УДК 621.03

В.Г. СЕРБІН, А.І. СУХОМЛИН

ВИЗНАЧЕННЯ І ФОРМАЛІЗАЦІЯ ОСНОВНИХ ПОКАЗНИКІВ ГАРАНТОЗДАТНОСТІ ЖИВУЧИХ КОМП'ЮТЕРНИХ СИСТЕМ КЕРУВАННЯ НА ОСНОВІ ЙМОВІРНІСНО-ФІЗИЧНОГО ПІДХОДУ ДЛЯ ЇХ ПРОЕКТНОЇ ОЦІНКИ І ПРОГНОЗУВАННЯ

Анотація. *У статті розглянуті питання щодо визначення і формалізації основних показників гарантоздатності живучих комп'ютерних систем керування на основі ймовірнісно-фізичного підходу. Приведені узагальнені методики розрахунку основних показників гарантоздатності живучих комп'ютерних систем керування для їх аналізу, проектної оцінки і прогнозування.*
Ключові слова: *гарантоздатність, безвідмовність, живучість, готовність, функціональна безпека, комп'ютерна система керування, ймовірнісно-фізичний підхід, ймовірність безвідмовної роботи.*

Аннотация*. В статье рассмотрены вопросы определения и формализации основных показателей гарантоспособности живучих компьютерных систем управления на основе вероятностно-физического подхода. Приведены обобщенные методики расчета основных показателей гарантоспособности живучих компьютерных систем управления для их анализа, проектной оценки и прогнозирования.*
Ключевые слова**:** *гарантоспособность, безотказность, живучесть, готовность, функциональная безопасность, компьютерная система управления, вероятностно-физический подход, вероятность безотказной работы.*

Abstract*. The questions of definition and formalization of the main indicators of dependability survivable computer control systems based on the probabilistic-physical approach were regarded. The generalized calculation methods of the main indicators of dependability survivable computer control systems for their analysis, engineering estimate and prediction were introduced.*
Keywords: *dependability, failure-free, survivability, availability, functional security, computer control system, probabilistic-physical approach, probability of failure-free operation.*

1. Вступ

Ймовірнісно-фізичний підхід [1] до вирішення проблеми проектної оцінки та прогнозування основних показників гарантоздатності живучих комп'ютерних систем керування (ЖКСК) базується на використанні законів розподілення відмов (моделей надійності), які витікають із аналізу фізичних процесів деградації, що призводять до відмови. При цьому фізичні процеси деградації ЖКСК і їх елементів розглядаються як випадкові процеси. Цей підхід безпосередньо встановлює рівень ймовірності досягнення критичного стану фізичним визначальним параметром об'єкта, тобто пов'язує значення ймовірності відмови із значенням (фізичним станом) деякого визначального фізичного параметра об'єкта, який обумовлює відмову.

Під визначальними параметрами у даному випадку маються на увазі «первинні» фізичні параметри (накопичення дислокацій та інших дефектів, пластичні та пружні деформації, механічний знос, провідність контактуючих елементів і суцільних провідників току, p / n -переходів та ін.), перевищення якими визначених граничних значень обумовлюються відмови.

ISSN 1028-9763. Математичні машини і системи, 2012, № 4

Використання цього підходу для вирішення проблем проектної оцінки і прогнозування показників гарантоздатності ЖКСК відображує ідею: функція розподілення напрацювання до відмови (до критичної відмови) виявляється функцією деяких статистичних фізичних характеристик (параметрів) об'єкта або процесу його деградації, який обумовлює ймовірність часткового або повного руйнування об'єкта.

Цей підхід обумовлює порядок формалізації, оцінювання та прогнозування показників гарантоздатності об'єкта з використанням *DN* (дифузійно-немонотонного)-розподілу випадкової величини.

2. Загальний аналіз рівня гарантоздатності ЖКСК

Гарантоздатність (dependability) як глобальне поняття вперше було представлено в роботах [2, 3]. Крім того, в цих же роботах була обґрунтована і прокоментована потреба введення терміна «гарантоздатність» як узагальненого універсального поняття до вже великого списку існуючих понять: безвідмовність, відмовостійкість, надійність, ремонтопридатність, готовність, доступність, довговічність та ін. Це обумовлено двома причинами: по-перше, необхідністю усунення наявної плутанини між поняттям надійності як загального значення (властивості надійної системи) і надійності як математичної кількісної величини, що характеризує міру надійності системи, і, по-друге, показати, що терміни вищенаведеного списку є лише кількісними характеристиками – мірами різних виявлень однієї і тієї ж властивості системи – її гарантоздатності. Тому гарантоздатність ЖКСК визначається як її властивість надавати узгоджені специфікацією послуги, яким можна виправдано довіряти.

Згідно з [4], гарантоздатність об'єднує такі основні атрибути (поняття):

– безвідмовність (reliability) – здатність системи (функціонального блока) виконувати необхідну функцію за певних умов на заданому інтервалі часу;

– живучість (survivability) – властивість системи (функціонального блока) зберігати і відновлювати свою здатність до виконання основних функцій у передбаченому обсязі і протягом заданого напрацювання при можливій зміні структури системи і (або) алгоритмів та умов її функціонування внаслідок непередбачених специфікацією несприятливих впливів [5];

– готовність (availability) – здатність системи (функціонального блока) виконувати необхідні функції за певних умов у заданий момент або фіксований інтервал часу у разі забезпеченості необхідними зовнішніми ресурсами;

– функціональна безпека (safety) – відсутність шкідливих (катастрофічних) наслідків для користувачів, інших систем і навколишнього середовища;

– конфіденційність (confidentiality) – відсутність неправомірного доступу до інформації;

– цілісність (intagrity) – властивість системи (функціонального блока) не допускати непередбачених змін і послуг, що надаються;

– обслуговуваність (maintainability) – здатність системи (функціонального блока) піддаватися обслуговуванню і модифікації;

– ремонтопридатність (maintainability) – здатність системи до виявлення і усунення відмов і пошкоджень шляхом проведення профілактик і ремонтів.

Безвідмовність, живучість, готовність і функціональна безпека є, на погляд авторів, основними багатофакторними показниками гарантоздатності ЖКСК. Тому їх доцільно розглядати як найбільш об'єктивні показники гарантоздатності, які дозволяють найкраще оцінювати всі аспекти структурно-функціональної надійності ЖКСК. Під час дослідження і оцінки якості цих показників головна увага повинна звертатися на здатність ЖКСК справно і своєчасно виконувати передбачені специфікацією функції впродовж усього їхнього життєвого циклу (ЖЦ). Ці показники ЖКСК забезпечуються такими факторами:

– надійністю складових частин і елементів;

– резервуванням;
– досконалістю методів і засобів технічної діагностики;
– реконфігурацією;
– своєчасністю, повнотою і якістю технічного обслуговування та ремонту;
– достовірним прогнозуванням.

Основним способом підвищення рівня гарантоздатності ЖКСК є використання надлишковості технічних і програмних засобів порівняно з мінімально необхідними для виконання нею заданих функцій.

Гарантоздатність аналізують і оцінюють на різних етапах проектування, моделювання і функціонування ЖКСК. Аналізуючи процес функціонування ЖКСК в конкретних умовах їх експлуатації, допустимо визначати як якісні, так і кількісні показники цих параметрів для даних умов функціонування кожної конкретної ЖКСК.

Залежно від обмежень на умови функціонування, якісні і кількісні показники гарантоздатності будуть, як правило, різними навіть для однієї і тієї ж ЖКСК.

Аналіз рівня гарантоздатності доцільно проводити за допомогою оцінки показників якості функціонування ЖКСК в умовах виникнення відмов впродовж усього терміну їх ЖЦ.

Якість функціонування ЖКСК, як правило, доцільно оцінювати за такими багатофакторними показниками [5]:

– відповідність ЖКСК цілям і задачам функціонування, передбаченим специфікацією;
– продуктивність ЖКСК та її складових частин і елементів;
– функціональна готовність та якість прикладних програм;
– інерційність ЖКСК (терміни реагування ЖКСК на сигнали управління);
– якість і своєчасність обслуговування користувачів;
– рівень раціональності використання ІТ-ресурсів.

3. Формалізація основних показників гарантоздатності ЖКСК для розрахунку, проектної оцінки і прогнозування

Формалізацію основних показників гарантоздатності ЖКСК проведено на основі відомої двохпараметричної ймовірнісно-фізичної моделі відмов – дифузійного розподілу (DN-розподілу) [1, 6] з використанням формульних виразів, наведених в ДСТУ [7–10].

3.1. Показники безвідмовності

Для опису безвідмовності системи введемо такі позначення:

s – кількість резервів, спочатку доступних для підключення;

q – кількість модулів одного типу, що працюють паралельно (характеристика актуальна для систем, продуктивність яких залежить від кількості одночасно працюючих ресурсів);

c – ступінь компенсації наслідків відмови (умовна ймовірність того, що при виникненні відмови у працюючій системі остання здатна відновити інформацію і продовжити її обробку без довготривалої втрати даних);

f – здатність модуля допускати f одиночних відмов до того, як він стане непрацездатним.

Основною характеристикою безвідмовності системи будемо вважати ймовірність безвідмовної роботи за час t $(R(t))$. Для зручності аналізу та систематизації значень кожну функцію безвідмовності будемо записувати у формі базової моделі ${}_c^f R_s^q$ [11]:

$$ {}_{c}^{f}R_{s}^{q} = c^{s}(1-{}^{f}F_{s}^{q}), \tag{3.1} $$

де ${}^{f}F_{s}^{q}$ – функція ймовірності відмови.

Приймаючи гіпотезу про DN-розподілення напрацювання до відмови елементів, модулів і системи в цілому, ймовірність відмови будемо вираховувати таким чином:

$$ {}^{f}F_{s}^{q} = DN(x; v, f, q, s), \tag{3.2} $$

де v – коефіцієнт варіації напрацювання до відмови;

x – відносне напрацювання ($x = \frac{t}{T}$, t – час роботи, T – середнє напрацювання до відмови (на відмову).

Функція ймовірності відмови для DN-розподілу має такий вигляд [1]:

$$ DN(x; v) = \Phi\left(\frac{x-1}{v\sqrt{x}}\right) + \exp\left(2v^{-2}\right)\Phi\left(-\frac{x+1}{v\sqrt{x}}\right), \tag{3.3} $$

де $\Phi(*)$ – функція нормованого нормального розподілу.

Якщо будь-який із параметрів базової моделі ${}_{c}^{f}R_{s}^{q}$ (3.1) не враховується, то припускається, що $q=1$, $c=1$, $f=0$, $s=0$. Параметри s, c і f є такі, що зростання їх призводить до підвищення загальної безвідмовності системи.

Крім того, для характеристики безвідмовності ЖКСК можливо використання традиційних показників [1], таких як:

• Параметр потоку відмов на довільний момент часу, $\omega(t)$:

$$ \omega(t) = \frac{d\Omega(t)}{dt} = \sum_{m=1}^{M} \frac{m\sqrt{T_1}}{\nu_1 t\sqrt{2\pi t}} \exp\left[-\frac{(t-mT_1)^2}{2\nu_1{}^2 tT_1}\right], \tag{3.4} $$

де t – довільний момент часу;

$\Omega(t)$ – математичне очікування числа відмов (функція відновлення) об’єкта на момент сумарного наробітку t;

ν_1 – коефіцієнт варіації наробітку (параметр форми розподілу наробітку) до першої відмови (між відмовами).

m – порядковий номер урахованого члена згортки розподілу $f^{m}(t)$;

M – число врахованих членів згортки розподілу $f^{m}(t)$ (при інженерних розрахунках приймають $3 \le M \le 5$);

T_1 – середній наробіток об’єкта до першої відмови.

Примітка:

1. Для електронних елементів коефіцієнт ν приймається рівним 0,75.
2. Параметр ν визначається залежно від структурної схеми надійності (ССН) об’єкта.

• Функція відновлення (математичне очікування числа відмов системи на наробітку t), $\Omega(t)$:

$$ \Omega(t) = \sum_{m=1}^{M}\left\{\Phi\left(\frac{t-mT_1}{\nu_1\sqrt{tT_1}}\right) + e^{2m\nu_1^{-2}}\Phi\left(-\frac{t+mT_1}{\nu_1\sqrt{tT_1}}\right)\right\}. \tag{3.5} $$

• Середній наробіток на відмову, $T_0(t)$, години:

$$T_0(t)=\frac{1}{\omega(t)} \quad \text{або} \quad T_0(t)=\frac{t_2-t_1}{[\Omega(t_2)-\Omega(t_1)]}=\frac{\Delta t}{[\Omega(t+\Delta t/2)-\Omega(t-\Delta t/2)]}, \tag{3.6}$$

де $t_1=t-\frac{\Delta(t)}{2}$, $t_2=t+\frac{\Delta(t)}{2}$, $\Delta t=t_2-t_1$;

$\Omega(t_i)$ – математичне очікування числа відмов (функція відновлення) системи на момент сумарного наробітку t_i.

Розрахунок показників безвідмовності систем ВФ (ймовірнісно-фізичним) – методом для різних ССН детально розглянутий в [1, 9].

3.2. Показники живучості

Систематизація показників живучості та їх класифікація здійснюються за ознаками ймовірності і детермінованості [12]. Пропонуються формалізовані визначення для кількісної оцінки таких показників живучості:

• Коефіцієнт живучості (відношення числа станів, відповідних працездатній системі, до усієї сукупності станів) [13], $G(q^i)$:

$$G(q^i)=M/C_l^i, \tag{3.7}$$

де M – кількість працездатних станів системи для узагальненої відмови i-тої кратності;

C_l^i – загальна кількість станів системи;

i – кратність узагальненої відмови;

l – кількість функціональних одиниць живучості системи.

• Коефіцієнт деградації (відношення числа станів N, відповідних непрацездатній системі, до загальної кількості станів системи C_l^i [13], $D(q^i)$:

$$D(q^i)=N/C_l^i. \tag{3.8}$$

Очевидно, що $G(q^i)+D(q^i)=1$.

• Умовний закон уразливості (ймовірність втрати працездатності при n-кратному несприятливому впливі (НВ)) [12], $Q(n)$:

$$Q(n)=P\left(F=0/A_n\right), \tag{3.9}$$

де F – функція працездатності системи, що приймає значення 1, якщо система працездатна, і 0, якщо система непрацездатна;

A_n – подія, яка відбувається при n-кратній появі НВ.

• Виживаність системи (ймовірність збереження працездатності при n-кратному НВ) [12], $R(n)$:

$$R(n)=1-Q(n)=P(F=1/A_n). \tag{3.10}$$

• Запас живучості (критичне число дефектів зменшене на одиницю) [12], d

$$d=C-1, \tag{3.11}$$

де C – критичне число дефектів, яке обумовлює втрату працездатності системи.

Примітка. Дефект – це одиниця виміру збитків, нанесених системі несприятливими впливами. Це може бути один елемент, який видаляється із системи в результаті НВ, визначена номінальна потужність у системі енергетики, яка втрачена для користувачів у результаті НВ, та ін.

• Середня кількість НВ, яка обумовлює втрату працездатності системи (математичне очікування кількості НВ, яке задається розподілом (3.10) [12], ϖ:

$$\varpi = \sum_{n=0}^{\infty} R(n). \tag{3.12}$$

3.3. Показники готовності

Для оцінки готовності системи доцільно використовувати такі показники:

• Коефіцієнт готовності об'єкта, $K_{\Gamma}(t)$:

$$K_{\Gamma}(t) = \frac{T_0(t)}{[T_0(t) + T_p + T_B]}, \tag{3.13}$$

де T_0 – середній наробіток на відмову, години;

T_p – середня тривалість виходу об'єкта на робочий режим, години;

T_B – середня тривалість відновлення об'єкта, години.

• Коефіцієнт оперативної готовності об'єкта, $K_{O\Gamma}(t)$:

$$K_{O\Gamma}(t) = K_{\Gamma}(t) P(\tau), \tag{3.14}$$

де $P(\tau)$ – ймовірність безвідмовної роботи об'єкта в інтервалі $(t,\ t+\tau)$, коли t збігається з моментом початку функціонування після чергової відмови (відновлення).

3.4. Показники функціональної безпеки

Функціональна безпека ЖКСК – це відсутність катастрофічних наслідків для користувачів і навколишнього середовища або функціональна відповідність ЖКСК вимогам специфікації, при яких відсутні небезпечні відмови і недопустимі збитки, пов'язані із завданням шкоди життю та здоров'ю людини, державному майну та навколишньому середовищу [4]. Ступінь функціональної безпеки конкретної ЖКСК найбільш повно характеризується величиною попередження шкоди (ризику), можливої при проявленні дестабілізуючих факторів і реалізації конкретних загроз безпеки.

Неправильне функціонування ЖКСК може призвести до людських жертв, екологічних катастроф, а також до великих фінансових втрат. Повністю виключити ситуації, що призводять до таких наслідків, неможливо. Мова може йти тільки про ймовірність виникнення таких ситуацій і допустимий при цьому рівень ризику.

Ризик в області безпеки часто визначають як добуток ймовірності виникнення небезпечної ситуації на тяжкість (вартість) наслідків. Допустимий рівень ризику оцінюється в кожному конкретному випадку індивідуально. З визначення ризику визначаються шляхи його зниження: зменшення ймовірності появи небезпечної ситуації і обмеження тяжкості її наслідків.

Підвищення рівня функціональної безпеки здійснюється шляхом аналізу виявлених у процесі функціонування ЖКСК дефектів і оперативного відновлення працездатності системи. Цьому сприяє накопичення, моніторинг і збереження даних про виявлені дефекти, збої та відмови апаратних і програмних засобів у процесі експлуатації на протязі усього життєвого циклу ЖКСК.

Функціональній безпеці програмованих електронних систем присвячені міжнародний стандарт IEC 61508, а також серія пов'язаних з ним стандартів [14–18].

Стандартом [16] пропонується виділяти чотири дискретні рівні безпеки складних динамічних систем, які називаються рівнями повної безпеки (РПБ):

– РПБ4 – найвищий і найбільш важко досяжний рівень повноти безпеки, який потребує використання надзвичайно високих прийомів і технологій і якого доцільно, по можливості, уникати при формалізації вимог до ЖКСК;

– РПБ3 – легше досяжний, ніж рівень РПБ4, але він також потребує високих технологій розробки системи і програмних засобів;

– РПБ2 – потребує якісного сучасного проектування, розробки і практики використання програмних засобів на рівні не нижче вимог стандарту ISO 9001;

– РПБ1 – найнижчий рівень, який також потребує використання сучасних технологій і суттєвого досвіду розробок.

Ці рівні вибираються в залежності від тяжкості наслідків, які можуть наступити при неправильному функціонуванні системи. Рівні РПБ визначають величину допустимого ризику для системи. Вони є мірою ймовірності того, що система буде правильно виконувати свої функції, що впливають на безпеку. Чим вищий РПБ системи, тим менша ймовірність її відмови під час виконання функцій безпеки.

Стандарт МЕК 61508 встановлює два способи розрахунку рівня ризику. Оскільки ризик визначається як добуток імовірності виникнення небезпечної ситуації на тяжкість (вартість) наслідків, першою стадією в оцінці ризику є визначення ймовірності виникнення небезпеки. Кількісний метод розрахунку ймовірності заснований на аналізі частоти відмов системи.

4. Висновки

1. Розглянуто загальний підхід до формалізації, визначення, оцінки і прогнозування деяких основних показників гарантоздатності живучих комп'ютерних систем керування.
2. Наведені методи оцінки основних показників безвідмовності, готовності і живучості базуються на ймовірнісно-фізичному підході до надійності систем.
3. Запропоновані методи оцінки деяких основних показників гарантоздатності можуть бути застосовані при аналізі, проектній оцінці і прогнозуванні характеристик живучих комп'ютерних систем керування.
4. Оцінка цих показників повинна виконуватись на всіх етапах проектування і підконтрольної експлуатації ЖКСК.

СПИСОК ЛІТЕРАТУРИ

1. Стрельников В.П. Оценка и прогнозирование надежности электронных элементов и систем / В.П. Стрельников, А.В. Федухин. – Киев: Логос, 2002. – 488 с.
2. Avizenis A. Dependable Computing: From concepts to design diversity / A. Avizenis, J.-K. Laprie // Proc. of the IEEE. – 1986. – Vol. 76, N 5. – P. 629 – 638; Авиженис А. Гарантоспособные вычисления: От идей до реализации в проектах / А. Авиженис, Ж.-К. Лапри; пер. с англ. // ТИИЭР. – 1987. – Т. 74, № 5. – С. 8 – 21.
3. Laprie J.-K. Dependable computing and fault–tolerance: concepts and terminology / J.-K. Laprie // Proc. 15th IEEE Int. Symp. on Fault-Tolerance Computing (FTCS), Ann Arbor. – Michigan, 1985. – June 1985. – P. 2 – 11.
4. Звіт про науково-дослідну роботу "Розробка теоретичних засад створення та дослідження високоефективних гарантоздатних комп'ютерних систем". – шифр "Гарантоздатність" / Б.Г. Мудла, В.Г. Сербін, А.І. Сухомлин [та ін.]. – Держреєстраційний №0105U000532. – Київ: ІПММС НАНУ, 2009. – 366 с.
5. Сербін В.Г. Деякі аспекти живучості складних гарантоздатних комп'ютерних систем критичних умов застосування / В.Г. Сербін, А.І. Сухомлин // Математичні машини і системи. – 2011. – № 4. – С. 183 – 191.
6. Азарсков В.Н. Надежность систем управления и автоматики: уч. пособ. / В.Н. Азарсков, В.П. Стрельников. – Киев: НАУ, 2004. – 164 с.

7. ДСТУ 2860-94. Надійність техніки. Терміни та визначення. – Київ: Держстандарт України, 1994. – 92 с. – (Державний стандарт України).
8. ДСТУ 2861 – 94. Надійність техніки: Аналіз надійності. Основні положення. – Київ: Держстандарт України, 1994. – 32 с. – (Державний стандарт України).
9. ДСТУ 2862-94. Надійність техніки. Методи розрахунку показників надійності. Загальні вимоги. – Київ: Держстандарт України, 1994. – 40 с. – (Державний стандарт України).
10. ДСТУ 3524-97 (ГОСТ 27.205-97). Надійність техніки. Проектна оцінка надійності складних систем з урахуванням технічного і програмного забезпечення та оперативного персоналу. Основні положення. – Київ: Держстандарт України, 1997. – 21 с. – (Державний стандарт України).
11. Федухин А.В. К вопросу о количественных характеристиках безотказности избыточных компьютерных систем / А.В. Федухин, В.П. Пасько // Математичні машини і системи. – 2012. – № 1. – С. 145 – 156.
12. Черкесов Г.Н. Методы и модели оценки живучести сложных систем / Черкесов Г.Н. – М.: Знание, 1987. – 32 с.
13. Березюк Н.Т. Живучесть микропроцессорных систем управления / Березюк Н.Т., Гапунин А.Я., Подлесный Н.И. – К.: Техника, 1989. – 143 с.
14. ГОСТ Р МЭК 61508-1-2007. Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 1. Общие требования. – Москва: Стандартинформ, 2008. – 45 с.
15. ГОСТ Р МЭК 61508-4-2007. Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 4. Термины и определения. – Москва: Стандартинформ, 2008. – 22 с.
16. ГОСТ Р МЭК 61508-5-2007. Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 5. Рекомендации по применению методов определения уровней полноты безопасности. – Москва: Стандартинформ, 2008. – 23 с.
17. ДСТУ ISO/IEC TR 13335-1:2003. Інформаційні технології. Настанови з керування безпекою інформаційних технологій (ІТ). Частина 1. Концепції та моделі безпеки ІТ. – Київ: Держстандарт України, 2003. – 17 с.
18. ДСТУ ISO/IEC TR 13335-2:2003. Інформаційні технології. Настанови з керування безпекою інформаційних технологій (ІТ). Частина 2. Керування та планування безпеки ІТ. – Київ: Держстандарт України, 2003. – 16 с.

Стаття надійшла до редакції 11.07.2012