НЕМОНОТОННЫЕ МОДЕЛИ ОЦЕНКИ НАДЕЖНОСТИ И БЕЗОПАСНОСТИ ФУНКЦИОНИРОВАНИЯ ПРОГРАММНЫХ СРЕДСТВ НА РАННИХ ЭТАПАХ ИСПЫТАНИЙ

***Марков Алексей Сергеевич**, кандидат технических наук,*
старший научный сотрудник, CISSP

Рассмотрены вопросы использования моделей роста надежности в рамках испытаний модифицируемых систем. Обоснованы немонотонные модели оценки надежности программ по результатам обновлений и исправлений. Получены оригинальные расчетные выражения параметров немонотонных моделей оценки надежности, оценки точности и планирования испытаний. Отмечено преимущество немонотонных моделей оценки надежности для программ с открытым кодом и для многоверсионного программного обеспечения.

***Ключевые слова**: надежность программ, технологическая безопасность программ, испытания программ, модели отладки, модели роста надежности, модели оценки надежности, немонотонные модели.*

NONMONOTONE MODELS OF RELIABILITY AND SECURITY OF SOFTWARE IN THE EARLY STAGES OF TESTING

***Alexey Markov**, Ph.D., Associate Professor, CISSP*

The use of reliability growth models of the modified systems in the testing phase is examined. The non–monotonic software reliability models on results updates and patches are substantiated. The original expressions of parameters of non–monotonic reliability assessment models, estimates of accuracy and test planning are obtained. The advantages of the non–monotonic reliability growth models for open source software and multi–version software are noted.

***Keywords**: software reliability, software security, software testing, debugging model, reliability growth models, software reliability models, non–monotonic model.*

Введение

На этапах предварительных испытаний и опытной эксплуатации информационных систем важным пунктом является определение момента, когда испытания могут считаться завершёнными[1]. Что касается программных средств (ПС) высокого уровня доверия (например, предназначенных для обработки и защиты гостайны), то современные нормативные документы определяют необходимость формализации результатов испытаний[2]. В таких случаях, к критериям завершения испытаний (которые фиксируются в протоколах испытаний), кроме собственно факта подтверждения выполнения заданных требований, также добавляют значения показателей полноты тестирования и показателей достигнутой степени надежности или корректности с учетом заданной точности оценки.

Для этих целей можно использовать математические модели [1, 3-5, 7-20], которые целесообразно разделить на четыре класса, а именно:

- отладочные модели, позволяющие оценить показатели надежности ПС в зависимости от результатов запусков программ на заданных областях данных и последующих модификаций программ;
- временные модели роста надежности, позволяющие оценить показатели надежности программ в зависимости от времени испытаний с учетом исправлений ошибок программ;
- модели полноты тестирования, позволяющие получить оценки показателей доверия к процессу испытаний;

1 ГОСТ 34.603-92.

2 ГОСТ ИСО/МЭК 15408-3-2013.

- модели сложности программ, основанные на связи метрик сложности ПС с показателями качества, надежности и безопасности программ.

На ранних этапах испытаний, в связи с интенсивной модификацией систем с целью исправления выявляемых ошибок, наиболее адекватными считаются отладочные модели, также называемые моделями роста надежности, основанными на областях входных данных и доработках [17-20]. Известные в литературе модели отражают монотонный рост надёжности функционирования ПС, что не всегда соответствует действительности, например, для случая внедрения программного обеспечения с открытым кодом, многоверсионных или многотиражируемых ПС, когда в процессе их создания в разное время задействованы совершенно различные группы программистов и т.д. Обоснованию немонотонных моделей и получению расчетных выражений их параметров посвящена данная статья.

Надежность программного обеспечения

Под надежностью программ обычно понимают совокупность свойств, характеризующих способность программы сохранять заданный уровень пригодности в заданных условиях в течение заданного интервала времени[3]. Если в качестве ограничения уровня пригодности рассматривать дефекты безопасности и уязвимости, то понятие надежности эквивалентно понятию **технологической безопасности**.

Напомним, что определение надежности ПС имеет принципиальное отличие от надежности аппаратных средств, что проявляется, главным образом, в отсутствии эффекта старения ПС во времени. Можно отметить два свойства надежности ПС:

1. Надежность как свойство может изменяться лишь при модификации ПС (т.е. при изменении объекта испытаний), причем степень надежности может как увеличиваться, так и уменьшаться;

2. Значения показателей надежности ПС действительны при тех классах исходных данных, при которых они рассчитывались.

Как отмечалось, в литературе предлагается ряд отладочных моделей, как-то: модель Нельсона [11] и ее модификации [14], модель Пальчуна [9], модель Lapadula [19] и другие [4, 15, 18, 20], которые отражают ступенчатый монотонный рост надежности, т.е. не учитывают возможность явного снижения степени надежности, например, в результате внесения волновых глобальных ошибок или добавления новых функциональных возможностей. Опыт показал, что применение таких математических моделей приводит либо к получению недостоверных результатов, либо существенно увеличивает длительность процесса оценивания надежности ПС. Поэтому требуется обосновать немонотонную модель надежности ПС, получить расчетные выражения ее параметров, в том числе для оценки ее точности.

Обоснование модели немонотонного роста надежности

Согласно указанному ранее первому свойству надежности ПС, процесс модификации ПС можно условно представить в виде случайного процесса переходов из одного надежностного состояния в другое. Моментами переходов являются модификации объекта испытаний, представляющие собой любые изменения программы с целью исправления обнаруженных ошибок либо развития программы. Определим основной показатель надежности ПС, как степень надежности программы, под которой будем понимать вероятность безошибочного запуска ее на наборе исходных данных из диапазона, определенного спецификациями. С учетом сказанного, имеем следующую модель изменения надежности ПС:

$$P_u = P_0 + \sum_{j=1}^{u} \Delta P_j,$$

где: P_0 - начальная степень надежности, $0 \le P_0 < 1$, u - число проведенных доработок ПС, ΔP_j - приращение степени надежности после j-ой доработки.

Графически процесс изменения надежности ПС представляется ступенчатой функцией роста надежности (рис.1).

Рассматривая ПС как модифицируемую систему, изменение степени надежности ПС после j-ой доработки можно представить следующим линейным оператором [2]:

$$\Delta P_j = A_j\left(1 - P_{j-1}\right) - B_j P_{j-1},$$

где: P_{j-1} - вероятность безошибочной работы ПС после *(j-1)*-ой доработки; $\left(1 - P_{j-1}\right)$ - вероятность обнаружения ошибок ПС после *(j-1)*-ой доработки; A_j - коэффициент «эффективности» доработки, характеризующий уменьшение вероятности ошибки за счет j-ой доработки; B_j - коэффициент «негативности» доработки, характеризующий снижение степени надежности за счет j-ой доработки.

[3] ГОСТ 28806-90.

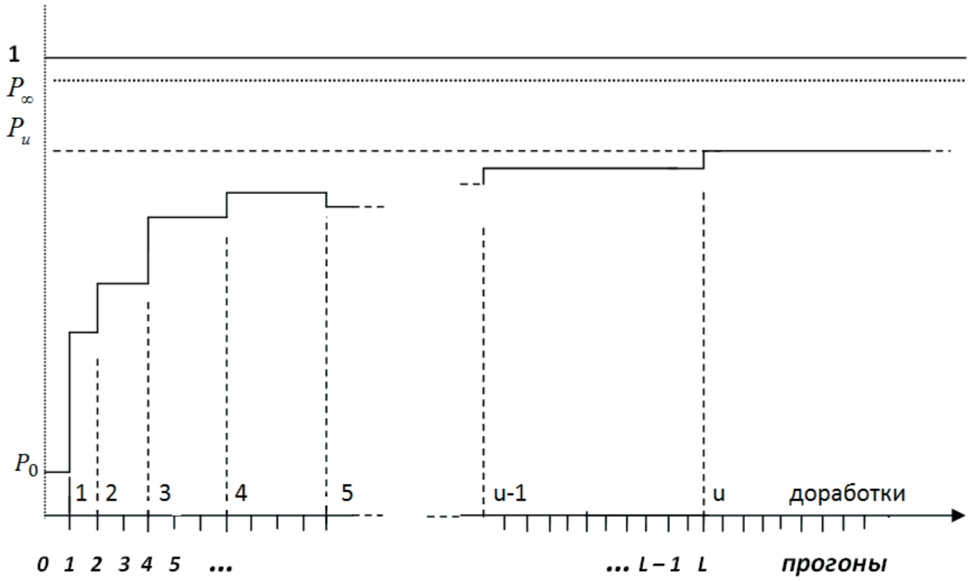

Рис.1. *Изменение степени надежности по результатам доработок*

Перейдя к рекуррентному выражению и считая предельную степень надежности равной $P_\infty = \frac{A_j}{A_j+B_j}$, можно получить модель оценки надежности ПС:

$$P_u = P_\infty - (P_\infty - P_0)\prod_{j=1}^{u}(1 - A_j/P_\infty), \quad (1)$$

где: P_0 - начальная степень надежности, P_∞ - предельная степень надежности, $0 \le P_0 < P_\infty \le 1$, u - число проведенных доработок.

Полученное выражение (1) учитывает возможность неравномерного роста степени надежности объекта испытаний и общую тенденцию к снижению роста ΔP_j при повышении степени надежности P_j [2]. Однако в таком представлении модель имеет в целом монотонный вид, так как не учитывается различное влияние принципиально разного рода модификаций, например, изменения ПС с целью исправления ошибок и изменения, связанные с добавлением новых функциональных элементов. Также модель не отражает уровень сложности доработки, а значит возможность внесения волновых ошибок. Иначе говоря, в таком виде модель сводится к классу монотонных моделей роста надежности.

Для исключения данного недостатка предлагается бигеминальная модель оценки надежности, в основе которой лежит использование метрик сложности модификации кода k_{ij}, например, при исправлении ошибок и при обновлении ПС. На указанную метрику не накладывают ограничения (т.е. метрика сложности может быть любая, наиболее адекватная программной системе и системе программирования[4]), что обеспечивает полноту описания рассматриваемого процесса [7]. Таким образом, полагая $A_j = \sum_{i=0}^{2} a_i k_{ij}$, можно получить основное расчетное выражение бигеминальной модели оценки надежности:

$$P_u = P_\infty - (P_\infty - P_0)\prod_{j=1}^{u}\left(1 - \sum_{i=1}^{2} a_i k_{ij}/P_\infty\right), \quad (2)$$

где: u - число проведенных доработок, a_1 - коэффициент эффективности доработки ПС с целью исправления ошибки, a_2 - коэффициент эффективности доработки ПС с целью добавления функциональных возможностей, k_{ij} - объем j-ой модификации с целью исправления или обновления.

Бигеминальная модель (2) зависит от 4-х параметров $(P_0, P_\infty, a_1, a_2)$, расчет которых не представляет труда, например, с помощью метода максимального правдоподобия [8].

Введя классификацию различного рода доработок, в том числе исправляемых ошибок, можно получить обобщенную немонотонную модель оценки надежности:

$$P_u = P_\infty - (P_\infty - P_0)\prod_{j=1}^{u}\left(1 - \sum_{i=1}^{e} a_i k_{ij}/P_\infty\right), \quad (3)$$

где: e - число классов модификаций ПС.

Данная модель зависит от $(e+2)$ параметров. Приведем пример расчета параметров модели.

Пример расчета параметров модели

Для расчета параметров обобщенной модели (3) можно воспользоваться методом максимального правдоподобия. В качестве исходной статистики можно использовать данные, фиксируемые при испытаниях ПС, а именно: множество испытаний $\{n_j\}$, множество неудачных испытаний (отказов) $\{\widehat{m}_j\}$ между доработками, а также множество метрик сложности доработок $\{k_{ij}\}$. Тогда при до-

4 IEEE Std. 1061-1998.

пущениях о независимости запусков ПС функция максимального правдоподобия представляет собой вероятность получения общей выборки $(n_i, \widehat{m}_j, j=\overline{1,u})$ числа отказов в проведенных сериях запусков ПС:

$$L_u = \prod_{j=1}^{u} C_{m_j}^{n_j} P_j^{n_i-\widehat{m}_j}(1-P_j)^{\widehat{m}_j},$$

где: $C_{m_j}^{n_j} = \frac{n_j!}{\widehat{m}_j!(n_j-\widehat{m}_j)}$, u - номер последней доработки ПС; P_j - вероятность успешного исхода каждого из n_j запусков j-ой серии; $\widehat{m}_j$ - число отказов в n_j запусках.

Для удобства можно прологарифмировать и преобразовать функцию L_u к следующему виду:

$$\ln(L_u) = \sum_{J=1}^{u}\Big(\widehat{m}_j \ln\Big(1-P_\infty+(P_\infty-P_0)\prod_{l=1}^{j}\Big(1-\sum_{i=1}^{e}\frac{a_i k_{ij}}{P_\infty}\Big)\Big) + (n_j-\widehat{m}_j)\ln\Big(P_\infty+(P_\infty-P_0)\prod_{l=1}^{j}(1-\sum_{i=1}^{e}\frac{a_i k_{ij}}{P_\infty})\Big)\Big).$$

Полученная приведенная функция является выпуклой и задана на выпуклом множестве. Поэтому, для нахождения максимума функции правдоподобия можно, например, использовать модифицированный метод наискорейшего спуска с переменным параметром шага h^r:

$$\begin{cases} P_0^{r+1} = P_0^r + h^r\left(\dfrac{\partial \ln L(P_0^r, P_\infty^r, a_1^r, \dots, a_e^r)}{\partial P_0}\right); \\ P_\infty^{r+1} = P_\infty^r + h^r\left(\dfrac{\partial \ln L(P_0^{r+1}, P_\infty^r, a_1^r, \dots, a_e^r)}{\partial P_\infty}\right); \\ a_1^{r+1} = a_1^r + h^r\left(\dfrac{\partial \ln L(P_0^{r+1}, P_\infty^{r+1}, a_1^r, \dots, a_e^r)}{\partial a_1}\right); \\ \dots \\ a_e^{r+1} = a_e^r + h^r\left(\dfrac{\partial \ln L(P_0^{r+1}, P_\infty^{r+1}, a_1^{r+1}, \dots, a_e^r)}{\partial a_e}\right), \end{cases}$$

где r - номер итерации.

Нетрудно показать, что расчетные выражения частных производных приведенной функции максимального правдоподобия имеют следующий вид:

$$\begin{cases} \dfrac{dlnL_j}{dP_0} = \sum_{l=0}^{j} w_l\, a_l; \\ \dfrac{dlnL_j}{dP_\infty} = \sum_{l=0}^{j}\left(w_l\left(\left(\dfrac{P_0-P_\infty}{P_\infty}\alpha_l\beta_l-\alpha_l\right)+1\right)\right) \\ \dfrac{dlnL_j}{da_i} = \sum_{l=0}^{j}\left(w_j\left(\dfrac{P_0-P_\infty}{P_\infty}\alpha_l\,\gamma_{li}\right)\right), \end{cases}$$

где $w_j = \frac{n_j-m_j}{P_j} - \frac{m_j}{1-P_j}$; $\alpha_j = \prod_{l=1}^{j}\left(1-\frac{\sum_{i=1}^{e} a_i k_{li}}{P_\infty}\right)$ $\beta_j = \sum_{l=1}^{j}\frac{\sum_{i=1}^{e} a_i k_{li}}{1-\sum_{i=1}^{e} a_i k_{li}/P_\infty}, \gamma_{ji} = \sum_{l=1}^{j}\frac{-k_{li}}{1-\sum_{i=1}^{e} a_i k_{li}/P_\infty}$.

Для определения оценок P_0 , P_∞, a_1, ..., a_e, как показала практика, достаточна следующая точность:

$$\begin{cases} P_0^{r+1} - P_0^r \le 0.001; \\ P_\infty^{r+1} - P_\infty^r \le 0.001; \\ a_i^{r+1} - a_i^r \le 0.0001. \end{cases}$$

Повышенная точность определения параметров a_i $(i=\overline{1,e})$ связана с их сильным влиянием на функцию P_j оценки надежности.

Нулевые приближения можно найти методом статистического моделирования на логически рассчитанных интервалах:

$$\begin{cases} 0 \le P_0 \le 1-\left(\dfrac{M_0}{N_0}\right); \\ 1-\left(\dfrac{M_\infty}{N_\infty}\right) \le P_\infty \le 1; \\ \dfrac{1}{K_i e}\left(1-\sqrt{\dfrac{M_\infty N_0}{N_\infty M_0}}\right) \le a_i \le \dfrac{1}{K_i^{max} e}, \end{cases}$$

где: M_0 - число отказов в первых N_0 запусках; M_∞ - число отказов в последних N_∞ запусках; K_i^{max} - максимальное значение k_{ij} при $\overline{j=1,u}$); $K_i = \sum_{i=1}^{e} k_{ji}$.

Таким образом, полагая, что $\widehat{P_0}$, $\widehat{P_\infty}$, $\widehat{a_1}$, ..., $\widehat{a_e}$, случайные величины, равномерно распределенные на указанных ранее интервалах, необходимо проделать определенное число проб и выбрать совокупность параметров, соответствующих максимальной функции правдоподобия. Эта совокупность принимается за искомые начальные значения.

Опыт показал, что на начальных этапах испытаний может возникнуть ситуация, когда не выполняется общая тенденция роста степени надежности ПС при доработках. Это может привести к неточности результатов, получаемых с помощью метода максимального правдоподобия (для расчета максимума функции потребуется бесконечное число итераций).

Для исключения данного недостатка целесообразно использовать метод минимизации относительной энтропии [7]:

$$I_u = \sum_{j=1}^{u}\Big(\frac{m_j}{n_j}\ln\frac{m_j}{n_j P_j} + \frac{n_j-m_j}{n_j}\ln\frac{n_j-m_j}{n_j(1-P_j)}\Big),$$

где: m_j - число неудачных запусков из общего числа n_j запусков j-серии; u - число проведенных доработок ПС.

Для проверки необходимого и достаточного условия допустимости метода максимального правдоподобия можно воспользоваться следующим соотношением:

$$\frac{\sum_{j=1}^{u}(j-1)(n_j-m_j)}{\sum_{j=1}^{u}(j-1)} > \frac{\sum_{j=1}^{u}(n_j-m_j)}{u}.$$

Оценка точности модели оценки надежности

Следует сказать, что подавляющее большинство моделей роста надежности представляются авторами без аналитической оценки их точности, что затрудняет их выбор. Данная работа исключает этот недостаток.

Точность оценивания степени надежности ПС можно характеризовать средним квадратическим отклонением. Для получения модели оценки точности удобно воспользоваться методом линеаризации [6]. Тогда среднее квадратическое отклонение находится по следующей формуле:

$$\sigma_j = ((\partial P_j/\partial P_0)^2 \delta_{P_0}^2 + \dots + (\partial P_j/\partial a_e)^2\ \delta_{a_e}^2 + $$
$$+ 2\left(\frac{\partial P_j}{\partial P_0}\right)\left(\frac{\partial P_j}{\partial P_\infty}\right)\delta_{P_0}\ \delta_{P_\infty}\ \rho_{P_0 P_\infty} + \dots + 2\left(\frac{\partial P_j}{\partial a_{e-1}}\right)\left(\frac{\partial P_j}{\partial a_e}\right)$$
$$\delta_{a_{e-1}}\ \delta_{a_e}\ \rho_{a_{e-1}a_e}\ )^{\frac{1}{2}},$$

где: ρ_{xy} - коэффициент корреляции параметров x и y.

Для получения значений частных производных функции роста надежности легко найти следующие расчетные выражения:

$$\begin{cases} \dfrac{dP_j}{dP_0} = \alpha_j; \\ \dfrac{dP_v}{dP_\infty} = \left(\dfrac{P_0 - P_\infty}{P_\infty^2}\alpha_j\beta_j - \alpha_j + 1\right); \\ \dfrac{dP_j}{da_i} = \dfrac{P_0 - P_\infty}{P_\infty}\alpha_j\gamma_{ji}, \end{cases}$$

где: $\alpha_j = \prod_{l=1}^{j}\left(1 - \frac{\sum_{i=1}^{e} a_i k_{li}}{P_\infty}\right)$, $\beta_j = \sum_{l=1}^{j}\frac{\sum_{i=1}^{e} a_i k_{li}}{1-\sum_{i=1}^{e} a_i k_{li}/P_\infty}$,

$$\gamma_{ji} = \sum_{l=1}^{j}\frac{-k_{li}}{1-\sum_{i=1}^{e} a_i k_{li}/P_\infty}.$$

Остальные параметры формулы можно получить из ковариационной матрицы, содержащей дисперсии и корреляционные моменты искомых оценок:

$$\mathcal{K} = \begin{bmatrix} \delta_{P_0}^2 & \delta_{P_0}\delta_{P_\infty}\rho_{P_0P_\infty} & \dots & \delta_{P_0}\ \delta_{a_e}\ \rho_{P_0 a_e} \\ \delta_{P_0}\ \delta_{P_\infty}\ \rho_{P_0P_\infty} & \delta_{P_\infty}^2 & \dots & \delta_{P_\infty}\ \delta_{a_e}\ \rho_{P_\infty a_e} \\ \dots & \dots & \dots & \dots \\ \delta_{P_0}\delta_{a_e}\ \rho_{P_0 a_e} & \delta_{P_\infty}\delta_{a_e}\ \rho_{P_\infty a_e} & \dots & \delta_{a_e}^2 \end{bmatrix}$$

Для ее построения можно воспользоваться следующим соотношением:

$$\mathcal{K} = -\mathcal{M}^{-1},$$

где: A - матрица вторых частных производных функции правдоподобия:

$$\mathcal{M} = \begin{bmatrix} \dfrac{\partial^2\ \ln L_u}{\partial\ P_0^2} & \dfrac{\partial^2\ \ln L_u}{\partial\ P_0 P_\infty} & \dots & \dfrac{\partial^2\ \ln L_u}{\partial\ P_0 a_e} \\ \dots & \dots & \dots & \dots \\ \dfrac{\partial^2\ \ln L_u}{\partial\ P_0 a_e} & \dfrac{\partial^2\ \ln L_u}{\partial P_\infty a_e} & \dots & \dfrac{\partial^2\ \ln L_u}{\partial\ a_e^2} \end{bmatrix}.$$

Для расчета вторых частных производных легко получить следующие расчетные выражения:

$$\begin{cases} \dfrac{dlnL_u}{dP_0} = \sum_{j=0}^{u} w_j\, a_j; \\ \dfrac{dlnL_u}{dP_\infty} = \sum_{j=1}^{u}\left(w_j\left(\left(\dfrac{P_0 - P_\infty}{P_\infty}\alpha_j\beta_j - \alpha_j\right) + 1\right)\right); \\ \dfrac{dlnL_u}{da_i} = \sum_{j=0}^{u}\left(w_j\left(\dfrac{P_0 - P_\infty}{P_\infty}\alpha_j\,\gamma_{ji}\right)\right), \end{cases}$$

где: $w_j = \frac{n_j - m_j}{P_j} - \frac{m_j}{1-P_j}$.

Планирование испытаний

В процессе управления надежностью ПС следует решать задачи планирования затрат на тестирование и испытания для достижения требуемого уровня надежности ПС. В таком случае полезно оценить тенденции по процессу развития и внедрения программного продукта, получить прогноз числа оставшихся ошибок и сложности их исправления.

Для расчета ряда показателей планирования можно воспользоваться моделями (1-3). К сожалению, статистические модели оценки надежности не позволяют спрогнозировать частоту исправлений конкретного типа, а лишь используют эту информацию. Проведение доработок конкретного типа зависит от условий эксплуатации, достигнутой степени надежности, требований по надежности к ПС, квалификации и опыта разработчиков и, следовательно, их содержание может меняться. Для учета типов доработок целесообразно воспользоваться теорией многофакторного анализа. Поскольку изменение числа исправлений конкретного типа рассматривается в масштабе проведений доработок, то для аппроксимации функции сложности модификации ПС можно использовать, например, многочлен второй степени от одной переменной:

$$k_j = \kappa_0 + \kappa_1 j + \kappa_2 j^2,$$

где: $\kappa_0, \kappa_1, \kappa_2$ - параметры многочлена; $j = \overline{1,u}$.

Легко показать, что параметры многочлена имеют следующий вид:

$$\begin{cases} \kappa_0 = \dfrac{30(\sum_{j=1}^{u}\widehat{k_J} - \dfrac{2}{u(u-1)}\sum_{j=1}^{u}\widehat{k_J}j^2 - \beta_2(2+3u-3u^2-2u^3)}{10(u-1)}; \\ \kappa_1 = \dfrac{6(\sum_{j=1}^{u}\widehat{k_J} - \dfrac{2}{u+1}\sum_{j=1}^{u}\widehat{k_J}j - \beta_2(1-u^2)u}{u(1-u)}; \\ \kappa_2 = \dfrac{\sum_{j=1}^{u}\widehat{k_J}\dfrac{u^2+3u-2}{2} - u\sum_{j=1}^{u}\widehat{k_J}j - \dfrac{2}{u-1}\sum_{j=1}^{u}\widehat{k_J}j^2}{u-(4-u^2)}. \end{cases}$$

Тогда, считая, что по имеющимся данным об испытаниях получены оценки параметров модели и достигнутой степени надежности ПС P_u, имеем следующее расчетное выражение модели прогноза степени надежности:

$$P_{\text{тр}}=P_\infty\text{-}(P_\infty\text{-}P_u)\prod_{i=u+1}^{u+j}(1-\sum_{i=1}^{e}a_i k_{ij}/P_\infty), \qquad (4)$$

где: $P_{\text{тр}}$ - требуемая степень надежности ПС; u - номер последней проведенной доработки; j - число планируемых доработок.

Расчет необходимого числа доработок для достижения требуемой степени надежности можно выполнить путем циклического пересчета выражения (4). Для этого рассчитывается значение P_u по формуле (4) и далее в цикле, увеличивая j, определяем значение P_{u+j}. При выполнении условия $P_{u+j} \geq P_{\text{тр}}$ осуществляется выход из цикла.

Для простоты использования прогнозирующей модели положим $A_j=a$, что соответствует переходу от модели (3) к (1). Тогда, упростив выражение (4) и прологарифмировав его, получим следующее выражение для оценки числа J необходимых доработок ПС для достижения требуемой степени надежности $P_{тр}$:

$$J = \left\| \left(\frac{\ln(\frac{P_\infty - P_{\text{тр}}}{P_\infty - P_u})}{\ln(1-a/P_\infty)} \right) \right\|,$$

где: $\|\aleph\|$ - операция получения ближайшего наибольшего целого $\aleph$, a – усредненный коэффициент эффективности доработки ПС.

Считая, что при доработках не вносятся дополнительные ошибки (т.е. P_∞ =1), можно получить формулу числа оставшихся ошибок после u-ой доработки:

$$N_u = \left\| \left(\frac{\ln(\frac{1-P_{\text{тр}}}{1-P_u})}{\ln(1-a)} \right) \right\|.$$

Апробация немонотонной модели оценки надежности

В результате исследований установлено, что предложенные немонотонные модели (2) и (3) обладают высокой точностью (σ_j<0.001) при числе доработок более 10 и числе запусков более 50. Для контроля согласованности модели с исходными данными использовался критерий Мизеса (при пороговом значении 0.01) [6].

Исследование влияния коэффициента эффективности доработок ПС на точность результатов модели (3) показало, что при учете категорирования доработок точность может повышаться на порядок.

Сравнительный анализ предложенных моделей с известными отладочными моделями показали ряд их преимуществ, а именно:

- учет возможного резкого снижения степени надежности при обновлениях;
- возможность учета сложности доработок;
- отсутствие ограничений на организацию испытаний и сбора информации;
- возможность учета показателей надежности ПС, полученных на предыдущих этапах разработки и внедрения;
- отсутствие субъективных параметров, как-то: квалификация программиста и уровень технологии программирования;
- простота использования - нет необходимости рассчитывать вероятности реализации всех путей программы, как, например, в модели Нельсона и её модификациях [11, 14].

Выводы

В работе, фактически, обоснован метод планирования испытаний, основанный на использовании обобщенной немонотонной модели оценки надежности ПС по результатам запусков и модификаций. В рамках предложенного метода получены расчетные выражения параметров модели оценки надежности ПС, а также оценки точности и планирования испытаний. Предложенная обобщённая немонотонная модель (3) позволяет учесть возможные моменты снижения степени надежности ПС, что свойственно, например, разработке программ с открытым кодом, многоверсионных программ и др. Точность обобщенной модели зависит от решения задачи классификации доработок ПС. Модель может быть интегрирована с показателями надежности функционирования ПС, полученными на ранних стадиях разработки программ. Упрощение модели позволяет свести ее к экспоненциальным NHPP-моделям роста надежности, используемым на этапах эксплуатации и совершенствования информационных систем [8].

Основным достоинством предложенных немонотонных моделей является возможность повышения точности (за счет категорирования модификаций) более чем на 10%, что равноценно снижению на 5-15% необходимого числа запусков ПС в процессе испытаний.

Следует отметить, что к недостаткам отладочных моделей относят их низкую точность при малой статистике, что, однако, можно избежать путем применения соответствующих приемов повышения точности, в том числе метода Вальда [10].

Предложенный метод и модели могут быть рекомендованы также для оценки показателей разного рода модифицируемых и обучающихся систем.

Литература

1. Александрович А.Е., Бородакий Ю.В., Чуканов В.О. Проектирование высоконадёжных информационно-вычислительных систем. М.: Радио и связь, 2004. 144 с.
2. Волков Л.И. Управление эксплуатацией летательных комплексов. М.: Высшая школа, 1981. 226 с.
3. Гуров Д.В., Гуров В.В., Иванов М.А. Использование моделей надежности программного обеспечения для оценки защищенности программного комплекса // Безопасность информационных технологий. 2012. № 1. С. 88-91.
4. Карповский Е.Я., Чижов С.А. Надежность программной продукции. Киев: Тэхника, 1990. 160 с.
5. Королев В.Ю. Некоторые критерии проверки надежности программного обеспечения // Системы и средства информатики. 2013. Т. 23. № 1. С. 132-142.
6. Ллойд Д., Липов М. Надежность. М.: Сов.радио, 1964. 668 с.
7. Марков А.С. Модели оценки и планирования испытаний программных средств по требованиям безопасности информации. Вестник МГТУ им. Н.Э.Баумана. Сер. «Приборостроение». 2011. Спецвыпуск. С.90-103.
8. Методы оценки несоответствия средств защиты информации / А.С.Марков, В.Л.Цирлов, А.В.Барабанов; под ред. А.С.Маркова. - М.: Радио и связь, 2012. 192 с.
9. Пальчун Б.П., Юсупов Р.М. Оценка надежности программного обеспечения. СПб.: Наука, 1994. 84 с.
10. Смагин В.А. Основы теории надежности программного обеспечения. - СПб.: ВКА им. А.Ф.Можайского, 2009. 336 с.
11. Тейер Т., Липов М., Нельсон Э. Надежность программного обеспечения: Анализ крупномасштабных разработок: Пер. с англ. М.: Мир, 1981. 323 с.

Reference

1. Aleksandrovich A.E., Borodakiy Yu.V., Chukanov V.O. Proyektirovaniye vysokonadezhnykh informatsionno-vychislitelnykh system. Moscow, Radio i svyaz, 2004. 144 p.
2. Volkov L.I. Upravleniye ekspluatatsiyey letatelnykh kompleksov, Moscow, Vysshaya shkola, 1981, 226 p.
3. Gurov D.V., Gurov V.V., Ivanov M.A. Ispolzovaniye modeley nadezhnosti programmnogo obespecheniya dlya otsenki zashchishchennosti programmnogo kompleksa, Bezopasnost informatsionnykh tekhnologiy, 2012, No 1, pp. 88-91.
4. Karpovskiy Ye.Ya., Chizhov S.A. Nadezhnost programmnoy produktsii, Kiyev: Tekhnika, 1990, 160 p.
5. Korolev V.Yu. Nekotoryye kriterii proverki nadezhnosti programmnogo obespecheniya, Sistemy i sredstva informatiki, 2013, Vol. 23, No 1, pp. 132-142.
6. Lloyd D., Lipow M. Nadezhnost. M.: Sov.radio, 1964. 668 p.
7. Markov A.S. Modeli otsenki i planirovaniya ispytaniy programmnykh sredstv po trebovaniyam bezopasnosti informatsii. Vestnik MGTU im. N.E.Baumana. Ser. «Priborostroyeniye», 2011, Spetsvypusk, pp.90-103.
8. Markov A.S., Tsirlov V.L., Barabanov A.V., Metody otsenki nesootvetstviya sredstv zashchity informatsii, by ed. A.S.Markov, Moscow, Radio i svyaz, 2012, 192 p.
9. Palchun B.P., Yusupov P.M. Otsenka nadezhnosti programmnogo obespecheniya. Saint Petersburg, Nauka, 1994, 84 p.
10. Smagin V.A. Osnovy teorii nadezhnosti programmnogo obespecheniya, Saint Petersburg, VKA im. A.F.Mozhayskogo, 2009, 336 p.
11. Teyer T., Lipow M., Nelson E. Nadezhnost programmnogo obespecheniya: Analiz krupnomasshtabnykh razrabotok, Moscow, Mir, 1981, 323 p.

12. Титов А.В., Харьковой А.А., Чуканов В.О. Модели надежности программного обеспечения ответственного назначения // Научно-технические ведомости Санкт-Петербургского государственного политехнического университета. Информатика. Телекоммуникации. Управление, 2011. Т. 2. № 120. С. 123-126.
13. Царевский А.В. Обеспечение надежности аппаратно-программных комплексов обмена информацией // Автоматизация процессов управления. 2011. №2. С. 56-65.
14. Черкесов Г. Н. Надежность аппаратно-программных комплексов. СПб.: «Питер», 2005. 479 с.
15. Штрик А.А., Осовецкий Л.Г., Мессих И.Г. Структурное проектирование надежных программ встроенных ЭВМ. Л.: Машиностроение, 1989. 296 с.
16. Шубинский И.Б., Замышляев А.М., Прошин Г.Б. Функциональная надежность программного обеспечения информационных систем // Надежность. 2011. Т. 38. № 3. С. 72-81.
17. Musa J.D. More Reliable Software Faster and Cheaper. 2nd Edition. TATA McGraw-Hill, 2004. 632 p.
18. Pham H. System Software Reliability. Springer Series in Reliability Engineering. Springer, 2006. 440 p.
19. Shanmugam L., Florence L. An Overview of Software Reliability Models // International Journal of Advanced Research in Computer Science and Software Engineering. 2012. Vol. 2. № 10. P. 36-42.
20. Xie M., Dai Y.-S., Poh K.-L. Computing Systems Reliability. Models and Analysis. Kluwer, 2004. 293 p.

12. Titov A.V., Kharkovoy A.A., Chukanov V.O. Modeli nadezhnosti programmnogo obespecheniya otvetstvennogo naznacheniya, Nauchno-tekhnicheskiye vedomosti Sankt-Peterburgskogo gosudarstvennogo politekhnicheskogo universiteta. Informatika. Telekommunikatsii. Upravleniye, 2011, Vol. 2, No 120, pp. 123-126.
13. Tsarevskiy A.V. Obespecheniye nadezhnosti apparatno-programmnykh kompleksov obmena informatsiyey, Avtomatizatsiya protsessov upravleniya, 2011, No 2, pp. 56-65.
14. Cherkesov G. N. Nadezhnost apparatno-programmnykh kompleksov. Saint Petersburg, Piter, 2005, 479 p.
15. Shtrik A.A., Osovetskiy L.G., Messikh I.G. Strukturnoye proyektirovaniye nadezhnykh programm vstroyennykh EVM. Leningrad, Mashinostroyeniye, 1989, 296 p.
16. Shubinskiy I.B., Zamyshlyayev A.M., Proshin G.B. Funktsionalnaya nadezhnost programmnogo obespecheniya informatsionnykh sistem, Nadezhnost, 2011, Vol. 38, No 3, pp. 72-81.
17. Musa J.D. More Reliable Software Faster and Cheaper. 2nd Edition. TATA McGraw-Hill, 2004. 632 p.
18. Pham H. System Software Reliability. Springer Series in Reliability Engineering. Springer, 2006. 440 p.
19. Shanmugam L., Florence L. An Overview of Software Reliability Models, International Journal of Advanced Research in Computer Science and Software Engineering, 2012, Vol. 2, No 10, pp. 36-42.
20. Xie M., Dai Y.-S., Poh K.-L. Computing Systems Reliability. Models and Analysis. Kluwer, 2004, 293 p.