https://doi.org/10.31891/2219-9365-2026-86-17
УДК 004.056:004.75:621.39

ХВОРОСТЯНИЙ Родіон
Державний університет інформаційно-комунікаційних технологій
https://orcid.org/0009-0004-4591-7100
rodionhvorostyanoy@gmail.com

МУЛЬТИАГЕНТНИЙ ПІДХІД ДО БАЛАНСУВАННЯ НАВАНТАЖЕННЯ ТА ЗАБЕЗПЕЧЕННЯ СТРУКТУРНОЇ СТІЙКОСТІ ТРАНСПОРТНИХ ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖ В УМОВАХ ВПЛИВУ КІБЕРАТАК

У статті розглядаються питання забезпечення кіберстійкості транспортних телекомунікаційних мереж на основі мультиагентного підходу. Показано, що сучасні транспортні телекомунікаційні мережі є критично важливими об'єктами інфраструктури держави та характеризуються високою вразливістю до деструктивних кібератак, які можуть призводити до перевантаження вузлів, порушення маршрутизації та втрати структурної зв'язності мережі. Проведений аналіз існуючих підходів до управління кібербезпекою транспортних телекомунікаційних мереж засвідчив їх недостатню адаптивність, автономність та обмежені можливості щодо забезпечення балансування навантаження і структурної стійкості в умовах динамічних атак. Запропоновано удосконалену модель мультиагентного балансування навантаження, яка враховує поточний рівень ризику компрометації вузлів і каналів зв'язку, а також дозволяє адаптивно перерозподіляти трафік між більш безпечними маршрутами. Модель базується на задачі багатотоварного оптимального потоку з урахуванням ризиків кібератак та реалізується у вигляді ітераційного алгоритму локальної взаємодії агентів. Розроблено метод мультиагентної взаємодії для забезпечення структурної стійкості транспортної телекомунікаційної мережі до кібератак, який базується на виявленні критичних вузлів та формуванні мінімально необхідної кількості резервних зв'язків для відновлення зв'язності мережі. Метод використовує матричний аналіз досяжності та графові алгоритми пошуку компонент зв'язності. Наведено результати моделювання, які підтверджують ефективність запропонованих рішень щодо підтримання працездатності мережі, зниження ризику компрометації маршрутів та забезпечення структурної стійкості транспортних телекомунікаційних мереж в умовах впливу кібератак.

Ключові слова: транспортна телекомунікаційна мережа, мультиагентна система, кібербезпека, кібератака, балансування навантаження, структурна стійкість, резервні канали зв'язку.

KHVOROSTIANYI Rodion
State University of Information and Communication Technologies

MULTI-AGENT APPROACH TO LOAD BALANCING AND ENSURING STRUCTURAL STABILITY OF TRANSPORT TELECOMMUNICATION NETWORKS UNDER THE IMPACT OF CYBERATTACKS

The paper addresses problem of ensuring cyber resilience of transport telecommunication networks based on multi-agent approach. It is shown that modern transport telecommunication networks are critical infrastructure objects characterized by high vulnerability to destructive cyberattacks that may cause node overloads, routing disruptions, and loss of structural connectivity. Analysis of existing approaches to transport network cybersecurity management demonstrates insufficient adaptability, autonomy, and limited ability to provide efficient load balancing and structural resilience under dynamic cyberattacks. An improved multi-agent load balancing model is proposed, which takes into account current compromise risk level of network nodes and communication channels and enables adaptive traffic redistribution through more secure routes. Proposed model is based on multi-commodity flow optimization problem with cyber risk metrics and is implemented as iterative algorithm of distributed interaction between local agents. A method of multi-agent interaction for ensuring structural resilience of transport telecommunication networks against cyberattacks is also developed. Method is based on identification of critical nodes and determination of minimum required number of backup links necessary to restore network connectivity after attacks. Proposed approach additionally provides decentralized coordination of agents during topology recovery and adaptive reconfiguration of routing structure under conditions of repeated attacks. Simulation results confirm effectiveness of proposed solutions in maintaining network operability, reducing compromise risk of routing paths, balancing traffic load, and preserving structural connectivity under destructive cyber impacts.

Keywords: transport telecommunication network, multi-agent system, cybersecurity, cyberattack, load balancing, structural resilience, backup communication links.

Стаття надійшла до редакції / Received 02.04.2026
Прийнята до друку / Accepted 28.04.2026
Опубліковано / Published 31.05.2026

ПОСТАНОВКА ПРОБЛЕМИ У ЗАГАЛЬНОМУ ВИГЛЯДІ ТА ЇЇ ЗВ'ЯЗОК ІЗ ВАЖЛИВИМИ НАУКОВИМИ ТА ПРАКТИЧНИМИ ЗАВДАННЯМИ

На теперішній час транспортні телекомунікаційні мережі (ТТМ) є одним з найбільш важливих об'єктів критичної інфраструктури держави [1]. Особливістю їх функціонування є розподілена архітектура, побудована на базі великої кількості взаємопов'язаних вузлів та високошвидкісних каналів зв'язку. Водночас їх висока складність та відкритість до інтеграції з іншими мережами обумовлюють підвищену вразливість до

кібератак, результатом яких можуть бути суттєві наслідки для держави. Типові атаки на ТТМ включають: класичні мережеві DDoS-атаки; атаки на протоколи та механізми маршрутизації; компрометацію керуючої площини; порушення роботи оптичних каналів та комбіновані атаки. У якості заходів протидії застосовуються: архітектурні рішення, динамічне управління ресурсами, гнучка маршрутизація на рівні рівні IP/MPLS та OTN/DWDM.

Разом з тим, як відмічається у [2], існуючі підходи щодо протидії атакам у ТТМ не володіють адаптивністю та автономністю і вкрай слабко забезпечують процеси управління навантаженням та забезпечення стурктурної стійкості мережі в умовах впливу кібератак. Це, в свою чергу, визначає необхідність переходу до мультиагентних технологій управління, які позбавлені цих недоліків і здатні забезпечити необхідний рівень кіберстійкості.

У роботах [3,4] було запропоновано модель ієрархічної мультиагентної системи (МАС) управління кібербезпекою ТТМ (рис. 1), яка, в процесах виявлення загроз та реагування на атаки, базується на принципах розподілу функцій і поєднання локальної автономії з глобальною координацією. У такій мультиагентній системі управління кібербезпекою ТТМ застосовуються наступні типи агентів [3,4]:

- ✓ агент моніторингу (MA), який здійснює збір і первинну обробку даних про стан елементів ТТМ та передає результати іншим агентам системи;
- ✓ агент виявлення загроз (TDA), який виявляє кібератаки на основі аналізу аномалій, сигнатур і поведінкових характеристик мережі;
- ✓ агент оцінки ризику (RAA), який кількісно оцінює ймовірність та наслідки атак;
- ✓ агент ухвалення рішень (DMA) – обирає оптимальну стратегію протидії загрозам;
- ✓ агент реагування (RA) – реалізує заходи щодо реагування на атаки (фільтрацію трафіку, зміну маршрутів, ізоляцію сегментів);
- ✓ агент координації та переговорів (CNA), який, відповідно до глобальної стратегії захисту, узгоджує локальні рішення агентів.

Також, як показано у [3,4], до мультиагентної системи управління кібербезпекою ТТМ включаються і інші типи агентів: агент сервісу (SA), агент навчання (LA), агент політик (PA) і агент узгодження політик (PCA). Формальні моделі таких агентів визначаються архітектурою конкретної ТТМ та типом реалізованих завдань кіберзахисту. Таким чином, ієрархічна мультиагентна система реалізує сукупність взаємопов'язаних в єдину систему локальних і глобальних контурів управління, які відповідають структурній ієрархії ТТМ.

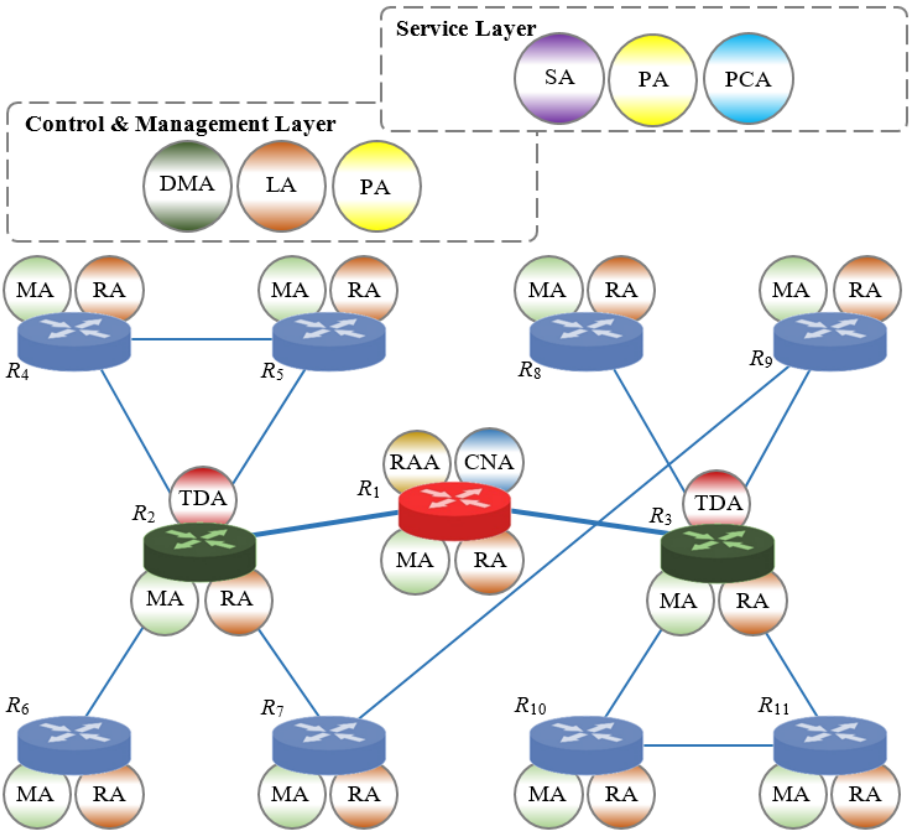


Рис. 1. Приклад структури мультиагентної системи управління кібербезпекою ТТМ [4]

Зважаючи на складність процесів функціонування мультиагентної системи управління кібербезпекою ТТМ загальна проблема на сьогоднішній день полягає у необхідності формування детального теоретичного опису процесів взаємодії агентів, який надав би дослідникам можливість вивчення систем управління такого типу. Основним фокусом при вирішенні такої проблеми можна вважати поєднання моделей та методів мультиагентного управління з функціоналом мережі, зокрема, у частині, що стосується забезпечення стійкості до атак різних типів шляхом запровадження ефективних механізмів балансування навантаження вузлів та забезпечення структурної стійкості мережі до атак.

АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ ТА ПУБЛІКАЦІЙ

Дослідженню питань застосування мультиагентного підходу в системах управління комп'ютерними мережами та у системах їх захисту присвячено достатньо велику кількість публікацій.

Так, публікація [5] надає глибокий огляд мультиагентних систем, які застосовуються в системах виявлення вторгнень (IDS). Автори пропонують таксономію існуючих підходів щодо застосування MAC в IDS. В той же час у роботі відзначається наявність проблеми недостатньої узгодженості стратегій взаємодії агентів та обробки складних подій на основі кореляційного аналізу у розподілених системах виявлення. Питання інтеграції MAC у розподілені IDS розглядаються у статті [6], де визначено, що MAC можуть покращити адаптивність та загальну ективність розподілених IDS при виявленні загроз. Разом з тим, автори не пропонують механізмів координації агентів у таких MAC в умовах обмеженої інформації та впливу перехресних загроз. Питання застосування розподілених IDS із застосуванням автономних агентів також розглядаються у [7], де автор пропонує архітектуру ієрархічної MAC без центрального елемента. Разом з тим, така модель розглядає лише механізми комунікації агентів і не охоплює питання щодо динамічності узгодження рішень у MAC, зокрема у випадку складних атак.

Робота агентів щодо спільного виявлення та реагування розглядається також в публікації [8], де описано MAC захисту в мережах IoT. В той же час ця робота пропонує лише загальні базові рішення, які не можуть бути реалізовані на практиці через складність процедур координації агентів. У [9] пропонується система мультиагентного навчання, яка може бути застосована для захисту мереж, хоча самі ж автори відмічають наявність проблем зі стійкістю у таких системах при застосуванні у складних сценаріях атаки.

В публікації [10] аналізуються приклади застосування MAC у кіберфізичних системах. Зокрема показано необхідність створення ефективних протоколів координації для обміну інформацією між агентами та вирішення конфліктів під час взаємодії. Архітектури мережевих IDS на базі MAC, які досліджуються у [11], свідчать про ефективність мультиагентної взаємодії на основі їх кооперації. Але, переважна більшість з них зводяться до централізованого аналізу даних, оскільки такі моделі не мають формальних механізмів розподіленої взаємодії агентів.

Таким чином, з наведеного огляду публікацій можна зробити висновок, що мультиагентний підхід є перспективним напрямом вирішення проблем кібербезпеки ТТМ. Разом з тим, залишається недослідженим широке коло питань розробки формальних моделей та методів взаємодії агентів у таких системах управління. Зокрема, функціонування агентів в системах управління кібербезпекою ТТМ на основі MAC має підпорядковуватись основному функціоналу ТТМ – передачі великих обсягів трафіку. Відтак, для подальші дослідження мають бути спрямовані саме на розроблення узгоджених моделей координації між агентами в складних мережевих середовищах, зокрема щодо балансування навантаження та забезпечення структурної стійкості ТТМ в умовах впливу кібератак.

Моделі балансування трафіку в комп'ютерних мережах розглядаються у роботах [12,13], проте, ключовою їх особливістю є необхідність присутності центрального спостерігача, в той час як концепція MAC передбачає розподілене вирішення проблеми балансування. Відтак, моделі [12,13] мають бути удосконалені з урахуванням прийнятої концепції управління кібербезпекою ТТМ на основі мультиагентного підходу. Методи забезпечення структурної стійкості є складовою частиною технології TI-LFA (Topology-Independent Loop-Free Alternate) з підтримкою BFD [12,13] – технологія швидкого резервування маршрутів у IP/MPLS-мережах, що забезпечує субсекундне переключення трафіку при відмові каналу або вузла. Разом з тим, така технологія також є централізованою і, за задумом розробників, придатна лише для захисту від фізичних відмов та не застосовується для протидії кібератакам. Зазначені обставини і визначають необхідність подальших досліджень у цьому напрямі.

ФОРМУЛЮВАННЯ ЦІЛЕЙ СТАТТІ (ПОСТАНОВКА ЗАВДАННЯ)

Метою статті є розробка теоретичних основ взаємодії агентів в мультиагентній системі управління кібербезпекою транспортної телекомунікаційної мережі, які б забезпечували баланс навантаження вузлів мережі та загальну стійкість її структури в умовах впливу на мережу деструктивних кібератак різних типів.

Досягнення поставленої мети передбачає вирішення наступних завдань:

удосконалення моделі мультиагентного балансування навантаження транспортної телекомунікаційної мережі в умовах впливу кібератак;

розробка методу мультиагентної взаємодії для забезпечення стійкості структури транспортної телекомунікаційної мережі до кібератак.

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ ДОСЛІДЖЕННЯ

Модель мультиагентного балансування навантаження транспортної телекомунікаційної мережі в умовах впливу кібератак

Вище було запропоновано ієрархічну мультиагентну систему управління кібербезпекою ТТМ, яка дозволяє діагностувати вузли мережі на предмет впливу наслідків кібератак. У результаті діагностування агентами MA, TDA та CNA визначається множина атакованих вузлів, які в подальшому виключаються з мережі, а трафік перерозподіляється неатакованими вузлами. Але, на практиці, повне виключення атакованих вузлів з роботи суттєво збільшує навантаження на решту неатакованих вузлів ТТМ. Атакований вузол у багатьох випадках може передавати деяку частину трафіку і, таким чином, забезпечити зв'язність мережі. Враховуючи розподілений характер роботи MAC, постає необхідність вирішення задачі щодо мультиагентного балансування навантаження ТТМ з урахуванням стану вузлів (атакований чи неатакований) та ступеня їх працездатності. У такому випадку необхідно до стандартної потокової моделі маршрутизації [13] додати ризики уразливості вузлів ТТМ та їх реальний стан, визначений на етапі мультиагентного діагностування.

Постановка задачі. Мережа ТТМ, зображена на рис. 1., задається графом $G=(R,E)$, де $R=\{R_i\}$ – вузли мережі (маршрутизатори), $E=\{E_{i,j}\}$ – канали зв'язку. Кожний канал $E_{i,j}$ володіє пропускною здатністю $\varphi_{i,j}$. Передача інформації від відправника до отримувача описується потоком k_i з інтенсивністю λ^k. Потоки розподіляються через маршрутні змінні $x_{i,j}^k$, які визначають частку потоку *k*, яка передається через канал $E_{i,j}$.

Безпека мережевих елементів описується змінними: w_i – ймовірність успішної атаки вузла R_i, $w_{i,j}$ – ймовірність успішної атаки каналу $E_{i,j}$. Локальні агенти керування трафіком (RA) розташовані на вузлах R_i. Агент перерозподіляє потік між сусідніми вузлами змінюючи маршрутні змінні $x_{i,j}^k$.

Для кожного каналу вводиться метрика ризику

$$\rho_{i,j}=\alpha w_i+\beta w_{i,j}+\gamma w_j, \tag{1}$$

де α,β,γ – вагові коефіцієнти.

Інтенсивність потоку у каналі складає

$$f_{i,j}=\sum_k \lambda^k x_{i,j}^k. \tag{2}$$

Мета балансування навантаження – забезпечити такий розподіл трафіку, за якого: 1) вузли та канали з меншими значеннями w_i, $w_{i,j}$ (більш безпечні) використовуються інтенсивніше; 2) мінімізується сумарний ризик компрометації переданого трафіку; 3) дотримуються обмеження щодо пропускної здатності каналів; 4) зберігається баланс навантаження між вузлами мережі.

Цільова функція мінімізації сумарного очікуваного ризику передавання трафіку:

$$\min_{x_{i,j}^k} J=\sum_{(i,j)\in E}\rho_{i,j}f_{i,j}, \text{ або } \min_{x_{i,j}^k} J=\sum_{(i,j)\in E}\rho_{i,j}\sum_k \lambda^k x_{i,j}^k. \tag{3}$$

Реалізація функції (3) забезпечує те, що більша частина трафіку спрямовується через канали з меншим ризиком.

Обмеженнями для такої задачі є:

1. Закон збереження потоку

$$\sum_{j:(i,j)\in E} x_{i,j}^k-\sum_{j:(j,i)\in E} x_{j,i}^k=b_i^k, \qquad \text{при } b_i^k=\begin{cases}1, & i=s^k;\\ -1, & i=d^k;\\ 0, & \text{інакше.}\end{cases} \tag{4}$$

де відповідно s^k – відправник, а d^k – отримувач.

2. Забезпечення пропускної здатності каналів:

$$\sum_k \lambda^k x_{i,j}^k\le\varphi_{i,j},\ \forall(i,j)\in E. \tag{5}$$

3. Невід'ємність потокових змінних:

$$x_{i,j}^k\ge 0. \tag{6}$$

4. Нормалізація змінних:

$$\sum_{j:(i,j)\in E} x_{i,j}^{k} \le 1 . \tag{7}$$

Наведена модель (1) – (7) є аналогом задачі *багатотоварного оптимального потоку* [14] з вагами, що відображають ризик компрометації мережевих елементів і вирішується шляхом застосування наступного алгоритму.

Алгоритм мультиагентного балансування навантаження базується на ідеї застосування розподіленої МАС, де кожний вузол мережі здатен виконувати локальну оптимізацію. Алгоритм реалізується агентами RA (схема на рис. 1) і включає наступні кроки:

Крок 1. Формування топології мережі $G=(R,E)$; визначення початкових значень маршрутних змінних $x_{i,j}^{k}$; параметрів безпеки w_i, $w_{i,j}$; інтенсивності трафіку λ^k.

Крок 2. Оцінка безпеки сусідніх маршрутів: агент вузла R_i за виразом (1) обчислює інтегральну метрику ризику каналу $\rho_{i,j}$ для всіх сусідів *j*.

Крок 3. Для кожного каналу визначається коефіцієнт привабливості:

$$a_{i,j} = \frac{1}{\rho_{i,j} + \varepsilon}, \tag{8}$$

де $\rho_{i,j}$ визаначається за виразом (1). Чим менший ризик маршруту $\rho_{i,j}$, тим більша його привабливість $a_{i,j}$.

Параметр ε у (8) – мала додатна константа для забезпечення коректності обчислень – ε запобігає діленню на нуль у випадку, якщо для деякого каналу $\rho_{i,j} \to 0$ (канал вважається повністю безпечним).

Крок 4. Нормалізація маршрутних змінних відповідно до коефіцієнтів $a_{i,j}$:

$$x_{i,j}^{k} = \frac{a_{i,j}}{\sum_{l\in N(i)} a_{i,l}}, \tag{9}$$

де $N(i)$ – множина сусідніх вузлів до вузла *i*. У результаті канали з більшими $a_{i,j}$ (безпечні) отримують більшу частку трафіку.

Крок 5. Після обчислення коефіцієнтів $a_{i,j}$ агент вузла R_i за (9) визначає попередній розподіл потоків. На основі цих часток за (2) визначається інтенсивність потоку у кожному каналі та перевіряється обмеження пропускної здатності $f_{i,j} \le \varphi_{i,j}$. Якщо $f_{i,j} > \varphi_{i,j}$, то агент вузла R_i виконує корекцію маршрутних змінних:

$$x_{i,j}^{k} \leftarrow x_{i,j}^{k} \cdot \frac{\varphi_{i,j}}{f_{i,j}} . \tag{10}$$

При цьому надлишковий трафік $\Delta f_{i,j} = f_{i,j} - \varphi_{i,j}$ призначається іншим каналам $E_{i,l} = l \in N(i)$, для яких умова $f_{i,l} \le \varphi_{i,l}$ виконується. Перерозподіл здійснюється пропорційно до коефіцієнтів привабливості $a_{i,l}$

Крок 6. Координація між агентами, яка базується на тому, що агент вузла R_i періодично обмінюється службовою інформацією із сусідніми агентами R_j, $j \in N(i)$ передаючи: поточне навантаження вузла $L_i = \sum_j f_{i,j}$; оцінки ризику каналів $\rho_{i,j}$ (1); доступну пропускну здатність каналів $\hat{\varphi}_{i,j} = \varphi_{i,j} - f_{i,j}$.

На основі такого обміну кожний агент коригує локальні коефіцієнти привабливості за (8), або застосовуючи удосконалений вираз

$$a_{i,j} = \frac{v_{i,j}}{\rho_{i,j} + \eta \dfrac{f_{i,j}}{\varphi_{i,j}} + \varepsilon}, \tag{11}$$

де $v_{i,j}$ – мультиплікативний коефіцієнт безпеки; η – коефіцієнт впливу поточного навантаження каналу.

Отже, привабливість каналу як при високому ризику компрометації, так і при значному завантаженні зменшується. При малих значеннях w_i, $w_{i,j}$ (більш безпечні вузли і канали) будуть отримувати більші значення $a_{i,j}$.

Крок 7. Процес балансування навантаження у МАС реалізується у вигляді ітераційного алгоритму, де на кожній ітерації t кожен агент виконує такі дії:

1) оцінює метрики ризику атаки на канал $\rho_{i,j}(t)$;

2) обчислює коефіцієнти привабливості $a_{i,j}(t) = \dfrac{1}{\rho_{i,j}(t) + \eta \dfrac{f_{i,j}(t)}{\varphi_{i,j}} + \varepsilon}$;

3) оновлює маршрутні змінні $x_{i,j}^k(t+1) = \dfrac{a_{i,j}(t)}{\sum\limits_{l \in N(i)} a_{i,l}(t)}$;

4) обчислює нові значення потоків $f_{i,j}(t+1) = \sum\limits_k \lambda^k x_{i,j}^k(t+1)$;

5) перевіряє обмеження пропускної здатності та коригує потоки.

Алгоритм припиняється при виконанні умови збіжності $\left|x_{i,j}^k(t+1) - x_{i,j}^k(t)\right| < \delta$, де δ – заданий поріг точності. Таким чином, у ТТМ формується розподіл потоків, за якого: канали з меншим ризиком атаки $\rho_{i,j}$ використовуються більш інтенсивно; відсутні перевантаження каналів; навантаження між вузлами мережі є збалансованим.

Параметр управління трафіком. До виразу локального коефіцієнта привабливості маршрутів $a_{i,j}$ (11) входить мультиплікативний коефіцієнт безпеки $v_{i,j}$. Головна ідея його запровадження полягає у створенні для агента можливості регулювати коефіцієнти привабливості маршрутів. У [13] пропонується декілька можливих варіантів такого коефіцієнта. Дослідимо можливість їх використання у МАС, при цьому вхідним параметром, від якого залежить $v_{i,j}$, буде ймовірність компрометації каналу $w_{i,j}$. За аналогією з [13] застосуємо також деякий параметр управління n, який, у загальному випадку, визначатиме політику безпеки мережі.

У першому випадку розглянемо функціональну залежність [13]

$$v_{i,j} = (1 - w_{i,j})^n. \tag{12}$$

Графік залежності (12) наведено на рис. 2.

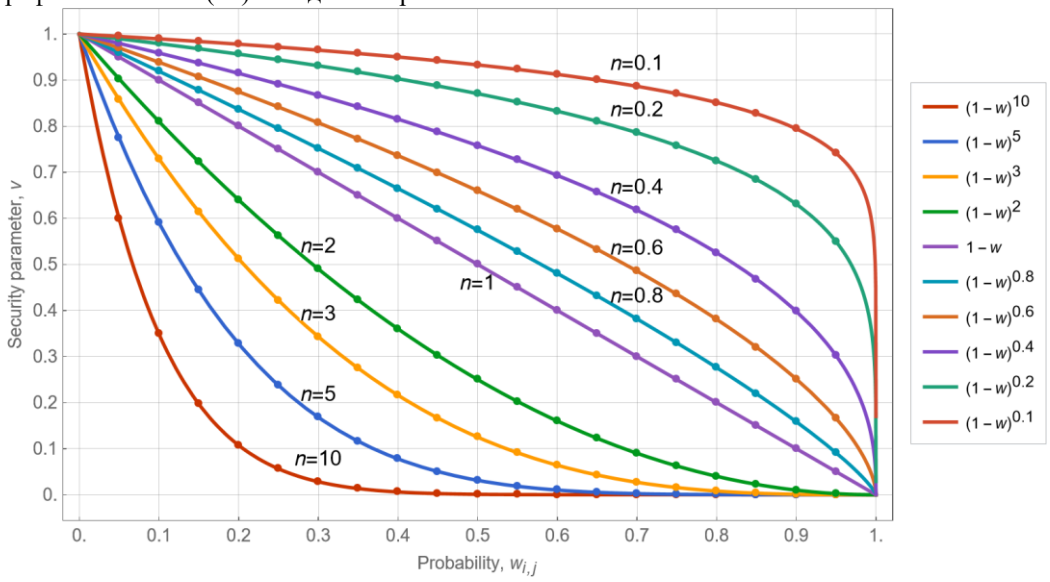


Рис. 2. Залежність коефіцієнта безпеки $v_{i,j}$ від $w_{i,j}$ та n для функції (12)

Як видно з рис. 2, при $n = 1$ система слабо реагує на ризик. При $n = 3...5$ безпечним каналам надається помірна перевага, а при $n > 6$ – система агресивно намагається уникати небезпечних маршрутів. При $0 < n < 1$ система формує політику маршрутизації, толерантну до ризику. Тут безпека враховується, але

над вимогами балансування навантаження і використання пропускної здатності мережі не домінує. Отже, як бачимо, у даному прикладі параметр керування *n* виступає як *регулятор жорсткості* політики безпеки ТТМ.

У більш складному випадку коефіцієнта безпеки у вигляді [13]

$$v_{i,j} = 1 - w_{i,j} + n\,\mathrm{Sin}\left(2\pi w_{i,j} + \theta\right), \tag{13}$$

де $\theta \in \{0, \pi\}$, закон управління буде мати вигляд (рис. 3).

Функція (13) складається з двох частин. Перша частина $1 - w_{i,j}$ є лінійною і визначає базову залежність між ризиком та безпечністю – зі збільшенням $w_{i,j}$ коефіцієнт безпеки монотонно зменшується від 1 до 0. Друга частина $n\,\mathrm{Sin}\left(2\pi w_{i,j} + \theta\right)$ вводить періодичність, яка модулює лінійну характеристику. Наявність в аргументі синуса множника 2π визначає, що на інтервалі $w_{i,j} \in [0,1]$ синусоїда виконує один повний період і тому коефіцієнт безпеки має хвилеподібну форму з максимальним відхиленням від лінійної моделі $\pm n$.

Зміна θ визначає фазове зміщення гармонічної складової, яка дає можливість враховувати також деякі зсуви між зміною $w_{i,j}$ та $v_{i,j}$. Максимум гармонічної складової досягається приблизно при $w_{i,j} \approx 0.25$, а мінімум – при $w_{i,j} \approx 0.75$, що визначає, що канали з помірним ризиком можуть отримувати підвищену привабливість у першій половині діапазону, та зменшену – у другій половині.

Функція (13) у МАС балансування навантаження може інтерпретуватися як *періодично модульована політика маршрутизації*. Її лінійна складова забезпечує тенденцію уникнення ризикованих каналів, а синусоїда створює локальні області підвищеної або зниженої привабливості. Це дозволяє гнучко керувати розподілом трафіку в певних діапазонах ризику або забезпечувати уникнення концентрації потоків лише на невеликій кількості каналів. Параметр θ дозволяє зміщувати ці області вздовж осі $w_{i,j}$, визначаючи, у яких інтервалах ризику МАС буде використовувати відповідні канали більш або менш активно.

Отже, у мультиагентній моделі балансування навантаження агент вузла, на основі знання поточних параметрів мережі та прогнозованої ймовірності компрометації каналів, може адаптивно обирати коефіцієнт безпеки $v_{i,j}$. Якщо значення $w_{i,j}$ змінюються у широкому діапазоні і необхідно жорстко уникати небезпечних маршрутів, доцільно застосовувати степеневі функції, які швидко зменшують $v_{i,j}$ зі зростанням ризику. У випадку необхідності періодичного перерозподілу навантаження між каналами може застосовуватися гармонічна модифікація коефіцієнта безпеки $v_{i,j}$. Таким чином агент обирає функцію $v_{i,j}$ на основі компромісу між мінімальним ризиком компрометації та ефективним використанням мережевих ресурсів.

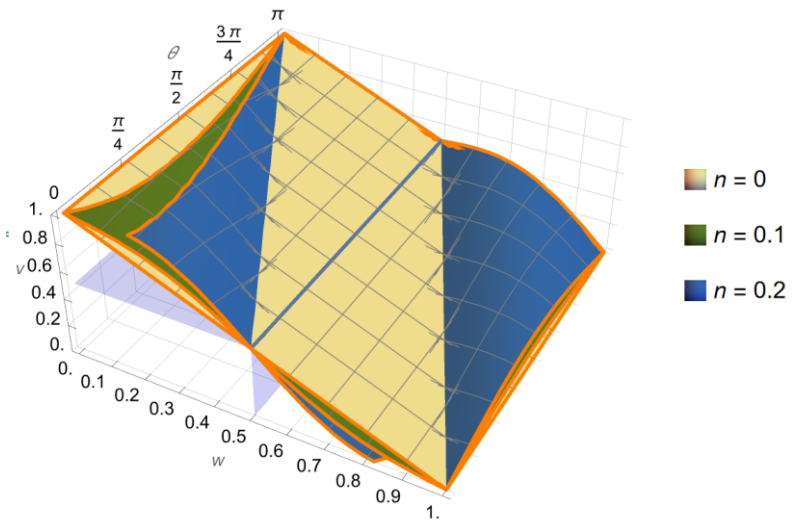


Рис. 3. Залежність коефіцієнта безпеки $v_{i,j}$ від $w_{i,j}$ та n для функції (13)

Метод мультиагентної взаємодії для забезпечення стійкості структури транспортної телекомунікаційної мережі до кібератак

Динамічні кібератаки, які порушують топологічну цілісність ТТМ, можуть призводити до відключення вузлів або блокування каналів зв'язку. Навіть наявність інформації про рівні ризику та поточний

стан елементів мережі не гарантує збереження працездатності ТТМ без своєчасної перебудови її топології. Відсутність механізму підтримання стійкості структури ТТМ може призвести до утворення в результаті атаки ізольованих підмереж, перевантаження окремих вузлів та зниження показників QoS. Крім того, задача ускладнюється також тим, що у розподіленому середовищі MAC підтримання стійкості має здійснюватися децентралізовано, з урахуванням лише локальної інформації. Це обумовлює необхідність розробки нового методу, який, на основі ідентифікації критичних вузлів, дозволить визначати мінімально необхідну кількість резервних зв'язків та забезпечувати відновлення зв'язності мережі з урахуванням заданого рівня безпеки.

Ідея методу. Для уникнення деградації мережі у разі кібератаки агенти (MA, RA) вузлів $R_i, i = 1...N$ періодично оцінюють стан доступних сусідів, каналів зв'язку та визначають необхідні заходи щодо нарощування мережі шляхом організації резервних каналів зв'язку [15]. Під резервними каналами розуміються додаткові або потенційно доступні канали між вузлами, які не використовуються у штатному режимі, але можуть бути оперативно задіяні у разі порушення зв'язності мережі. Такі канали забезпечують структурну надлишковість, яка дозволить відновити цілісність топології мережі при відмовах окремих вузлів. Такі канали не використовуються у штатному режимі роботи і розглядаються як стратегічний ресурс, що активується лише за наявності ознак деградації мережі, забезпечуючи адаптивне відновлення її структури.

Метод реалізується шляхом виконання послідовності етапів.

Eman 1. На основі обміну службовими повідомленнями між суміжними агентами кожен агент формує уявлення про потенційну уразливість топології ТТМ.

Eman 2. Кожен агент ініціює застосування *алгоритму визначення критичних вузлів та мінімальної кількості резервних зв'язків* до поточної структури мережі, що дозволяє ідентифікувати критичні елементи, відмова яких призведе до порушення зв'язності, та визначити необхідні резервні канали.

Eman 3. На основі врахування наявних ресурсів, показників завантаженості та оцінок безпечності каналів агенти виконують ранжування можливих варіантів відновлення.

Eman 4. Агенти узгоджують рішення щодо активації резервних зв'язків для забезпечення відновлення доступності між ключовими вузлами. Також, агенти ініціюють зміну маршрутних змінних $x_{i,j}^k$ (10) та перерозподіляють трафік відповідно до оновленої топології.

Eman 5. Повторна оцінка ризиків, балансування навантаження та моніторинг стабільності відновленої структури. За необхідності – ітеративне повторення процесу, що забезпечує стійкість ТТМ до повторних кібератак.

Алгоритм. В основі запропонованого методу лежать процедури діагностування, оптимізації та структурного відновлення, включені в алгоритм визначення критичних вузлів і мінімально необхідних резервних зв'язків. Логіка роботи алгоритму базується на поетапному моделюванні відмов вузлів і аналізі структурної стійкості мережі.

Так, на етапі ініціалізації формується матриця суміжності A розмірності n, а також вектор працездатності вузлів $OD = (1,1,...,1)$, де значення 1 означає нормальну роботу вузла. Множина атакованих вузлів: $s = \{1,2,...,n\}$. Початково множина критичних вузлів *criticalNodes* є порожньою.

Далі алгоритм здійснює пошук критичних комбінацій вузлів. Для кожної можливої кількості одночасно атакованих вузлів $ix = 1...attackNum$ генеруються всі підмножини $\text{subset}_j \subseteq s$ розміру ix. Кожна така підмножина моделює окремий сценарій атаки. Для вузлів із subset_j у векторі *OD* встановлюється значення 0, що означає виведення їх з ладу в результаті атаки. На основі цього формується діагональна матриця $ODN = \text{diag}(OD)$, яка використовується для модифікації початкової матриці суміжності: $B = ODN \cdot A \cdot ODN$. Це "виключає" атаковані вузли з мережі разом з їх каналами зв'язку.

Перевірка зв'язності здійснюється через транзитивне замикання, для чого визначається матриця досяжності $C = \sum_{k=1}^{n-1} B^k$,та застосовується операція $\text{unitize}(C)$, яка переводить всі ненульові елементи у 1, формуючи бінарну матрицю досяжності. Далі виділяється підматриця $C_1 = C[keep, keep]$, де $keep = \{i \mid OD[i] == 1\}$ – множина працездатних (неатакованих) вузлів.

Якщо в C_1 є хоча б один нульовий елемент $C_1[i,j] == 0$, то це означає, що між деякими неатакованими вузлами відсутній канал і мережа стала незв'язною. У такому випадку підмножина subset_j вважається критичною ($critNode = subset_j$), а всі такі підмножини накопичуються у *criticalNodes* , після чого формується загальна множина *allCriticalCombinations* шляхом виключення порожніх підмножин.

Під час наступного етапу для кожної критичної комбінації $X \in allCriticalCombinations$ аналізується структура мережі після атаки та формується модифікована матриця B, у якій рядки та стовпці, що відповідають вузлам із X, прирівнюються до 0. Далі, застосовуючи процедуру BFS (обхід в ширину), визначаються компоненти зв'язності, які реєструються у векторі *visited* для уникнення повторного обходу, та накопичуються у множині *components*. Ізольовані вершини $isolated = \{i \mid \text{degree}(i) = 0 \;\&\&\; i \notin X\}$ обробляються окремо. В результаті утворюється повний набір компонент мережі після атаки.

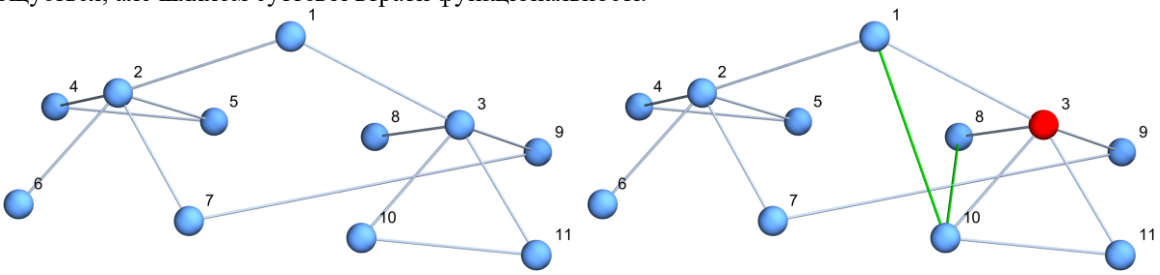
На кінцевому етапі визначається мінімальна кількість необхідних резервних зв'язків. При кількості компонент $k = \text{NumberOf}(components)$ для відновлення зв'язності необхідно $\text{minEdges} = k - 1$ додаткових зв'язків.

Для виведення результатів формується множина додаткових каналів extraEdges шляхом послідовного з'єднання окремих компонент. Тобто, у кожній парі сусідніх компонент між їх першими вершинами $(\text{first}(components[i]), \text{first}(components[i+1]))$ додається ребро, що забезпечує мінімальну кількість з'єднань всієї мережі.

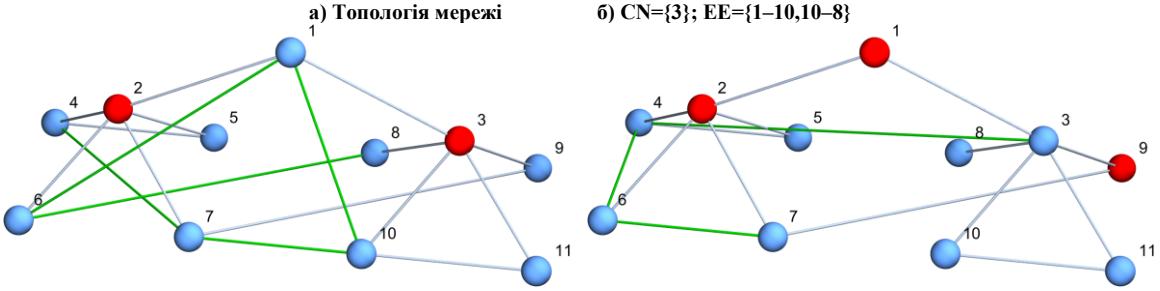
Таким чином, алгоритм передбачає перебір сценаріїв атак та виявлення критичних вузлів, на основі чого, через додавання резервних каналів зв'язку, будується мінімальний план відновлення зв'язності. Математичною основою алгоритму є поєднання матричного аналізу досяжності [16] та графових методів пошуку (BFS) [17], що дозволяє забезпечити структурну стійкість ТТМ у мультиагентному середовищі.

Приклад. Для перевірки працездатності методу розглянемо раніше наведений приклад (рис. 1). Така топологія може бути подана у вигляді тривимірної моделі (рис. 4а) з виділенням ключового маршрутизатора (вузол 1), регіональних маршрутизаторів (вузли 2 та 3), та маршрутизаторів решти вузлів (вузли 4–11). Застосовуючи наведений алгоритм будемо визначати критичні комбінації вузлів та необхідні резервні канали зв'язку для $n = 1...N-2$ атакованих вузлів. У даному випадку значення $N-2$ є мінімальною топологією ТТМ, за якої ще можлива передача інформації.

Роботу алгоритму наведено на рис. 4б – 4г., де позначено атаковані вузли (червоні кулі) та необхідні резервні канали зв'язку (зелені лінії). Як бачимо, відмова навіть одного вузла може призводити до розпаду мережі на декілька відокремлених компонент, що свідчить про наявність структурно вразливих елементів у ТТМ. Аналіз середніх значень кількості відокремлених компонент $N_{\text{від}}$ та необхідних резервних каналів $N_{\text{дод}}$ (рис. 5) свідчить про виражену нелінійну залежність від кількості атакованих вузлів (маршрутизаторів). При $n = 4...5$ спостерігається максимум значень ($N_{\text{від}} \approx 4.1-4.5$, $N_{\text{дод}} \approx 3.1-3.5$), де зв'язність мережі порушується найсуттєвіше. Це підтверджує існування критичного порогу руйнування мережі, де її структура спрощується, але шляхом суттєвої втрати функціональності.



а) Топологія мережі **б) CN={3}; EE={1–10,10–8}**



в) CN={2,3}; EE={4–7,7–10,10–1,1–6,6–8} **г) CN={1,2,9}; EE={3–4,4–6,6–7}**

Рис. 4. Визначення критичних вузлів (CN) та резервних каналів (EE)

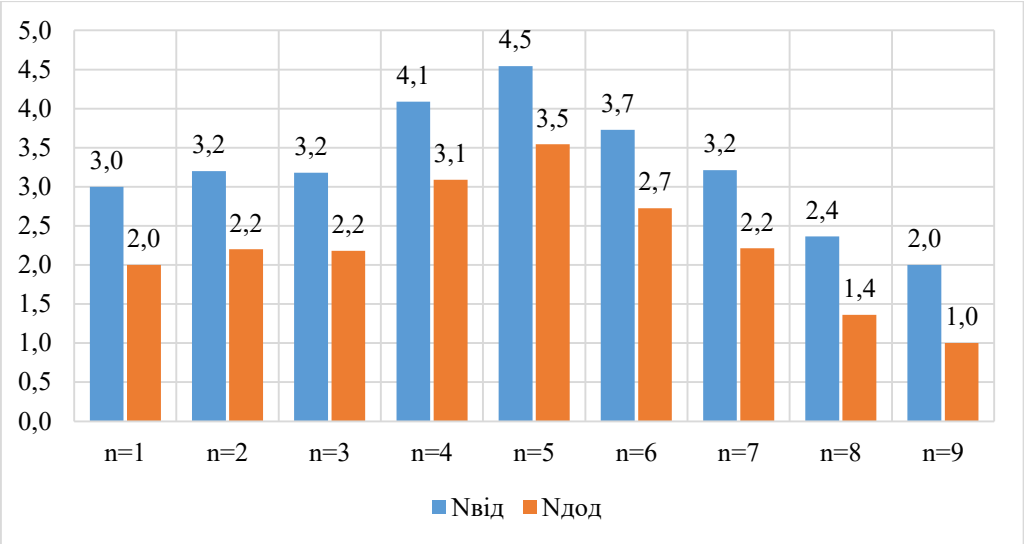


Рис. 5. Середня кількість відокремлених компонент (Nвід) та необхідних додаткових зв'язків (Nдод) для кількості атакованих вузлів (n)

В цілому, наведені результати підтверджують доцільність використання запропонованого алгоритму для виявлення критично важливих вузлів, а також для синтезу мінімально необхідної структури резервних зв'язків для забезпечення стійкості мережі до кібератак.

ВИСНОВКИ З ДАНОГО ДОСЛІДЖЕННЯ І ПЕРСПЕКТИВИ ПОДАЛЬШОГО РОЗВИТКУ У ДАНОМУ НАПРЯМІ

1. Сучасні транспортні телекомунікаційні мережі є важливим елементом критичної інфраструктури держави. Для забезпечення захищеності таких мереж від кібератак найбільш доцільною вбачається система управління їх кібербезпекою на базі мультиагентного підходу, який поєднує розподілене виявлення кібератак на компоненти мережі з автономним реагуванням на їх наслідки шляхом балансування навантаження та забезпечення структурної зв'язності мережі.
2. Існуючі моделі балансування навантаження у мережі орієнтуються переважно на статичні або централізовано визначені метрики каналів, що створює єдину точку відмови та призводить до суттєвих затримок у роботі мереж. Запропонована удосконалена модель мультиагентного балансування навантаження ТТМ в умовах впливу кібератак, на відміну від існуючих моделей, враховує динамічні зміни ступеня уразливості вузлів та реалізує адаптивний розподіл трафіку шляхом вирішення задачі оптимізації з обмеженнями на пропускну здатність каналів і допустимий рівень довіри до вузлів. Це дозволяє перенаправляти потоки даних на більш захищені маршрути при виявленні атак на окремі елементи мережі, забезпечуючи збереження цільових показників якості обслуговування в умовах деструктивного впливу кібератак.
3. У випадку масованих атак навіть наявність інформації про рівні ризику та поточний стан елементів мережі не гарантує збереження працездатності ТТМ без своєчасної перебудови її топології. В рамках запропонованої концепції побудови мультиагентної системи управління кібербезпекою ТТМ для побудови повністю функціональної системи є необхідність розробки методу мультиагентної взаємодії при забезпеченні стійкості структури ТТМ до кібератак.
4. Розроблений метод мультиагентної взаємодії для забезпечення стійкості структури ТТМ до кібератак базується на оптимізації та структурного відновлення мережі шляхом застосування алгоритму визначення критичних вузлів і мінімально необхідної кількості резервних зв'язків. З метою забезпечення стійкості структури мережі в умовах динамічного впливу кібератак такий підхід забезпечує децентралізоване формування раціональної конфігурації додаткових зв'язків для збереження або відновлення зв'язності мережі з мінімальними витратами ресурсів.
5. Перспективами подальшого розвитку у даному напрямі є широке коло питань щодо розробки інтелектуальних методів кооперативної взаємодії агентів, прогнозування кібератак, адаптивного перерозподілу мережевих ресурсів та інтеграції технологій машинного навчання для підвищення ефективності балансування навантаження і забезпечення структурної стійкості транспортних телекомунікаційних мереж в умовах динамічних кіберзагроз.

Література

1. Голь В. Д., Ірха М. С. Телекомунікаційні та інформаційні мережі. Київ, ІСЗЗІ КПІ ім. Ігоря Сікорського, 2021. 250 с. https://ela.kpi.ua/server/api/core/bitstreams/35d4a2d2-53ed-453f-9bcd-fa883a982f53/content

2. Пановик У. П. Кібербезпека в Телекомунікаційних Мережах та Системах. Наукові Записки, 2024, № 1(68). – С. 122–135. https://nz.uad.lviv.ua/media/1-68/13.pdf

3. Хворостяний Р. В. Мультиагентна модель управління кібербезпекою транспортної телекомунікаційної мережі. Сучасний захист інформації, 2026, № 1(65). – С. 119–131. https://doi.org/10.31673/2409-7292.2026.011588

4. Хворостяний Р. В., Туровський О. Л. Метод взаємодії агентів в мультиагентній системі управління кібербезпекою транспортної телекомунікаційної мережі під час діагностування. Телекомунікаційні та інформаційні технології, 2026, № 1(90). – С. 38–49. https://doi.org/10.31673/2412-4338.2026.019005

5. Bougueroua N., Mazouzi S., Belaoued M., Seddari N., Derhab A., Bouras A. A Survey on Multi-Agent Based Collaborative Intrusion Detection Systems. Journal of Artificial Intelligence and Soft Computing Research, 2021, №11(2). – P. 111–142. https://doi.org/10.2478/jaiscr-2021-0008

6. Torres M. Enhancing Distributed Intrusion Detection Systems Using Multi-Agent AI Models. International Annals of Intelligent Learning Systems Research (IAILSR), 2025, №9. – P. 22–35. https://iailsr.org/index.php/iailsr/article/view/13

7. Sen J. A Distributed Intrusion Detection System Using Cooperating Agents. arXiv:1111.0382, (2011). https://doi.org/10.48550/arXiv.1111.0382

8. Aydın H., Aydın G. Z. G., Sertbaş A., Aydın M. A. Internet of things security: A multi-agent-based defense system design. Computers and Electrical Engineering, 2023, №111(B). – P.n. 108961, https://doi.org/10.1016/j.compeleceng.2023.108961

9. Landolt C. R., Würsch C., Meier R., Mermoud A., Jang-Jaccard J. Multi-Agent Reinforcement Learning in Cybersecurity: From Fundamentals to Applications. arXiv:2505.19837, (2025). https://doi.org/10.48550/arXiv.2505.19837

10. Козловський О. В., Жарікова М. В. Розробка моделі безпеки для багатоагентної мережі в кіберфізичній системі. Вісник Херсонського національного технічного університету, 2025, Т. 2, №1(92). – С. 76–83. https://doi.org/10.35546/kntu2078-4481.2025.1.2.11

11. Shamshirband S., Anuar N. B., Kiah M. L. M., Patel A. An appraisal and design of a multi-agent system based cooperative wireless intrusion detection computational intelligence technique. Engineering Applications of Artificial Intelligence, 2013, 26(9). – P. 2105–2127. https://doi.org/10.1016/j.engappai.2013.04.010

12. Лемешко О. В., Єременко О. С., Невзорова О. С. Потокові моделі та методи маршрутизації в інфокомунікаційних мережах: відмовостійкість, безпека, масштабованість. – Харків: ХНУРЕ, 2020. – 308 с. https://doi.org/10.30837/978-966-659-282-1

13. Лемешко О. В., Єременко О. С., Євдокименко М. О., Шаповалова А. С., Слейман Б. Моделювання та оптимізація процесів безпечної та відмовостійкої маршрутизації в телекомунікаційних мережах: Монографія. – Харків: ХНУРЕ, 2022. – 198 с. https://doi.org/10.30837/978-966-659-378-1

14. Salimifard K., Bigharaz S. The multicommodity network flow problem: State of the art classification, applications, and solution methods. Operational Research, 2022, №22. – P. 1–47. https://doi.org/10.1007/s12351-020-00564-8

15. Стрелковська І. В., Соловська І. М. Маршрутизація в мережі MPLS-TE з додатковими напрямами передавання трафіку. Зв'язок, 2016, №1. – С. 15–20. https://con.dut.edu.ua/index.php/communication/article/view/1263/1198

16. Невзоров А., Скляренко О., Колодінська Я., Ніколаєвський О. Моделі оцінки структурної живучості та надійності комп'ютерних мереж. Measuring and Computing Devices in Technological Processes, 2023, №3. – P. 164–169. https://doi.org/10.31891/2219-9365-2023-75-19

17. Chor B., Rubinstein A. Shortest paths and breadth first search. In Computational thinking for life scientists. – Cambridge University Press, 2022. – P. 113–122. https://doi.org/10.1017/9781108178327.010

References

1. Gol V. D., Irkha M. S. Telecommunications and Information Networks. Kyiv, Igor Sikorsky Kyiv Polytechnic Institute, 2021. 250 p. https://ela.kpi.ua/server/api/core/bitstreams/35d4a2d2-53ed-453f-9bcd-fa883a982f53/content

2. Panovyk U. P. Cybersecurity in Telecommunication Networks and Systems. Naukovi Zapisky, 2024, No. 1(68). – P. 122–135. https://nz.uad.lviv.ua/media/1-68/13.pdf

3. Khvorostyanyi R. V. Multiagent model of cybersecurity management of a transport telecommunication network. Modern Information Protection, 2026, No. 1(65). – P. 119–131. https://doi.org/10.31673/2409-7292.2026.011588

4. Khvorostyanyi R. V., Turovsky O. L. Method of interaction of agents in a multi-agent system of management of cybersecurity of a transport telecommunication network during diagnostics. Telecommunications and Information Technologies, 2026, No. 1(90). – P. 38–49. https://doi.org/10.31673/2412-4338.2026.019005

5. Bougueroua N., Mazouzi S., Belaoued M., Seddari N., Derhab A., Bouras A. A Survey on Multi-Agent Based Collaborative Intrusion Detection Systems. Journal of Artificial Intelligence and Soft Computing Research, 2021, №11(2). – P. 111–142. https://doi.org/10.2478/jaiscr-2021-0008

6. Torres M. Enhancing Distributed Intrusion Detection Systems Using Multi-Agent AI Models. International Annals of Intelligent Learning Systems Research (IAILSR), 2025, №9. – P. 22–35. https://iailsr.org/index.php/iailsr/article/view/13

7. Sen J. A Distributed Intrusion Detection System Using Cooperating Agents. arXiv:1111.0382, (2011). https://doi.org/10.48550/arXiv.1111.0382

8. Aydın H., Aydın G. Z. G., Sertbaş A., Aydın M. A. Internet of things security: A multi-agent-based defense system design. Computers and Electrical Engineering, 2023, №111(B). – P.n. 108961, https://doi.org/10.1016/j.compeleceng.2023.108961

9. Landolt C. R., Würsch C., Meier R., Mermoud A., Jang-Jaccard J. Multi-Agent Reinforcement Learning in Cybersecurity: From Fundamentals to Applications. arXiv:2505.19837, (2025). https://doi.org/10.48550/arXiv.2505.19837

10. Kozlovskyi O. V., Zharikova M. V. Development of a security model for a multi-agent network in a cyber-physical system. Bulletin of the Kherson National Technical University, 2025, Vol. 2, No. 1(92). – P. 76–83. https://doi.org/10.35546/kntu2078-4481.2025.1.2.11

11. Shamshirband S., Anuar N. B., Kiah M. L. M., Patel A. An appraisal and design of a multi-agent system based cooperative wireless intrusion detection computational intelligence technique. Engineering Applications of Artificial Intelligence, 2013, 26(9). – P. 2105–2127. https://doi.org/10.1016/j.engappai.2013.04.010

12. Lemeshko O. V., Eremenko O. S., Nevzorova O. S. Flow models and routing methods in infocommunication networks: fault tolerance, security, scalability. – Kharkiv: KhNURE, 2020. – 308 p. https://doi.org/10.30837/978-966-659-282-1

13. Lemeshko O. V., Eremenko O. S., Yevdokymenko M. O., Shapovalova A. S., Sleiman B. Modeling and optimization of secure and fault-tolerant routing processes in telecommunication networks: Monograph. – Kharkiv: KhNURE, 2022. – 198 p. https://doi.org/10.30837/978-966-659-378-1

14. Salimifard K., Bigharaz S. The multicommodity network flow problem: State of the art classification, applications, and solution methods. Operational Research, 2022, №22. – P. 1–47. https://doi.org/10.1007/s12351-020-00564-8

15. Strelkovska I. V., Solovska I. M. Routing in the MPLS-TE network with additional traffic transmission directions. Svyazok, 2016, No. 1. – P. 15–20. https://con.dut.edu.ua/index.php/communication/article/view/1263/1198

16. Nevzorov A., Sklyarenko O., Kolodinska Ya., Nikolaevsky O. Models for assessing the structural survivability and reliability of computer networks. Measuring and Computing Devices in Technological Processes, 2023, No. 3. – P. 164–169. https://doi.org/10.31891/2219-9365-2023-75-19

17. Chor B., Rubinstein A. Shortest paths and breadth first search. In Computational thinking for life scientists. – Cambridge University Press, 2022. – P. 113–122. https://doi.org/10.1017/9781108178327.010