УДК 621.396.66

Л.Д. Озірковський, Т.І. Панський
Національний університет "Львівська політехніка",
кафедра теоретичної радіоелектроніки та радіовимірювання

МОДЕЛЬ ПОВЕДІНКИ ПРОГРАМНО-АПАРАТНИХ ЕЛЕКТРОННИХ СИСТЕМ

L.D. Ozirkovskyi, T.I. Panskyi

THE BEHAVIORAL MODEL OF HARDWARE-SOFTWARE ELECTRONIC SYSTEMS

Запропоновано модель для оцінювання надійності програмно-апаратних електронних систем на етапі експлуатації. Вона враховує поведінку електронних систем у разі появи відмов і збоїв апаратних засобів та збоїв програмного забезпечення.

Ключові слова: надійність, програмне забезпечення, апаратне забезпечення, програмно-апаратні системи.

In this paper a model for assessing the reliability of hardware-software electronic systems during their operation cycle is proposed. It takes into account the behaviour of electronic systems at the appearance of hardware faults and failures as well as software failures.

Key words: reliability, hardware-software system, hardware, software, fault tolerant systems.

Вступ

На етапі системотехнічного проектування електронних програмно-апаратних систем (ПАС) важливим завданням є оцінювання їх надійності на етапі експлуатації. Це необхідно як для правильного вибору варіанта реалізації структури системи, елементної бази, способів резервування, так і для визначення архітектури та способів реалізації програмного забезпечення, оскільки надійність ПАС визначається як надійністю апаратних засобів (АЗ), так і надійністю програмних засобів (ПЗ). Причому показники надійності АЗ і ПЗ пов'язані між собою, бо вихід з ладу АЗ призводить до виходу з ладу ПАС, загалом, а збої в АЗ призводять до збоїв ПЗ, що, своєю чергою, може призвести до тривалої зупинки (простою) АЗ, що часто еквівалентно відмові ПАС [1].

Завдання оцінювання надійності ПАС, сьогодні, виконують або шляхом натурних випробувань експериментальних зразків, що потребує значних часових і матеріальних затрат, або моделюванням. Якщо на етапі системотехнічного проектування є декілька конкурентних варіантів ПАС з різною структурою АЗ та архітектурою ПЗ, то перший шлях є неефективним, з погляду часових і, особливо, матеріальних затрат. Під час оцінювання показників надійності ПАС шляхом моделювання спочатку здійснюють декомпозицію системи і оцінюють окремо показники надійності АЗ і ПЗ, а потім об'єднують ці показники у комплексний показник надійності ПАС, нехтуючи взаємними впливами АЗ і ПЗ.

Для оцінювання показників надійності АЗ існують адекватні моделі та ефективні методики [2, 3]. Методи оцінювання надійності ПЗ дозволяють лише прогнозувати його надійність на основі експериментів та тестів у період розроблення та тестування [4, 5, 6], проте автори не виявили моделі для практичного оцінювання надійності ПЗ у період експлуатації.

Сучасні підходи до аналізу надійності програмно-апаратних систем

Під час оцінювання надійності ПАС у деяких підходах [3, 7] вважають надійність ПЗ такою, що дорівнює одиниці і розглядають тільки надійність АЗ, що завищує показники надійності. В інших підходах вважається, що надійність ПАС (1) залежить як від надійності ПЗ, так і від надійності АЗ [2, 5], що у вигляді структурної схеми надійності наведено на рис. 1.

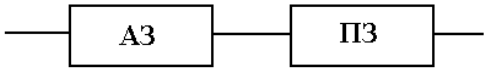

Рис. 1. Структурна схема надійності ПАС

$$P_{HSS}(t) = P_{HW}(t) \cdot P_{SW}(t), \quad (1)$$

де $P_{HSS}(t)$ – ймовірність безвідмовної роботи ПАС, $P_{HW}(t)$ – ймовірність безвідмовної роботи АЗ, $P_{SW}(t)$ – ймовірність правильного виконання ПЗ.

У цьому випадку вважають, що моделі надійності АЗ і ПЗ є аналітичними. Для надійнісної характеристики АЗ використовують або миттєву інтенсивність відмов $\lambda_{HW}(t)$, або ймовірність безвідмовної роботи $P_{HW}(t)$, від моменту запуску АЗ до першої відмови [2,3]:

$$P_{HW}(t) = e^{-l_{HW} \cdot t}. \quad (2)$$

Як надійнісну характеристику ПЗ на етапі експлуатації використовують або миттєву інтенсивність відмов $\lambda_{SW}(t)$, або ймовірність правильного виконання відповідних функцій програмного забезпечення $P_{SW}(t)$, від моменту запуску ПЗ до першого збою і для оцінювання надійності ПЗ використовують аналогічну, як у випадку АЗ, модель [7]:

$$P_{SW}(t) = e^{-l_{SW} \cdot t}. \quad (3)$$

Тобто, у якості моделі надійності ПЗ використовують експоненційні моделі, аналогічні для АЗ, механічно переносячи властивості АЗ на ПЗ. Однак механічне перенесення моделі АЗ для визначення надійності ПЗ є некоректним, оскільки особливості АЗ і ПЗ на етапі експлуатації ПАС істотно відрізняються (див. табл. 1).

Таблиця 1

Особливості апаратного та програмного забезпечення на етапі експлуатації

Програмне забезпечення	Апаратне забезпечення
Не старіє протягом часу експлуатації	Старіє протягом часу експлуатації
Несправності виявлені на етапах (тестування, верифікації, атестації) усуваються шляхом поновлень	Несправності усуваються до початку виробництва, або за рахунок ремонту
Надійність є незмінною (якщо не здійснюється поновлення, чи випуск нової версії), або зростає (при поновленні версії ПЗ)	Надійність зменшується з часом
При усуненні одних помилок можуть бути введені інші	При відновленні (ремонті) інші несправності не вводяться

Істотним недоліком оглянутих підходів оцінювання надійності електронних ПАС [2-7] є те, що в них використовують експоненційні моделі надійності ПЗ, які є адекватними тільки для етапів розроблення і тестування ПЗ і не враховують особливості етапу експлуатації. Тому оцінювання надійності ПАС за допомогою таких моделей є неточним, оскільки на етапі експлуатації надійність ПЗ є незмінною величиною і змінюється стрибкоподібно (здебільшого зростає) при оновленні ПЗ чи переході на іншу версію. Отже, для оцінки надійності ПАС на етапі експлуатації необхідно розробити адекватну модель, яка враховує, на відміну від (3), всі особливості ПЗ, перераховані в табл. 2.

Крім цього, оцінювання надійності ПАС згідно з (1) передбачає, що система є працездатною, коли АЗ перебувають в працездатному стані і ПЗ правильно виконується, а це справедливо лише для окремих різновидів нерезервованих ПАС. Сучасні ПАС реалізуються як відмовостійкі системи [2,7] і вихід з ладу окремих елементів АЗ не призводить до виходу з ладу ПАС загалом. Те саме стосується і ПЗ [2, 4–6]. Отже, точність оцінювання надійності відмовостійких ПАС з використанням (1) є невисокою, а з врахуванням (3) взагалі робить непридатною цю модель для практичного застосування на етапі системотехнічного проектування.

Для високої точності оцінювання надійності відмовостійких електронних ПАС, у практиці системотехнічного проектування, використовують марковські моделі [2, 3, 7, 8], які адекватно описують поведінку АЗ відмовостійких ПАС у разі появи відмов та збоїв. Такі моделі дають змогу розрізнити стани непрацездатності, в які може перейти ПАС у результаті апаратних відмов та стани непрацездатності, в які ПАС потрапляє у результаті неправильного виконання (збоїв) ПЗ. Однак побудова таких моделей є трудомісткою задачею, яка потребує значних затрат часу [2, 3, 8].

Тому актуальною задачею є розробка моделі для оцінювання надійності ПАС, яка адекватно відображає її поведінку при різних видах порушення працездатності та враховує особливості надійності ПЗ (згідно з табл.1.) на етапі експлуатації. Разом з цим модель повинна враховувати взаємні впливи АЗ і ПЗ з погляду надійності, що дозволить точніше здійснювати розрахунок показників надійності ПАС. Розроблення такої моделі потребує розв'язання задач, а саме: розроблення моделі ПЗ, яка враховує всі особливості етапу експлуатації; розроблення марковської моделі поведінки ПАС у вигляді графу станів та переходів та системи диференціальних рівнянь Колмогорова–Чепмена; визначення ймовірності перебування у тих станах, які залежать від надійності ПЗ; визначення показників надійності ПАС на основі моделі поведінки та розробленої моделі надійності ПЗ.

Розроблення надійнісної моделі програмного забезпечення на етапі експлуатації

Процес створення та використання ПЗ від початкової ідеї до остаточного морального старіння називається життєвим циклом програмного забезпечення, який складається з шести етапів [9]. Для перших п'яти етапів життєвого циклу, за винятком етапу експлуатації, існують моделі для визначення надійності ПЗ [4–6], які наведено на рис. 2. Однак ці моделі стосуються процесу розроблення ПЗ і є непридатними для етапу експлуатації ПЗ, що не дає змоги визначити показники надійності ПАС на етапі системотехнічного проектування.

Для оцінки надійності ПЗ на етапі експлуатації пропонуємо використовувати показник надійності ПЗ – ймовірність правильного виконання $P_{SW}(t)$, яку можна представити у вигляді кусково-лінійної ступінчатої функції. Вибір такої функції ґрунтується на тому, що на етапі тестування виявляються і усуваються дефекти ПЗ, що підвищує його надійність, а після виходу кінцевої версії програми і встановлення її в ПАС надійність ПЗ не змінюється.

У момент часу t_1 (момент виходу кінцевої версії ПЗ – початок етапу експлуатації) ймовірність правильного виконання ПЗ має певне стале значення P_1. Це значення є основним параметром ПЗ, яке отримується (розраховується) на основі експериментальних даних після завершення етапу тестування та верифікації. Стрибкоподібне зростання надійності ПЗ ($P_2 > P_1$) зумовлене виходом оновлення для ПЗ, в результаті чого зменшується кількість ситуацій, коли ПЗ не функціонує належно (збої, зависання тощо) і, відповідно, підвищується ймовірність правильного виконання до значення P_2. Якщо ж оновлення є невдалим, то надійність ПЗ стрибкоподібно зменшується ($P_2 < P_1$).

Частота оновлень на початковому етапі експлуатації ПЗ є вищою (оновлення 1, оновлення 2), згодом зменшується (оновлення 3) і після деякого часу оновлення припиняється взагалі у зв'язку з випуском нової версії, переходу на інше АЗ тощо. Для визначення значень $P_1 ... P_n$ необхідно мати вхідні дані від розробника ПЗ (кількість виявлених та виправлених помилок ПЗ на етапі тестування, кількість циклів тестування, тривалість тестування тощо). На основі цих даних можна визначити початкові ймовірності правильного виконання P_i на етапі експлуатації, застосувавши моделі збільшення надійності. Ці моделі (Гоель–Окумото, Гомперца, Парето, Вейбула, Ямада експоненційна, Ямада–Релея) дають змогу оцінити початкову надійність P_i програмного продукту наприкінці етапу тестування [10, 11].

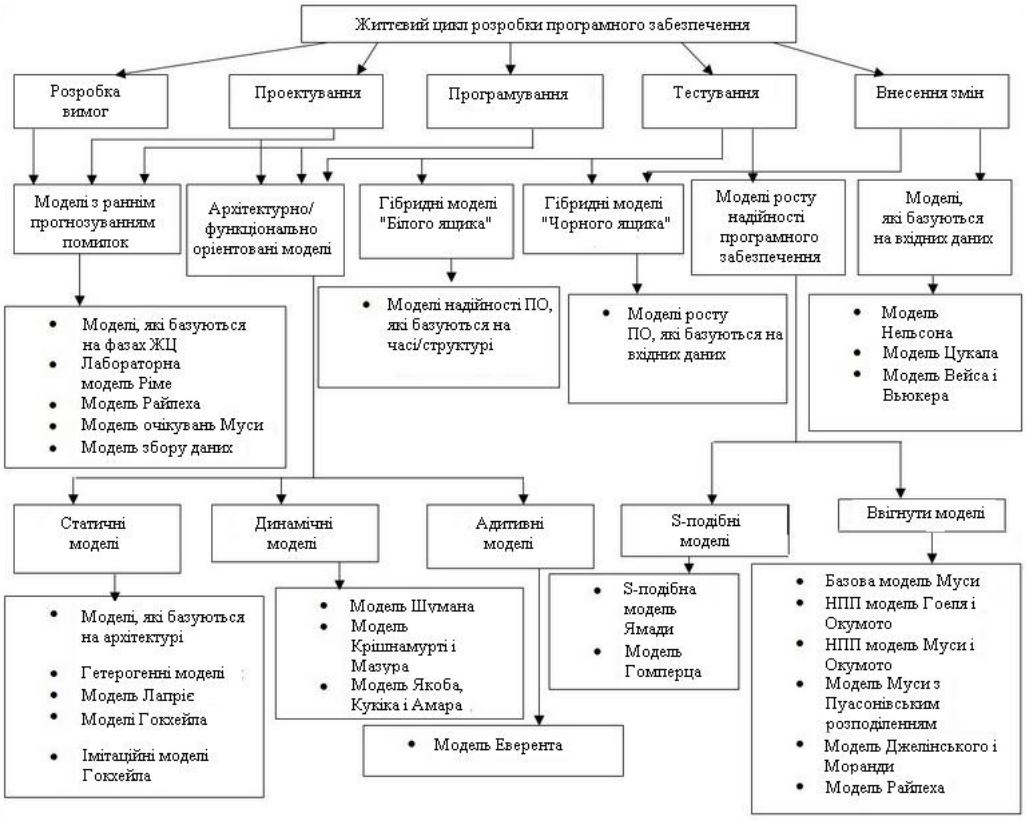

Рис. 2. Класифікація моделей надійності програмного забезпечення на етапах життєвого циклу

У роботі для визначення початкової надійності ПЗ застосовано стандартну модель Гомперца [10,11], яка набула широкого застосування для оцінки надійності у провідних виробників ПЗ, зокрема Reliasoft [12]. Стандартна модель Гомперца має вигляд

$$R(t) = a \times b^{c^T},$$

де $0 < a < 1$; $0 < b < 1$; $0 < c < 1$, T – час тестування ПЗ, $R(t)$ – надійність ПЗ на етапі тестування, $a \cdot b$ – початкова надійність ПЗ, коли $T = 0$, c – показник зростання моделі (мале значення показника c, показує раннє швидке зростання надійності ПЗ, велике значення показника c – повільне зростання надійності ПЗ).

Схему отримання початкових значень P_i на основі стандартної моделі Гомперца [10–12] показано на рис. 3. Момент t_1 – час виходу першої версії ПЗ; t_2 , t_3 – моменти виходу оновлення 1 та 2. Між виходом оновлень надійність ПЗ на етапі

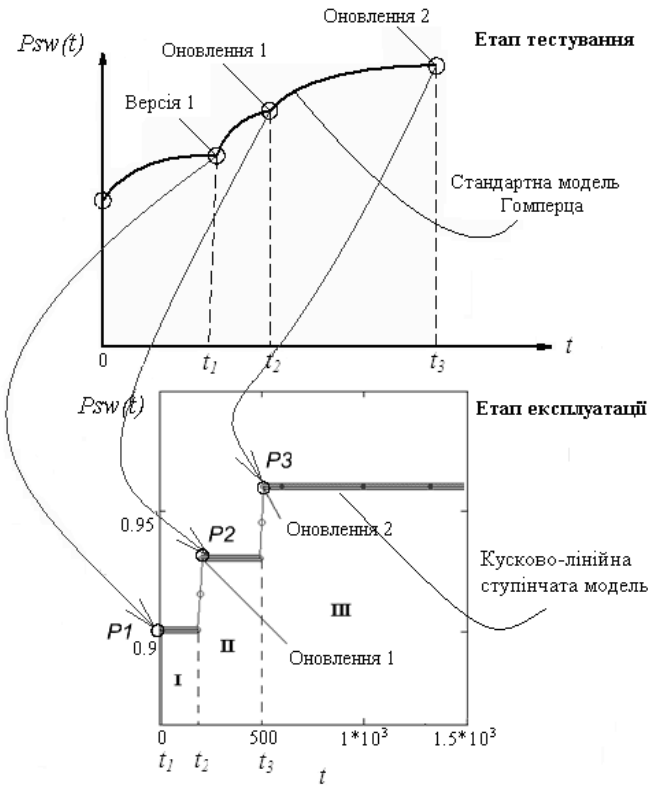

Рис. 3. Схема отримання початкових значень P_i на основі стандартної моделі Гомперца

тестування зростає за рахунок виправлення помилок, а на етапі експлуатації надійність ПЗ до моменту оновлення є незмінною.

Аналітично запропонована модель надійності ПЗ на етапі експлуатації має вигляд сукупності функцій Хевісайда.

$$P_{SW}(t) = P_1 \cdot H(t) + P_2 \cdot H(t - T_1) + ... + P_n \cdot H(t - T_{n-1}), \quad (4)$$

де $H(t)$ – функція Хевісайда; P_1 – початкове значення ймовірності правильного виконання на момент закінчення етапу тестування і виходу першої версії ПЗ; P_2 – значення ймовірності правильного виконання після виходу (закінчення етапу тестування) першого оновлення (оновлення 1); P_3 – значення ймовірності правильного виконання після другого оновлення (оновлення 2); P_n – значення ймовірності правильного виконання після $(n-1)$-го оновлення.

Розробка надійнісної моделі апаратного забезпечення

Для оцінювання надійності АЗ доцільно побудувати марковську модель, яка дасть змогу врахувати поведінку ПАС у разі появи відмов та збоїв. Побудова марковської моделі, при детальному врахуванні нюансів поведінки ПАС, вимагає значних затрат часу на розроблення графу станів і переходів, тому в роботі застосовано автоматизовану технологію побудови [8], яка передбачає побудову структурно-автоматної моделі (САМ). Структурно-автоматна модель є формалізованим описом структури і поведінки ПАС в умовах дії відмов і збоїв. Побудова САМ здійснюється на основі вербальної моделі [8], яка задає вхідні дані об'єкта дослідження (ПАС) у вигляді переліку базових подій, умов і обставин, за яких ці події відбуваються. При розробці САМ необхідно виконати такі завдання: сформувати вектор станів; визначити множину формальних параметрів моделі; описати поведінку системи у вигляді базових подій, які відбуваються у системі, а також умов і обставин, за яких відбуваються ці події; сформувати формули розрахунку інтенсивностей переходів між станами; сформувати формули розрахунку ймовірностей альтернативних переходів; встановити правила модифікації компонент вектора станів. Наступним кроком є використання програмного забезпечення ASNA [13], розробленого на кафедрі теоретичної радіотехніки та радіовимірювань Національного університету «Львівська політехніка». Це програмне забезпечення використовує САМ як вхідні дані і на їх основі автоматизовано формує модель поведінки ПАС у вигляді графу станів і переходів. На основі графу станів і переходів програмне забезпечення ASNA складає систему диференційних рівнянь Колмогорова-Чепмена (марковська модель) та розв'язує. На основі отриманого розподілу ймовірностей перебування у станах можна сформувати показники надійності досліджуваної ПАС, а саме: залежності імовірності безвідмовної роботи від часу та середнього часу напрацювання системи до відмови.

Модель поведінки програмно-апаратних електронних систем для оцінювання їх надійності

Модель поведінки ПАС будується на основі марковської моделі АЗ, з якої визначаються стани, пов'язані з надійністю ПЗ, і стани, які від надійності ПЗ не залежать. З першої групи станів отримують ймовірність $P_{HW1}(t)$, а з другої – $P_{HW2}(t)$. Ймовірність безвідмовної роботи ПАС на основі моделі поведінки визначається згідно з (5), причому $P_{SW}(t)$ визначається згідно з (4). Слід зазначити, що сума ймовірностей $P_{HW1}(t)$ і $P_{HW2}(t)$ дорівнює одиниці.

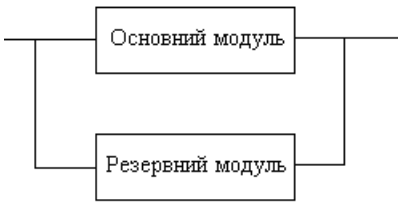

Рис. 4. Структурна схема надійності програмно-апаратної системи

$$P_{HSS}(t) = P_{HW1}(t) \cdot P_{SW} + P_{HW2}(t). \quad (5)$$

Отримання показників надійності на основі моделі (5), моделі (1) та за умови, що $P_{SW}(t) = 1$ проілюстровано на прикладі відмовостійкої ПАС, яка складається з одного основного та одного резервного модуля. Система працює без відновлень. Структурна схема надійності ПАС наведена на рис. 4.

Для цієї ПАС побудовано САМ, яка складається з трьох множин даних: вектора станів, який визначає зміст станів і призначений для їх кодування; множини формальних параметрів, яка описує структуру ПАС і параметри її складових; дерева правил та модифікацій, яке формалізовано описує поведінку ПАС у разі появи відмов і збоїв.

Ввівши САМ у програмний модуль ASNA, автоматизовано отримують граф станів та переходів ПАС. Специфікація отриманих станів ПАС наведена у табл. 2.

Таблиця 2

Специфікація станів

№ стану	Опис стану
1	Всі модулі справні
2	Відмова основного або резервного модуля
3	Збій апаратних засобів
4	Відмова одного з модулів і збій апаратних засобів
5	Збій програмних засобів
6	Відмова одного з модулів і збій програмних засобів
7	Стан зупинки
8	Стан зупинки, відмова резервного модуля
9	Стан катастрофічної відмови

Граф станів і переходів, який відображає поведінку ПАС, зображено на рис. 5.

Отримана модель поведінки дає змогу визначити залежність надійності електронних ПАС не тільки від відмов та збоїв, пов'язаних з апаратною частиною (стани: 2, 3, 4, 8, 9) – $P_{HW2}(t)$, але й від збоїв на програмному рівні (стани: 5, 6, 7) – $P_{HW1}(t)$. Визначальним є те, що збої ПЗ спричиняються збоями АЗ, а не виникають самостійно. Стани 7 та 8 є станами простою – система не працює (простоює), але катастрофічна відмова ще не настала. Стани 1–6 є працездатними станами. Стан 9 – стан катастрофічної відмови, яка настає у разі виходу з ладу обох модулів. Отримана модель буде типовою для резервованих ПАС без відновлення.

На основі графу станів і переходів за допомогою програмного забезпечення ASNA сформовано аналітичну модель ПАС у вигляді системи диференційних рівнянь Колмогорова–Чепмена, здійснено її розв'язок і сформовано розподіл ймовірностей перебування ПАС в усіх станах.

Показники надійності ПАС, отримані в результаті моделювання, наведено на рис. 7.

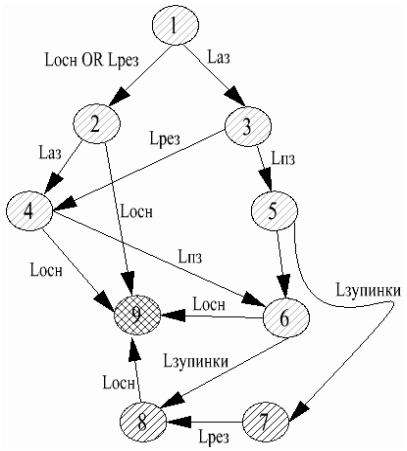

Рис. 5. Граф станів і переходів програмно-апаратної системи

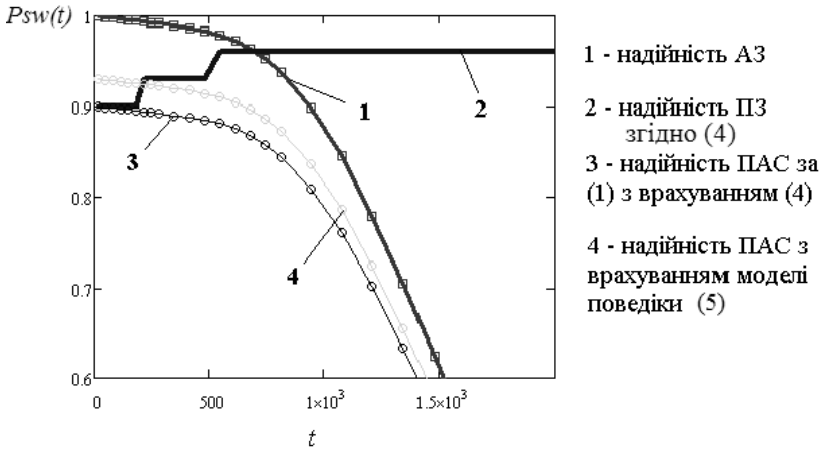

Рис. 7. Показники надійності програмно-апаратної системи, отриманої на основі різних моделей

Крива 1 – ймовірність безвідмовної роботи ПАС за умови, що ПЗ абсолютно надійне ($P_{SW}(t) = 1$) і отримується як сума ймовірностей перебування у станах 1-8. У такому разі цей показник збігається з ймовірністю безвідмовної роботи АЗ. Крива 2 – ймовірність правильного виконання ПЗ з врахуванням двох оновлень на етапі експлуатації, отримана згідно з (4). Крива 3 – ймовірність безвідмовної роботи ПАС, визначена згідно з (1) у випадку, якщо надійність АЗ визначається як сума ймовірностей перебування ПАС в усіх працездатних станах (1)–(8), а надійність ПЗ згідно з (4). Тобто у цьому випадку поведінка ПАС не враховується. Крива 4 – ймовірність безвідмовної роботи ПАС, отримана згідно з (5).

Висновки

Застосування моделі поведінки для оцінювання показників надійності на етапі системотехнічного проектування дає змогу адекватно оцінити взаємний вплив надійності ПЗ і АЗ на надійність ПАС, яка істотно залежить від надійності ПЗ на початкових етапах експлуатації, коли надійність ПЗ є найнижчою, а з деякого моменту часу, коли в результаті оновлення та модернізації надійність ПЗ зростає, визначальною є надійність АЗ. Неврахування надійності ПЗ призводить до збігу ймовірності безвідмовної роботи ПАС з ймовірністю безвідмовної роботи АЗ, що істотно завищує показники надійності ПАС.

Для оцінювання надійності ПАС необхідно адекватно враховувати особливості ПЗ на етапі експлуатації. Для цього можна застосувати розроблену модель (4). Ця модель використовує припущення, що надійність ПЗ зростає стрибкоподібно під час його оновлення. Це припущення ґрунтується на зменшенні кількості дефектів, виявлених на етапі тестування. Однак, навіть у разі використання (4) як моделі надійності ПЗ при застосуванні (1) показники надійності ПАС будуть заниженими, оскільки не враховується поведінка системи у разі появи відмов і збоїв.

Особливістю викладеного підходу є те, що він придатний для багатоваріантного аналізу надійності ПАС: для інших значень вхідних даних (інтенсивність відмов АЗ, ймовірність правильного виконання ПЗ, кількість резерву тощо) необхідно лише зробити зміни у множину формальних параметрів і повторно запустити модуль ASNA. При різних наборах вхідних даних зміниться початкове значення надійності ПЗ (P_1), нахил кривої надійності АЗ, однак характер залежностей показників надійності (рис. 7) залишиться незмінним.

1. *Altera Measurable Advantage [Електронний ресурс] – Режим доступу: \www/ URL: http://www.altera.com/search?output=xml_no_dtd&sort=date%3AD%3AL%3Ad1&client=www_frontend&proxystylesheet=www_frontend&ie=UTF-8&oe=UTF-8&site=www&q=reliability.*
2. *Иыуду К.А. Метематические модели отказоустойчивых вычеслительных систем / К.А. Иыуду, С.А. Кривощеков. – М.: Изд-во МАИ, 1989. – 144 с.*
3. *Половко А.М. Основы теории надежности/ А. М. Половко, С.В. Гуров. – СПб.: Изд-во БВХ-Петербург, 2006. – 702 с.*
4. *Pham H Software Reliability models for Critical Applications/ H. Pham, M. Pham. – Published December 1991 – 107 p. – EGG-2663.*
5. *Pham H. Handbook of Reliability Engineering/ H. Pham – London.: British Library Cataloguing in Publication Data. 2003. – 696 p.*
6. *Lyu M. R. Handbook of Software Reliability Engineering / M.R. Lyu. – USA.: Copyright by The McGraw-Hill Companies, 1996. – 851 p.*
7. *Черкесов Г.Н. Надежность апаратно-программных комплексов: Учебное пособие / Г. Черкесов. – СПб.: Питер, 2005. – 479 с.*
8. *Волочій Б.Ю. Технологія моделювання алгоритмів поведінки інформаційних систем / Б.Ю. Волочій. – Львів: Вид-во Нац. ун-ту "Львівська політехніка", 2004. – 220 с.*
9. *Инженерный вестник Дона [Електронний ресурс] – Режим доступу: \www/ URL: http://www.ivdon.ru/magazine/ archive/n4p2y2012/1319.*

10. *Марков А.С. Модели оценки и планирования испытаний программных средств по требованиям безопасности информации // Вестник МГТУ им. Н.Э. Баумана. Сер. «Приборостроение», 2011. Специальный выпуск «Технические средства и системы защиты информации». – С. 90-103.*
11. *Brian Hall.J. Methodology for Evaluating Reliability Growth Programs of Discrete Systems.: Dissertation submitted to the Faculty of the Graduate School of the University of Maryland: 25.04.2008. / J. Brian Hall; University of Maryland. – Maryland, 2008. – 276 p.*
12. *Reliasoft RGA [Електронний ресурс] – Режим доступу: \www/ URL: http://www.weibull.com/RelGrowthWeb/Gompertz_Standard_Model_Overview.htm.*
13. *Bohdan Volochiy, Leonid Ozirkovskyy, Phillip Klochko The software for the analysis of reliability of fault-tolerant radio-electronic systems // Uradzenia I systetemy radioelektroniczne UiSR'09, III Konferencja naukowa, Sochewka 23-25 wresnia, 2009, Polska.*