УДК 004.056:004.89:621.39
DOI: 10.31673/2409-7292.2026.011588

Хворостяний Р. В.

МУЛЬТИАГЕНТНА МОДЕЛЬ УПРАВЛІННЯ КІБЕРБЕЗПЕКОЮ ТРАНСПОРТНОЇ ТЕЛЕКОМУНІКАЦІЙНОЇ МЕРЕЖІ

У статті розглянуто проблему побудови ефективної системи управління кібербезпекою транспортної телекомунікаційної мережі (ТТМ) в умовах зростання масштабованості, динамічності та часткової спостережуваності мережевих процесів. Обґрунтовано доцільність застосування ієрархічного мультиагентного підходу як методологічної основи формування адаптивної та відмовостійкої системи управління. Запропоновано формалізований опис ієрархічної мультиагентної моделі, у межах якої функції моніторингу, виявлення загроз, оцінювання ризиків і реагування розподілено між агентами різних рівнів відповідно до їх цілей, часових масштабів та ресурсних обмежень. Модель реалізує принципи ієрархічної декомпозиції, поєднання локальної автономії з глобальною координацією та поетапного залучення механізмів захисту залежно від складності кіберзагроз. Розроблено систему показників ефективності функціонування та визначено узагальнені вагові коефіцієнти для формування інтегрального критерію оцінювання альтернативних архітектур управління кібербезпекою ТТМ. Проведений порівняльний аналіз централізованих, децентралізованих і ієрархічних централізованих систем засвідчив переваги ієрархічної мультиагентної моделі за показниками адаптивності, стійкості, часу реакції та узгодженості управлінських рішень. Отримані результати підтверджують перспективність використання запропонованого підходу для створення масштабованих і інтелектуалізованих систем управління кібербезпекою транспортних телекомунікаційних мереж.

Ключові слова: ієрархічна мультиагентна система, кібербезпека, управління кібербезпекою, транспортна телекомунікаційна мережа, розподілене управління.

Вступ

Транспортні телекомунікаційні мережі (ТТМ) є базовою інфраструктурною складовою інформаційно-комунікаційних систем і забезпечують міжзонну передачу великих обсягів даних між мережами доступу, корпоративними сегментами, центрами обробки даних та сервісними платформами [1]. На відміну від мереж доступу, вони виконують функції агрегації, маршрутизації та узгодженого розподілу потоків, підтримуючи цілісність і стабільність функціонування всієї інфраструктури. З позицій теорії багаторівневих систем ТТМ доцільно розглядати як ієрархічно організований об’єкт управління з власними цілями, критеріями ефективності та обмеженнями, що обумовлює необхідність застосування спеціалізованих ієрархічних моделей управління, зокрема у сфері кібербезпеки [2].

Постановка проблеми дослідження

У процесі функціонування ТТМ на її елементи здійснюються кібератаки різного типу та інтенсивності, що призводить до порушення доступності, цілісності або конфіденційності інформаційних ресурсів. Ефективне управління кібербезпекою в таких умовах потребує своєчасного виявлення аномальних станів, оцінювання ризиків та формування узгоджених керуючих дій з урахуванням поточного стану всієї мережі [3]. Централізовані підходи до управління кібербезпекою в ТТМ мають обмеження, пов’язані з високим обсягом телеметричних даних, затримками передавання інформації та зниженням надійності при відмові центрального вузла. Натомість мультиагентний підхід передбачає розподіл функцій моніторингу, аналізу та реагування між автономними агентами, що взаємодіють у межах ієрархічної структури [4]. *Проблема* полягає у формалізації такої ієрархічної мультиагентної системи: визначенні її рівнів, складу агентів, множин станів та керуючих впливів, а також описі інформаційних і функціональних зв’язків між ними. Розв’язання цієї проблеми сворює підґрунтя для подальшого моделювання процесів діагностування, оцінювання достовірності та часу реагування в умовах дестабілізуючих впливів.

Аналіз публікацій

Мультиагентні технології є окремим напрямом досліджень в системах управління складними об’єктами. В аспекті управління ТТМ такі системи досліджуються у [5], де було розроблено модель функціонування та управління транспортною мережею зв’язку, як

© Хворостяний Р.В. Мультиагентна модель управління кібербезпекою транспортної телекомунікаційної мережі. Сучасний захист інформації, 1(65), 119–131.
https://doi.org/10.31673/2409-7292.2026.011588

складову мультиагентної системи управління. Це дозволило враховувати стани елементів транспортної мережі (справний чи несправний) через стани відповідних агентів з урахуванням надійності та готовності до функціонування кожного агента.

У дослідженні [6] розглядається застосування мультиагентних моделей для управління телекомунікаційними мережами 5-го покоління (5G), де підкреслюється, що традиційні централізовані підходи виявляються неефективними через високу динамічність і різнорідність мереж, а мультиагентні системи забезпечують адаптивність і гнучкість управління в таких умовах. У контексті моніторингу складних мережних інфраструктур агентний підхід також використовується для розподіленого виявлення аномалій та забезпечення функціональної безпеки [7], де локальні інтелектуальні агенти спільно працюють над виявленням порушень, що дозволяє зменшити обсяг телеметрії та скоротити час реакції порівняно з централізованими методами.

З інших джерел, наприклад [8], також видно, що мультиагентні архітектури розглядаються як засіб для масштабованого управління різнорідними елементами систем, де кожен агент забезпечує контекстно залежну інформацію для прийняття рішень, а ієрархічна структура дозволяє інтегрувати локальні дані в глобальний контекст, підтримуючи прийняття рішень на різних рівнях системи. Більш спеціалізовані роботи з ієрархічного мультиагентного навчання у сфері кібербезпеки, такі як [9], демонструють, що розподіл завдань між агентами за рівнями (наприклад, дослідження підзадач і їх узгодження на вищому рівні) дозволяє моделювати складні політики захисту і досягати більш високої ефективності захисту мереж від складних загроз. Крім того, концептуальні огляди, зокрема [10] показують, що мультиагентні системи здатні забезпечувати адаптивність, відмовостійкість та масштабованість завдяки розподіленій обробці даних, відсутності єдиної точки відмови і здатності до колективного навчання – властивості, які є критичними для кібербезпеки великих мережних інфраструктур.

В цілому, наведений огляд джерел підкреслює, що сучасні транспортні телекомунікаційні мережі в аспекті їх захисту вимагають управлінських моделей, які поєднують локальну автономію агентів з глобальною координацією, а це, зокрема, реалізується саме через ієрархічні мультиагентні підходи, що робить їх доцільними для розробки моделей управління кібербезпекою ТТМ.

Метою даної статті є розробка формалізованого опису ієрархічної мультиагентної системи управління кібербезпекою транспортної телекомунікаційної мережі, яка забезпечує масштабованість, адаптивність та узгодженість прийняття рішень у розподіленому середовищі.

Кібербезпека ТТМ, як об’єкт управління

На рис. 1 наведено загальну ієрархічну організацію ТТМ, як об’єкта управління.

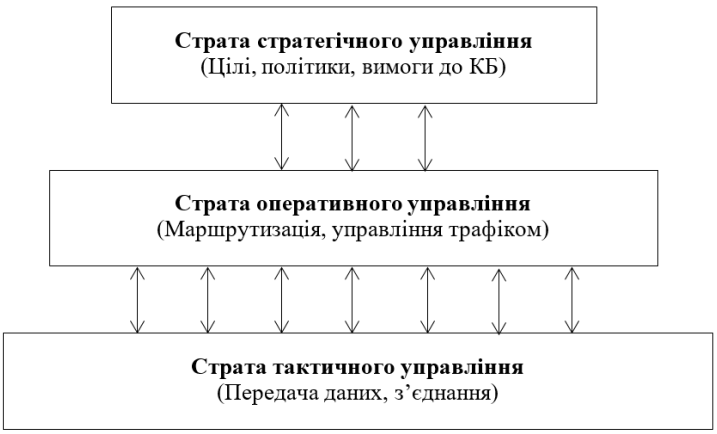

Рис. 1. Ієрархічне подання ТТМ як об’єкта управління

© Хворостяний Р.В. Мультиагентна модель управління кібербезпекою транспортної телекомунікаційної мережі. Сучасний захист інформації, 1(65), 119–131.
https://doi.org/10.31673/2409-7292.2026.011588

У запропонованій системі функції розподілено між стратами управління відповідно до рівня прийняття рішень, їх цілей, часових масштабів та обмежень: нижні рівні забезпечують безперервність і якість передавання даних та оперативне реагування на прості загрози, тоді як вищі – координують ресурси, оптимізують функціонування та реалізують політики безпеки. Така ієрархія передбачає поетапне залучення складніших і ресурсомістких механізмів захисту лише за потреби, що підвищує ефективність і швидкодію системи порівняно з використанням виключно засобів найвищого рівня.

Розроблена ієрархічна мультиагентна модель (рис. 2) відображає багаторівневу структуру ТТМ, розміщення функціональних агентів на кожному рівні та їх логічні зв'язки, реалізуючи принципи декомпозиції, розподілу функцій і поєднання локальної автономії з глобальною координацією в процесах виявлення загроз, оцінювання ризиків і реагування.

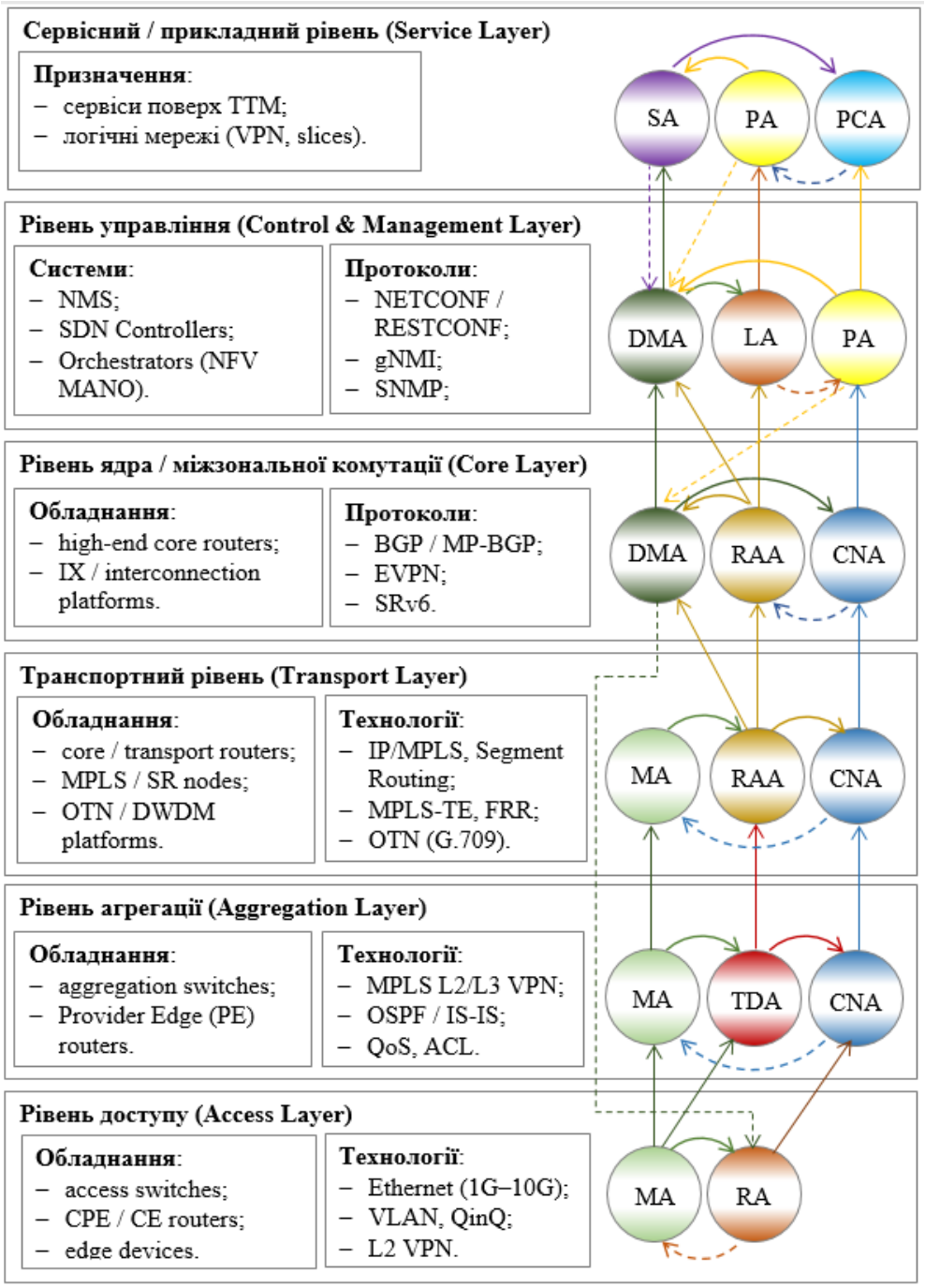

Рис. 2. Рівні ТТМ та відповідні їм агенти

© Хворостяний Р.В. Мультиагентна модель управління кібербезпекою транспортної телекомунікаційної мережі. Сучасний захист інформації, 1(65), 119–131.
https://doi.org/10.31673/2409-7292.2026.011588

Базові типи агентів системи управління кібербезпекою ТТМ

1. Monitoring Agent (MA) – агент моніторингу, призначений для збору та первинної обробки інформації про стан елементів ТТМ. Агент розташовується безпосередньо біля мережевого обладнання, передає дані агентам реагування RA, виявлення загроз TDA та оцінки ризиків RAA, отримує параметри збору від RA та агента координації/переговорів CNA. Формальна модель такого агента:

$$MA = \langle X, O, M, S, C, J_{MA} \rangle, \tag{1}$$

де $X(t) = \left[x_1(t), x_2(t), ..., x_n(t) \right]^T$ – вектор стану мережі (конфігурація обладнання, затримки передавання, втрати пакетів, завантаженість каналів); $O(t) = \left[o_1(t), o_2(t), ..., o_m(t) \right]^T$ – вектор спостережень (SNMP-лічильники, NetFlow або IPFIX записи, SDN-телеметрія); $M : X \times \eta \to O$ – оператор моніторингу – перетворення реального стану мережі у доступні для агента спостереження (η – похибки та шуми); $S = \{ s_1, s_2, ..., s_k \}$ – стратегії спостереження (частота опитування, метрики, пріоритети джерел, глибина деталізації); $C = \{ c_1, c_2, ..., c_k \}$ – обмеження моніторингу (пропускна здатність, обчислювальні ресурси, допустиме навантаження); $J_{RA} = E\left[\sum_{t=0}^{T} \left(\alpha I(t) - \beta L(t) - \gamma C(t) \right) \right]$ – функція якості моніторингу ($I(t)$ – інформативність спостережень, $L(t)$ – затримка отримання даних, $C(t)$ – вартість моніторингу, α, β, γ – вагові коефіцієнти).

2. Threat Detection Agent (TDA) – агент виявлення загроз, призначений для виявлення ознак кібератак на основі аналізу статистичних аномалій, сигнатур або поведінки мережі. Він отримує $O_i(t)$ від агента моніторингу (MA) і може передавати події до RAA та CNA. Результати роботи TDA використовуються агентами оцінювання ризиків (RAA) і прийняття рішень. Формально може бути поданий у вигляді:

$$TDA = \langle O, Z, H, D, C, J_{TDA} \rangle, \tag{2}$$

де $O(t) = \left[o_1(t), o_2(t), ..., o_m(t) \right]^T$ – вектор спостережень (показники телеметрії, потоки NetFlow та IPFIX, журнали подій); $Z(t) = \left[z_1(t), z_2(t), ..., z_m(t) \right]^T$ – вектор ознак (статистичні параметри, кореляційні показники, шаблони поведінки); $H = \{ H_0, H_1, ..., H_r \}$ – множина гіпотез загроз (H_0 – гіпотеза штатного режиму, H_i – гіпотеза наявності загрози чи атаки типу *i*; $D : Z \to H \times [0,1]$ – оператор детекції; $C = \{ c_1, c_2, ..., c_q \}$ – множина обмежень (ресурси, хибні спрацювання, політики конфіденційності); $J_{TDA} = E\left[\sum_{t=0}^{T} \left(\alpha P_{\text{det}}(t) - \beta P_{\text{fp}}(t) - \gamma \tau(t) \right) \right]$ – якість виявлення ($P_{\text{det}}(t)$ – коректне виявлення, $P_{\text{fp}}(t)$ – хибне спрацювання, $\tau(t)$ – затримка, α, β, γ – вагові коефіцієнти).

3. Risk Assessment Agent (RAA) – агент оцінки ризику, призначений для кількісної оцінки ймовірності та наслідків атак, формування метрик ризику. Він отримує дані від агента виявлення загроз (TDA) та передає оцінки агенту прийняття рішень (DMA). Формально може бути описаний кортежем:

$$RAA = \langle H, A, R, E_R, C, J_{RAA} \rangle, \tag{3}$$

де $H = \{ H_0, H_1, ..., H_r \}$ – множина гіпотез загроз, де H_i – гіпотеза щодо наявності загрози з апостеріорною імовірністю $P(H_i)$; $A = \{ A_1, A_2, ..., A_n \}$ – множина активів (канали, вузли,

© Хворостяний Р.В. Мультиагентна модель управління кібербезпекою транспортної телекомунікаційної мережі. Сучасний захист інформації, 1(65), 119–131.
https://doi.org/10.31673/2409-7292.2026.011588

керуючі площини, ресурси управління); $R(t)=\left[R_1(t),R_2(t),...,R_n(t)\right]^T$ – вектор ризиків, де $R_j(t)$ – оцінка ризику для активу A_j у момент t; $E_R: H\times A\to R$ – оператор оцінювання ризику; $C=\{c_1,c_2,...,c_q\}$ – множина обмежень (періодичність оновлення, рівень невизначеності, регуляторні вимоги); $J_{RAA}=E\left[\sum_{t=0}^{T}\left(\alpha\Delta R(t)-\beta U(t)-\gamma\tau(t)\right)\right]$ – якість оцінювання ризику ($\Delta R(t)$ – зниження ризику внаслідок управлінських рішень, $U(t)$ – рівень невизначеності оцінки, $\tau(t)$ – затримка актуалізації ризиків).

4. Decision-Making Agent (DMA) – агент прийняття рішень, який здійснює прийняття рішень щодо реагування на загрози шляхом вибору оптимальної стратегії реагування. Агент є ключовою ланкою між аналітичними агентами (TDA, RAA) та виконавчими агентами (RA). Під час роботи він отримує R_j від агента оцінки ризику (RAA), координується агентом політик (PA) та керує агентом реагування (RA). Формально може бути поданий як:

$$DMA=\langle A,X,D,M,R,C,J_{DMA}\rangle, \tag{4}$$

де $A=\{a_1,a_2,...,a_n\}$ – множина керуючих дій (механізми реагування, передача події на вищий рівень управління, передача команди агенту реагування (RA), зміна політик безпеки (через CNA), запит додаткових даних); $X=\left[x_1,x_2,...,x_m\right]^T$ – вектор вхідних станів (загрози від TDA, ризики від RAA, параметри мережі (навантаження), стан ресурсів, обмеження SLA та політик безпеки); $D=\{d_1,d_2,...,d_k\}$ – множина можливих рішень (блокування, обмеження доступу, спостереження без втручання, комбіновані сценарії); $M: X\to D$ – модель прийняття рішень; $R=\{r_1,r_2,...,r_l\}$ – множина обмежень: політики безпеки, часові затримки, обмеження ресурсів, вимоги до сервісів, регуляторні вимоги; $C=\{c_1,c_2,...,c_p\}$ – контекст рішень (рівень ієрархії, стан TTM, фаза атаки, історія інцидентів, цілі системи управління кібербезпекою); $J_{DMA}=\min\limits_{d\in D}F\left(Risk,Damage,Cost,Delay\right)$ – цільова функція агента, спрямована на мінімізацію кіберризику та зниження потенційних збитків.

5. Response Agent (RA) – агент реагування, призначений для реалізації технічних заходів реагування (фільтрація трафіку, зміна маршрутів, ізоляція сегментів, застосування політик безпеки). Агент виступає виконавчим компонентом мультиагентної системи, забезпечуючи трансляцію абстрактних рішень управління у конкретні технічні дії. Узагальнено RA можна подати кортежем:

$$RA=\langle A,X,T,P,C,J_{RA}\rangle, \tag{5}$$

де $A=\{a_1,a_2,...,a_m\}$ – множина керуючих дій RA; $X(t)=\left[x_1(t),x_2(t),...,x_n(t)\right]^T$ – динаміка стану мережі; $T: X\times A\times W\to X$ – оператор переходу станів (W – вектор зовнішніх та внутрішніх збурень; $P=\{p_1,p_2,...,p_l\}$ – множина політик безпеки; $C=\{c_1,c_2,...,c_k\}$ – множина обмежень технічного характеру; $J_{RA}=E\left[\sum_{t=0}^{T}\left(\alpha D(t)+\beta Q(t)+\gamma C(t)\right)\right]$ – функція якості (втрат) реагування ($D(t)$ – рівень загрози після реагування, $Q(t)$ – деградація якості сервісу, $C(t)$ – вартість заходів, α,β,γ – вагові коефіцієнти).

© Хворостяний Р.В. Мультиагентна модель управління кібербезпекою транспортної телекомунікаційної мережі. Сучасний захист інформації, 1(65), 119–131.
https://doi.org/10.31673/2409-7292.2026.011588

6. Coordination–Negotiation Agent (CNA) – агент координації та переговорів, який забезпечує узгодження локальних рішень при глобально оптимальній стратегії управління кібербезпекою ТТМ. Дозволяє реалізувати локальну автономію агентів при збереженні глобальної керованості. Структура такого агента може бути наведена у вигляді:

$$CNA = \langle A, X, G, S, P, C, J_{CNA} \rangle, \quad (6)$$

де $A = \{a_1, a_2, ..., a_n\}$ – множина координаційних/переговорних дій (пріоритети реагування, розподіл ресурсів між RA та DMA, синхронізація планів, вирішення конфліктів); $X = [x_1, x_2, ..., x_m]^T$ – вектор вхідних інформаційних станів (рішення DMA, дії агентів реагування (RA), конфлікти різних агентів, глобальний стан ТТМ, сигнали деградації сервісів); $G = \{g_1, g_2, ..., g_k\}$ – множина цілей (мінімізація ризику, збереження критичних сервісів, стабілізація сегментів мережі); $S = \{s_1, s_2, ..., s_l\}$ – стани взаємодії агентів (узгодженість рішень, наявність конфліктів, сесії переговорів); $P = \{p_1, p_2, ..., p_q\}$ – протоколи координації (обмін повідомленнями, механізми консенсусу, аукціонні моделі); $C = \{c_1, c_2, ..., c_r\}$ – контекст координації (ієрархія CNA, обмеження, критичність події); $J_{CNA} = \max\limits_{d \in D} H(Consistency, Cooperation, Timeliness)$ – цільова функція агента, спрямована на максимізацію узгодженості дій агентів.

Крім базових агентів (1) – (6) до складу мультиагентної системи управління кібербезпекою ТТМ включаються також агенти сервісного рівня та підтримки управління, зокрема SLA / Service Agent (SA), Learning Agent (LA), Policy Agent (PA) та Policy Compliance Agent (PCA). Формальні моделі таких агентів визначаються конкретною архітектурою ТТМ та класом завдань управління кібербезпекою, що розв'язуються в ТТМ. Наведена модель ієрархічної мультиагентної системи управління кібербезпекою ТТМ функціонує як сукупність взаємопов'язаних локальних та глобальних контурів управління, узгоджених з ієрархічною структурою самої ТТМ.

Обгрунтування доцільності застосування ієрархічної мультиагентної моделі управління кібербезпекою транспортної телекомунікаційної мережі

Для перевірки гіпотези щодо доцільності застосування запропонованої моделі розглянемо основні класи систем управління, які можуть бути застосовані для управління кібербезпекою ТТМ, зокрема: 1) централізовані; 2) децентралізовані (peer-to-peer); 3) ієрархічні централізовані; 4) ієрархічні мультиагентні системи управління. Для отримання чисельних показників доцільності скористаємось підходом, запропонованим у [11], в якому використовується метод аналізу ієрархій (MAI). Такий метод дозволяє формалізувати експертні думки та отримати узгоджену кількісну оцінку доцільності застосування ієрархічної мультиагентної моделі. Суть методу полягає в наступному [12, 13].

1. Побудова багаторівневої ієрархії показників (рис. 3).

Перший рівень – головна мета оцінювання I_1, яку можна визначити як "Ефективність функціонування системи управління кібербезпекою ТТМ".

Другий рівень – показники $I_{2i}, i = 1...k$, які "забезпечують" головну мету і за якими можна порівняти різні підходи при виборі "найкращого" класу систем управління: I_{21} – якість управління – здатність системи управління кібербезпекою своєчасно виявляти загрози та забезпечувати стійке функціонування ТТМ; I_{22} – вартість експлуатації – економічна ефективність системи управління на всьому життєвому циклі;

Третій рівень $I_{31}, ..., I_{3l}$ – показники порівняння різних класів систем управління: I_{31} – масштабованість – збереження ефективності управління кібербезпекою без суттєвого ускладнення архітектури; I_{32} – час реакції – своєчасність виявлення та нейтралізації

© Хворостяний Р.В. Мультиагентна модель управління кібербезпекою транспортної телекомунікаційної мережі. Сучасний захист інформації, 1(65), 119–131.
https://doi.org/10.31673/2409-7292.2026.011588

кіберзагроз; I_{33} – стійкість – здатність зберігати працездатність навіть за умов часткових відмов або цілеспрямованих атак; I_{34} – адаптивність до загроз – здатність системи управління оперативно змінювати стратегії захисту; I_{35} – спостережність – здатність отримувати інформацію про стан мережі та поведінку її компонентів; I_{36} – локальність прийняття рішень – перенесення частини управлінських рішень на нижчі рівні ієрархії.

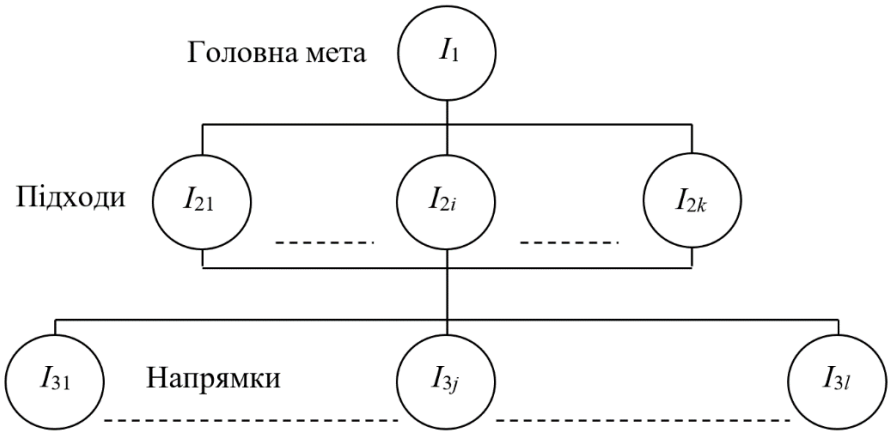

Рис. 3. Багаторівнева ієрархія оцінювання [11]

2. Попарне порівняння елементів на другому рівні: $I_{2i} \div I_{2j},\ i \neq j,\ i,j = 1,2$, на основі матриці парних порівнянь (табл. 1).

Таблиця 1

Матриця парних порівнянь показників на другому рівні

для I_1	I_{21}	I_{2i}	I_{2k}	$\tilde{P}_2(\cdot)$
I_{21}	1	α_{21}^{2i}	α_{21}^{2k}	$\tilde{P}_2(I_{21})$
I_{2i}	α_{2i}^{21}	1	α_{2i}^{2k}	$\tilde{P}_2(I_{2i})$
I_{2k}	α_{2k}^{21}	α_{2k}^{2i}	1	$\tilde{P}_2(I_{2k})$

На головній діагоналі матриці знаходяться 1. Застосовується нормалізована форма показників відносно відповідних I_{2j} до головної мети I_1. Значення $\alpha_{2n}^{2m},\ n,m = 1...k$ формуються на основі оцінок експертів за шкалою 0…10 в результаті чого отримується відношення ваги I_{2i}/I_{2j} (у скільки разів вплив I_{2i} є більш важливим, ніж вплив I_{2j} на головну мету I_1). Отже, α_{2n}^{2m} характеризує вагу I_{2n} за впливом на I_1 відносно I_{2m}:

$$\alpha_{21}^{22} = \frac{I_{21}}{I_{22}};\ \alpha_{2l}^{2i} = \frac{I_{2l}}{I_{2i}};\ \alpha_{2l}^{2k} = \frac{I_{2l}}{I_{2k}};\ \alpha_{2j}^{2j} = 1;\ \alpha_{2n}^{2m} = \frac{I_{2n}}{I_{2m}},\ m,n = 1...k, \tag{7}$$

при чому $\alpha_{2n}^{2m} = \dfrac{1}{\alpha_{2m}^{2n}} = \left[\alpha_{2m}^{2n}\right]^{-1}$.

3. Визначення пріоритетів $\tilde{P}_2(I_{2k})$ показників $I_{2i}, i = 1...k$, як нормованої суми рядків матриці парних порівнянь. Спочатку необхідно визначити суму рядків:

© Хворостяний Р.В. Мультиагентна модель управління кібербезпекою транспортної телекомунікаційної мережі. Сучасний захист інформації, 1(65), 119–131.
https://doi.org/10.31673/2409-7292.2026.011588

$$P_2(I_{21})=1+\alpha_{21}^{22}+\ldots+\alpha_{21}^{2k}=\sum_{r=1}^{k}\alpha_{21}^{2r};$$

$$\ldots;$$

$$P_2(I_{2i})=\alpha_{2i}^{21}+\ldots+1+\ldots+\alpha_{2i}^{2k}=\sum_{r=1}^{k}\alpha_{2i}^{2r}; \quad (8)$$

$$\ldots;$$

$$P_2(I_{2k})=\alpha_{2k}^{21}+\ldots+\alpha_{2k}^{2k-1}+1=\sum_{r=1}^{k}\alpha_{2k}^{2r}.$$

Визначення пріоритетів показників другого рівня шляхом нормування сум рядків (8)

$$\tilde{P}_2(I_{21})=\frac{P_2(I_{21})}{\sum_{r=1}^{k}P_2(I_{2r})};\ \ldots;\ \tilde{P}_2(I_{2i})=\frac{P_2(I_{2i})}{\sum_{r=1}^{k}P_2(I_{2r})};\ \ldots;\ \tilde{P}_2(I_{2k})=\frac{P_2(I_{2k})}{\sum_{r=1}^{k}P_2(I_{2r})}. \quad (9)$$

Тобто:

$$\tilde{P}_2(I_{2i})=\frac{\sum_{r=1}^{k}\alpha_{2k}^{2r}}{\sum_{r=1}^{k}\alpha_{21}^{2r}+\cdots+\sum_{r=1}^{k}\alpha_{2k}^{2r}}=\frac{\sum_{r=1}^{k}\alpha_{2k}^{2r}}{\sum_{s=1}^{k}\sum_{r=1}^{k}\alpha_{2s}^{2r}}. \quad (10)$$

4. Попарне порівняння елементів ієрархії на третьому рівні для кожного $I_{3i} \div I_{3j},\ i \neq j,\ i,j=1...6$ з елементів другого рівня (табл. 2). Здійснюється аналогічно (9) – (10) у нормованій формі і є відношенням показників I_{3i} та $I_{3j},\ i,j=1...l$ до ступеня їх впливу на $I_{2l}, l=1...k$, ${}_1\beta_{3n}^{3m}=\frac{I_{3n}}{I_{3m}},\ m,n=1...l$, ${}_1\beta_{3i}^{3i}=1$.

Таблиця 2

Матриця парних порівнянь показників на третьому рівні

для I_{21}	I_{31}	I_{3i}	I_{3l}	${}_1\tilde{P}_3(\cdot)$
I_{31}	1	${}_1\beta_{31}^{3i}$	${}_1\beta_{31}^{3l}$	${}_1\tilde{P}_3(I_{31})$
I_{3i}	${}_1\beta_{3i}^{31}$	1	${}_1\beta_{3i}^{3l}$	${}_1\tilde{P}_3(I_{3i})$
I_{3l}	${}_1\beta_{3l}^{31}$	${}_1\beta_{3l}^{3i}$	1	${}_1\tilde{P}_3(I_{3l})$
для I_{2j}	I_{31}	I_{3i}	I_{3l}	${}_j\tilde{P}_3(\cdot)$
I_{31}	1	${}_j\beta_{31}^{3i}$	${}_j\beta_{31}^{3l}$	${}_j\tilde{P}_3(I_{31})$
I_{3i}	${}_j\beta_{3i}^{31}$	1	${}_j\beta_{3i}^{3l}$	${}_j\tilde{P}_3(I_{3i})$
I_{3l}	${}_j\beta_{3l}^{31}$	${}_j\beta_{3l}^{3i}$	1	${}_j\tilde{P}_3(I_{3l})$
для I_{2k}	I_{31}	I_{3i}	I_{3l}	${}_k\tilde{P}_3(\cdot)$
I_{31}	1	${}_k\beta_{31}^{3i}$	${}_k\beta_{31}^{3l}$	${}_k\tilde{P}_3(I_{31})$
I_{3i}	${}_k\beta_{3i}^{31}$	1	${}_k\beta_{3i}^{3l}$	${}_k\tilde{P}_3(I_{3i})$
I_{3l}	${}_k\beta_{3l}^{31}$	${}_k\beta_{3l}^{3i}$	1	${}_k\tilde{P}_3(I_{3l})$

© Хворостяний Р.В. Мультиагентна модель управління кібербезпекою транспортної телекомунікаційної мережі. Сучасний захист інформації, 1(65), 119–131.
https://doi.org/10.31673/2409-7292.2026.011588

5. Визначення пріоритетів ${}_i\tilde{P}_3(I_{3i})$, $j=1...l$, $i=1...k$ показників I_{3i}, як нормованої суми рядків відповідної матриці парних порівнянь:

$$
\begin{gathered}
{}_1P_3(I_{31})=1+{}_1\beta_{31}^{32}+...+{}_1\beta_{31}^{3l}=\sum_{r=1}^{l}{}_1\beta_{31}^{3r};\\
...;\\
{}_iP_3(I_{3i})={}_i\beta_{3i}^{31}+...1+...+{}_i\beta_{3i}^{3l}=\sum_{r=1}^{l}{}_i\beta_{3i}^{3r};\\
...;\\
{}_kP_3(I_{3k})={}_k\beta_{3k}^{31}+...+{}_k\beta_{3k}^{3l-1}+1=\sum_{r=1}^{l}{}_k\beta_{3k}^{3r}.
\end{gathered}
\tag{11}
$$

6. Визначення узагальнених ваг показників по відношенню до головної мети – Ефективність функціонування системи управління кібербезпекою ТТМ. Для врахування впливу другого рівня на третій (рис. 3) необхідно здійснити корекцією елементів матриці $\tilde{P}_3$, яка складається з пріоритетів показників I_{3i} з (11) і має назву матриці пріоритетів. Колонками матриці $\tilde{P}_3$ є праві стовпчики табл. 2:

$$
\tilde{P}_3=\begin{bmatrix}
{}_1\tilde{P}_3(I_{31}) & \cdots & {}_k\tilde{P}_3(I_{31})\\
\cdots & \cdots & \cdots\\
{}_1\tilde{P}_3(I_{3l}) & \cdots & {}_k\tilde{P}_3(I_{3l})
\end{bmatrix}.
\tag{12}
$$

Далі матриця пріоритетів $\tilde{P}_3$ (12) модифікується до ${}_м\tilde{P}_3$ з урахуванням пріоритетів $\tilde{P}_2$ шляхом множення матриці $\tilde{P}_3$ на діагональну матрицю $\tilde{P}_2$, де:

$$
\tilde{P}_2=\begin{bmatrix}
\tilde{P}_2(I_{21}) & 0 & 0 & 0 & 0\\
0 & \cdots & 0 & 0 & 0\\
0 & 0 & \tilde{P}_2(I_{2i}) & 0 & 0\\
0 & 0 & 0 & \cdots & 0\\
0 & 0 & 0 & 0 & \tilde{P}_2(I_{2k})
\end{bmatrix}.
\tag{13}
$$

Множення (12) на (13) дає матрицю:

$$
{}_м\tilde{P}_3=\tilde{P}_3\cdot\tilde{P}_2=\begin{bmatrix}
\tilde{P}_2(I_{21})\cdot{}_1\tilde{P}_3(I_{31}) & \cdots & \tilde{P}_2(I_{2k})\cdot{}_k\tilde{P}_3(I_{31})\\
\cdots & \cdots & \cdots\\
\tilde{P}_2(I_{21})\cdot{}_1\tilde{P}_3(I_{3l}) & \cdots & \tilde{P}_2(I_{2k})\cdot{}_k\tilde{P}_3(I_{3l})
\end{bmatrix}.
\tag{14}
$$

Узагальнені ваги V показників I_{3i}, $i=1...l$ по відношенню до I_1 знаходяться шляхом множення матриці ${}_м\tilde{P}_3$ (14) на одиничний вектор $\mathbf{1}_{(l)},\mathbf{1}_{(l)}\in\mathbf{R}^l$, в результаті чого отримується сума рядків ${}_м\tilde{P}_3$

$$
V={}_м\tilde{P}_3\cdot\mathbf{1}_{(l)}=\begin{bmatrix}V_1 & ... & V_l\end{bmatrix}^T,
\tag{15}
$$

© Хворостяний Р.В. Мультиагентна модель управління кібербезпекою транспортної телекомунікаційної мережі. Сучасний захист інформації, 1(65), 119–131.
https://doi.org/10.31673/2409-7292.2026.011588

тобто:

$$\tilde{P}_2(I_{21})\cdot {}_1\tilde{P}_3(I_{31})+\ldots+\tilde{P}_2(I_{2k})\cdot {}_k\tilde{P}_3(I_{31})=\sum_{i=1}^{k}\tilde{P}_2(I_{2i})\cdot {}_i\tilde{P}_3(I_{31});$$

$$\ldots; \qquad (16)$$

$$\tilde{P}_2(I_{21})\cdot {}_1\tilde{P}_3(I_{3l})+\ldots+\tilde{P}_2(I_{2k})\cdot {}_k\tilde{P}_3(I_{3l})=\sum_{i=1}^{k}\tilde{P}_2(I_{2i})\cdot {}_i\tilde{P}_3(I_{3l}).$$

7. За (15) – (16) визначається показник, який максимально впливає на I_1, $V_i : max\left[V_1 \quad \ldots \quad V_l\right]$.

Визначення узгоджених кількісних оцінок моделей управління кібербезпекою ТТМ

Базуючись на попередньому розгляді, визначимо граф показників для моделей управління кібербезпекою ТТМ (рис. 4).

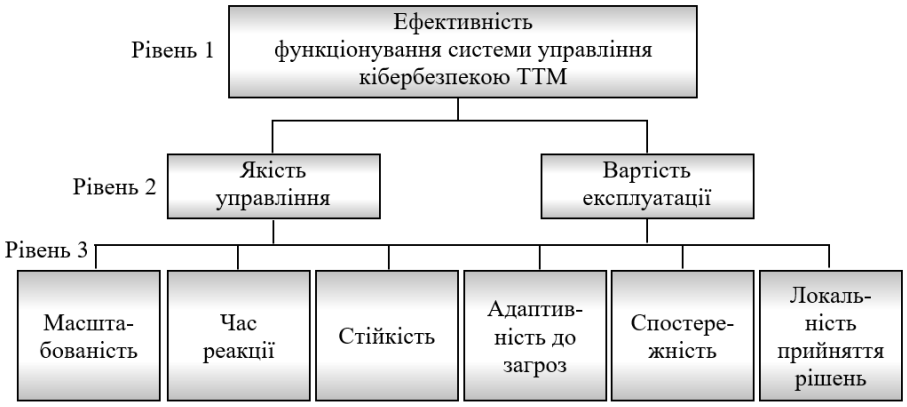

Рис. 4. Граф показників управління кібербезпекою ТТМ

Залучивши групу експертів, для показників, наведених на рис. 3, встановимо відповідну матрицю парних порівнянь другого рівня (табл. 3).

Таблиця 3

Матриця парних порівнянь другого рівня

Ефективність	Якість	Вартість	Σ	Пріоритети $\tilde{P}_2$
Якість	1	2	3.0	0.67
Вартість	1/2	1	1.5	0.33

Матриці парних порівнянь третього рівня для ієрархічної мультиагентної моделі управління мають вигляд (табл. 4, 5).

Таблиця 4

Матриця парних порівнянь третього рівня для показника “якість”

Якість	Масшта-бованість	Час реакції	Стійкість	Адаптив-ність	Спостере-жність	Локаль-ність	Σ	$\tilde{P}_3$
Масштабованість	1	1/3	1/3	1/2	1/2	2	4.67	0.09
Час реакції	3	1	1	2	2	4	13.00	0.26
Стійкість	3	1	1	2	2	4	13.00	0.26
Адаптивність	2	1/2	1/2	1	2	3	9.00	0.18
Спостережність	2	1/2	1/2	1/2	1	3	7.50	0.15
Локальність	1/2	1/4	1/4	1/3	1/3	1	2.67	0.06

© Хворостяний Р.В. Мультиагентна модель управління кібербезпекою транспортної телекомунікаційної мережі. Сучасний захист інформації, 1(65), 119–131.
https://doi.org/10.31673/2409-7292.2026.011588

Так, з табл. 4 видно, що запропоновані попарні оцінки відносно якості управління відображають пріоритетність часу реакції та стійкості над архітектурними та організаційними характеристиками управління кібербезпекою ТТМ, що відповідає вимогам до захисту критичної інфраструктури в умовах динамічних загроз. Відносно вартості експлуатації (табл. 5) найбільший вплив мають масштабованість і локальність прийняття рішень, тоді як мінімальний час реакції та підвищена відмовостійкість потребують, як правило, додаткових ресурсів і збільшують сукупну вартість системи.

Таблиця 5

Матриця парних порівнянь третього рівня для показника “вартість”

Вартість	Масштабованість	Час реакції	Стійкість	Адаптивність	Спостережність	Локальність	Σ	$\tilde{P}_3$
Масштабованість	1	5	3	2	2	2	15.00	0.30
Час реакції	1/5	1	1/2	1/3	1/3	1/4	2.62	0.05
Стійкість	1/3	2	1	1/2	1/2	1/3	4.67	0.09
Адаптивність	1/2	3	2	1	2	1	9.50	0.19
Спостережність	1/2	3	2	1/2	1	1/2	7.50	0.15
Локальність	1/2	4	3	1	2	1	11.50	0.22

В результаті обчислень отримуємо:

– матриця узагальнених ваг $\tilde{P}_3 = \begin{bmatrix} 0.09 & 0.30 \\ 0.26 & 0.05 \\ 0.26 & 0.09 \\ 0.18 & 0.19 \\ 0.15 & 0.15 \\ 0.06 & 0.22 \end{bmatrix}$;

– модифікована матриця $_{\text{м}}\tilde{P}_3 = \begin{bmatrix} 0.09 & 0.30 \\ 0.26 & 0.05 \\ 0.26 & 0.09 \\ 0.18 & 0.19 \\ 0.15 & 0.15 \\ 0.06 & 0.22 \end{bmatrix} \cdot \begin{bmatrix} 0.67 & 0 \\ 0 & 0.33 \end{bmatrix} = \begin{bmatrix} 0.0603 & 0.0990 \\ 0.1742 & 0.0165 \\ 0.1742 & 0.0297 \\ 0.1206 & 0.0627 \\ 0.1005 & 0.0495 \\ 0.0402 & 0.0726 \end{bmatrix}$;

– узагальнені ваги $V = \begin{bmatrix} 0.0603 & 0.0990 \\ 0.1742 & 0.0165 \\ 0.1742 & 0.0297 \\ 0.1206 & 0.0627 \\ 0.1005 & 0.0495 \\ 0.0402 & 0.0726 \end{bmatrix} \cdot \begin{bmatrix} 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 0.1593 \\ 0.1907 \\ 0.2039 \\ 0.1833 \\ 0.1500 \\ 0.1128 \end{bmatrix}$.

Сформований вектор узагальнених ваг відображає ступінь впливу кожного показника третього рівня на загальну ефективність функціонування системи управління кібербезпекою та використовується для побудови інтегрального критерію оцінювання альтернатив у межах

© Хворостяний Р.В. Мультиагентна модель управління кібербезпекою транспортної телекомунікаційної мережі. Сучасний захист інформації, 1(65), 119–131.
https://doi.org/10.31673/2409-7292.2026.011588

ієрархічної мультиагентної системи управління кібербезпекою ТТМ. За аналогічною методикою визначено узагальнені ваги показників ефективності для інших класів систем управління кібербезпекою ТТМ, зокрема централізованих, децентралізованих (peer-to-peer) та ієрархічних централізованих архітектур (рис. 5).

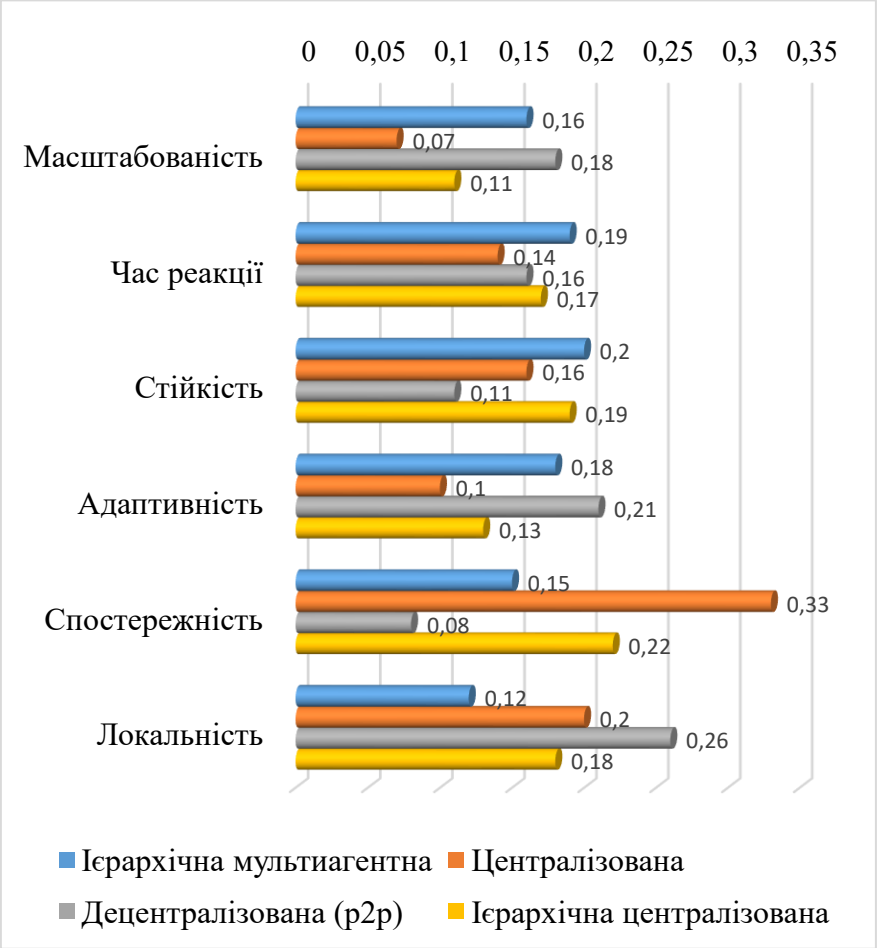

Рис. 5. Узагальнені ваги показників

Згідно з даними, наведеними на рис. 5, ієрархічна мультиагентна модель управління кібербезпекою ТТМ характеризується найбільш збалансованим розподілом вагових коефіцієнтів між ключовими показниками функціонування системи. На відміну від централізованої архітектури, для якої притаманна домінантна роль показника спостережуваності (0.33) за рахунок зниження масштабованості та адаптивності, запропонована модель демонструє відносно рівномірні та високі значення ваг для часу реакції (0.19), стійкості (0.20) та адаптивності (0.18), що є принципово важливим для ТТМ як динамічної та розподіленої системи. Порівняно з децентралізованими (peer-to-peer) системами, у яких переважають локальність прийняття рішень (0.26) та адаптивність (0.21) при знижених показниках спостережуваності й стійкості, ієрархічна мультиагентна модель забезпечує раціональне поєднання локальної автономії та глобальної координації. Водночас ієрархічна централізована система, хоча й частково нівелює обмеження повністю централізованого підходу, зберігає акцент на централізованому контролі (спостережуваність – 0.22), що стримує гнучкість реагування на локальні події. Отримані вагові коефіцієнти кількісно підтверджують доцільність застосування ієрархічної мультиагентної моделі для управління кібербезпекою ТТМ в умовах масштабованості, часткової спостережуваності та динамічного характеру кіберзагроз.

© Хворостяний Р.В. Мультиагентна модель управління кібербезпекою транспортної телекомунікаційної мережі. Сучасний захист інформації, 1(65), 119–131.
https://doi.org/10.31673/2409-7292.2026.011588

Висновки

Отримані результати підтверджують, що ієрархічна мультиагентна модель є обґрунтованим та доцільним підходом до побудови системи управління кібербезпекою транспортної телекомунікаційної мережі, оскільки забезпечує узгоджене поєднання локальної автономії агентів і глобальної координації управління, збалансований розподіл функцій між рівнями ієрархії та адаптивне залучення ресурсів захисту відповідно до складності загроз. Порівняльний аналіз альтернативних архітектур і отримані вагові коефіцієнти показників ефективності кількісно засвідчили її переваги в умовах масштабованості, часткової спостережуваності та динамічного характеру кіберзагроз, що створює підґрунтя для подальшої алгоритмічної деталізації та практичної реалізації запропонованої моделі.

Перелік посилань

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

2. Khoroshko, V., Khokhlachova, Y., & Vyshnevska, N. (2023). Decomposition of Computer Network Technology In Their Design. Ukrainian Scientific Journal of Information Security, 29(3), 130–137. https://doi.org/10.18372/2225-5036.29.18072.

3. Пановик, У. П. (2024). Кібербезпека в Телекомунікаційних Мережах та Системах. Наукові Записки, 1(68), 122–135. https://nz.uad.lviv.ua/media/1-68/13.pdf

4. Khavina, I. P., Hnusov, Yu. V., & Mozhaiev, O. O. (2022). Development of multi-agent information security management system. Law and Safety, 87(4), pp. 171–183. https://doi.org/10.32631/pb.2022.4.14.

5. Кітура, О. В. (2023). Методика формування системи управління транспортною мережею зв'язку. Дис. докт. філософії за спец. 172 "Телекомунікації та радіотехніка". Київ, ДУТ, 133 с. https://duikt.edu.ua/uploads/p_2625_85571738.pdf.

6. Дакова, Л. В. (2023). Мультиагентні моделі керування та самоорганізації в мережах 5-го покоління. Зв'язок, 5, 9–14. https://doi.org/10.31673/2412-9070.2023.050914.

7. Прокопенко, А. Г. (2024). Метод розподіленого моніторингу телекомунікаційних мереж на основі агентного підходу. Наукові записки Державного університету інформаційно-комунікаційних технологій, 2, 104–115. https://journals.dut.edu.ua/index.php/sciencenotes/article/view/3096/2986.

8. Кубрак, Ю. О., Плечистий, Д. Д., & Романішин, В. В. (2022). Принципи формування мультиагентної системи штучного інтелекту. Комп'ютерно-інтегровані технології: освіта, наука, виробництво, 48, 76–82. https://cit.lntu.edu.ua/bot-check.php?destination=/index.php/cit/article/view/372/473.

9. Singh, A. V., Rathbun, E., Graham, E., Oakley, L., Boboila, S., Oprea, A., & Chin, P. Hierarchical Multi-agent Reinforcement Learning for Cyber Network Defense. arXiv:2410.17351. https://doi.org/10.48550/arXiv.2410.17351.

10. Персунов, Д. О., & Апенько, Н. В. (2025). Інтелектуальні агенти в системах кібербезпеки: концепція адаптивного захисту на основі ШІ. Штучний інтелект і безпека: науково-практична конференція Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України, 04 грудня 2025 р. Київ : ІПМЕ ім. Г.Є.Пухова НАН України. 271 с. https://ipme.kiev.ua/wp-content/uploads/2025/12/%D0%97%D0%B1%D1%96%D1%80%D0%BD%D0%B8%D0%BA-%D0%BC%D0%B0%D1%82%D0%B5%D1%80%D1%96%D0%B0%D0%BB%D1%96%D0%B2-%D0%A8%D0%86%D0%91-2025.pdf.

11. Савченко, В. А., & Рибальченко, О. Г. (2024). Побудова ефективної системи мережевої безпеки підприємства на основі методу аналізу ієрархій показників якості. Сучасний захист інформації, 1(57), 6-14. https://doi.org/10.31673/2409-7292.2024.010001.

12. Нісфоян, С. С., Сисоліна, Н. П, Савеленко, Г. В. (2020). Розвиток методу аналізу ієрархій як механізму вибору інвестиційного проєкту на підприємстві. Центральноукраїнський науковий вісник. Економічні науки, вип. 5(38), 228–237. https://doi.org/10.32515/2663-1636.2020.5(38).228-237.

13. Шаповалова, О. О., & Бурменський, Р. В. (2017). Розробка програмного додатка для реалізації методу аналізу ієрархій. Системи обробки інформації, 3(149), 45–48. https://doi.org/10.30748/soi.2017.149.09.

Надійшла до редакції (Received): 15.02.2026
Прийнята до друку (Accepted): 17.03.2026
Опубліковано онлайн (Available online): 30.03.2026

http://creativecommons.org/licenses/by/4.0/
This work is licensed under Creative Commons Attribution-noncommercial-sharealike 4.0 International License.

© Хворостяний Р.В. Мультиагентна модель управління кібербезпекою транспортної телекомунікаційної мережі. Сучасний захист інформації, 1(65), 119–131.
https://doi.org/10.31673/2409-7292.2026.011588