АНАЛІЗ І СИНТЕЗ СКЛАДНИХ СИСТЕМ ЗА КРИТЕРІЄМ НАДІЙНОСТІ

УДК 681.3.06

В.С. Харченко, О.М. Тарасюк
Національний аерокосмічний університет ім. М.Є. Жуковського "ХАІ",
кафедра КСМ

ПРОЦЕДУРИ АНАЛІЗУ І СИНТЕЗУ МОДЕЛЕЙ НАДІЙНОСТІ ПРОГРАМНИХ ЗАСОБІВ З ВИКОРИСТАННЯМ МАТРИЦЬ ПРИПУЩЕНЬ

Запропоновано комплекс формальних процедур для систематизації, аналізу, комплексування, верифікації та синтезу моделей надійності програмних засобів. Сформульовано послідовність використання процедур при оцінці надійності.

Formalized procedures of systematization, analysis, complexation, verification and synthesis of software reliability models are developed. A general algorithm of using these procedures is proposed.

Постановка задачі. Надійність комп'ютерних систем, важливих для безпеки комплексів критичного призначення (аерокосмічних, енергетичних та інших) , стає все більш залежною від надійності програмних засобів (ПЗ). Це підтверджується динамікою зростання відносної частки причин аварій і катастроф таких комплексів внаслідок дефектів ПЗ [1]. Забезпечення надійності ПЗ неможливе без розробки методів адекватної оцінки її рівня.

Методи кількісного та якісного аналізу надійності ПЗ, що активно розвиваються останні два десятиріччя [1–4], відповідають різним принципам і навіть філософіям оцінки. Незважаючи на це, вони можуть ефективно доповнювати один одного при проведенні верифікації та експертизи критичних ПЗ, оцінці та атестуванні софтверних фірм згідно з моделлю технологічної зрілості CMM-SEI.

У [5, 6] запропоновано метод вибору моделей надійності ПЗ, який поєднує переваги та використовує елементи як кількісного, так і якісного підходів і базується на аналізі матриць припущень (МП), характерних для програмних засобів і процесів їх розробки, тестування та використання. Ці припущення визначаються експертним методом і за результатами обстеження проекту ПЗ відповідно до спеціально розроблених шаблонів. Слід зазначити, що МП-метод надає потенційну можливість не тільки вибирати моделі, але й проводити їх верифікацію та формувати рекомендації щодо синтезу нових моделей. Для цього необхідно створити операційний базис і розробити спеціальні процедури, які б дозволили аналізувати і перетворювати моделі відповідно до множини припущень.

Мета статті — подальший розвиток МП-методу шляхом розробки комплексу формальних процедур і операцій аналізу, вибору та синтезу МНПЗ. Процедури, на базі яких можуть синтезуватися нові моделі, уніфікуються з відповідними процедурами для аналізу вибору МНПЗ.

Вихідні поняття. Матрицею припущень МНПЗ є бульова матриця

$RD = ||\alpha_{ij}||$, $i = \overline{1, n_D}$, $j = \overline{1, n_M}$, де $n_M = card\ MM$, $n_D = card\ MD$ ($MM=\{M_j\}$ і $MD=\{D_i\}$ — відповідно множини моделей і припущень); $\alpha_{ij} = 0$ (1), якщо $D_i\ \overline{S}\ M_j$ ($D_i\ S\ M_j$);

S ($\overline{S}$) — відношення суттєвості (не суттєвості) припущення D_i для моделі M_j.

Слід зазначити, що множини *MM* і *MD* декомпозуються і подаються далі у вигляді ієрархій, що формуються за результатами аналізу та систематизації моделей і припущень відповідно до [6]. Рядки та стовпці матриці *RD* утворюють вектори моделей і припущень $\overline{\alpha_{Mi}}$, $\overline{\alpha_{Dj}}$. Для порівняння моделей надійності (припущень) за векторами $\overline{\alpha_{Dj}}$ ($\overline{\alpha_{Mi}}$) визначається D — відстань моделей M_j і M_f (припущень D_i і D_k):

$$DM_{jf} = \sum_{i=1}^{n_D} \alpha_{ij} \oplus \alpha_{if},\ DD_{ik} = \sum_{j=1}^{n_M} \alpha_{ij} \oplus \alpha_{kj}.$$

Для подальшого, більш детального аналізу можуть бути введені поняття простих і унікальних моделей та припущень відповідно до виду векторів $\overline{\alpha_{Mi}}$, $\overline{\alpha_{Dj}}$, а також сусідніх моделей і припущень.

Процедура формування МП. Формування вихідної матриці RD_0 (процедура P_0) здійснюється шляхом побудови ієрархії елементів множин MM_0, MD_0 і визначення векторів $\overline{\alpha_{D}}$ для кожної з моделей.

Внесення нових моделей $M_н$ до бази даних (БД) МНПЗ, що полягає у розширенні матриці RD_0 (процедура P_1), реалізується через операції визначення елементів вектора $\overline{\alpha_{Dн}}$. Цей вектор є конкатенацією елементів вектора $\overline{\alpha_{D_0}}$, які визначаються відносно вихідної множини MD_0, і елементів вектора $\Delta\overline{\alpha_{Dн}}$, що описують припущення для моделі $M_н$. Крім того, визначаються відношення суттєвості S додаткових припущень моделей $M_н$ для всіх моделей множини MM_0, тобто фіксуються додаткові елементи α_{jk}, $j \in \overline{1, n_{mo}}$, $k = \overline{n_{Do}+1, n_{Do}+|\Delta\overline{\alpha_{Dн}}|}$. Місце (номер стовпця в МП) моделі залежить від її типу відповідно до вихідної ієрархії МНПЗ.

Процедура внесення нових припущень $D_н$ в БД МНПЗ (процедура P_2) виконується шляхом визначення елементів вектора $\overline{\alpha_{Miн}}$ і розміщення цього припущення в матриці RD_0 відповідно до ієрархії.

Процедури комплексування МНПЗ. Оскільки моделі надійності описують характеристики ПЗ на різних етапах життєвого циклу, доречно проаналізувати їх вхідні-вихідні параметри з точки зору сумісності і можливості об'єднання (комплексування) МНПЗ. Така задача реалізується шляхом побудови графа сумісності моделей (процедура P_3) і визначення груп МНПЗ, що можуть комплексуватися (процедури P_4). Прикладом комплексування є побудова узагальненої моделі надійності на базі МНПЗ Холстеда і Муси-Окумото [1, 2]. Метрика Холстеда (очікувана кількість дефектів ПЗ) є вихідним параметром моделі Муси-Окумото, що визначає функцію ризику (інтенсивність прояву дефектів ПЗ).

Процедури вибору МНПЗ. Базова процедура вибору моделей P_5 полягає у формуванні фактичного вектора припущень $\overline{\alpha_{Df}}$ за результатами аналізу ПЗ, порівнянні

його з усіма векторами $\overline{\alpha_{Dj}}$, j = $\overline{1, n_M}$, і визначенні моделі, для якої $\overline{\alpha_{Df}}$ = $\overline{\alpha_{Dj}}$. Тоді модель M_j є остаточно вибраною моделлю.

Якщо в *RD* така модель відсутня, формується підмножина моделей ΔMM, для яких *D*-відстань є мінімальною (процедура P_6). Надалі проводиться аналіз $M_f \in \Delta MM$ з метою визначення можливості їх відповідної доробки або уточнення критичності припущень, що обумовлюють ненульову *D*-відстань (процедура P_7). Крім того, виконується процедура визначення параметрів моделі (процедура P_8) з використанням методів регресійного аналізу, найменших квадратів та ін.

Процедури верифікації МНПЗ. Верифікація моделей надійності може проводитись при розробці та експертизі ПЗ, що обумовлюється деякими міжнародними стандартами, зокрема [7]. Ця задача виконується шляхом перевірки відповідності вектора $\overline{\alpha_{Dв}}$ вибраної моделі надійності векторові $\overline{\alpha_{Df}}$, що залежить від фактичних припущень, характерних для ПЗ (процедура P_9). Елементи $\overline{\alpha_{Df}}$ визначаються експертним шляхом.

Крім того, повинні верифікуватися параметри моделі та оцінюватися точність їх обчислення (процедура P_{10}) [4].

Процедури синтезу МНПЗ. Розробка нових моделей необхідна, якщо БД моделей не вміщує задовільних (за результатами виконання процедур P_6, P_7) МНПЗ. Пропонується для всіх критичних припущень сформувати додаткові ієрархії (процедура P_{11}), що деталізують її особливості. Зокрема, припущення щодо однакового впливу всіх дефектів ПЗ на їх працездатність може буде подане дворівневою ієрархією (перший рівень — "впливає–не впливає"; другий рівень — "впливає у межах виконання команди або циклу обчислень і не потребує відновлення — впливає і потребує відновлення — відновлення неможливе").

Після цього визначають відношення суттєвості за всіма припущеннями для існуючих моделей. Логічно передбачити, що для додаткових припущень (другого рівня ієрархії для наведеного вище прикладу) вектори $\overline{\alpha_D}$ будуть нульовими. Тому надалі проводиться фіксація усіх додатково введених ієрархій (множин) припущень MD_t^*, $t=1,..., n_D$.

Розширення ієрархії припущень формує багатовимірний простір (процедура P_{12}), що описується декартовим добутком множин:

$$MB^{**} = MB_1^{**} \text{ Ч } MB_2^{**} \text{ Ч } \ldots \text{Ч } MB\,n_D^{**} \text{ б } MB_e^{**} = MB \cup MB_e^{*} \text{ б } e=1 \text{бююю} b\, n_D \text{ ю}$$

Множина MD^{**} надалі може стискатися з урахуванням несумісності елементів множини MD^{**} і після цього утворювати базу для задання вимог (специфікацій) до нових моделей. Ці моделі синтезуються шляхом модифікації (узагальнення) існуючих МНПЗ (процедура P_{13}).

Особливості розробки МНПЗ багатокомпонентних програмних засобів. Частковими варіантами синтезу є розробка моделей надійності багатоверсійних [8] і багатокомпонентних ПЗ з раніше створеними спеціальними або комерційними, так званими COTS (Commercial-Off-The-Shelf) – елементами [9, 10]. Для цього формуються процедури P_{14} і P_{15} .

Багатоверсійне ПЗ може розглядатися як "біла скриня", і тоді для кожної з версій та відновлювальної підсистеми модель надійності вибирається відповідно до процедур $P_5 – P_7$ (або $P_{11} – P_{13}$), а загальна модель визначається з урахуванням архітектури системи загалом.

Якщо такі ПЗ розглядаються як “чорна скриня”, то реалізуються процедури вибору (синтезу) за умов наявності у БД моделей багатоверсійних програмних засобів і характерних для таких ПЗ припущень. Для багатокомпонентних ПЗ доцільнішим є перший підхід.

Практичні результати. Загальна послідовність оцінки надійності програмних засобів має такі етапи:

– формування і поповнення матриці МП (БД МНПЗ) з використанням процедур $P_0 – P_2$;

– комплексування і вибір моделей відповідно до припущень, характерних для ПЗ (процедури $P_3 – P_8$). Якщо ці процедури не дозволяють вибрати модель з урахуванням наявних припущень або незадовільною є точність обчислення параметрів, здійснюється перехід до процедур синтезу або до пошуку моделей іншого класу (параметричних, лінгвістичних та ін.);

– синтез нової моделі із застосуванням процедур P_{11} - P_{13} (або процедур P_{14}, P_{15} для багатоверсійного і багатокомпонентного програмного забезпечення);

– перевірка адекватності моделей надійності програмному проекту шляхом верифікації вибраних (синтезованих) моделей за процедурами P_9, P_{10}.

На базі МП–методу та формалізованих процедур $P_0 – P_{15}$ розроблено базу даних МНПЗ, архітектуру інструментальної системи оцінки надійності ПЗ і окремі утиліти, що підтримують процес вибору (синтезу) та верифікації моделей. Відповідні алгоритми пройшли експериментальну перевірку при розробці операційної системи реального часу авіаційного комплексу та на тестовому завданні [1]. Подальший розвиток інструментальних системи планується шляхом інтегрування з базами метрик якості та надійності ПЗ і засобами їх оцінки при незалежній верифікації і валідації та експертизі [11,12].

1. Lyu M.R. (ed.) Handbook of Software Reliability Engineering. McGraw-Hill Company. US. — 1996. — 803 p. 2. Musa J.D., Okumoto K. Software Reliability Models: Concepts, Classification, Comparisons and Practice, Electronic Systems Effectiveness and Life Cycle Costing. — NATO ASI Series, F3. Springer-Verlag. Heidelberg. 1993. — P. 395—424. 3. Полонников Р.И., Никандров А.В. Методы оценки надежности программного обеспечения. — Санкт-Петербург. Политехник. — 128 с. 4. Nikora A. P., Lyu M. R. An experiment in determining software reliability model applicability // Proceedings of the 6th International Symposium on Software Reliability Engineering. US. — June 1995. — P. 304—313. 5. Харченко В.С., Скляр В.В., Вилкомир С.А. Выбор моделей надежности программных средств для критического применения. Управляющие системы и машины. — 2000. — № 3. — С.59—69. 6. Kharchenko V.S., Tarasyuk O.M., Sklyar V.V., Dubnitsky V.Yu. The Method of Software Reliability Growth Models Choice Using Assumptions Matrix // Proceedings of 26th Annual International Computer Software and Applications Conference (COMPSAC). — England. — Aug. 2002. — P. 54—546. 7. IAEA Safety Standards Series. — No. NS-G-1.1. Software for Computer-based Systems Important to Safety in Nuclear Power Plants. — 2000. 8. Kharchenko V.S. Multiversion Systems: Models, Reliability, Design Technologies // Proceeding of 10th European Conference on Safety and Reliability. — Germany. — September. 1999. — Vol. 1. — P. 73—77. 9. Scott J.A., Preckshot G.G., Gallagher J.M. Using Commercial-Off-The-Shelf (COTS) Software in High-Consequence Safety Systems. Lawrence Livermore National Laboratory. UCRL—122246. 10. Харченко В.С., Харченко К.В. COTS- і CrOTS-подходы к повышению эффективности критических и коммерческих IT-проектов // Системи обробки

інформації. — Харків. НАНУ. — 2002. Вип. 2 (18). — С.252—258. 11. Vilkomir S.A., Kharchenko V.S., Ponomaryev A.I., Gorda A.A. The System Safety Assessment by the Use of Tools // Proceedings of the 17th International System Safety Conference. — USA. — Aug., 1999. P. 222—227. 12. Харченко В.С., Ястребенецкий М.А., Васильченко В.Н. Нормирование и оценка безопасности информационных и управляющих систем АЭС: регулирующие требования к программному обеспечению // Ядерная безопасность. —2002. — №2. С.14-27.

УДК 621.391.18

Б.Ю. Волочій, Л.Д. Озірковський, *Д.О. Улибін
Національний університет "Львівська політехніка", кафедра ТРР,
*Український Львівський інститут бізнесу та інформатики

МАРКОВСЬКА МОДЕЛЬ ЯК ЗАСІБ КОМПЛЕКСНОГО МОДЕЛЮВАННЯ ІНФОРМАЦІЙНИХ СИСТЕМ З ФУНКЦІОНАЛЬНИМ РЕЗЕРВУВАННЯМ

Комплексне моделювання передбачає побудову моделі інформаційної системи, яка поєднувала би функціональний і надійнісний аспекти її проектування. Запропоновано спосіб побудови комплексної моделі.

Complex modeling provides for developing a model of information system which would combine functional and reliability aspects of system designing. The report presents the method of complex model development.

Вступ. Інформаційна система з функціональним резервуванням є комплексом інформаційних систем, здатних при певних умовах автономно або при взаємодії кількох систем вирішувати поставлене завдання. Порядок використання інформації від кожної інформаційної системи на основі оцінки їх стану і умов функціонування комплексу здійснює людина-оператор. Якість роботи такого комплексу значною мірою залежить від психофізіологічного стану людини-оператора. Робота людини-оператора може бути представлена відповідним алгоритмом поведінки. Таких алгоритмів може бути розроблено багато варіантів і відповідь на питання **"**який кращий?" можна отримати на основі тривалого випробування комплексу інформаційних систем з кожним варіантом побудови алгоритму поведінки. На основі зібраних статистичних даних про роботу комплексу інформаційних систем можна визначити його показники ефективності для кожного варіанта побудови алгоритму поведінки і отримати відповідь на запитання, який алгоритм поведінки є найкращим.

Така задача може вирішуватись за значно коротший термін, якщо проектант буде мати в своєму розпорядженні математичну модель інформаційної системи з функціональним резервуванням для кожного варіанта побудови алгоритму поведінки.