

## ВИЯВЛЕННЯ НЕСПРАВНИХ ПАРАМЕТРІВ У ХОДІ МОНІТОРИНГУ МЕРЕЖІ

UDC 004.94

N. M. Holovetskyi

## DETECTION OF FAULTY PARAMETERS DURING NETWORK MONITORING

Розглянемо постановку задачі моніторингу комп'ютерної мережі. Загалом завдання моніторингу можна описати в такий спосіб: події, що відбуваються в комп'ютерних мережах та інформаційних системах, мають випадковий характер. У зв'язку з цим для їх вивчення найбільше підходять ймовірнісні математичні моделі теорії масового обслуговування, наприклад теорія марковських ланцюгів [1].

Для моделювання спочатку необхідно визначити вхідні дані. Розглянемо події, пов'язані з детектуванням аномалій у процесі діагностики та контролю досліджуваних системою параметрів обладнання в мережі, як стан аналізованої системи моніторингу мережі. Виходячи з викладеного вище, виведемо можливі стани в процесі моніторингу метрик (параметрів) мережного обладнання:  $S_0$  – відсутність несправностей;  $S_1$  – навантаження мережі;  $S_2$  – зниження пропускної спроможності;  $S_3$  – відсутність мережного порту;  $S_4$  – фізична недоступність пристрою;  $S_5$  – фрагментація пакета;  $S_6$  – повна відмова системи.

Описаний ланцюг подій під час моніторингу мережі можна подати у вигляді графа станів, як показано на рис. 1.

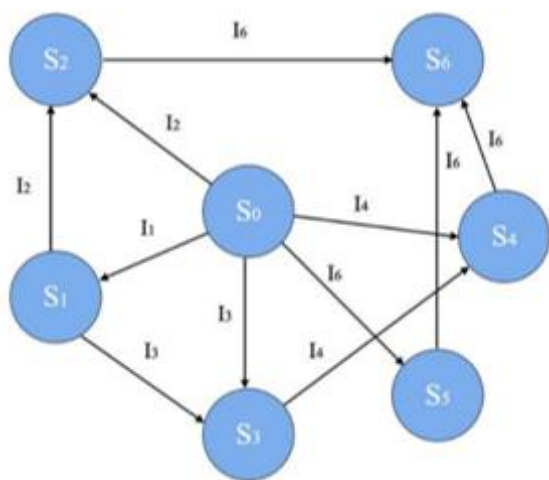


Рис. 1 - Граф виявлення несправних параметрів у ході моніторингу мережі

Імовірність виявлення несправного параметра в мережі визначається в даному випадку як ймовірність знаходження системи в стані  $S_i$ .

На графі кожна стрілка відповідає інтенсивності потоку подій, який переводить систему з одного стану в інший. Послідовність опитування визначається призначенням системним адміністратором пріоритетом. Чим вищий пріоритет у параметра мережного пристрою, тим вище інтенсивність його опитування. За інтенсивності переходів у разі приймається  $I_i$  – інтенсивність опитування  $i$ -го параметра у системі моніторингу.

Зважаючи на описані вище метрики роботи, система моніторингу виходить, що вона зі стану  $S_0$  при виконанні опитування мережних пристроїв при відмові будь-якого компонента переходить у стан виявлення несправностей  $S_i$  з інтенсивністю  $I_i$ . За графом можна скласти математичну модель процесу

моніторингу мережі з урахуванням ймовірностей  $p_i$  як системи рівнянь. Її розв'язок дозволяє відстежити динаміку діагностування несправних параметрів у процесі мережного моніторингу через відстеження ймовірностей у певні проміжки часу.

## Література

- Погоруй А. О., Чемерис О.А. Вступ до теорії випадкових процесів : навчальний посібник. Житомир : Вид-во ЖДУ ім. І. Франка, 2020. 70 с.