УДК 004.415.2.052.3 DOI: 10.31673/2412-9070.2023.023742

С. С. БУЧИК[1], доктор техн. наук, професор;
С. В. ТОЛЮПА[1], доктор техн. наук, професор;
О. В. КІТУРА[2], аспірант,
[1] Київський національний університет імені Тараса Шевченка
[2] Державний університет телекомунікацій, Київ

АНАЛІЗ І РОЗПІЗНАННЯ МЕРЕЖНИХ ВІДМОВ В ІНФОРМАЦІЙНІЙ МЕРЕЖІ

У статті показано, що кожна інформаційна система має свої особливості, зумовлені сферою її застосування. Важливість і відповідальність задач, розв'язуваних за допомогою систем у реальному масштабі часу, зумовили високі вимоги до надійності цих систем, а відмова всієї інформаційної системи або її окремих компонентів може призвести до негативних наслідків. В основу розпізнання мережних відмов покладено принцип визначення за системою продукцій характеру мережних відмов. Цей принцип реалізовано діалоговою процедурою в межах байєсівського підходу, який дає змогу нагромаджувати інформацію, що надходить із різних джерел, з метою підтвердження (не підтвердження) певної гіпотези. Розроблено стратегію керування логічним висновком, керувальними параметрами якої є поточна ймовірність істинності гіпотез, межі їх зміни і ваги асоційованих із цими гіпотезами ознак. Облік поточної ймовірності гіпотез і меж їх зміни дає змогу в процесі висновку, по-перше, фокусувати увагу на найбільш перспективній (імовірній) гіпотезі, а по-друге, припиняти висновок, досягнувши верхнього порогу, що уможливить скорочення кількості ознак, котрі перевіряються, і в такий спосіб скоротити час діалогу. Крім цього, досягнувши нижнього порогу, гіпотеза відкидається як неправдоподібна і в процесі висновку більше не бере участі, що також призводить до скорочення часу розпізнання. Облік ваг ознак у процесі логічного висновку дає змогу передусім перевіряти ті ознаки, які максимально збільшують імовірність правдоподібності гіпотез. Загалом, розроблена стратегія, на відміну від класичної схеми, породжує цілеспрямований процес перевірки правдоподібності гіпотез, що зумовлює скорочення часу розпізнання.

Ключові слова: інформаційна система; мережні відмови; імовірність гіпотез; розпізнавання; правдоподібність гіпотез.

Вступ

Лавиноподібний процес розвитку та впровадження новітніх інформаційних технологій забезпечують безпрецедентні умови для нагромадження і використання інформації, а також створюють фундаментальну залежність від їх нормального функціонування всіх сфер життєдіяльності суспільства та держави: економіки, політики, сфери національної та міжнародної безпеки тощо. Така залежність стає вразливим місцем у функціонуванні систем і об'єктів критичних національних інфраструктур і дає можливість негативно налаштованим елементам і угрупованням скористатися нею для реалізації протиправних дій у кібернетичному просторі через порушення цілісності, доступності й конфіденційності інформації та нанесення шкоди інформаційним ресурсам і інформаційним системам [1].

З початком широкомасштабного вторгнення російської федерації в Україну значно зросла кількість кібератак на органи державної влади, об'єкти критичної інфраструктури та підрозділи, діяльність яких передбачає оброблення критично важливої інформації, зокрема інформаційні системи державного керування. Сучасні інформаційні системи є складовою частиною будь-якої системи керування об'єктом критичної інфраструктури держави і відіграють важливу роль у державному керуванні.

Сьогодні вирішення питань керування інформаційними мережами описується в працях таких вітчизняних та закордонних дослідників, як Беркман Л. Н., Климаш М. М., Демидов І. В., Поповський В. В., Стеклов В. К., Єременко О. С., Башлей М. І., T. Ptaceka, G. Elmasry, P. Albers, O. Camp та ін.

В основі сучасної інформаційної системи (ІС) містяться засоби зберігання та оброблення первинної інформації, комунікаційні сервери, сервери вторинної і третинної інформації, різного типу процесори оброблення інформації, обчислювальні комплекси системи, пристрої передавання інформації.

Кожна інформаційна система має свої особливості, спричинені сферою її застосування. Важливість і відповідальність задач, розв'язуваних за допомогою систем у реальному масштабі часу, зумовили високі вимоги до надійності цих систем, в яких, найчастіше, неможливе проведення технічного обслуговування під час функціонування, а, отже, відмова всієї інформаційної системи або її окремих компонентів може призвести до негативних наслідків [2-4].

Дослідження сучасних науково-обґрунтованих підходів підвищення ефективності складних технічних систем, до яких цілком можна віднести розподілені інформаційні системи, дали змогу дійти висновку, що за останні роки сформувався новий пріоритетний підхід, пов'язаний із забезпеченням в ІС властивості функціональної стійкості.

Властивість функціональної стійкості розглядається як можливість складної технічної системи, до якої належить РІС, успішно завершити поставлене завдання із регламентованою кількістю змін у стані самої системи, тобто зберегти її працездатність після прояву припустимої кількості відмов і зовнішніх дестабілізувальних впливів.

Проблему функціональної стійкості інформаційних систем досліджували у свої працях Машков О. А., Барабаш О. В., Обідін Д. М., Кравченко Ю. В., Кононов О. А. Питання відмовостійкості систем розглядали Авіжиєніс А. А., Машков В. А., Ільїн О. Ю., Коростіль Ю. М., Савченко В. А. та інші вчені.

Основна частина

Аналіз стану інформаційної мережі (ІМ) здійснюється стандартними процедурами із застосуванням відповідних діагностичних засобів. Основним змістом цього процесу є виявлення відхилення параметрів заданих характеристик мережі від установлених значень, що є підставою віднести поточний (спостережуваний) стан мережі до стану нештатної (аварійної) роботи мережі. Процедуру аналізу станів формально можна подати таким виразом:

$$П_A = < V, V', V'', P >,$$

де V, V' — вектори вхідних і заданих параметрів; V'' — вектор відхилень вхідних параметрів від заданих значень; P — кореляційна процедура.

Для виявлення таких відхилень нині розроблено досить-таки багато кореляційних методів і процедур, які можуть бути ефективно застосовані.

Як відомо, будь-яка аварійна ситуація характеризується деякою множиною ознак її прояву. В ІМ ці ознаки можуть бути зафіксовані як діагностичними програмами, так і зовнішніми джерелами (користувачами, операторами і т. ін.). Оскільки ознаки є наслідком прояву відмови, то задача розпізнання мережної відмови полягає у визначенні причини її виникнення за наявності спостережуваних ознак. У нашому випадку під причиною мережної відмови розумітимемо відмову деякого апаратно-програмного засобу системи [5].

Визначимо аварійну ситуацію як множину понять, на якій задано систему бінарних відносин.

Нехай $P = \{P_i \,|\, i \in I = \overline{1,n}\}$ — безліч ознак мережної відмови.

Поставимо кожній ознаці P_i у відповідність деякий терм E_i. Тоді під описом E мережної відмови розумітимемо ланцюжок вигляду

$$E_1 \wedge E_2 \wedge \ldots \wedge E_n.$$

Далі, в ІМ спостережувані ознаки можуть виявлятися як на рівні технічних засобів і їх компонент, так і на рівні компонент системи загалом. Ці рівні можна описати деякими класами ознак мережних відмов, а задачу розпізнання структурувати відносно цих класів.

Нехай $K = \{K_i \,|\, K_i = (E^i_1, E^i_2, \ldots, E^i_{mi}),\ i = 3,2,1\}$ — безліч класів ознак мережних відмов, де E^i_j — асоційована ознака класу K_i.

Кожну причину E^i_j кожного рівня (окрім першого) подамо як $E^i_j = < N^i_j, S^i_j >$, де N^i_j — найменування ознаки; S^i_j — його структура.

Під структурою ознаки E^i_j розумітимемо множину $S^i_j = (E^{i-1}_{j1}, \ldots, E^{i-1}_{jm_{i-1}})$,
де E^{i-1}_{jl} — ознака $i-1$-го рівня, який індукує появу ознаки E^i_j. Інакше кажучи, ця ознака, по суті, є причиною появи ознаки E^i_j.

Тоді всю сукупність ознак мережних відмов, що виникають в ІМ, і можливих причин їх появи можна подати наступною ієрархічною структурою й інтерпретувати як класифікатор ознак, на першому рівні якого розміщено ознаки компонент технічних засобів, на другому — ознаки технічних засобів, а на третьому — ознаки компонент мережі.

З огляду на зазначене в основу розв'язання задачі розпізнання доцільно покласти логіко-лінгвістичний підхід. Згідно з цим підходом модель розпізнання формально подамо таким виразом:

$$П_p = < K, E, R, П >,$$

де K — класифікатор ознак; $E = \{E_i \,|\, E_i \in K\}$ — безліч ознак, що описують аварійну ситуацію; $R = \{R_i\}$ — безліч правил розпізнання причини $П \in K$ появи ознак E_i.

Беручи до уваги структуру класифікатора, розпізнання мережних відмов можна окреслити таким ітераційним процесом.

Нехай ознаки, що описують аварійну ситуацію, належать третьому рівню класифікатора. У цьому разі за відповідними правилами визначається причина їх виникнення другого рівня. Якщо для ідентифікації мережної відмови достатньо цієї причини, то процес закінчується. Інакше ця причина береться як ознака й аналогічно визначається причина його появи на першому рівні.

Розглянуту модель розпізнання мережних відмов можна реалізувати продукційною процедурою, згідно з якою з безлічі гіпотез про причину мережної відмови за відповідними продукційними правилами розпізнання потрібно визначити найбільш правдоподібну гіпотезу.

Кожну гіпотезу H_i представлятимемо продукційним правилом вигляду

$$R_i : E_{i1} \wedge ... \wedge E_{ik} \rightarrow H_i , \quad (1)$$

де E_{i1} — асоційовані ознаки гіпотези H_i.

Тоді задача розпізнання полягає в пошуку такого правила, умова застосування якого здійсненна.

У традиційних продукційних системах, якщо немає додаткової інформації про гіпотези, їх перевірка на правдоподібність здійснюється послідовно, зазвичай методом «спроб і помилок», що нерідко призводить до збільшення часу пошуку, оскільки підсумкова гіпотеза може виявитися останньою гіпотезою, що перевіряється. Щоб обійти цей недолік у статті запропоновано інший підхід, заснований на таких ідеях.

Перша. Серед можливих гіпотез спочатку перевіряється на правдоподібність найбільш перспективна гіпотеза, що дасть змогу підвищити ймовірність правильного вибору і, як наслідок, скоротити час розпізнання мережної відмови.

Друга. Незважаючи на те, що перевірка найбільш перспективної гіпотези підвищує ймовірність правильного вибору, однак вона не гарантує отримання підсумкового висновку. Тому необхідно, щоб одночасно з перевіркою найбільш перспективної гіпотези перевірялися інші. Це уможливить розпаралелювання процесу ідентифікації, що також дасть можливість скоротити час пошуку підсумкового висновку.

Цей підхід у статті реалізовано такою процедурою.

Кожній гіпотезі H_i приписується деяка апріорна ймовірність $P(H_i)$ її істинності, а кожній її ознаці E_{ik} ставиться у відповідність деяка ціна, яка відображає важливість цієї ознаки в процесі логічного висновку. Так, ціна $C(E_{ik})$ ознаки E_{ik} визначається як сума максимально можливих змін імовірності за всіма гіпотезами, тобто $C(E_{il}) = \sum_{j=1}^{n} \left| P(H_j / E_{il}) - P(H_j / \overline{E}_{il}) \right|$. Однак, як відомо, у разі такого визначення максимальна ціна деякої ознаки буде знівельована сумою нижчих цін решти ознак. Інакше кажучи, у цьому разі не можна визначити домінуючу ознаку для даної гіпотези, яка потрібна для здійснення цілеспрямованого пошуку необхідних фактів, що підтверджують правдоподібність даної гіпотези. Тому конструктивнішим є використання як ціни ознаки E_{ik} величини приросту ймовірності гіпотези H_i за наявності цієї ознаки, тобто

$$C(E_{ik}) = P(H_i / E_{ik}) - P(H_i), \quad (2)$$

де $P(H_i / E_{ik})$ — обчислюється за формулою Байєса; $P(H_i)$ — поточна ймовірності гіпотези H_i.

Крім цього, кожній ознаці E_{ik} також ставиться у відповідність деяке запитання q_{i_1}, відповідь на яке дасть змогу визначити істинність цієї ознаки. Тоді кожне правило $E_{i1} \wedge ... \wedge E_{ik} \rightarrow H_i$ можна описати безліччю запитань $Q_i = (q_{i1}, ..., q_{ik})$.

З огляду на сказане процес розпізнавання можна подати в такий спосіб.

Спочатку за описом мережної відмови визначається безліч можливих (релевантних) гіпотез.

Нехай $E = \{E_i | i = \overline{1,n}\}$ — опис мережної відмови S_A; $H = \{H_j | j = \overline{1,m}\}$ — повна безліч гіпотез, де $H_j = \{E_{kj} | k = \overline{1,l_j}\}$. Гіпотеза H_j релевантна ситуації S_A тоді і тільки тоді, коли $E \cap H_j \neq \varnothing$.

Далі, нехай H_{S_A} — безліч гіпотез, релевантних ситуації S_A. Серед цих гіпотез вибирається гіпотеза, імовірність якої найбільша, і перевіряється її правдоподібність. Якщо таких гіпотез виявиться кілька, то вибирається та гіпотеза, в якої асоційованих ознак менше. Потім серед ознак цієї гіпотези вибирається ознака E_{ik} із найбільшою ціною і оператору ставиться відповідне запитання q_{ik} з метою уточнення наявності цієї ознаки.

Якщо отримано позитивну відповідь, то ймовірність усіх гіпотез перераховується за формулою Байєса

$$P(H_j / E_{ik}) = \frac{P(E_{ik} / H_i) P(H_i)}{P(E_{ik} / H_i) P(H_i) + P(E_{ik} / \overline{H}_i) P(\overline{H}_i)}, \quad (3)$$

де $P(E_{ik} / H_i)$ — імовірність появи ознаки E_{ik} за наявності гіпотези H_i; $P(E_{ik} / \overline{H}_i)$ — імовірність появи свідчення E_{ik} за відсутності гіпотези H_i; $P(\overline{H}_i) = 1 - P(H_i)$.

Отже, набувши ознаки E_{ik}, імовірність $P(H_i)$ перераховується за формулою (3) і замінюється на $P(H_i / E_{ik})$. Крім цього, перераховується ймовірність $P(H_i)$ тих гіпотез, для яких ця ознака є також асоційованою. Інакше кажучи, отримання чергової ознаки зумовлює оновлення (збільшення або зменшення) цієї ймовірності. Потім ознака E_{ik} відкидається з асоційованих ознак відповідних гіпотез. Це дасть змогу, у разі їх перевірки, обійти уточнення наявності цієї ознаки і в такий спосіб скоротити загальний час розпізнавання.

Якщо отримано негативну відповідь, тобто якщо не підтверджено наявність ознаки E_{ik}, то в цьому разі ймовірність $P(H_i)$ відповідних гіпотез замінюється на $P(H_i / \overline{E}_{ik})$. Якщо $P(H_i / \overline{E}_{ik}) = 0$, то цими гіпотезами можна знехтувати під час розгляду.

І, нарешті, можуть бути випадки, коли оператор не має у своєму розпорядженні достатньої інформації (відповідь «НЕ ЗНАЮ»). У цьому разі це запитання розсилається іншим операторам, які обслуговують сегмент системи, в якому виникла мережна відмова.

Отже, використовуючи фреймову побудову як комунікаційне середовище, ми маємо можливість пошук цієї ознаки розосередити по вузлах мережі і в результаті здобути стверджувальну відповідь щодо її наявності.

Потім знову вибирається найімовірніша гіпотеза і процес повторюється. У результаті, найбільш імовірна гіпотеза береться як кінцевий висновок.

За такого підходу актуальною стає задача зупинки логічного висновку. З цією метою пропонується використовувати верхній $M_1(H_i)$ і нижній $M_2(H_i)$ пороги для ймовірності. Якщо $P(H_i) > M_1(H_i)$, то гіпотеза H_i береться як основа для можливого висновку. Якщо $P(H_i) < M_2(H_i)$, то ця гіпотеза відкидається як неправдоподібна. Як такі пороги можна використовувати наступні вирази:

$$M_1(H_i) = 0{,}9P_{\max}(H_i) \text{ і } M_2(H_i) = 0{,}5M_1(H_i),$$

де $P_{\max}(H_i)$ — максимальна можлива ймовірність, досяжна для цієї гіпотези, за умови, що всі її асоційовані ознаки будуть підтверджені на користь гіпотези H_i.

Варто зауважити, що за класичної схеми, щоб переконатися в правдоподібності тієї або іншої гіпотези досить перебрати всі її ознаки. Однак у нашому разі закінчення процесу може настати значно раніше (досягнувши верхнього порога), що дасть змогу зменшити кількість ознак, що перевіряються, і в такий спосіб скоротити час діалогу. Крім цього, досягнувши нижнього порога, гіпотеза відкидається як неправдоподібна і в процесі висновку більше не бере участі, а це також призводить до скорочення часу.

Розглянутий підхід можна подати таким алгоритмом.

1. Визначення релевантних гіпотез. Нехай $E = \{E_i\}$ — опис мережної відмови, $H = \{H_j\}$ — повна безліч гіпотез. Гіпотеза $H_j \in H$ є релевантною аварійній ситуації E, коли $E \cap H_j \neq \varnothing$.

2. Вибір серед релевантних гіпотез найбільш перспективної. Нехай $H_{\text{Re}l} = (H_1,\ldots,H_n)$ — безліч релевантних ситуацій. Гіпотеза $H_k \in H_{\text{Re}l}$ вважається найбільш перспективною, якщо $H_k \triangleq \max P(H_i)$.

3. Вибір серед ознак гіпотези H_k найбільш важливої ознаки. Нехай $E^k = (E_1,\ldots,E_{m_k})$ — безліч асоційованих ознак гіпотези H_k. Ознака $E_l \in E^k$ є найбільш важливою для даної гіпотези, якщо $E_l \triangleq \max C(E_j)$.

4. Формування запитання оператору для уточнення наявності ознаки E_l.

5. Якщо одержано негативну відповідь, то ця гіпотеза H_k вилучається з розгляду $H_{\text{Re}l} \setminus H_k$ і вибирається наступна найбільш перспективна гіпотеза. Якщо відповідь «НЕ ЗНАЮ», то запитання про наявність даної ознаки розсилається мережею іншим операторам із метою отримання стверджувальної відповіді.

6. Якщо відповідь позитивна, то ймовірність усіх релевантних гіпотез перераховується за формулою Байєса: $(\forall_i)P(H_i) = P(H_i/E_l)$.

7. Перевірка верхнього і нижнього порогів. Якщо поточна ймовірність гіпотези H_k перевищує верхній поріг $P(H_k) > M_1(H_k)$, то ця гіпотеза приймається як результат розпізнання, тобто ця гіпотеза є причиною мережної відмови.

Якщо її ймовірність нижча за нижній поріг $P(H_k) < M_1(H_k)$, то вона відкидається як неправдоподібна і вибирається наступна найбільш перспективна гіпотеза.

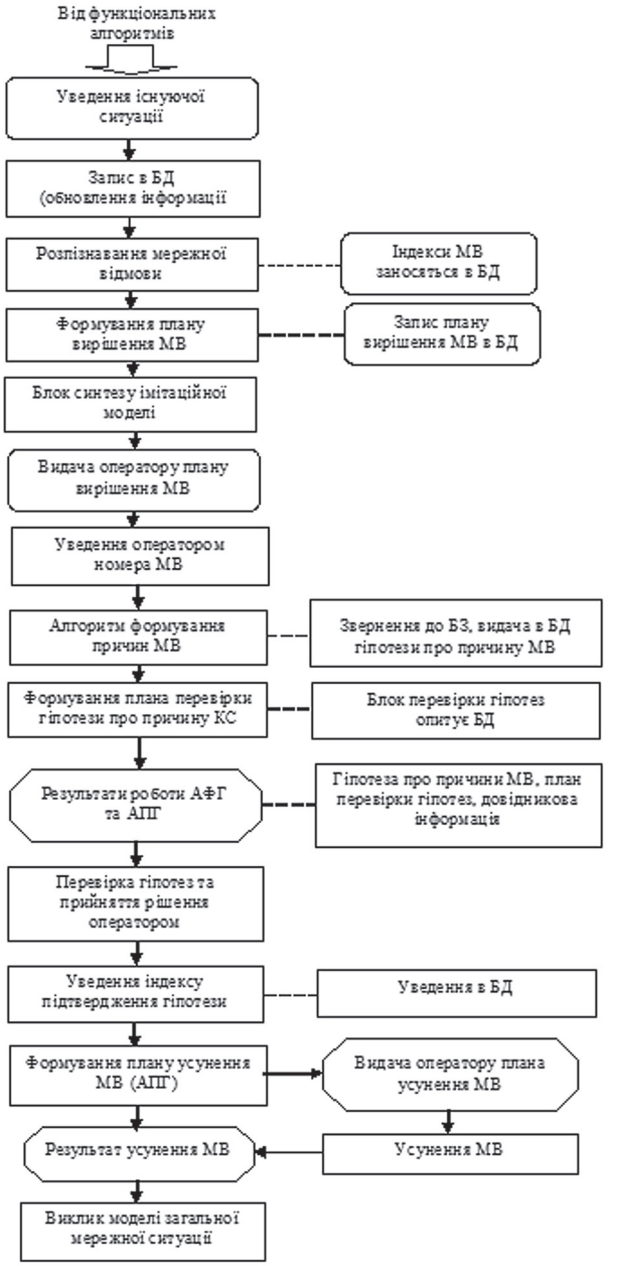
Якщо ймовірність цієї гіпотези перебуває в межах цих порогів, то ознака E_l видаляється з асоційованих ознак усіх гіпотез $(\forall_i)E^i \setminus E_l$ і вибирається наступна найбільш важлива ознака для даної гіпотези і процес повторюється.

План відновлення інфокомунікаційної мережі — це послідовність керувальних дій, які в сукупності переводять інфокомунікаційну мережу з аварійного стану в стан нормального її функціонування.

Отже, формування такого плану можна пов'язати з розв'язанням задачі планування шляху досягнення заданої мети з деякої фіксованої початкової ситуації. Алгоритм функціонування розподіленої системи інформаційного підтримання ухвалення рішень зображено на рисунку.

Вибір керувальних дій має ґрунтуватися на ситуативному підході, згідно з яким кожній типовій аварійній ситуації відповідає конкретний план відновлення. Тобто, такий підхід припускає існування матриці рішень, яка встановлює взаємно однозначну відповідність між мережними відмовами і керувальними діями. Таку матрицю можна побудувати з огляду на те, що для кожної типової мережної відмови (залежно від використовуваних апаратно-програмних засобів) існують стандартні алгоритми відновлення штатного функціонування системи.

Варто зазначити, що розглянутий алгоритм має важливу особливість. А саме, послідовно перетворюючи початкову ситуацію за допомогою застосування відповідних керувальних дій, ми в такий спосіб, по-перше, кожного разу маємо опис одержуваної ситуації, а отже, можемо класифікувати й оцінювати її конфліктність або неконфліктність у процесі оперативного відновлення системи; по-друге, можемо прослідкувати (екстраполювати) розвиток початкової ситуації в часі. Тобто, даний алгоритм можна



Алгоритм функціонування розподіленої системи інформаційного підтримання ухвалення рішень

розглядати одночасно і як алгоритм формування альтернативних рішень, і як алгоритм екстраполяції.

Крім цього, застосування процедурної моделі алгоритму дає змогу зменшити час вибору раціональної дії завдяки скороченню кількості запитань, що ставляться.

Якщо розглядати принцип функціонування системи інформаційного підтримання ухвалення рішень, то на початковому етапі функціонування база даних заповнюється параметрами, що характеризують технічний стан, різними значеннями цих параметрів, що визначають різні варіанти ситуацій, які постають у процесі функціонування мережі. У базу знань експерти записують правила, за якими, на їхню думку, може визначатися технічний стан і причини мережних відмов. Також у базу знань записується інформація, що характеризує важливість ситуацій та інформативність використовуваних параметрів. Подальше заповнення БЗ відбувається в процесі функціонування ІМ.

У процесі роботи СІППР на її вхід надходять інформація і параметри, що характеризують технічний стан мережі. Ці параметри порівнюються з еталонними, взятими з бази даних, і якщо ніяких відхилень немає, то система на дисплей видає повідомлення про справність мережі.

Якщо один або відразу кілька параметрів вишли за межі норми, СІППР шукає в базі знань ситуацію, схожу на ту, що виникла, і видає підказку можливої причини відмови. Оператор перевіряє дану підказку, і якщо вона виявляється вірною, то за допомогою діалогових засобів підтверджує висунену альтернативу.

Якщо внаслідок перевірки з'ясовується, що підказка є невірною або не приводить до відшукання причини виникнення відмови, то оператор за допомогою діалогових засобів дає команду на обчислення функцій належності й ухвалення рішень по них на блоки побудови функцій належності і ухвалення рішень.

Побудова функцій належності й ухвалення рішень виробляється методами, найбільш оптимальними для даної мережі. Розраховане значення функції належності виводиться на екран монітора, і якщо за цим значенням оператору важко визначити технічний стан і вказати вузол, що відмовив, то на наступному етапі на екран виводиться найбільш вигідне рішення з блока ухвалення рішень.

Якщо передбачуване рішення є правильним, то за допомогою блока навчання інженер з експлуатації вносить необхідну корективу в базу знань і записує ознаки даної ситуації в БД. Унаслідок тривалого функціонування СІППР нагромаджує досить відомостей, що дають можливість без додаткового оброблення ухвалювати рішення щодо технічного стану ІМ.

Висновки

В основу розпізнання мережних відмов покладено принцип визначення за системою продукцій характеру мережних відмов. Такий принцип реалізовано діалоговою процедурою в межах байєсівського підходу, який дає змогу нагромаджувати інформацію, що надходить із різних джерел, з метою підтвердження (не підтвердження) певної гіпотези.

Розроблено стратегію керування логічним висновком, керувальними параметрами якої є поточна ймовірність істинності гіпотез, межі їх зміни і ваги асоційованих із цими гіпотезами ознак. Облік

поточної ймовірності гіпотез і меж їх зміни дає можливість у процесі висновку, по-перше, фокусувати увагу на найбільш перспективній (імовірній) гіпотезі, а по-друге, припиняти висновок, досягнувши верхнього порога, що дозволить зменшити кількість ознак, які перевіряються, і в такий спосіб скоротити час діалогу. Крім цього, діставшись нижнього порога, гіпотеза відкидається як неправдоподібна і в процесі висновку участі більше не бере, що також зумовлює скорочення часу розпізнання.

Облік ваг ознак у процесі логічного висновку дає змогу передусім перевіряти ті ознаки, які максимально збільшують імовірність правдоподібності гіпотез. Загалом, розроблена стратегія, на відміну від класичної схеми, породжує цілеспрямований процес перевірки правдоподібності гіпотез, спричинюючи скорочення часу розпізнання.

Список використаної літератури

1. ***Системи*** *виявлення вторгнень та функціональна стійкість розподілених інформаційних систем до кібернетичних загроз / Н. В. Лукова-Чуйко, С. В. Толюпа, В. С. Наконечний, М. М. Браіловський: монографія. Київ: Формат, 2021. 407 с.*

2. ***Кривуца В. Г., Беркман Л. Н., Толюпа С. В.*** *Інфокомунікаційні мережі нового покоління: монографія. Київ: ДУІКТ. 2012. 286 с.*

3. ***Book Chapter****. Calculation of Quality Indicators of the Future Multiservice Network Lecture Notes / B. Zhurakovskyi, S. Toliupa, V. Druzhynin [et al.] // Electrical Engineering. 2022. 831. P. 197–209.*

4. ***Система*** *керування сучасними телекомунікаційними мережами: монографія / В. Г. Кривуца [та ін.]; за ред. В. Г. Кривуци. Київ: ДУІКТ, 2009. 268 с.*

5. ***Методи*** *визначення параметрів об'єктів керування телекомунікаційних мереж/ Л. Н. Беркман, А. О. Макаренко, Ю. М. Зіненко, А. Г. Захаржевський // Наукові записки Україн. наук.-дослід. ін-ту зв'язку. 2020. № 1. С. 5–9.*

S. S. Buchyk, S. V. Toliupa, O. V. Kitura

ANALYSIS AND IDENTIFICATION OF NETWORK FAILURES IN THE INFORMATION NETWORK

This article shows that each information system has its own characteristics, which are determined by the scope of its application. The importance and responsibility of tasks solved using real-time systems have led to high requirements for the reliability of these systems, and the failure of the entire information system or its individual components can lead to negative consequences. Network failure recognition is based on the principle of determining the nature of network failures based on the product system. This principle is implemented through a dialogue procedure within the framework of the Bayesian approach, which allows you to accumulate information coming from various sources in order to confirm (not confirm) a certain hypothesis. A logical conclusion management strategy was developed, the control parameters of which are the current probability of the truth of the hypotheses, the limits of their change, and the weight of the signs associated with these hypotheses. Accounting for the current probability of hypotheses and the limits of their change allows in the process of conclusion, firstly, to focus attention on the most promising (probable) hypothesis, and secondly, to stop the conclusion after reaching the upper threshold, which will reduce the number of signs to be checked, and thus shorten the dialogue time yourself. In addition, having reached the lower threshold, the hypothesis is rejected as implausible and no longer participates in the conclusion process, which also leads to a reduction in recognition time. Accounting for the weights of signs in the process of logical inference allows you to first of all check those signs that maximize the probability of the plausibility of hypotheses. In general, the developed strategy, unlike the classical scheme, generates a purposeful process of testing the plausibility of hypotheses, which leads to a reduction in recognition time.

Keywords: information system; network failures; probability of hypotheses; recognition; plausibility of hypotheses.