УДК 004.65

д.т.н., доц. **Собчук В.В.** (ДУТ)
д.т.н., проф. **Барабаш О.В.** (НТУ«КПІ»)
д.т.н., доц. **Мусієнко А.П.** (НТУ«КПІ»)

DOI: https://doi.org/10.17721/2519-481X/2021/70-08

ВПЛИВ МЕТОДУ АДАПТИВНОГО САМОДІАГНОСТУВАННЯ НА ПРОЦЕС ПОПЕРЕДЖЕННЯ НАСЛІДКІВ ВІДМОВ МОДУЛІВ ІНФОРМАЦІЙНОЇ СИСТЕМИ ПІДПРИЄМСТВА

У роботі продовжуються дослідження властивості функціональної стійкості. Під функціональною стійкістю розуміється властивість інформаційної системи зберігати функціонування, можливо із зменшенням якості, протягом вказаного часу під впливом зовнішніх і внутрішніх дестабілізуючих факторів. Під зовнішніми та внутрішніми дестабілізуючими факторами розуміються відмови, збої модулів системи, механічні пошкодження, теплові впливи, помилки обслуговуючого персоналу. Основними етапами забезпечення функціональної стійкості є виявлення модуля, який відмовив при контролі, діагностування модуля, який відмовив та відновлення функціонування інформаційної системи підприємства. Особливістю інформаційних систем підприємств є те що вони повинні функціонувати автономно. За їх допомогою можна забезпечити підвищення продуктивності праці усіх виробничих центів при зменшенні числа зайнятих у виробництві людей та значному зменшенні частки ручної праці.

У роботі досліджується, як на основі функціональної залежності ймовірності пропуску відмов від певного значення ймовірності при різних значеннях ймовірність помилки контролю другого роду можна визначити рекомендований інтервал видачі результату, який забезпечить, при даній інтенсивності контролю готовності допустиму ймовірність пропуску відмови. Ілюструється як при заданій інтенсивності видачі результату можна визначити таку інтенсивність контролю готовності при якій ймовірність пропуску не буде перевищувати максимально допустимого значення. Показано, що можна говорити про слабку залежність ймовірності пропуску від помилки контролю другого роду, що означає, що досягнення заданої достовірності контролю забезпечується на основі інтенсивності контролю готовності і менше залежить від достовірності окремих елементарних перевірок. Для випадку коли в проміжках між моментами видачі результату системою контроль готовності модулів відбувається випадковим чином описано методику розрахунку ймовірності пропуску.

Ключові слова: функціональна стійкість, діагностування, адаптивне діагностування, структура перевірочних зв'язків, синдром, контроль готовності.

Вступ та постановка задачі. Розвиток сучасного суспільства вимагає інтенсивного розвитку інформаційних технологій з високим ступенем автономності. Особливо гостро ця проблематика стосується виробничих підприємств, які функціонують в умовах впливу екстремальних факторів. Серед таких підприємств вирізняються підприємства металургії, енергетики, хімічної промисловості тощо. Функціонування виробничих підрозділів таких підприємств забезпечують інформаційні системи різного типу. За допомогою цих систем здійснюється планування та контроль усіх процесів [1]. Вони працюють в автономному режимі під впливом зовнішніх та внутрішніх дестабілізуючих факторів [2–4]. За допомогою інформаційних систем підприємства (ІСП) можна забезпечити підвищення продуктивності праці усіх виробничих центів при зменшенні числа зайнятих у виробництві людей та значному зменшенні частки ручної праці [5,6]. Системи постійно модернізуються завдяки інтенсифікації капіталовкладень у виробничий процес.

Аналіз останніх досліджень. Як вже було підкреслено, інформаційні системи підприємств функціонують в умовах впливу зовнішніх та внутрішніх дестабілізуючих факторів. За негативного впливу модулі систем можуть виходити з ладу. Проте, системи повинні функціонувати в автономному режимі протягом заданого часу. Таку умову функціонування можна виконати завдяки забезпеченню властивості функціональної стійкості. Функціональна стійкість – це запорука функціонування інформаційної системи, можливо із

зменшенням якості, протягом вказаного часу під впливом зовнішніх і внутрішніх дестабілізуючих факторів [8,9]. Під зовнішніми та внутрішніми дестабілізуючими факторами розуміються відмови, збої модулів системи, механічні пошкодження, теплові впливи, помилки обслуговуючого персоналу. Основними етапами забезпечення функціональної стійкості є виявлення модуля, який відмовив при контролі, діагностування модуля, який відмовив та відновлення функціонування інформаційної системи підприємства.

Відтак однією з найголовніших передумов забезпечення функціональної стійкості є побудова ефективної системи діагностування та самодіагностування ключових агрегатів на кожному виробничому центрі виробничого підприємства [7].

Метою роботи є розробка методу діагностування складних технічних систем. Основна відмінність запропонованого методу полягає в новому підході до виконання процедури діагностування інформаційної системи підприємства. Основна суть якого полягає в такому:

по-перше, процедура діагностування може бути закінчена в будь який момент часу; по-друге, вільному виборі модуля, який приймає рішення про стан інформаційної системи підприємства.

Виклад основного матеріалу. Коли система працює за призначенням перевірки відбуваються випадковим чином. Випадковість стосується вибору пари модулів, що перевіряють один одного та часу перевірки між ними. Тому після деякого часу в інформаційній системі може бути здійснено довільну кількість елементарних перевірок. Оцінка стану інформаційної системи підприємства на основі елементарних перевірок може бути представлена у вигляді двох методів:

- методу самоконтролю;
- методу адаптивного самодіагностування.

Адаптивність полягає в тому, що даний метод пристосовується до відмовної ситуації в інформаційній системі. При цьому діагностична інформація про стан модулів накопичується хаотичним чином. Обсяг такої інформації залежить від відмовної ситуації. Після накопичення інформації про стан системи отримана інформація обробляється і виявляється несправність із достовірністю не нижче заданої.

Метод самоконтролю використовуємо з метою перевірки наявності в інформаційній системі несправних модулів [10]. У випадку виявлення несправних модулів використовується метод адаптивного самодіагностування. На основі даного методу локалізується знаходження несправного модуля інформаційної системи підприємства.

Однією із задач є визначення моменту закінчення роботи методу самоконтролю і видачі результату у випадку коли, результат всіх елементарних перевірок показує, що несправні модулі відсутні. При цьому результат контролю має певну достовірність, яка залежить від надійності модулів інформаційної системи та кількості виконаних перевірок.

Під час функціонування інформаційної системи підприємства за призначенням модулі системи окрім основних задач виконують взаємні перевірки [11]. Період часу між двома послідовними видачами результату контролю інформаційної системи назвемо циклом самоконтролю. Цикл виконується або заданий час або задану кількість разів. Якщо під час виконання циклу самоконтролю не було отримано жодної елементарної перевірки, результат якої свідчить про наявність несправності в модулях системи, то видається результат самоконтролю тобто інформація, що система працює в штатному режимі. Після видачі результатів самоконтролю починається новий цикл перевірок. У випадку, коли під час виконання методу самоконтролю один з результатів елементарних перевірок виявляє несправність, то цикл самоконтролю припиняється і розпочинається робота методу адаптивного самодіагностування.

В залежності від того, який момент часу приймається за початок процедури адаптивного самодіагностування, можливі дві стратегії адаптивного самодіагностування.

Перша стратегія. Метод адаптивного самодіагностування починається в момент початку останнього циклу самоконтролю t_k. При цьому враховуються елементарні перевірки виконані за час τ. Згідно даної методики після появи результату елементарної перевірки, що

показує наявність несправності в інформаційній системі підприємства, результати отримані до цього часу не аналізуються й апріорні ймовірності справного стану модулів системи на момент часу t_0 не визначаються. Дешифрація синдрому здійснюється після закінчення роботи методу адаптивного самодіагностування.

Друга стратегія. Метод адаптивного самодіагностування починається в момент часу t_0. На основі результатів елементарних перевірок, які виконані за час τ, визначаються апріорні ймовірності справності модулів інформаційної системи підприємства. Після виконання методу адаптивного самодіагностування обчислюються апріорні ймовірності справного та несправного стану модулів на основі якого формується результат адаптивного самодіагностування та визначається його достовірність.

Розробка методу адаптивного самодіагностування інформаційної системи підприємства. Важливим є випадок коли допускається робота несправного модуля на протязі деякого часу, а також коли відключення підозрілої пари від виконання роботи і забезпечення їхньої участі тільки в елементарних перевірках (з обмеженням на перевірки між ними) викликає деякі складності. За таких обставин стає можливим застосувати відмінну від вищезгаданих стратегій.

Третя стратегія адаптивного самодіагностування: після отримання одиничного результату однією з елементарних перевірок процедура виконання взаємних перевірок в інформаційній системі підприємства продовжується на протязі наперед заданого часу t_d.

Після завершення даного часу проводиться аналіз отриманого синдрому на основі якого або вказується несправний модуль (у випадку коли достовірність діагностування менше заданої), або процедура виконання елементарних перевірок продовжується, або виключається пара підозрілих модулів. Час t_d визначається з розрахунку отримання *структури перевірочних зв'язків* (СПЗ), яка характеризується встановленою достовірністю діагностування (ймовірністю правильного самодіагностування).

Адаптивне самодіагностування, яке ґрунтується на виключені підозрілої пари модулів від виконання поточних завдань також зводиться до отримання СПЗ з заданими характеристиками. Проте, в даному випадку при визначені ймовірності утворення характерної СПЗ необхідно враховувати обмеження на виконання елементарних перевірок, що ускладнює дану задачу.

Розглянемо метод адаптивного самодіагностування заснований на третій стратегії.

Припускається, що однієї елементарної перевірки достатньо щоб визначити стан модуля, що перевіряється при умові коли перевіряючий модуль справний. Тоді для виконання методу адаптивного самодіагностування необхідно ідентифікувати структуру перевірочних зв'язків в якій справні модулі перевіряють усі інші модулі інформаційної системи підприємства. Ймовірність правильного адаптивного самодіагностування P_{AS} розглядається як ймовірність утворення такої структури перевірочних зв'язків.

Визначення ймовірності правильного адаптивного самодіагностування. Серед всіх модулів системи визначимо групу модулів (домінуючу підмножину), яка буде перевіряти всі інші модулі інформаційної системи підприємства. Таку структуру перевірочних зв'язків (СПЗ) назвемо достатньою структурою. Якщо ця домінуюча підмножина виявиться справною, то результат адаптивного самодіагностування буде правильним.

Процедура правильного адаптивного самодіагностування є складною та визначається двома подіями:

- подія, суть якої полягає в тому, що буде утворена достатня СПЗ (структура з необхідною кількістю вершин, які утворюють домінуючу підмножину);
- подія, суть якої полягає в тому, що домінуючі модулі після дешифрації синдрому будуть визнані справними.

Нехай X_i, $i=1,2,...n$, $n \in N$ подія утворення СПЗ, де домінуючою підмножиною є множина з i модулів. Для кожного значення i визначається мінімальна домінуюча структура $G_i(D_i,T_i)$, яка є частиною графа $G(D,T)$ та задовольняє наступні властивості:

1. $|V_i| = i, \quad T_i \subseteq T$

2. Будь-яка вершина з $\bar{D}_i$ отримує хоча б одне ребро з D_i .

3. Видалення будь-якого ребра з T_i суперечить властивості 2.

Оскільки структур з домінуючою підмножиною модулів можна утворити декілька, то ймовірність P_{AS} визначається наступним чином

$P_{AS} = P\{Y_1 \cup Y_2 \cup ... \cup Y_n\},$

де Y_i, $i = 1, 2, ... n$, $n \in N$ – подія, яка полягає в тому, що в результаті виконання елементарних перевірок утворюється структура G_i зі справною домінуючою підмножиною модулів D_i.

Оскільки події $Y_1, Y_2, ..., Y_n$ сумісні та незалежні має місце рівність

$$P_{AS} = 1 - \prod_{i=1}^{n} [1 - (Y_i)]. \qquad (1)$$

Ймовірність $P(Y_i), \quad i = 1, ..., n$ можна представити у вигляді

$P(Y_i) = P\{Z_{i1} \cup Z_{i2} \cup ... \cup Z_{im}\},$

де Z_{ij} – подія, суть якої полягає в тому, що в результаті виконання елементарних перевірок утворюється структура G_{ij} зі справною домінуючою підмножиною модулів D_j , яка складається з i модулів.

Події Z_{ij}, $i = 1, ..., n, \quad j = 1, ..., m$ сумісні та незалежні. Тому для ймовірності $P(Y_i)$ можна записати

$$P(Y_i) = 1 - \prod_{j=1}^{m} [1 - P(Z_{ij})].$$

Ймовірність події Z_{ij} для системи, яка складається з однакових модулів визначається

$P(Z_{ij}) = P_M^i \cdot R(G_{ij}),$

де P_M – ймовірність справного стану модулів інформаційної системи підприємства $R(G_{ij})$ – ймовірність утворення структури $G_{ij} \quad i = 1, ..., n, \quad j = 1, ..., m, \quad n, m \in N$.

Ймовірність утворення достатніх структур перевірочних зв'язків. В якості вихідної інформації для визначення достатніх структур можуть використовуватись:

- кількість перевірок в інформаційній системі підприємства;
- значення локальних степенів вершини діагностичного графу ІСП;
- матриця суміжності діагностичного графу (ДГ).

Якщо матриця суміжності ДГ не відома, то тоді потрібно використати ймовірнісний підхід до визначення наявності в ДГ достатніх структур.

Ймовірність утворення достатніх структур G_{ij} на основі використання локальних степенів вершин ДГ може бути визначена при наступних умовах:

1) обмежень на виконання елементарних перевірок немає;

2) є лише одне обмеження на виконання елементарних перевірок – не допускаються кратні ребра в ДГ;

3) є два обмеження на виконання елементарних перевірок – це не допускаються кратні ребра в ДГ і якщо $v_j \in \Gamma(v_i)$, то $v_i \notin \Gamma(v_j)$ для $i, j = 1, ..., N, \quad i \neq j$, $v_i, v_j \in V$, де V – множина вершин ДГ;

4) є обмеження – в ДГ не повинно бути ребер між вершинами v_i та v_j .

Для випадків 1)–4) вважаємо, що вершини не мають петель тобто виключаємо можливість самоперевірки модуля.

Для випадку коли не має обмежень на виконання елементарних перевірок основною для визначення ймовірності $R(G_{ij})$ є наступна формула

$$s = \sum_{i=1}^{\omega} \alpha_i^+ - \Omega ,$$

де s – кількість ребер, що йде від домінуючої підмножини вершин D_i до вершин графа G_{ij} , які залишилися; ω – кількість вершин в домінуючій підмножині D_i; α_i^+ – кількість ребер, що виходять з *i*-тої вершини графа G_{ij}; Ω – сумарна кількість взаємних перевірок між модулями, які утворюють домінуючу підмножину D_i.

В якості додаткового графа розглянемо граф H_{ij}, який утворюється з графа G_{ij} шляхом додавання ребра в граф, що утворює домінуючу підмножину вершин D_i. Таким чином щоб ця частина $G(D_i)$ представляла повний граф.

Позначимо ребра в графі H_{ij} через b_{ij} і поставимо їм у відповідність випадкові величини ζ_{ij}. Випадкова величина ζ_{ij} може приймати значення

$$\zeta_{ij} = \begin{cases} 1 & \exists(v_i, v_j), \quad v_i, v_j \in V_H; \\ 0 & \overline{\exists}(v_i, v_j), \quad v_i, v_j \in V_H, \end{cases} \tag{2}$$

де V_H – множина вершин графа H_{ij}.

Далі складемо наступну суму

$$\zeta_{ij} = \zeta_{ij}^{(1)} + \zeta_{ij}^{(2)} + ... + \zeta_{ij}^{(k)} , \tag{3}$$

для всіх $i, j : v_i, v_j \in V_H$, $i \neq j$, де $\zeta_{ij}^{(l)}$ – випадкова величина, яка приймає значення 0 або 1 в залежності від того виконана чи ні елементарна перевірка τ_{ij} в l-му випробувані. Тут під випробуванням розуміється випадковий процес утворення перевірочних зв'язків між модулями інформаційної системи підприємства в проміжку часу τ .

Величина інтервалу часу τ вибирається за умови $t_{en} < \tau < \alpha$, де α – середній час зайнятості модуля системи. Експеримент повторюється k разів. Отже, загальний час накопичення елементарних перевірок складає $k\tau$.

Оскільки в кожній елементарній перевірці задіяно два модуля, то максимально в кожному експерименті може бути виконано q перевірок, де

$$q = \left[\frac{\omega}{2} \right].$$

Для визначення ймовірності утворення достовірних структур перевірочних зв'язків розглянемо випадок коли в системі може бути виконано не більше однієї елементарної перевірки одночасно.

Представимо ліві частини сум (3) у вигляді прямокутної матриці $[\zeta_{ij}]$ і виберемо з кожного її стовпця 0 або 1 елемент. Визначимо загальне число γ різних варіантів вибору елементів матриці розмірності $[r \times k]$ (по 0 або 1 з кожного стовпця матриці $[\zeta_{ij}]$). Для цього спочатку розглянемо кількість варіантів в яких є 1 елемент, 2 елементи, …, k елементів.

Позначимо дані величини через $Q_1, Q_2, ..., Q_k$. Можна показати, що

$$Q_1[r\times k]=r\cdot k;$$
$$Q_2[r\times k]=r\cdot\sum_{i=1}^{k-1}Q_1[r\times(k-i)];$$
$$Q_3[r\times k]=r\cdot\sum_{i=1}^{k-2}Q_2[r\times(k-i)]; \quad (4)$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$Q_k[r\times k]=r\cdot Q_{k-1}[r\times(k-1)],$$

де $r,\ k$ – кількість рядків та стовпців матриці $[\zeta_{ij}]$ відповідно.

На основі $Q_1[r\times k], Q_2[r\times k],\ldots, Q_k[r\times k]$ визначається загальне число різних варіантів вибору елементів із початкової матриці з 0 або 1 елемента з кожного стовпця:

$$\gamma=\sum_{j=1}^{k}Q_j\ .$$

Для кожного варіанту $U_m,\quad m=1,\ldots,\gamma$ вибору елементів з вихідної матриці утворимо нову суму $\mu_m=\sum\varsigma_{ij},$ де $\varsigma_{ij}\in U_m$.

Введемо подію $A_i^{\beta}=\{\mu_i=\beta\}$. Тоді для випадкової величини Ω

$$P(\Omega=\beta)=P\{A_1^{\beta}\cup A_2^{\beta}\cup\ldots\cup A_{\gamma}^{\beta}\}\ . \quad (5)$$

Оскільки події $A_1^{\beta}, A_2^{\beta},\ldots, A_{\gamma}^{\beta}$ сумісні і незалежні вираз (5) можна представити у вигляді

$$P(\Omega=\beta)=1-\prod_{j=1}^{\gamma}[1-P(A_j^{\beta})]\ . \quad (6)$$

Ймовірність $P(A_j^{\beta})$ знаходиться як ймовірність того, що сума біноміальних випадкових величин буде дорівнювати певному значенню. При цьому враховуються всі ймовірності $P\{\varsigma_{ij}^{(l)}=1\}$ для $l=1,\ldots,k$ рівні $P_{\varsigma}=\dfrac{1}{N(N-1)}$. Тоді

$$P(A_i^{\beta})=C_{K_j}^{\beta}\cdot P_{\zeta}^{\beta}(1-P_{\zeta})^{K_j-\beta}, \quad (7)$$

де K_j – кількість сумованих елементів для μ_j .

Враховуючи те, що кількість сум з одним елементом дорівнює Q_1, з двома – Q_2, з k елементами – Q_k, перетворимо (5) наступним способом

$$P(\Omega=\beta)=1-\prod_{i=1}^{k}[1-C_i^{\beta}P_{\zeta}^{\beta}(1-P_{\zeta})^{i-\beta}]^{Q_i}\ . \quad (8)$$

На основі виразу (8) визначається функція розподілу випадкової величини Ω тобто $P(\Omega<\beta)$ для $\beta=1,2,\ldots,r$.

Введемо наступне позначення $\Omega_{\beta}=(\Omega=\beta)$ і $S_{\beta}=L-\Omega_{\beta}$, де $L=\sum_{i=1}^{\omega}\alpha_i^{+}$. Тоді

$$P_{S_{\beta}}=P\{S<S_{\beta}\}=P\{S<L-\Omega_{\beta}\}=P(\Omega<\beta),\ \text{де}\ \beta=0,1,\ldots,r\ . \quad (9)$$

Далі для кожного значення S_{β} визначається ймовірність того, що всі вершини, які не входять в домінуючу підмножину D_i, отримують хоча б одне ребро з D_i .

Позначимо таку ймовірність R_{S_β}. Вона знаходить повторні випадки розподілу, коли кожний експеримент може мати $M = N - \omega$ виключаючи один одного з рівними ймовірностями $P = \frac{1}{M}$. В даному випадку під експериментом розуміється розподіл одного ребра між вершинами, які не входять в D_i.

Ймовірність R_{S_β} можна знайти наступним чином

$$R_{S_\beta} = \sum P_{m_1, m_2, ..., m_M; s_\beta} \text{ , де } \prod_{i=1}^{M} m_i \geq 1, \quad \sum_{i=1}^{M} m_i = S_\beta \ . \tag{10}$$

Сума поширюється на всі можливі способи розбиття числа S_β на M доданків $m_1, m_2, ..., m_M$ $(0 \leq m_j \leq S_\beta, \ j = 1, ..., M)$. Сумовані ймовірності дорівнюють

$$P_{m_1, m_2, ..., m_M; s_\beta} = \frac{S_\beta !}{m_1 ! m_2 ! ... m_M !} \cdot \frac{1}{M^{S_\beta}} .$$

Для розглянутого випадку ймовірність $R(G_{ij})$ знаходиться за формулою повної ймовірності

$$R(G_{ij}) = \sum_{S_\beta = M}^{K} R_{S_\beta} \cdot P_{S_\beta} ,$$

де ймовірності R_{S_β} та P_{S_β} знаходяться з виразів (8) та (9) відповідно.

Значення ймовірності $R(G_{ij})$, яке характеризує СПЗ та кількісний показник надійності окремих модулів інформаційної системи підприємства дозволяє визначити ймовірність правильного адаптивного самодіагностування P_{AS}.

Таким чином, на основі проведених досліджень отримано ймовірність P_{AS}, яка характеризує достовірність адаптивного самодіагностування і є початковою величиною для організації методу адаптивного самодіагностування інформаційної системи підприємства.

Дослідження впливу методів контролю та адаптивного самодіагностування на процес попередження наслідків відмов модулів інформаційної системи підприємства.

В більшості випадків функціональний контроль системи здійснюється завдяки забезпеченню неперервного *контролю обчислювального процесу* (КОП). Типовим прикладом такого контролю є використання мажоритарних структур. Однак, для неперервного контролю обчислювального процесу характерні всі недоліки функціонального контролю ІСП. Тому потрібно використовувати інші типи контролю.

Одним зі способів вирішень проблеми контролю на протязі часу коли ІСП використовується за призначенням є перехід від неперервного КОП до часткового або періодичного. Такий контроль може бути виконаний на основі апаратних і програмних способів контролю. При частковому контролі обчислювального процесу є ймовірність неправильного розв'язання задачі. Проте, з'являється можливість організації взаємного контролю (контролю готовності (КГ)) модулів ІСП. Це дозволяє значно зменшити ймовірність видачі неправильного результату модулями ІСП.

Ймовірність видачі неправильного результату позначимо через P_r та визначимо таким способом

$$P_r = P\{A_1 \cup A_2\} = P_{A_1} + P_{A_2} ,$$

де

$$P_{A_1} = P_{X_0} P(X_1 / X_0) P(X_2 / X_0 X_1) P(X_3 / X_0 X_1 X_2); \tag{11}$$

$$P_{A_2} = P_{\bar{X}_0} P(X_1 / \bar{X}_0) P(X_2 / \bar{X}_0 X_1) P(X_3 / \bar{X}_0 X_1 X_2). \quad (12)$$

Через X_0, $\bar{X}_0$, X_i, $i = 1,2,3$ позначимо події: X_0 – інформаційна система підприємства несправна; X_1 – в результаті контролю готовності (КГ) ІСП визнана справною; X_2 – виникає порушення обчислювального процесу; X_3 – в результаті виконання КОП відхилень в результатах обчислювального процесу не виявлено. Ймовірності в формулах (11) та (12) дорівнюють відповідно

$$P_{X_0} = 1 - P_0; \quad P(X_1 / X_0) = \beta; \quad P(X_2 / X_0 X_1) = P_1; \quad P(X_3 / X_0 X_1 X_2) = P_w; \quad (13)$$

$$P_{\bar{X}_0} = P_0; \quad P(X_1 / \bar{X}_0) = 1 - \alpha; \quad P(X_2 / \bar{X}_0 X_1) = P_s; \quad P(X_3 / \bar{X}_0 X_1 X_2) = 1 - P_w. \quad (13')$$

В формулах (13) – (13') прийняті наступні позначення: $P_0 -$ ймовірність справного стану ІСП в деякий момент часу; P_1 – ймовірність виникнення порушень обчислювального процесу внаслідок апаратної несправності ІСП. В загальному випадку $P_1 \to 1$; P_s – ймовірність порушення обчислювального процесу внаслідок випадкових збоїв; α – ймовірність помилки контролю першого роду (хибна тривога); β – ймовірність помилки контролю другого роду (прохід відмови); P_w – ймовірність виявлення відхилень в результаті обчислювального процесу при виконанні КОП. Тоді

$$P_r = (1 - P_0)(1 - P_w)\beta + (1 - \alpha)(1 - P_w) \cdot P_0 \cdot P_s. \quad (14)$$

У випадку, коли контроль готовності ІСП виконується на основі результатів взаємних перевірок між модулями системи можна вважати, що $\alpha = 0$, а $\beta = 1 - D$, де D – достовірність контролю. З врахуванням цього, (14) набуває вигляду

$$P_r = K + B - KD, \quad (14')$$

де

$$K = (1 - P_0)(1 - P_w); \qquad B = (1 - P_w) P_0 P_s.$$

Відтак, має місце твердження.

Твердження 1. *Ймовірність видачі неправильного результату слідуючи* (14') *можна представити у вигляді функціональної залежності від достовірності контролю, тобто* $P_r = \varphi(D)$. *При чому зменшення ймовірності* P_w *на деяку величину* ω *призведе до збільшення ймовірності* P_r *на деяку величину* μ, *де* $\mu = (1 - P_0)\omega + \xi$ *при* $D = 0$ *і на* $\xi = P_0 P_s \omega$ *при* $D = 1$.

Отже, при високій достовірності контролю системи $D \to 1$ можна понизити вимоги до КОП і при цьому ймовірність P_r збільшиться несуттєво (на величину ξ).

У випадку коли в проміжках між моментами видачі результату системою *контроль готовності* (КГ) модулів відбувається випадковим чином, то ймовірність $P(X_1 / X_0)$ обчислюється за наступною методикою.

Крок 1. Вихідна ймовірність представляється у вигляді

$$P(X_1 / X_0) = P\{E_1 \cup E_2\} = P_{E_1} + P_{E_2},$$

де E_1 – подія того, що в інтервалі часу R не буде контролю готовності $(S = 0)$; E_2 – подія того, що в інтервалі часу R буде контроль готовності S $(S \neq 0)$ та відмова не буде знайдена.

Крок 2. Кількість КГ, які можна виконати за час R, знаходиться як число відновлень за випадковий час. В даному випадку S можна знайти як

$$G(z) = \int_0^\infty G(t, z) f_R(t) dt, \quad (15)$$

де $f_R(t)$ – щільність розподілу випадкової величини R. В рівності (15) через $G(t,z)$ позначена твірна функції випадкової величини N_t (число КГ в інтервалі $(0,t)$).

Крок 3. Для випадку коли інтенсивність виникнення відмов стала, щільність розподілу випадкової величини R в інтервалі часу $[t_i, t_{i+1}]$ також стала й дорівнює

$$f_R(t) = \begin{cases} \dfrac{1}{\Delta t}, & при \quad t \le \Delta t \\ 0, & при \quad t > \Delta t, \end{cases} \tag{16}$$

де $\Delta t = t_{i+1} - t_i$, $t \ge 0$.

Крок 4. Для інформаційних систем підприємств з більшим числом модулів можна вважати, що випадкові величини проміжків часу між сусідніми КГ мають показниковий розподіл з параметром μ. Тому перетворення Лапласа твірної функції $G(t,z)$ має вигляд

$$G(p,z) = \frac{1}{p + \mu(1-z)}.$$

Перетворення $G(p,z)$ дозволяє отримати твірну функцію $G(t,z)$. Після підстановки $G(t,z)$ в (15) з врахуванням (16) отримаємо

$$G(z) = \frac{1}{\mu\Delta t(1-z)}\left[1 - e^{-\mu\Delta t(1-z)}\right].$$

Крок 5. Ймовірності P_{E_1} і P_{E_2} знаходяться як коефіцієнти при відповідних степенях Z^S розкладу функції $G(z)$ в ряд за степенями z.

$$P_{E_1} = G(0) = \frac{1 - e^{-\mu\Delta t}}{\mu\Delta t},$$

$$P_{E_2}(s) = f_S = \frac{1}{s!}\frac{d^s G(z)}{dz^s}\Big|_{z=0}.$$

Ймовірність того, що в інтервалі часу R буде S $(S \ne 0)$ КГ і відмова не буде виявлена можна обчислити за формулою повної ймовірності

$$P_{E_2} = \sum_{s=1}^{L} P_{E_2}(s)\beta^s.$$

Крок 5. Тоді шукана ймовірність $P(X_1 / X_0)$ обчислюється як

$$P(X_1 / X_0) = P_{E_1} + P_{E_2} = \frac{1 - e^{-\mu\Delta t}}{\mu\Delta t} + \sum_{s=1}^{L}\frac{1}{s!}\frac{d^s G(z)}{dz^s}\Big|_{z=0} \times \beta^s.$$

Необхідно зауважити, що оскільки значення β мале, то із збільшенням S функція $P_{E_2}(s)\beta^s$ швидко спадає. Тому можна обмежитися першими двома членами тобто $S = 1$ і $S = 2$. Відтак

$$P(X_1 / X_0) = \frac{1 - e^{-\mu\Delta t}}{\mu\Delta t} + \frac{1 - e^{-\mu\Delta t}(1 + \mu\Delta t)}{\mu\Delta t}\beta + \frac{2 - (2 + 2\mu\Delta t + \mu^2\Delta t^2)e^{-\mu\Delta t}}{\mu\Delta t}\beta^2.$$

На основі функціональної залежності ймовірності пропуску відмов від значення $\mu\Delta t$ при різних значеннях β можна визначити рекомендований інтервал видачі результату Δt, який забезпечить, при даній інтенсивності КГ (μ) допустиму ймовірність пропуску відмови $P(X_1 / X_0)$. Або при заданій інтенсивності видачі результату Δt можна визначити таку інтенсивність КГ μ при якій ймовірність $P(X_1 / X_0)$ не буде перевищувати максимально допустимого значення. Крім того можна говорити про слабку залежність ймовірності

$P(X_1 / X_0)$ від β. Це означає, що досягнення заданої достовірності контролю забезпечується на основі інтенсивності КГ і менше залежить від достовірності окремих елементарних перевірок. Справедливе твердження.

Твердження 2. *Якщо при жорсткому виконанні контролю готовності системи (тобто в строго фіксовані моменти часу) достовірність контролю кожного модуля була рівна* $D = 1 - \beta$, *то при випадкових виконаннях КГ достовірність визначається як* $D = 1 - P(X_1 / X_0)$. *Крім того, вона може бути підвищена до заданого значення за рахунок збільшення інтенсивності виконання КГ в проміжках часу між двома послідовними моментами видачі результатів. Інтенсивність виконання КГ залежить, переважно, від степеня завантаженості модулів інформаційної системи підприємства та часу виконання елементарних перевірок*.

Особливості об'єктів на яких встановлюються інформаційні системи вимагають для попередження відмов модулів використовувати і контроль обчислювального процесу, і контроль технічного стану апаратних можливостей ІСП. При цьому погіршення характеристик контролю обчислювального процесу може бути компенсоване за рахунок підвищення відповідних показників контролю технічного стану ІСП. Ефект компенсації залежить від кількості елементарних перевірок (чим більше елементарних перевірок тим краще). В умовах функціонування ІСП найбільш реальним способом збільшення кількості елементарних перевірок є організація даних перевірок хаотичним чином.

Висновки. В роботі показано, як на основі функціональної залежності ймовірності пропуску відмов від певного значення ймовірності при різних значеннях ймовірність помилки контролю другого роду можна визначити рекомендований інтервал видачі результату, який забезпечить, при даній інтенсивності контролю готовності допустиму ймовірність пропуску відмови. Проілюстровано як при заданій інтенсивності видачі результату можна визначити таку інтенсивність контролю готовності при якій ймовірність пропуску не буде перевищувати максимально допустимого значення. Крім того показано, що можна говорити про слабку залежність ймовірності пропуску від помилки контролю другого роду. Це означає, що досягнення заданої достовірності контролю забезпечується на основі інтенсивності контролю готовності і менше залежить від достовірності окремих елементарних перевірок. Для випадку коли в проміжках між моментами видачі результату системою контроль готовності модулів відбувається випадковим чином описано методику розрахунку ймовірності пропуску.

ЛІТЕРАТУРА:

1. Sobchuk A.V., Barabash O.V., Musienko A.P. Assessment methods of functional stability of wireless sensor networks. Науковий журнал «Телекомунікаційні та інформаційні технології». Київ: ДУТ, 2019. № 3 (64). С. 46 – 54.

2. Sobchuk Valentyn, Barabach Oleg, Musienko Andrii The algorithm of control pricing policy in trade networks on the market of ferrous metals. Науковий журнал «Телекомунікаційні та інформаційні технології». Київ: ДУТ, 2020. № 1 (66). С. 120 – 128.

3. Mashkov ., Bicanek J., Bardachov Y., Voronenko M. Unconventional Approach to Unit Self-diagnosis. Advances in Intelligent Systems and Computing, 2020, 1020, pp. 81 – 96.

4. Mashkov V., Fiser J., Lytvynenko V., Voronenko M. Diagnosis of intermittently faulty units at system level. Data, 2019, 4(1), pp. 44 – 50.

5. Mashkov V., Lytvynenko V., Fiser J., Voronenko M. Self-Diagnosis of the Systems with Intermittently Faulty Units. Proceedings of the 2018 IEEE 2nd International Conference on Data Stream Mining and Processing, DSMP 2018, 2018, pp. 411 – 414.

6. Zhang H., Shen H. Balancing Energy Consumption to Maximize Network Lifetime in Data-Gathering Sensor Networks. IEEE Trans. Parallel Distrib. Syst. 2009. Vol. 20, No. 10, pp. 1526 – 1539.

7. Xie L., Shi Y., Hou Y.T., Sherali H.D. Making sensor networks immortal: An energyrenewal approach with wireless power transfer. IEEE/ACM Trans. on Networking. Dec. 2012. Vol. 20. No. 6, pp. 174 – 176.

8. Пампуха І.В., Самолов І.В., Толюпа С.В., Берназ Н.М. Інтелектуальний підхід до управління мережними відмовами систем передачі даних. Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. К: ВІКНУ, 2008. № 20. С. 18 – 21.

9. Hryshchuk R. Korobiichuk I., Horoshko V., Khokhlacheva Y. Microprocessor Means for Technical Diagnostics of Complex Systems. Computer Modeling and Intelligent Systems, 2019. Vol. 2353, pp. 1020 – 1029.

10. Olexandr Laptiev, German Shuklin, Spartak Hohonianc, Amina Zidan, Ivanna Salanda. Dynamic model of Ceber Defence Diagnostics of information Systems with the Use of Fozzy Technologies. IEEE ATIT 2019 Conference Proceedings. Kyiv, Ukraine, December 18-20, pp.116 – 120.

11. Vitalii Savchenko, Oleh Ilin, Nikolay Hnidenko, Olga Tkachenko, Oleksander Laptiev, Svitlana Lehominova. Detection of Slow DDoS Attacks based on User's Behavior Forecasting. International Journal of Emerging Trends in Engineering Research (IJETER). Vol. 8., No. 5, May 2020, pp. 2019 – 2025. ISSN 2347 – 3983. (Scopus)

REFERENCES:

1. Sobchuk A.V., Barabash O.V., Musienko A.P. (2019), "Assessment methods of functional stability of wireless sensor networks". Naukovyi zhurnal "Telekomunikatsiini ta informatsiini tekhnolohii". Kyiv: DUT, 2019. No. 3 (64), pp. 46 – 54.

2. Sobchuk Valentyn, Barabach Oleg, Musienko Andrii (2020), "The algorithm of control pricing policy in trade networks on the market of ferrous metals". Naukovyi zhurnal "Telekomunikatsiini ta informatsiini tekhnolohii". Kyiv: DUT, 2020. No. 1 (66), pp. 120 – 128.

3. Mashkov V., Bicanek J., Bardachov Y., Voronenko M. (2020), "Unconventional Approach to Unit Self-diagnosis". Advances in Intelligent Systems and Computing, 2020, 1020, pp. 81 – 96.

4. Mashkov V., Fiser J., Lytvynenko V., Voronenko M. (2019), "Diagnosis of intermittently faulty units at system level". Data, 2019, No. 4 (1), pp. 44 – 50.

5. Mashkov V., Lytvynenko V., Fiser J., Voronenko M. (2018), "Self-Diagnosis of the Systems with Intermittently Faulty Units". Proceedings of the 2018 IEEE 2nd International Conference on Data Stream Mining and Processing, DSMP 2018, pp. 411 – 414.

6. Zhang H., Shen H. (2009), "Balancing Energy Consumption to Maximize Network Lifetime in Data-Gathering Sensor Networks". *IEEE Trans. Parallel Distrib. Syst.* 2009. Vol. 20, No. 10, pp. 1526 – 1539.

7. Xie L., Shi Y., Hou Y.T., Sherali H.D. (2012), "Making sensor networks immortal: An energyrenewal approach with wireless power transfer". *IEEE/ACM Trans. on Networking*. Dec. 2012. V. 20. No. 6, pp. 174 – 176.

8. Pampukha I.V., Samolov I.V., Toliupa S.V., Bernaz N.M. (2008), "Intelektualnyi pidkhid do upravlinnia merezhnymy vidmovamy system peredachi danykh" [An intelligent approach to network failure management of data transmission systems]. Zbirnyk naukovykh prats Viiskovoho instytutu Kyivskoho natsionalnoho universytetu imeni Tarasa Shevchenka. Kyiv: VIKNU, 2008. No. 20. P. 18 – 21.

9. Hryshchuk R. Korobiichuk I., Horoshko V., Khokhlacheva Y. (2019), "Microprocessor Means for Technical Diagnostics of Complex Systems". Computer Modeling and Intelligent Systems, 2019. Vol. 2353, pp. 1020 – 1029.

10. Olexandr Laptiev, German Shuklin, Spartak Hohonianc, Amina Zidan, Ivanna Salanda (2019), "Dynamic model of Ceber Defence Diagnostics of information Systems with the Use of Fozzy Technologies". IEEE ATIT 2019 Conference Proceedings. Kyiv, Ukraine, December 18-20, pp.116 – 120.

11. Vitalii Savchenko, Oleh Ilin, Nikolay Hnidenko, Olga Tkachenko, Oleksander Laptiev, Svitlana Lehominova/ (2020), Detection of Slow DDoS Attacks based on User's Behavior Forecasting. International Journal of Emerging Trends in Engineering Research (IJETER) Volume 8. No. 5, May 2020, pp. 2019 – 2025. ISSN 2347 – 3983. (Scopus).

Doct. of Sc. Sobchuk V.V, Doct. of Sc. Barabash O.V., Doct. of Sc. Musienko A.P.

THE INFLUENCE OF THE METHOD OF ADAPTIVE SELF-DIAGNOSIS ON THE PROCESS OF PREVENTING THE CONSEQUENCES OF MODULE FAILURES ENTERPRISE INFORMATION SYSTEM

The study continues the properties of functional stability. Functional stability means the property of an information system to maintain its functioning, possibly with a decrease in quality, for a specified time under the influence of external and internal destabilizing factors. External and internal destabilizing factors are failures, failures of system modules, mechanical damage, thermal effects, errors of service personnel. The main stages of ensuring functional stability are the detection of the module that failed in the control, diagnosing the module that failed and the restoration of the information system of the enterprise. The peculiarity of enterprise information systems is that they must function autonomously. With their help, the systems can increase the productivity of all production centers while reducing the number of people employed in production and significantly reducing the share of manual labor.

The paper investigates how, based on the functional dependence of failure probability on a certain probability value at different values, the probability of control error of the second kind can determine the recommended interval of the result, which will provide, given the intensity of readiness control allowable failure probability. It is illustrated how at a given intensity of the result it is possible to determine such an intensity of readiness control at which the probability of skipping will not exceed the maximum allowable value. It is shown that we can talk about the weak dependence of the probability of skipping on the control error of the second kind, which means that the achievement of a given control reliability is based on the intensity of readiness control and less depends on the reliability of individual basic checks. For the case when in the intervals between the issuance of the result the system checks the readiness of the modules is randomly described the method of calculating the probability of skipping.

Keywords: functional stability, diagnosis, adaptive diagnosis, structure of test connections, syndrome, readiness control.