $\mu(t)$, данной в дискретном времени (т.е. даны $\mu(t_1),\ldots\mu(t_n)$).

2.6 На самом деле валидность вероятностных и термодинамических моделей надёжности существенно зависит от сценария диагностики и ликвидации дефектов, который реализуется в отношении данной ПС на каждом этапе процесса обнаружения-исправления дефектов [1]. Формализация и анализ таких сценариев помогают обоснованно формировать процедуры моделирования и прогноза дальнейшей эволюции характеристик ПС (пример имеем в [9,1]).

«Вторичные дефекты» рассмотренных ВМН представлены в них дополнительными параметрами, а методы оценки используют величины, которые *предположительно* связанны с реально вносимыми в ПО дефектами. Тем самым, мы имеем дело с *метриками* для оценок числа таких дефектов, а не

с реальной характеристикой числа вторичных дефектов. Верификация этих метрик (в смысле корреляции их значений с числом фактических дефектов) и, тем более, валидация, на основе доступной и общепринятой статистики реальных программных проектов пока не представляется реальной. Больше того, прямой учёт вторичных дефектов, даже, если бы его пытались налаживать, сам по себе затруднён по многим причинам. Всё это авторы описанных подходов учитывали: «Основной проблемой при развитии и реализации предложенного подхода (как и для количественной оценки надежности ПС в целом) является получение репрезентативной информации о дефектах как первичных, так и вторичных …» [4, С. 216]. Поэтому они шли, преимущественно, по пути косвенной верификации, понимаемой их полезность для уточнения существующих процедур оценки надёжности в динамике.

Актуальным является поиск новых перспективных путей построения математических моделей надёжности ПС с учётом вторичных дефектов, и, что представляется ещё более важным, практичного способа верификации процедур оценки характеристик надёжности таких моделей. Этому поиску посвящена данная работа.

3 Феноменологический и статистический подходы к термодинамике ПС при вторичных ошибках

Наряду со статистикой дефектов и сценариями работы с ними, важен учёт особенностей разработки и проверки программ, в процессе которых и возникают дефекты. Это отмечают все исследователи. Однако в силу разнообразия и сложности механизмов этих процессов, их полный учёт, как и понимание относительной роль в конкретных проектах, пока что проблематичны.

Это подсказывает, что вместо многих деталей следовало бы, применяя *термодинамический подход*, отражать указанные механизмы с помощью макропараметров. Шаги в этом направлении вполне реальны.

Уже существующая *феноменологическая* термодинамическая модель процесса разработки ПС трактует его как эволюцию параметров взаимосвязанных исходных текстов модулей этой системы [10, раздел 4]. Время при этом удобно исключать, рассматривая вместо этого изменяющиеся объёмы разработки модулей, от которых *в зависимости от характера процесса* зависят трудность разработки (аналог давления в физике) и потенциальный объём (аналог температуры, - название параметра традиционное, хотя не во всех отношениях удачное). Эволюция параметров всех модулей продолжается, естественно, и в процессе их отладки, и в процессе испытаний и опытной эксплуатации. Установим, однако, два рубежа ЖЦ, связанных с обсуждавшимся во введении понятием зрелости ПС, как важным аспектом её надёжности.

Первый рубеж связан со стабилизацией интегральной метрики ПС – интеллектуального тепла [10,11]. График этой величины (разности между метриками спецификационной энергией и работы программирования системы [11]) демонстрирует в начале разработки колебания с большим размахом, амплитуда которых в какой-то момент резко сокращается. До этого в системе шли значительные архитектурные перестройки, изменения в интерфейсах и (или) включения или исключения больших объёмов кода. После этого рубежа происходит доработка сложившейся базовой версии. В непрерывном времени

этот рубеж, разумеется, был бы сильно размыт, но на практике речь идёт об оценке некоторого числа версий, относимых к дискретным моментам. Момент, начиная с которого размах колебаний графика интеллектуального тепла сокращается на порядок, определяется без труда, причём так, что в дальнейшем значения этой метрики чаще всего монотонно выходят на стационар. Смысл данного рубежа в том, что все проектные решения окончательно отработаны и реализованы, но ещё сохраняются последствия не проявивших себя случайных недосмотров, ошибки спецификаций, ошибки интерпретации спецификаций, последствия поздних изменений в требованиях заказчика (напр. [7,С.106-107]).

Второй рубеж соответствует прекращению заметных (т.е., хотя бы порядка нескольких %) флуктуаций потенциальных объёмов модулей и суммы их объёмов разработки. По смыслу это соответствует наступлению ситуации, когда в устранении дефектов данной системы накоплен большой опыт, а сохранившиеся дефекты объективно разделяются в артефактах проекта. В этих условиях шансы на то, что исправление дефекта породит новые ошибки или разблокирует другие скрытые дефекты, минимальны.

Эти рубежи зрелости интересны возможностью индикации признаков своего прохождения в реальном времени разработки проекта на основе статических метрик энергетического анализа программ. Они, по сути, определяют *период ЖЦ* ПС, для которого наиболее *актуален* учёт вторичных дефектов. Действительно, до наступления первого из рубежей моделировать эволюцию «дефектов в системе», «первичных» и «вторичных» дефектов, в том числе, с построением гладких зависимостей, нет смысла, поскольку такие изменения в системе, как например, удаление одних компонент и добавление других, меняют функцию количества дефектов скачкообразно и непредсказуемо. После прохождения второго рубежа новые вторичные дефекты не появляются, а возникшие раньше должны при моделировании динамики дефектов рассматриваться на этом интервале как первичные (чем оправдывается использование классических уравнений вероятностной теории надёжности). С общей точки зрения феноменологической термодинамики ПС, первый рубеж следует считать началом фазового перехода системы от фазы активной разработки к фазе доводки по надёжности, а второй рубеж – как завершение этого фазового перехода. Об аналогии с фазовыми переходами в материальных средах уместно говорить потому, что после второго рубежа термодинамическое и калорическое уравнения состояния модулей этой системы (точнее, модулей её СПС) [10,11], аналогичные уравнениям состояния газов, не могут описывать дальнейшую эволюцию надёжности. Действительно, интеллектуальное тепло при исправлении дефектов поступать в систему должно, и часто немало, но макроскопические параметры модулей при этом практически не изменяются.

Переходя собственно к моделированию процесса роста надёжности ПС за счёт исправления дефектов, мы должны обратиться к «микроскопическому» описанию процессов (*статистическая* термодинамика). К сожалению, на «микроуровне» коды программ и действия с ними при исправлениях настолько разнородны и уникальны, что использовать «закон больших чисел» и вывести уравнения макроднамики из принятых уравнений микродинмики (как в физике) не получится. Придётся идти обходным путём.

Приведём неформальные соображения. В этих рассуждениях под *вероятностной моделью надёжности* (ВМН) будем понимать вероятностную модель надёжности ПС, которая определяет некий закон динамики первично образованных дефектов, а предусматривать вторичные дефекты не обязана.

Всякая такая ВМН основывается на определённых допущениях, аксиомах. Из системы предположений данной ВМН выводится (математически или эмпирически) *способ оценки динамики* (СОД) выявления-ликвидации дефектов на интервале наблюдения, имея в виду в дальнейшем экстраполяцию с целью прогноза. Представим себе *генераторы* (математические описания вычислительных процедур), порождающие объекты, называемые «дефектами», и стохастический *процесс их обнаружения-ликвидации*, промежуточные итоги которого в конце каждого периода заданной длины сообщаются внешним наблюдателям для статистики. Данному СОД (не обязательно построенному по ВМН), сопоставим класс *согласованных с ним генераторов*, обладающих тем свойством, что применяя к статистике их процессов эту СОД можно получить точный в заранее выбранном смысле прогноз такой статистики на будущем (контрольном) интервале времени. В частности, для согласованности генератора с такими СОД, которые позволяют оценивать числа первоначальных дефектов D_0 и вторичных дефектов S_T, обнаруженных к моменту T, будем требовать, достаточной точности оценок чисел D_0 и S_T, наблюдаемых в порождённых генератором процессах. Для СОД классических ВМН очевидно, что классы согласованных генераторов не пусты (предположения ВМН, по сути, описывают процесс генерации). Если непустой класс генераторов факторизовать по отношению «сложнее», то в нём выделится подкласс минимальной сложности. Представителей таких классов будем называть *минимальными генераторами* данного СОД. Для ВМН это те генераторы, которые буквально реализуют их предположения. Примером согласованных генераторов являются ПС и реальные процессы их отладки/испытаний с чётким сценарием, если с выполняются предположения ВМН. Ясно, что такие генераторы не минимальны.

В чём смысл проведенного рассмотрения? Обсуждавшиеся выше СОД, учитывают вторичные дефекты, связанные с обобщением классических ВМН (пункты 2.1, 2.4), как, впрочем, и с иными соображениями (пункты 2.3-2.5). Они используют обобщения систем уравнений ВМН либо предположения о случайных отклонениях процессов от классических гладких трендов. Из нашего рассмотрения вытекает другая возможность: строить, по возможности, более согласованные с реальными процессами генераторы, не заботясь об их формальной согласованности с классическими ВМН.

Определение 1. Некоторую вероятностную модель надёжности назовём *естественной вероятностной моделью надёжности* (ЕВМН) программных систем, если она определяется параметризованным генератором, который допускает математическое описание в терминах случайных величин и воспроизводит «первичные» и «вторичные» дефекты.

Собственный СОД ЕВМН тривиален, поскольку генератор ЕВМН как раз и производит идеализированную статистику ***всех*** дефектов. Если описание такого генератора ЕВМН не может быть содержательно редуцировано, то этот

генератор является минимальным генератором (не обязательно единственным) собственной СОД ЕВМН. Самые простые ЕВМН имеют более сложные минимальные генераторы, чем классические ВМН (и подобные им) в аспекте явного механизма генерации «вторичных» дефектов. Если же генератор ЕВМН таков, что при частных и только частных, значениях своих параметров вырождается в генератор кокой-то ВМН, то он будет сложнее минимального генератора этой ВМН по всем аспектам.

Прикладное использование собственного СОД ЕВМН возможно на основе идентификации параметров генератора этой ЕВМН по известной статистике фактических дефектов ПС.

С учётом этого, плодотворное использование ЕВМН в моделировании процесса роста надёжности ПС с учётом «вторичных дефектов» может быть реализовано благодаря решению задач трёх типов:

- Отыскание эффективных методов идентификации параметров ЕВМН по известной статистике фактических дефектов и проверка точности предсказаний модели на данных, полученных при отладке (испытаниях или эксплуатации) реальных ПС;
- *Относительная верификация* или, как минимум, *оценка точности* СОД ВМН классического типа, с помощью данных, полученных в процессах генерации на основе ЕВМН с характерными параметрами (подразумевается верификация в смысле достаточной точности предсказаний *по отношению* к одной или множеству *ЕВМН*);
- *Верификация* СОД некоторой ВМН относительно ЕВМН, которая сама имеет точный СОД по отношению к какому-то классу *реальных* ПС.

В данной работе, посвященной выработке концепций, мы ограничимся простейшей постановкой вопроса: не приведут ли простейшие ЕВМН (которые, безусловно, представляют первоочередной интерес) к генерации в точности тех процессов, к которым с успехом применимы известные модели со вторичными дефектами, прежде всего, упоминавшиеся в пунктах 2.3, 2.4?

Что касается модели, п. 2.5, то для её разностного аналога легко строится минимальный генератор, близкий к ЕВМН, но нарушено условие определения 1: процесс не описан в терминах «первичных» и «вторичных» дефектов. Вместо этого фигурируют термины «выходящие» и «входящие» дефекты с иной семантикой. Можно ли в модели п. 2.5 оценить число S вторичных дефектов обнаруженных к моменту t? Выше мы условно называли «входящие» в систему вторичными, но в выходной поток наряду с первичными дефектами попадают не «входящие» непосредственно, а «созревшие»! Как оценить их число:

$$\int_0^t A_1(-f_2)d\tau = \frac{F_0 A_1 A_2}{A_1^2 - A_2^2} - \frac{F_0 A_1}{2}\left(\frac{e^{A_2 t}}{A_1 - A_2} - \frac{e^{-A_2 t}}{A_1 + A_2}\right)e^{-A_1 t} \qquad \text{или}$$

$$\int_0^t A_2 f_1 d\tau = \frac{F_0 A_2 A_1}{A_1^2 - A_2^2} - \frac{F_0 A_2}{2}\left(\frac{e^{A_2 t}}{A_1 - A_2} + \frac{e^{-A_2 t}}{A_1 + A_2}\right)e^{-A_1 t} \text{ или } S = \int_0^t A_1(-f_2)d\tau \text{ ? } (5)$$

Эти величины при нетривиальных значениях параметров A_1, A_2 не совпадают, исключая отдельные значения t. Средств, позволяющих отличить первичные

дефекты от вторичных на выходе, модель не предлагает. Не ясно и со вторичными дефектами среди остаточных. Если это f_2, то они неравноправны с первичными в плане обнаружения, да и помимо них при $t > 0$ есть ещё бывшие дефекты входного потока, перешедшие в выходной… Поэтому модель, основанную на (1), имеет смысл рассмотреть в будущем отдельно и тщательно.

4 Пример построения простой ЕВМН

Идея состоит в следующем. Введём m-мерное *пространство возможных дефектов* и выделим в нём некоторый объём, который в простейшем случае может быть кубом $(0;l)\times(0;l)..\times(0;l)$. Назовём его *объёмом системы*. Точки с целыми координатами будут множеством мест потенциальных дефектов. Заполним случайным образом некоторые из этих мест *первичными дефектами* (в простейшем случае число дефектов задано, а их вероятностное распределение равномерно по объёму). Дефект – это точка m–мерного пространства дефектов, причём для каждой координаты возможно l вариантов значений. Каждая координатная ось символизирует отдельный вид дефектов (или ошибок), а целая точка на ней – разновидность внутри вида. Если дефект имеет смешанный (при другой интерпретации – комплексный) характер, он, всё же, тяготеет к одному и только одному из видов, т.е осей, 1 .. m, пространства возможных дефектов. По определению, расстояние от дефекта $D = (D_i)_{i=1}^{m}$ до оси тяготения k должно быть минимальным (при справедливости этого условия для нескольких осей выбор из них оси тяготения случаен):

$$D\ тяготеет\_к\_оси\ k \quad \Rightarrow \quad \sum_{\substack{i=1 \\ i\neq k}}^{m} D_i^2 \xrightarrow[k]{} \min . \qquad (6)$$

Вероятность обнаружения дефекта на каждом шаге по времени равна или (при усложнении модели) является функцией от числа наличных дефектов, делённого на число мест для дефектов (т.е. на выделенный объём пространства возможных дефектов). В реализованном простейшем варианте после обнаружения дефекта он должен быть удалён с уменьшением вероятности отыскания одного из оставшихся дефектов на следующем шаге времени. При этом с некоторой вероятностью может быть сделана ошибка, угрожающая новым дефектом S (пусть одним). В реальных условиях такая ошибка совершается в условиях, отличных от тех, при которых возникали первичные дефекты: возрос опыт разработчиков, усовершенствовались тесты и т.п. Поэтому «вторичная ошибка», ведущая к дефекту S, может быть обнаружена сразу. Это имитируется так. S не учитывается, если при просмотре обнаруженных дефектов D окажется, что

$$\exists D\ \exists k : (D\ тяготеет\_к\_оси\ k) \wedge (S\ тяготеет\_к\_оси\ k) \wedge (\forall i \neq k : S_i = D_i) . \qquad (7)$$

Иначе S включается в число дефектов, а вероятность обнаружения дефекта на следующем шаге увеличивается. Далее цикл поиска-ликвидации продолжается аналогично, причём после появления вторичных дефектов возможна реализация двух вариантов поиска, соответствующих различным сценариям тестирования. При первом (принятом в статье) вероятность обнаружения дефекта не зависит от

того, является ли он первичным или вторичным. При другом - зависит (основанием к такому предположению может быть то, что обычно можно назвать вероятные места локализации вторичных дефектов, если они есть, и очередной шаг тестирования начинается с тщательной проверки их появления). После определённого число шагов по времени выводится статистика, доступная на практике, как и та, которая доступна лишь при имитационном моделировании (действительное число остаточных дефектов, первичных и вторичных).

Этому описанию очевидным образом соответствует математический генератор с параметрами, который включает случайные величины с известными распределениями. Поэтому условия определения 1 выполнены.

В численных экспериментах использовалась компьютерная реализация Reliability_Simulation описанной ЕВМН на языке Ада. Такая реализация всегда является носителем не выбранной ЕВМН, а несколько иной модели того же типа. Например, элементом такого различия является то, что случайные величины замещаются псевдослучайными последовательностями значений по алгоритму, предусмотренному в системе программирования (в данном случае GNAT AdaCore) и настроенному (преобразованному) в процессе разработки программы путем того или иного использования компонент стандартной библиотеки системы программирования. Очевидно, что эти различия не играют в данном случае принципиальной роли.

5 Точность некоторых ВМН относительно простой ЕВМН

Как пояснялось выше, целью проведения численных экспериментов данной работы было выяснить, нет ли признаков того, что ЕВМН, по крайней мере, в простейшем варианте, является методом воспроизводства процессов илиминации ошибок, который покрывается известными моделями. Эта проверка произведена в формате проверки точности некоторых известных ВМН, учитывающих вторичные ошибки. В контексте темы это – как раз точность прогноза динамики вторичных дефектов.

Оценим на примерах правдоподобность гипотезы о том, что на данных имитационного моделирования, напоминающих реальные, тестируемая ВМН предсказывает появление вторичных дефектов в количестве, не более, чем на 25% отличном от действительной величины (однократного процесса имитационного моделировании с помощью генератора Reliability_Simulation).

В [7,8] приведены данные по динамике выявления ошибок ПО учётной ИС «Агрокомплекс»: 43 контрольных точек в концах периодов продолжительностью, в среднем, по 51 дню. Кумулятивные числа обнаруженных и исправленных дефектов составляли соответственно: 72, 133, 156, 176, 226, … 578, 580, 583, 584, 585. Просматривая результаты имитации процесса обнаружения дефектов при разных параметрах, мы обратили внимание на следующий вариант - виртуальный проект 5451. При $m = 4$, $l = 5$ и вероятности вторичной ошибки $p = 0.2$ вводятся 34 контрольные точки периодов, содержащих по 79 шагов процесса (считайте, «дней»). Получен ряд кумулятивных чисел найденных ошибок: 73, 134, 186, 234, 285, … 614, 617, 618, 620, 620. На 43-х периодах (при числе шагов 2686 против 2191 в 34 периодах) обнаруживается лишь немногим больше дефектов, а в целом данные имитационного моделирования вполне напоминают статистику реального

процесса. В табл. 1 помещены полные итоги генерации дефектов для этого варианта, включая «секретную» статистику вторичных и остаточных дефектов.

Таблица 1. Итоги генерации процесса обнаружения дефектов - проект 5451.

№ периода	Всего дефектов	В этом периоде	Всего первичных	Всего вторичных	Остаточных дефектов	Из них вторичных
1	73	73	72	1	538	10
2	134	61	133	1	479	12
3	186	52	185	1	429	14
4	236	50	234	2	382	16
5	285	49	281	4	337	18
6	317	32	312	5	307	19
7	355	38	348	7	270	18
8	379	24	370	9	247	17
9	406	27	395	11	221	16
10	431	25	416	15	196	12
11	452	21	437	15	175	12
12	470	18	454	16	157	11
13	490	20	471	19	138	9
14	502	12	483	19	126	9
15	518	16	498	20	110	8
16	530	12	510	20	98	8
17	540	10	520	20	88	8
18	558	18	536	22	70	6
19	568	10	544	24	60	4
20	576	8	551	25	52	3
21	584	8	558	26	44	2
22	589	5	563	26	39	2
23	591	2	565	26	37	2
24	595	4	568	27	33	1
25	598	3	571	27	30	1
26	603	5	576	27	25	1
27	609	6	581	28	19	0
28	612	3	584	28	15	0
30	614	1	586	28	14	0
31	617	3	589	28	11	0
32	618	1	590	28	10	0
33	620	2	592	28	8	0
34	620	0	592	28	8	0

Для процесса, представленного табл. 1, нами в соответствии с [5,7,1] рассчитывался тренд экспоненциального закона роста надёжности:

$$q(t) = R_0\left(1 - e^{ht}\right), \tag{8}$$

где R_0 – параметр, имеющий смысл общего числа обнаруженных дефектов при неограниченном времени их поиска при условии точного следования процесса своему тренду;

h – параметр, который рекомендуется находить первым, используя, возможно, в качестве приближения для R_0 общее число дефектов, обнаруженных на момент окончания процесса;

t – «время», под которым в данном случае понимается номер периода.

Элементарная приближенная оценка [7; 1, С. 91-92] привела к значению $h = h(1) = -0.1851$, а на основе оптимизационного подхода к аппроксимации мы получили $h = h(2) = -0.1111$. Значения R_0 в соответствии с [7; 1, С. 92] уточнялись локальной подгонкой (для выполнения равенства (1)) с подстановкой туда экспериментальных значений кумулятивных чисел дефектов вместо $q(t)$ для точек t_i ($q(t) = q(t_i) = q_i$) и последующим усреднением. Получились такие оценки: $R_{0(1)} = 552.9$ и $R_{0(2)} = 645.4$. В первом случае получим оценку 424 вторичных ошибок (?), а во втором **39**. Если же действовать по плану [8] и воспользоваться аппроксимацией кумулятивной кривой методом наименьших квадратов (МНК), подбирая «тип тренда» по качеству этой аппроксимации, то аппроксимирующая зависимость будет такой:

$$a(t) = 780.6 \cdot \left(1.0 - t^{0.8711} \cdot e^{-0.03015t}\right) \quad (9)$$

По ней прогноз вторичных ошибок составил **96**.

К данным табл. 1 нами был также применён метод работы [9; 1, С. 132]. Число обнаруженных дефектов хорошо приближается зависимостью

$$D(t) = 771.00 \cdot t^{0.0088} \cdot e^{-0.1185t} \quad (10)$$

(против альтернатив с «чистыми» степенями или экспонентами). Вот предсказанные этим методом числа обнаруженных вторичных дефектов по 34-рём периодам моделирования:

$$3 + 0 + 1 + 0 + 4 + 6 + 2 + 6 + 0 + 1 + 0 + 0 + 1 + 2 + 1 + 0 + 0 +$$

$$+ 8 + 0 + 0 + 1 + 0 + 2 + 0 + 0 + 1 + 3 + 0 + 1 + 6 + 1 + 0 + 1 + 1 = \mathbf{52}. \quad (11)$$

Если подключить упомянутую в пункте 2.5 эвристику, то концовку этого ряда можно было бы считать такой: … + 3 + 0 + 1 + **1** + 1 + 0 + **0** + **0** = **45**. Интересно было расширить статистическую базу, продолжив процесс имитации ещё на 8 периодов (отметим, что к 40-му периоду вообще все моделируемые дефекты, вторичные и первичные, были ликвидированы). Тогда метод предсказывает 49 вторичных дефектов, но после эвристической правки на отрезке последних 5 периодов это число можно сократить только до 43.

По табл. 1 в процессе имитации последний **28** вторичный дефект в «действительности» вылавливается на 26 периоде, и больше они не образуются. Оценки всех рассмотренных методов показали на данном примере завышение числа вторичных дефектов (не менее, чем на 30%).

В литературе по обсуждаемой теме неоднократно использовались данные по динамике выявления ошибок ПО учётной ИС платежей населения за природный газ малого государственного предприятия «Лайф» г Измаила [5,9,1]: 12 контрольных точек, соответствующих 12 месяцам эксплуатации при одинаковом примерно (по 12 тыс.) числе «транзакций» в месяц [5]. Числа обнаруженных и исправленных ошибок составляли: 13, 11, 8, 7, 6, 5, 4, 6, 3, 2, 1, 1 (всего 67 дефектов). Мы подобрали близкий вариант генерации, в котором обнаружвается 65 дефектов. Это виртуальный «проект 1060»: $m = 3$, $l = 6$, вероятность вторичной ошибки $p = 0.225$, 12 контрольных точек (в периодах бралось всего по 53 шага процесса, поскольку периоды, имеющие десятки тыс. шагов при 5-6

обнаруженных дефектах, имитировать не практично). Итоги однкратного имитационного моделирования для этого варианта помещены в табл. 2.

Таблица 2. Итоги генерации процесса обнаружения дефектов - проект 1060.

№ периода	Всего дефектов	В этом периоде	Всего первичных	Всего вторичных	Остаточных дефектов	Из них вторичных
1	17	17	17	0	53	4
2	32	15	30	2	38	2
3	40	8	36	4	31	1
4	43	3	39	4	29	2
5	47	4	43	4	25	2
6	49	2	44	5	23	1
7	53	4	48	5	21	3
8	56	3	50	6	18	2
9	59	3	53	6	15	2
10	62	3	55	7	12	1
11	63	1	56	7	11	1
12	65	2	57	8	9	0

К этому процессу мы применяли те же СОД аналогично предыдущему, и поэтому ограничимся кратким сообщением по итогам. По методам [7,8] подбор трендового закона вида (8) и «МНК» применительно к кумулятивным числам дали оценки: **22** и **19** вторичных дефектов соответственно.

Применение метода [9; 1, С. 132] привело к таким результатам: закон убывания обнаруженных дефектов - степенной с показателем -0,8024, оценка числа вторичных дефектов – **4** (рис. 1), причём, начиная с 7-го периода данный метод их не обнаруживает (в «действительности» они были, табл. 2).

"Время"	Дефекты	Погрешн.аппроксим.			"Мат.ож."	Инд-тор	Втор.ош.
1	18	-1,35E+00	1,35	12	2,286736	-0,93674	0
2	16	4,90E+00	4,9	11	2,096174	2,803826	3
3	9	9,86E-01	0,986	10	1,905613	-0,91961	0
4	4	-2,36E+00	2,36	9	1,715052	0,644948	1
5	5	-3,19E-01	0,319	8	1,52449	-1,20549	0
6	3	-1,60E+00	1,6	7	1,333929	0,266071	0
7	5	9,40E-01	0,94	6	1,143368	-0,20337	0
8	4	3,52E-01	0,352	5	0,952807	-0,60081	0
9	4	6,81E-01	0,681	4	0,762245	-0,08125	0
10	4	9,50E-01	0,95	3	0,571684	0,378316	0
11	2	-8,25E-01	0,825	2	0,381123	0,443877	0
12	3	3,65E-01	0,365	1	0,190561	0,174439	0
Сандарт=	5,247655					Всего :	4

Рис.1.2 Расчёт оценки числа обнаруженных вторичных дефектов для проекта 1060

Согласно табл. 2 среди обнаруженных на 12 периодах моделируемого процесса дефектов присутствовало **8** вторичных. Как видим, оценки всех применённых методов отклоняются от виртуальной «действительностью» не менее, чем на 50%.

Можно сделать такой общий вывод. Гипотеза о том, что простейшие ЕВМН не привносят ничего нового в вероятностное моделирование надёжности программных систем по сравнению с хорошо известными методами оценки числа вторичных дефектов, должна быть отвергнута ввиду контрпримеров. Действительно, хотя генерируемые зависимости числа дефектов от «времени» демонстрируют близость в смысле МНК к традиционным экспоненциальным и степенным зависимостям аналогично реальным процессам, число вторичных дефектов в сгенерированных по ЕВМН примерах, оценивалось рассмотренными известными СОД с точностью, не достигавшей даже 25%.

6 Заключение

В данной работе сформулирована и апробирована концепция нового способа моделирования процессов обнаружения-исправления дефектов программных систем с учётом вторичных дефектов с помощью генераторов. Прежде всего, этот путь может быть использован для верификации существующих моделей и основанных на них методов прогноза. Основанный на имитации процесса обнаружения-исправления, он, в отличие от статистики реальных проектов, позволяет иметь информацию об «истинном» числе вторичных дефектов, равно как и об остаточных дефектах.

Уже эксперименты с простейшим вариантом представителя ЕВМН показали, что по доступной извне системы статистике её дефектов вероятностные модели надёжности, предполагающие объективную значимость трендов, могут не оценить число вторичных дефектов с приемлемой точностью. Однако все СОД классических ВМН, если разобраться, имеют резерв в виде тех или иных параметров (констант, вспомогательных методов и т.п.), которые можно настраивать для оценки процессов тех или иных классов, если доступна статистика *многих* проектов данного класса. Как правило, она недоступна, тогда как имитационное моделирование доступно всегда. При этом даже в простейшей версии хватает собственных параметров настройки для воспроизводства разных по характеру процессов обнаружения и исправления дефектов. В этом состоит практическое значение данной работы.

В дальнейшем требует исследования точность известных моделей, но уже не с точки зрения отдельных примеров их несоответствия, а с точки зрения средней точности с обязательной оценкой разброса. Другое направление дальнейших исследований – совершенствование используемых ЕВМН. В частности, их потенциал состоит в том, что, в отличие от существующих ВМН, они способны отражать влияние на динамику повышения надёжности ПС в терминах уменьшения числа дефектов особенностей архитектуры этих систем. Это направление усовершенствования ВМН с точки зрения появления вторичных дефектов, насколько известно, ещё не исследовалось.

ЛИТЕРАТУРА

1. CASE-оценка критических программных систем. Т. 2. Надежность [Монография] / Одарущенко О . Н. , Харченко В. С. , Маевский Д. А. и др. – Под ред. Харченко В. С. – Х. : Нац. аэрокосм. ун-т и м. Н . Е . Жуковского "ХАИ", 2012. – 292 с.
2. Мищенко В.О. Термодинамический подход к моделированию процесса программирования / В. О. Мищенко // Моделирование и программное обеспечение систем и технологий. Часть 1. Математическое моделирование физических процессов и технических систем. – научно-методический сб. – Харьков, 2014. – С. 209-260.
3. Maevsky D. A. Software reliability. what is it? / Dmitry A. Maevsky, Igor A. Ushakov, Ludmila N. Shapa // RT&A # 04 (31) (Vol.8) 2013, December. – P. 60-65.
4. Одарущенко О. Н. Учет вторичных дефектов в моделях надежности программных средств / О. Н. Одарущенко, А. А. Руденко, В. С. Харченко // Математичні машини і системи, 2010, № 1. – С. 205-217.
5. Антощук С. Г. Прогнозирование количества ошибок на этапе эксплуатации адаптируемых учетных информационных систем / С. Г. Антощук, Д. А.Маевский, С. А.Яремчук // Радіоелектронні і комп'ютерні системи. – 2010. – № 6 (47). – С. 204-210.
6. Маевський Д. А. Влияние вторичных дефектов на надежность динамичных информационных систем / Д. А. Маевский // Вісник НТУ "ХПІ» . – 2012. – №50 (956). – С. 54-58.
7. Маєвський Д. А. Структурна динаміка програмних систем і прогнозування їх надійності при наявності вторинних дефектів / Д. А. Маевский // Радіоелектронні і комп'ютерні системи. – 2010. – № 3 (44). – С. 103-109.
8. Маевский Д. А. Использование теории временных рядов для выделения вторичных ошибок на этапе тестирования программного обеспечения / Д. А. Маевский, О. П. Жеков // Радіоелектронні і комп'ютерні системи. – 2011. – № 2 (16). – С. 82-85.
9. Одарущенко О. Н. Метод оценивания надежности программных средств с учетом вторичных дефектов / О. Н. Одарущенко, А. А. Руденко, В. С. Харченко // Радіоелектронні і комп'ютерні системи. – 2012. – № 7 (59). – С. 294-300.
10. Мищенко В. О. CASE–оценка критических программных систем. Том 1. Оценка качества [Монография] / В. О.Мищенко, О. В.Поморова, Т. А. Говорущенко ; под ред. Харченко В. С. – Х : Нац. аэрокосмический ун–т «Харьк. авиац. ин–т», 2012. – 201 с.
11. Мищенко В. О. Энергетический анализ программного обеспечения с примерами реализации для Ада–программ / В. О. Мищенко Х. : ХНУ имени В.Н. Каразина, 2007. – 129 с.

Надійшла у першій редакції 15.10.2015, в останній - 22.10.2015.