УДК 621.396 DOI 10.31673/2412-4338.2025.017512

Жебка Вікторія Вікторівна
Державний університет інформаційно-комунікаційних технологій, м. Київ
ORCID 0000-0003-4051-1190

Нестеренко Катерина Сергіївна
Державний університет інформаційно-комунікаційних технологій, Київ
ORCID 0000-0001-7672-7386

Жебка Сергій Валентинович
Державний університет інформаційно-комунікаційних технологій, Київ
ORCID 0009-0007-4620-9888

МЕТОДИ УПРАВЛІННЯ СТІЙКОЮ ГЕТЕРОГЕННОЮ ТЕЛЕКОМУНІКАЦІЙНОЮ МЕРЕЖЕЮ В УМОВАХ ВПЛИВУ ДЕСТАБІЛІЗУЮЧИХ ЧИННИКІВ

Анотація. *У статті розглянуто методи управління стійкою гетерогенною телекомунікаційною мережею в умовах впливу дестабілізуючих чинників. Проведено аналіз існуючих підходів до забезпечення стійкості мережевої інфраструктури, включаючи адаптивні алгоритми маршрутизації, методи прогнозування навантаження, ймовірнісні моделі оцінки надійності, стратегії резервування ресурсів та блокчейн-орієнтовані механізми безпеки. Показано, що кожен із цих методів має свої переваги та обмеження, які необхідно враховувати при розробці ефективних механізмів управління.*

Дослідження адаптивних алгоритмів маршрутизації, зокрема Беллмана-Форда та Dijkstra, свідчить про їхню ефективність у статичних умовах, однак вони демонструють недостатню продуктивність у високодинамічних середовищах через високу обчислювальну складність та необхідність попереднього обчислення маршрутів. Методи прогнозування навантаження, зокрема ARIMA та LSTM, дозволяють підвищити ефективність управління мережею, забезпечуючи точне прогнозування змін у трафіку, проте вони мають значну обчислювальну складність та потребують якісних вхідних даних.

Розглянуто ймовірнісні підходи до моделювання стійкості мережі, включаючи використання Марковських ланцюгів для оцінки рівня ризиків відмов та забезпечення надійності функціонування інфраструктури. Однак встановлено, що ці методи часто базуються на припущеннях, які не завжди відповідають реальним умовам експлуатації. Стратегії резервування ресурсів, зокрема динамічне резервування каналів зв'язку та моделі M/M/1, сприяють підвищенню стійкості мережі, однак вимагають точного прогнозування навантаження та оптимального розподілу обчислювальних ресурсів.

Окрему увагу приділено використанню блокчейн-технологій у процесах авторизації, захисту переданих даних та децентралізованого розподілу ресурсів. Запропоновано використання смарт-контрактів для автоматизації управління мережею, що дозволяє знизити вплив людського фактора та підвищити безпеку телекомунікаційних систем.

Перспективи подальших досліджень охоплюють розробку гібридних методів управління, що поєднують штучний інтелект, машинне навчання та блокчейн для забезпечення адаптивності телекомунікаційних мереж. Зокрема, запропоновано використання глибоких нейронних мереж для оптимізації трафіку та інтеграцію квантових обчислень для прискорення обробки маршрутних даних. Також актуальним є напрям розробки методів раннього виявлення кібератак на основі аналізу аномалій у мережевому трафіку.

Таким чином, проведене дослідження демонструє важливість комплексного підходу до управління гетерогенними телекомунікаційними мережами та підкреслює необхідність подальшої інтеграції сучасних технологій для підвищення рівня стійкості системи в умовах дестабілізуючих чинників.

Ключові слова: *стійкість, телекомунікаційні мережі, адаптивне управління, прогнозування навантаження, маршрутизація, ймовірнісні моделі, блокчейн, штучний інтелект, машинне навчання, резервування ресурсів.*

Zhebka Viktoriia
State university of information and communication technologies, Kyiv
ORCID 0000-0003-4051-1190

Nesterenko Kateryna
State university of information and communication technologies, Kyiv
ORCID 0000-0001-7672-7386

Zhebka Serhii
State university of information and communication technologies, Kyiv
ORCID 0009-0007-4620-9888

METHODS OF MANAGING A FUNCTIONALLY RESILIENT HETEROGENEOUS TELECOMMUNICATION NETWORK UNDER THE INFLUENCE OF DESTABILIZING FACTORS

Abstract. *The article examines methods for managing a functionally resilient heterogeneous telecommunication network under the influence of destabilizing factors. An analysis of existing approaches to ensuring network infrastructure resilience has been conducted, including adaptive routing algorithms, traffic load prediction methods, probabilistic reliability assessment models, resource reservation strategies, and blockchain-oriented security mechanisms. It is shown that each of these methods has its own advantages and limitations that must be considered when developing effective management mechanisms.*

The study of adaptive routing algorithms, particularly Bellman-Ford and Dijkstra, demonstrates their efficiency in static conditions; however, they exhibit insufficient performance in highly dynamic environments due to high computational complexity and the necessity of precomputing routes. Load forecasting methods, such as ARIMA and LSTM, enhance network management efficiency by accurately predicting traffic changes. However, they have significant computational complexity and require high-quality input data.

Probabilistic approaches to network resilience modeling have been considered, including the use of Markov chains for assessing failure risks and ensuring infrastructure reliability. However, it has been found that these methods are often based on assumptions that do not always correspond to real operational conditions. Resource reservation strategies, particularly dynamic channel reservation and M/M/1 models, contribute to improving network resilience. Nevertheless, they require precise load forecasting and optimal allocation of computational resources.

Special attention is given to the use of blockchain technologies in authorization processes, data transmission security, and decentralized resource distribution. The use of smart contracts for network management automation is proposed, which reduces the influence of human factors and enhances the security of telecommunication systems.

Prospects for further research include the development of hybrid management methods that combine artificial intelligence, machine learning, and blockchain to ensure the adaptability of telecommunication networks. In particular, the use of deep neural networks for traffic optimization and the integration of quantum computing to accelerate route data processing have been proposed. Additionally, the development of methods for early cyberattack detection based on network traffic anomaly analysis remains a relevant direction.

Thus, the conducted research demonstrates the importance of a comprehensive approach to managing heterogeneous telecommunication networks and emphasizes the need for further integration of modern technologies to enhance the functional resilience of systems under destabilizing factors.

Keywords: *functional resilience, telecommunication networks, adaptive management, load forecasting, routing, probabilistic models, blockchain, artificial intelligence, machine learning, resource reservation.*

1. Вступ. Сучасні телекомунікаційні мережі стають все більш гетерогенними, оскільки вони включають різноманітні технології, пристрої та підключення, що створює нові виклики для їх ефективного управління. Гетерогенні мережі потребують застосування комплексних методів для забезпечення їх безперебійної роботи, що є особливо важливим у випадку виникнення дестабілізуючих чинників, таких як технічні збої, природні катастрофи, кібератаки, зміни в навантаженні або політичні та економічні фактори, що можуть впливати на їх функціонування.

Одним із ключових аспектів цього дослідження є забезпечення стійкості мережі, що передбачає здатність мережі відновлювати свою нормальну роботу після виникнення несправностей чи змін у зовнішньому середовищі, а також оптимізувати використання ресурсів з урахуванням змін у навантаженні та умовах експлуатації.

2. Аналіз останніх досліджень і публікацій. У дослідженнях щодо управління стійкими гетерогенними телекомунікаційними мережами в умовах впливу дестабілізуючих чинників велика увага приділяється використанню різних методів моделювання та управління для забезпечення стійкості мережі. Однією з важливих тенденцій є розробка методів, що дозволяють адаптувати телекомунікаційні мережі до змінних умов, таких як навантаження або зовнішні загрози, включаючи кібератаки та фізичні пошкодження.

Одним із прикладів є робота Джонса і Паркера [1], в якій запропоновано новий підхід до моніторингу і прогнозування потенційних збоїв у мережах на основі штучного інтелекту. Цей підхід дозволяє виявляти та запобігати можливим уразливим точкам у мережі шляхом використання адаптивних моделей, що враховують як статистичні, так і динамічні характеристики мережі. Однак, попри високий рівень теоретичного аналізу, практичне застосування цих моделей на великих масштабах вимагає подальшого вивчення, особливо в умовах реальних телекомунікаційних мереж, де виявлення збоїв у реальному часі є критичним.

Подібне дослідження було проведене Лопесом і співробітниками [2], де обговорюється роль математичних моделей, зокрема методів перколяції для оцінки стійкості гетерогенних мереж до фізичних і кібератак. Вони використовують моделі для прогнозування наслідків порушення роботи мережевих компонентів і виявляють ключові елементи, які є найбільш вразливими до дестабілізуючих чинників. Однак цей підхід не враховує інтеграцію таких моделей з реальними системами управління, що є важливим напрямком для подальших досліджень.

Крім того, робота Брауна та Сміта [3] детально аналізує використання технології SDN (Software-Defined Networking) для забезпечення стійкості телекомунікаційних мереж в умовах динамічного зміщення трафіку. Їх методика дозволяє прогнозувати навантаження на окремі елементи мережі і автоматично перенаправляти трафік в разі перевантаження. Однак, варто зазначити, що в реальних умовах, де мережі можуть бути частково гетерогенними або складними за своєю структурою, ці методи потребують додаткової адаптації та дослідження щодо ефективності їх впровадження на різних етапах життєвого циклу мережі.

У свою чергу, в дослідженнях Квіні й Хуана [4] запропоновано підхід, який об'єднує використання традиційних моделей та адаптивних алгоритмів управління, що дозволяє забезпечити стабільність роботи мереж навіть при виникненні неочікуваних збитків. Проте ці методи вимагають глибшого аналізу ефективності у реальних умовах, оскільки їх застосування не завжди є можливим в умовах повної динаміки мережі, де фактори ризику можуть змінюватися значно швидше, ніж ці алгоритми можуть реагувати.

Також варто відзначити роботи таких авторів, як Умберг та Габріел [5], які аналізують застосування теорії ігор для оптимізації ресурсів у гетерогенних мережах. Вони фокусуються на балансуванні навантаження між різними мережами, що є важливим аспектом для забезпечення стійкості в умовах навантаження та можливих атак. Водночас, їх підхід вимагає додаткових досліджень щодо застосування цих теорій у контексті телекомунікаційних систем з високою варіативністю умов, що потребують не лише математичної моделі, але й гнучких адаптивних стратегій управління.

Водночас важливим напрямком є використання блокчейн-технології для забезпечення надійності й безпеки гетерогенних мереж, що розглядають такі автори, як Скотт і Севілле [6]. Вони пропонують інтеграцію блокчейн для управління стійкістю в умовах великих і складних мереж, однак, незважаючи на перспективність цієї технології, її застосування вимагає додаткових досліджень щодо сумісності з різними типами мережевих архітектур і її масштабованості на великі телекомунікаційні системи.

Дослідження вказаних авторів показують, що існує великий потенціал для розробки нових підходів до управління стійкістю гетерогенних мереж, але водночас вони підкреслюють, що існує низка відкритих питань, які потребують подальших досліджень, зокрема щодо адаптації теоретичних моделей до практичних умов, інтеграції нових технологій і методів на рівні реальних мереж та розробки ефективних механізмів адаптації в умовах постійно змінюваного середовища.

3. Мета і задачі дослідження. Метою дослідження є аналіз методів та підходів до управління гетерогенними телекомунікаційними мережами, які дозволяють підтримувати їх стійкість навіть за умов впливу дестабілізуючих факторів, оптимізуючи баланс між надійністю, швидкодією та ресурсною ефективністю. Це включає в себе аналіз та моделювання різних сценаріїв впливу на мережу, створення алгоритмів для адаптивного управління та механізмів відновлення після збоїв, а також інтеграцію технологій штучного інтелекту та машинного навчання для автоматизації процесів прийняття рішень.

Дане дослідження є важливим для розвитку майбутніх телекомунікаційних систем, де забезпечення стійкості та адаптації до змінних умов є критичним фактором для забезпечення безперебійної роботи на глобальному рівні.

4. Результати дослідження. Управління стійкою гетерогенною телекомунікаційною мережею в умовах впливу дестабілізуючих чинників є важливою проблемою, яка вимагає розробки адаптивних і динамічних методів для забезпечення безперервної роботи мережі. Гетерогенні мережі, що складаються з різноманітних компонентів, таких як різні типи мережевих технологій, інфраструктур, пристроїв і протоколів, є надзвичайно чутливими до зовнішніх та внутрішніх збоїв. Однак вони також забезпечують високу гнучкість, що дозволяє використовувати їх для вирішення складних завдань управління ресурсами в реальному часі.

Загалом, для управління такими мережами в умовах дестабілізуючих чинників необхідно застосовувати різноманітні підходи, що включають математичні моделі, технології прогнозування, адаптивні алгоритми, методи оптимізації та захисту. Ключовим аспектом є прогнозування і виявлення потенційних загроз на основі аналізу даних, а також адаптація мережі до змінних умов.

Використання адаптивних алгоритмів у таких мережах дозволяє мінімізувати наслідки збоїв і забезпечити їх відновлення в реальному часі. Наприклад, підхід, заснований на використанні штучного інтелекту (ШІ) для прогнозування навантаження та виявлення аномалій у мережі, дозволяє швидко реагувати на зміну ситуації. Моделі ШІ можуть бути реалізовані на основі алгоритмів машинного навчання, таких як нейронні мережі, які вчаться на історичних даних і роблять прогнози для майбутніх сценаріїв. Це дозволяє своєчасно виявляти уразливості в мережі та адаптувати її до зміни навантаження або можливих атак.

Ці алгоритми динамічно змінюють маршрути передачі даних у відповідь на зміну стану мережі. Одним з найпоширеніших є **алгоритм Беллмана-Форда**, який мінімізує вагу шляху між вузлами:

$$d(v)=min_{(u,v)\in E}\{d(u)+w(u,v)\} \quad (1)$$

де $d(v)$ — найкоротша відстань до вузла v, $w(u,v)$ — вага (затримка, пропускна здатність) між вузлами u і v.

Також використовується алгоритм **Dijkstra**, який забезпечує швидкий пошук найкоротших маршрутів для критично важливого трафіку.

Алгоритм Беллмана-Форда знаходить найкоротший шлях у зваженому графі, що дозволяє враховувати зміну топології мережі та зміну стану каналів зв’язку, проте його обчислювальна складність робить його менш ефективним для великих мереж. Dijkstra забезпечує швидке знаходження найкоротших маршрутів, що корисно для статичних мереж,

але вимагає попереднього обчислення таблиць маршрутів, що робить його менш придатним для мобільних мереж.

Методи прогнозування навантаження, такі як ARIMA (AutoRegressive Integrated Moving Average), забезпечують аналіз часових рядів та прогнозування змін у мережевому трафіку, що дозволяє оптимізувати розподіл ресурсів, проте вони чутливі до різких змін у навантаженні. LSTM-мережі, використовуючи довготривалу пам'ять, здатні моделювати залежності у часі та враховувати нетривіальні закономірності в трафіку, що є значною перевагою для мереж 5G, але потребують значних обчислювальних ресурсів і попереднього навчання.

Для прогнозування навантаження в телекомунікаційних мережах використовується авторегресивна модель з ковзним середнім ARIMA:

$$\mathrm{Y_t} = \mathrm{c} + \sum_{i=1}^{p} \varphi_i Y_{t-i} + \sum_{j=1}^{q} \theta_j \, \varepsilon_{t-j} + \varepsilon_t \qquad (2)$$

де p – порядок авторегресії, q – порядок ковзного середнього, ε_t – шум.

Нейронні мережі LSTM **(Long Short-Term Memory)** використовуються для прогнозування трафіку на основі часових рядів:

$$h_t=\sigma(W_h h_{t-1}+W_x X_t+b), \qquad (3)$$

де h_t – прихований стан, W_h,W_x – ваги моделі, X_t – вхідний трафік, σ – функція активації (наприклад, сигмоїда).

Іншим важливим методом є застосування теорії ймовірності та статистичних методів для оцінки ризиків і визначення найлегших шляхів для адаптації мережі до непередбачуваних обставин. Наприклад, методи Монте-Карло або марковські процеси можуть бути використані для моделювання ймовірностей збоїв, а також для прогнозування ефективності різних стратегій управління.

Система моделюється як ланцюг Маркова з можливими станами:

$$P(t)=P(0)e^{Qt}$$

де $P(t)$ – ймовірність того, що система функціонує у стані t, Q – матриця ймовірностей переходу між станами.

Ймовірнісні моделі, зокрема Марковські ланцюги, дають змогу прогнозувати стани мережі в умовах випадкових відмов, допомагаючи оцінити рівень стійкості. Однак вони обмежені припущенням про експоненційний розподіл відмов, що не завжди відповідає реальним умовам експлуатації телекомунікаційних мереж.

Одним із важливих аспектів є також використання технологій для відновлення після збоїв. Наприклад, методи резервування та багаторівневих схем управління трафіком допомагають забезпечити безперервність роботи мережі навіть при часткових порушеннях її компонентів. Технічне резервування може бути організовано на рівні маршрутизаторів або каналів зв'язку, що дозволяє здійснювати перенаправлення трафіку на інші, менш навантажені канали або маршрути в разі аварій.

Модель рівноваги між використанням і резервуванням каналів визначається через функцію корисності:

$$\mathrm{R} = \arg\max \sum_{i=1}^{n} (Ui(Ci - Ri))$$

де R_i – зарезервовані ресурси, C_i — загальна ємність, U_i – функція корисності.

Модель оптимального розподілу ресурсів (M/M/1)

Оцінка часу очікування в черзі:

$$W=1/(\mu-\lambda)$$

де λ – інтенсивність надходження заявок, μ – швидкість обслуговування.

Методи резервування ресурсів включають динамічне резервування каналів, яке дозволяє мінімізувати втрати пакетів у періоди пікових навантажень, і модель M/M/1, яка допомагає оцінити необхідну кількість ресурсів для забезпечення якості обслуговування. Використання оптимального розподілу ресурсів сприяє підвищенню стійкості мережі, але вимагає точного прогнозування навантаження.

Блокчейн-орієнтовані методи, такі як авторизація трафіку на основі криптографічних хеш-функцій, забезпечують безпеку обміну даними в розподілених мережах та дозволяють знизити ймовірність атак на інфраструктуру мережі. Смарт-контракти автоматизують процес резервування ресурсів, зменшуючи вплив людського фактора, що особливо корисно у складних мережевих середовищах із великою кількістю вузлів.

Блокчейн для авторизації трафіку використовує механізм перевірки достовірності даних реалізується через хеш-функції:

$$H=SHA\text{-}256(B_{prev}||T_{data}||N)$$

де B_{prev} – хеш попереднього блоку, T_{data} – транзакційні дані, N – nonce.

Розподілене управління ресурсами за допомогою смарт-контрактів використовує формалізацію процесу резервування ресурсів через смарт-контракти:

$$S = \sum_{i=1}^{n} T_i \times P_i$$

де S – загальна вартість резервування, T_i – час використання ресурсу, P_i – ціна за одиницю ресурсу.

Таблиця 1

Порівняння методів управління стійкою гетерогенною телекомунікаційною мережею

Метод/Підхід	Опис	Приклад застосування
Адаптивні алгоритми	Алгоритми, які налаштовуються відповідно до змін у мережевих умовах. Включають методи машинного навчання та ШІ.	Використання нейронних мереж для прогнозування навантаження та виявлення аномалій.
Прогнозування навантаження	Використання статистичних та математичних моделей для прогнозування майбутніх станів мережі на основі поточних та історичних даних.	Прогнозування трафіку для оптимізації використання мережевих ресурсів.
Теорія ймовірності та статистика	Методи для оцінки ймовірності збоїв і розробки стратегій управління на основі ризиків.	Використання марковських процесів для прогнозування відмов у мережах.
Резервування та багаторівневі схеми	Методи для відновлення роботи мережі після збоїв, включаючи фізичне резервування та логічні схеми для перенаправлення трафіку.	Створення резервних каналів для перенаправлення трафіку при відмовах.
Технології блокчейн	Використання блокчейн для забезпечення надійності та безпеки мережі через децентралізоване управління доступом і моніторинг.	Впровадження блокчейн для захисту даних у мережах IoT.

На рис. 1 представлена методика реалізує адаптивне управління мережею, використовуючи три ключові підходи: методи глибокого навчання (LSTM), алгоритм пошуку найкоротшого шляху (Dijkstra) та блокчейн-технології. Алгоритм починається з отримання вхідних параметрів, що включають поточний стан мережі, рівень завантаженості та потенційні загрози. Після цього проводиться класифікація навантаження: якщо воно є динамічним,

застосовується метод LSTM для прогнозування та оптимізації розподілу ресурсів у реальному часі.

Якщо навантаження має статичний характер, використовується алгоритм Dijkstra, що дозволяє знаходити оптимальні маршрути передавання даних. У разі, коли мережа зазнає критичного збою (наприклад, відмови вузлів або кібератаки), активуються блокчейн-методи для забезпечення цілісності та стійкості інфраструктури. Блокчейн дозволяє відстежувати транзакції та підтримувати безпечну маршрутизацію даних. Завершальним етапом є формування та передача результатів управління мережею.

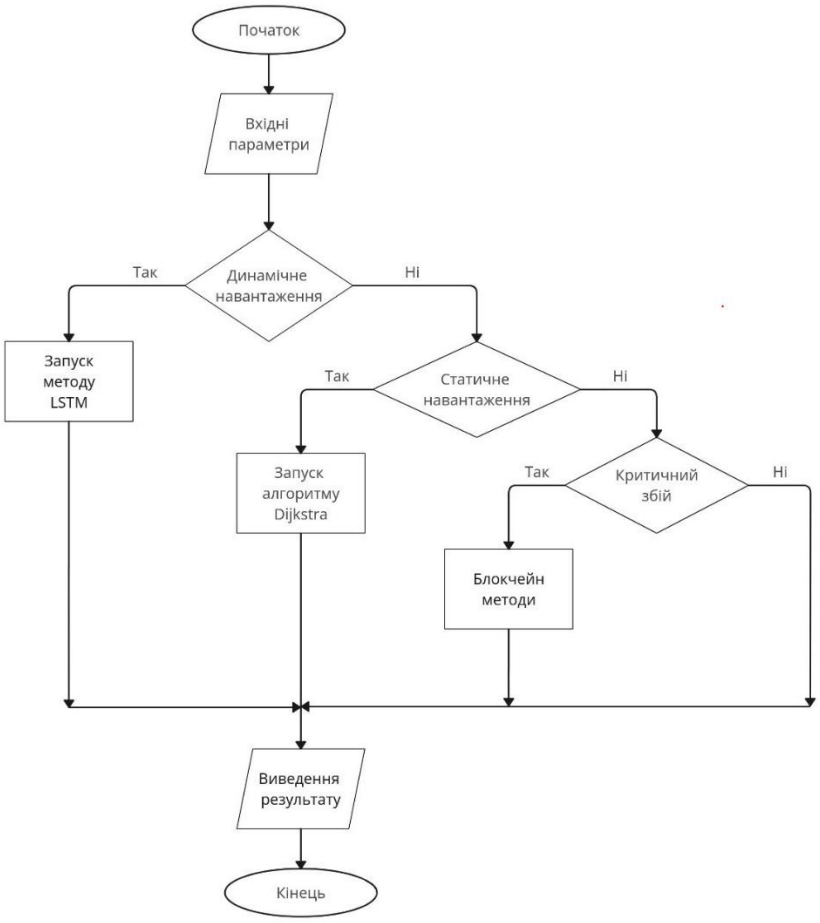

Рис. 1. Методика управління стійкою гетерогенною телекомунікаційною мережею

Оскільки алгоритм орієнтований на адаптивне управління, одним із напрямів його вдосконалення є впровадження гібридних моделей, що комбінують LSTM з іншими методами прогнозування, такими як GRU або XGBoost. Також можливе розширення блокчейн-функціональності для автоматичної аутентифікації вузлів та виявлення аномалій. Додатково варто розглянути інтеграцію методів оптимізації навантаження в умовах швидких змін у топології мережі, що підвищить ефективність управління в режимі реального часу.

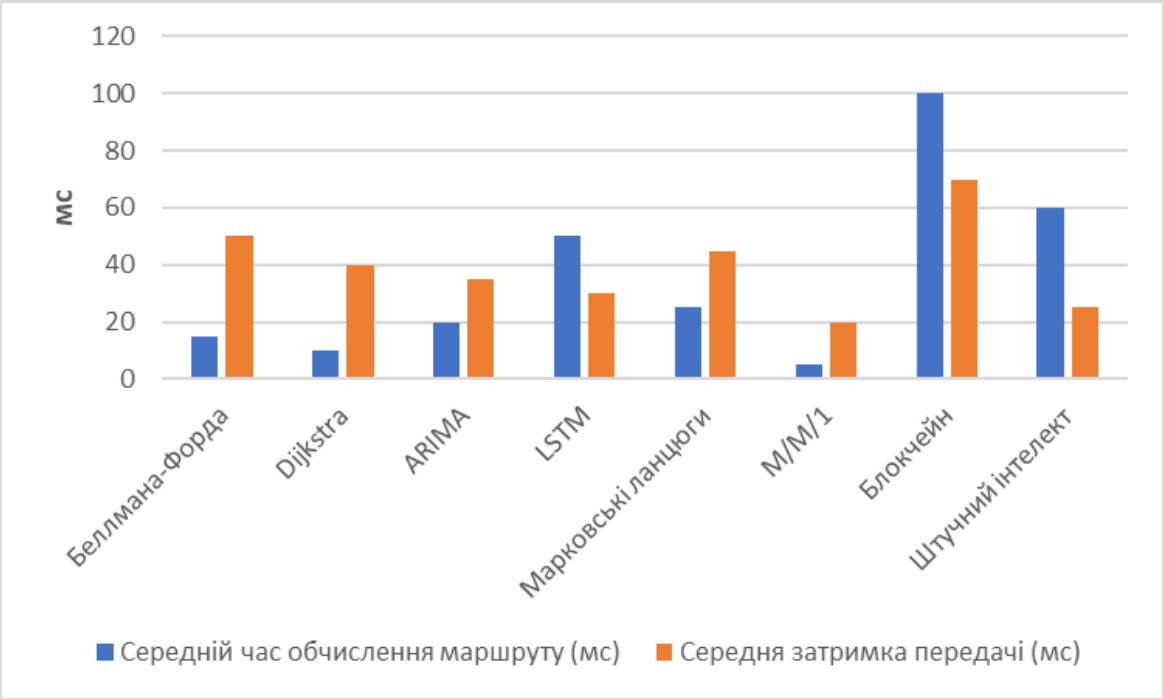

Рис. 2. Порівняння методів управління стійкою гетерогенною телекомунікаційною мережею за середнім часом та середньою затримкою

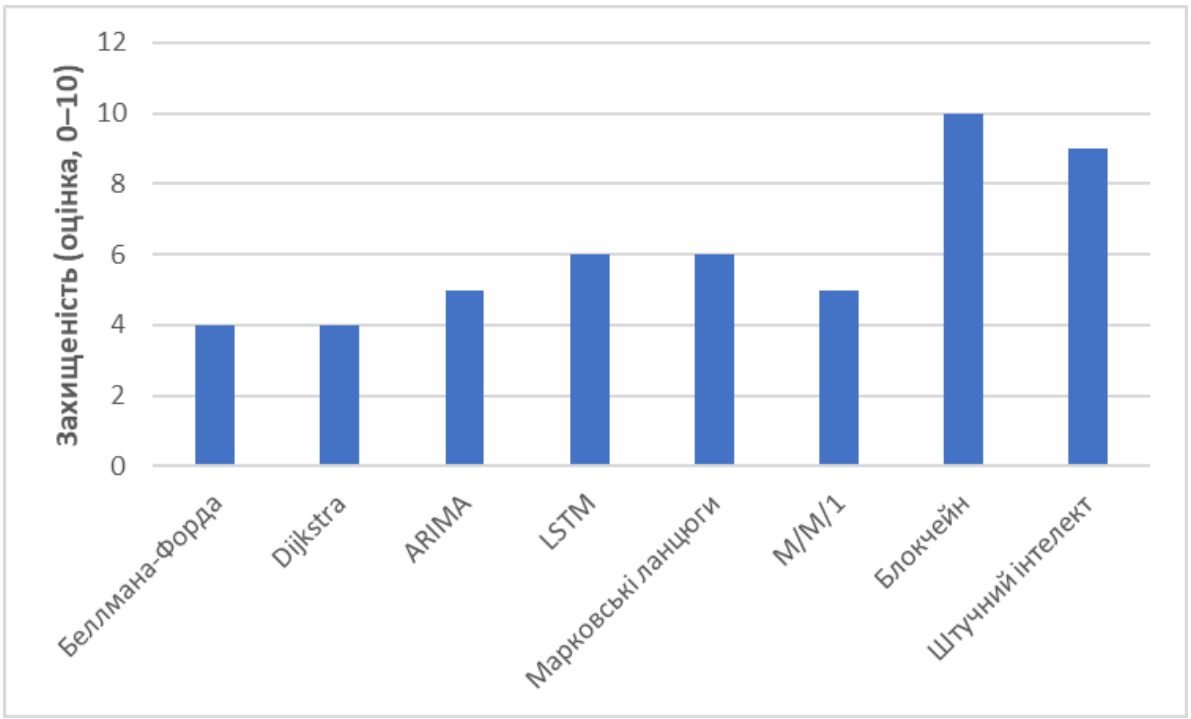

Рис. 3. Порівняння методів управління стійкою гетерогенною телекомунікаційною мережею за рівнем захищеності

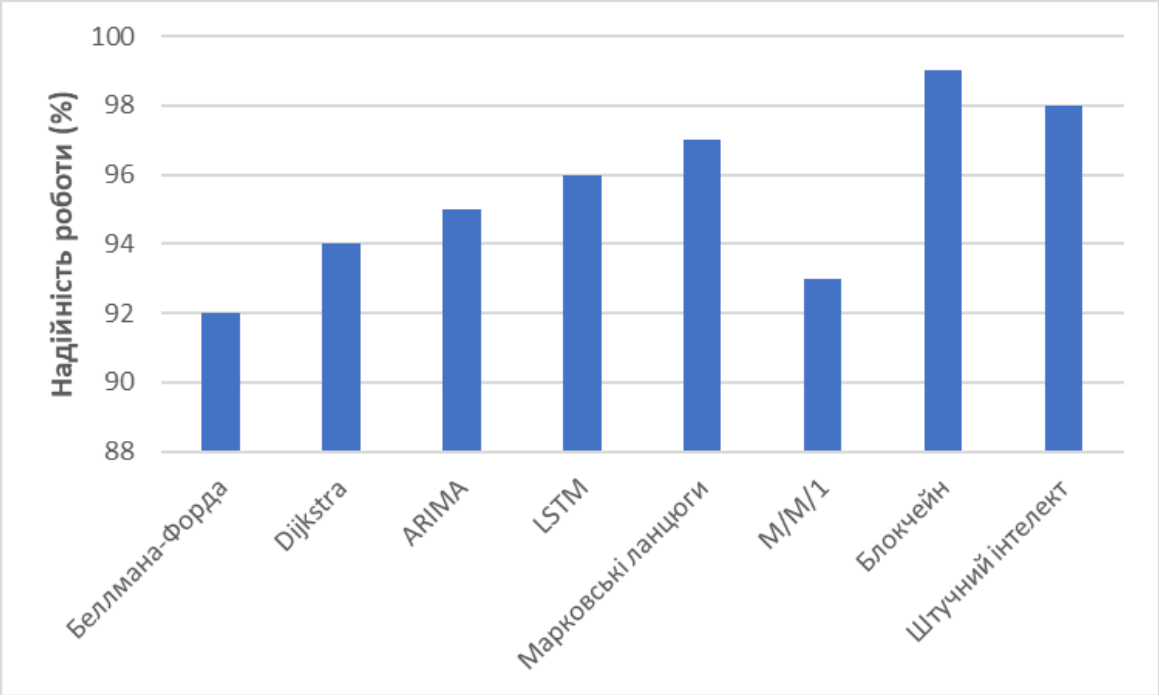

Рис. 4. Порівняння методів управління стійкою гетерогенною телекомунікаційною мережею за надійністю

Методи на основі машинного навчання (LSTM) та блокчейн-смартконтрактів демонструють високу точність і стійкість, тоді як класичні алгоритми маршрутизації (Беллман-Форд, Dijkstra) мають більшу затримку.

Таким чином, для забезпечення стійкості гетерогенних телекомунікаційних мереж в умовах дестабілізуючих чинників необхідно комбінувати різні методи управління та розробляти нові інтегровані рішення, які можуть ефективно реагувати на постійно змінювані умови. В майбутньому важливо буде зосередити увагу на розробці методів, що дозволяють інтегрувати різні технічні рішення в єдину систему управління, що забезпечує надійність і стійкість мережі на всіх етапах її життєвого циклу.

Така інтеграція різних методів дозволить створити більш стійку та адаптивну інфраструктуру для телекомунікаційних мереж, яка зможе ефективно реагувати на несподівані ситуації, забезпечуючи безперервність і надійність у роботі.

5. Висновки. У дослідженні було проведено огляд існуючих підходів до прогнозування Аналіз існуючих методів показав, що жоден із них окремо не може повністю вирішити проблему стійкості в умовах реальних експлуатаційних загроз, однак їх поєднання дозволяє значно покращити ефективність управління.

Адаптивні алгоритми маршрутизації, зокрема Беллмана-Форда та Dijkstra, демонструють високу ефективність у випадку статичних і предиктивних умов, але їх обчислювальна складність та залежність від топологічних змін потребують вдосконалення. Методи прогнозування навантаження, такі як ARIMA та LSTM, дозволяють здійснювати більш точне управління ресурсами, але вимагають оптимізації параметрів для швидкої адаптації до змінних умов експлуатації. Ймовірнісні моделі та методи резервування ресурсів сприяють забезпеченню стабільності в умовах випадкових відмов, однак обмежені припущеннями про розподіли часу простоїв та відмов. Використання блокчейну дозволяє підвищити рівень безпеки мережі, проте збільшує затримки у процесах авторизації та розподілу ресурсів.

Перспективи подальших досліджень спрямовані на створення гібридних методів управління, що поєднують можливості штучного інтелекту, машинного навчання та

блокчейн-технологій. Одним із ключових напрямів є розробка глибоких нейронних мереж для адаптивного управління трафіком, які зможуть самонавчатися на основі реальних даних про стан мережі та змінювати стратегії управління в режимі реального часу. Додатково актуальним є питання розробки вдосконалених алгоритмів динамічного розподілу ресурсів, які б базувалися на ймовірнісних моделях та методах нечіткої логіки.

Ще одним перспективним напрямом є інтеграція квантових обчислень для підвищення ефективності алгоритмів маршрутизації, що дозволить суттєво зменшити час обчислень і забезпечити оптимізацію процесів управління в масштабних телекомунікаційних системах. Також варто приділити увагу створенню механізмів прогнозування кібератак на основі аналізу аномалій у трафіку, що дозволить підвищити стійкість гетерогенних мереж у разі зовнішнього втручання.

Таким чином, подальші дослідження мають бути спрямовані на розробку адаптивних багатофакторних підходів до управління мережею, що враховуватимуть змінність навантажень, динаміку мережевої топології та можливі загрози, що дозволить значно покращити стійкість телекомунікаційних систем.

Список використаної літератури

1. Jones, D., & Parker, A. (2022). AI-based predictive maintenance models for network stability in telecommunications. Journal of Telecommunications and Network Management, 35(2), 124-138.

2. Lopez, R., & Rodriguez, M. (2020). Mathematical models for assessing the resilience of heterogeneous networks to cyber-attacks. International Journal of Network Security, 28(4), 215-227.

3. Brown, L., & Smith, J. (2021). SDN-based strategies for dynamic traffic management and network resilience. Journal of Software-Defined Networks, 19(1), 92-104.

4. Quin, T., & Juan, P. (2020). Adaptive algorithms for resource management in dynamic networks. Journal of Network and Systems Management, 28(3), 445-457.

5. Umberg, M., & Gabriel, P. (2019). Game theory approaches for load balancing in heterogeneous communication networks. Journal of Communications and Network Optimization, 11(2), 59-73.

6. Scott, R., & Seville, D. (2021). Blockchain technology for ensuring network reliability in large-scale telecommunications systems. Blockchain and Telecommunications, 5(1), 33-45.

7. Zhebka V., Berkman L., Kriuchkova L., Strelnikova S. Universal Method of Multidimensional Signal Formation for Any Multiplicity of Modulation in 5G Mobile Network / Lecture Notes in Electrical Engineering. 2022, 831, p. 305–321.

8. Жебка В.В., Бондарчук А.П. Захист гетерогенної телекомунікаційної мережі від впливу дестабілізуючих факторів / Телекомунікаційні та інформаційні технології. 2023. – № 1. – С. 4-16.

9. Zhebka V., Anakhov P., Bondarchuk A., Storchak K., Sablina M. Increasing the Reliability of a Heterogeneous Network using Redundant Means and Determining the Statistical Channel Availability Factor / CEUR Workshop Proceedings. 2023, 3421, p. 231–236

10.Ільїн О.Ю., Балашова Є.О., Чепур М.К., Жебка В.В., Корецька В.О. Удосконалення інформаційної технології для підвищення функціональної стійкості мережі за допомогою теорії графів /Телекомунікаційні та інформаційні технології, 2024, 46-53