УДК 681.51

Т. М. Боровська, канд. техн. наук, доц.;
Є. П. Хомин, асп.;
П. В. Северілов

МОДЕЛІ ЕФЕКТИВНОСТІ І ЖИВУЧОСТІ ТЕХНІЧНИХ СИСТЕМ

Вартість втрат у результаті аварій в сучасних технічних системах в декілька разів перевищує вартість самої системи, тому введені десятки стандартів відмовобезпечності, катастрофостійкості. Пропонується підхід на базі створення єдиної моделі для аналізу ефективності і живучості. Введені поняття «конфігурація модифікації системи» і «конфігурація відмови». Запропоновано об'єднання показників відмовостійкості як інтервалів області визначення функції живучості.

Вступ

Ефективність і масштаби застосування сучасних систем швидко зростають. Безпосередні чинники — високі технології в поєднанні з комп'ютеризацією всіх аспектів діяльності. Однак, темпи зростання втрат у разі різноманітних відмов набагато вищі. Це безпрецедентна проблема для теорії і практики. Класична теорія надійності — досконала теорія, але з багатьох причин недостатня для вирішення проблем безпечності технічних систем. Теорія живучості, що займається відмовобезпечністю, катастрофостійкістю та іншими подібними аспектами розробки та використання технічних систем, поки не є цілісною наукою — існують галузеві напрями — живучість будівельних конструкцій, живучість кораблів і літальних апаратів, швидко розвивається живучість комп'ютерних систем. Ще одна ознака актуальності — ця тематика постійно присутня в численних наукових конференціях під егідою IEEE.

Свідоцтвом актуальності теми є велика кількість публікацій, в тому числі нормативних документів, відповідних монографій підручників з розділами, в яких розглянуто живучість. Відібрано і переглянуто велику кількість публікацій релевантних для цієї статті. Прямих аналогів не знайдено. Типові приклади робіт — [1, 2, 3]. В роботі [1] розглянуто питання живучості телекомунікаційних мереж у разі відмов різного рівня. В роботі використовуються паралельно імітаційні та аналітичні моделі. В роботі [2] розглядається «робастність» нечутливість до відмов структурованих систем, що можуть бути подані графами. Використовуються тільки статистичні та ймовірнісні моделі. Робота [3] — найближчий аналог за методологією: вводиться метрика для величини відмов і наслідків відмов. Однак методи прив'язані до конкретної задачі — стійкості трафіка в оптоволоконних мережах.

Мета дослідження — побудувати цілісну технологію конструювання моделей, що об'єднує аналіз проектних рішень одночасно за критеріями ефективності і живучості. База для побудови технології — ресурсний підхід «витрати—втрати» та трирівнева декомпозиція технічної системи не тільки на функціональні підсистеми, але структурні, редукційні. В теорії надійності такій декомпозиції відповідає неідентичне резервування.

Термінологія у області надійності і безпеки як така не склалася. Уточнимо відому термінологію стосовно задач роботи і вибраної концепції «витрати—ефект».

Ефективність в номінальних умовах — для конкретних класів технічних систем ці вимоги стандартизовані, наприклад, для автомобіля це мінімізація експлуатаційних витрат, в першу чергу, — витрат палива. Останнє стало значущим після введення екологічних обмежень. Подібні показники ефективності встановлені для хімічних реакторів.

Ефективність в неномінальних умовах — відомі випадки займання ноутбуків і електрочайників, скандальні дефекти в програмному забезпеченні бірж і аеропортів. Тому безпека — найнеобхідніша вимога на всіх рівнях «неномінальності», що знайшло віддзеркалення в професійній термінології (кальки з англійського): «нечутливість до одиничної відмови», «чудовий відгук на подвійну відмову», «задовільний відгук на потрійну відмову». Ефективність в неномінальних умовах розпадається на низку стандартизованих показників.

Надійність статистична (ймовірність безвідмовної роботи на заданому часовому інтервалі системи або елемента) важливий показник, предмет запеклих науково-технічних дискусій і спроб змінити суть і назву поняття, наприклад, «гарантоздатність», «живучість».

Відмовонечутливість — властивість технічної системи у разі відносно малих за вартістю відмов не погіршувати рівень якості функціонування системи. Сучасні серверні кластери продовжують нормально працювати після вилучення одного з процесорів, висмикування шнура з розетки. Аналогічно організовуються системи енерго- і теплопостачання.

Відмовостійкість — властивість технічної системи у разі середніх за вартістю відмов певних елементів (система працює гірше, але ще задовільно, наприклад, у разі відмови 2-х з 3-х процесорів сервер обробляє дані повільніше, лайнер може летіти на двох двигунах з чотирьох). Головне в цій властивості те, що відмови не спричиняють за собою нові відмови. Аналіз катастрофічних пожеж показує, що забезпечення вогнестійкості не вимагає великих витрат, якщо це зробити на стадії проектування, безвідносно до ймовірності всіх можливих подій.

Відмовобезпечність — за великих відмов система перестає працювати, але, по можливості, безпечно для персоналу і навколишнього середовища.

Вважається, що вимоги номінальної і неномінальної ефективності суперечливі, тому високої ефективності можна досягти ціною зниження безпеки, а задоволення вимог безпеки веде до зниження ефективності. У техніці такі ситуації проектування називають «або—або». Ці твердження істинні, якщо процес проектування складається з двох етапів, які стисло назвемо «проектування ефективності в номінальних режимах», «проектування ефективності в неномінальних режимах». Приклад: на другому етапі підсилювач резервують ще двома підсилювачами, розміщеними в тому ж корпусі. В підсумку у разі виходу з ладу будь-якого підсилювача виходять з ладу всі інші.

Задачі дослідження:

1. Об'єднати два види проектування. Це дозволить вже в процесі проектування виявляти несумісні проектні рішення і дає шанс знайти проектні рішення класу «I—I»: і ефективність, і живучість.

2. Об'єднати показники надійності, відмовонечутливості, відмовостійкості і відмовобезпечності в один — функцію живучості.

Концепція проектування ефективності і живучості

У книгах з надійності зустрічаються такі вислови: «надійність — не вправа в статистиці, а пошук конкретних конструкторських рішень», «закласти надійність в ідею, концепцію проекту». Класична теорія надійності пропонує, в основному, схеми ідентичного резервування. Високі технології майже «вбили» класичну надійність: у номінальних умовах багато технічних пристроїв мають напрацювання на відмову мільйони і мільярди років, а відмовляють за істотного порушення режимів функціонування (температура, перевантаження, радіація) [1—3].

Виходячи з того, що інноваційні системи не створюються з нуля, а від деякого прототипу, варіанту, сформулюємо сценарії для процедур оцінки ефективності і живучості на деякому кроці проектування. На рис. 1 показані два сценарії проектного аналізу: введення або заміна деяких підсистем; відмова або вилучення деяких підсистем [4—6].

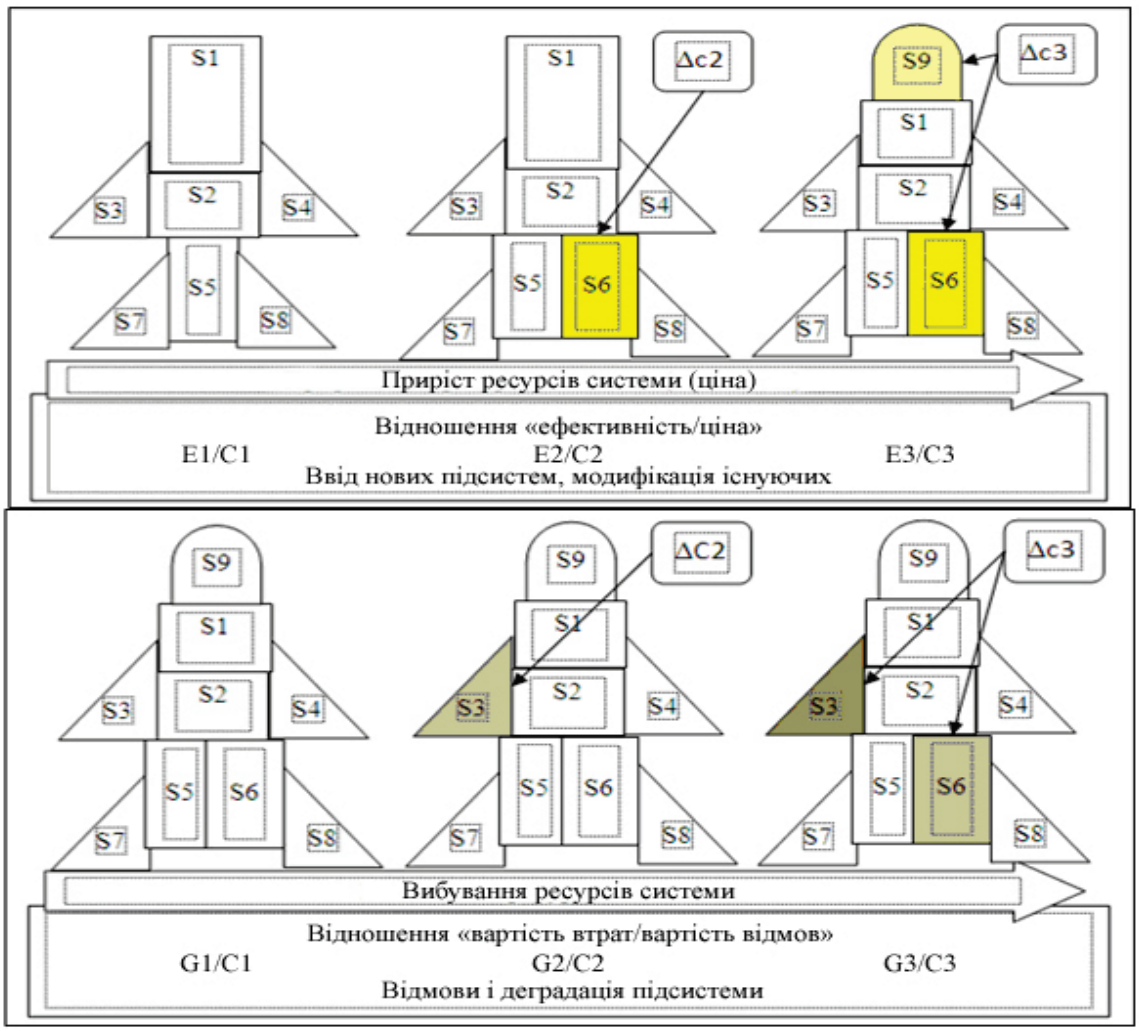

Рис. 1. Схема проектування системи для режимів номінального і неномінального функціонування

Процедура аналізу конфігурації проектних змін. «Включимо» (з урахуванням всіх інтерфейсних проблем) до складу наявної системи (прототипу) нову підсистему і оцінимо підвищення ефективності системи, а потім «виключимо» цю підсистему і оцінимо зміну ефективності системи. Так в режимі «крок вперед, крок назад» нарощуємо і удосконалюємо систему (на рис. 2, 4 показано умовно по два кроки проектування), поки не досягнемо границі обмеження витрат на проектування, на ціну об'єкта проектування. Узагальнимо сценарій: є деякий варіант поліпшення системи ціною $dC2$. Розглядатимемо безліч варіантів поліпшення системи ціною $dC2$. Природно в проектуванні вибрати варіант, що дає максимальний приріст ефективності, а в проектуванні живучості теж максимальний приріст втрат для відмови ціною $dC2$ — розраховуємо на гірше. Після цього шукаємо нові проектні рішення для зменшення втрат і підвищення ефективності.

Процедура аналізу конфігурації відмови. Для визначення функцій ефективності і живучості введемо такі поняття: початкова конфігурація відмови (ПКВ) — поєднання підсистем, що одночасно відмовили. Термін «початкова» означає, що існує динаміка відмов в системі і, відповідно: статичні відмови, динамічно наростаючі і динамічні (само) усуваються.

Якщо систему розглядати як множину підсистем $\{P_i\}$, $i = 1,...,N$, очевидно, множина всіх ПКВ $\{KG_l\}$, $l = 1,...L$ буде підмножиною множини $\{P_i\}$. Можливі два підходи до опису ПКВ — кількість елементів в ПКВ, — сумарна вартість цих елементів. Вибираємо другу альтернативу.

Для кожної ПКВ визначити: $C(KG_l)$ — сумарна вартість всіх підсистем цієї ПКВ; $G(KG_l)$ — сумарні втрати цієї ПКВ (вартість втрачених підсистем, втрата ефективності, аварія...). Інтервал вартостей відмови $(0, Csys)$ розбиваємо на інтервали $C_j \pi C(KG) \le C_j + \delta C_j$.

Визначимо функцію живучості $Gf(C_j) = \max(G(KG_j))$ для всіх конфігурацій відмов, вартість

яких лежить у відповідному інтервалі (0, *Csum*), де *Csum* — вартість системи. Запишемо загальні словесні і математичні формулювання розширеного сценарію проектування:

— розбиваємо інтервал вартостей відмов на деяке число *K* інтервалів;

— розбиваємо множину конфігурацій відмов (0, *Csum*) на підмножини *KGj* відповідні інтервалам вартості відмов;

— визначаємо для кожної ПКВ втрати *G*(*KGj*), для кожного інтервалу вартості відмови будуємо рангові і частотні розподіли, знаходимо конфігурацію з максимальними втратами.

Ця конфігурація і її околи — об'єкти для пошуку конструкторських рішень, що дозволяють зменшити втрати.

Процедура проектування ефективності симетрична процедурі проектування живучості. На рис. 2 подані відповідні графіки і математичні моделі. Для кожного інтервалу вартості відмови будуємо рангові і, можливо, частотні розподіли, знаходимо конфігурацію з максимальними втратами. Ця конфігурація і її околи — об'єкти для пошуку конструкторських рішень, що дозволяють зменшити втрати. Сценарій проектування ефективності подібний сценарію проектування живучості [6].

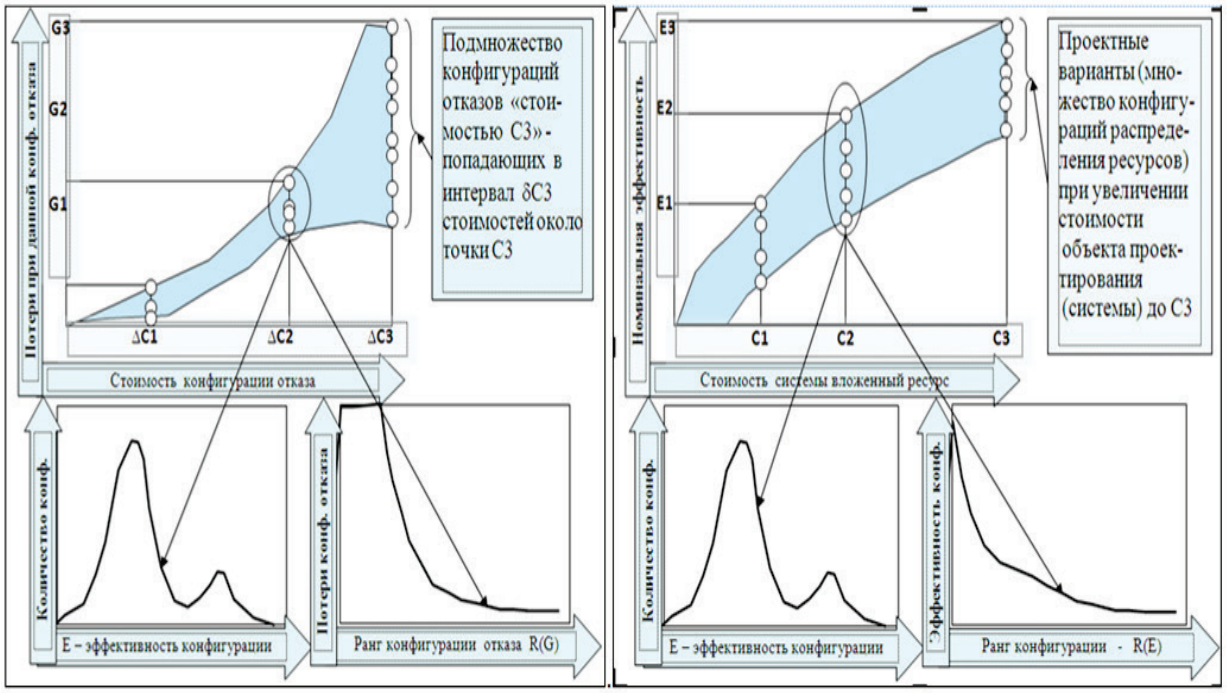

Рис. 2. Аналіз конфігурацій системи в номінальних і неномінальних режимах

Проаналізуємо процедури аналізу ефективності і живучості:

— в проектуванні для номінальних режимів (немає поки вдалих і загальноприйнятих термінів для двох видів проектування) *проектувальник сам винаходить і вибирає елементи і конфігурації;*

— в проектуванні для неномінальних режимів *навколишнє середовище створює конфігурації відмов на базі елементів вибраних і зв'язаних проектувальником*, який повинен виконати оцінку втрат і за необхідності модифікувати систему.

Модель: «функція живучості». Те, що подано на рис. 2 як гіпотези про властивості «живучість» і «ефективність» на множині проектних варіантів технічної системи, базується на пошукових робочих моделях — реалізаціях гіпотез і знань.

На рис. 3 показані приклади побудови таких апроксимацій нечіткої функції живучості. Дискретна модель — для представлення втрат окремих конфігурацій відмов. Неперервна модель — «згладжена» апроксимація дискретної моделі.

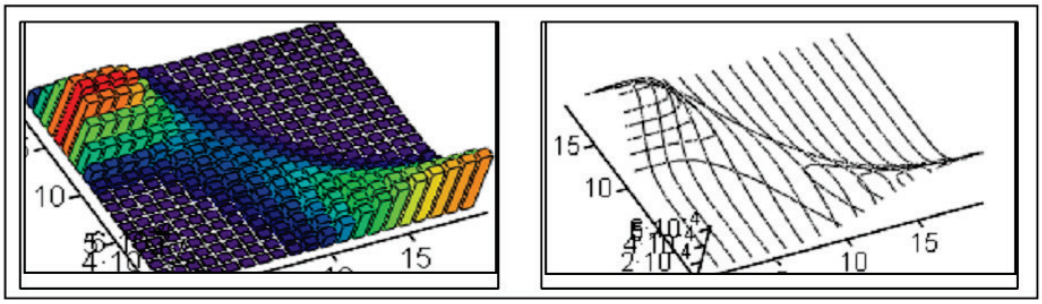

Рис. 3. Дискретна і неперервна моделі функції живучості

На рис. 4 показано графічне представлення понять, які звичайно визначаються і обговорюються на словесному рівні. Бачимо, що компоненти поняття «живучість» можуть бути представлені нечіткими інтервалами на графіку функції живучості.

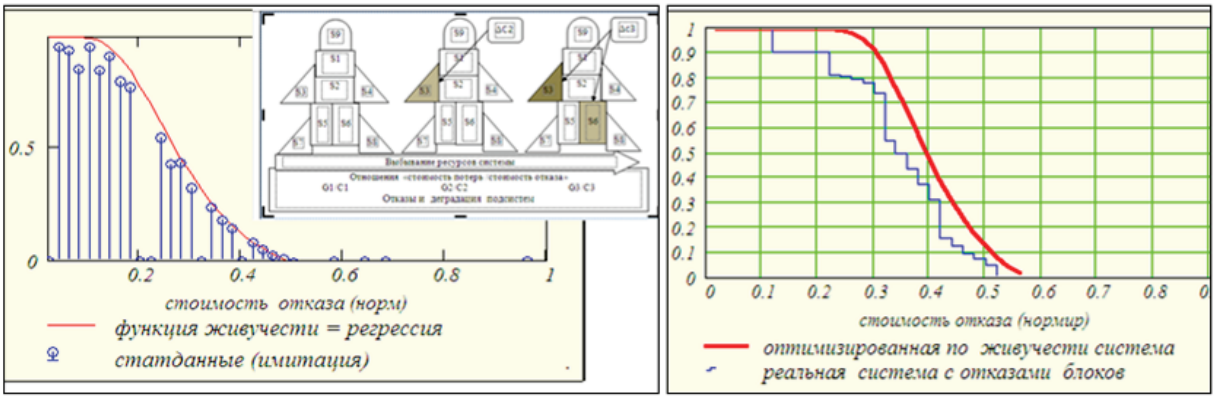

Рис. 4. Побудова функції живучості на основі аналізу конфігурацій відмов

На рис. 5 показаний приклад аналізу окремих показників живучості. Такий аналіз дозволяє оперувати з властивостями цілісної системи.

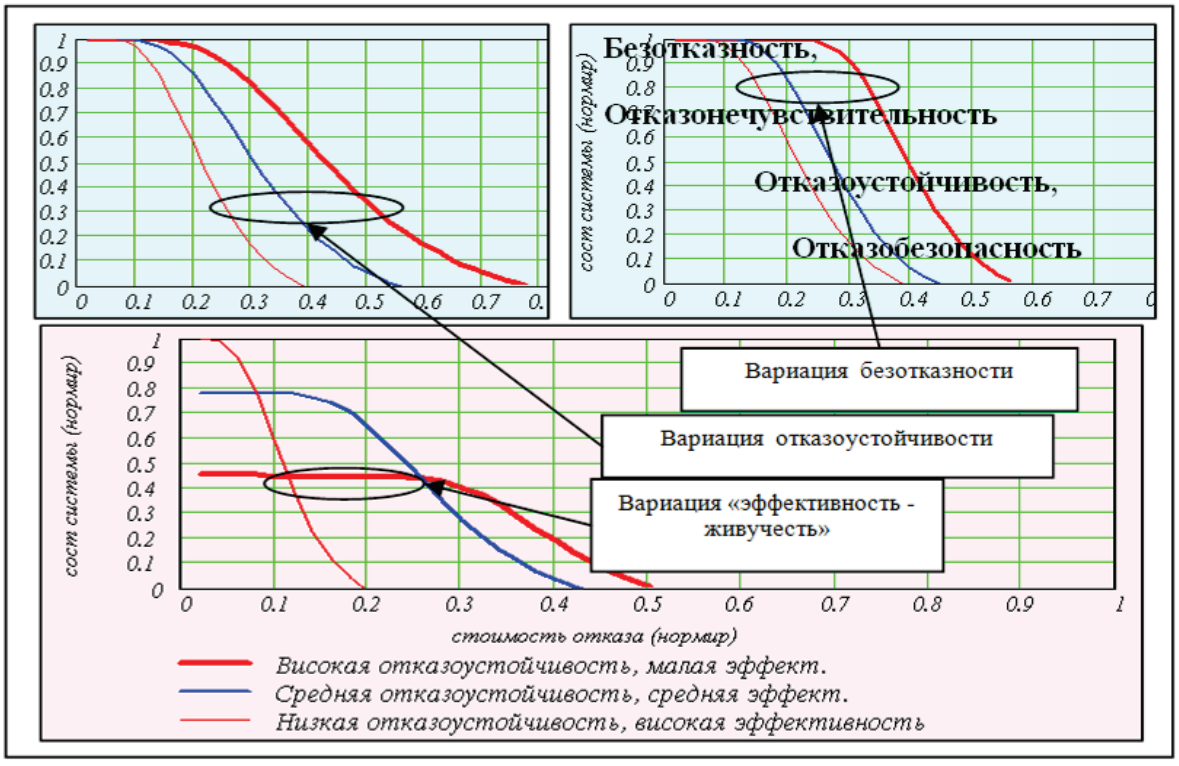

Рис. 5. Варіації моделі живучості

Варіації функцій живучості на рис. 5, по суті, — результат певних конструктивних змін в технічній системі. Для певних впорядкованих і стандартизованих класів технічних систем, наприклад, мікропроцесори, автомобілі, танки, сервери — складна, але здійснима задача знаходження залежності між витратами і варіаціями функції живучості. Це окрема тема.

Методи забезпечення живучості

За методами забезпечення живучості системи можна розділити на два класи: системи без реконфігурації, системи з реконфігурацією. У літературі розглядаються задачі реконфігурації для літальних апаратів, проте, цей підхід продуктивний для задач управління виробничими системами [1—3]. Розглянемо робочі моделі для двох варіантів реконфігурації деякої лінеаризованої динамічної системи.

Задана модель динаміки об'єкта

$$\frac{d}{dt}X = A \cdot X + Bo \cdot Ro \cdot uo = \frac{d}{dt}Xc + \frac{d}{dt}Xu, \tag{1}$$

де $\frac{d}{dt}Xc$ — власний рух; $\frac{d}{dt}Xu$ — вимушений рух; $Ro \cdot uo = u$ — m-мірний вектор управління; uo — n-мірний вектор базового управління, Ro — матриця розподілу базового управління між функціонуючими елементами. Запишемо умову відмовочутливості

$$\frac{d}{dt}Xuf = \frac{d}{dt}Xun, \tag{2}$$

де $\frac{d}{dt}Xuf$ — прискорення від управління у разі відмов, $\frac{d}{dt}Xun$ — прискорення від номінального управління. Враховуючи (1), зводимо (2) до вигляду

$$Bo \cdot Ro \cdot uo = B1 \cdot R1 \Rightarrow B_0 \cdot R_0 = B1 \cdot R1.$$

Після алгебраїчних перетворень отримуємо:

$$R1 = B1^{-1} \cdot Bo \cdot Ro, \tag{3}$$

де Bo, Ro — номінальні, $B1$, $R1$ — «збурені» (за наявності відмов) значення відповідних матриць. Отримані результати справедливі для $m = n$. За невиконання умови використовують «псевдозворотні матриці».

$$\left.\begin{array}{ll} m = n, & B1qv^{-1} = B1^{-1}; \\ m \succ n, & B1qv^{-1} = \left(B1^T \cdot B1\right)^{-1} \cdot B1^T; \\ m \prec n, & B1qv^{-1} = B1^T \cdot \left(B1 \cdot B1^T\right)^{-1}. \end{array}\right\} \tag{4}$$

Для останніх двох випадків умова нечутливості (3) виконується приблизно. Суть псевдозворотності — знаходження матриці, яка дає мінімальну помилку в (3). Ми використали мультиплікативну компенсацію впливу відмов $Bo \cdot Ro \cdot uo = B1 \cdot R1 \cdot uo$. Можлива інша альтернатива — адитивна компенсація

$$Bo \cdot uoo = B1\left(uoo + \delta uoo\right), \tag{5}$$

де $uoo = Ro \cdot uo$.

Розв'язуємо (5) відносно δuoo:

$$\delta uoo = B1qv^{-1} \cdot \left(Bo - B1\right) \cdot uoo. \tag{6}$$

Після перетворень алгебри отримуємо:

$$un = \left[I + B1qv^{-1} \cdot \left(Bo - B1\right)\right] \cdot uoo. \tag{7}$$

Отримане управління має корисну властивість $Bo = B1 \Rightarrow un = uoo$, тобто за відсутності збурень система реконфігурації не заважає процесам номінального управління. В рамках цієї статті

зберемо викладене в загальні моделі і, для порівняння, дамо дві схеми проектування (рис. 6).

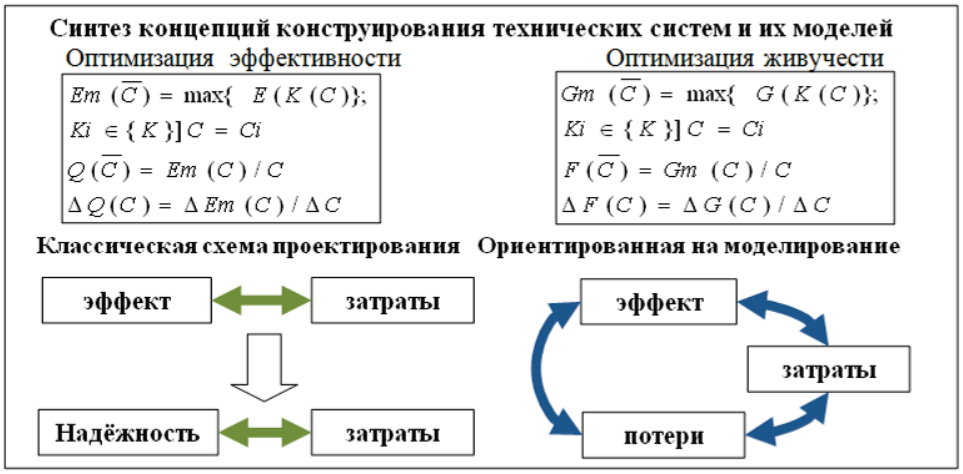

Рис. 6. Схема інтегрованої моделі для аналізу ефективності і живучості

Висновки

На базі декомпозиційного підходу отримані моделі проектування технічних систем, які дозволяють об'єднати окремі показники надійності і безпеки у функцію живучості. Запропоновані сценарії одночасного проектування системи на основі критеріїв ефективності в номінальних і неномінальних режимах. Запропонована інформаційна технологія конструювання моделей дозволяє раціонально упорядковувати проектні варіанти технічних систем. Розроблені імітаційні моделі функцій живучості, що дозволяють будувати ці функції як за статистичними даними, так і за даними імітаційного моделювання і використовувати методи теорії імовірності і нечіткості в проектному аналізі. Показано, що існуючу множину показників живучості можна подати як інтервали на шкалі вартості наслідків відмов.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. E. Heegaard. Network survivability modeling / E. Heegaard, K. S. Trivedi // Computer Networks, June, 2009. — Vol. 53. — No 8. — P. 1215—1234.

2. Robustness of structural systems — a new focus for the joint committee on structural safety (JCSS) Applications of statistics and probability in civil engineering — Kanda, Takada 2007, London.

3. Wojciech Molisz. Survivability function-a measure of disaster-based routing performance / Molisz Wojciech // IEEE Journal on Selected Areas in Communications. — November, 2004. — Vol. 22. — No 9. — P. 1876—1883.

4. Боровська Т. М. Використання декомпозиційних структур для синтезу регуляторів / Т. М. Боровська // Вісник Вінницького політехнічного інституту. — 2000. — № 1. — С. 5—14.

5. Боровська Т. М. Нечітка оптимізація розподілу обмеженого ресурсу у виробничій системі з неопуклими виробничими функціями елементів / Т. М. Боровська, І. С. Колесник, В. А. Северілов // Вісник Вінницького політехнічного інституту. — 2003. — № 5. — С. 36—41.

6. Боровская Т. Н. Декомпозиционный подход к анализу эффективности и живучести технических систем / Т. Н. Боровская // Dynamika naukowych badan — 2010 : materialy VI miedzynarodowej naukowi-praktycznej konferencji Przemysl (Polska). — 07.07—15.07.2010. — Przemysl: Nauka i studia, 2010. — Volume 10. — Str. 17—22.

Рекомендована кафедрою комп'ютерних систем управління

Стаття надійшла до редакції 22.12.10
Рекомендована до друку 17.01.11

Боровська Таїса Миколаївна — доцент, ***Хомин Євген Петрович*** — аспірант, ***Северілов Павло Вікторович*** — здобувач.

Кафедра комп'ютерних систем управління, Вінницький національний технічний університет, Вінниця