**УДК 004.942+004.519.876.5**

*О.Б. Одарущенко, к.т.н., доцент*

*В.В. Москалець, магістр*

*Полтавський національний технічний університет*

*імені Юрія Кондратюка*

**МОДЕЛЬ ЗАБЕЗПЕЧЕННЯ ФУНКЦІОНАЛЬНОЇ БЕЗПЕКИ СИСТЕМИ АВАРІЙНОГО ЗАХИСТУ НА ОСНОВІ ПЛАТФОРМ, ЯКІ САМОДІАГНОСТУЮТЬСЯ ТА ПРОГРАМУЮТЬСЯ**

Стрімкий розвиток суспільства, вирішення проблем забезпечення високого рівня безпеки держави неможливе без розробки і реалізації проектів складних технічних комплексів. При цьому складно уявити етап проектування таких систем без застосування їх моделювання. Моделювання дозволяє провести дослідження складних систем, які не можуть бути виконані традиційними методами, визначити їх надійність. Воно істотно знижує терміни і вартість проектування і за рахунок аналізу великої кількості варіантів підвищує ефективність розроблюваної системи [1, ст. 8].

Дуже важливим таке моделювання є для розробки систем аварійного захисту (САЗ), які встановлюються практично на всіх атомних електричних станціях (АЕС), наприклад, для їх реакторів [2].

Розглянемо ряд ключових понять:

**САЗ** – це система, яка забезпечує захист певного контрольованого процесу від небажаного розвитку подій, тобто система повинна спрацювати у випадку аварії. Обов'язковою умовою побудови такої системи є переведення контрольованого процесу в результаті її спрацювання в «безпечний» стан [3].

**Функціональна безпека (ФБ)** – частина безпеки, що відноситься до керованого обладнання та керуючої системи, яка залежить від правильного функціонування електричних, електронних і програмованих електронних (Е/Е/ПЕ) систем, пов'язаних із безпекою технологічних систем та обладнання для зниження зовнішнього ризику [4, ст. 105].

**Інформаційно-керуюча система** (**ІКС**) – це сукупність керованого об'єкта й автоматичних вимірювальних та керуючих пристроїв, у якій частину функцій виконує людина [2].

**Теорія надійності** – наука, яка вивчає закономірності розподілу відмов технічних пристроїв, причини і моделі їх виникнення [5].

**Надійність** – властивість об'єкта зберігати в часі у встановлених межах значення всіх параметрів, що характеризують здатність виконувати необхідні функції в заданих режимах і умовах застосування, технічного обслуговування, зберігання і транспортування [5].

**Ступінь жорсткості s(x)** – умовний номер, що відображає інтенсивність діючих перешкод з параметрами, які регламентуються в нормативній документації; характеризує рівень точності чисельних обрахунків, на його основі підбирають методи для розв’язання СДР:

$Re λ\_{i}<0, i=1,2,…,n$;

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

де *λi* – власні числа матриці Якобі [6, ст. 6].

**Функція готовності** **(ФГ)** – 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 [7, ст. 206].

Існує ряд державних стандартів України (див. [8] та [9]) і ряд міжнародних стандартів, що регламентують вимоги до надійності й функціональної безпеки САЗ. Міжнародний стандарт МЕК 61508, який описано в [10], розглядає весь життєвий цикл електричних, електронних або програмованих електронних (E / E / PE) систем і виробів.

Розглянемо структурну схему САЗ, яка побудована на основі двох підсистем з мажоритарною структурою (див. рис. 1).



*Рисунок 1. Структурна схема САЗ, яка побудована по схемі двох підсистем з мажоритарною структурою*

Кожна підсистема побудована на основі архітектури M out of N (MооN). Це означає, що для виконання функцій повинні працювати хоча б M каналів із N (у нашому випадку – два канали з трьох) [4, ст. 116].

Для аналізу даної моделі було використано марковське моделювання й теорія марковських процесів з дискретними станами й неперервним часом, які описані в [1] та [11].

Розглянемо дерево відмов (див. рис. 2).



*Рисунок 2.* *Дерево відмов САЗ, яка побудована по схемі двох підсистем з мажоритарною структурою*

Кожна його вершина відповідає конкретному станові САЗ, який обумовлюється комбінацією станів двох підсистем. Причому кожна підсистема може знаходитись в **одному** **з** **п’яти станів**, а саме:

* 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.

Розглянемо **багатофрагментну марковську модель надійності** (БФ ММН) САЗ, яка була побудована з врахуванням появи описаних вище відмов та неідеальних засобів контролю й діагностики (див. рис. 3).



*Рисунок 3.* *БФ ММН САЗ*

Вершини відповідають функціональним станам САЗ. Всього їх 30, і вони розподіляються на **три категорії**:

1. функціональні стани, при яких система **справна** (**S0 (3,3)**, **S18 (3,3)**);
2. функціональні стани, при яких система **працездатна** (**S1 (3,2)**, **S2 (3,2F)**, **S4 (2,2)**, **S6 (2F,2)**, **S7 (2F,2F)**, **S19 (3,2)**, **S20 (3,2F)**, **S22 (2,2)**, **S24 (2F,2)**, **S25 (2F,2F)**);
3. функціональні стани, при яких система **непрацездатна** (**S3 (3,1)**, **S5 (3,1F)**, **S8 (2,1)**, **S9 (2F,1)**, **S10 (2,1F)**, **S11 (2F,1F)**, **S12 (3,3)**, **S13 (3,2)**, **S14 (3,2F)**, **S15 (2,2)**, **S16 (2F,2)**, **S17 (2F,2F)**, **S21 (3,1)**, **S23 (3,1F)**, **S26 (2,1)**, **S27 (2F,1)**, **S28 (2,1F)**, **S29 (2F,1F)**).

В БФ ММН САЗ застосовуються **наступні параметри:**

*  – інтенсивність відмов апаратного забезпечення;
* $λ\_{d}$ – інтенсивність відмов програмного забезпечення;
* $μ\_{p}$ – інтенсивність відновлення апаратного забезпечення;
* $μ\_{d}$ – інтенсивність відновлення програмного забезпечення;
* $D$ – параметр достовірності контролю й діагностики.

На основі складеної БФ ММН САЗ була побудована система диференціальних рівнянь Колмогорова–Чепмена (СДР КЧ):





яка з початковими умовами  та умовою нормування  утворює задачу Коші. ЇЇ розв’язок дає ймовірності перебування САЗ у кожному функціональному стані. Для розв’язання СДР КЧ доцільно перевірити стійкість її розв’язку за Ляпуновим (показує, чи відображає дана СДР реальний процес, див. [12]) та визначити ступінь жорсткості.

Підібравши набір таких параметрів: , , $λ\_{d}=5∙10^{-5}$$μ\_{p}=1$, $μ\_{d}=0,01$, $D=0,95$ і , $t\in \left[0;10000\right]$$e=10^{-6}$ – точність обрахунків,  – кількість ітерацій для покрокових методів; було підтверджено стійкість розв’язків отриманих СДР КЧ, встановлено низький рівень жорсткості СДР КЧ та визначено функцію готовності САЗ на базі архітектури 2оо3&2оо3 на інтервалі часу $t\in \left[0;10000\right]$ (див. рис. 4).



*Рисунок 4. Функція готовності САЗ*

Керуючись попередніми даними, для розв’язання СДР КЧ було обрано два методи:

а) явний метод Ругне-Кутта 4-го порядку, який описаний в [13], реалізований в пакетах комп’ютерної математики MATLAB, MATHEMATICA;

б) модифікований експоненціальний метод (програма EXPMETH.EXE), який описаний в [13].

Проаналізувавши графіки функції готовності САЗ для обох випадків, можемо зробити такі висновки:

1. у першому випадку ФГ на інтервалі часу  різко спадає від 1 до 0.995, а потім при  плавно спадає від 0.995 до 0.991;
2. у другому випадку ФГ на інтервалі часу  різко спадає від 1 до 0.995, а потім при  плавно зростає від 0.995 до 0.9965

Отже, якщо показник достовірності діагностики й контролю , то маємо вищий рівень надійності системи.

Практичне значення отриманих результатів визначається тим, що вони дозволяють отримати оцінку надійності та сформулювати рекомендації щодо архітектурної побудови моделі забезпечення функціональної безпеки системи аварійного захисту на основі платформ, які самодіагностуються і програмуються.

**Список використаної літератури:**

1. 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.
2. Безопасность атомных станций : системы управления и защиты ядерных реакторов: [монография] / М. А. Ястребенецкий, Ю. В. Розен, С. В. Виноградская, Г. Джонсон, В. В. Елисеев, А. А. Сиора, В. В. Скляр, Л. И. Спектор, В. С. Харченко ; под ред. М. А. Ястребенецкого. – К. : Основа-Принт, 2011. – 768 с. – ISBN : 798-966-2044-52-2.
3. Аварийная защита [Електронный ресурс] // Свободная энциклопедия Википедия. – Режим доступа : https://ru.wikipedia.org/wiki/%D0%90%D0%B2%D0%B0%D1%80%D0%B8%D0%B9%D0%BD%D0%B0%D1%8F\_%D0%B7%D0%B0%D1%89%D0%B8%D1%82%D0%B0.
4. Федоров Ю. Н. Справочник инженера по АСУПТ : Проектирование и разработка [Текст] : учеб.-пр. пособие / Ю. Н. Федоров. – М. : Инфа-Инженерия, 2008. – 928 с. – ISBN : 978-5-9729-0019-0.
5. ГОСТ 27.002-89 Надійність в техніці. Основні поняття. Терміни і визначення [Текст]. – 1989.
6. Kharchenko, V. Markov’s model and tool-based assessment of safety-critical I&C systems: gaps of the IEC 61508 [Electronic source] / V. Kharchenko, O. Odarushchenko, V. Butenko, P. Popov, V.Sklyar, E. Odarushchenko // in digital collection Proc. 12-th Int. conf. on probabilistic safety assessment and modeling, USA, Hawaii, Honolulu, June 2014 – Access : http://psam12.org/proceedings/paper/paper\_455\_1.pdf.
7. Инструментированное оценивание надежности программно-технических комплексов при росте интенсивности отказов / Ю. Н. Соколов, В. С. Харченко, Ю. Л. Поночовный // Системи обробки інформації. – Харьков : Национальный аэрокосмический университет им. Н. Е. Жуковского «Харьковский авиационный институт», 2014. – Вып. 19. – С. 205-211. – ISSN : 1681-7710.
8. ГОСТ 24.701-86 Єдина система стандартів автоматизованих систем управління. Надійність автоматизованих систем управління [Текст]. – Введ. 1987-08-01. – М. : СТАНДАРТИНФОРМ, 2009. – 12 с.
9. ДСТУ 2941-94 Системи оброблення інформації. Розроблення систем. Терміни та визначення [Текст]. – 1994.
10. МЕК 61508 Функціональна безпека електричних / електронних / програмованих електронних систем (Е/Е/ПЕ), що пов’язані з безпекою систем [Текст]. – 1998-2000.
11. Теория вероятностей : учеб. для вузов / Е. С. Вентцель. – 6-е изд. стер. – М. : Высш. шк., 1999. – 576 c.
12. Варченко Т. В. Стійкість розв’язків систем диференціальних рівнянь : дипломна робота бакалавра / Тетяна Володимирівна Варченко. – Полтава: Полтавський національний технічний університет імені Юрія Кондратюка, 2013. – 33 с.
13. Арушанян О. Б. Численное решение обыкновенных дифференциальных уравнений на Фортране [Текст] / О. Б. Арушанян, С. Ф. Залеткин. – М. : Изд-во МГУ, 1990. – 336 с. – ISBN 5-211-09957-6.

*О.Б. Одарущенко, к.т.н., доцент*

*В.В. Москалець, магістр*

*Полтавський національний технічний університет*

*імені Юрія Кондратюка*

**МОДЕЛЬ ЗАБЕЗПЕЧЕННЯ ФУНКЦІОНАЛЬНОЇ БЕЗПЕКИ СИСТЕМИ АВАРІЙНОГО ЗАХИСТУ НА ОСНОВІ ПЛАТФОРМ, ЯКІ САМОДІАГНОСТУЮТЬСЯ ТА ПРОГРАМУЮТЬСЯ**

*У даній статті розглядається розробка, побудова та аналіз моделі забезпечення функціональної безпеки системи аварійного захисту на основі платформ, які самодіагностуються і програмуються, на базі архітектури 2оо3&2оо3.*

***Ключові слова:*** *система аварійного захисту, функціональна безпека, інформаційно-керуюча система, багатофрагментна марковська модель, система диференціальних рівнянь Колмогорова-Чепмена, функція готовності.*

*Е.Б. Одарущенко, к.т.н., доцент*

*В.В. Москалец, магистр*

*Полтавский национальный технический университет*

*имени Юрия Кондратюка*

**МОДЕЛЬ ОБЕСПЕЧЕНИЯ ФУНКЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ СИСТЕМЫ АВАРИЙНОЙ ЗАЩИТЫ НА ОСНОВЕ САМОДИАГНОСТИРУЕМЫХ ПРОГРАМИРУЕМЫХ ПЛАТФОРМ**

*В данной статье рассматривается разработка, построение и анализ модели обеспечения функциональной безопасности системы аварийной защиты на основе самодиагностируемых программируемых платформ на базе архитектуры 2оо3&2оо3.*

***Ключевые слова:*** *система аварийной защиты, функциональная безопасность, информационно-управляющая система, многофрагментная марковская модель, система дифференциальных уравнений Колмогорова-Чепмена, функция готовности.*

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

*V.V. Moskalets, undergraduate*

*Poltava National Technical Yuri Kondratyuk University*

**MODEL OF PROVIDE THE FUNCTIONAL SAFETY OF EMERGENSY PROTECTION SYSTEMS BASED ON SELF-DIAGNOSTIC AND PROGRAMMABLE PLATFORMS**

*This article describes* *development, construction and analysis of model providing the functional of emergency protection systems based on self-diagnostic and programmable platforms based on architecture 2oo3&2oo3.*

***Keywords:*** *emergency protection system, functional safety, information and control system, multiple-fragment Markov model, differential equations system of the Kolmogorov-Chapman, readiness function.*