УДК 004.4 https://doi.org/10.32515/2664-262X.2025.11(42).2.52-62

Б. Ю. Вінтенко[1,2], **О. А. Смірнов**[3], проф., д-р техн. наук,
І. В. Миронець[1], доц., канд. техн. наук, **Т. В. Смірнова**[3], канд. техн. наук,
О. В. Коваленко[3], проф., д-р техн. наук, **А. М. Мацуй**[3], проф., д-р техн. наук
[1]*Черкаський державний технологічний університет, Черкаси, Україна*
[2] *ПАТ "Науково-виробниче підприємство "Радій", м. Кропивницький, Україна*
[3]*Центральноукраїнський національний технічний університет, м. Кропивницький, Україна*
e-mail: boris.vintenko@gmail.com, dr.smirnovoa@gmail.com, i.myronets@chdtu.edu.ua, sm.tetyana@gmail.com, dr.kovalenkoov@gmail.com, matsuyan@ukr.net

Модель шляхів отримання вхідних даних комп'ютерної інтелектуальної системи підтримки оперативного персоналу АЕС

У статті досліджуються методи підвищення відмовостійкості комп'ютерної інтелектуальної системи підтримки оператора енергоблоку АЕС. Метою даного дослідження є підвищення відмовостійкості інтелектуальних систем підтримки оператора при отриманні інформації про стан технологічних параметрів, важливих для процедур керування енергоблоком. Об'єктом дослідження є шляхи отримання вхідних даних комп'ютеризованою інтелектуальною системою підтримки оператора АЕС. Предметом дослідження є модель шляхів надходження вхідної інформації до комп'ютерної інтелектуальної системи підтримки оператора АЕС. Розглянуто задачу забезпечення надійності вхідної інформації та способи її вирішення, які основані на резервуванні та багатоверсійності застосованих компонентів. Розроблена імітаційна модель шляхів вхідних даних комп'ютерної інтелектуальної системи підтримки оператора енергоблоку АЕС, що відрізняється від відомих врахуванням показників багатоверсійності компонентів.

система підтримки прийняття рішень, резервування, відмово стійкість, надійність, багатоверсійність, імітаційна модель

Постановка проблеми. Енергоблок АЕС є складним технологічним об'єктом, керування яким здійснюється оперативним персоналом (ОП) на блочному щиті керування (БЩК). Під час роботи ОП використовує інформацію, яка надається йому за допомогою індикаторів та приладів панелей керування, а також за допомогою цифрових інформаційних систем. Прийняття рішень ОП здійснюється на основі технологічних регламентів.

Для підвищення ефективності та надійності роботи ОП, актуальною науково-практичною задачею є створення комп'ютеризованих інтелектуальних систем підтримки оператора (СПО) [1].

Інформація про значення технологічних параметрів отримується з датчиків, що встановлені на обладнанні енергоблоку. Дані з цих датчиків електричними каналами передаються до програмно-технічних комплексів (ПТК) енергоблоку. Інформація про параметри у вигляді значень аналогових та дискретних значень реєструється на серверах ПТК та за допомогою комп'ютерних мереж передається до інших систем енергоблоку, зокрема і до СПО.

Актуальність даних про стан технологічних параметрів є необхідною умовою для функціонування СПО. Тому важливою задачею при створенні СПО є підвищення відмовостійкості СПО в частині отримання цих даних.

Метою дослідження є підвищення відмовостійкості СПО при отриманні інформації про стан технологічних параметрів, важливих для процедур керування енергоблоком.

Об'єктом дослідження є шляхи отримання вхідних даних комп'ютеризованою інтелектуальною системою підтримки оператора АЕС.

Предметом дослідження є модель шляхів надходження вхідної інформації до комп'ютерної інтелектуальної системи підтримки оператора АЕС.

Аналіз останніх досліджень і публікацій. Систему підтримки оператора можна розглядати як набір об'єктів, одним з яких є підсистема отримання вхідних даних.

Стійкість систем до відмов, тобто здатність виконувати основні функції при виникненні відмов окремих компонентів, може реалізовуватися різними способами.

Так, популярним методом підвищення відмовостійкості є резервування обладнання, програмного забезпечення та інформації. Також для підвищення стійкості до відмов програмного забезпечення та інформації є застосування самоконтролю та блоків відновлення [2]. При використанні даної технології результати обчислень перед передачею в іншу підсистему перевіряються на коректність, і у випадку непроходження перевірки ті ж самі обчислення виконуються повторно, іншими способами, до досягнення потрібного результату.

В галузях, що вимагають високої надійності та стійкості до відмов, останніми десятиліттями набуває популярності використання багатоверсійних технологій [4]. Так, для підвищення відмовостійкості апаратного забезпечення використовуються різні типи мікросхем (мікропроцесори та FPGA) [5], для підвищення відмовостійкості програмного забезпечення використовується N-версійне програмування [6], [7].

Відмови з загальної причини є проблемою для резервованих систем [8]. У випадку виникнення загальної причини можуть відмовити одразу декілька компонентів. Такою причиною може бути як апаратна (наприклад, зникнення електричного живлення основного та резервованого сервера), так і недолік у проєктуванні (розміщення резервованих ліній зв'язку в одній кабельній шахті та вихід з ладу обох при пожежі), а також дефект програмного забезпечення, що використовується у резервованих каналах.

Для зменшення імовірності відмови з загальної причини використовується багатоверсійне програмне забезпечення. Багатоверсійність може бути застосована для даних, програмного коду, та функціональності [9]. Після виконання функції різними версіями програмного забезпечення відбувається аналіз отриманих результатів, порівняння їх між собою та фільтрування результатів, що не відповідають вимогам. В Також використовуються різні схеми голосування. Найпоширенішими схемами є «1/2», «2/3», «2/4» або «3/4». Вибір схеми залежить від вимог до безпеки, надійності, допустимого рівня хибних спрацювань та неспрацювань. В рамках вирішення даного завдання у попередніх роботах авторів розглянуті питання дослідження нормативних документів та галузевих стандартів розробки програмного забезпечення комп'ютерних систем управління АЕС, важливих для безпеки й дослідження вимог міжнародних стандартів IEC60880 та IEC62138 з розробки програмного забезпечення інформаційно-керуючих систем АЕС, важливих для безпеки [11], [12] та дослідження вимог та аналіз кібербезпеки програмного забезпечення інформаційно-керуючих систем АЕС, важливих для безпеки та дослідження інформаційного забезпечення та технологічних регламентів процесів керування критичною інфраструктурою енергоблоку АЕС з реактором типу ВВЕР-1000 [13], [14].

Таким чином, підвищення відмовостійкості підсистеми отримання вхідних даних СПО доцільно проводити на основі аналізу відмовостійкості джерел отримання цих даних та шляхів їх передачі.

Постановка завдання. У даному дослідженні необхідно створити модель шляхів вхідних даних системи підтримки оператора, в якій буде міститися інформація про використані технології та їх версійні відмінності.

Виклад основного матеріалу. Методи забезпечення відмовостійкості СПО. Джерела вхідних даних для СПО. Основною функцією підсистеми отримання вхідних даних СПО є прийом значень технологічних параметрів від зовнішнього оточення. Точками взаємодії підсистеми з зовнішнім оточенням є вхідні сигнали. Вхідні сигнали можуть бути розділені на первинні та вторинні.

Значення первинних вхідних сигналів отримуються шляхом вимірювань. Прикладами таких значень є тиск, температура, тощо. Також, до первинних вхідних сигналів можна віднести інформацію, яка отримана від оператора: введені через інтерфейс користувача значення, натиснуті оператором кнопки, сформовані команди за допомогою ключів керування тощо.

Вторинними сигналами можна вважати сигнали, значення яких отримані в результаті обробки даних первинних сигналів: швидкість, температура насичення, спрацювання уставок, тощо.

У найпростішому випадку, вхідна інформація СПО може бути представлена у вигляді множини технологічних параметрів P:

$$P = \{P_1, P_2, P_3, \ldots, P_n\} \quad (1)$$

де P_i – окремий вхідний параметр, n – загальна кількість параметрів. Проте таку модель не можна використовувати безпосередньо. На практиці, між параметром та алгоритмом СПО існує система вимірювання з проміжних апаратних та програмних елементів, які забезпечують прийняття, первинну обробку, перетворення, передачу інформації. Це обумовлено такими причинами:

– необхідність фільтрації та обробки даних у випадку наявності шумів, перешкод або нестабільності;

– наявність параметрів, що формуються на основі сигналів з декількох датчиків або обчислень;

– конверсія сигналів з одного типу в інший, стандартний та придатний для обробки;

- фізична віддаленість елементів не дозволяє підключити датчики безпосередньо до системи;

– наявність фізичних бар'єрів захисту;

– необхідність захисту даних від зовнішніх атак: додаткові елементи (брандмауери, системи контролю доступу, дата-діоди), що забезпечують інформаційну безпеку;

– необхідність протоколювання та моніторингу;

– координація та інтеграція великої кількості ПТК, реалізація різних протоколів зв'язку за допомогою шлюзів, тощо.

Елементи шляхів. Враховуючи наявність системи вимірювання та обробки, для кожного параметру можна визначити шляхи передачі, що складаються з множини елементів. Для представлення шляху Path використаємо векторну модель:

$$Path = \{E_1, E_2, E_3, \ldots, E_i\} \quad (2)$$

де E_{ni} – елемент, через який проходять дані сигналу.

Елементи шляху передачі параметру приведений на рисунку 1.

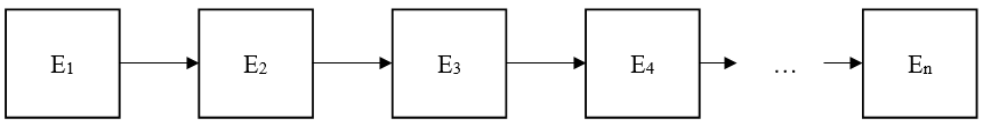

Рисунок 1 – Елементи шляху вхідних даних

Джерело: розроблено авторами

Кожний елемент у векторі *Path* може мати набір атрибутів: тип, продуктивність, надійність, протокол обміну, час затримки, тощо.

Приклад набору елементів шляху вхідних даних для параметру:

– E_1 – датчик;

– E_2 – перетворювач форми сигналу (аналоговий-цифровий);

– E_3 – фільтр;

– E_4 – кабельний канал;

– E_5 – комутатор;

– E_6 – модуль контролю безпеки;

– E_7 – мережева карта;

– E_8 – сервер;

– E_9 – програмне забезпечення сервера.

Така модель отримання вхідних даних СПО, з точки зору теорії надійності, є найменш стійкою до відмов, оскільки передбачає послідовне з'єднання елементів.

Резервування шляхів передачі вхідних сигналів. Одним з поширених способів підвищення відмовостійкості систем вимірювання та передачі критичних параметрів є резервування. Зазвичай для вимірювання значення одного технологічного параметру застосовуються декілька датчиків, які мають незалежну схему живлення, конструкцію та канали передачі інформації (багатоверсійний підхід). При відмові елементів одного каналу отримання даних інформація про параметр залишається актуальною через інші датчики та канали зв'язку.

На АЕС можуть бути використані наступні види резервування:

– резервування датчиків;

– резервування ліній зв'язку;

– резервування програмного забезпечення;

– резервування комунікаційних пристроїв;

– резервування серверів тощо.

Таким чином, для отримання значення одного параметра може використовуватися матриця шляхів

$$\begin{Bmatrix} Path_1 \\ Path_2 \\ \\ Path_n \end{Bmatrix} = \begin{bmatrix} E_{11} & E_{12} & E_{1m} \\ E_{21} & E_{22} & E_{2m} \\ \\ E_{n1} & E_{n2} & E_{nm} \end{bmatrix}, \quad (3)$$

де E_{ij}- елементи шляхів.

При резервуванні отримується паралельна робота шляхів вимірювання (або їх частин), що підвищує відмовостійкість системи.

Слід зазначити, що створення окремих шляхів отримання вхідної інформації для кожного ПТК є складною та не завжди можливою задачею. Зазвичай інформація про критично важливі параметри отримується з резервованих датчиків, розмножується та передається у різні ПТК. В свою чергу, підсистема отримання вхідних даних СПО може отримати значення одного і того самого параметру від різних ПТК. Наприклад, інформація про температуру теплоносія в реакторі реєструється в системах захисту (АЗ), системах безпеки (СБ), системах нормальної експлуатації (СНЕ). Кожна точка реєстрації параметру в ПТК є окремим сигналом з унікальним ідентифікатором. Таким чином, СПО може отримати інформацію про значення технологічного параметру з різних сигналів, що надходять різними шляхами, з залученням різних елементів.

Багатоверсійність елементів шляхів. Кожний елемент вносить певну інтенсивність відмов у систему. Всі відмови можуть бути розподілені на дві категорії: відмови з фізичних причин та відмови через недоліки у проєктуванні.

Для оцінки інтенсивності відмов через фізичні дефекти використовуються довідкові дані виробників. Інтенсивність відмов через дефекти проєктування може бути оцінена статистичним шляхом.

Метод кількісної оцінки зменшення інтенсивності відмов при використанні двоверсійної (диверсної) системи описаний у [10].

У відповідності до даного методу, множина всіх відмов N у двоверсійній системі визначається як

$$N=N_1 \cup N_2 \cup N_{12}, \quad (4)$$

де N_1 – множина відмов тільки першої версії системи, N_2 – множина відмов тільки другої версії системи, N_{12} – множина одночасних відмов першої та другої версії системи (рисунок 2).

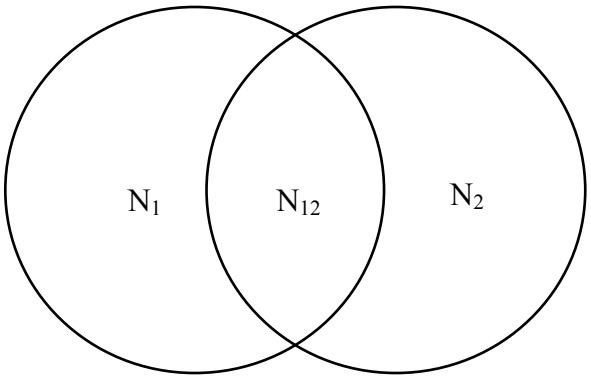

Рисунок 2 – Множини відмов двоверсійної системи

Джерело: розроблено авторами

Інтенсивність відмов двоверсійної системи визначає потужність множини N_{12}. Очевидно, що ця множина зменшується зі зростанням відмінностей у проєктуванні двоверсійної системи.

Кількісне співвідношення інтенсивності відмов двоверсійної системи та одноверсійної системи визначається коефіцієнтом диверсності:

$$K_D = \frac{|N_{12}|}{|N^{1в}|} \quad (5)$$

де $|N_{12}|$ – потужність множини відмов двоверсійної системи, а $|N^{1в}|$ – потужність множини відмов одноверсійної системи.

В результаті застосування диверсності, інтенсивність відмов двоверсійної системи λ_{12}, що викликані загальними дефектами проектування обох версій становить:

$$\lambda_{12} = K_D \cdot \lambda^{1B} \quad (6)$$

де λ_{12} – інтенсивність відмов одноверсійної системи, K_D – коефіцієнт диверсності.

Для кількісної оцінки глибини різниці між версіями елементів системи використовуються метрики диверсності. Значення 0 метрики відповідає відсутності різниці між версіями (одноверсійна система), 4 – максимальній різниці.

Коефіцієнт диверсності K_D системи обернено пропорційний до інтегрального показника диверсності системи: при відсутності диверсності ($D = 0$) коефцієнт K_D буде рівний одиниці, що згідно (6), не знизить інтенсивність відмов з загальної причини.

Розробка моделі шляхів отримання вхідних даних СПО. Відмінність елементів шляхів вхідних даних. Для забезпечення відмовостійкої роботи СПО має використовувати резервовані дані у вигляді сигналів. Як було показано, ці дані можуть надходити різними шляхами через різні послідовності елементів. Відповідно, задачею

розробника СПО є вибір сигналів та шляхів їх прийому з урахуванням обраної схеми голосування.

У шляхах передачі інформації, які можуть забезпечувати СПО вхідними даними, можуть застосовуватися різні типи елементів. До кожного з виду елементів може бути застосована шкала відмінностей між їх версіями.

Таким чином, для аналізу відмовостійкості шляхів вхідних даних СПО необхідно сформувати наступні дані:

– для кожного типу елемента на основі статистичних даних має бути визначена базова кількість відмов, що сформує показник $N^{lв}$;

– на основі відмінностей для кожного набору шляхів вхідних даних має бути сформований набір показників глибини диверсності, які сформують загальний показник диверсності D.

Розробка моделі шляхів вхідних даних

До складу кожного ПТК входять модулі прийому інформації, логічні модулі, сервери та програмне забезпечення. Кожний ПТК цифровим каналом передає необхідну інформацію до суміжних систем. Інформацію про один і той самий технологічний параметр СПО може запитувати у різних серверів різних ПТК.

Узагальнена архітектура отримання даних може бути представлена у вигляді мережі. Приклад такої мережі приведений на рисунку 3.

На даній схемі використовуються такі вузли: датчики (S), перетворювачі (C), кабелі, модулі вхідних сигналів (In), логічні модулі та модулі передачі інформації (Lm), комутатори (Comm), сервери (Srv), комп’ютери (Pc) з мережевими картами та програмним забезпеченням.

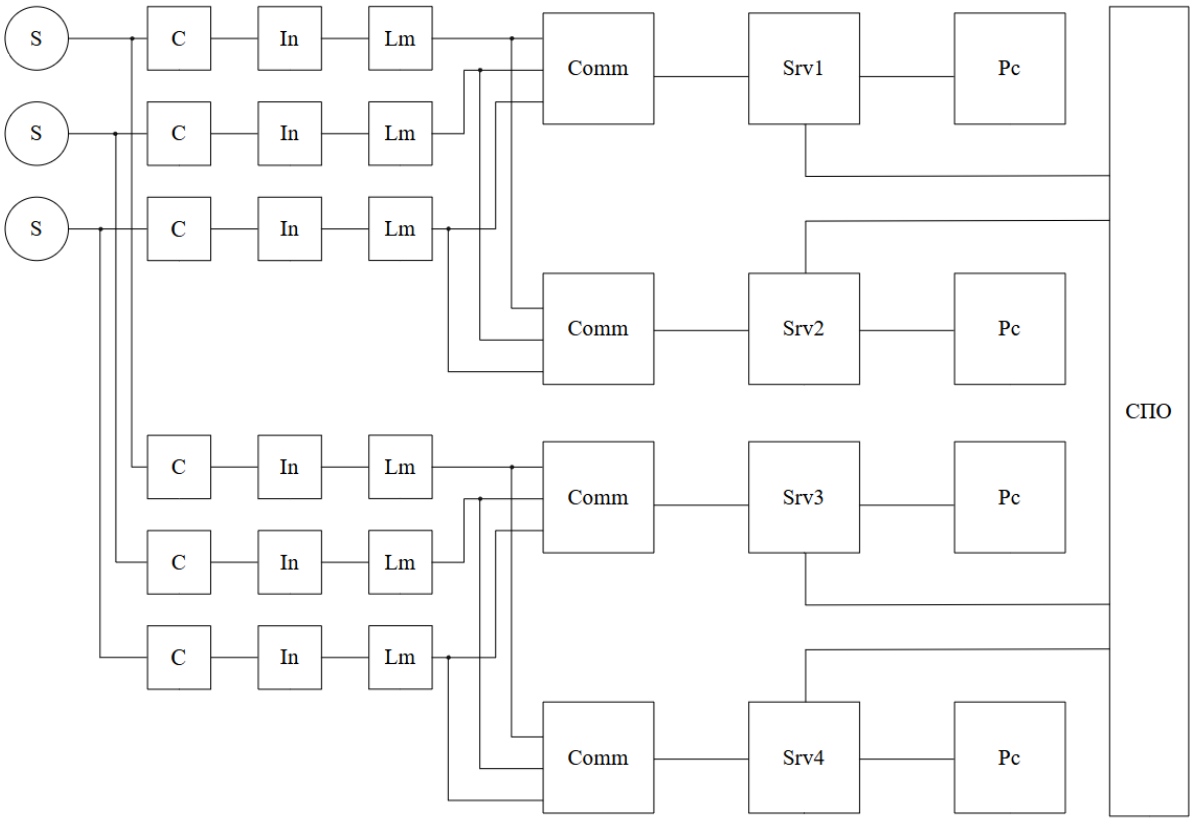

Рисунок 3 – Архітектура мережі прийому вхідних даних

Джерело: розроблено авторами

Дана мережа може бути представлена у вигляді графу $G = (E, L)$, вершини E якого – елементи каналів зв'язку, а ребра L – канали передачі інформації.

Основні властивості даного графу будуть наступними:

– граф є деревом;

– граф має одну початкову точку, яка визначає собою вимірюваний технологічний параметр;

– граф має одну кінцеву точку, яка є входом до системи, вхідні дані якої аналізуються;

– граф є орієнтованим, оскільки сигнали від джерел до системи передаються в одному напрямку;

– від початку вимірювання до точки прийому інформації є як мінімум один шлях;

– для первинних параметрів шлях сигналу починається з пристрою, який реєструє сигнал (датчика);

– для вторинних параметрів шлях сигналу починається з логічного модуля ПТК, який обчислює значення даного параметру. Наприклад, якщо вхідними даними є значення температури насичення, то до складу шляху включаються також датчики температури та тиску, а також компоненти, які виконують обчислення даного сигналу.

Приклад графу шляхів вхідних даних приведений на рисунку 4. Рамками окреслені окремі підсистеми.

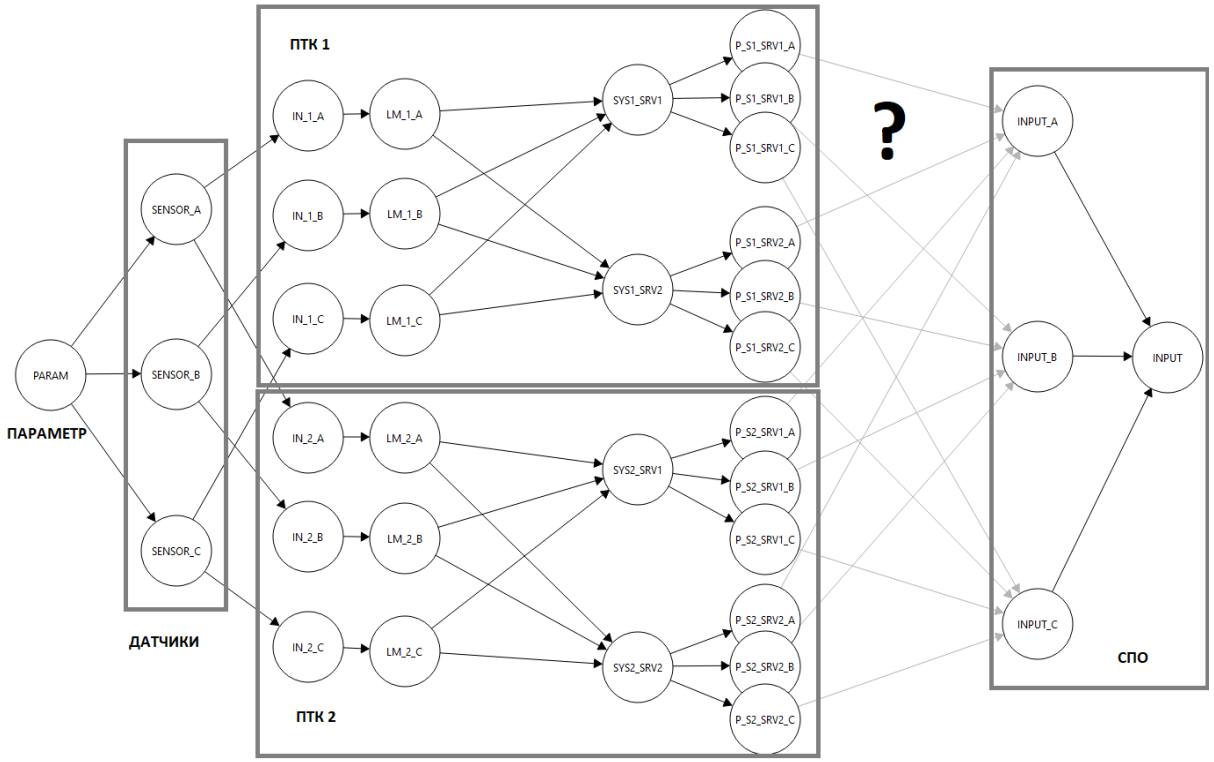

Рисунок 4 – Граф шляхів вхідних даних

Джерело: розроблено авторами

Кожна вершина графу $e \in E$ описується набором наступних властивостей:

$$e = \{Type, \{Tech\}, \{Versions\}, Tag\}. \quad (7)$$

Ці властивості мають наступні значення:

– **тип елементу** Type – код типу елементу, що є складовим шляху передачі. На шляху передачі використовуються різні типи елементів, такі як датчики, кабелі,

комутатори, сервери, програмне забезпечення. Кожний тип характеризується власним набором параметрів, за яким його можна порівнювати з іншими елементами. В таких задачах, як визначення відмовостійкості шляху, порівняння доцільно виконувати між компонентами, які мають один тип;

– **коди технологій** {Tech} – номери технологій, що використовуються у даному елементі. Використовуються для визначення можливості відмови з загальної причини для обраних елементів;

– **версії технологій** {Versions} – версії технологій, що використовуються у даному елементі. Використовуються для визначення глибини версійної відмінності між шляхами;

– **тег** Tag – означає додаткову інформацію, зокрема початок та кінець шляху (“param” та “source”).

Крім графу мережі, до складу моделі входить інформація про технології, що використовуються в елементах. Кожна технологія $tech \in Tech$ описується часом напрацювання на відмову, переліком версій та версійною відмінністю (глибиною диверсності):

$$tech = \{MTTF, \{Version, D\}\}. \quad (8)$$

Ці властивості мають наступні значення:

– час напрацювання на відмову MTTF – прогнозований час напрацювання на відмову, що є наслідком застосування даної технології. Ця величина визначається за статистичною інформацією або за документацією виробника елементу. З цього показника отримується **інтенсивність відмов елементу** λ:

$$\lambda = \frac{1}{MTTF}, \quad (9)$$

– **масив пар значень версії та диверсності** {*Version, D*} характеризує наявні версії даної технології та їх версійні відмінності. В цьому масиві присутня мінімум одна базова версія 0 з показником диверсності $D = 0$, для якої визначений базовий час напрацювання на відмову. Для інших версій значення D представлене цілими значеннями від 1 до 4, яке характеризує версійну відмінність у порівнянні з базовою.

В якості версійної відмінності між парою версій технології застосовується максимальне значення показника D для заданої пари версій:

$$D(v1, v2) = \max\big(D(v1), D(v2)\big). \quad (10)$$

В залежності від виду елемента, число D формується у відповідності до методології, описаної вище.

Приклади відомостей про технології та їх базовий час напрацювання на відмову приведений в таблиці 1.

Таблиця 1 – Приклади відомостей про технології та їх базовий час напрацювання на відмову

Найменування технології	**Код**	**Час напрацювання на відмову**
Мова програмування	1	1020
…	…	…
Мережевий протокол	3	920
…	N	

Джерело: розроблено авторами

Приклад версійної відмінності між різними версіями технології (мова програмування високого рівня) приведений в таблиці 2.

Таблиця 2 – Приклад версійної відмінності між різними версіями технології (мова програмування високого рівня)

Version	0 (C++11)	1 (C++14)	2 (C++20)	C#	Python
D	0	1	1	2	4

Джерело: розроблено авторами

Версійна віддаленість може бути представлена у вигляді геометричної форми. Якщо позначити кожну окрему версію точками, то відстань між точками є пропорційною до версійної віддаленості відповідно до (2.4).

Наприклад, для трьох версій, одна з яких базова ($D = 0$), друга – відрізняється незначно ($D = 1$), а третя – радикально ($D = 4$), геометрична форма відображається як трикутник, приведений на рисунку 5.

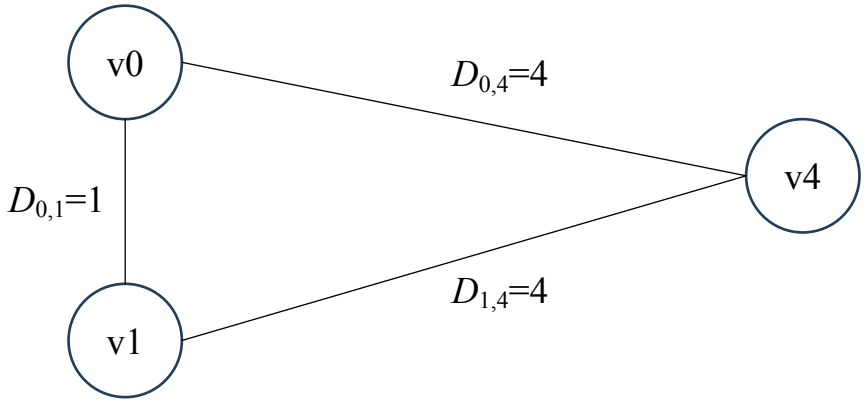

Рисунок 5 – Версійна відмінність у графічній формі

Джерело: розроблено авторами

Висновки. У даному дослідженні було показано, що при забезпеченні відмовостійкості системи підтримки оператора АЕС необхідно використовувати такі підходи як резервування, голосування та багатоверсійність.

Було показано, що вхідні дані до системи підтримки можуть надходити різними шляхами, що складаються з множини елементів.

Створено модель вхідних шляхів у вигляді графу, вершини якого визначають елементи шляхів, а ребра – напрямки передачі інформації. Дана модель включає в себе інформацію про базову інтенсивність відмов технологій елементів та їх версійну відмінність.

У подальших дослідженнях буде розглянутий аналіз відмовостійкості шляхів вхідних даних та розроблений метод вибору комбінації шляхів для максимізації відмовостійкості та мінімізації відмов в загальної причини в системі підтримки оператора АЕС.

Список літератури

1. Вінтенко Б., Миронець І., Смірнов О., Коваленко А., Конопліцька-Слободенюк О., Смірнова Т., Константинова Л. Дослідження застосування систем підтримки оперативного персоналу об’єкту критичної інфраструктури при керуванні енергоблоком АЕС з реактором типу ВВЕР-1000. *Кібербезпека: освіта, наука, техніка*. 2024. № 2(26). С. 6–26. URL: https://doi.org/10.28925/2663-4023.2024.26.673 (дата звернення: 11.04.2025).
2. Shooman M. *Reliability of Computer Systems and Networks: Fault Tolerance, Analysis, and Design*. JOHN WILEY & SONS, INC., 2002. URL: http://dx.doi.org/10.1002/047122460X.fmatter_indsub (дата звернення: 11.04.2025).

3. Kumar V., Singh L., Tripathi A. K. Reliability analysis of safety-critical and control systems: a state-of-the-art review. *IET Software*. 2018. Vol. 12. P. 1–18. URL: https://doi.org/10.1049/iet-sen.2017.0053 (дата звернення: 11.04.2025).
4. Харченко В. С. Гарантоздатні системи та багатоверсійні обчислення: аспекти еволюції. *Радіоелектронні і комп'ютерні системи*. 2009. № 7. С. 46–59. URL: http://nbuv.gov.ua/UJRN/recs_2009_7_9 (дата звернення: 11.04.2025).
5. Kharchenko V. S., Bakhmach E. S., Siora A. A., Sklyar V. V., Tokarev V. I. Diversity-Oriented FPGA-Based NPP I&C Systems: Safety Assessment, Development, Implementation. *Proc. of the 18th Int. Conf. on Nuclear Engineering (ICONE18)*. Xi'an, China. 2010. Vol. 1. P. 755–764. URL: https://doi.org/10.1115/ICONE18-29754 (дата звернення: 11.04.2025).
6. Lyu M., Jia-hongchen, Avizienis A. Experience in Metrics and Measurements for N-Version Programming. *International Journal of Reliability, Quality and Safety Engineering*. 1994. Vol. 1, № 1. P. 41–62. URL: https://doi.org/10.1142/S0218539394000052 (дата звернення: 11.04.2025).
7. Avizienis A. The Methodology of N-Version Programming. 1995.
8. Jones H. Common Cause Failures and Ultra Reliability. *42nd International Conference on Environmental Systems*. AIAA 2012-3602. 2012.
9. Strigini L., Littlewood B. A discussion of practices for enhancing diversity in software designs. London: Centre for Software Reliability, City University London, 2000. URL: https://openaccess.city.ac.uk/id/eprint/275/ (дата звернення: 11.04.2025).
10. Бахмач Є. С., Герасименко О. Д., Головір В. А., Сіора О. А., Скляр В. В., Токарєв В. І., Харченко В. С. Стійкі до відмов інформаційно-керуючі системи на програмованій логіці. Харків–Кіровоград : НАУ «ХАІ», НВП «Радій», 2008.
11. Вінтенко Б. Ю., Смірнов О. А., Коваленко О. В., Смірнов С. А., Коваленко А. С. Дослідження нормативних документів та галузевих стандартів розробки програмного забезпечення комп'ютерних систем управління АЕС, важливих для безпеки. *Системи управління, навігації та зв'язку*. 2023. Вип. 2(72). С. 170–178. URL: https://doi.org/10.26906/SUNZ.2023.2.170 (дата звернення: 11.04.2025).
12. Вінтенко Б. Ю., Смірнов О. А., Коваленко А. С., Смірнов С. А., Буравченко К. О. Дослідження вимог міжнародних стандартів IEC60880 та IEC62138 з розробки програмного забезпечення інформаційно-керуючих систем АЕС, важливих для безпеки. *Системи управління, навігації та зв'язку*. 2023. Вип. 3(73). С. 155–166. URL: https://doi.org/10.26906/SUNZ.2023.3.155 (дата звернення: 11.04.2025).
13. Вінтенко Б., Миронець І., Смірнов О., Кравчук О., Козірова Н., Савеленко Г., Коваленко А. Дослідження вимог та аналіз кібербезпеки програмного забезпечення інформаційно-керуючих систем АЕС, важливих для безпеки. *Кібербезпека: освіта, наука, техніка*. 2024. № 3(23). С. 111–131. URL: https://doi.org/10.28925/2663-4023.2024.23.111131 (дата звернення: 11.04.2025).
14. Вінтенко Б. Ю., Миронець І. В., Смірнов О. А., Коваленко О. В., Смірнов С. А., Буравченко К. О., Якименко Н. М. Дослідження інформаційного забезпечення та технологічних регламентів процесів керування критичною інфраструктурою енергоблоку АЕС з реактором типу ВВЕР-1000. *Кібербезпека: освіта, наука, техніка*. 2024. № 1(25). С. 253–278. URL: https://doi.org/10.28925/2663-4023.2024.25.253278 (дата звернення: 11.04.2025).

References

1. Vintenko, B., Myronets, I., Smirnov, O., Kovalenko, A., Konoplytska-Slobodeniuk, O., Smirnova, T., Konstantinova, L. (2024) "Study of the application of support systems for operational personnel of a critical infrastructure facility when managing a nuclear power plant unit with a VVER-1000 reactor". Electronic professional scientific publication "Cybersecurity: education, science, technology", No. 2(26), pp. 6-26. URL: https://doi.org/10.28925/2663-4023.2024.26.673 [in Ukrainian].
2. Shooman M. (2002). Reliability of Computer Systems and Networks: Fault Tolerance, Analysis, and Design. JOHN WILEY & SONS, INC. URL: http://dx.doi.org/10.1002/047122460X.fmatter_indsub
3. Kumar, V., Singh, L. and Tripathi, A.K. (2018), Reliability analysis of safety-critical and control systems: a state-of-the-art review. IET Softw., 12: 1-18. URL: https://doi.org/10.1049/iet-sen.2017.0053
4. Kharchenko V. S. (2009) Warranty-ready systems and multi-version computing: aspects of evolution / V. S. Kharchenko // Radioelectronic and computer systems. No. 7. P.46-59. URL: http://nbuv.gov.ua/UJRN/recs_2009_7_9 [in Ukrainian].
5. Kharchenko, VS, Bakhmach, ES, Siora, AA, Sklyar, VV, & Tokarev, VI. (2010) "Diversity-Oriented FPGA-Based NPP I&C Systems: Safety Assessment, Development, Implementation." *Proceedings of the 18th International Conference on Nuclear Engineering. 18th International Conference on Nuclear Engineering: Volume 1*. Xi'an, China. May 17–21, pp. 755-764. ASME. URL: https://doi.org/10.1115/ICONE18-29754

6. Lyu, Michael & Jia-hongchen, & Algirdasavi Žienis,. (1994). Experience in Metrics and Measurements for N-Version Programming. International Journal of Reliability, Quality and Safety Engineering. Vol| 01. No 01. pp. 41-62. URL: https://doi.org/10.1142/S0218539394000052
7. Avizienis, Algirdas. (1995). The Methodology of N-Version Programming.
8. Harry Jones. (2012) "Common Cause Failures and Ultra Reliability," AIAA 2012-3602. *42nd International Conference on Environmental Systems*.
9. Strigini, L. & Littlewood, B. (2000). A discussion of practices for enhancing diversity in software designs. London, UK: Centre for Software Reliability, City University London. URL: https://openaccess.city.ac.uk/id/eprint/275/
10. Bakhmach E. S., Gerasimenko O. D., Golovir V. A., Siora O. A., Sklyar V. V., Tokarev V. I., Kharchenko V. S. (2008) "Fault-Resistant Information and Control Systems Based on Programmable Logic." NAU "Khayar", Scientific Research Enterprise "Radius", Kharkiv-Kirovograd.
11. Vintenko B.Yu., Smirnov O.A., Kovalenko O.V., Smirnov S.A., Kovalenko A.S. (2023) "Study of regulatory documents and industry standards for the development of software for computer control systems of nuclear power plants important for safety". Control, navigation and communication systems, issue 2(72), pp. 170-178. URL: https://doi.org/10.26906/SUNZ.2023.2.170 [in Ukrainian]
12. Vintenko B.Yu., Smirnov O.A., Kovalenko A.S., Smirnov S.A., Buravchenko K.O. (2023) "Study of the requirements of international standards IEC60880 and IEC62138 for the development of software for information and control systems of nuclear power plants important for safety". Control, navigation and communication systems, issue 3(73), pp. 155-166.URL: https://doi.org/10.26906/SUNZ.2023.3.155 [in Ukrainian].
13. Vintenko, B., Myronets, I., Smirnov, O., Kravchuk, O., Kozirova, N., Savelenko, G., Kovalenko, A. (2024) "Research on requirements and analysis of cybersecurity of software of information and control systems of nuclear power plants important for safety". Cybersecurity: education, science, technology. No. 3(23), pp. 111-131. URL: https://doi.org/10.28925/2663-4023.2024.23.111131 [in Ukrainian].
14. Vintenko B.Yu., Myronets I.V., Smirnov O.A. Kovalenko O.V., Smirnov S.A., Buravchenko K.O., Yakymenko N.M. (2024) "Study of information support and technological regulations of critical infrastructure control processes of a nuclear power plant with a VVER-1000 reactor". Electronic professional scientific publication "Cybersecurity: education, science, technology". No. 1(25), pp. 253–278. URL: https://doi.org/10.28925/2663-4023.2024.25.253278 [in Ukrainian].

Borys Vintenko[1,2], **Oleksii Smirnov**[3], Prof., Dr. tech. sci., **Iryna Myronets**[1], Assoc. Prof., PhD tech. sci., **Tetiana Smirnova**[3], PhD tech. sci., **Oleksandr Kovalenko**[3], Prof., Dr. tech. sci., **Anatolii Matsui**[3], Prof., Dr. tech. sci.
[1]*Cherkasy State Technological University, Cherkasy, Ukraine*
[2]*PJSC "Scientific and Production Enterprise "Radius", Kropyvnytskyi, Ukraine*
[3]*Central Ukrainian National Technical University, Kropyvnytskyi, Ukraine*

Model of Ways to Obtain Input Data for a Computer Intelligent System to Support Operational Personnel of a Nuclear Power Plant

This article investigates methods for increasing the fault tolerance of a computer intelligent support system for a nuclear power plant operator. The purpose of this study is to increase the fault tolerance of intelligent support systems for the operator when receiving information about the state of technological parameters important for the power plant control procedures. The object of the study is the ways of receiving input data by a computer intelligent support system for a nuclear power plant operator. The subject of the study is a model of the ways of receiving input information to a computer intelligent support system for a nuclear power plant operator. The problem of ensuring the reliability of input information and methods for solving it, which are based on the redundancy and multi-version of the components used, is considered. A simulation model of the input data paths of a computer intelligent support system for a nuclear power plant operator has been developed, which differs from the known ones by taking into account the indicators of multi-version of components.

decision support system, redundancy, fault tolerance, reliability, multi-versioning, simulation model

Одержано (Received) 11.04.2025 *Прорецензовано (Reviewed) 02.05.2025*
Прийнято до друку (Approved) 06.05.2025