УДК: 004.738 DOI: 10.31673/2786-8362.2024.022709

Прокопенко А.Г.

МЕТОД РОЗПОДІЛЕНОГО МОНІТОРИНГУ ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖ НА ОСНОВІ АГЕНТНОГО ПІДХОДУ

Prokopenko A.G. A method of distributed monitoring of telecommunication networks based on an agent-based approach. The purpose of the article is to develop a method of distributed monitoring of information and telecommunication networks (ITN) based on an agent-based approach and implementing a step-by-step detection of abnormal situations in networks. The article deals with the urgent problem of ensuring reliability and functional security of elements of modern network infrastructures. Particular attention is paid to heterogeneous general and special-purpose networks, which are characterised by heterogeneity in the use of various network technologies, information security tools and software and hardware solutions.

The proposed approach is based on the principles of decentralisation and multi-level monitoring. The solution is aimed at overcoming the difficulties arising from the distribution of network resources, variability of network traffic characteristics and heterogeneity of ITCM elements. The article focuses on the need to create monitoring subsystems that can take into account the heterogeneity and diversity of network elements, as well as ensure the continuity of critical nodes.

The authors propose the use of intelligent agents to monitor the functional state of network elements and detect anomalies. The first stage of monitoring involves detecting violations at the local level, while subsequent stages clarify the degree and type of violation. This approach makes it possible to increase the reliability of the ITCM functioning, reduce the response time to critical situations and reduce the volume of data circulation in the network, which is an important factor for distributed networks with limited resources.

Keywords: information network, monitoring subsystem, information transfer, heterogeneous networks, intelligent agents

Прокопенко А.Г. Метод розподіленого моніторингу телекомунікаційних мереж на основі агентного підходу. Метою статті є розробка методу розподіленого моніторингу інформаційно-телекомунікаційних мереж (ІТКМ), який базується на агентно-орієнтованому підході та реалізує поетапне виявлення аномальних ситуацій у мережах. У статті розглядається актуальна проблема забезпечення надійності та функціональної безпеки елементів сучасних мережевих інфраструктур. Особливу увагу приділено гетерогенним мережам загального та спеціального призначення, які характеризуються неоднорідністю у використанні різних мережевих технологій, засобів захисту інформації та програмно-апаратних рішень.

Запропонований підхід базується на принципах децентралізації та багаторівневості моніторингу. Рішення спрямоване на подолання складнощів, які виникають через розподіленість мережевих ресурсів, варіативність характеристик мережевого трафіку та неоднорідність елементів ІТКМ. Стаття акцентує увагу на необхідності створення підсистем моніторингу, здатних враховувати гетерогенність і різнорідність елементів мережі, а також забезпечувати безперервність роботи критично важливих вузлів.

Автори пропонують використання інтелектуальних агентів для відстеження функціонального стану мережевих елементів та виявлення аномалій. Перший етап моніторингу передбачає виявлення порушень на локальному рівні, тоді як наступні етапи уточнюють ступінь та тип порушення. Такий підхід дозволяє підвищити надійність функціонування ІТКМ, скоротити час реагування на критичні ситуації та знизити обсяги циркуляції даних у мережі, що є важливим фактором для розподілених мереж з обмеженими ресурсами.

Ключові слова: інформаційна мережа, підсистема моніторингу, передача інформації, гетерогенні мережі, інтелектуальні агенти

Вступ

Проблема забезпечення надійності та функціональної безпеки елементів мережевих інфраструктур на сучасному етапі розвитку інформаційно-телекомунікаційних мереж (ІТКМ) та систем є пріоритетною.

Аналіз останніх досліджень і публікацій. У сучасних дослідженнях ІТКМ розглядаються як складні системи, що вимагають особливих підходів до забезпечення надійності та функціональної безпеки. Зокрема, наголошується на проблемах моніторингу таких мереж, що

пов'язані з їх гетерогенністю, географічною розподіленістю, різнорідністю елементів та технологій, а також складністю математичного опису [5]. Також дослідники підкреслюють важливість використання децентралізованих підходів до моніторингу, таких як агентні системи, що дозволяють ефективно керувати ресурсами та знижувати втрати під час функціонування мереж [6].

Публікації підтверджують необхідність застосування методів інтелектуального моніторингу, зокрема з використанням інтелектуальних агентів, які здатні збирати дані в реальному часі та аналізувати аномальні ситуації [7]. Також досліджується питання скорочення обсягу вимірювальної інформації в умовах зниженої пропускної здатності каналів зв'язку, що є ключовим аспектом для забезпечення ефективності таких систем [8]. Особлива увага приділяється автоматизованим системам моніторингу, які здатні працювати в режимі реального часу та реагувати на критичні ситуації з мінімальними затримками.

Постановка завдання. Однією з недостатньо досліджених і невирішених задач є побудова підсистеми моніторингу процесів функціонування територіально-розподілених систем різної складності. При цьому, сучасні ІТКМ, як загального користування (ЗК), так і спеціального призначення (СП) [1] можна повністю віднести до гетерогенних мереж, що також накладає певні труднощі та особливості для побудови їх підсистем моніторингу (гетерогенними називають, як правило, мережеві структури, що утворюються за допомогою об'єднання різних відомчих мереж, що мають різні принципи побудови, мережеві технології передачі та/або захисту інформації та/або програмно-апаратні засоби [2]. Дійсно, гетерогенність (неоднорідність) мережі передбачає несумісність вузлів, що належать до однієї мережі, або до суміжних сегментів мережі за однією або декількома логічними ознаками, а саме за типом операційних систем, що застосовуються, форматів кадрів мережі, моделям безпеки, способам захисту інформації та інші. З цього випливає, що на гетерогенних ІТКМ підсистема моніторингу повинна будуватися на основі принципів децентралізації та багаторівневості. При тому, що ІТКМ СП, як правило, має строго ієрархічну структуру, її підсистема моніторингу повинна дозволяти здійснення перерозподілу функцій центру управління функціонування та периферією залежно від стану системи.

Однією із особливостей гетерогенних мережевих інфраструктур, як правило, є міжвідомчий характер. При цьому створення таких міжвідомчих ІТКМ пов'язане з низкою особливостей, що відрізняють їх від традиційних. Перша особливість полягає в географічній розподіленості мережевих ресурсів, а також джерел та одержувачів інформації [3]. Друга – визначається пульсуючим характером мережевого трафіку [3]. Третя – прихована у різнорідності елементів та застосовуваних мережевих технологіях [3]. Четверта – полягає у неможливості повного математичного опису (побудови повноцінної математичної моделі) як мультисервісної ІТКМ загалом, і окремих телекомунікаційних мереж у її складі, якщо є така необхідність [4]. П'ята особливість полягає у випадковості функціонування ІТКМ, яка спричиняє труднощі при проведенні аналізу її стану (моніторингу) та організації управління [4]. Шоста особливість полягає в тому, що гетерогенна мережа зв'язку призначена для поєднання та передачі інформації, а не для управління нею, тобто функціонує незалежно від системи управління. Сьома особливість випливає зі складності сучасних гетерогенних ІТКМ і полягає у суттєвій нестаціонарності (або дрейфі основних характеристик), що викликає різну реакцію мережі на ту саму ситуацію або управління в різні моменти часу [4].

Складність та актуальність створення підсистем моніторингу для таких гетерогенних ІТКМ пов'язано з низкою особливостей та обмежень, серед яких також можна виділити наступні: наявність різнорідних протоколів взаємодії між вузлами та периферійними мережевими пристроями, сполучення сегментів малопотужних та високопродуктивних елементів мережі, постійні трансформації мережевих топологів , широке застосування малопотужних станцій і пристроїв, які можуть переноситися (мобільні) (низьке енергоспоживання, слабкі обчислювальні потужності, малі обсяги пам'яті). Всі ці перелічені особливості дозволяють вести мову про недосконаліть існуючих систем контролю,

орієнтованих на використання в гомогенних мережевих структурах та необхідність пошуку нових технологій та підходів до побудови підсистем розподіленого моніторингу функціонального стану елементів сучасних гетерогенних ІТКМ, у тому числі на основі методів інтелектуального моніторингу їх технічного стану (ТС).

Метою роботи є розробка методу розподіленого моніторингу телекомунікаційних мереж на основі агентного підходу, що дозволяє підвищити надійність та ефективність функціонування гетерогенних інформаційно-телекомунікаційних мереж (ІТКМ). Основна увага приділяється розв'язанню задачі виявлення та ідентифікації аномальних станів мережевих елементів із мінімізацією втрат інформації, а також побудові системи моніторингу, що забезпечує своєчасне реагування на критичні зміни в умовах високої динамічності мережевих процесів.

Виклад основного матеріалу дослідження.

Інформаційно-телекомунікаційна мережа як об'єкт моніторингу. Інформаційно-телекомунікаційні мережі відносять до систем безперервного режиму функціонування з високим ступенем доступності, для яких має бути забезпечена безвідмовність та безперервність роботи вузлів системи та їхніх сервісів. Таким чином кожна хвилина простою для постачальників телекомунікаційних послуг та їхніх клієнтів тягне за собою суттєві фінансові та репутаційні витрати. Це робить пріоритетним завдання забезпечення надійної роботи мережевих елементів і пристроїв на кожному з ієрархічних рівнів ІТКМ у сфері телекомунікацій. У зв'язку з чим останніми роками чимало уваги приділяють питанню побудови автоматизованих систем моніторингу зі спостереженням у режимі реального часу за функціональним станом мережевих елементів з метою оперативного виявлення критичних аномальних ситуацій і скорочення часу їх усунення. Так, із доповіді ACFE [9] випливає, що організації, які застосовують у повсякденній діяльності інструменти моніторингу та прогнозу в інформаційно-телекомунікаційних (ІТ) системах, знижують свої втрати на 60 % порівняно з організаціями, які їх ігнорують.

При цьому моніторинг функціонального стану мережевих елементів передбачає:

- збір даних із різного роду датчиків про стан контрольованих об'єктів, а також аналіз неструктурованої інформації з метою вилучення даних;
- автоматичну (ручну - оператором) постановку об'єктів моніторингу на контроль;
- відображення об'єктів моніторингу за шкалою технічного (функціонального) стану за критеріями (інтегральними показниками) співвідношення поточного (або прогнозованого значення) індикатора (метрик) із пороговим значенням, яке забезпечує класифікацію стану («нормальний», «аварійний», «передаварійний» чи подібні до них).

Під час розробки підсистем мережевого моніторингу на ІТКМ досліджувані характеристики відхилення експлуатаційних параметрів (метрик) від порогової норми можливо одержати як внаслідок процедур пасивного моніторингу, застосовуючи систему вбудованого контролю мережевого елемента з трансляцією результатів на диспетчерський рівень ІТКМ (сервер моніторингу), так і дистанційно шляхом активного опитування периферії за допомогою агентного підходу, коли інтелектуальні агенти (ІА) застосовують керуючі пакети сервера моніторингу, які реалізують керування ІТКМ, а саме: «аномальні» або «аварійні» параметри. При цьому вбудована система контролю (моніторингу) функціонує на локальному рівні ІТКМ, в інтересах периферійного мережевого елемента визначає «аномальний» («аварійний» або «передаварійний») технічний стан щодо «нормального» на основі статистичних даних його характеристик (параметрів). А сервер моніторингу, переглядаючи систему широким оперативним полем, здатний розв'язувати проблеми функціональної безпеки всієї ІТКМ, не допускаючи її блокування або зниження рівня надійності та деградації.

Уявімо гетерогенну ІТКМ у вигляді ієрархічної територіально-розподіленої системи, що дає змогу здійснювати перерозподіл функцій моніторингу (серверу моніторингу) в залежності від поточного на даний момент часу стану рис. 1.

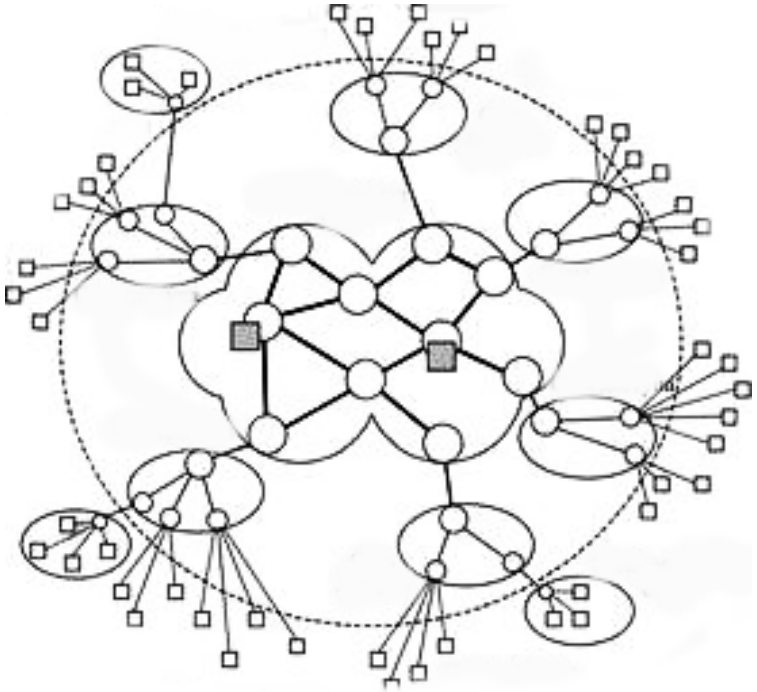

Рис. 1. Рівні розукрупнення інформаційно-телекомунікаційної мережі

Така структура ІТКМ дає змогу відійти від чіткої централізації управління нею до децентралізованого управління, а отже і моніторингу. При цьому, управління такою глобальною системою не може бути централізованим через зміни поточного стану мережі, затримки, що виникають, а також величезний потік керуючої інформації. Для сучасних ІТКМ ЗК, побудованих на базі широкосмугових і високонадійних волоконно-оптичних і космічних каналах зв'язку, це не є проблемою, проте для гетерогенних ІТКМ (особливо для ІТКМ СП), які функціонують на основі низькошвидкісних мереж з високим коефіцієнтом помилок (радіомережі та мережі бездротового радіодоступу) скорочення обсягу керувальної і вимірювальної інформації (ВІ) у підсистемах моніторингу й керування функціонуванням, є актуальною задачею. Це пов'язано з тим, що в алгоритмах роботи таких ІТКМ продуктивність систем залежить від прийнятих рішень, які ухвалюють з урахуванням поточного стану мережі, її деградації та дестабілізуючих впливів зовнішнього середовища.

Опис процесу моніторингу інформаційно-телекомунікаційної мережі на основі поетапного принципу з застосуванням мультиагентного підходу. Такий опис ІТКМ дає змогу реалізувати поетапний процес моніторингу, коли на першому етапі за локальною ВІ про стан периферії визначаються наявність порушення режиму роботи, а на другому і наступних етапах уточнюються ступінь і тип порушення. При цьому кожен з етапів пов'язаний із відповідним рівнем ієрархії ІТКМ. У разі виявлення аномалії у змінах значень контрольованих параметрів мережевих елементів і каналів зв'язку здійснюється розсилка інтелектуальних агентів, що мають нумерацію за рівнями ІТКМ (рис. 2). Аномалією на мережевій структурі при цьому розуміють такий стан мережевого елемента, коли спостерігається відхилення підконтрольного параметра за межі допуску.

В таких умовах моніторинг не може бути суворо централізованим за будь-якої широкосмугової системи внаслідок затримок, що виникають під час збирання ВІ та передання керуючих дій, через зниження швидкості поширення в протяжних каналах.

Важливість реалізації розподіленого опрацювання інформації в ІТКМ підіймає питання розробки нових методів керування інформаційними ресурсами, на основі моніторингу стану мережевих елементів, що дають змогу підвищити оперативність обміну даними, а також істотно скоротити обсяги циркулюючої мережею ВІ та керуючої інформації, не знижуючи якості функціонування системи загалом. Організація управління ресурсами ІТКМ сьогодні охоплює такі заходи: збір ВІ про стан мережевих елементів, аналіз якісних характеристик

роботи комунікаційного обладнання, застосування рішення про стан мережі та розробку керуючих впливів. Реалізація ж завдань системи моніторингу мережевих елементів досягається шляхом виконання такого функціоналу: збір оперативних і статистичних даних про якість роботи ІТКМ; збір даних про навантаження мережевого устаткування та каналів зв'язку; динамічний контроль мережевих обчислювальних і телекомунікаційних процесів, імовірнісно-тимчасові характеристики доставки інформації, а також розробка рішень з підтримкою їх у заданих межах; розподіл за сегментами мережі ВІ про зміни структури та про її функціональний стан.

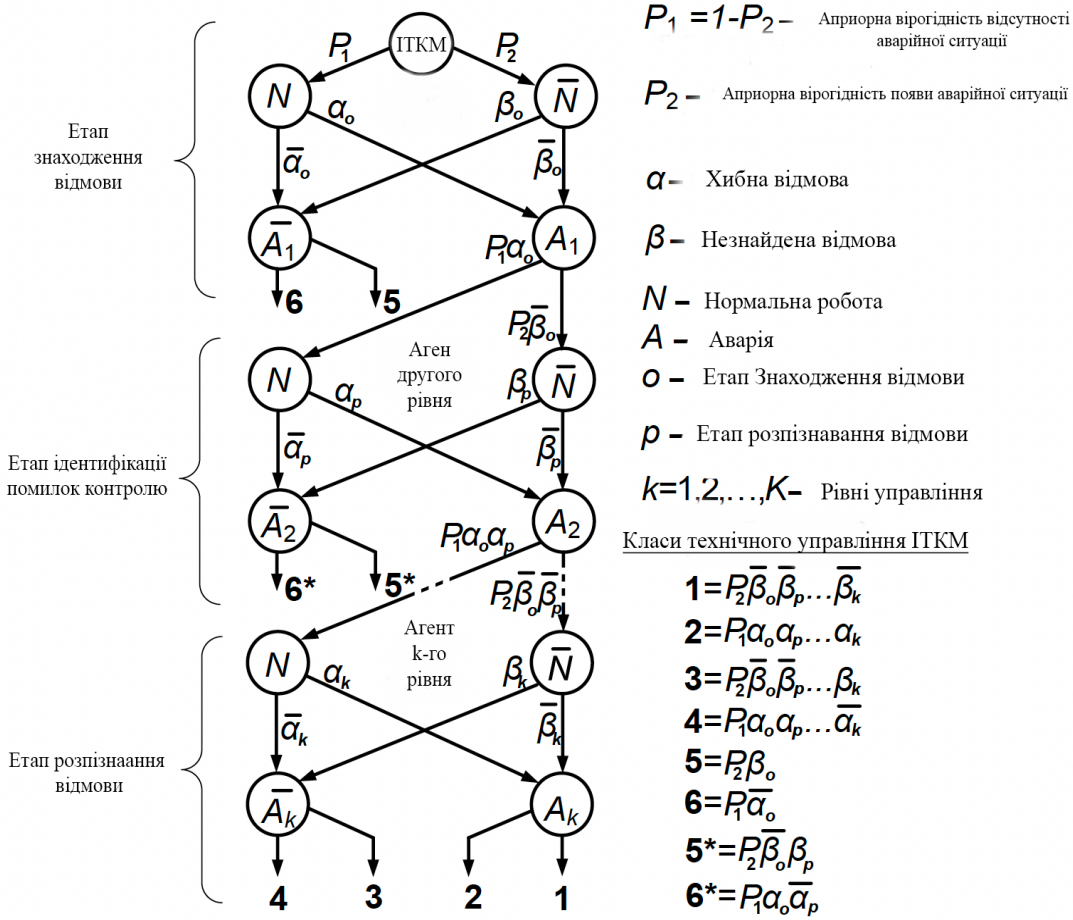

Рис. 2. Імовірнісний граф виявлення аномальної ситуації на ІТКМ

При цьому на першому етапі моніторингу за локальною інформацією, що міститься в мережевому елементі (вузлі комутації), визначають наявність порушення режиму роботи, а на другому і наступних етапах уточнюють ступінь і тип порушення. Фактично реалізується інтелектуальна система моніторингу, що отримала назву в телебаченні - системи зі змінною апертурою, коли за нормального функціонування ІТКМ розподілена структура є широким оперативним полем усіх підсистем вбудованого контролю з малою роздільною здатністю, достатньою лише для виявлення на локальному рівні порушення функціонування мережевого елемента (вихід із ладу вузла комутації, лінії зв'язку, переповнення буфера пам'яті, блокування мережі тощо) та надсилання інтелектуального агента на вищий рівень (розпізнавання).

Класифікація функціонального стану ІТКМ на основі критерію Байєса. Перелічені функції підсистеми моніторингу, що отримали назву сетеметрії, дозволяють сформулювати завдання управління мережевими ресурсами з позиції математичної статистики, що входить до завдань ідентифікації стану мережі та представляє собою завдання розрізнення гіпотез. З аналізу функцій управління поточний стан ІТКМ описують вектором $S = S(x_1, x_2, \ldots, x_n)$ в n-мірному просторі ознак, що формується з простору вихідного опису. При цьому теорія

статистичних рішень дозволяє знайти метод, заснований на результатах аналізу, що дає з мінімальною ймовірністю помилки відповідь на питання, якого з двох множин N чи $\bar{N}$ належить цей стан ІТКМ і відповідний вектор S, де $N \in \bar{A}$ – нормальний або $\bar{N} \in \bar{A}$ – аномальний стан.

У процесі визначення класу технічного стану мають місце помилки: першого роду α, коли гіпотеза U_1 $(S = \bar{N})$ відхиляється, хоча вона справедлива; та другого роду β, коли приймається гіпотеза U_2 $(S = N)$, але виявляється справедливою гіпотеза U_1 $(S = \bar{N})$.

Як основне вирішальне правило системи моніторингу обрано критерій Байєса, що забезпечує найвищу точність вирішення двоальтернативних завдань ідентифікації. При цьому важливо мінімізувати середній ризик W, або середню вартість ухвалення рішення про наявність помилок першого та другого роду: $W = \delta_a \cdot \alpha + \delta_b \beta$, де – δ_a вага помилки першого роду, а – δ_b вага помилки другого роду. Запишемо це правило:

$$S \in N, \text{ якщо} \frac{P(x_1,\dots,x_n/N)}{P(x_1,\dots,x_n/\bar{N})} > \frac{\delta_a P(\bar{N})}{\delta_b P(N)} = \theta;$$

$$S \in \bar{N}, \text{ якщо } \frac{P(x_1,\dots,x_n/N)}{P(x_1,\dots,x_n/\bar{N})} << \frac{\delta_a P(\bar{N})}{\delta_b P(N)} = \theta,$$

де $P(x_1, \dots, x_n/N)$ та $P(x_1, \dots, x_n/\bar{N})$ – умовні щільності ймовірності нормального та аварійного стану ІТКМ відповідно, $P(\bar{N}) = 1 - P(N)$ –апріорна ймовірність виникнення аварії. Це правило θ мінімізує середній ризик і порівнює відношення ймовірностей з порогом θ, що є постійною величиною для значень ваг δ_a та δ_b. Його називають критерієм Байєса, а відношення $L(x_1, \dots, x_n) = \frac{(P(x_1,\dots,x_n/N))}{(P(x_1,\dots,x_n/\bar{N}))}$ – відношення правдоподібності.

Умовні щільності ймовірності $P(x/N)$ та $P(x/\bar{N})$ формуються у процесі навчання системи моніторингу, при цьому слід припустити, що вони виявляються близькими до істинних, оскільки критерій Байєса забезпечує найвищу точність рішення двоальтернативних завдань розпізнавання (ідентифікації).

Оскільки на k-му етапі підсистема моніторингу може робити помилки першого $\alpha(x_{0k})$ і другого роду $\beta(x_{0k})$, то необхідно розв'язання задачі вибору порогів x_{0k} на К етапах. Тоді з урахуванням прийнятих позначень запишемо вирази для визначення ймовірності хибної тривоги (ХТ)

$$\alpha(x_{ok}) = \int_{x_{ok}}^{\infty} f(x_k/N)dx_k$$

та пропуску відмови (ПВ),

$$\beta(x_{ok}) = \int_{-\infty}^{x_{ok}} f(x_k/\bar{N})dx_k$$

З наведеного на рис.2 ймовірнісного графа виявлення аномалій отримаємо сумарні помилки пропуску відмови $P_{пв} = P_2\left[1 - \prod_{k=1}^{K} \beta(x_{ok})\right]$ і хибної тривоги $P_{хт} = P_1 \cdot \prod_{k=1}^{K} \alpha(x_{ok})$, для всієї системи, де $P_1 = 1 - P_2$ – апріорна ймовірність появи аварії, P_2– апріорна ймовірність її відсутності. Відповідно до критерію Неймана-Пірсона зафіксуємо ймовірність $P_{хт}$ на заданому рівні та мінімізуємо$P_{пв}^{min}$. Мінімізація $P_{пв}$ в якій змінні X_{0k} пов'язані функціональною залежністю $P_{хт}$, є умовним завданням оптимізації з функціоналом:

$$\Phi = P_2\left[1 - \prod_{k=1}^{K} \beta(x_{ok})\right] + \lambda P \prod_{k=1}^{K} \alpha(x_{ok}),$$

де λ – невизначений множник Лагранжа. Знайшовши приватні похідні $\frac{\partial \Phi}{\partial x_0 k}$ отримаємо систему К рівнянь, що спільно з рівняннями $P_{пв}$ та $P_{хт}$ дозволить знайти множник λ і К змінних $x_0 k$. Продиференціювавши результат в отриманих рівняннях шуканими будуть оптимальні пороги класифікації кожному етапі $(x_{01}^*, x_{02}^*, \dots, x_{0k}^*, \dots x_{0K}^*)$ які мінімізують ймовірність пропуску відмови $P_{пв}^{min}$, пов'язану з найменшою ймовірністю помилки виникнення аварії. Це рішення дозволяє однозначно визначити можливість застосування правильного рішення про відсутність відмови у роботі підсистем ІТКМ: $\overline{P}_{пв} = 1 - P_{пв}^{min}$. На наступних етапах аналізу

піддається інформація про прийняття вірного рішення $\overline{\beta}_k = 1 - \beta_k$, тобто про нормальне функціонування ІТКМ. Оскільки рішення про нормальне функціонування системи на першому етапі може бути прийнято на основі локальної інформації про стан мережного вузла, наприклад, завантаження процесора, обсяг буферної пам'яті та ін.), то немає необхідності обміну інформацією з іншими вузлами мережі. На другому та останньому етапах поряд з $\overline{P}_{\text{пв}} = 1 - P_{\text{пв}}^{\min}$ аналізу піддається впливу та частина інформації, яка обумовлює появу ймовірностей хибної тривоги: $P_1\alpha_1, P_1\alpha_1\alpha_2, \dots, P_1\alpha_1\alpha_2, \dots, \alpha_k$ і яка повинна піддаватися подальшому аналізу.

Поетапний принцип моніторингу при виявленні аномалії на ІТКМ забезпечує точність не гірша за байєсову, тому що використовує на кожному з етапів незалежні ознаки розпізнавання аномальних ситуацій у кожному з мережевих елементів та сегментів мережі. При цьому ступінь скорочення обсягу II залежить від величини помилок першого роду (хибної відмови), що виникають кожному з етапів функціонування підсистеми моніторингу. На останньому k-му етапі роботи інтелектуального агента підсистеми моніторингу виділено фінальні ймовірності стану ІТКМ, якими визначають клас її технічного стану: «1» – ІТКМ заблокована, відмова виявлена та розпізнана; «2» – ІТКМ працездатна, хибне виявлення та розпізнання (хибна тривога); «3» – ІТКМ заблоковано, відмову виявлено, але не розпізнаний (перепустка відмови); «4» – ІТКС працездатна, хибне виявлення та правильне розпізнавання; «5» – ІТКМ заблоковано, відмову не виявлено; «6» – ІТКМ працездатна, визнано такою.

Етапи реалізації процедури моніторингу функціонального стану ІТКМ. Поданий на рис. 2 ймовірнісний граф виявлення аномальної ситуації на ІТКМ ліг в основу методу розподіленого моніторингу багаторівневої системи, здатного працювати у трьох режимах: виявлення відмови; оцінки помилок контролю та режим навчання [10].

У режимі виявлення відмови на ІТКС (перший етап моніторингу) проводять вимірювання уз агальненого показника системи $\bar{x}$, та виміряне значення перетворюється відповідно до виразу $\Lambda(x) = ln\frac{f(x/N)}{f(x/\overline{N})}$, де Λ(x)- ставлення правдоподібності. Далі відбувається порівняння величини $\Lambda(x)$ з пороговим значенням x_0. Якщо $\Lambda(\text{x}) > x_0$ тобто порушення режиму функціонування ІТКМ не виявлено, то фіксується нормальне (N) працездатний стан системи. В іншому випадку (якщо $\Lambda(\text{x}) < x_0$), фіксується

аномальний ($\overline{N}$) стан системи та виробляється більш достовірна оцінка її стану шляхом дослідження набору ознак $y_i, \dots, \gamma_i$, що надходять з підсистем вбудованого контролю мережевих елементів контурів управління різних рівнів ієрархії системи, де $i = \overline{1, M}$. Значення виміряних ознак k-го контуру управління, де $k = 1, 2, \dots, K$ переводять в ознаки «параметри», за якими формують величини від $\Lambda(y_i) = ln\frac{f(y_i/N)}{f(y_i/\overline{N})}$ і т.д., до $(\gamma_i) = ln\frac{f(\gamma_i/N)}{f(\gamma_i/\overline{N})}$, надалі сумуються за рівнями управління для порівняння отриманих сум із порогами $y_0 \dots \gamma_0$. У випадку, коли $\sum_{i=1}^{n}\Lambda(y_i) < y_0$, то формується сигнал, що фіксує екстремальну ситуацію, що надходить у сервер моніторингу для реєстрації та в інтересах системи підтримки прийняття рішень (СППР). Аналогічно відбувається виявлення порушення працездатності системи та на наступних контурах моніторингу ІТКМ. Порядок реалізації методу наведено у [10]. У режимі ідентифікації помилок контролю ІТКМ (другий етап моніторингу) використовується генератор штучного трафіку, який моделює нормальний N і аномальний $\overline{N}$ стан багаторівневої телекомунікаційної системи відповідно до апріорних ймовірностей $P_1 = P(N)$ і $P_2 = 1 - P_1 = P(\overline{N})$. Залежно від величини порогового значення x_0, та реалізацією випадкової величини Λ(x), приймають рішення про стан системи. При цьому фіксуються стани «хибної тривоги» та сумарного, обумовленого виявником (в) і розпізнавачем (р) «перепустки відмови» при достатньо великому числі випробувань: $P_{\text{хт}} = P_1\alpha_{\text{в}}\alpha_{\text{р}}$; $P_{\text{пв}} = P_2\left(1 - \overline{\beta_{\text{в}}\beta_{\text{р}}}\right)$. Аналогічно відбувається фіксація «перепустки відмови» та «хибної тривоги» і на наступних за ієрархією рівнях моніторингу ІТКМ.

У режимі навчання підсистеми моніторингу у зв'язку із багатоетапним принципом роботи передбачається розпізнавання функціонального стану за сигналом з виявника, коли

відбувається зменшення $P_{\text{хт}}$ рахунок збільшення $P_{\text{пв}}$. При оптимізації сумарної величини $P_{\Sigma} = \lambda P_{\text{хт}} + P_{\text{пв}}$, де $0 \le \lambda \le 1$ невизначений множник Лагранжа, зменшення другого доданку може бути досягнуто за рахунок оптимального вибору порогів $(x_0^*, y_0^*, \dots, \gamma_0^*)$. При цьому зменшення значень $x_0, y_0, \dots \gamma_0$ проводиться за m випробувань шляхом уточнення $(m-1)$ випробування $x_0(m-1), y_0(m-1), \dots \gamma_0(m-1)$ за рахунок $\Delta x_0^m, \Delta y_0^m, \dots, \Delta \gamma_0^m$ відомими методами, наприклад, методом стохастичної апроксимації.

Оптимізація порогів класифікації виду функціонального стану ІТКМ. У тому випадку, коли детектор і розпізнавач стану ІТКМ відповідно на першому і другому етапах - припускаються помилок першого (α_0, α_p) і другого (β_0, β_p) роду, стає актуальним питання вибору порогів під час класифікації стану системи на наявність (А) і відсутність ($\overline{\text{А}}$) аномалій. Розрахуємо оптимальні значення порогів класифікації, що забезпечують мінімальну похибку ідентифікації стану для дворівневої ІТКМ.

Оскільки $\bar{\alpha}_0 = 1 - \alpha_0$, $\bar{\alpha}_p = 1 - \alpha_p$, $\bar{\beta}_0 = 1 - \beta_0$, $\bar{\beta}_p = 1 - \beta_p$ з графа, що пояснює роботу підсистеми моніторингу ІТКМ (рис. 2), як показано вище, отримаємо вирази для ймовірності $P_{\text{хт}}$ і $P_{\text{пв}}$ при двоетапній процедурі контролю стану системи. Відповідно до критерію Неймана-Пірсона вимагатимемо мінімуму $P_{\text{пв}}$ за умови $P_{\text{хт}} = cont = c$:

$$\text{Min} P_2\left(1 - \overline{\beta_0 \beta_p}\right) \tag{1}$$

З урахуванням наведених на рис. 3 кривих густин розподілу ознаки *x* за нормального стану ІТКМ $f\left(\frac{x}{N}\right) = f_1(x)$і $f\left(\frac{x}{\bar{N}}\right) = f_2(x)$- за її аномального стану, маємо:

$$\begin{cases} \alpha_0 = \int_{x_0}^{\infty} f_1(x)dx \\ \beta_0 = \int_{-\infty}^{x_0} f_2(x)dx \end{cases} \tag{2}$$

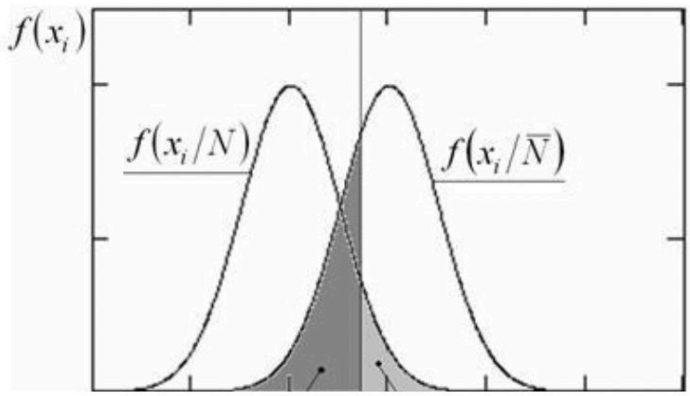

Рис. 3. Закони розподілення ознак

Вигляд густин імовірностей розподілу ознак x і y для двоетапної процедури контролю показано на рис. 4 а) і б), з чого випливає:

$$\begin{cases} \alpha_p = \int_{y_0}^{\infty} f_1(y)dx \\ \beta_p = \int_{-\infty}^{y_0} f_2(y)dx \end{cases} \tag{3}$$

Тоді умови (1) з урахуванням (2) і (3) представимо в такому вигляді:

$$P \int_{x_0}^{\infty} f_1(x)dx \int_{y_0}^{\infty} f_1(y)dy = c \tag{4}$$

У тому разі, коли на другому етапі розпізнавання здійснюють за кількома довільно розподіленими ознаками $\bar{y} = [y_1, y_2, \dots, y_n]$, для знаходження результуючої помилки розпізнавання можна скористатися відомими методами. Оскільки в цьому разі пороги класифікації на першому і другому етапах пов'язані функціональною залежністю $[x = \varphi(y_0)]$, то в результаті диференціювання за нижньою межею отримаємо умову, що дає змогу знайти

оптимальне значення порогів класифікації, що забезпечують мінімальну похибку ідентифікації стану телекомунікаційної системи.

Пропонований метод розподіленого моніторингу ІТКМ на основі поетапної процедури ухвалення рішення, порівняно з відомими технічними рішеннями, дає змогу обґрунтувати вибір граничних значень x_0, y_0, вирішуючи дану задачу. В ІТКМ краще мати помилку першого роду α_0 (хибну тривогу), ніж помилку другого роду β_0, (пропуск відмови). У зв'язку з чим, кращими на рис. 2 будуть стани системи «6» і «1».

Помилки контролю пропонованого методу можна знизити завдяки навчанню системи керування шляхом аналізу поточної інформації, що накопичується в процесі функціонування системи, методами статистичної теорії розпізнавання образів.

Коли вигляд функцій $f_1(x), f_2(x), f_1(y), f_2(y)$, дає змогу проводити оптимізацію аналітичними методами, завдання значно спрощується, наприклад, у разі релеївських законах.

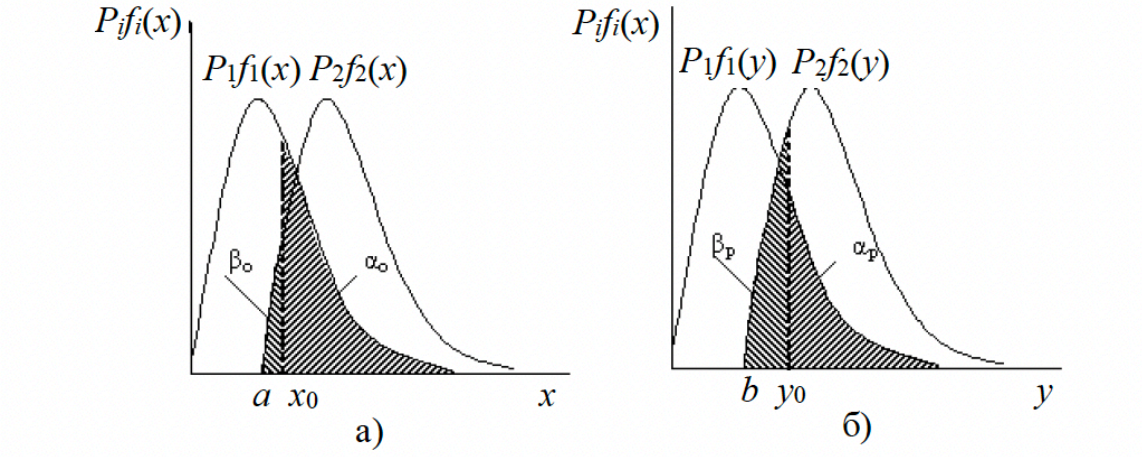

Рис. 4. Закони розподілення ознак x та y для двоетапної процедури контролю

$$\frac{dx_0}{dy_0} f_2(x_0) \int_{y_0}^{\infty} f_2(y)dy + f_2(y_0) \int_{x_0}^{\infty} f_2(x)dx = 0 \qquad (5)$$

Нехай $f_1(x) = xe^{\frac{x^2}{2}};\ f_2(x) = (x-a)e^{\frac{(x-a)^2}{2}};$

$f_1(y) = ye^{\frac{y^2}{2}};\ f_2(y) = (y-b)e^{\frac{(y-b)^2}{2}};$

В цьому разі рівняння (4), (5) приводяться до вигляду:

$$x_0^2 + y_0^2 = 2ln\frac{P_1}{c} \qquad (6)$$

$$\frac{dx_0}{dy_0}(x_0 - a) + (y_0 - b) = 0 \qquad (7)$$

Продиференціювавши (6) за y_0 і підставивши результат у (7), отримаємо їхнє спільне рішення

$$x_0^* = \sqrt{\frac{2ln^{P_1}/_c}{1+\left(b/a\right)^2}}, \quad y_0^* = \sqrt{\frac{2ln^{P_1}/_c}{1+\left(a/b\right)^2}} \qquad (8)$$

Використовуючи рівняння (8), одержимо значення мінімальної ймовірності «пропуску відмови» (невиявлюваного порушення режиму нормального функціонування) ІТКМ:

$$P_{\text{пв}}^{min} = P\left\{1 - \frac{c}{P}\exp\left[\sqrt{2(a^2+b^2)ln^{P_1}/_c} - \frac{1}{2}(a^2+b^2)\right]\right\} \qquad (9)$$

Скорочення обсягу вимірювальної інформації за рахунок поетапного моніторингу. Порівняння двох і одноетапної процедур виявлення аномальних станів ІТКМ через відношення відповідних потужностей розв'язання [11] $k_c = \bar{\beta}_2/\bar{\beta}_1$, за однієї й тієї самої

ймовірності «хибного» розв'язку c, дає змогу зробити висновок, що виграш стосовно зменшення ймовірності $P_{ПР}^{min}$ суттєво зростає зі зменшенням величини $P_{хт}$ та ступеню перетину класів під час виявлення і розпізнавання (величин a і b):

$$k_c = \exp\left\{\sqrt{ln\,{}^{P_1}/_c}\left[\sqrt{2(a^2+b^2)-a\sqrt{2}}\right]-{}^{b^2}/_2\right\}$$

Криві залежності $k_c = f(c)$ (за a = 1 і різних значень b), що ілюструють величину виграшу, подано на рис. 5

Оскільки рішення про нормальне функціонування ІТКМ на першому етапі може бути ухвалене на основі локальної інформації про стан вузла (наприклад, обсяг буферної пам'яті, стан каналів зв'язку та ін.), то немає необхідності обміну інформацією з іншими вузлами мережі.

На другому і наступних етапах аналізу піддається та частина інформації, що зумовлює появу ймовірностей хибної тривоги $P_1\alpha_1, P_1\alpha_1\alpha_2, \ldots, P_1\alpha_1\alpha_2, \ldots, \alpha_n$ ІТКМ за рахунок збільшення числа (2, 3, 4, 5, 10) його етапів.

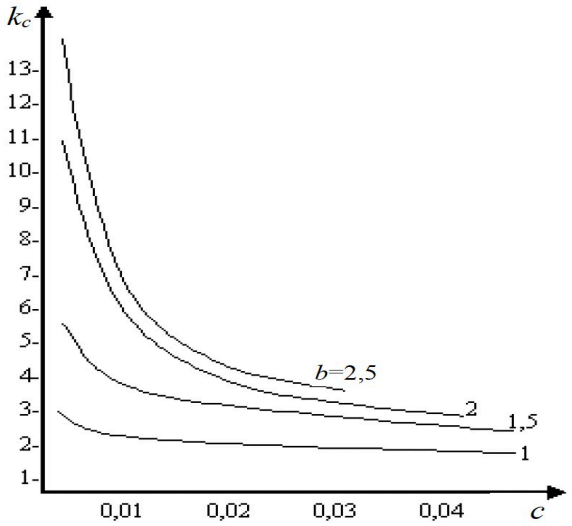

Рис. 5. Порівняльна оцінка багатоетапних процедур контролю

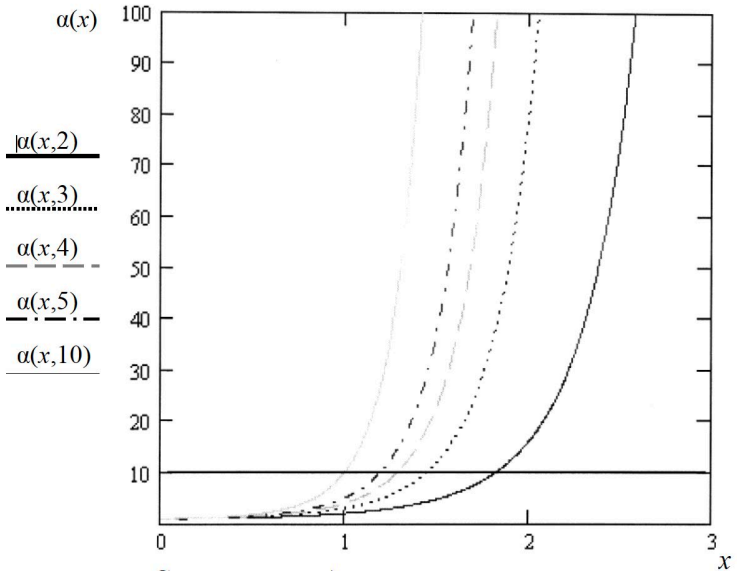

Рис. 6. Скорочення обсягу ВІ у системі моніторингу

Значення $P_{хв} = P_1\alpha_1(1+\alpha_2+\alpha_2\alpha_3+\cdots+\alpha_2\alpha_3,\ldots\alpha_k)$ визначає ту частину потоку вимірювальної інформації, прийняту за 1, що підлягає аналізу на другому та наступних етапах,

і фактично вона визначає ступінь скорочення з η_c обсягу інформації, що має передаватися між вузлами мережі для уточнення типу порушення: $\eta_c = {}^{1}/_{P_1\alpha_1}(1+1+\alpha_2+\alpha_2\alpha_3+\cdots+\alpha_2\alpha_3,\ldots\alpha_k)$.

Висновки

Таким чином, ступінь скорочення обсягу ВІ, що циркулює в системі моніторингу, залежить від величини помилок першого роду, що виникають на кожному з етапів, і становить величину від 1,1 до 3 разів (рис. 6). При цьому поетапна процедура моніторингу ІТКМ забезпечує найвищу точність виявлення аномальних ситуацій у системі, оскільки використовує на кожному етапі незалежні ознаки розпізнавання і, отже, є не гіршою за байєсову. За поетапного моніторингу застосування рішення про стан ІТКС здійснюється із залученням додаткових ознак у міру необхідності. Число включень етапів зменшується в міру зростання номера етапу в хі разів. Контроль закінчується в тому разі, якщо ухвалено рішення про нормальне функціонування системи. Останні етапи використовують досить рідко, при цьому сумарна кількість ШІ в межі досягає максимальної величини, практично використовуючи всю доступну виміру інформацію, яку постачає система мережеметрії, для ухвалення рішення про стан багаторівневої ІТКМ.

Аналіз результатів моделювання (рис. 6) показує, що виграш у скороченні обсягу ВІ порівняно з відомими підходами [12] залежить від інформативності ознак розпізнавання на другому й наступних етапах, оскільки вона на першому етапі виявляється фіксованою і визначається обсягом вільного буферного простору, величину якого можна строго контролювати за локальною інформацією від вузлів ІТКМ.

Однак збільшення інформативності ознак на наступних етапах пов'язано з вимірами в системі, обсяг яких визначає якість прийняття рішення при поетапному контролі. Ці вимірювання для підвищення інформативності пов'язані з необхідністю залучення додаткових вимірювальних ресурсів і збільшенням часу аналізу.

Побудова багаторівневої ІТКМ на основі багатоетапної процедури моніторингу порівняно з іншими відомими технічними рішеннями дає змогу обґрунтувати вибір порогових значень $x_0, y_0, \ldots\gamma_0$, розв'язуючи дану задачу оптимальним чином у сенсі мінімуму помилок класифікації аномальних станів системи.

Помилки контролю пропонованого методу можна знизити завдяки навчанню підсистеми моніторингу шляхом аналізу поточної інформації, що накопичується в процесі функціонування ІТКМ, методами статистичної теорії розпізнавання образів.

Таким чином, під час реалізації пропонованого методу розподіленого моніторингу багаторівневої гетерогенної ІТКМ мережу розбивають на деякі множини пов'язаних між собою підмереж, що об'єднують близько розташовані вузли. У кожній підмережі існує місцевий центр моніторингу (сервер моніторингу), який одержує інформацію про стан цієї підмережі і виробляє для них директиви. Усі місцеві центри моніторингу (сервери моніторингу) з'єднані між собою широкосмуговими каналами та обмінюються інформацією, використовуючи керувальні пакети з високим пріоритетом. Це дає можливість серверам моніторингу враховувати не тільки локальну картину стану ІТКМ, а й глобальну.

Використовуючи подібний принцип, створюється адаптивна система управління. При нормальному функціонуванні розподілена структура проглядається широким оперативним полем з малою роздільною здатністю, достатньою для виявлення локального порушення режиму. Надалі відбувається звуження оперативного поля в околиці порушення, яке проглядається більш детально, і шляхом більш тонкого аналізу проводиться виявлення характеру (розпізнавання).

Список використаної літератури:

1. A Software Deep Packet Inspection System for Network Traffic Analysis and Anomaly Detection / W. Song et al. Sensors. 2020. Vol. 20, no. 6. P. 1637. URL: https://doi.org/10.3390/s20061637.

2. IMPROVING THE QUALITY OF HETEROGENEOUS TELECOMMUNICATION NETWORKS WITH THE HELP OF FORECAST-BASED RESOURCE ALLOCATION. Telecommunication and Information Technologies. 2024. Vol. 82, no. 1. URL: https://doi.org/10.31673/2412-4338.2024.018894.

3. Machine Learning in Network Anomaly Detection: A Survey / S. Wang et al. IEEE Access. 2021. Vol. 9. P. 152379–152396. URL: https://doi.org/10.1109/access.2021.3126834.

4. Trace-Ability and Security Detection of Container Image Based on Inheritance Graph, Y. Zheng, W. Dong and J. Zhao et al. IEEE Access. 2021 IEEE 5th International Conference on Cryptography, Security and Privacy (CSP), Zhuhai, China, 2021, pp. 186-192, URL: https://doi.org/10.1109/CSP51677.2021.9357496.

5. Сучасні технології безпроводового доступу в телекомунікаційних системах / Стелюк, Б.Б., Костенко В.В., Семененко О.А. Міжнародна наукова конференція «Інноваційні технології, моделі управління кібербезпекою ІТМК-2021» 14-16 квітня 2021. Збірник тез, Дніпро, 2021, с. 13

6. Підвищення ефективності гетерогенних телекомунікаційних мереж / Васильківський М.В., Чанхао Ю. (2019) (Doctoral dissertation, ВНТУ) с. 74-79.

7. Report to the Nations on Occupational Fraud and Abuse. URL: https://www.acfe.com/rttn/docs/ 2014-report-to-nations.pdf

8. Probabilistic Graphical Models: Principles and Techniques. The MIT Press, 2009. p. 1231. Nir Friedman D. K.

9. Detection of abrupt changes: Theory and application. Englewood Cliffs, N.J : Prentice Hall, 1993. P. 528. Basseville M.

10. Paradigms for Mobile Agent-Based Active Monitoring of Network Systems https://ajanta.cs.umn.edu/papers/monitoring-paradigms.pdf.

11. "Multi-Agent Systems: An Introduction to Distributed Artificial Intelligence"/ Jacques Ferber. Addison-Wesley, 1999

Автор статті

Прокопенко Андрій – аспірант, Державний університет інформаційно-комунікаційних технологій, Київ, Україна.

ORCID: 0009-0009-7227-3458

Author of the article

Prokopenko Andrii – postgraduate, State University of Information and Communication Technologies, Kyiv, Ukraine.

ORCID: 0009-0009-7227-3458