дерева подій (ETA - Event Tree analysis), аналіз дерева відмов (FTA - Fault Tree analysis) та аналіз режимів і наслідків відмов (FMEA - failure modes and effects analysis) [3]. Загальні таксономії ризиків, запропоновані SEI, корисні для ідентифікації загальних джерел ризиків проекту, але вимагають пристосування до конкретних умов.

II. Мета роботи

Метою роботи є розробка методу оцінювання ризиків відмов ПЗ, що базується на диференційованому підході до розподілу часу тестування між модулями ПЗ за умов обмежених ресурсів на тестування.

III. Особливості методу оцінювання ризиків відмов програмних модулів

Будемо розглядати ризик виникнення загрози як величину збитків обумовлених здійсненням загрози, тобто потенційно можливої події при роботі ПЗ, яка може призвести до нанесення збитків користувачам [4]. Тоді, за умови, що процес виникнення відмови описується неоднорідним процесом Пуассона та при експоненційній моделі надійності, функція зниження ризику відмови модуля матиме вигляд:

$$\Delta R(t_0|t_e) = C_м(\mu(t_0) - \mu(t_0 + t_e) + \mu(t_e)),$$

де $C_м = \sum_{i=1}^{n}\left[P(S_i)\sum_{j=1}^{r}P(H_j|S_i)\cdot C_j\right]$ - внесок даного модуля в загальний ризик ПЗ; $\Delta R(t_0|t_e)$ – функція зниження ризику відмови модуля за час його виконання t_0 в процесі експлуатації ПС, за умови, що модуль тестувався час t_e; $H = \{H_i,\ i=1,2,\ldots,r\}$ – множина всіх потенційних загроз ПЗ, обумовлених відмовами через дефекти в її програмних модулях; $S = \{S_i,\ i=1,2,\ldots,n\}$- множина всіх можливих сценаріїв функціонування ПЗ; $C_м$ – внесок модуля у ризик відмов ПЗ (вартість можливих збитків через відмови модуля за час його виконання t_0 при експлуатації ПЗ); $R(t_0) = C_м\mu(t_0)$ - величина ризику відмови модуля за час t_0; $\mu(t)$ – функція зростання надійності; $P(S_i)$ – ймовірність того, що при реалізації сценарію S_i $(i=1,2,\ldots,n)$ буде виконуватися даний модуль; $P(H_j|S_i)$ – умовна ймовірність того, що при реалізації сценарію S_i причиною виникнення загрози H_j буде відмова саме даного модуля; C_j - вартість наслідків реалізації загрози H_j $(j=1,2,\ldots,r)$.

Висновок

В умовах обмежених ресурсів на тестування ПЗ критерій завершення повинен встановлюватися, виходячи з оцінок ризику відмови ПЗ. Наведений метод дозволяє на основі функції зниження ризику відмови модулів ПЗ будувати оптимальні процеси тестування ПЗ.

Список використаних джерел

1. Управление риском проектов программного обеспечения / Андон Ф.И. Суслов В.Ю. Коротун Т.М., Коваль Г.И. Слабоспицкая О.А. // Проблемы программирования. – 1999. - № 1. – С. 53-62.
2. Higuera R., Haimes Y. Software Risk Management // CMU/SEI-96-TR-012, Pittsburg, Pa.: Software Engineering Institute, Carnegie Mellon University. – 1996. – 49 p.
3. Leveson N. Safeware: system safety and computers. Addison-Wesley Publishing Company, 1995. - 680 p.
4. Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу. НД ТЗІ 1.1-003-99. – 1999. 51 с.

УДК 681.3.06

МАТЕМАТИЧНА МОДЕЛЬ ОПТИМІЗАЦІЇ ЧАСУ ТЕСТУВАННЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Логін Т.І.

Тернопільський національний економічний університет, магістрант

I. Постановка задачі

В інженерії програмного забезпечення (ПЗ) питання якості набуває дедалі вагомішого значення. На сьогодні розроблено значну кількість різноманітних альтернативних програмних засобів для різних системних та прикладних задач. Тому як користувачі, так і розробники ПЗ, віддаючи перевагу тому чи іншому ПЗ в таких конкурентних умовах, все більшу вагу надають їх якості.

Однією з важливих характеристик якості ПЗ, зокрема транзакційного типу, є його надійність [1]. Математично надійність часто розраховують як характеристики відмов на етапах тестування та в процесі експлуатації ПЗ.

Під загрозою відмови ПЗ зазвичай розуміють потенційно можливу подію при роботі ПЗ, яка може призвести до нанесення збитків користувачам (фінансових втрат або втрат часу), а під ризиком виникнення загрози – величину збитків обумовлених здійсненням загрози [2]. Загрози можуть виникати з різних причин (апаратні збої, помилки користувачів, дефекти у ПЗ, тощо). У роботі розглядаються лише ті з них, які спричинені відмовами ПЗ через недосконале тестування, пов'язане з існуванням певного «компромісу» між обмеженими термінами і потенційно необмеженою кількістю тестів [3]. Звідси виникають важливі проблеми тестування – ухвалення рішення про адекватність тестування, і керування – оцінка витрат (вартості, часу, персоналу) на тестування.

II. Мета роботи

Метою роботи є створення математичної моделі оптимізації часу тестування програмного забезпечення, що дозволяє знайти такий час тестування, при якому повна вартість усунення дефектів під час тестування та експлуатації буде мінімальною, і тим самим вирішити одну з найважливіших проблем керування проектом – прийняття обґрунтованого рішення щодо завершення тестування та випуску ПЗ.

III. Особливості побудови математичної моделі

Математична модель оптимізації часу тестування побудована на основі стохастичного підходу і базується на припущенні, що процес виникнення відмови описується неоднорідним процесом Пуассона [4]. За критерій оптимізації часу тестування, який і слугує критерієм завершення тестування ПЗ, вибрано максимізацію різниці між зменшенням ризику і повною вартістю його тестування.

Результуюча модель оптимізації часу тестування ПЗ у випадку експоненційної моделі надійності набула виду:

$$T = -\frac{1}{a}\ln\left(\frac{k_1}{a * m * (K_s(1-\exp(-a * t_e)) - k_2)}\right),$$

де T – оптимальний час тестування; t_e - час виконання модуля в період експлуатації ПЗ; K_s – внесок модуля у ризик відмов ПЗ (вартість можливих збитків через відмови модуля за час його виконання t_e при експлуатації ПЗ); m – кількість дефектів, які має модуль на початку тестування; a – коефіцієнт пропорційності, що дорівнює швидкості виявлення одного дефекту; k_1 – вартість одиниці часу тестування; k_2 – вартість усунення дефекту, що призвів до відмови в процесі тестування.

Список використаних джерел

1. Musa J.D., Everett W.W. Software-Reliability Engineering: Technology for the 1900 // IEEE Software. - 1990. - № 11. - P. 36-43.
2. Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу. НД ТЗІ 1.1-003-99. – 1999. 51 с.
3. Канер С., Фолк Д., Нгуен Е.К. Тестирование программного обеспечения: Пер с англ. - К.: DiaSoft. – 2000. – 544 с.
4. Коваль Г. И, Коротун Т. М, Яблокова Т. Л, Куцаченко Л. И. Подход к тестированию и оценке надежности программного обеспечения при управлении проектом. // Проблемы программирования. – 2000. - № 3-4. – С. 83-88.