**УДК 004.942+004.519.876.5**

***О.Б. Одарущенко****, к.т.н., доцент*

*М.В. Кисла, магістр*

*Полтавський національний технічний університет*

*імені Юрія Кондратюка*

**МОДЕЛЬ ЗАБЕЗПЕЧЕННЯ ФУНКЦІОНАЛЬНОЇ БЕЗПЕКИ СИСТЕМИ НОРМАЛЬНОЇ ЕКСПЛУАТАЦІЇ НА ОСНОВІ ПЛАТФОРМ, ЯКІ САМОДІАГНОСТУЮТЬСЯ І ПРОГРАМУЮТЬСЯ**

У наш час існує багато важливих для нормального життя людини систем. За деякими з них потрібно постійно спостерігати і контролювати їхню роботу. Одним із різновидів таких систем є інформаційно-керуючі системи (ІКС). Відповідно до державного стандарту України 2941-94 «*Інформаційно-керуюча система* – це сукупність керованого об'єкта й автоматичних вимірювальних та керуючих пристроїв, у якій частину функцій виконує людина» [1].

*Нормальна експлуатація* – це експлуатація виробів, згідно з дійсною експлуатаційною документацією. Системи, що призначені для здійснення нормальної експлуатації, називаються системами нормальної експлуатації (СНЕ). Представлена система має архітектуру 2оо3. *Архітектура* – це ряд спеціальних проектних рішень, які дозволяють наділити систему набором якостей, що збільшують її надійність. Дана архітектура складається з трьох каналів, з'єднаних паралельно з мажоруванням вихідних сигналів так, що вихідний стан не змінюється, якщо результат, що видається одним з каналів, відрізняється від результату, що видається двома іншими каналами [2, с.165-166].

Система складається з трьох ідентичних шаф формування сигналів, які утворюють три незалежних канали захисту, що резервують один одного. *Система справна*, коли вона здатна виконувати покладені на неї функції і в повній мірі відповідає нормативно-технічній документації. *Система* залишається *працездатною*, коли вона здатна виконувати покладені на неї функції, але не повністю відповідає нормативно-технічній документації. Коли система не здатна виконувати покладені на неї функції і при цьому не відповідає нормативно-технічній документації, то вона є *непрацездатною* *системою*. СНЕ, якій відповідає архітектура 2оо3, представлена на рис. 1.



*Рис. 1. Структура СНЕ*

Для забезпечення нормального функціонування СНЕ використовують поняття «функціональна безпека». Відповідно до міжнародного стандарту МЕК 61508 «*Функціональна безпека (ФБ)* – це безпека, пов’язана з ненавмисно викликаними відмовами у виконанні окремих функцій системи» [3]. ФБ відноситься до систем, що відповідають за функції безпеки, вихід з ладу яких створює значні ризики для людей і навколишнього середовища.

Щоб домогтися ФБ, система у випадку аварії повинна привести обладнання в безпечний стан або забезпечити збереження такого стану. Зазвичай, аварії відбуваються через відмову фізичної чи програмної частини системи. *Відмова* – подія, яка полягає у втраті об'єктом здатності виконувати потрібну функцію, тобто в порушенні працездатного стану об'єкта. Відмови бувають виявлені та невиявлені. *Невиявлена відмова* – це відмова системи (елементу), яка не виявляється в момент свого виникнення за нормальної експлуатації і не виявляється передбаченими засобами контролю відповідно до регламенту техобслуговування і перевірок [4, с.46-48].

Відповідно до структури СНЕ було побудоване дерево відмов (рис. 2) [4, с.49]. *Дерево відмов* – це логічна діаграма, яка відображає відмови частин системи, внутрішніх подій або їх комбінацій, що призводять до визначеної небажаної події. Вершини графа описують наступні функціональні стани СНЕ:

* 3 – система справна;
* 2 – система працездатна, відмовив канал (система несправна), відмова виявлена і канал відновлюється;
* 1 – система непрацездатна, відмовили два канали, відмови виявлені і канал відновлюється;
* 2F – система працездатна, відмовив канал (система несправна), відмова не виявлена і канал не відновлюється;
* 1F – система непрацездатна, відмовили два канали, виявлена відмова одного каналу і канал відновлюється, відмова іншого каналу не виявлена і канал не відновлюється.



*Рис. 2. Дерево відмов СНЕ*

Використовуючи дерево відмов і марковське моделювання, була побудована багатофрагментна марковська модель (БФМ) СНЕ (рис. 3). *БФМ СНЕ* – це представлення ланок марковського ланцюга (МЛ) у вигляді сукупності фрагментів, що повторюються і відрізняються одним або декількома параметрами. У БФМ СНЕ враховано як фізичні, так і програмні відмови та відновлення системи [4, с.32-34, 76-78].



*Рис. 3. Модель надійності СНЕ (БФМ СНЕ)*

В моделі надійності СНЕ застосовуються наступні параметри із такими значеннями:

* $λ\_{p}=10^{-4}$ – інтенсивність відмов фізичної (апаратної) частини системи;
* $λ\_{d}=5∙10^{-5}$ – інтенсивність відмов програмного забезпечення;
* $μ\_{p}=1$ – інтенсивність відновлення фізичної (апаратної) частини системи;
* $μ\_{d}=0,01$ – інтенсивність відновлення програмного забезпечення;
* $D=0,95$ і $D=0,99$ – достовірність контролю і діагностики.

Всі обрахунки проводилися на проміжку $t\in \left[0;10000\right]$ із точністю $e=10^{-6}$.

Були описані функціональні стани БФМ СНЕ та виділені стани, при яких система справна, працездатна та непрацездатна. Відповідно до побудованої БФМ склали систему диференціальних рівнянь (СДР) Колмогорова-Чепмена, що у загальному вигляді має вид:

$\left\{\begin{matrix}P\_{0}^{'}\left(t\right)=-\left(3λ\_{p}+λ\_{d}\right)P\_{0}\left(t\right)+μ\_{p}P\_{1}\left(t\right)\\P\_{1}^{'}\left(t\right)=-\left(μ\_{p}+2λ\_{p}+λ\_{d}\right)P\_{1}\left(t\right)+3λ\_{p}DP\_{0}\left(t\right)+2λ\_{p}DP\_{2}\left(t\right)+2μ\_{p}P\_{3}\left(t\right)\\\begin{matrix}P\_{2}^{'}\left(t\right)=-\left(2λ\_{p}+λ\_{d}\right)P\_{2}\left(t\right)+3λ\_{p}\left(1-D\right)P\_{0}\left(t\right)\\P\_{3}^{'}\left(t\right)=-2μ\_{p}P\_{3}\left(t\right)+2λ\_{p}DP\_{1}\left(t\right)+λ\_{p}DP\_{4}\left(t\right)\\\begin{matrix}P\_{4}^{'}\left(t\right)=-λ\_{p}DP\_{4}\left(t\right)+2λ\_{p}\left(1-D\right)P\_{1}\left(t\right)+2λ\_{p}\left(1-D\right)P\_{2}\left(t\right)\\P\_{5}^{'}\left(t\right)=-μ\_{d}P\_{5}\left(t\right)+λ\_{d}P\_{1}\left(t\right)\\\begin{matrix}P\_{6}^{'}\left(t\right)=-μ\_{d}P\_{6}\left(t\right)+λ\_{d}P\_{0}\left(t\right)\\P\_{7}^{'}\left(t\right)=-μ\_{d}P\_{7}\left(t\right)+λ\_{d}P\_{2}\left(t\right)\\\begin{matrix}P\_{8}^{'}\left(t\right)=-3λ\_{p}P\_{8}\left(t\right)+μ\_{d}P\_{6}\left(t\right)+μ\_{p}P\_{9}\left(t\right)\\P\_{9}^{'}\left(t\right)=-\left(μ\_{p}+2λ\_{p}\right)P\_{9}\left(t\right)+3λ\_{p}DP\_{8}\left(t\right)+2λ\_{p}DP\_{10}\left(t\right)+2μ\_{p}P\_{11}\left(t\right)+μ\_{d}P\_{5}\left(t\right)\\\begin{matrix}P\_{10}^{'}\left(t\right)=-2λ\_{p}P\_{10}\left(t\right)+μ\_{d}P\_{7}\left(t\right)+3λ\_{p}\left(1-D\right)P\_{8}\left(t\right)\\P\_{11}^{'}\left(t\right)=-2μ\_{p}P\_{11}\left(t\right)+2λ\_{p}DP\_{9}\left(t\right)+λ\_{p}DP\_{12}\left(t\right)\\\begin{matrix}P\_{12}^{'}\left(t\right)=-λ\_{p}DP\_{12}\left(t\right)+2λ\_{p}\left(1-D\right)P\_{9}\left(t\right)+2λ\_{p}\left(1-D\right)P\_{10}\left(t\right)\\\sum\_{i=0}^{12}P\_{i}\left(t\right)=1\end{matrix}\end{matrix}\end{matrix}\end{matrix}\end{matrix}\end{matrix}\end{matrix}\right.$ (1)

В СДР загального вигляду (1) підставили параметри і отримали дві СДР, що відрізняються різними коефіцієнтами достовірності і контролю.

Для того, щоб побачити відображає чи ні СДР реальний процес, була оцінена *стійкість за Ляпуновим*. Для вибору чисельного методу (ЧМ), оцінили таку метрику системи як жорсткість. *Коефіцієнт жорсткості* $s\left(x\right)$ (2, 3) СДР є базовою метрикою властивості жорсткості. Для визначення коефіцієнта жорсткості використали найвідоміший підхід – за допомогою власних чисел матриці Якобі.

$Re λ\_{i}<0, i=1,2,…,n$ (2)

$s\left(x\right)=\frac{\max\_{i=1,n}Re\left(\left|-λ\_{i}\right|\right)}{\min\_{i=1,n}Re\left(\left|-λ\_{i}\right|\right)}\gg 1$ (3)

де *λi* – власні числа матриці Якобі.

Для визначення власних чисел був застосований пакет комп’ютерної математики (ПКМ) Maple. *Кількісні значення коефіцієнта жорсткості* (ступінь жорсткості) можуть бути розділені на три групи:

1. $s\left(x\right)\leq 10^{2}$ – низька (мала) жорсткість;
2. $10^{2}\leq s\left(x\right)<10^{4}$– середня жорсткість;
3. $s\left(x\right)\geq 10^{4}$– висока жорсткість [4].

В результаті проведеного аналізу отримали стійкі СДР з низькою жорсткістю в обох випадках.

Для дослідження ММ були обрані найоптимальніші методи: прямі методи (вбудований метод Рунге-Кутта, що був реалізований в ПКМ Mathematica) та модифіковані методи розв’язання СДР Колмогорова-Чепмена (експоненціальний метод, реалізований без допомоги ПКМ) [5, с.186-206].

Після розв’язання СДР Колмогорова-Чепмена обраними методами, була обрахована функція готовності СНЕ.

*Функція готовності* (рис. 4) – це сума ймовірностей перебування системи в працездатних станах, що обраховується за формулою $A\left(t\right)=\sum\_{i=0}^{n}P\_{i}\left(t\right)$, де $P\_{i}\left(t\right)$ - ймовірність знаходження системи в працездатних станах [4, с.74-75].



*Рис. 4. Функція готовності СНЕ*

Аналіз результатів моделі забезпечення ФБ СНЕ для платформ, які самодіагностуються і програмуються дозволяє відзначити такі особливості. Найбільш «сприятливою» при обрахунку обома методами є модель із достовірністю контролю та діагностики $D=0,99$. При достовірності контролю та діагностики $D=0,95$ на проміжку часу $\left[0;\right.\left.500\right)$ відзначимо різкий спад функції готовності системи, а на проміжку $\left[500;10000\right]$ – спостерігаємо поступовий спад функції готовності. При достовірності контролю та діагностики $D=0,99$ спостерігаємо дещо іншу ситуацію: на проміжку часу $\left[0;\right.\left.1000\right)$ відзначимо різкий спад функції готовності системи, а на проміжку $\left[1000;10000\right]$ – спостерігаємо поступове зростання функції готовності системи.

Аналіз графіків дозволяє зробити висновок, що модель із достовірністю контролю і діагностики $D=0,99$ може забезпечити більш високий рівень готовності системи нормальної експлуатації.

Також були досліджені відмінності у чисельних значеннях функції готовності СНЕ для різних реалізацій. Їх відображено в таблиці 1. Введемо позначення:

* 1 - метод Рунге-Кутта, реалізований в ПКМ Mathematica;
* 2 - модифікований експонеціальний метод, реалізований за допомогою програмного продукту комерційної розробки ExpMeth.exe.

*Таблиця 1. Різниця в обчисленнях функції готовності СНЕ*

|  |  |
| --- | --- |
|  | ***Методи, що порівнюються*** |
| ***Показники порівняння*** | ***1 & 2 D=0,95*** | ***1 & 2 D=0,99*** |
| ***Мінімальне значення різниці*** | 0,00 | 0,00 |
| ***Максимальне значення різниці*** | 1,00E-06 | 4,82E-03 |

Можемо зробити висновок, що результати обчислень **«**1 & 2 D=0,95» збігаються з точністю , «1 & 2 D=0,99» – з точністю .

Отже, практична цінність отриманих результатів дозволяє чисельно оцінити готовність побудованої системи і обраної архітектури, а також розробити рекомендації щодо покращення побудованої моделі забезпечення функціональної безпеки системи нормальної експлуатації на основі платформ, які самодіагностуються і програмуються.

**Література:**

1. *ДСТУ 2941-94 Системи оброблення інформації. Розроблення систем. Терміни та визначення*
2. *Федоров Ю. Н. Справочник инженера по АСУТП: Проектирование и разработака. Учебно-практическое пособие / Юрий Николаевич Федоров. – Москва: Инфра-Инженерия, 2008. – 928 с.*
3. *IEC 61508. Functional safety of electrical/electronic/programmable electronic safety-related systems [Text]. Published. 2010-04. – IEC Standards, 2010. – 594 p.*
4. *Одарущенко Е. Б. Моделирование отказоустойчивых компьютерных систем с учетом изменяющихся параметров потоков отказов и восстановлений программных средств : дис. канд. техн. наук : 01.05.02 – математическое моделирование и вычислительные методы / Одарущенко Елена Борисовна – Харьков: Национальный аэрокосмический университет им. Н. Е. Жуковского «Харьковский авиационный институт», 2007. – 210 с.*
5. *Арушанян О. Б. Численное решение обыкновенных дифференциальных уравнений на Фортране / О. Б. Арушанян, С. Ф. Залеткин. – Москва: Издательство МГУ, 1990. – 336 с.*

*О.Б. Одарущенко, к.т.н., доцент*

*М.В. Кисла, магістр*

*Полтавський національний технічний університет*

*імені Юрія Кондратюка*

**МОДЕЛЬ ЗАБЕЗПЕЧЕННЯ ФУНКЦІОНАЛЬНОЇ БЕЗПЕКИ СИСТЕМИ НОРМАЛЬНОЇ ЕКСПЛУАТАЦІЇ НА ОСНОВІ ПЛАТФОРМ, ЯКІ САМОДІАГНОСТУЮТЬСЯ І ПРОГРАМУЮТЬСЯ**

*Стаття присвячена розробці, побудові та аналізу моделі забезпечення функціональної безпеки системи нормальної експлуатації на основі платформ, які самодіагностуються і програмуються.*

***Ключові слова:*** *система нормальної експлуатації, функціональна безпека, інформаційно-керуюча система, дерево відмов, багатофрагментна марковська модель, система диференціальних рівнянь Колмогорова-Чепмена.*

***Е.Б. Одарущенко, к.т.н., доцент***

***М.В. Кислая, магистр***

***Полтавский национальный технический университет***

***имени Юрия Кондратюка***

**МОДЕЛЬ ОБЕСПЕЧЕНИЯ ФУНКЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ СИСТЕМЫ НОРМАЛЬНОЙ ЭКСПЛУАТАЦИИ НА ОСНОВЕ САМОДИАГНОСТИРУЕМЫХ И ПРОГРАММИРУЕМЫХ ПЛАТФОРМ**

*Статья посвящена разработке, построению и анализу модели обеспечения функциональной безопасности системы нормальной эксплуатации на основе самодиагностируемых и программируемых платформ.*

***Ключевые слова:*** *система нормальной эксплуатации, функциональная безопасность, информационно-управляющая система, дерево отказов, многофрагментная марковская модель, система дифференциальных уравнений Колмогорова-Чепмена.*

*O.B. Odarushchenko, PhD, Associate Professor,*

*M.V. Kysla, undergraduate*

*Poltava National Technical Yuri Kondratyuk University*

**MODEL OF PROVIDE THE FUNCTIONAL SAFETY OF NORMAL MAINTENANCE SYSTEM BASED ON SELF-DIAGNOSTIC AND PROGRAMMABLE PLATFORMS**

*Article is devoted to the development, construction and analysis of model of providing the functional safety of normal maintenance system based on self-diagnostic and programmable platforms.*

***Keywords*** *normal maintenance system, functional safety, information and control system, fault tree, multiple-fragment Markov model, differential equations system of the Kolmogorov-Chapman.*