Голові разової спеціалізованої вченої ради
Національного університету «Львівська політехніка»
доктору технічних наук, професору
Кирику М.І.

ВІДГУК
офіційного опонента

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

1. Актуальність теми дисертації

В умовах стрімкого зростання обсягів мережного трафіку, зміни його структури та необхідності підтримки великої кількості користувачів обґрунтованою стає поява нових архітектурних підходів щодо побудови телекомунікаційних мереж, які складаються з високопродуктивних кластерів для оброблення великих обсягів даних і гнучких масштабованих віртуалізованих середовищ для надання хмарних сервісів. Одним із сучасних підходів до вирішення описуваних проблем є використання сервіс-орієнтованої архітектури (SOA). Підвищення рівня апаратної потужності, пришвидшення обробки і аналізу службової інформації, ефективне використання пропускної здатності каналів зв’язку вимагають від інженерів розробки нових методів та алгоритмів, які б задовольняли вимоги користувачів. Здавалося б сучасні технології, такі як хмарні обчислення, мають на меті задовольнити доступ до великої кількості обчислювальних потужностей, адже функціонують в умовах агрегації ресурсів та надання єдиного системного підходу по їх управлінню.

З появою великих потоків даних необхідні не лише нові підходи по удосконаленню, зберіганню та управлінню, а й до їх аналізу і, як наслідок обробки службових даних, оскільки її кількість збільшується в геометричній прогресії. Крім того, враховуючи такі фактори, як витрати на міграцію хмари, різні базові технології, що обслуговують аварійне відновлення даних та відповідають за безпеку та розгортання сервісів, одна хмара сама по собі не може задовольнити всі вимоги не лише користувачів, а й провайдерів. Тому, багато провайдерів створюють інтегровані мережі, які дають змогу поєднувати усі переваги хмарних систем задовільняючи постійно зростаючі вимоги для кінцевих користувачів та бізнес підприємств.

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, адже при інтеграції хмарних систем у наявні вже інформаційно-комунікаційні сервісно-орієнтовані мережі провайдерам слід враховувати, що підприємства переважно використовують частину хмарних сервісів.

При цьому, основними вимогами є інтеграція та підключення наявної хмарної системи із забезпеченням такої ж гнучкість та швидкості надання сервісів. Для такого випадку, провайдер повинен забезпечити постійно діючий високошвидкісний канал передавання, який фактично буде активним протягом 24 годин на добу 7 днів на тиждень. Однак надання такого каналу передавання потребує від провайдера високоефективного планування та перерозподілу своїх потоків даних. З іншого боку, слід пам’ятати, що для відкриття фактично наскрізних каналів для передавання одному користувачеві, необхідно забезпечувати вимоги корпоративності надання послуг. Налаштування і конфігурація системи управління потоками трафіку потребуватиме великої кількості програмно-апаратних ресурсів провайдера та часу (тижнів або навіть місяців) для відлагодження роботи мережі. Таким чином, оператори повинні оновити наявні інформаційно-комунікаційні сервісно-орієнтовані мережі до інтелектуальних хмарних мереж з інтегрованим плануванням системи управління потоками трафіку та постійно підвищувати ефективність їх функціонування. В паралелі із моніторингом параметрів якості QoS (Quality of Service, якість послуг) необхідно забезпечувати і безпеку та реалізовувати політику конфіденційності даних користувачів, оскільки її реалізація прописану в рамках специфікацій SLA (Service Level Agreement, угода про рівень надання послуг).

Таким чином, перед інженерами, що намагаються забезпечити функціонування таких інтегрованих систем виникає багатокритеріальна задача раціонального вибору та балансування між реалізацією чи розгортанням веб-сервісів, їх наданням і підвищенням захищеності даних від несанкціонованого доступу до них.

У зв'язку з цим, тематика дисертаційної роботи Пелеха Назара Володимировича, яка присвячена розробленню нових методів та моделей підвищення ефективності функціонування хмарних систем при їх інтеграції у сучасні інформаційно-комунікаційні сервісно-орієнтовані мережі та розвитку систем інтелектуального виявлення мережевих атак є досить актуальною.

2. Загальна характеристика роботи

Дисертаційна робота Пелеха Назара Володимировича стосується розв’язання наукового завдання - підвищення ефективності функціонування хмарних систем при їх інтеграції у сучасні інформаційно-комунікаційні сервісно-орієнтовані мережі шляхом удосконалення моделей та методів оцінки ефективності функціонування хмарних систем в умовах обслуговування групових потоків запитів, кластеризації серверних вузлів із

реалізацією інтелектуального мережевого захисту хмарних веб сервісів від кіберзагроз.

Робота складається зі переліку умовних скорочень, вступу, чотирьох розділів, висновків, списку використаних джерел та двох додатків. Обсяг роботи є досить повним і складає 170 сторінок друкарського тексту, із них: 7 сторінок вступу, 115 сторінок основного тексту, 65 рисунків, 6 таблиць, список використаних джерел із 120 найменувань.

У **вступі** подано загальну характеристику дисертаційної роботи, обґрунтовано актуальність теми дисертаційної роботи, сформульовано мету і визначені завдання для її досягнення, наукову новизну та практичне значення отриманих результатів. Наведено дані про впровадження результатів роботи, їх апробацію, публікації та особистий внесок здобувача..

В **першому розділі** проведено аналіз існуючих методів інтеграції хмарних систем у сучасні інформаційно-комунікаційні мережі. Визначено, що попри усі переваги, які підприємства й провайдери отримують при інтеграції хмарних систем, їх ефективність функціонування ускладняється динамічним характером хмарного середовища та різноманітністю запитів користувачів. Встановлено, що під'єднання хмарної інфраструктури займає досить тривалий час і при її реалізації необхідно залучати не лише висококваліфікований персонал, а й затрачати достатньо велику кількість програмно-апаратних засобів. Доведено, що важливе значення при інтеграції хмарних систем відіграє ступінь віртуалізації, тобто число розгорнутих і функціонуючих машин. Достатньо високий ступінь віртуалізації, і відповідно велика кількість запитів, які обслуговують віртуальні машини, може призвести до перевантаження мережі в цілому. Констатовано, що управління інтегрованою мережевою інфраструктурою зводиться до проблеми підвищення захищеності даних від несанкціонованого доступу. Рішенням такого роду проблеми може бути впровадження машинного навчання, особливо в рамках реалізації концепції програмно-конфігурованих дата центрів.

У **другому розділі** роботи викладено основну частину методичної бази досліджень, в якій удосконалено математичну модель оцінки ефективності функціонування хмарних систем в умовах групового надходження запитів від користувачів. Вона базується на двоступеневій техніці апроксимації та забезпечує повний імовірнісний розподіл часу очікування запитів, часу відгуку щодо виконання запитів і кількості запитів у системі. На відмінну від існуючих моделей запропонована 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. Результати перевірки адекватності та результативності роботи моделі оцінки ефективності функціонування хмарних систем в умовах обслуговування групових потоків запитів підтверджують її ефективність та сприяють зменшенню рівня використання ресурсів хмарними провайдерами і як

наслідок забезпечується стабільне функціонування системи. 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. Такий підхід базується на групуванні в кластер пулу віртуальньних 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 ефективність функціонування хмарних систем шляхом збільшення життєвого циклу фізичних машин, особливо в умовах великої кількості віртуальних машин та обслуговування групових потоків запитів.

У **третьому розділі** розроблено імітаційну модель інфокомунікаційної мережі для оцінки ефективності запропонованого методу кластеризації вузлів хмарних систем із застосуванням правил нечіткої логіки та моніторингу параметрів вузлів. Шляхом проведення моделювання вказано на зменшення тривалості пошуку маршруту між довільною парою віртуалізованих вузлів в межах одного кластеру у 1,3 рази, що дає змогу пришвидшити процес надання сервісу кінцевому клієнту із гарантованим рівнем QoS. Порівняльний аналіз та моделювання показують, що розроблений алгоритм кластеризації та вибору головного вузла кластеру зменшує споживання енергії на 45% і продовжує життєвий цикл мережі на 8% в порівнянні з відомими алгоритмами. Ефективності запропонованих методів та моделей підвищення ефективності функціонування хмарних систем доведено на практиці на основі розгорнутої моделі інформаційно-комунікаційної сервісно-орієнтованої мережі з використанням CDN серверів як PaaS сервісу та хмарної архітектури Azure Cloud. Реалізація удосконаленої математичної моделі оцінки ефективності функціонування хмарних систем в умовах групового надходження запитів та методу кластеризації вузлів хмарних систем дала змогу зменшити тривалість завантаження статичного контенту з кеш-серверів (які виступали головними вузлами кластерів, визначеними з використанням алгоритму вибору головного кластерного вузла з використанням центральності по діаграмах Вороного, правил нечіткої логіки та моніторингу параметрів вузлів) у порівняні із завантаженням з базового сервера в 4 рази.

У **четвертому розділі** запропоновано 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, та аналізує потенційні проблеми й запускає запобіжні механізми, або може повідомляти системних адміністраторів про порушення безпеки мережі. Розроблено 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. Інформація отримана в результаті

комплексного аналізу лог журналів дасть змогу виявляти аномалії при поступленні потоків запитів, здійснюючи постійний моніторинг сесій та прописувати правила роботи контролера, який відповідає за управління мережею. Запропоновано неструктурований метод аналізу даних, який реалізує алгоритм знаходження ентропії записів, створених за певний проміжок часу та аналізі останніх значень ентропії для всіх файлів журналу в системі. Розроблено структурований метод аналізу даних, який 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. 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 елементу машинного навчання як окремої підсистеми інтегрованої архітектури управління мережею. В результаті використання такого навчання та відповідно постійного моніторингу сесій, SDN контролер блокуватиме IP домени, з яких лише розпочинаються DDoS атаки

Висновки до дисертації включають узагальнені результати дослідження та рекомендації щодо їх практичного застосування

В додатку до роботи подано 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 підтверджуються коректним використанням теоретичних та експериментальних методів досліджень, зокрема методів математичного моделювання, а також актами впровадження результатів дисертаційних досліджень.

4. Достовірність і новизна наукових положень, висновків і рекомендацій.

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

1. Вперше запропоновано інтегровану архітектуру системи інтелектуального виявлення DDoS атак у інформаційно-комунікаційних мережах на основі комплексного підходу до аналізу лог журналів, яка дає змогу відстежувати як наявні загрози, так і прогнозувати атаки на веб сервіси.

2. Удосконалено математичну модель оцінки ефективності функціонування хмарних систем в умовах обслуговування групових потоків запитів, яка, на відмінну від існуючих, враховує можливість обслуговування

при груповому надходженні запитів та розподілений час обслуговування запитів.

3. 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, що дало змогу зменшити тривалість пошуку маршруту між довільною парою вузлів та підвищити ефективність інтеграції хмарних систем.

5. Практична значимість результатів роботи

Отримані в дисертаційній роботі наукові результати мають практичну цінність та можуть використовуватися на етапі трансформації сучасних інформаційно-комунікаційних сервісно-орієнтованих мереж з метою підвищення ефективності функціонування хмарних систем при їх інтеграції у мережі провайдерів телекомунікацій.

Зокрема:

- реалізація на практиці удосконаленого методу кластеризації вузлів хмарних систем в умовах обслуговування групових потоків запитів, дозволило зменшити тривалість пошуку маршруту між довільною парою віртуалізованих вузлів, які обслуговують один і той же груповий потік у 2,5 рази.
- використання розробленого алгоритму вибору головного кластерного вузла з використанням центральності по діаграмах Вороного, правил нечіткої логіки та моніторингу параметрів вузлів дало 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;
- реалізація удосконаленої математичної моделі оцінки ефективності функціонування хмарних систем, яка на відмінну від існуючих враховує можливість обслуговування при груповому надходженні запитів і розподілений час обслуговування запитів та методу кластеризації вузлів хмарних систем в умовах обслуговування групових потоків запитів дало змогу зменшити тривалість завантаження статичного контенту з кеш-серверів у порівнянні із завантаженням з базового сервера в 4 рази;
- використання комплексного підходу до аналізу лог журналів із використанням як структурованого так і неструктурованого аналізу службових файлів, дозволило виявляти атаки, які вже проводяться на мережі використовуючи інформацію про стан потоку, тривалість сесії та джерела його походження та блокувати «подібні» потоки запитів без втручання системних адміністраторів.

Важливість результатів дисертації для практики підтверджена актами впровадження в телекомунікаційних мережах ТОВ «Аркада-Х» та ТзОВ «МаксіТех»

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

За результатами досліджень, які викладено у дисертаційній роботі, опубліковано 12 наукових праць, серед них 2 статті у закордонних фахових виданнях, що індексуються міжнародними науково-метричними базами, 3 статті у фахових виданнях України за переліком МОН та 7 публікацій у збірниках праць міжнародних і всеукраїнських конференцій.

7. Відповідність теми дисертації профілю спеціальності

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

8. 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.

9. Зауваження до дисертаційної роботи

1. Залишається не до кінця зрозумілим поняття «інформаційно-комунікаційні сервісно-орієнтовані мережі», яке використовує автор у своїх дисертаційних дослідженнях. Як відомо, під поняттям «інформаційно-комунікаційні мережі» розуміють мережі з інтегрованим використанням програмного забезпечення, накопичувальних та аудіовізуальних систем та інформаційних технологій, які дозволяють користувачам створювати, одержувати доступ, зберігати, передавати та змінювати інформацію. Сервісно-орієнтовані мережі це по-суті певний архітектурний і програмний шаблон, який використовується у інформаційно-комунікаційних мережах орієнтованих на надання веб сервісів кінцевим користувачам. У дисертаційній роботі автор нівелює чітко цих два поняття.

2. У другому розділі роботи (формула (2.4)) наведено визначення нормалізованого значення середнього часу обслуговування як функцію залежну від кількості елементів та ступеня віртуалізації відповідно до залежності середнього часу обслуговування від кількості розгорнутих на фізичних машинах віртуальних машин, яка нормалізована за часом обслуговування, отриманого за рахунок роботи фізичних машин як окремого елементу (рис. 2.2). Проте не описано, яким чином відбувається визначення середнього часу обслуговування, тобто мається на увазі, які параметри чи коефіцієнти взято за основу? Аналогічно, не наведено та не роз’яснено, звідки з’явилися відповідні числові значення для досліджуваного параметру?

3. Для дослідження показників ефективності функціонування хмарної системи як функції середнього розміру групового потоку (рис. 2.7) використовується коефіцієнт варіації часу обслуговування запитів. Проте, у дисертаційній роботі не обґрунтовано не лише визначення цього коефіцієнту

та його вплив на показники ефективності, а й вибір значень, які використовувалися при проведені імітаційного моделювання.

4. В процесі моделювання, що наведено у п. 3.1 доведено ефективність запропонованого алгоритму кластеризації на основі комплексного критерію ефективності: тривалості пошуку маршрутів, споживання енергії в мережі і життєвий цикл мережі. Проте його ефективність викликає сумніви, оскільки незрозуміло, який протокол чи алгоритм маршрутизації використовувався для пошуку маршрутів між віртуалізованими вузлами. Що бралося за основу вибору метрики маршруту? Даний нюанс є досить важливим, оскільки від нього напряму залежить чи запропонований алгоритм кластеризації дозволить підвищити ефективність функціонування хмарної системи та як результат зменшити час надання сервісу користувачеві.

5. Залишається не зрозумілим, яким чином реалізовано удосконалену математичну модель оцінки ефективності функціонування хмарних систем в умовах групового надходження запитів на платформі Microsoft Azure. Деталізація її інтеграції дозволить чітко зрозуміти за рахунок чого вдалося зменшити тривалість завантаження статичного контенту з кеш-серверів та чи вливає час розгортання цієї моделі на загальний час надання веб сервісу кінцевому користувачеві.

6. п. 4.3. дисертації, де проведено дослідження ефективності інтеграції архітектури інтелектуального виявлення DDoS атак на основі розробленої імітаційної моделі інформаційно-комунікаційної сервісно-орієнтованої мережі, перенасичений деталізацією процесу та графічною інформацію щодо отриманих результатів. Доцільно було б узагальнити цю інформацію акцентуючи увагу лише на отриманих результатах.

7. Не проведено порівняльного аналізу розробленої системи інтелектуального виявлення DDoS атак із уже існуючими системами, що працюють з використанням Mashine Learning. Це ставить під сумнів перевагу та ефективність розробленої дисертантом системи виявлення кіберзагроз.

Зазначені недоліки не знижують загальної позитивної оцінки дисертаційної роботи.

10. Відповідність дисертації встановленим вимогам

Анотація дисертації ідентично та повністю розкриває зміст дисертаційної роботи, яка, в цілому, відповідає усім вимогам до робіт, що подаються на здобуття наукового ступеня доктора філософії, має завершеність, виконана та оформлена на достатньо високому рівні. Стиль викладення матеріалів досліджень, наукових положень, висновків і рекомендацій забезпечує доступність їх якісного сприйняття.

11. Загальні висновки

1. На підставі розгляду змісту дисертації, 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

«Підвищення ефективності функціонування хмарних систем для інформаційно-комунікаційних сервісно-орієнтованих мереж» є завершеною науковою працею, в якій отримані нові наукові результати, що, в сукупності, забезпечили розв'язання актуального наукового завдання в галузі телекомунікацій та радіотехніки.

2. Дисертаційна робота за змістом та оформленням відповідають установленим вимогам. Результати дисертації достатньо повно опубліковані у фахових наукових виданнях та апробовані на конференціях і семінарах.

3. Дисертація відповідає 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), і може бути розглянута спеціалізованою вченою радою на предмет допуску до захисту на здобуття наукового ступеня доктора філософії за спеціальністю 172 «Телекомунікації та радіотехніка».

ОФІЦІЙНИЙ ОПОНЕНТ
доктор технічних наук, професор,
професор кафедри кібербезпеки
та захисту інформації
Київського національного університету
імені Тараса Шевченка Сергій ТОЛЮПА

Підпис професора С. Толюпи засвідчую
Перший проректор В.С. Ільченко
25.05.22р