https://doi.org/10.31891/2307-5732-2026-365-3
УДК 004.056.53(045)

БІЛОУС ВІТАЛІЙ
Вінницький національний технічний університет
https://orcid.org/0009-0001-2350-1583
e-mail: pydev@ukr.net
КАТАЄВ ВІТАЛІЙ
Вінницький національний технічний університет
https://orcid.org/0000-0002-7458-7807
e-mail: kataev@vntu.net
ГУМЕНЮК В'ЯЧЕСЛАВ
Вінницький національний технічний університет
https://orcid.org/0009-0004-0348-7616
e-mail: hvv@vntu.edu.ua
ШЕНДЕРУК ОЛЕГ
Вінницький національний технічний університет
https://orcid.org/0009-0000-5218-4137
e-mail: shenderuk2002@ukr.net

БАГАТОРІВНЕВА ПРОКСІ-СЕРВЕРНА СИСТЕМА З ДИНАМІЧНИМ КОНТРОЛЕМ МАРШРУТИЗАЦІЇ ТА ГІБРИДНИМ СТОХАСТИЧНИМ ПЕРЕМІШУВАННЯМ МАРШРУТІВ

У статті описано підхід до побудови багаторівневої проксі-системи з динамічним маршрутизаційним контролем, котра орієнтована на підвищення рівня захищеності інформаційних ресурсів та оптимізацію керування мережевим трафіком. Запропонована авторами архітектура ґрунтується на ієрархічній організації проксі-серверів, у межах якої кожен рівень виконує спеціалізовані функції. Зокрема, реалізується первинна фільтрація з'єднань, поглиблений аналіз безпеки, кешування даних, контроль доступу та фінальна маршрутизація. Такий підхід забезпечує поетапну обробку мережевих запитів, підвищує надійність системи та сприяє її масштабованості за умов зростання навантаження.

Особливу увагу приділено моделі динамічної маршрутизації, що реалізується на основі гібридного стохастичного алгоритму. Запропонований алгоритм поєднує ймовірнісний вибір маршрутів із детермінованим аналізом історичних характеристик трафіку та стану мережі. Стохастичний компонент дозволяє знизити передбачуваність маршрутів і мінімізувати ризик локальних перевантажень, тоді як детермінований складник забезпечує стабільність функціонування та підвищує ефективність використання мережевих ресурсів.

Алгоритм враховує поточні параметри мережі, зокрема затримки, пропускну здатність і рівень завантаженості серверів, та здійснює динамічне коригування вагових коефіцієнтів маршрутів у режимі реального часу. Це забезпечує адаптивне балансування навантаження та автоматичне перенаправлення трафіку у разі виникнення перевантажень або змін топології мережі.

Запропонований підхід підвищує стійкість багаторівневих проксі-систем до мережевих атак і забезпечує стабільну передачу даних в умовах інтенсивного та змінного трафіку. Отримані результати свідчать про доцільність використання гібридних стохастичних методів маршрутизації в сучасних інформаційних мережах.

Ключові слова: *багаторівнева проксі-система; динамічна маршрутизація; гібридний стохастичний алгоритм; балансування мережевого трафіку; інформаційна безпека; адаптивні мережі.*

.

BILOUS VITALII, KATAIEV VITALII, HUMENIUK VIACHESLAV, SHENDERUK OLEG
Vinnytsia National Technical University

MULTI-LEVEL PROXY SERVER SYSTEM WITH DYNAMIC ROUTING CONTROL AND HYBRID STOCHASTIC ROUTE SHUFFLING

The article considers an approach to designing a multi-tiered proxy system with dynamic routing control, aimed at enhancing information resource security and optimizing network traffic management. The proposed architecture is based on a hierarchical organization of proxy servers, where each tier performs specialized functions. Specifically, it implements initial connection filtering, deep security analysis, data caching, access control, and final routing. This approach provides phased processing of network requests, increases system reliability, and promotes its scalability under conditions of increasing load.Particular attention is paid to the dynamic routing model, which is implemented based on a hybrid stochastic algorithm. The proposed algorithm combines probabilistic route selection with deterministic analysis of historical traffic characteristics and network status. The stochastic component allows reducing the predictability of routes and minimizing the risk of local overloads, while the deterministic component ensures stable operation and increases the efficiency of using network resources.

The algorithm takes into account current network parameters, including latency, bandwidth, and server load, and dynamically adjusts route weights in real time. This provides adaptive load balancing and automatic traffic redirection in the event of overloads or changes in network topology.

The proposed approach increases the resistance of multi-level proxy systems to network attacks and ensures stable data transmission in conditions of intensive and variable traffic. The results obtained indicate the feasibility of using hybrid stochastic routing methods in modern information networks.

Keywords: *multi-level proxy system; dynamic routing; hybrid stochastic algorithm; network traffic balancing; information security; adaptive networks.*

Стаття надійшла до редакції / Received 11.02.2026
Прийнята до друку / Accepted 11.03.2026
Опубліковано / Published 28.05.2026

Постановка проблеми у загальному вигляді
та її зв'язок із важливими науковими чи практичними завданнями

Стрімкий розвиток інформаційних технологій та зростання обсягів мережевого трафіку зумовлюють підвищені вимоги до ефективності й надійності сучасних комп'ютерних мереж. Одночасно з цим ускладнюється характер мережевих атак, зокрема атак типу DDoS, цільових атак на інфраструктурні вузли та спроб несанкціонованого доступу до інформаційних ресурсів. За таких умов традиційні підходи до організації мережевої безпеки та статичні алгоритми маршрутизації виявляються недостатньо адаптивними, оскільки не враховують динамічні зміни стану мережі та рівень завантаженості її компонентів.

Особливо актуальною є проблема забезпечення захищеної та стабільної передачі даних у багаторівневих проксі-системах, які широко застосовуються для фільтрації трафіку, контролю доступу та оптимізації взаємодії між користувачами й сервісами. Використання фіксованих маршрутів у таких системах призводить до локальних перевантажень, зниження продуктивності та підвищує вразливість до цільових атак, що негативно впливає на загальний рівень інформаційної безпеки.

У зв'язку з цим виникає науково-практичне завдання розробки адаптивних методів динамічної маршрутизації, здатних забезпечити ефективне балансування мережевого трафіку, підвищити стійкість системи до атак і оптимізувати використання мережевих ресурсів. Розв'язання зазначеної проблеми має важливе значення для проєктування сучасних захищених мережевих інфраструктур, орієнтованих на роботу в умовах інтенсивного та змінного трафіку.

Аналіз досліджень та публікацій

Протягом тривалого часу проводяться інтенсивні наукові дослідження, орієнтовані на підвищення рівня безпеки інформаційних систем, зокрема на вдосконалення механізмів захисту комп'ютерних мереж.

Аналіз сучасних наукових досліджень і нормативних документів свідчить, що маршрутизаційний контроль є одним із ключових механізмів підвищення захищеності мереж інформаційних систем. Особливу увагу в публікаціях після 2020 року приділено захисту міждоменної маршрутизації, зокрема протоколу BGP, який залишається критично вразливим до атак типу перехоплення маршрутів, витоку префіксів та підміни маршрутної інформації.

Значна частина робіт зосереджена на криптографічному захисті маршрутизації. У стандарті BGPsec запропоновано механізм перевірки цілісності AS-шляху з використанням цифрових підписів, що дозволяє забезпечити достовірність маршрутних оголошень та унеможливити їх несанкціоновану модифікацію. Подальший розвиток цього підходу пов'язаний із впровадженням інфраструктури RPKI та механізмів валідації походження маршрутів (Route Origin Validation), які дозволяють перевіряти відповідність оголошених префіксів авторизованим джерелам [1], [2].

Окремий напрям досліджень стосується управління політиками маршрутизації та фільтрації маршрутів. У роботах і стандартах зазначається, що застосування списків дозволених префіксів, фільтрації AS-path та обмеження маршрутних політик є ефективним засобом зниження ризику як навмисних атак, так і конфігураційних помилок [3]. У звітах європейських експертних органів підкреслюється, що відсутність базових механізмів фільтрації залишається однією з основних причин масштабних інцидентів маршрутизації в Інтернеті [4].

Важливу роль у забезпеченні безпеки відіграє також захист BGP-сесій. Запропоновані в сучасних стандартах механізми, зокрема TCP-AO, спрямовані на захист транспортного рівня обміну маршрутною інформацією та запобігання атакам типу підміни або відмови в обслуговуванні [5]. Це дозволяє підвищити стабільність маршрутизації та зменшити ймовірність порушення роботи мережі.

У низці досліджень акцент зроблено на моніторингу та виявленні аномалій маршрутизації. Аналіз змін у топології маршрутів, нетипових AS-шляхів або раптових змін префіксів дозволяє своєчасно виявляти атаки та мінімізувати їх наслідки [6]. Подальший розвиток цього підходу пов'язаний із застосуванням методів машинного та глибокого навчання, які дають змогу автоматизувати процес аналізу великих обсягів маршрутних даних і підвищити точність виявлення складних атак [7] , [8].

Окремо в сучасній літературі розглядаються архітектурні підходи до маршрутизаційного контролю, зокрема використання програмно-керованих мереж (SDN). Централізований контроль маршрутів на основі SDN-контролерів дозволяє оперативно впроваджувати політики безпеки, ізолювати небезпечні маршрути та підвищувати керованість мережевої інфраструктури [9], [10].

Таким чином, аналіз досліджень і публікацій показує, що сучасні підходи до підвищення захищеності мереж інформаційних систем ґрунтуються на поєднанні криптографічного захисту маршрутизації, валідації походження маршрутів, ефективних політик і фільтрації, захисту BGP-сесій, моніторингу аномалій та використанні інтелектуальних і програмно-керованих механізмів контролю. Комплексне застосування цих методів забезпечує підвищення стійкості мереж до сучасних маршрутних атак.

Попри значний обсяг наукових напрацювань у цій сфері, сучасні кіберзагрози характеризуються високим рівнем складності та різноманіттям методів атак, що дозволяє зловмисникам обходити наявні засоби захисту. У таких умовах система інформаційної безпеки повинна володіти адаптивністю та здатністю оперативно реагувати на зміни загрозового середовища шляхом застосування більш ефективних і гнучких механізмів протидії. У зв'язку з цим у даній роботі пропонується підвищення рівня захищеності інформаційних систем, зокрема комп'ютерних мереж, за рахунок використання сукупності взаємопов'язаних проксі-серверів із динамічною маршрутизацією та гібридним стохастичним перемішуванням маршрутів.

Формулювання цілей статті

Метою роботи є створення комплексного підходу, заснованого на застосуванні групи взаємодіючих проксі-серверів із механізмами динамічної маршрутизації та гібридного стохастичного перемішування маршрутів, що спрямований на підвищення рівня захищеності комп'ютерних мереж інформаційних систем.

Виклад основного матеріалу

Запропонована багаторівнева архітектура проксі-серверів із механізмами динамічного маршрутизаційного контролю являє собою інтегроване рішення для підвищення рівня захисту інформаційних ресурсів і оптимізації керування мережевим трафіком. Архітектура системи, представлена на діаграмі (рис. 1) є логічно послідовною, відповідає класичним моделям secure proxy / service chaining, сумісна з сучасними підходами Zero Trust / defense-in-depth і охоплює декілька ієрархічних рівнів проксі-серверів, кожен з яких виконує визначені функції, зокрема фільтрацію, аналіз, маршрутизацію, кешування та контроль доступу. Такий підхід забезпечує стійкість до високих навантажень, підвищує захищеність і загальну надійність функціонування системи.

Згідно з діаграмою, багаторівнева організація проксі-серверів забезпечує послідовну обробку мережевого трафіку на кожному етапі, що дозволяє адаптуватися до динамічних змін мережевого середовища, реалізувати ефективне балансування навантаження та підтримувати високу продуктивність.

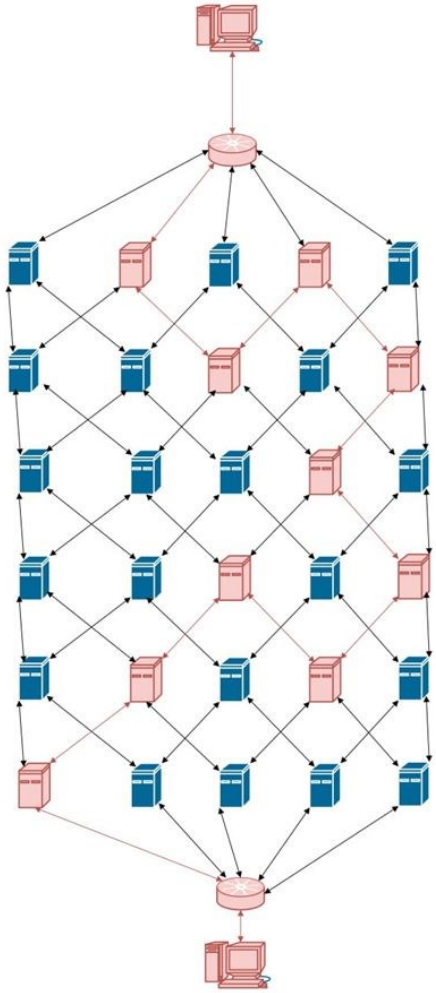

Рис. 1. Діаграма динамічної маршрутизації з використанням гібридного підходу

На початковому етапі обробки трафіку функціонує вхідний вузол, який приймає всі зовнішні мережеві запити. Його основними завданнями є виконання первинного аналізу з'єднань, зокрема перевірка IP-адрес, типів використовуваних протоколів, заголовків пакетів і джерел запитів. Така перевірка дає змогу своєчасно ідентифікувати потенційно загрозливі або небажані з'єднання, зменшуючи ймовірність проникнення атак на ранньому етапі. Крім того, вхідний вузол здійснює розподіл трафіку між проксі-серверами першого рівня з метою оптимізації навантаження.

Після проходження вхідного вузла запити передаються на перший рівень проксі-серверів, призначений для поглибленої фільтрації та аналізу безпеки. Цей рівень складається з декількох паралельно працюючих серверів, що забезпечує високу пропускну здатність системи і дозволяє впровадити горизонтальне масштабування для зменшення latency через послідовне проходження рівнів. На даному етапі застосовуються засоби міжмережевого екранування та системи виявлення вторгнень, які здійснюють аналіз мережевих потоків у режимі реального часу з метою виявлення аномальної поведінки. Реалізація таких механізмів дозволяє ефективно протидіяти атакам типу DDoS, фішинговим загрозам і поширенню шкідливого вмісту.

Запити, які успішно пройшли первинну перевірку, надходять на другий рівень проксі-серверів, що відповідає за кешування та оптимізацію доступу до ресурсів. Кешування часто використовуваних даних сприяє зменшенню навантаження на мережу та скороченню часу відповіді. Як показано на діаграмі, сервери цього рівня мають зв'язки з попередніми та наступними компонентами системи, що забезпечує гнучке керування потоками трафіку та динамічний вибір маршрутів передачі даних.

На третьому рівні проксі-серверів реалізуються механізми контролю доступу та автентифікації користувачів. Кожен запит перевіряється з використанням багатофакторних методів автентифікації, після чого визначається роль користувача і відповідні права доступу до ресурсів. Такий підхід дозволяє запобігти несанкціонованому доступу до конфіденційної інформації та забезпечує дотримання встановлених політик інформаційної безпеки.

Завершальним етапом обробки трафіку є вихідний вузол, який здійснює фінальну маршрутизацію та контроль цілісності передаваних даних. Вихідний вузол об'єднує оброблений трафік і забезпечує його безпечну передачу до кінцевих адресатів, одночасно виконуючи журналювання запитів для подальшого аналізу та аудиту.

Динамічний маршрутизаційний контроль реалізується на всіх рівнях системи із застосуванням стохастичних алгоритмів маршрутизації, що враховують поточний стан мережі, рівень завантаженості серверів та історичні характеристики трафіку. Це дає змогу адаптивно обирати оптимальні маршрути передачі даних і автоматично перенаправляти трафік у разі перевантаження окремих ділянок мережі, зберігаючи стабільність і ефективність роботи системи.

Запропонована модель динамічної маршрутизації ґрунтується на гібридному стохастичному алгоритмі, який забезпечує здатність проксі-системи оперативно адаптуватись до змін мережевого середовища та сприяє раціональному розподілу трафіку. Основним завданням моделі є визначення найбільш ефективного шляху передавання даних між вузлами з урахуванням поточного стану мережі, рівня завантаженості серверних ресурсів і вимог до інформаційної безпеки.

Реалізація моделі базується на поєднанні стохастичних і детермінованих підходів до вибору маршрутів. Стохастична складова передбачає імовірнісний вибір одного з допустимих маршрутів, що дає змогу знизити ризик локальних перевантажень і забезпечити балансування навантаження. Водночас детермінований компонент використовує накопичені статистичні дані про характеристики трафіку та стан мережі, що сприяє зменшенню флуктуацій у роботі системи та підвищенню її стабільності.

Структурна схема відображає багаторівневу архітектуру вузлів, у межах якої кожен сервер має декілька альтернативних маршрутів передавання даних. Така організація дозволяє вузлам у режимі реального часу обирати оптимальний напрямок з урахуванням поточного навантаження та затримок у мережі. Сервери кожного рівня здійснюють вибір наступного вузла на основі аналізу актуального стану мережі; у разі виникнення перевантаження на окремому маршруті трафік автоматично перенаправляється на менш завантажені канали.

Запропонований алгоритм гібридного стохастичного перемішування маршрутів створений на основі аналізу ключових обмежень і недоліків сучасних механізмів, які виконують маршрутизацію в багаторівневих проксі-серверних системах.

Основні проблеми, на подолання яких спрямовано даний підхід, охоплюють такі аспекти:

- обмежена адаптивність статичних алгоритмів маршрутизації, що спираються на фіксовані правила або таблиці маршрутів і не враховують динамічні зміни, які відбуваються в стані мережі. Це призводить до неефективного використання ресурсів і локальних перевантажень окремих вузлів;

- уразливість стабільних маршрутів до цільових атак. У традиційних багаторівневих архітектурах зловмисники можуть ідентифікувати постійні шляхи передавання даних і використовувати їх для організації атак, зокрема типу DDoS. Застосування гібридного стохастичного підходу з динамічною зміною маршрутів знижує передбачуваність їх використання та підвищує рівень захищеності;

- актуальною є задача балансування навантаження в умовах інтенсивного трафіку. Запропонований алгоритм враховує завантаженість серверів в реальному часі і коригує ймовірності вибору маршрутів. Це забезпечує рівномірний розподіл потоків даних;

- сучасні адаптивні методи часто характеризуються високими вимогами до обчислювальних ресурсів. Алгоритм використовує поєднання стохастичних механізмів з обмеженою складністю обчислень, що робить його використання доцільним, особливо, в ресурсно обмежених середовищах.

В основу алгоритму покладено низку принципів:

- вибір шляху передавання даних здійснюється не за детермінованою схемою, а на основі імовірнісної моделі, у межах якої кожному можливому маршруту призначається ваговий коефіцієнт. Такий підхід зменшує передбачуваність структури трафіку та сприяє підвищенню стійкості системи до мережевих атак;

- під час формування маршрутів ураховуються поточні експлуатаційні характеристики мережі, зокрема рівень навантаження серверних вузлів і показники затримки. На основі цих даних імовірності вибору маршрутів коригуються в режимі реального часу. Це дозволяє забезпечити більш рівномірний розподіл трафіку та зростання продуктивності системи загалом;

- алгоритм використовує аналіз історичних даних щодо використання маршрутів для прогнозування їх ефективності завдяки проведенню їх лцінювання. Це дає змогу обмежити повторне застосування маршрутів, які асоціюються з підвищеними затримками або перевантаженням мережевих ресурсів.

Таким чином, алгоритм забезпечує динамічне керування маршрутами в багаторівневих проксі-системах. Його основною метою є формування механізму, здатного враховувати поточний стан мережі, уникаючи перевантажених каналів виконувати рівномірне розподілення трафіку, підтримувати стабільність пропускної здатності при високих навантаженнях. Поєднання стохастичних методів вибору маршрутів із детермінованим аналізом історичних даних дозволяє одночасно забезпечити випадковість і контроль ефективності передавання.

Наведено структуру основних компонентів алгоритму та описано етапи його функціонування, що дає змогу глибше зрозуміти процес динамічної маршрутизації (рис. 2). Особливу увагу приділено механізмам коригування маршрутів у режимі реального часу. Оновлення ймовірнісних ваг маршрутів відбувається відповідно до поточних мережевих умов, що дозволяє проксі-серверам оперативно реагувати на перевантаження або зміни топології. Завдяки цьому система демонструє підвищену стійкість до раптових стрибків навантаження та забезпечує надійну передачу даних за умов інтенсивної мережевої активності.

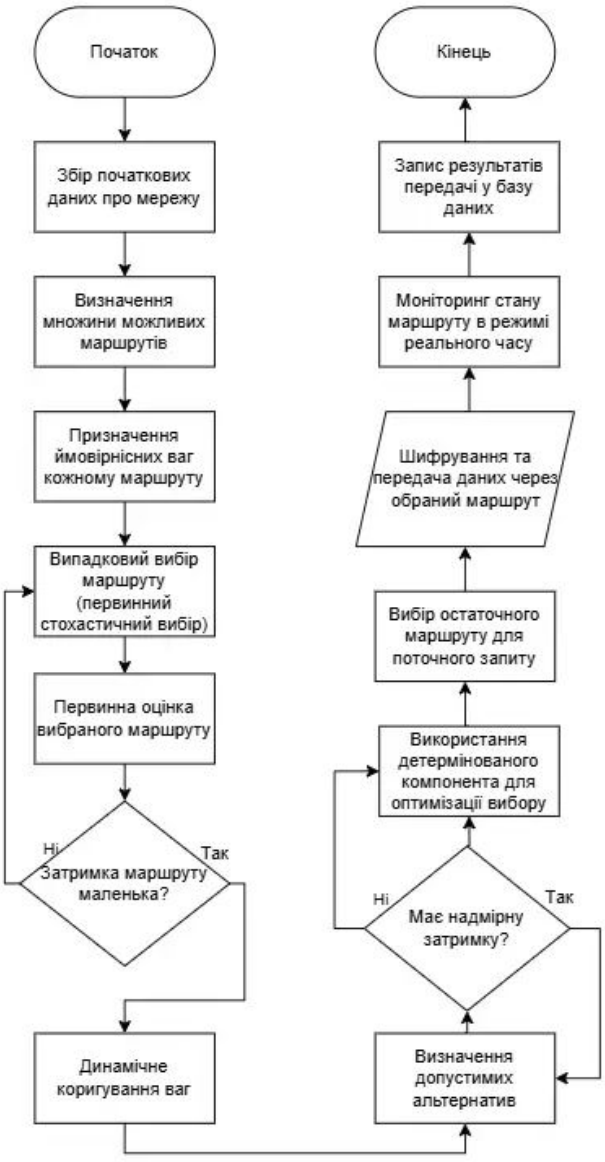

Рис. 2. Схема алгоритму гібридного стохастичного перемішування маршрутів

Алгоритм реалізується за такою послідовністю кроків.

Крок 1: Збір метрик про стан мережі.

На початковому етапі відбувається збір відомостей про актуальні параметри функціонування мережі, зокрема значення затримок на окремих маршрутах, інтенсивність трафіку, доступну пропускну спроможність, а також історичні показники завантаження кожного маршруту. Отримана інформація використовується для подальшого аналітичного опрацювання та визначення найбільш доцільного маршруту обслуговування кожного запиту.

Крок 2: Формування множини всіх допустимих маршрутів.

Система здійснює пошук усіх потенційних шляхів передавання даних від вихідного до цільового вузла з урахуванням наявної інфраструктури проксі-серверів. Кожен маршрут описується набором параметрів, зокрема кількістю проміжних вузлів, прогнозованою затримкою та рівнем пропускної здатності. Отримані

характеристики використовуються для формування множини допустимих маршрутів, що надалі слугує основою для процедури вибору оптимального шляху.

Крок 3: Формування ймовірнісних ваг для кожного з маршрутів.

Кожному допустимому маршруту надається ймовірнісна вага, що визначається на основі проаналізованих показників. Зокрема, маршрути з нижчими значеннями затримки та більшою пропускною здатністю отримують підвищену ймовірність вибору. Застосування такого підходу забезпечує побудову початкової системи пріоритетів для всіх маршрутів.

Крок 4: Стохастичний вибір маршруту (первинна фаза).

З урахуванням попередньо визначених ймовірнісних ваг система здійснює випадкову селекцію маршруту. Запровадження стохастичного механізму формує контрольований рівень випадковості, що запобігає систематичному використанню одного й того самого шляху передавання даних та зменшує ймовірність його перевантаження. Такий підхід сприяє більш рівномірному розподілу мережевого трафіку між доступними маршрутами.

Крок 5: Початкова оцінка обраного маршруту.

Після визначення маршруту система здійснює його початковий аналіз з метою перевірки відповідності заданим критеріям. У разі, якщо рівень затримки або ступінь завантаженості обраного маршруту перевищують допустимі порогові значення, система ініціює процедуру повторного вибору маршруту.

Крок 6: Оцінювання затримки маршруту.

У разі перевищення затримкою маршруту допустимого рівня алгоритм повертається до кроку 4. Якщо ж значення затримки є незначним, виконується перехід до наступного етапу.

Крок 7: Динамічне коригування вагових коефіцієнтів.

З урахуванням інформації про актуальний стан мережі система здійснює оновлення ймовірнісних коефіцієнтів для кожного маршруту. У разі виявлення ознак перевантаження окремого маршруту його вага зменшується, що відповідно скорочує ймовірність його подальшого вибору. Такий механізм динамічного коригування забезпечує в реальному часі більш ефективну оптимізацію маршрутизації.

Крок 8: Формування набору допустимих альтернатив.

У разі, якщо вибраний маршрут характеризується перевищенням рівня завантаженості або значними затримками, система здійснює відбір альтернативних маршрутів із тієї самої множини. Такий підхід дозволяє виконувати перенаправлення трафіку на менш навантажені шляхи, що сприяє підтриманню стабільної роботи та належного рівня продуктивності системи.

Крок 9: Оцінювання наявності затримки.

У разі виявлення затримки алгоритм повертається до попереднього етапу коригування маршруту (крок 8). За відсутності затримок процес переходить до наступного кроку алгоритму.

Крок 10: Залучення детермінованого компонента для оптимального вибору.

Алгоритм, користуючись детермінованим компонентом, здійснює аналіз накопичених історичних даних щодо раніше використаних маршрутів і на цій основі визначає найбільш ефективні варіанти. Зокрема, маршрути, які стабільно демонстрували мінімальні затримки, отримують підвищений пріоритет.

Крок 11: Формування остаточного маршруту.

Остаточний вибір маршруту для поточного запиту виконується з урахуванням результатів стохастичного відбору, механізмів динамічного налаштування ваг та детермінованого аналізу накопичених показників. Обраний маршрут характеризується найвищою ймовірністю забезпечення ефективної передачі даних, де затримки і навантаження будуть мінімальними.

Крок 12: Шифрування та передавання даних обраним маршрутом.

Передавання інформації здійснюється через визначений маршрут із застосуванням криптографічного захисту. Для забезпечення конфіденційності та цілісності даних використовуються протоколи SSL/TLS, що гарантують безпечну взаємодію між проксі-серверами завдяки шифруванню даних при передачі.

Крок 13: Моніторинг параметрів маршруту.

При передачі даних система відстежує основні характеристики маршруту, зокрема затримку, рівень навантаження та стабільність з’єднання. У випадку виявлення ознак перевантаження здійснюється оперативне коригування маршруту.

Крок 14: Збереження результатів передавання у базі даних.

Всі зібрані параметри маршруту, включаючи показники затримки, пропускної здатності та надійності, фіксуються в базі даних для подальшого використання.

Крок 15: Оцінювання ефективності обраного маршруту.

Виконується аналіз результативності використаного маршруту з подальшим коригуванням імовірнісних ваг. Маршрути з високими показниками ефективності отримують підвищені вагові коефіцієнти, тоді як менш результативні будуть знижені.

Розроблений підхід дозволяє досягти компромісу між випадковістю вибору маршрутів і детермінованими рішеннями, забезпечуючи як ефективне балансування навантаження, так і стабільність передавання даних. Стохастичний компонент мінімізує утворення «вузьких місць» у мережі, тоді як детермінований аналіз історичних результатів підвищує точність прогнозування майбутніх навантажень. Така гібридна модель є доцільною для сучасних мереж із динамічними характеристиками трафіку.

Для підвищення надійності алгоритм передбачає безперервний моніторинг активних маршрутів у процесі передавання даних. У разі виявлення перевантаження трафік автоматично перенаправляється альтернативними шляхами, що зменшує затримки та забезпечує безперервність обміну даними. Подібна динамічна маршрутизація є особливо ефективною в мережах зі змінними умовами функціонування.

Динамічний маршрутизаційний контроль реалізується на всіх рівнях системи із застосуванням стохастичних алгоритмів маршрутизації, що враховують поточний стан мережі, рівень завантаженості серверів та історичні характеристики трафіку. Це дає змогу адаптивно обирати оптимальні маршрути передачі даних і автоматично перенаправляти трафік у разі перевантаження окремих ділянок мережі, зберігаючи стабільність і ефективність роботи системи.

Висновки з даного дослідження
і перспективи подальших розвідок у даному напрямі

У роботі представлено підхід до побудови багаторівневої проксі-архітектури з динамічним маршрутизаційним контролем, спрямованої на підвищення рівня інформаційної безпеки та ефективності керування мережевим трафіком. Запропонована система поєднує принципи багаторівневої обробки запитів, гнучкого балансування навантаження та адаптивної маршрутизації, що відповідає сучасним концепціям захисту мереж, зокрема Zero Trust і defense-in-depth.

Архітектура системи базується на ієрархічній організації проксі-серверів, кожен рівень яких виконує чітко визначені функції — від первинної фільтрації та виявлення загроз до кешування, автентифікації користувачів і фінальної маршрутизації трафіку. Така структуризація забезпечує поетапний контроль мережевих потоків, підвищує стійкість системи до атак і дозволяє ефективно масштабувати інфраструктуру за умов зростання навантаження.

Ключовим елементом запропонованого підходу є модель динамічної маршрутизації, що грунтується на гібридному стохастичному алгоритмі. Поєднання ймовірнісного вибору маршрутів із детермінованим аналізом історичних даних дозволяє досягти компромісу між випадковістю та прогнозованістю процесу передавання даних. Це знижує ризик утворення локальних перевантажень, ускладнює ідентифікацію стабільних маршрутів зловмисниками та підвищує загальну стійкість системи до цільових атак.

Запропонований алгоритм забезпечує адаптивне реагування на зміни стану мережі в режимі реального часу, автоматичне перенаправлення трафіку та оптимізацію використання ресурсів без істотного зростання обчислювальної складності. Отримані результати свідчать про доцільність застосування гібридних стохастичних методів у багаторівневих проксі-системах сучасних інформаційних мереж. У подальшому доцільним є виконання експериментального оцінювання запропонованого підходу та його адаптацію до програмно-керованих мереж і хмарних середовищ.

References

1. Mirdita D., Schulmann H., Waidner M. SoK: An Introspective Analysis of RPKI Security. arXiv preprint arXiv:2408.12359v1. 2024. URL: https://doi.org/10.48550/arXiv.2408.12359

2. Schulmann H., Zhao S. Learning to identify conflicts in RPKI. arXiv preprint arXiv:2502.03378. 2025. URL: https://doi.org/10.48550/arXiv.2502.03378

3. Kowalski M., Nowak P., Zieliński K. Toward the mutual routing security in wide area networks: A scoping review of current threats and countermeasures. Computer Networks. 2023. URL: https://doi.org/10.1016/j.comnet.2023.109778

4. Reuter A., Birge-Lee H., Chi A. et al. Securing BGP ASAP: ASPA and other post-ROV defenses. Proceedings of the Network and Distributed System Security (NDSS) Symposium. 2025. URL: https://dx.doi.org/10.14722/ndss.2025.240675

5. Cameron Morris C., Herzberg A, Wang B., Secondo S. BGP-iSec: Improved Security of Internet Routing Against Post-ROV Attacks. Network and Distributed System Security (NDSS) Symposium. 2024, URL: https://dx.doi.org/10.14722/ndss.2024.241035

6. Sermpezis P., Kotronis V., Arakadakis K., & Vakali A. Estimating the Impact of BGP Prefix Hijacking. In 2021 IFIP Networking Conference (IFIP Networking). P. 1-10 IEEE. URL: https://doi.org/10.23919/IFIPNetworking52078.2021.9472813

7. Alshamrani A., Myneni S., Chowdhary A., & Huang D. A Survey on Advanced Persistent Threats: Techniques, Solutions, Challenges, and Research Opportunities. In 2019 IEEE Communications Surveys & Tutorials. P. 1851-1877 IEEE. URL: https://doi.org/10.1109/COMST.2019.2891891

8. Shen C., Wang R., Li X., Zhang P., Liu K., Tan L. Border Gateway Protocol Route Leak Detection Technique Based on Graph Features and Machine Learning. Electronics 2024, 13, 4072. URL: https://doi.org/10.3390/electronics13204072

9. Jafarian T., Ghaffari A., Seyfollahi A., Arasteh B. Detecting and mitigating security anomalies in Software-Defined Networking (SDN) using Gradient-Boosted Trees and Floodlight Controller characteristics, Computer Standards & Interfaces, Volume 91, 2025, 103871, ISSN 0920-5489, URL: https://doi.org/10.1016/j.csi.2024.103871

10. Junjie O., Yanai N., Takemura T. APVAS: Reducing memory size of AS_PATH validation by using aggregate signatures. arXiv preprint arXiv.2008.13346. 2020. URL: https://doi.org/10.48550/arXiv.2008.13346