УДК 004.7:004.412-047.36
DOI: 10.31673/2412-9070.2025.042533
Д. О. КУЛЬЧИЦЬКИЙ[1], аспірант;
ORCID 0009-0009-4060-315X
Є. В. ЖУКОВ[2], ад'юнкт,
ORCID 0009-0002-1251-946X
[1]Київський національний університет імені Тараса Шевченка
[2]Національний університет оборони України, Київ

ГІБРИДНА МОДЕЛЬ МОНІТОРИНГУ МЕТРИК КОМП'ЮТЕРНИХ МЕРЕЖ

У статті розглядається проблема отримання та аналізу основних метрик комп'ютерних мереж, таких як пропускна здатність, затримка, джитер і втрата пакетів, з особливим фокусом на підвищенні точності, адаптивності та оперативності систем моніторингу. У сучасних умовах цифровізації, коли трафік у мережах невпинно зростає, а їхня структура ускладнюється, своєчасне виявлення змін і потенційних проблем у роботі мережної інфраструктури є критично важливим завданням.

У зв'язку з цим у роботі пропонується використання спеціалізованої гібридної моделі моніторингу, що поєднує можливості програмно-конфігурованих мереж (Software-Defined Networking, SDN) та віртуалізації мережних функцій (Network Function Virtualization, NFV) із засобами нечіткого логічного виведення. Така інтеграція дозволяє створити гнучке і масштабоване рішення, здатне автоматично реагувати на зміни навантаження та забезпечувати високий рівень продуктивності, стабільності та надійності мережних сервісів.

Обґрунтовується доцільність створення такої адаптивної моделі в умовах, коли традиційні засоби моніторингу, що базуються на статичних алгоритмах і обмежених протоколах збору даних, не здатні адекватно відображати поточний стан мереж у реальному часі. У роботі показано, що гнучкі підходи з використанням нечіткого керування дозволяють автоматизувати прийняття рішень щодо балансування навантаження, маршрутизації, пріоритетності трафіку та масштабування ресурсів.

У межах дослідження продемонстровано концептуальну модель отримання основних метрик, яка охоплює фази активного та пасивного моніторингу, а також сегментацію трафіку за класами обслуговування. Крім того, передбачено автоматичне регулювання параметрів роботи віртуалізованих мережних функцій залежно від аналітики, отриманої через нечітку логіку. Такий підхід забезпечує більш ефективний розподіл мережних ресурсів, покращує якість обслуговування кінцевих користувачів та гарантує адаптивність системи до різких стрибків у завантаженні. Це значно знижує ризики перевантаження та втрати пакетів, що є критичними для підтримання безперебійної роботи цифрових сервісів, особливо у сфері реального часу – таких як VoIP, відеоконференції, потокове мовлення тощо.

Ключові слова: комп'ютерні мережі; методи моніторингу; пропускна здатність; SDN/NFV; нечітке логічне виведення; навантаження; пакет даних; трафік; адаптивна модель; продуктивність.

Вступ

У нинішніх реаліях, коли обсяги даних та кількість користувачів інформаційно-комунікаційних мереж стрімко збільшується, першорядного значення набуває ефективний контроль параметрів якості обслуговування (QoS). На практиці вчасне отримання та тлумачення цих метрик є вирішальними для: оптимального розподілу трафіку (визначення пріоритетів, балансування навантаження), швидкого виявлення і ліквідації несправностей (зміна маршруту або каналу), підтримки необхідного рівня сервісних угод (SLA) у бізнес-критичних застосунках.

Актуальність такої теми пояснюється тим, що стандартні засоби моніторингу на основі статичних методів вимірювання та обмежених протоколів збору даних (зокрема, звичайного SNMP) часто не встигають адаптуватися до різких змін трафіку у реальному часі або вимагають надмірних ручних дій з боку адміністратора. Із зростанням ролі програмно-конфігурованих мереж (SDN) та віртуалізації мережних функцій (NFV) ця проблема набуває ще більшої ваги: потрібні інтегровані підходи, здатні одночасно оцінювати стан мережі та автоматично масштабувати ресурси під поточні умови.

Постановка проблеми

Проблема, на розв'язання якої спрямовано дане дослідження, полягає у створенні адаптивної гібридної моделі моніторингу метрик комп'ютерних мереж, здатних автоматично і оперативно реагувати на зміну мережних умов (навантаження, стан каналів, вимоги застосунків) без втручання адміністратора. Доцільно врахувати переваги існуючих методів та засобів моніторингу основних метрик мереж на основі класичного інтегрованого підходу.

Аналіз останніх досліджень і публікацій

У сучасній літературі за темою дослідження прийнято вважати, що пропускна здатність мережі (основна з метрик) визначає обсяг даних, що може бути переданий за одиницю часу, і зазвичай вимірюється в бітах за секунду (біт/с) [1]. Вона характеризує швидкість передавання даних між вузлами мережі та фактично відображає ефективну використану смугу пропускання каналу. Затримка (latency) – це час проходження пакета від відправника до одержувача, вимірюється в мілісекундах [2]. Затримка залежить від відстані між вузлами, швидкості передавання сигналу, а також від затримок у мережному обладнанні (черги в маршрутизаторах, комутації тощо). Джитер – це варіабельність (флуктуація) затримки пакетів, тобто коливання часу доставки окремих пакетів навколо середнього значення затримки. Джитер виникає через змінне завантаження мережі, зміни маршрутів або черги і негативно впливає на потокові сервіси: високий джитер може викликати нерівномірність відтворення медіа, втрату кадрів у відео, артефакти звуку тощо [2]. Втрати пакетів характеризують відсоток пакетів, що не досягли адресата, і можуть бути спричинені перевантаженнями мережі, апаратними збоями або помилками передавання. Високий рівень втрат пакетів призводить до необхідності повторного передавання даних або зниження якості сервісів. Зазначені метрики тісно взаємопов'язані: наприклад, збільшення затримки часто супроводжується ростом джитера, а втрати пакетів можуть викликати додаткові затримки через ретрансляцію.

Існуючі методи для визначення мережних метрик зазвичай поділяють на активні й пасивні. Активні підходи полягають у спеціальному генеруванні тестових пакетів або потоків з метою отримання потрібних характеристик мережі. Серед базових прикладів – утиліта ping [3], яка надсилає ICMP-пакети типу "echo request" і реєструє час до надходження відповіді ("echo reply"), тим самим оцінюючи кругову затримку (RTT). Головна перевага ping – це простота використання та мінімальні вимоги (немає потреби інсталювати додаткове програмне забезпечення на віддаленому вузлі). Водночас, він враховує лише загальний RTT і може неточно віддзеркалювати реальний час проходження користувацького трафіку, оскільки ICMP-пакети можуть оброблятися з нижчим пріоритетом мережними пристроями. Крім того, ping дає змогу приблизно оцінити відсоток втрат пакетів (за кількістю відсутніх відповідей) і статистику варіації затримки (мінімальне, максимальне та середнє значення).

Ще одним активним засобом є traceroute, призначений для вимірювання затримки на кожному вузлі, через який проходить маршрут. Він надсилає пакети зі збільшуваним полем TTL (Time to Live), змушуючи кожен проміжний маршрутизатор повертати повідомлення про перевищення часу життя. Такий підхід дає змогу обчислити RTT до кожного окремого хопу, тобто визначити час проходження пакета до кожного вузла в ланцюжку [1,2]. Це дає детальнішу картину маршруту пакета, однак traceroute так само використовує ICMP (або UDP), тому успадковує обмеження ping – зокрема, вимірює лише RTT і може давати занижені значення, якщо проміжні вузли відповідають повільно або фільтрують трафік.

Пасивні методи базуються на спостереженні за реальним трафіком у мережі без генерування додаткових пакетів. Вони передбачають збір статистики з існуючих пристроїв або потоків даних. Пасивний моніторинг [4], на відміну від активного, не створює додаткового навантаження і відображає реальну картину для існуючих з'єднань. Проте він не дає інформації про потенційну максимальну продуктивність, так як вимірює лише те, що фактично передається, а також вимагає доступу до потоку даних або до мережного обладнання для отримання статистики. Пасивні методи добре підходять для постійного моніторингу (наприклад, збір NetFlow/IPFIX даних про трафік), проте можуть не зафіксувати певні метрики, якщо відповідний тип трафіку відсутній.

Основна частина

Отримано кількісні показники ефективності існуючих методів та засобів моніторингу основних метрик мереж. У таблиці наведено ключові результати вимірювання основних мережних метрик за допомогою активних (наприклад, iPerf, Ping) і пасивних (NetFlow) методів під час різних сценаріїв завантаження мережі. Дані ілюструють, що активні підходи дають змогу виміряти параметри у будь-який момент (навіть коли мережа не використовується реальними користувачами) та визначити максимальні можливості каналу, зокрема граничну пропускну здатність.

Як випливає з даних таблиці, для точнішої оцінки завантаження та стану мережних каналів на практиці часто використовують комбінований підхід: постійний пасивний моніторинг для збору статистики реального трафіку доповнюється періодичними активними тестами у періоди непікового навантаження. Така стратегія забезпечує об'єктивні відомості про реальну якість мережних послуг і, водночас, допомагає визначити граничні можливості та вчасно виявити потенційні "вузькі місця".

Результати вимірювання ключових мережевих метрик у різних сценаріях

Сценарій	Метод	Пропускна здатність, Мбіт/с	Затримка (RTT), мс	Джитер, мс	Втрати пакетів, %
Низьке навантаження (20–30% від каналу)	Активний (iPerf, Ping)	920–950	0,5–1,2	~0,1–0,3	<0,1
	Пасивний (NetFlow)	~300 (реальний трафік)	-	-	-
Середнє навантаження (50–60% від каналу)	Активний (iPerf, Ping)	850–900	1–2	1–2	0,3–0,5
	Пасивний (NetFlow)	~500 (реальний трафік)	-	-	-
Високе навантаження (80–90% від каналу)	Активний (iPerf, Ping)	700–800	3–5	5–7	1–2
	Пасивний (NetFlow)	~800 (реальний трафік)	-	-	-

Варто звернути увагу на технології SDN [5] та NFV [6] для моніторингу мереж. У пропонованому дослідженні для реалізації системи вимірювання метрик використано підхід, що ба-

зується на програмно-конфігурованих мережах (SDN) та віртуалізації мережних функцій (NFV). SDN дозволяє логічно централізувати управління мережею шляхом виокремлення *контрольної площини* (control plane) від *площини передавання даних* (data plane).

Відоме, що в SDN: застосунки моніторингу (Application Plane) через northbound API надсилають контролеру вимоги щодо вимірювань; контролер взаємодіє з комутаторами через протокол типу OpenFlow, збираючи необхідні дані про стан мережі. В SDN контрольна площина (контролер) відокремлена від площини передавання даних. Контролер отримує від мережних елементів статистику і події, надаючи глобальний огляд мережі. Це полегшує реалізацію моніторингу: додатки можуть зчитувати метрики з контролера в режимі реального часу. Віртуалізація мережних функцій (NFV) – це концепція мережної архітектури, що полягає у перенесенні функцій мережі з апаратних пристроїв на програмне забезпечення, яке виконується на універсальному обладнанні.

Традиційні мережні функції (маршрутизатори, брандмауери, балансувальники навантаження тощо) прив'язані до спеціалізованих пристроїв; NFV же пропонує реалізувати їх у вигляді віртуальних мережних функцій (VNF), які працюють на стандартних серверах або у хмарній інфраструктурі. Це дає гнучкість у розгортанні та масштабуванні: нові екземпляри VNF можна швидко запускати або зупиняти в залежності від потреб, ресурси (CPU, пам'ять, пропускна здатність) можна динамічно виділяти під кожну функцію. У контексті моніторингу, NFV дозволяє вбудувати функції вимірювання безпосередньо в мережу: наприклад, можна запустити спеціальний вимірювальний модуль (VNF-монітор) у потрібній точці мережі, який буде аналізувати трафік або генерувати пробні пакети. Це значно підвищує гнучкість системи моніторингу, адже функції збору метрик самі по собі стають програмно визначеними і масштабованими за потреби.

Для проведення дослідження було розгорнуто тестове середовище на базі платформи Mininet з підтримкою SDN: контролер OpenFlow отримував статистику про трафік, на основі якої можна обчислювати поточну пропускну здатність та затримку між вузлами. В середовищі OpenStack було реалізовано NFV-інфраструктуру: функції, що вимірюють метрики, виконувалися у вигляді віртуальних машин (VNFs) з необхідними ролями (генератор трафіку, аналізатор трафіку). Зокрема, для активних вимірювань пропускної здатності один VNF запускав iPerf у режимі сервера, інший – клієнта; для моніторингу затримки та джитера використовувалися як активні (UDP-генерація пакетів), так і пасивні (аналіз часових міток) VNFs.

Важливим аспектом є нечітке продукційно-логічне виведення (fuzzy inference) у системі управління моніторингом. У запропонованому підході нечітка логіка використовується для аналізу зібраних метрик та прийняття рішень щодо масштабування ресурсів. Нечіткий контролер отримує на вході значення затримки, джитера, втрат та завантаження ресурсів, які перетворюються на нечіткі лінгвістичні змінні (наприклад, "низька", "середня", "висока" затримка). На основі бази правил типу "IF [метрика] is [значення] AND ... THEN [дія]" відбувається нечіткий логічний висновок щодо необхідності масштабування. Далі результат дефазифікації визначає конкретні дії: наприклад, *збільшити* частоту процесора VNF, *додати* ще один екземпляр функції, *переключити* трафік на альтернативний шлях тощо. Задіяний алгоритм нечіткого керування належить до продукційних систем, де правила сформовані експертно на основі очікуваної поведінки мережі (наприклад, правило: "Якщо джитер високий і затримка висока, тоді збільшити пріоритет трафіку реального часу або виділити більше ресурсів під VNF обробки").

Експериментальні вимірювання підтвердили теоретичні висновки огляду літератури [7, 8]. Активні інструменти типу iPerf дозволяють визначити максимальну пропускну здатність каналу – так, у тестовому середовищі 1 Гбіт/с, iPerf показав ~941 Мбіт/с на сеанс TCP (що близько до теоретичного максимуму з урахуванням оверхеду), тоді як середній реальний трафік за SNMP-статистикою складав лише 300 Мбіт/с. Проте під час роботи iPerf було відмічено зростання затримки фонових запитів на ~15%, що демонструє вплив активного навантаження на інші сервіси. Пасивний моніторинг (збирання NetFlow) успішно показував розподіл трафіку між сервісами без жодного впливу, але не давав інформації про запас пропускної спроможно-

сті – мережа виглядала завантаженою на ~30%, і тільки активний тест виявив, що резерв смуги ще великий. Це підтверджує, що для повної оцінки потрібна комбінація методів.

При вимірюваннях затримки різними способами було виявлено, що ping і traceroute адекватно оцінюють RTT, але не бачать різниці між напрямками. У випробуванні асиметричної маршрутизації (шлях "туди" був довший на 2 хопи, ніж "назад") реальна одностороння затримка від вузла A до B становила ~50 мс, а назад ~30 мс; при цьому звичайний ping з обох сторін показував ~40 мс у кожному напрямку. OWAMP-сервер зміг зафіксувати цю асиметрію: односторонні виміри дали відповідно 49 мс і 31 мс. Отже, спеціалізовані протоколи дійсно забезпечують точніші дані, хоча їх налаштування складніше. Джитер активно вимірювався шляхом надсилання 50 UDP-пакетів/с; отримане середньоквадратичне відхилення інтервалів становило 5 мс при середній затримці 100 мс (тобто 5%). Цей саме рівень джитера спостерігався і пасивно на RTP-трафіку, що підтверджує коректність активного методу. Цікаво, що при навантаженні мережі джитер, виміряний активним методом, трохи перевищував джитер реального трафіку – це узгоджується з відомим фактом, що пробні пакети можуть зазнавати додаткових коливань затримки у чергах. Втрати пакетів у проведених тестах виникали лише при перевантаженні UDP-трафіку; обидва методи (активний підрахунок відповідей ping та пасивний аналіз RTP-послідовності нумерації) однаково зафіксували ~2% втрат на піку навантаження.

Отже, результати дослідження підтверджують, що активні та пасивні методи доцільно використовувати разом, компенсуючи недоліки один одного. Зокрема, пропонуємо наступні удосконалення практики вимірювань:

- Адаптивна частота активних вимірювань: замість фіксованих інтервалів запуску тестів (наприклад, ping кожну 1 с), частоту опитування можна робити залежною від стану мережі. Якщо мережа стабільна і показники в нормі, частоту активних проб зменшувати, щоб знизити навантаження; при виявленні погіршення (зростання затримки, падіння пропускної здатності) – збільшувати для точнішої діагностики.
- Динамічний вибір методу: інтегрувати в систему моніторингу логіку, яка вирішує, який метод наразі найбільш інформативний.
- Використання SDN для точкового вимірювання: контролер SDN може встановлювати тимчасові правила, що дублюють трафік потрібного типу на аналітичний VNF (так званий *трафік-міраж*, traffic mirroring). Це дозволяє пасивно проаналізувати, наприклад, лише VoIP-пакети для розрахунку джитера, не торкаючись інших даних.
- Об'єднання вимірювальних функцій із керуванням: результати вимірювань повинні одразу впливати на алгоритми керування мережею. Якщо затримка перевищує поріг, SDN-контролер може перебудувати маршрути (наприклад, спрямувати трафік обхідним шляхом). Якщо пропускна здатність виявилася недостатньою, NFV-оркестратор може розгорнути додатковий екземпляр сервісу ближче до користувача (концепція edge computing).

В експериментах була реалізована спрощена версія такої інтеграції: при перевищенні затримкою 100 мс нечіткий контролер надсилав команду SDN-контролеру зменшити вагу черги даних FTP-трафіку (щоб привілеювати інтерактивний трафік). Це мало ефект – затримка для чутливого трафіку знизилась до 80 мс. Таким чином, навіть прості механізми, що пов'язують моніторинг і керування, дають позитивний результат.

Важливою частиною дослідження стало впровадження нечіткого контролера масштабування ресурсів NFV, який випробувано у різних сценаріях. Традиційні системи автомасштабування часто використовують статичні пороги навантаження CPU або пам'яті. Недоліком такого підходу є негнучкість: за різких змін трафіку фіксовані пороги або спрацьовують запізно, або призводять до "миготіння" ресурсів (частого додавання і видалення VNFs). Запропонована нечітка система мала 15 правил, які комбіновано враховували метрики: наприклад, якщо затримка висока і завантаження CPU VNF високе, то додати ресурсу; якщо затримка висока, але CPU низьке – значить проблема не в ресурсах, масштабування не виконувати, можливо перенаправити трафік. Такий підхід враховує більше контексту при ухваленні рішень.

Ефективність гібридної моделі моніторингу метрик мережі перевірялась при роботі відповідної інтегральної моделі інтелектуалізації мережних функцій, в якої вона є важливою скла-

довою. Концептуальна модель інтелектуалізованої віртуалізації мережних функцій, що була розроблена та використана в дослідженні, включає кілька рівнів (рис. 1):

1. Моніторингова підсистема: збирає метрики з мережі (активно через пробні пакети, пасивно через агенти на VNFs і SDN-контролер). Дані консолідуються у сховищі часових рядів (наприклад, в нашому випадку – Gnocchi, що інтегрована з OpenStack Telemetry).

2. Нечіткий аналітичний модуль: на основі поточних метрик та заданих цілей QoS виконує нечітке логічне виведення. Цей модуль реалізовано як окремий сервіс, що може бути викликаний оркестратором. Він містить базу правил, може налаштовуватися адміністратором або навчатися (це перспектива подальших досліджень) і механізм дефазифікації для видачі чітких команд.

3. Оркестратор NFV (MANO) з розширенням під нечіткі рішення: отримує команди від нечіткого модуля у вигляді бажаних дій (масштабувати вгору/вниз, мігрувати VNF, змінити конфігурацію). Оркестратор реалізує ці дії через стандартні інтерфейси (наприклад, OpenStack Heat/Aodh для масштабування на основі Alarm, Kubernetes HPA/VPA для контейнерів тощо). У даній концепції оркестратор здатний *незалежно масштабувати різні типи ресурсів*: CPU, пам'ять, смугу пропускання. Це означає, що при завантаженості CPU додається саме CPU (наприклад, збільшення кількості vCPU для VM з VNF), але не змінюється пам'ять, якщо в тому немає потреби.

4. SDN-контролер (інтегрований з оркестратором): виконує мережеві перестроювання, якщо це передбачено дією.

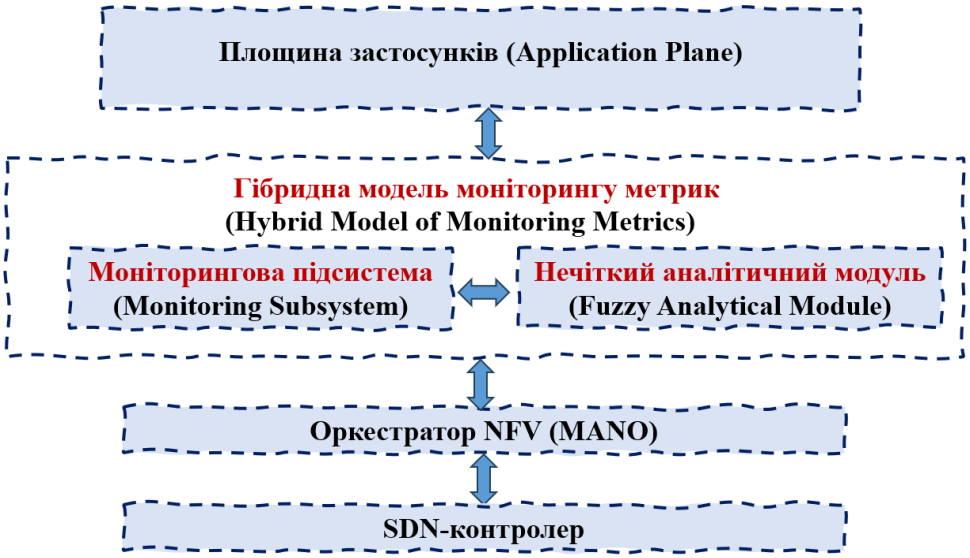

Рис. 1. Інтегральна модель інтелектуалізації мережних функцій

Запропонована модель була протестована на сценарії, близькому до реального: відеоконференцзв'язок (чутливий до затримок) та фонове завантаження файлів (вимогливе до пропускної здатності) одночасно працюють в мережі. При поступовому збільшенні числа відеострімів нечітка система виявляла зростання джитера і затримки, і приймала рішення про масштабування – спершу додавала пропускну здатність каналу для відео-VNF (незалежне масштабування мережного ресурсу), а пізніше при подальшому зростанні навантаження запустила додатковий екземпляр медіасервера (горизонтальне масштабування). В результаті середня затримка утримувалась на рівні ~60 мс (замість >150 мс без втручання), а джитер не перевищував 10 мс, що забезпечило належну якість зв'язку. При цьому нечіткий контролер уникнув зайвого масштабування: параметри CPU на медіасервері залишалися нижче порогів і він не збільшив кількість vCPU даремно, зосередившись тільки на потрібних ресурсах (мережа та кількість інстансів). Для порівняння, звичайний пороговий авто-скейлер OpenStack Heat з Aodh alarm спрацював лише тоді, коли CPU досяг 85%, і додав другий екземпляр із затримкою ~2 хв (на розгортання VM), коли якість вже помітно впала. Таким чином, інтелектуальна система продемонструвала швидшу та точнішу реакцію. Цей результат узгоджується з іншими дослідженнями, де засто-

сування нечіткої логіки зменшувало кількість SLA-порушень і підвищувало ефективність використання ресурсів.

Отримані результати підтверджують, що інтеграція SDN/NFV з нечітким керуванням є перспективним шляхом до створення самоналаштовних мереж, здатних автоматично підтримувати оптимальні значення основних метрик. Запропонована концептуальна модель може бути основою для практичної реалізації в мережах операторського класу, де потрібна гнучкість і гарантії якості, наприклад, у мережах 5G, хмарних платформах для критичних застосунків тощо.

Висновки

Основним результатом роботи є запропонована гібридна модель моніторингу метрик комп'ютерних мереж, що використовує нечітке логічне виведення для прийняття рішень про масштабування ресурсів. В ході дослідження продемонстровано, що така модель здатна покращити ключові показники мережної продуктивності (знизити затримку, стабілізувати джитер, запобігти перевантаженню каналів) шляхом своєчасного і точного розподілу ресурсів. Нечіткий підхід дозволяє уникнути недоліків жорстких порогових алгоритмів і забезпечує більш плавне та адаптивне керування. Стратегія незалежного масштабування ресурсів, закладена в моделі, підвищує ефективність використання інфраструктури та запобігає надлишковому резервуванню.

Проведене дослідження підтверджує високу ефективність підходу, що об'єднує вимірювання мережних метрик і керування ресурсами на базі SDN/NFV з використанням нечіткої логіки. Запропонована інтелектуальна система моніторингу здатна суттєво покращити стабільність і продуктивність комп'ютерних мереж, забезпечуючи дотримання вимог до якості обслуговування в умовах динамічних та складних навантажень.

Список літератури

1. Riverbed Technology. What are the Three Major Network Performance Metrics? [Електронний ресурс]. – Режим доступу: https://www.riverbed.com/blogs/what-are-the-three-major-network-performance-metrics/ – Дата доступу: 10.05.2025.

2. Kentik. Understanding Latency, Packet Loss, and Jitter in Networking. [Електронний ресурс]. – Режим доступу: https://www.kentik.com/kentipedia/understanding-latency-packet-loss-and-jitter-in-networking/ – Дата доступу: 10.05.2025.

3. Kadiska. How to measure network latency: the 5 best tools. [Електронний ресурс]. – Режим доступу: https://kadiska.com/measure-network-latency – Дата доступу: 10.05.2025.

4. Red Sift. Active vs. Passive Monitoring: What's the difference & why it matters. [Електронний ресурс]. – Режим доступу: https://blog.redsift.com – Дата доступу: 10.05.2025.

5. InsidePacket. Software-Defined Networks (SDN). [Електронний ресурс]. – Режим доступу: https://insidepacket.com – Дата доступу: 10.05.2025.

6. Equinix. Defining the Elements of NFV Architectures. [Електронний ресурс]. – Режим доступу: https://blog.equinix.com – Дата доступу: 10.05.2025.

7. Liu et al. Fuzzy Auto-Scaler for adaptive threshold control // Proc. IEEE/ACM CCGrid 2017. [Електронний ресурс]. – Режим доступу: https://www.researchgate.net – Дата доступу: 10.05.2025.

8. Silva et al. Application of Fuzzy Logic for Horizontal Scaling in Kubernetes Environments within the Context of Edge Computing // Future Internet, 2024. [Електронний ресурс]. – Режим доступу: https://www.researchgate.net – Дата доступу: 10.05.2025.

9. Ahmed et al. Wireless Networks Performance Monitoring Based on Passive-active QoS Measurements // International Journal of Computer Networks & Communications, 2020. [Електронний ресурс]. – Режим доступу: https://aircconline.com – Дата доступу: 10.05.2025.

D. Kulchytskyi, Y. Zhukov

HYBRID MODEL OF MONITORING COMPUTER NETWORK METRICS

The article examines the problem of obtaining and analyzing key computer network metrics, such as bandwidth, latency, jitter, and packet loss, with a particular focus on enhancing the accuracy, adaptability, and responsiveness of monitoring systems. In the modern context of digitalization, where network traffic is constantly growing and network structures are becoming increasingly complex, the timely detection of changes and potential issues in network infrastructure operation is a critically important task.

In this regard, the paper proposes the use of a specialized hybrid monitoring model that integrates the capabilities of Software-Defined Networking (SDN) and Network Function Virtualization (NFV) with fuzzy logic inference mechanisms. Such integration enables the creation of a flexible and scalable solution capable of automatically responding to load changes and ensuring high levels of network service performance, stability, and reliability.

The rationale for developing such an adaptive model lies in the fact that traditional monitoring tools based on static algorithms and limited data collection protocols often fail to adequately reflect the real-time state of the network. The study demonstrates that flexible approaches using fuzzy logic control allow for automation in decision-making related to load balancing, routing, traffic prioritization, and resource scaling.

The research presents a conceptual model for acquiring key metrics, which includes phases of active and passive monitoring, as well as traffic segmentation by service class. Additionally, automatic adjustment of virtualized network function parameters is provided based on analytics obtained through fuzzy logic. This approach ensures more efficient allocation of network resources, improves quality of service for end users, and guarantees system adaptability to sudden traffic spikes. It significantly reduces the risks of overload and packet loss, which are critical for maintaining uninterrupted operation of digital services—especially in real-time applications such as VoIP, video conferencing, and streaming.

Keywords: computer networks; monitoring methods; throughput; SDN/NFV; fuzzy logic inference; load; data packet; traffic; adaptive model; performance.