

*Голові разової спеціалізованої
вченої ради
Національного університету
«Львівська політехніка»
д. т. н., проф. Кирику М.І.*

ВІДГУК ОФІЦІЙНОГО ОПОНЕНТА

на дисертаційну роботу Пелеха Назара Володимировича
"Підвищення ефективності функціонування хмарних систем для інформаційно-комунікаційних сервісно-орієнтованих мереж",
подану до захисту на здобуття наукового ступеня доктора філософії
за спеціальністю 172 «Телекомунікації та радіотехніка»
в галузі знань 17 «Електроніка та телекомунікації»

1. Актуальність теми дисертації

Стрімкий розвиток мережевих технологій ставить все нові і нові вимоги перед провайдерами телекомунікацій. Взаємодія між різними технологіями передавання інформації не лише ускладнює її сприйняття, але й потребує удосконалення механізмів балансування трафіку, спричиняє значне збільшення кількості процесів оброблення даних та, як наслідок, завантажує мережні вузли. Дотримання вимог щодо якості обслуговування, зокрема дотримання умов SLA ставить додаткові рамки перед надавачами сервісів. Для них постає завдання модернізувати наявну телекомунікаційну систему з мінімізацією витрат на її удосконалення. Виходом стають інфокомунікаційні мережі на основі сервісно-орієнтованих архітектур, які базуються на інтеграції відомих методів передавання інформаційних потоків у рамках концепції композитних сервісів, що виражається в здатності забезпечити якісну підтримку процесів, що відбуваються як у мережному середовищі, так і у центрах обробки даних. Така інтеграція стає особливо актуальною в еру цифровізації, оскільки підприємства продовжують прискорювати свою цифрову трансформацію, а вимоги до мережі постійно змінюються. Розподіленість сервісів, сукупна взаємодія між приватними та гібридними хмарними системами спонукають провайдерів, як основних надавачів такого роду послуг, безперервно адаптуватися під швидкі зміни до потреб користувачів.

Проте, різноманітність запитів на надання таких сервісів та їх обслуговування ускладнюють не тільки процеси оброблення інформації мережними вузлами, а й спричиняють нерівномірність завантаження каналів зв'язку. З одного боку, завдяки функції віртуалізації, що дозволяє абстрагуватися від апаратних засобів до точки, де програмні стеки можуть бути розгорнуті і задіяні, не будучи прив'язаними до конкретного фізичного сервера, можна частково вирішити цю проблему; з іншого – створення динамічних центрів обробки даних (ЦОД), де сервери забезпечують пул ресурсів, які будуть використовуватися для надання сервісів і де додатки для обчислення, зберігання і, відповідно, мережні ресурси, змінюватимуться динамічно з метою задоволення потреб –

вносить додаткові часові затримки в процес надання сервісу. Особливо критичним це стає в моменти міграцій сервісів та/або даних, коли система керування проводить реконфігурацію структури мережі та здійснює пошук нових оптимальних маршрутів. Нерівномірність завантаження каналів зв'язку потребує нових підходів до процесів розподілу обчислювальних ресурсів, забезпечуючи при цьому високу масштабованість, енергоефективність, швидкодію, гнучкість, низьку операційну складність та ресурсоемність.

Управління будь якою мережевою інфраструктурою зводиться до проблеми підвищення захищеності даних від несанкціонованого доступу до них. Для цього необхідні певні механізми моніторингу стану кожної системи, яка буде аналізувати можливі проблеми, що можуть виникати під час роботи, і запускати системи захисту або повідомляти адміністраторів про можливу загрозу. Тому розроблення моделі підвищення ефективності функціонування хмарних систем при їх інтеграції у сучасні інформаційно-комунікаційні сервісно-орієнтовані мережі з одночасним інтелектуальним виявленням кіберзагроз в умовах різкого зростання розмірів та динаміки потоків стає необхідним в умовах сьогодення. У зв'язку з цим тематика дисертаційної роботи Пелеха Назара Володимировича, яка присвячена підвищенню ефективності функціонування хмарних систем при їх інтеграції у сучасні інформаційно-комунікаційні сервісно-орієнтовані мережі шляхом розроблення методу кластеризації серверних вузлів, удосконалення моделей оцінки ефективності функціонування хмарних систем в умовах обслуговування групових потоків запитів та розвитку систем інтелектуального виявлення мережевих атак для надання інформаційно-комунікаційних сервісів кінцевим користувачам є актуальною.

2. Загальна характеристика роботи

Дисертаційна робота Пелеха Назара Володимировича стосується завдання розроблення нових та удосконалення існуючих моделей та методів підвищення ефективності функціонування хмарних систем в умовах їх інтеграції у мережі провайдерів послуг, в яких основний акцент відводиться на знаходженні балансу між кількістю віртуальних машин, що здійснюють обслуговування групових потоків запитів та кількістю запитів, що вже знаходяться на обслуговуванні в системі, з урахуванням географічної близькості вузлів між собою та моніторингу доступних програмно-апаратних та телекомунікаційних ресурсів та інтелектуального виявлення DDoS атак на веб сервіси, що надаються користувачам у таких інформаційно-комунікаційних сервісно-орієнтованих мережах.

Робота складається зі вступу, чотирьох розділів, висновків, списку використаних джерел та двох додатків. Загальний обсяг роботи складає 170 сторінок друкарського тексту, із них: 7 сторінок вступу, 115 сторінок основного тексту, 65 рисунків, 6 таблиць, список використаних джерел зі 120 найменувань, додаток на 4 сторінках.

У вступі подано загальну характеристику дисертаційної роботи, обґрунтовано всі процедурні положення та подано зв'язок роботи з науковими програмами, планами, темами.

У першому розділі розглянуто основні принципи побудови, підходи та особливості інтеграції хмарних систем у інформаційно-комунікаційні мережі провайдерів

телекомунікацій. Проведено аналіз основних вимог щодо якості надання послуг в сервісно-орієнтованих телекомунікаційних мережах. Констатовано, що під'єднання хмарної інфраструктури займає досить тривалий час та потребує відповідної кваліфікації системних адміністраторів, а реалізація та налаштування систем управління такими компонентами мережі є складним процесом. Аналіз основних підходів, щодо інтеграції хмарних систем, показав необхідність врахування ступеню віртуалізації та їх величини, особливостей обробки потоків запитів, при оцінці ефективності функціонування хмарних систем. Встановлено, що динамічна конфігурація мережі за допомогою контролера мережі без оцінки ефективності функціонування апаратного і програмного забезпечення мережевих пристроїв привела до того, що сьогодні більшість провайдерів телекомунікаційних мереж частково впроваджують цю технологію, але при цьому виникають складнощі з управлінням інтегрованою мережевою інфраструктурою. У зв'язку з цим проблема зводиться не лише до підвищення ефективності функціонування інформаційно-комунікаційних сервісно-орієнтованих мереж, а й підвищення захищеності даних від несанкціонованого доступу, що є особливо актуальним на сьогоднішній день.

У другому розділі роботи удосконалено математичну модель оцінки ефективності функціонування хмарних систем в умовах групового надходження запитів від користувачів. Вона враховує можливість обслуговування при груповому надходженні запитів та розподілений час обслуговування запитів, що дасть змогу в моменти пікових навантажень не порушувати працездатність мережі з високим ступенем віртуалізації за рахунок зменшення тривалості очікування запитів в черзі та дозволяє знаходити баланс між кількістю віртуальних машин, що здійснюють обслуговування групових потоків запитів та кількістю запитів, що вже знаходяться на обслуговуванні в системі. У розділі доведено адекватність моделі оцінки ефективності функціонування хмарних систем в умовах обслуговування групових потоків запитів. Удосконалено метод кластеризації вузлів хмарних систем в умовах обслуговування групових потоків запитів, що дозволить підвищити ефективність функціонування хмарних систем, в яких одночасне обслуговування групових потоків запитів забезпечує велика кількість віртуальних машин. В основі удосконаленого методу лежить процес групування в кластер пулу віртуальних машин, які будуть використовуватися під обслуговування чітко визначеного групового потоку із врахуванням географічної близькості вузлів між собою та моніторингу доступних програмно-апаратних та телекомунікаційних ресурсів, що дасть змогу підвищити життєвий цикл фізичних машин за рахунок збільшення рівня залишкової енергії. Розроблено алгоритм кластеризації і вибору головного вузла кластера, особливістю якого є визначення головного вузла кластера із врахуванням центральності по діаграмах Вороного, правил нечіткої логіки та моніторингу параметрів вузлів. Ухвалення рішення про вибір головного вузла здійснюється методами нечіткої логіки за допомогою правила Мамдані та центру ваги, а також із врахуванням достатніх програмно-апаратних ресурсів для подальшого функціонування вузла в якості центроїда кластеру.

У третьому розділі проведено моделювання та дослідження ефективності запропонованого алгоритму кластеризації на основі комплексного критерію ефективності: тривалості пошуку маршрутів, споживання енергії в мережі і життєвий цикл мережі. Завдяки реалізації розробленого методу кластеризації вузлів хмарних систем вдалося досягти зменшення тривалості пошуку маршруту між довільною парою віртуалізованих

вузлів в межах одного кластера у 1,3 рази. Завдяки визначенню головного вузла кластера із врахуванням центральності по діаграмах Вороного, правил нечіткої логіки та моніторингу параметрів вузлів вдалося досягти зменшення тривалості пошуку маршруту між довільною парою віртуалізованих вузлів, які обслуговують один і той же груповий потік у 2,5 рази. Доведено, що розроблений алгоритм зменшує споживання енергії на 45% і продовжує життєвий цикл мережі на 8% в порівнянні з відомими алгоритмами. Для доведення ефективності запропонованих методів та моделей підвищення ефективності функціонування хмарних систем у розділі проведено дослідження на основі розгорнутої моделі інформаційно-комунікаційної сервісно-орієнтованої мережі з використанням CDN серверів як PaaS сервісу. В результаті дослідження запропонованих рішень досягнуто зменшення тривалості завантаження статичного контенту з кеш-серверів у порівнянні із завантаженням з базового сервера в 4 рази. Використання пропускної здатності каналу при доступі до контенту із віддалених серверів зростає до 700 Кбіт/с. Дослідження показали, що контент не повинен кешуватись на POP або HTTP-клієнтом. Лише в одному випадку на 0,05 с. кешована версія запитуваного ресурсу не була знайдена на найближчому до клієнта POP.

У четвертому розділі розроблено інтегровану архітектуру системи інтелектуального виявлення DDoS атак у інформаційно-комунікаційних мережах. Основною особливістю архітектури є реалізація Підсистеми аналізу лог файлів, яка є елементом інтегрованої системи управління, що аналізує потенційні проблеми і запускає запобіжні механізми, або може повідомляти системних адміністраторів про порушення безпеки мережі. В основі даної Підсистеми лежить комплексний підхід до аналізу логів, особливістю якого є проведення паралельного дослідження ентропійних властивостей потоків запитів. Для його реалізації використовується два методи: структурований та неструктурований аналіз даних. Неструктурований метод аналізу даних реалізує алгоритм знаходження ентропії записів, створених за певний проміжок часу та аналізу останніх значень ентропії для всіх файлів журналу в системі. Структурований метод аналізу даних базується на визначенні метрики поведінки трафіку використовуючи підхід Кульбака — Лейблера для виявлення аномалій потоку за часом тривалості сесії. Проведено моделювання та дослідження ефективності інтеграції архітектури інтелектуального виявлення DDoS атак на основі розробленої імітаційної моделі інформаційно-комунікаційної сервісно-орієнтованої мережі. Дослідження проводилося на основі розробленої імітаційної моделі інформаційно-комунікаційної сервісно-орієнтованої мережі на базі НТЦ МТ Національного університету «Львівська політехніка» на одній із підмереж, яка була ізольована від всієї мережі. Модель базується на взаємодії між клієнтами і сервером, на якому розміщено веб сервіс, а також програмного аналогу SDN контролеру. Доведено, що використання комплексного підходу до аналізу лог журналів із використанням як структурованого так і неструктурованого аналізу службових файлів дало змогу відстежувати як наявні загрози, так і прогнозувати атаки на мережу в цілому за рахунок використання елемента машинного навчання як окремої підсистеми інтегрованої архітектури управління мережею. Реалізація машинного навчання дозволило класифікувати клієнтів по категоріям на основі значень ентропії та виявляти зловмисника. В результаті використання такого навчання та відповідно постійного моніторингу сесій, SDN контролер блокуватиме IP домени, з яких лише розпочинаються DDoS атаки.

В додатку до роботи надано акти впровадження її результатів.

3. Ступінь обґрунтованості наукових положень, висновків, рекомендацій, наданих в дисертації, їхня достовірність

Обґрунтованість і достовірність наукових положень, висновків та рекомендацій, сформульованих у дисертаційній роботі Пелеха Назара Володимировича, впливають з наступного:

- достовірність отриманих дисертантом науково-практичних результатів засвідчено актами впровадження;
- отримані нові результати гармонійно доповнюють відомі;
- матеріали дисертації обговорювались на Міжнародних і Всеукраїнських науково-технічних конференціях, які проводилися під егідою IEEE, а також на наукових семінарах та отримали схвальну оцінку.

4. Наукова новизна результатів, отриманих в дисертаційній роботі

У ході розв'язання поставленої наукової задачі здобувачем отримані наступні основні наукові результати:

1. Удосконалено математичну модель оцінки ефективності функціонування хмарних систем в умовах обслуговування групових потоків запитів. Дана модель враховує можливість обслуговування при груповому надходженні запитів та розподілений час обслуговування запитів, що дасть змогу в моменти пікових навантажень не порушувати працездатність мережі з високим ступенем віртуалізації за рахунок зменшення тривалості очікування запитів в черзі.

2. Удосконалено метод кластеризації вузлів хмарних систем в умовах обслуговування групових потоків запитів, який відрізняється від відомих врахуванням правил нечіткої логіки та центральності по діаграмах Вороного для визначення головного вузла кластера. Це дасть змогу зменшити тривалість пошуку маршруту між довільною парою вузлів та підвищити ефективність інтеграції хмарних систем.

3. Вперше запропоновано інтегровану архітектуру системи інтелектуального виявлення DDoS атак у інформаційно-комунікаційних мережах на основі комплексного підходу до аналізу лог журналів із використанням як структурованого так і неструктурованого аналізу службових файлів. Реалізації на практиці запропонованої інтегрованої архітектури системи інтелектуального виявлення атак, дасть змогу відстежувати атаки, які вже почалися, так і прогнозувати атаки на мережу в подальшому.

5. Повнота викладу наукових положень, висновків, рекомендацій в опублікованих працях

За результатами досліджень, які викладені у дисертаційній роботі, опубліковано 12 наукових праць, серед них 3 статті у наукових фахових виданнях України та 1 стаття у науковому періодичному виданні інших держав, що входять до міжнародних науково-метричних баз даних, 1 стаття у науковому періодичному виданні інших держав; 7

публікацій у збірниках тез наукових конференцій (зокрема 6 – у виданнях, які входять до наукометричних баз даних Scopus та Web of Science).

6. Відповідність теми дисертації профілю спеціальності

Дисертація Пелеха Н.В. повністю відповідає стандарту спеціальності 172 «Телекомунікації та радіотехніка».

7. Відсутність порушення академічної доброчесності

Підстав для сумнівів у науковій доброчесності здобувача під час детального ознайомлення з дисертаційною роботою не виявлено. Узгодженість тексту дисертації з науковими працями дисертанта свідчить про відсутність ознак фальсифікації. Проведений аналіз основних ідей та методів дотичних до тематики інших робіт містить відповідні посилання.

8. Важливість та практичне значення одержаних результатів

1. Удосконалений метод кластеризації вузлів хмарних систем в умовах обслуговування групових потоків запитів, дозволяє зменшити тривалість пошуку маршруту між довільною парою віртуалізованих вузлів у 2,5 рази;

2. Розроблений алгоритм вибору головного кластерного вузла з використанням центральності по діаграмах Вороного, правил нечіткої логіки та моніторингу параметрів вузлів, дав змогу зменшити споживання енергії на 45% і продовжити життєвий цикл мережі на 8% та підтримувати якість надання послуг користувачам в умовах обслуговування групових потоків запитів;

3. Удосконалена математична модель оцінки ефективності функціонування хмарних систем дала змогу зменшити тривалість завантаження статичного контенту з кеш-серверів в 4 рази.

4. Розроблена інтегрована архітектура системи інтелектуального виявлення загроз на основі комплексного підходу до аналізу лог журналів із використанням як структурованого так і неструктурованого аналізу службових файлів за рахунок використання елементу машинного навчання як окремої підсистеми інтегрованої архітектури управління мережею, дозволяє проводити інтелектуальне виявлення атак використовуючи інформацію про стан потоку, тривалість сесії та джерела його походження, а також навчити SDN контроллер блокувати «подібні» потоки запитів без втручання системних адміністраторів.

9. Зауваження до дисертаційної роботи

1. Не наведено пояснення стосовно отримання залежності представленої на рисунку 2.3 “Приклад надходження задачі від первісного процесу, вбудованого напів марківського процесу і вбудованого марківського процесу”. Якщо на його основі будується, напів марківський процес, то доцільно було б або вставити посилання на його першоджерело, або детальніше описати принцип його побудови.

2. Для оцінки ефективності функціонування хмарної системи із врахуванням переходів зі стану в стан, що наведена у 2 розділі, необхідно визначити передавальну ймовірнісну матрицю, елементами якої є кількість запитів, що відправляються із системи в проміжку часу між двома прибулими послідовними груповими потоками запиті. Проте, у хмарних системах існує ймовірність, того, що в певний момент часу черга запитів порожня і запити на обслуговування не надходять. Не зрозуміло, яким чином це враховано при побудові матриці переходів, яка представлена формулою 2.21.

3. Не наведено пояснення стосовно отримання залежності представленої формулою 2.37. Які змінні використовуються при визначенні ймовірності вибору головного вузла в кластері?

4. При виборі головного вузла в кластері залишається не зрозумілим, яким чином після процесу дефазифікації здійснюється оцінка параметрів віртуальних машин, які здійснюють обробку запитів із групового потоку. Який елемент мережі проводить таку оцінку? Автором не конкретизовано компонент, який проводить моніторинг вільних програмних та телекомунікаційних ресурсів фізичних або віртуальних машин, що значно ускладнює розуміння суті методу кластеризації.

5. Залежності отримані із середовища моделювання представлені на рис. 3.2-3.4 складні для читання, через надто малий шрифт. Можливо варто винести текст за межі рисунку, щоб покращити його сприйняття та розуміння.

6. При верифікації запропонованих рішень важливим також є питання щодо кількості експериментів, що виконуються: їх недостатня кількість призводить до зниження достовірності отриманих характеристик. Експериментальні результати, які отримані у 4-му розділі були проведені на розробленій імітаційній моделі інформаційно-комунікаційної сервісно-орієнтованої мережі та виконувались одноразово, без вказання похибки самої моделі та доведення її адекватності, тому інформація стосовно отриманих вирашів виглядає неповною.

7. Відсутність веб версії системи аналізу трафіку та виявлення аномалій, що представлено у 4 розділі дисертації, дещо ускладнює її сприйняття.

10. Загальні висновки

На підставі розгляду змісту дисертації, її анотації, праць здобувача, актів впровадження, аналізу ступеня новизни наукових положень та практичної значимості отриманих у роботі результатів, висновків та рекомендацій можна зробити висновок, що дисертаційна робота Пелеха Назара Володимировича є завершеною працею, в якій отримані нові наукові результати, що в сукупності забезпечило розв'язання актуального наукового завдання підвищення ефективності функціонування хмарних систем при їх інтеграції у сучасні інформаційно-комунікаційні сервісно-орієнтовані мережі шляхом розроблення методу кластеризації серверних вузлів, удосконалення моделей оцінки ефективності функціонування хмарних систем в умовах обслуговування групових потоків запитів та розвитку систем інтелектуального виявлення мережевих атак.. Сама робота достатньо повно опублікована та апробована, відповідає «Паспорту» заявленої спеціальності, вимогам наказу МОН України № 40 від 12.01.2017р. «Про затвердження вимог до оформлення дисертації», Порядку присудження ступеня

доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії (Постанова Кабінету Міністрів України від 12 січня 2022 р. № 44), а її автор заслуговує присудження наукового ступеня доктора філософії зі спеціальності 172 «Телекомунікації та радіотехніка».

Офіційний опонент

доктор технічних наук, професор,
професор кафедри інформаційних систем та технологій
Національного технічного університету України
«Київський політехнічний інститут
імені Ігоря Сікорського»

Богдан Жураковський

Підпис д.т.н., професора Богдана Жураковського засвідчую.

Вчений секретар

Національного технічного університету України
«Київський політехнічний Інститут
імені Ігоря Сікорського»,
кандидат технічних наук, доцент



Валерія Холявко