

**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ЛЬВІВСЬКА ПОЛІТЕХНІКА»**

Кваліфікаційна наукова
праця на правах рукопису

ДЕМИДОВ ІВАН ВАСИЛЬОВИЧ

УДК 621.391

ДИСЕРТАЦІЯ

Синтез телекомунікаційних сервісних платформ національного масштабу

05.12.02 – телекомунікаційні системи та мережі

(шифр і назва спеціальності)

05 «Технічні науки»

(галузь знань)

Подається на здобуття наукового ступеня
доктора технічних наук

Дисертація містить результати власних досліджень. Використання ідей,
результатів і текстів інших авторів мають посилання на відповідне джерело

(підпис, ініціали та прізвище здобувача)

Науковий консультант –
Климаш Михайло Миколайович,
д.т.н., професор

Ідентичність всіх примірників дисертації

ЗАСВІДЧУЮ:

*В.о. вченого секретаря спеціалізованої
вченої ради*

/А.П. Бондарєв/

Львів – 2017

АНОТАЦІЯ

Демидов І.В. Синтез телекомунікаційних сервісних платформ національного масштабу. - Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня доктора технічних наук за спеціальністю 05.12.02 «Телекомунікаційні системи та мережі» (172 – Телекомунікації та радіотехніка). – Національний університет «Львівська Політехніка» МОН України, Львів, 2017.

Дисертаційну роботу присвячено проблематиці структурно-функціональної сегментації глобальної інформаційної інфраструктури з метою ефективної реалізації національного сегменту телекомунікаційних сервісних платформ за критеріями системної продуктивності, сервісної доступності, а також функціональної стійкості. Враховуючи динаміку розвитку сучасних інфокомунікаційних технологій та еволюцію пов'язаних із ними організаційних і ринкових чинників, нагальну потребу в масштабованості систем надання електронних послуг у всіх галузях народного господарювання України, в умовах впровадження концепцій «Інтернету речей» (IoT) та «повсюдного комп'ютингу», необхідною є адаптація потужностей хмарних мережних систем множини операторів інфокомунікацій під управлінням та в інтересах держави.

В роботі продемонстровано передумови для виникнення протиріччя, оскільки процеси впровадження повсюдного комп'ютингу в умовах неефективного масштабування хмарних телекомунікаційних платформ призводять до потреби у надлишковому споживанні їх ресурсів і обмеження переліку та обсягів завдань оброблення інформації, що можуть розв'язуватись в рамках надання розподілених сервісів.

У дисертаційній роботі представлено розв'язання актуальної наукової проблеми розроблення методологічного забезпечення синтезу телекомунікаційних сервісних платформ національного рівня для оптимального впровадження концепції повсюдного комп'ютингу (розподілених обчислень) із заданими рівнями якості сервісу, продуктивності та функціональної стійкості.

Перший розділ роботи містить огляд літературних джерел за темою дисертації в рамках проведення аналізу методології створення та впровадження розподілених сервісних мережних систем у національному сегменті глобальної інформаційної інфраструктури. Розглянуто особливості еволюції, а також проблематику ефективного управління телекомунікаційними сервісними платформами на основі аналізу сервісно-орієнтованих архітектур різної технологічної реалізації.

Другий розділ роботи присвячено визначенню та дослідженню найбільш ефективних за імовірно-часовими показниками методів підвищення продуктивності сервісних мережних платформ. Ці методи, як було показано в роботі, в основному, ґрунтуються на удосконаленні процесів опрацювання користувачького навантаження засобами мережного рівня, а також на адаптації, відповідно до його розподілу та характеру, коефіцієнтів утилізації мережних ресурсів. На основі запропонованих у розділі теоретичних методів та структурно-математичних моделей показано, що у сучасних розподілених сервісних мережних платформ є значний потенціал для оптимізації за критерієм продуктивності.

У третьому розділі виконано дослідження моделей і методів визначення статистичних характеристик сервісних вузлів телекомунікаційних платформ із використанням інтерфейсів відкритої системної архітектури (OSA) на прикладі Parlay API; запропоновано використовувати метод поліваріантного доступу для збільшення пропускної здатності розподіленої мережної платформи SOA шляхом створення реплікацій веб-сервісів та балансування між ними навантаження. В розділі також проведено визначення та аналіз критеріїв функціональної стійкості сервісних мережних систем, що дозволило визначити загальний критерій ефективності захисту мультисервісних інфокомунікаційних систем в національному сегменті сервісної мережної інфраструктури, крім цього виконано загальний аналіз загроз поширенню даних та функціональній стійкості у мультисервісних інфокомунікаційних системах, які реалізують телекомунікаційну сервісну платформу національного сегменту глобальної

інформаційної інфраструктури. У розділі виконано експериментальне статистичне дослідження мультисервісного навантаження в гетерогенній корпоративній мережній системі з метою аналізу показників його самоподібності для окремих типів трафіку; показано, що основні типи навантаження мають доволі високий ступінь самоподібності; продемонстровано, що завдання оптимального структурно-параметричного синтезу сервісних мережних платформ може бути зведене до завдання вибору їх оптимальних структурних та функціональних параметрів у рамках деякої заданої архітектури виду SOA.

В четвертому розділі роботи проведено дослідження характеристик продуктивності та сервісної доступності телекомунікаційних сервісних платформ у процесі їх структурно-параметричного синтезу, зокрема при масштабуванні; проведено аналіз сучасних підходів до виявлення та запобігання функціональним втручанням у розподілені мережні системи, а також розроблення концепції та моделі мігруючого мережного екрану на основі концепції точок присутності й інформаційної присутності у відкритій функціональній моделі гетерогенної сервісної системи, досліджено стратегії управління процесами міграції ресурсів в гетерогенних сервісних платформах.

У п'ятому розділі проаналізовано принципи оптимізації конвергованих ресурсів мережно-залежних рівнів гетерогенних розподілених сервісних систем, проведено пошук шляхів оптимізації ресурсів множини взаємопоеднаних сервісних мережних платформ. Розглянуто і досліджено запропонований метод та алгоритм наскрізного структурного трасування, що дозволяє оперативне визначення структурних змін, а отже – і відмов мережних елементів, а також флуктуацій обсягів трафіку в телекомунікаційній сервісній платформі.

Шостий розділ роботи присвячений адаптації розробленої у дисертації методології для трансформації телекомунікаційних сервісних платформ з метою їх прикладного застосування в критично важливих інфокомунікаційних системах національного масштабу. Зокрема, запропоновано модифікований

метод обслуговування черг на основі диференціації сервісів у моделі IaaS. У дисертаційній роботі запропоновано методи аналітичного представлення мережних метаданих (інформації про структурний розподіл мережних потоків) шляхом їх репрезентації у якості об'єкта для цифрового голографічного перетворення та створення компактного голографічного образу, втрата або пошкодження частини якого не призведе до втрати всіх даних.

Національний сегмент глобальної інформаційної інфраструктури, що формується множиною сервісних мережних систем є чутливим до: змін ринкової кон'юнктури з боку споживачів електронних сервісів, виду, флуктуацій та просторового перерозподілу навантаження, що ними створюється, а також до різного роду деструктивних впливів, які представляють загрозу його функціональній стабільності. В роботі поставлено та розв'язано низку взаємопов'язаних науково-прикладних завдань, які спрямовані на оптимальний вибір та структурно-параметричне конфігурування архітектурної реалізації сервісних мережних систем на кожному з найбільш розповсюджених рівнів їх модельних представлень: IaaS, PaaS, SaaS. Результатом розв'язання цих завдань стали удосконалені або запропоновані математичні, структурно-параметричні та структурно-функціональні моделі: оптимального структурно-параметричного синтезу названих систем за критеріями якості сервісу (із урахуванням рівня сервісної доступності), системної продуктивності та функціональної стійкості; процесів диференційованого обслуговування потоків запитів; адаптивного резервування та перерозподілу ресурсів мережно-залежних рівнів телекомунікаційних сервісних платформ, зокрема на основі застосування методів теорії нечітких множин; опрацювання диференційованих потоків навантаження розпаралеленими віртуалізованими мережними засобами; компактного представлення мережних метаданих засобами на основі концепції цифрового голографічного оброблення.

В роботі досліджено ефективність масштабування платформ надання телекомунікаційних послуг, а також їх структурних перетворень, крім того

враховано вплив самоподібності й інших характеристик трафіку (які були вивчені експериментально) на зазначені вище критерії технічної ефективності. Було запропоновано зміни у механізмах пріоритетного обслуговування трафіку навантаження, що покращило часові показники якості сервісу у 2-7 разів, у залежності від показників рівня завантаження мультисервісної мережної платформи (за результатами моделювання). Визначено шляхи та особливості адаптації моделі IaaS для масштабованих мереж цивільного і спеціального призначення. Представлено концептуальні засади розроблення мігруючого мережного екрану (брандмауера), як ефективної системи виявлення вторгнень для телекомунікаційних платформ національного масштабу, проведено поглиблений аналіз викликів запровадженню хмарного комп'ютингу в Україні. Будучи складною для подолання та надійною системою, він може служити в якості платформи для розгортання багатопарової масштабованої хмарної мережі, яка потребує високого рівня захисту від різного роду шкідливих атак та мережних впливів. Коротко розглянуто механізм активації захисту з використанням основних визначень семантичних і технічних точок присутності.

Було покращено показники якості сервісу в мобільних системах доступу, що реалізують принципи ефективного використання мережних та радіо-ресурсів, як часткового випадку гетерогенних мережних сервісних платформ і, відповідно, запропоновано оптимальну процедуру інтелектуального вертикального хендоверу на основі хмарних технологій і методів нечіткої логіки. Для розв'язання завдання ініціювання передачі обслуговування між різними групами мережних ресурсів було запропоновано висористання централізованого способу управління хендовером. Розроблений підхід, у порівнянні з існуючими, використовує теорію нечітких множин. Ця теорія була обрана в якості інструменту для розв'язання завдань агрегації амбівалентних, суб'єктивних і нечітких оціночних суджень про стан конкретних параметрів, як критеріїв оптимального вибору мережних ресурсів (комірок гетерогенної системи безпроводного доступу). Таким чином, якщо модель ресурсного

менеджменту побудувати відповідно до запропонованих підходів, то вона стає кількісною, на відміну від існуючих методів, що забезпечують отримання лише суб'єктивних оцінок. Для цілей проведення дослідження процесів функціонування гетерогенної бездротової мережі в умовах, наближених до реальних, а також за високої мобільності користувачів була розроблена і апробована імітаційна комп'ютерна модель.

Сформовано методологію та методи, що дозволяють оптимальне за техніко-економічними показниками впровадження телекомунікаційних сервісних платформ для ефективного та динамічного розвитку процесів надання електронних сервісів і використання засобів повсюдного комп'ютеризованого підприємствами та відомствами з використанням відкритої системної архітектури.

Ключові слова: масштабована сервісна мережна система, гетерогенна телекомунікаційна платформа, сервісно-орієнтована архітектура, структурно-параметричний синтез, ресурсна оптимізація, хмарна мережна платформа, національний сегмент, глобальна інформаційна інфраструктура.

Список публікацій здобувача:

Наукові праці, в яких опубліковані основні наукові результати дисертації:

1. Demydov I. The Research of the Availability at Cloud Service Systems / I. Demydov, M. Klymash, Z. Kharkhalis, B. Strykhaliuk, P. Komada // Proceedings of SPIE: Photonics Applications in Astronomy, Communications, Industry, and High-Energy Physics Experiments, USA. – 2017. – Vol. 10445. – doi: 10.1117/12.2280885.

2. Demydov I. The Structural-Functional Synthesis of IoT Service Delivery Systems by Performance and Availability Criteria / Ivan Demydov, Yulia Klymash, Mykola Brych, Mykhailo Klymash // Internet of Things (IoT) and Engineering Applications (Canada). – May, 2017. – Vol. 2. – Issue 1. – P. 1-13.

3. Demydov I. Features of the cloud services implementation in the national network segment of Ukraine / I. Demydov, M. Klymash, M. Beshley, O. Shpur // Information and telecommunication science. K.: NTUU «KPI», 2016. - No.1. - P. 31-38.

4. Бешлей М. І. Розвиток методів передавання даних реального часу шляхом вдосконалення процесів пріоритезації потоків у маршрутизаторах / М. І. Бешлей, В. В. Червенець, І. В. Демидов, В. І. Романчук, О. М. Панченко // Системи обробки інформації. — 2016. — № 5. — С. 114-123.

5. Климаш М.М. Дослідження доступності у хмарних сервісних системах / М.М. Климаш, І.В. Демидов, Мохамед Мехді Ель Хатрі, Ю.Л. Дещинський // Радіoeлектроніка та телекомунікації. Вісник Національного університету «Львівська політехніка». – Львів, 2016. – №849. – С. 218-229.

6. Демидов І.В. Моделювання процесів диференційованого обслуговування користувачів хмаринкових сервісних мережних систем / І. В. Демидов, Мухамед Мехді Ель Хатрі, Укаблі Юсеф // Наукові записки Українського науково-дослідного інституту зв'язку. – 2016. – №1(41). – с. 26-34.

7. Демидов І. В. Аналіз методів підвищення продуктивності телекомунікаційних мереж хмарних сервісних систем / І. В. Демидов, Мухамед Мехді Ель Хатрі, Укаблі Юсеф // Телекомунікаційні та інформаційні технології. – 2016. – №1. – С. 41-47.

8. Демидов І. В. Дослідження імовірнісних характеристик трафіку опорно-транспортної підсистеми мережі мобільного зв'язку / І. В. Демидов, М.М. Климаш, П. О. Гуськов, Мухамед Мехді Ель Хатрі // Наукові записки Українського науково-дослідного інституту зв'язку. – 2015. – №6(40). – С. 11-18.

9. Demydov I. V. The structural-functional synthesis of cloud service delivery platform after service availability and performance criteria / I. V. Demydov, В.М. Strykhalyuk, О. М. Shpur, Mohamed Mehdi El Hatri, Y. V. Klymash // Системи обробки інформації. — 2015. — № 1. — С. 144-159.

10. Демидов І. В. Моделювання процесів обслуговування потоків запитів у розподілених сервісних мережних архітектурах / І. В. Демидов, П. О. Гуськов, Мухамед Мехді Ель Хатрі // Наукові записки Українського науково-дослідного інституту зв'язку. – 2015. – №5(39). – С. 44-51.

11. Стрихалюк Б.М. Дослідження статистичних параметрів та характеристик інформаційних потоків в гетерогенних мережах /

Б.М.Стрихалюк, І.В. Демидов, В.І. Романчук, М.І. Бешлей // Наукові записки УНДІЗ. – 2014. – №6(34). – С. 82-92.

12. Стрихалюк Б.М. Структурно-функціональна оптимізація процесів міграції віртуальних машин в розподілених дата-центрах / Б.М. Стрихалюк, З.В. Хархаліс, І.В. Демидов // Комп'ютерні технології друкарства: збірник наукових праць. - 2014. - №32. - С. 69-81.

13. Стрихалюк Б. Моделювання хмаринкової мережної системи у гіперболічних віртуальних координатах / Б. Стрихалюк, М. Климаш, І. Демидов // Комп'ютерні технології друкарства. - 2014. - № 32. - С. 3-19.

14. Красько О. В. Аналіз параметрів оптичного сигналу в повністю оптичній мережі з комутацією за довжинами хвиль / О. В. Красько, І.В. Демидов, М.В. Брич // Вісн. Нац. ун-ту «Львів. політехніка». - 2014. - № 796. - С. 140-146. - Бібліогр.: 23 назв. - укр.

15. Klymash M. A Novel Approach of Optimum Multi-Criteria Vertical Handoff Algorithm for Heterogeneous Wireless Networks / M. Klymash, B. Stryhaliuk, I. Demydov, M. Beshley, M. Seliuchenko // International Journal of Engineering and Innovative Technology (IJEIT). – November 2014. – Volume 4, Issue 4(5). – P. 42-52.

16. Климаш М.М. Забезпечення якості обслуговування та оптимізація бізнес-процесів у розподілених системах на основі сервісно-орієнтованої архітектури / М.М. Климаш, І.В. Демидов, М.О. Селюченко, І.Д. Орлевич // Радіoeлектроніка та телекомунікації. Вісник Національного університету «Львівська політехніка». – Львів, 2013. – №766. – С. 150-155.

17. Demydov I. Analysis of service workflows distribution and service delivery platform parameters / Ivan Demydov, Orest Lavriv, Bohdan Buhyl, Yuriy Dobush, Mykhailo Klymash // Int. J. Services, Economics and Management. -2013. - Vol. 5. - No. 4. - P. 280-290.

18. Demydov I. Enterprise Distributed Service Platform – Network Architecture and Topology Optimization / I. Demydov, M. Klymash, N. Kryvinska, C. Strauss // Int. J. Space-Based and Situated Computing. -2012. – Vol. 2. - № 1. - pp. 23-30.

19. Бугиль Б.А. Підвищення ефективності розподілу ресурсів телекомунікаційної мережі шляхом зміни маршрутів передавання даних

[Електронний ресурс] / Б.А. Бугиль, М.М. Климаш, О.А. Лаврів, І.В. Демидов // Проблеми телекомунікацій. – 2012. – № 4 (9). – С. 32 - 44. – Режим доступу до журн.: http://pt.journal.kh.ua/2012/4/1/124_bugil_resource.pdf.

20. Klymash M.M. Analysis of service workflows distribution and SDP parameters / M.M. Klymash, I.V. Demydov, O.A. Lavriv, Yu.D. Dobush // Системи обробки інформації. – Харків, 2012. – Вип. 6 (104). – С. 103-107.

21. Добуш Ю.Д. Аналіз загроз передавання даних у системі «електронного урядування» та оцінка її ефективності / Ю.Д. Добуш, І.В.Демидов, М.М. Климаш // Вісник Державного університету інформаційно-комунікаційних технологій. – К., 2012. - Т.10, №3. – С.29-36.

22. Добуш Ю.Д. Дослідження відкритих сервісних інтерфейсів Parlay в концепції «електронного урядування»/ Ю.Д. Добуш, І.В.Демидов, М.М. Климаш // Комп'ютерні технології друкарства: Зб. наук. пр. – Львів: Українська Академія Друкарства, 2012. – №28. – С. 170-186.

23. Самер Аввад. Дослідження обслуговування трафіку на транзитній мережі оператора мобільного зв'язку / Самер Аввад, М. М. Климаш, І.В. Демидов, Б.В. Коваль // Наукові записки Українського науково-дослідного інституту зв'язку. – 2011. – №1 (17). – С. 51-55.

24. Klymash M. Traffic routing in telecommunication nets and its diakoptics representation / M. Klymash, B. Strykhalyuk, M. Kaidan, I. Demydov // Computation Problems of Electrical Engineering. –Lviv, 2011. - №1(1). – P.15-19.

Наукові праці, які засвідчують апробацію матеріалів дисертації:

25. Demydov I. The Synthesis Methodology of Scalable Telecommunication Service Platforms / Ivan Demydov, Zenoviy Kharkhalis // 2nd IEEE International Conference on Advanced Information and Communication Technologies-2017 (AICT-2017): Conference Proceedings. – Lviv, 2017. – P. 199-203.

26. Demydov I. The Method of Improving the Availability at Cloud Service Systems / Ivan Demydov, Olga Shpur, Rakhman Lutfor, Yurii Deshchynskyi // Матеріали Міжнародної конференції з інформаційно-телекомунікаційних технологій та радіоелектроніки (УкрМіКо'2016/UkrMiCo'2016): Збірник тез. – К.: НТУУ «КПІ», 2016. – С. 446 - 448.

27. Демидов І.В. Впровадження хмарних сервісних систем в національному мережному сегменті України / І.В. Демидов, О.М. Шпур // X Міжнародна науково-технічна конференція «Проблеми телекомунікацій» ПТ-2016: Збірник матеріалів конференції (19-22 квітня 2016р. м. Київ) - К.: НТУУ «КПІ», 2016. – С. 342-344.

28. Demydov I. Concept of the Migrating Firewall to Scalable Cloud Networks / Ivan Demydov, Orest Lavriv, Zenoviy Kharkhalis, Mohamed Mehdi El Hatri // Сучасні проблеми радіоелектроніки, телекомунікацій, комп'ютерної інженерії TCSET'2016 : матеріали XIII Міжнародної конференції, 23-26 лютого 2016, Львів, Славське, Україна / Міністерство освіти і науки України, Національний університет «Львівська політехніка». - Львів : Видавництво Львівської політехніки, 2016. – С. 643-645.

29. Demydov I. Dynamic Correction of Routing Metrics by Pervasive Structural Routing in the Scalable Distributed Service Networks / Ivan Demydov, Mohamed Mehdi El Hatri, Olga Shpur // Problems of Infocommunications Science and Technology (PIC S&T), 2015 Second International Scientific-Practical Conference, 13-15 Oct. 2015, Kharkiv, Ukraine. – P. 164-166.

30. Demydov I.V. The features of cloud service delivery platform structural-functional synthesis / I.V. Demydov, M.M. Klymash, O.M. Shpur, Z.V.Kharkhalis // Міжнародна науково-технічна конференція «Сучасні інформаційно-телекомунікаційні технології»: матеріали науково-технічної конференції (17-20 листопада 2015 р. м.Київ), Т.3 – К: ДУТ. – 2015. – С. 19-21.

31. Demydov I. Mobility Management and Vertical Handover Decision in an Always Best Connected Heterogeneous Network / Ivan Demydov, Marian Seliuchenko, Mykola Beshley, Mykola Brych // Proceedings of XIIIth international conference «The experience of designing and application of CAD Systems in microelectronics» CADSM'2015, 24-27 February, Lviv-Poljana, Ukraine. – 2015. - P. 103-105.

32. Strykhalyuk B. Synthesis of distributed service-oriented structures cloud networks is based on algorithm for determining hyperbolic virtual coordinates / Bogdan Strykhalyuk, Olga Shpur, Ivan Demydov, Yulia Klymash // Proceedings of XIIIth international conference «The experience of designing and application of CAD

Systems in microelectronics» CADSM'2015, 24-27 February, Lviv-Poljana, Ukraine. – 2015. - P. 231-235.

33. Демидов І.В. Доступність композитних застосувань у сервісо-орієнтованих системах / І.В. Демидов, О.А. Лаврів, О.М. Шпур, М.О. Селюченко // Вимірювальна та обчислювальна техніка в технологічних процесах: матеріали XIII Міжнародної науково-технічної конференції (6-12 червня 2014 р. м. Одеса). – 2014. - с.119-121.

34. Demydov I. The Holographic Network Analysis / Ivan Demydov, Bohdan Strykhalyuk, Mykhailo Klymash // The 2014 IEEE International Black Sea Conference on Communications and Networking (IEEE BlackSeaCom 2014), Odessa, Ukraine – Chisinau, Moldova, May 27-30, 2014. – Chisinau:TUM, 2014. - pp. 66-68. - ACM ISBN: 978-1-4799-4067-7/14 (electronic).

35. Демидов І.В. Методи фіксації метаданих з'єднань глобальних мобільних телекомунікаційних мереж / І.В. Демидов, Ю.Д. Добуш // Всеукраїнська Науково-практична конференція «Сучасні проблеми телекомунікацій і підготовка фахівців в галузі телекомунікацій – 2013». Матеріали конференції 30 жовтня - 2 листопада 2013 р. – Львів, 2013. – С.167-170.

36. Добуш Ю.Д. Загрози поширенню даних в інфокомунікаційних системах «електронного урядування» / Ю.Д. Добуш, М.М. Климаш, І.В. Демидов // Матеріали Международной научно-технической конференции «Информационные проблемы теории акустических, радиоэлектронных и телекоммуникационных систем» (IPST-2012): Тезисы докладов. – АР Крым, Алушта, 2012. – С.165-166.

37. Dobush Yu. Approach to Secure Distributed Data Storing by Quasi-Random FAT Network Mapping / [Yuri Dobush, Ivan Demydov] // Матеріали Міжнародної науково-технічної конференції «Сучасні проблеми радіоелектроніки, телекомунікацій, комп'ютерної інженерії». – Львів –Славське, Україна, 2012. – P. 335.

38. Demydov I. Methods of traffic load balancing in telecommunication networks / Ivan Demydov, Yasser Muayyad Al-Hayali // Науково-методична конференція „Сучасні проблеми телекомунікацій і підготовка фахівців в галузі

телекомунікацій – 2012”. Матеріали конференції 1-4 листопада 2012 р. – Львів, 2012. – С.28-30.

39. Samer Awwad. Traffic Design in 4G Broadband Backbone Nets / Samer Awwad, Mykhailo Klymash, Ivan Demydov // Матеріали 11-ї Міжнародної науково-технічної конференції «Досвід розробки та застосування приладотехнологічних САПР в мікроелектроніці». – Львів – Поляна, Україна, 2011. – Р. 145 – 146.

40. Добуш Ю.Д. Застосування широкосмугових бездротових мереж UMTS/3G для організації мереж моніторингу параметрів розподілених об’єктів / [Ю.Д. Добуш, І.В. Демидов] // Матеріали VII Міжнародної науково-технічної конференції «Сучасні інформаційно-комунікаційні технології» (COMINFO’2011-Livadia): Збірник тез. – К.: ДУІКТ, 2011. – С.154 -155.

ABSTRACT

Demydov I.V. Synthesis of telecommunication service platforms on a national scale. - Proficiency scientific treatise on the rights of the manuscript.

A thesis submitted in fulfilment of the Doctor of Engineering Science degree in technical sciences on specialty 05.12.02 «Telecommunication systems and networks» (172 - Telecommunications and Radioengineering). - Lviv Polytechnic National University of Ministry for Education and Science of Ukraine, Lviv, 2017.

The thesis is devoted to the problems of structural and functional segmentation of the global information infrastructure for effective implementation of the national segment of telecommunication service platforms by criteria for system performance, service availability, and functional stability. Given the dynamics of modern information and communication technologies and the evolution of related organizational and market factors, the urgent need for scalability of electronic services in all economic sectors of Ukraine, within the implementation of the concepts of "Internet of things" (IoT) and "ubiquitous computing" the adaptation is essential of cloud capacities of network info communications operators set under control and in the public interest.

The paper demonstrated prerequisites for the appearance of contradiction, since processes of an ubiquitous computing introduction under inefficient scaling of telecommunications platforms leads to the necessity of their resources superfluous consumption reducing the range and scope of information processing tasks that must be solved in the framework of distributed services.

The thesis solves the actual scientific problem of methodological means development for telecommunication service platforms synthesis at the national level for the optimal implementation of the ubiquitous computing concept (distributed computing) with specified levels of quality of service, performance, and functional stability.

The first chapter of this thesis provides an overview of the literature on the topic of the dissertation as part of analysis methodology for creation and implementation of distributed service networks in the domestic segment of the global information infrastructure. The features of evolution, as well as issues of effective management of telecommunication service platforms based on analysis of service-oriented architectures of different technological implementation.

The second chapter is devoted to the definition of and research on the most effective by probabilistic and time methods for performance improving of network service platforms. These methods as have been shown in this thesis mainly based on improving the load processing of the users by means of the network layer, as well as adaptation, per its distribution and character, and utilization ratios of network resources. Based on the proposed in the chapter theoretical methods and structural and mathematical models it was shown that in today's distributed network service platforms there is considerable potential for optimizing by the criterion of performance.

The third chapter has explored models and methods of the statistical characteristics determining of telecommunication service platforms nodes, using interfaces of open system architecture (OSA) for example Parlay API; multivariate method of access is proposed to be used for increasing of distributed SOA platform network bandwidth by creating a replication of web services and balancing the

common load between them. In the chapter it was also conducted identification and analysis of the criteria of functional stability of the service network systems, allowing to determine the overall protection efficiency criterion of multi-service information nets within the national segment of the service network infrastructure, in addition, there was general analysis carried out of the threats to the data and functional stability in multiservice information and communication systems that implement telecommunications service platform of the national segment of the global information infrastructure. In this section a statistical study of heterogeneous multiservice corporate network system load was performed to analyze the indices of its self-similarity for certain types of traffic and it shows that the main types of workload have quite a high degree of self-similarity; it was also demonstrated that the problem of optimal structural and parametric synthesis of network service platforms can be reduced to the task of selecting their optimal structural and functional parameters within certain specified architecture of SOA type.

In the fourth chapter there was research presented of performance characteristics and service availability of telecommunication service platforms in the process of their structural and parametric synthesis, including scaling; and also analysis provided of modern approaches to detection and prevention of functional intrusions in distributed network systems, as well as developing concepts and models of migration firewall based on the definitions of points of presence and information presence in an open functional model of heterogeneous service systems; strategies were investigated for managing of resources migration processes in heterogeneous service platforms.

The fifth section analyzes the principles of convergent network-dependent service levels resources optimizing of heterogeneous distributed systems, carried finding the ways to optimize resources of interconnected network service platforms plurality. Considered and studied the proposed method and algorithm of traversal structural tracing that allows rapid determination of structural changes, and therefore - network elements failures, as well as fluctuations in the volumes of traffic in telecommunication service platform.

The sixth chapter is dedicated to adaptation of the developed in the thesis methodology to transform telecom service platforms for their applications in mission-critical information and communication systems nationwide. The modified method is also proposed of queues processing based on the service differentiation model in IaaS. In the thesis, the methods of network metadata analytical representation were proposed (information about the structural distribution of network flows) through their representation as the object of digital holographic transformation and creation of compact holographic image, loss of or damage of which does not result in the loss of the mentioned data at all.

The national segment of the global information infrastructure, formed by a plurality of service network systems is sensitive to: changes in market conditions on the part of consumers of electronic services: the type, fluctuations, and spatial redistribution of loads, which they created, as well as various kinds of destructive influences that threatening its functional stability. There were defined and solved several interrelated tasks intended to produce an optimum choice and structural-parametric architectural configuration of the service implementation of network systems at each of the most common levels of model representations: IaaS, PaaS, SaaS. As the result of these tasks solution have become improved or proposed mathematical, structural and parametric and structural-functional models of: the optimal structural and parametric synthesis of these systems on the service quality criteria (taking into account the level of service availability), system performance and operational stability; differentiated processing of requests' flows; adaptive redundancy and redeployment of network-dependent levels' resources of service platforms, including through the application of fuzzy set theory methods; load flows differentiated processing by parallelized virtualized network resources; compact representation of network resources metadata by digital holographic processing concept.

The efficiency of the telecommunication service platform scaling and its structural transformations were investigated, as well as impact of the self-similarity and other traffic features (that were examined experimentally) to the defined above

criteria of the technical efficiency. The prioritized traffic service processing was modified has improved timing indexes of service quality in 2-7 times, depending on the level of multiservice network platform units loading. The ways and features of IaaS model adaptation for scalable networks of civil and special purpose were defined. The conceptual basics of the migrating firewall as intrusion detection system for telecommunication platforms of national scale are given, as well as deep analysis of cloud networking implementation challenges in Ukraine was conducted. Being sophisticated to bypass and robust, it could serve as the multilayer platform of scalable cloud network that demand high level of the defense from different kind of harmful impact and network attacks. A mechanism of defense activation was briefly considered using basic definitions of the semantic and technical presence points.

A quality of service indexes were increased in mobile systems based on efficient network- and radio-resources utilization of heterogeneous service network platform and proposed optimal procedure of intellectual vertical handover based on cloud technology and fuzzy logic technique. In order to solve a task of handover initiation and performing a centralized method of handover management has been proposed. Developed approach in comparison to existing ones uses the theory of fuzzy sets. This theory was chosen as a tool for solving tasks of aggregation of double-meaning, subjective and fuzzy evaluative judgments about state of particular parameters as criteria of optimal resource (cell) selection. Thus, if the resource management model is built according to such approaches, then it becomes quantitative unlike existing subjective evaluations. For investigation purposes of real heterogeneous wireless network operation under conditions of high user mobility the computer simulation model has been developed and verified.

The methodology and methods were formed that allow the implementation of the telecommunication service platforms for the optimum technical and economic indicators accomplishment to make process development of e-services distribution and ubiquitous computing means implementation by companies and agencies using open system architecture more efficient and dynamic.

Keywords: scalable service network system, heterogeneous telecommunication platform, service-oriented architecture, structural and parametric synthesis, resource optimization, cloud networking platform, the national segment, global information infrastructure.

The list of author's publications:

Proceedings where basic scientific results of thesis were published:

1. Demydov I. The Research of the Availability at Cloud Service Systems / I. Demydov, M. Klymash, Z. Kharkhalis, B. Strykhaliuk, P. Komada // Proceedings of SPIE: Photonics Applications in Astronomy, Communications, Industry, and High-Energy Physics Experiments, USA. – 2017. – Vol. 10445. – doi: 10.1117/12.2280885.

2. Demydov I. The Structural-Functional Synthesis of IoT Service Delivery Systems by Performance and Availability Criteria / Ivan Demydov, Yulia Klymash, Mykola Brych, Mykhailo Klymash // Internet of Things (IoT) and Engineering Applications (Canada). – May, 2017. – Vol. 2. – Issue 1. – P. 1-13.

3. Demydov I. Features of the cloud services implementation in the national network segment of Ukraine / I. Demydov, M. Klymash, M. Beshley, O. Shpur // Information and telecommunication science. K.: NTUU «KPI», 2016. - No.1. - P. 31-38.

4. Beshley M.I. The Development of Methods for Real-Time Data Transferring by Improving the Flows' Prioritization Processes in Routers / M.I. Beshley, V.V. Chervenets, I.V. Demydov, V.I. Romanchuk, O.M. Panchenko // Information processing systems. — 2016. — № 5. — P. 114-123.

5. Klymash M.M. The investigation of the availability at cloud service systems / M.M. Klymash, I.V. Demydov, Mohamed Mehdi El Hatri, Yu.L. Deshchynskyi // Radioelectronics and telecommunications. The Herald of Lviv Polytechnic National Univeristy. – Lviv, 2016. – Vol. 849. – P. 218-229.

6. Demydov I.V. The simulation of differentiated consumers servicing priocesses in the cloud service networks / I.V. Demydov, Mohamed Mehdi El Hatri, Oukabli Youssef // Scientific proceedings of Ukrainian Research Institute of Communications. – 2016. – №1(41). – P. 26-34.

7. Demydov I.V. The analysis of the performance increasing methods at the telecommunication networks of the cloud service systems / I. V. Demydov, Mohamed Mehdi El Hatri, Oukabli Youssef // Telecommunication and informational technologies. – 2016. – Issue 1. – P. 41-47.
8. Demydov I.V. The investigation of the traffic probabilistic characteristics at the backbone subsystem of the mobile communications network / I.V. Demydov, M.M. Klymash, P. O. Huskov, Mohamed Mehdi El Hatri // Scientific proceedings of Ukrainian Research Institute of Communications. – 2015. – №6(40). – P. 11-18.
9. Demydov I. V. The structural-functional synthesis of cloud service delivery platform after service availability and performance criteria / I. V. Demydov, B.M. Strykhalyuk, O. M. Shpur, Mohamed Mehdi El Hatri, Y. V. Klymash // Information Processing Systems. - 2015. - № 1. - P. 144-159.
10. Demydov I.V. The simulation of the requests' flows servicing processes at the distributed service network architectures / I.V. Demydov, P. O. Huskov, Mohamed Mehdi El Hatri // Scientific proceedings of Ukrainian Research Institute of Communications. – 2015. – №5(39). – P. 44-51.
11. Strykhalyuk B.M. A statistical parameters and characteristics study of informational flows in heterogeneous networks / B.M. Strykhalyuk, I.V. Demydov, V.I. Romanchuk, M.I.Beshley // Scientific proceedings of Ukrainian Research Institute of Communications. – 2014. – №6(34). – P. 82-92.
12. Strykhalyuk B.M. The structural and functional optimization of virtual machines migration processes at distributed datacenters / B.M. Strykhalyuk, Z.M. Kharkhalis, I.V. Demydov // Computer technologies of printing: scientific proceedings. - 2014. - №32. - P. 69-81.
13. Strykhalyuk B.M. Simulating of the cloud network system in the hyperbolic virtual coordinates / B.M. Strykhalyuk, M.M. Klymash, I.V. Demydov // Computer technologies of printing: scientific proceedings. - 2014. - № 32. - C. 3-19.
14. Krasko O. V. Analysis of optical signal parameters at all optical net with wavelength switching / O. V. Krasko, I.V. Demydov, M.V. Brych // Radioelectronics and telecommunications. The Herald of Lviv Polytechnic National Univeristy. – Lviv, 2014. – Vol. 796. – P. 140-146.

15. Klymash M. A Novel Approach of Optimum Multi-Criteria Vertical Handoff Algorithm for Heterogeneous Wireless Networks / M. Klymash, B. Stryhaliuk, I. Demydov, M. Beshley, M. Seliuchenko // International Journal of Engineering and Innovative Technology (IJEIT). – November 2014. – Volume 4, Issue 4(5). – P. 42-52.

16. Klymash M.M. Quality of service guarantee and business processes optimization in distributed systems based on service-oriented architecture / M.M. Klymash, I.V. Demydov, M.O. Seliuchenko, I.D. Orlevych // Radioelectronics and telecommunications. The Herald of Lviv Polytechnic National University. – Lviv, 2013. – Vol. 766. – P. 150-155.

17. Demydov I. Analysis of service workflows distribution and service delivery platform parameters / Ivan Demydov, Orest Lavriv, Bohdan Buhyl, Yuriy Dobush, Mykhailo Klymash // Int. J. Services, Economics and Management. -2013. - Vol. 5. - No. 4. - P. 280-290.

18. Demydov I. Enterprise Distributed Service Platform – Network Architecture and Topology Optimization / I. Demydov, M. Klymash, N. Kryvinska, C. Strauss // Int. J. Space-Based and Situated Comput. -2012. - Vol. 2. - № 1. - pp. 23-30.

19. Buhil B.A. The efficiency increasing of telecommunication network resources distribution by the data transferring routes changing [Electronic resource] / B.A. Buhil, M.M. Klymash, O.A. Lavriv, I.V. Demydov // Problems of Telecommunications. – 2012. – № 4 (9). – P. 32 – 44.

20. Klymash M.M. Analysis of service workflows distribution and SDP parameters / M.M. Klymash, I.V. Demydov, O.A. Lavriv, Yu.D. Dobush // Information Processing Systems. –2012. – № 6 (104). – P. 103-107.

21. Dobush Yu.D. Analysis of the data transferring threats in the e-government system and its efficiency assessment / Yu.D. Dobush, I.V. Demydov, M.M. Klymash // The Herald of State University of Informational and Communication Technologies. – Kyiv, 2012. - Vol.10. - №3. – P.29-36.

22. Dobush Yu.D. Investigation of the Parlay open service interfaces at the concept of e-government / Yu.D. Dobush, I.V. Demydov, M.M. Klymash // Computer technologies of printing: scientific proceedings. - 2012. - № 28. - P. 170-186.

23. Awwad Samer. An investigation of the traffic servicing in the transit network of the mobile communications operator / Samer Awwad, M.M. Klymash, I.V. Demydov, B.V. Koval // Scientific proceedings of Ukrainian Research Institute of Communications. – 2011. – №1 (17). – P. 51-55.

24. Klymash M. Traffic routing in telecommunication nets and its diakoptics representation / M. Klymash, B. Strykhalyuk, M. Kaidan, I. Demydov // Computation Problems of Electrical Engineering. –Lviv, 2011. - №1(1). – P.15-19.

Proceedings that certify an approvement of thesis materials:

25. Demydov I. The Synthesis Methodology of Scalable Telecommunication Service Platforms / Ivan Demydov, Zenoviy Kharkhalis // 2nd IEEE International Conference on Advanced Information and Communication Technologies-2017 (AICT-2017): Conference Proceedings. – Lviv, 2017. – P. 199-203.

26. Demydov I. The Method of Improving the Availability at Cloud Service Systems / Ivan Demydov, Olga Shpur, Rakhman Lutfor, Yurii Deshchynskyi // 2016 IEEE International conference of information-telecommunication technologies and radio electronics (UkrMiCo'2016): Materials of scientific and technical conference. – Kyiv: Igor Sikorsky Kyiv Polytechnic Institute, 2016. – P. 446 - 448.

27. Demydov I.V. An implementation of the cloud servicing systems in the national networking segment of Ukraine / I.V. Demydov, O.M. Shpur // Xth International scientific and technical Conference «Problems of Telecommunications» PT-2016: Conference proceedings (April 19-22, 2016, Kyiv) - K.: NTUU «KPI», 2016. – P. 342-344.

28. Demydov I. Concept of the Migrating Firewall to Scalable Cloud Networks / Ivan Demydov, Orest Lavriv, Zenoviy Kharkhalis, Mohamed Mehdi El Hatri // Modern Problems of Radio Engineering, Telecommunications, and Computer Science TCSET'2016 : Proceedings of the XIIIth International Conference, February 23-26, 2016, Lviv-Slavske, Ukraine / Ministry of Education and Science of Ukraine, Lviv Polytechnic National Univeristy. - Lviv: Lviv Polytechnic Publishing House, 2016. – P. 643-645.

29. Demydov I. Dynamic Correction of Routing Metrics by Pervasive Structural Routing in the Scalable Distributed Service Networks / Ivan Demydov, Mohamed

Mehdi El Hatri, Olga Shpur // Problems of Infocommunications Science and Technology (PIC S&T), 2015 Second International Scientific-Practical Conference, 13-15 Oct. 2015, Kharkiv, Ukraine. – P. 164-166.

30. Demydov I.V. The features of cloud service delivery platform structural-functional synthesis / I.V. Demydov, M.M. Klymash, O.M. Shpur, Z.V.Kharkhalis // International scientific and technical Conference «Modern Information and Communication technologies»: Conference proceedings (November, 17-20, 2015, Kyiv), Vol.3 – Kyiv: State University of Telecommunications. – 2015. – C. 19-21.

31. Demydov I. Mobility Management and Vertical Handover Decision in an Always Best Connected Heterogeneous Network / Ivan Demydov, Marian Seliuchenko, Mykola Beshley, Mykola Brych // Proceedings of XIIIth international conference «The experience of designing and application of CAD Systems in microelectronics» CADSM'2015, 24-27 February, Lviv-Poljana, Ukraine. – 2015. - P. 103-105.

32. Strykhalyuk B. Synthesis of distributed service-oriented structures cloud networks is based on algorithm for determining hyperbolic virtual coordinates / Bogdan Strykhalyuk, Olga Shpur, Ivan Demydov, Yulia Klymash // Proceedings of XIIIth international conference «The experience of designing and application of CAD Systems in microelectronics» CADSM'2015, 24-27 February, Lviv-Poljana, Ukraine. – 2015. - P. 231-235.

33. Demydov I.V. An availability of composite applications at the service-oriented systems / I.V. Demydov, O.A. Lavriv, O.M. Shpur, M.O. Seliuchenko // Measuring and computing means in technological processes: The Conference Proceedings of XIIIth International scientific and technical Conference (June, 6-12, 2014, Odessa). – 2014. - P. 119-121.

34. Demydov I. The Holographic Network Analysis / Ivan Demydov, Bohdan Strykhalyuk, Mykhailo Klymash // The 2014 IEEE International Black Sea Conference on Communications and Networking (IEEE BlackSeaCom 2014), Odessa, Ukraine – Chisinau, Moldova, May 27-30, 2014. – Chisinau:TUM, 2014. - pp. 66-68. - ACM ISBN: 978-1-4799-4067-7/14 (electronic).

35. Demydov I.V. Methods of connections metadata fixing at global mobile telecommunications networks / I.V. Demydov, Yu.D. Dobush // Ukrainian Scientific

and Practical Conference «Modern problems of telecommunications and professionals tuition in the field of telecommunications – 2013». Conference Proceedings, 30 of October - 2 of November, 2013. – Lviv, 2013. – pp. 167-170.

36. Dobush Yu.D. Data transferring threats in the e-government infocommunication system / Yu.D. Dobush, M.M. Klymash, I.V. Demydov // Proceedings of the International scientific and technical Conference «Informational problems in acoustic, electronic, and telecommunication systems theory» (IPST-2012): Conference Proceedings. – Crimea, Alushta, 2012. – pp. 165-166.

37. Dobush Yu. Approach to Secure Distributed Data Storing by Quasi-Random FAT Network Mapping / [Yuri Dobush, Ivan Demydov] // Modern Problems of Radio Engineering, Telecommunications, and Computer Science TCSET'2016 : Proceedings of the Xth International Conference, 21-24 February 2012, Lviv-Slavske, Ukraine / Ministry of Education and Science of Ukraine, Lviv Polytechnic National Univeristy. - Lviv: Lviv Polytechnic Publishing House, 2012. – P. 335.

38. Demydov I. Methods of traffic load balancing in telecommunication networks / Ivan Demydov, Yasser Muayyad Al-Hayali // Scientific and Methodical Conference «Modern problems of telecommunications and professionals tuition in the field of telecommunications – 2012». Conference Proceedings, November, 1-4, 2012. – Lviv, 2012. – pp. 28-30.

39. Samer Awwad. Traffic Design in 4G Broadband Backbone Nets / Samer Awwad, Mykhailo Klymash, Ivan Demydov // Conference Proceedings of the 11th International Conference «The Experience of Designing and Application of CAD Systems in Microelectronics». – Lviv – Polyana, Ukraine, 2011. – P. 145 – 146.

40. Dobush Yu.D. The usage of broadband wireless UMTS / 3G networks to organize the monitoring of distributed objects parameters / [Yu.D. Dobush, I.V. Demydov] // Conference Proceedings of the VIIth International scientific and technical Conference «Modern Informational and Communication Technologies» (COMINFO'2011-Livadia): Conference Proceedings. – Kyiv: SUIKT, 2011. – pp.154 -155.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ.....	30
ВСТУП.....	36
РОЗДІЛ 1. Аналіз методів побудови сервісних мережних систем	50
1.1. Аналіз особливостей створення масштабованих сервісних мережних систем.....	50
1.1.1. Проблематика ефективного управління розподіленими сервісними платформами	53
1.1.2. Особливості реалізації та моніторингу телекомунікаційних сервісних платформ національного сегменту.....	56
1.1.3. Ключові цілі управління сервісними мережними системами.....	61
1.2. Визначення вимог до сучасних сервісних мережних систем національного сегменту.....	65
1.2.1. Загальні принципи трансформації сервісних мережних систем України на основі хмарних технологій.....	69
1.2.2. Етапи впровадження хмарних технологій у національному сегменті сервісної мережної інфраструктури.....	73
1.3. Порівняльний аналіз розподілених архітектур телекомунікаційних сервісних платформ.	80
1.4. Характеристика та обґрунтування критеріїв оптимального вибору телекомунікаційних технологій шарів: доступу, агрегації, ядра.	87
1.4.1. QoS і підходи до управління потоками завдань у сервісній мережній платформі.....	89
1.4.2. Особливості використання ресурсів телекомунікаційної сервісної платформи мультисервісними потоками.....	91
1.4.3. Підходи до моделювання та параметризації мережної інфраструктури сервісної платформи.	94
1.5. Висновки до 1-го розділу.....	94
РОЗДІЛ 2. Моделювання імовірно-часових характеристик телекомунікаційних сервісних платформ.....	99

2.1. Дослідження методів підвищення продуктивності розподілених сервісних мережних систем.	99
2.1.1. Аналіз існуючих методів підвищення продуктивності телекомунікаційних сервісних платформ.....	102
2.2. Моделювання процесів обслуговування потоків запитів у розподіленій сервісній мережній платформі.....	107
2.2.1. Постановка задачі побудови математичної моделі обслуговування потоків запитів у телекомунікаційній сервісній мережній системі.....	110
2.2.2. Побудова структурно-математичної моделі обслуговування потоків запитів у телекомунікаційному сегменті сервісної мережної системи.....	113
2.3. Дослідження імовірнісних характеристик трафіку магістральної мережі на прикладі опорно-транспортної підсистеми RAN LTE	120
2.3.1. Постановка задачі математичного моделювання процесів обслуговування трафіку в розподіленій сервісній мережній архітектурі... ..	121
2.3.2. Дослідження процесів потокового резервування у розподіленій сервісній мережній архітектурі шляхом моделювання процесів обслуговування користувачьких запитів.....	128
2.4. Моделювання процесів диференційованого обслуговування користувачів хмарних сервісних платформ	131
2.4.1. Математична модель диференційованого обслуговування користувачів.	133
2.4.2. Аналіз результатів імітаційного моделювання процесів диференційованого обслуговування користувачів.....	136
2.5. Висновки до 2-го розділу.....	144
РОЗДІЛ 3. Дослідження телекомунікаційних сервісних платформ з відкритою архітектурою	148
3.1. Дослідження ефективності застосування відкритої архітектури у телекомунікаційних платформах національного масштабу на прикладі Parlay/OSA.....	148
3.1.1. Математичне моделювання PaaS, як відкритої системної архітектури.	152

3.1.2. Аналітичне дослідження статистичних характеристик телекомунікаційних сервісних платформ на основі відкритої системної архітектури.	157
3.1.3. Залежності базових характеристик опрацювання запитів від параметрів телекомунікаційної сервісної платформи.....	163
3.1.3.1. Залежність характеристик сервісної мережної платформи від кількості реалізованих комплексних сервісів.....	163
3.1.3.2. Залежність характеристик сервісної мережної платформи від кількості серверів послуг/сервісних застосувань.....	166
3.1.3.3. Залежність характеристик сервісної мережної платформи від інтенсивності надходження запитів на сервери застосувань.....	167
3.1.3.4. Залежність характеристик сервісної мережної платформи від ймовірності повторного обслуговування запитів сервісними застосуваннями.	169
3.1.4. Порівняльний аналіз характеристик відкритої сервісної платформи та класичного сервісного вузла.....	171
3.1.5. Порівняльний аналіз характеристик відкритих сервісних платформ розподіленої та централізованої архітектури.....	175
3.2. Аналіз недоліків сервісних мережних систем з відкритою архітектурою, характеристика їх функціональної стійкості.....	177
3.2.1. Класифікація загроз обробленню даних в інфокомунікаційній площині сервісних платформ національного масштабу.....	177
3.2.2. Оцінювання ефективності захисту мультисервісних інфокомунікаційних систем в національному сегменті сервісної мережної інфраструктури.....	185
3.2.3. Критерії оцінювання ефективності реалізації інфокомунікаційної системи передавання даних для сервісної мережної інфраструктури національного масштабу, що функціонує в захищеному режимі.....	188
3.2.4. Забезпечення якості обслуговування та оптимізація бізнес-процесів у розподілених телекомунікаційних системах на основі сервісно-орієнтованої архітектури.	190
3.2.4.1. Аналіз технології веб-сервісів.....	191
3.2.4.2. Характеристика якості обслуговування веб-сервісами.	193
3.2.4.3. Забезпечення якості обслуговування веб-сервісами за допомогою методу поліваріантного доступу.	195
3.3. Експериментальні дослідження статистичних параметрів та характеристик інформаційних потоків в гетерогенних телекомунікаційних мережах.	199

3.3.1. Загальна характеристика досліджуваних мережних потоків	201
3.3.2. Підбір теоретичних законів розподілу і їх параметрів.	207
3.4. Завдання оптимізації розподілу телекомунікаційних мережних ресурсів хмарних платформ для обслуговування сервісного навантаження із заданою якістю.	212
3.4.1. Критерії оптимального структурно-параметричного синтезу та пов'язані з ними параметри.	219
3.4.2. Розрахунок критеріїв у оптимізаційній задачі структурно-параметричного синтезу сервісної мережної системи.	224
3.5. Висновки до 3-го розділу.	227
РОЗДІЛ 4. Розроблення та моделювання процесів забезпечення функціональної стійкості телекомунікаційних сервісних платформ	232
4.1. Дослідження характеристик продуктивності та сервісної доступності розподілених сервісних мережних платформ у процесі їх структурно-параметричного синтезу.	232
4.1.1. Аналіз результатів моделювання функціональних характеристик масштабованих хмарних сервісних платформ.	234
4.2. Аналіз сучасних підходів до виявлення та запобігання функціональним втручанням у розподілені мережні системи.	242
4.2.1. Особливості застосування мережних екранів.	243
4.2.2. Порівняльний аналіз рівнів функціональності мережних екранів.	244
4.2.3. Технології подолання мережних екранів.	247
4.2.4. Об'єднані системи виявлення функціональних втручань.	248
4.2.5. Особливості мережних загроз для SDN.	251
4.3. Концепції точок присутності й інформаційної присутності у відкритій функціональній моделі гетерогенної сервісної системи.	252
4.4. Розроблення методу та моделі мігруючого мережного екрану.	258
4.5. Дослідження методів оптимального управління процесами міграції ресурсів в гетерогенних сервісних системах.	261
4.6. Висновки до 4-го розділу.	276

РОЗДІЛ 5. Розроблення методів оптимізації конвергованих ресурсів мережно-залежних рівнів гетерогенних розподілених сервісних систем	281
5.1. Розроблення методу динамічної корекції маршрутних метрик шляхом наскрізного структурного трасування.	281
5.2. Моделювання процесів гіперагрегації трафіку у транспортних платформах сервісних мережних систем.....	284
5.3. Оптимізація протоколів маршрутизації та призначення мережних ресурсів на основі застосування методів нечіткої логіки за критеріями якості сервісу (приклад оптимізації процесів вертикального хендовера в гетерогенних безпроводних мережах).....	286
5.3.1. Метод інтелектуального вертикального хендовера на основі гетерогенної телекомунікаційної платформи.	287
5.3.2. Багатокритерійний алгоритм вертикального хендовера користувачького навантаження.....	291
5.3.3. Моделювання процесу прийняття рішення щодо вертикального хендовера на основі використання нечіткої логіки.	295
5.3.4. Моделювання процесів оптимального розподілу ресурсів у гетерогенній мережній платформі безпроводного доступу.	301
5.3.5. Аналіз результатів моделювання.....	306
5.4. Висновки до 5-го розділу.....	310
РОЗДІЛ 6. Дослідження особливостей трансформації архітектури телекомунікаційних сервісних платформ для застосування в критично важливих системах національного масштабу	313
6.1. Дослідження ефективності застосування вдосконалених протокольних засобів мережного рівня для спеціалізації гетерогенних сервісних мережних платформ.	313
6.1.1. Практична реалізація модифікованого методу обслуговування черг на основі диференціації сервісів у моделі IaaS.....	315
6.1.2. Вдосконалена телекомунікаційна платформа IaaS магістрального рівня з можливістю організації масштабованих мереж цивільного та спеціального призначення.....	330
6.2. Голографічна модель функціонального аналізу мережних систем.....	332
6.2.1. Голографічна модель мережної системи.	334

6.2.2. Визначення функціональних метаданих мережної системи на основі її цифрового голографічного представлення.	337
6.2.3. Точкове відновлення функціональних мережних метаданих.....	338
6.3. Метод скоординованої фіксації мережних метаданих телекомунікаційних платформ в центрах оброблення даних національного рівня	340
6.4. Узагальнена методологія синтезу телекомунікаційних сервісних платформ національного масштабу.	344
6.4.1. Результати дослідження ефективності застосування методології синтезу ТКСП.....	351
6.5. Висновки до 6-го розділу.....	354
ВИСНОВКИ.....	358
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ.....	361
ДОДАТОК А. Початковий код програми для комп'ютерного моделювання процесів обслуговування запитів користувачів у ВН RAN безпроводного сегменту сервісної мережної системи.....	389
ДОДАТОК Б. Програмний код для реалізації моделі SaaS на основі функціональної парадигми системного програмування.	403
ДОДАТОК В. Акти впровадження результатів дисертаційної роботи	406
ДОДАТОК Г. Список публікацій здобувача за темою дисертації та відомості про апробацію результатів дисертації.....	410

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

- 4G – 4th Generation – Четверте покоління мобільного зв'язку;
- AET – Advanced Evasion Technologies - Технології подолання мережних екранів;
- AG - Application Gateway – Шлюз застосувань;
- API – Application Programming Interface – Прикладний програмний інтерфейс;
- ARPU - Average Revenue Per User - Середній дохід від одного користувача;
- ASP – Application Service Provider – Провайдер надання послуг;
- B2B – Business to Business – Модель взаємодії «бізнес – бізнесу»;
- BER – Bit Error Rate - Коефіцієнт бітових помилок;
- BH – backhaul – опорно-транспортна мережна система;
- CBN - Cloud Based Networking – Мережне середовище, що інтегроване у хмарну інфраструктуру;
- CDR – Call Detail Record - Детальний звіт про дзвінки;
- CEN – Cloud Enabled Networking – Мережне середовище, що використовує хмарні сервіси;
- CIDN – Collaborative Intrusion Detection Network – Спільна мережа виявлення функціональних втручань;
- COTS - Commercial off-the-shelf - Готові комерційні пакетні пропозиції апаратних та програмних рішень;
- CR - Circuit Relay – Фільтрування каналів;
- CRM - Customer relationship management - Управління відносинами з клієнтами;
- DaaS – Data as a Service – Дані (та їх оброблення), як сервіс;
- DC – Data Center – ЦОД;
- DDoS – Distributed DoS – Розподілена версія мережної атаки виду DoS;
- DMZ – Демілітаризована зона;

DoS – Denial of Service - Відмова у обслуговуванні внаслідок перевантаження запитами сервісної мережної платформи;

DPI – Deep Packet Inspection – Технологія глибокого аналізу змісту пакетів;

ERM - Enterprise risk management – управління ризиками суб'єкта господарювання;

ESC – Elementary Service Components – Елементарні сервісні компоненти;

FTP – File Transfer Protocol – Протокол передавання файлів;

G2B – Government to Business - Модель взаємодії «уряд – бізнесу»;

GTP - GPRS Tunneling Protocol- Група комунікаційних протоколів на базі IP, які використовуються для перенесення GPRS трафіку середені мереж GSM, UMTS та LTE;

Haas – Hardware as a Service – Апаратне забезпечення, як сервіс;

HE – Harmful Elects – шкідливі впливи;

HLR – Host Location Register - Базовий реєстр місцезнаходження абонентів;

HTTP – Hyper Text Transfer Protocol – Протокол передавання гіпертексту;

HTTP - Hyper Text Transfer Protocol - Протокол передачі гіпер-текстових документів;

HTTPS – HTTP протокол із додатковим шаром шифрування/аутентифікації;

HV – Hypervisor – Програмний гіпервізор;

IaaS – Infrastructure as a Service – Інфраструктура, як сервіс;

IAM – Initial Address Message - Початкове адресне повідомлення;

ID – Identifier – Ідентифікатор;

IDS – Intrusion Detection System - Система виявлення функціональних втручань;

IMS - IP Multimedia Subsystem - мультимедійна підсистема на основі протоколу IP;

IMSI – International Mobile Subscribers' Identifier – Міжнародний ідентифікатор користувача мобільних мереж зв'язку;

IN – Intellectual Network – Інтелектуальна мережа;

INAP - Intelligent Network Application Protocol - Протокол користувача інтелектуальної мережі;

IoT – Internet of Things – Концепція «Інтернету речей»;

IP – Internet Protocol – Інтернет протокол;

IPS – Intrusion Prevention System – Система запобігання функціональним втручанням;

ISDN - Integrated Services Digital Network — Цифрова мережа з інтегрованими службами (послугами);

JAIN - Java APIs for Integrated Networks – Програмні інтерфейси Java для інтегрованих мереж;

L2TP – Layer 2 Tunneling Protocol — Протокол тунелювання другого рівня для підтримки VPN;

LBS – Location Based Services – Сервіси локалізації місцезнаходження користувача;

LBS – Location Based Services – Сервіси на основі технологій визначення місцезнаходження;

LTE – Long Term Evolution - довготерміновий розвиток систем мобільного зв'язку (група концепцій та стандартів);

MAN - Metropolitan Area Network – Мережа регіонального значення;

MF – Migrating Firewall – Мігруючий мережний екран;

MSC – Mobile switching center – Центр комутації мобільного зв'язку;

MSISDN - Mobile Station ISDN Number — Міжнародний номер рухомої ISDN-станції;

NFC – Near Field Communication – Зв'язок на невеликих відстанях;

NFV – Network Functions Virtualization – Віртуалізація мережних функцій;

NGN – Next Generation Network – Мережа наступного покоління;

NSA - Network Stream Analyser – Аналізатор мережних потоків;

NSP – Nominal Statistical Profile – Номінальний статистичний профіль;

OAL - Overlay Analytical Layer – Шар аналізу потоків;

OSA – Open Systems Architecture – Відкрита системна архітектура;

OSS/BSS - Operation Support System/Business Support System — система підтримки операцій/система підтримки бізнесу;

PaaS – Platform as a Service – Платформа, як сервіс;

PER – Packet Error Rate – Коефіцієнт пакетних помилок;

PF – Packet Filters – Фільтрування пакетів;

PINT - PSTN/Internet Interworking – Взаємодія PSTN та Інтернету;

PLR – Packet Loss Rate – Коефіцієнт втрат пакетів;

PoIP – Point of Informational Presence – Точка інформаційної присутності;

PoP – Point of Presence – Точка (операторської) присутності;

PSTN – Public Switched Telephone Network – Телефонна мережа загального користування;

QoE – Quality of Experience – Якість сприйняття сервісу;

QoS – Quality of Service – Якість сервісу;

RAN – Radio Access Network – Радіомережа доступу;

RSS – Received Signal Strength – Потужність прийнятого радіосигналу;

SAAD – Statistical Abnormal Activity Detection system – Система виявлення аномальної статистичної активності;

SaaS - Software as a Service – Програмне забезпечення, як сервіс;

SAN – Storage Area Network – Мережа зберігання даних;

SAP – Service Access Point – Точка доступу до сервісу;

SCF - Service Capability Features - Функціональні можливості серверів послуг;

SCF - Service Control Functions – Функції управління послугами;

SCM - Supply Chain Management - Управління ланцюгом поставок;

SCS – Service Capability Server- Сервер послуг Parlay / OSA;

SDN – Software-defined Networking – Програмно-конфігурована мережа;

SDP - Service data point - Модуль зберігання даних для послуг;

SDP – Service Delivery Platform – Сервісна платформа;

SIF – Stateful Inspection Firewall – Технологія інспектування пакетів зі збереженням стану;

SIP – Session Initiation Protocol – Протокол встановлення сесії (як правило, VoIP);

SLA – Service Level Agreement – Угода про рівень якості обслуговування;

SMTP – Simple Mail Transfer Protocol – Простий протокол пересилання пошти;

SMTP – Simple Mail Transfer Protocol – Простий протокол пересилання пошти;

SN – Service Node - сервісний вузол (вузол служб);

SOA – Service-Oriented Architecture – Сервісно орієнтована архітектура;

SOAP – Simple Object Access Protocol - Протокол обміну структурованими повідомленнями в розподілених обчислювальних системах;

SPIRITS - Service in the PSTN/IN Requesting InTernet Service – Сервіс в PSTN/IN, що залучає Інтернет сервіси;

SSP – Services Switching Point - Точка комутації послуг IN;

SSP – Service Switching Part – Модуль комутації послуг;

SCP – Service Control Part - Модуль управління послугами;

TAPI - Telephony Application Programming Interface - Прикладний програмний інтерфейс телефонії;

TINA - Telecommunication Information Network Architecture - Телекомунікаційна архітектура інформаційних мереж;

TSAPI - Telephony Server Application Programming Interface - Прикладний програмний інтерфейс сервера телефонії;

UDDI – Universal Description Discovery & Integration — Платформово-незалежний інструмент для розміщення описів веб-сервісів;

URI - Uniform Resource Identifier - Уніфікований ідентифікатор ресурсів;

VM – Virtual Machines – Віртуальні машини;

VoIP – Voice over IP – Голос поверх IP (сервіс IP-телефонії);

VPN – Virtual Private Network – Віртуальна приватна мережа;

WSDL – Web Services Description Language — мова опису зовнішніх інтерфейсів веб-служби;

WSP - Wireless Session Protocol – Відкритий протокол безпроводних сесій;
XML – Extensible Markup Language – Розширювана мова розмітки;
ГНН – години найбільших навантажень;
ЗКС № 7 – Загальноканальна система сигналізації №7;
ІМ – інформаційна мережа;
МеМО – Мережа масового обслуговування;
МС – мережа сигналізації;
МСЕ-Т – Міжнародний Союз Електрозв’язку, секція телекомунікацій;
НКРЗІ - Національна комісія, що здійснює державне регулювання у сфері зв'язку та інформатизації (Україна);
НСД – несанкціонований доступ;
СМО – Система масового обслуговування;
СУБД – Система управління базами даних;
ТКСП – телекомунікаційна сервісна платформа;
ЦОД – центр оброблення даних.

ВСТУП

Загальна характеристика роботи. Дисертаційну роботу присвячено проблематиці структурно-функціональної сегментації глобальної інформаційної інфраструктури з метою ефективної реалізації національного сегменту телекомунікаційних сервісних платформ (ТКСП) за критеріями системної продуктивності, сервісної доступності, а також функціональної стійкості. Враховуючи динаміку розвитку сучасних інфокомунікаційних технологій та еволюцію пов'язаних із ними організаційних і ринкових чинників, нагальну потребу в масштабованості систем надання електронних послуг у всіх галузях народного господарювання України, в умовах впровадження концепцій «Інтернету речей» (IoT) та «повсюдного комп'ютингу», необхідною є адаптація потужностей хмарних мережних систем множини операторів інфокомунікацій під управлінням та в інтересах держави.

Актуальність теми. Процеси проектування та розвитку сучасних телекомунікаційних мережних платформ спрямовані на розв'язання широкого кола науково-прикладних завдань. Серед них на варто виділити завдання, пов'язані зі структурно-параметричним синтезом масштабованих сервісних мережних систем, оскільки недостатньо обґрунтований вибір їх архітектури (локальної та об'єднаної), конфігурації програмно-апаратних засобів, спеціальних методів опрацювання навантаження, що ними реалізуються може в процесі експлуатації викликати перевантаження окремих їх елементів або цілих сегментів, призвести до неефективного використання мережних ресурсів, невиправданого збільшення вартості або ж до неспроможності виконувати основні функції, тобто до порушення функціональної стійкості, системної дезінтеграції.

Особливої актуальності дані дослідження набувають в умовах інформаційної боротьби, оскільки більшість окремих телекомунікаційних сервісних платформ можуть використовувати критично важливі мережні елементи, що перебувають під контролем сторін, відсутність координації та контролю діяльності яких впливатиме на стабільність та якість функціонування

національного інформаційного простору. Національний інфокомунікаційний сегмент телекомунікаційних сервісних платформ підприємств та державних відомств, незалежно від їх розташування, масштабу та виду діяльності, потребує надійного архітектурного базису, що якомога меншою мірою залежний від окремо взятих операторів телекомунікацій, але, в той же час, більшою мірою відповідає сукупності стратегічних і тактичних цілей, які ставляться перед такими системами в разі їх спеціалізованого застосування, в тому числі – у розподіленому режимі. Очевидно, що розгляд телекомунікаційної складової при вивченні інфокомунікаційних мереж у сукупності з тими технологіями, що ними використовуються, дозволяє більш повно врахувати характерні системні особливості розвитку сервісної мережної інфраструктури методами теорії систем масового обслуговування.

Розвиток мережних технологій на сьогодні досяг рівня, коли можливо констатувати перехід до моделі взаємодії «термінал користувача – хмара». Багатошарова сервісна модель SaaS-PaaS-IaaS породжує крос-платформні відгалуження, зокрема «дані, як сервіс» DaaS, «апаратні комплекси, як сервіс» NaaS, враховуючи можливості віртуалізації мережних функцій (NFV). Хмарно-базовані системи почали витіснення мережних систем, що використовувались як транзитні потужності при доступі у хмарну інфраструктуру. Відтак, в Україні подібні зміни на рівні регіональних точок обміну трафіком (MAN-рівня) в мережі Інтернет реалізовані компанією Google, що орендує власні широкопasmові канали міжнародного зв'язку. На черзі та в процесі трансформування – інші широкопasmові сервіс-провайдери. Змінюються підходи до надання електронних послуг, коли їх базовий пакет доступний для переважної більшості потенційних споживачів на конкурентній основі. Відповідно, зростає рухомість користувачів, змінюється їх розподіл за групами пріоритетності в обслуговуванні, значно збільшуються запитувані обсяги трафіку до телекомунікаційних сервісних платформ, в тому числі й тих, які розвиваються в рамках запровадження державою систем «електронного урядування».

Проблематикою сервісних інфокомунікаційних платформ займається багато вітчизняних та зарубіжних вчених. Управління сучасними інфокомунікаційними мережними системами розглядають такі науковці, як Беркман Л.Н., Толубко В.Б., Глоба Л.С., Поповський В.В., Теленик С.Ф., Andriy Luntovskiyy, Alexander Schill, Hong J.W. та інші; сервісно-орієнтовані телекомунікаційні мережні системи докладно вивчали у своїх працях Ложковський А.Г., Стрихалюк Б.М., Лемешко О.В., Ролік О.І., Гольдштейн Б.С., Шнепс-Шнеппе М.А., Natalia Kryvinska, Christine Strauss, Yu C.Z. тощо; питання ресурсного управління в гетерогенних мережних системах досліджували Агеев Д.В., Богатырев В.А., Воробієнко П.П., Гаркуша С.В., Додонов А.Г., Xiaohu Ge, Jo M., Aramudhan M., Schmidt H., Walter F. Witt, Zhao X., Bloomers J. та інші. Проте, особливості створення та розвитку національного сегменту телекомунікаційних сервісних платформ у існуючих літературних джерелах висвітлені поверхнево.

На сучасному еволюційному етапі методи теорії телекомунікаційних систем дозволяють проведення узагальненого структурного синтезу розподілених сервісних мережних платформ, проте для більш повного врахування особливостей їх розвитку (масштабування, характеристик навантаження, архітектури, функціональних та інших якісних вимог) такі методи необхідно вдосконалювати. Відтак, необхідно більш детально дослідити імовірно-часові характеристики подібних систем, особливо для випадку використання відкритої архітектури, що набуває останнім часом широкого поширення. Дослідження масштабованих сервісних мережних архітектур щодо продуктивності апаратно-програмних комплексів, показників доступності сервісів, які ними реалізуються, методів та засобів забезпечення їх функціональної стійкості до зовнішніх впливів практично не проводились. Це, в свою чергу, спонукає до більш докладного вивчення методів оптимального розподілу ресурсів мережно-залежних рівнів у гетерогенних телекомунікаційних платформах, у тому числі – методів управління потоками. В умовах значного зростання попиту на нові технології безпроводного доступу

для широкопasmового передавання даних у рамках реалізації концепції повсюдного комп'ютингу, необхідною є взаємна адаптація архітектури платформ хмарних обчислень і гетерогенних систем безпроводного доступу 4-5G. Враховуючи складність останніх, перспективними виглядають підходи до керування розподілом мережних ресурсів на основі застосування методів теорії нечітких множин. Для ефективного, масштабованого впровадження концепції повсюдного комп'ютингу актуальними є також питання інтеграції сервісних мережних платформ різного рівня (SaaS, PaaS, IaaS) при реалізації відомчих інфокомунікаційних мереж, моделювання розподіленої гетерогенної телекомунікаційної сервісної платформи на основі стаціонарно-нестационарних сегментів інфраструктури доступу, дослідження особливостей забезпечення функціональної стійкості сервісних мережних систем, моніторингу та збору інформації щодо їх функціонування.

Таким чином, виникає невідповідність існуючого методологічного забезпечення архітектурного синтезу масштабованих сервісних мережних платформ сучасному рівню розвитку теорії та практики побудови телекомунікаційних систем в умовах збільшення ступеня проникнення розподілених обчислень в усі галузі господарювання, зокрема в рамках розбудови сервісної мережної інфраструктури згідно сучасної концепції IoT. Проте, споживання більших обсягів електронних сервісів призводить до зростання витрат операторів інфокомунікацій на організацію нарощування обсягів обчислювальних і телекомунікаційних потужностей (у разі досягнення меж їх консолідації), які, природно, з метою забезпечення прибутковості, перекладаються на плечі споживачів, у тому числі – державних.

Отже, виникає *протиріччя*, оскільки процеси впровадження повсюдного комп'ютингу в умовах неефективного масштабування хмарних телекомунікаційних платформ призводять до потреби у надлишковому споживанні їх ресурсів і обмеження переліку та обсягів завдань оброблення інформації, що можуть розв'язуватись в рамках надання розподілених сервісів.

На сьогодні дане протиріччя можливо розв'язати удосконаленням методів консолідації розподілених мережних і обчислювальних ресурсів в рамках побудови масштабованих сервісних платформ, що, разом із сукупністю порушених вище питань, дозволяє сформулювати актуальну *наукову проблему* розроблення методологічного забезпечення синтезу телекомунікаційних сервісних платформ національного рівня для оптимального впровадження концепції повсюдного комп'ютингу (розподілених обчислень) із заданими рівнями якості сервісу, продуктивності та функціональної стійкості.

Зв'язок роботи з науковими програмами, планами, темами. Тематика дисертаційної роботи безпосередньо пов'язана з положеннями Постанови Верховної Ради України про «Концепцію національної інформаційної політики», «Концепції конвергенції телефонних мереж і мереж з пакетною комутацією в Україні», «Стратегії розвитку інформаційного суспільства в Україні», Закону України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки». Дисертаційні дослідження виконувались у відповідності до наукового напрямку кафедри телекомунікацій Національного університету «Львівська політехніка» - «Інфокомунікаційні системи та мережі», в рамках низки держбюджетних науково-дослідних тем «Дослідження та розроблення телекомунікаційних мережних систем для застосувань телематики і телеметрії» (ДБ/КОМ) (2011-2012 рр.), № держреєстрації 0111U001223, «Моделі та структури конвергентних телекомунікаційних мереж на основі CLOUD – технологій» («ДБ/CLOUD») (2013-2014 рр.), № держреєстрації 0113U003184, «Методи побудови та моделі інформаційно-телекомунікаційної інфраструктури на основі SDN-технологій для систем електронного урядування» (ДБ/SDN) (2015-2016), № держреєстрації 0115U000444, а також госпдоговірної тематики «Проектування та впровадження локальної мережі передачі мультимедійних даних на базі Ethernet технологій» (2016 р.), ГД № 0548.

Мета і завдання дослідження. Метою представленої дисертаційної роботи є підвищення якості сервісу, продуктивності та функціональної

стійкості телекомунікаційних сервісних платформ національного рівня шляхом розроблення адаптивних методів для ефективного розв'язання завдань їх синтезу при впровадженні концепції повсюдного комп'ютингу (розподілених обчислень).

Для досягнення поставленої мети в межах дисертаційних досліджень були сформульовані та розв'язані наступні завдання:

1. Аналіз методів побудови національного сегменту сервісних мережних систем: проблематика мережного управління, моніторингу, мережної трансформації та конвергенції під егідою хмарних технологій, якості сервісу;

2. Моделювання імовірно-часових характеристик телекомунікаційних сервісних платформ: дослідження методів підвищення системної продуктивності, зокрема пріоритезації (диференціації) обслуговування користувачів і динамічного резервування мережних ресурсів;

3. Дослідження особливостей реалізації телекомунікаційних мережних платформ з відкритою сервісно-орієнтованою архітектурою та їх характеристик, визначення та аналіз критеріїв їх функціональної стійкості;

4. Дослідження статистичних характеристик навантаження гетерогенних сервісних мережних платформ;

5. Розроблення методології структурно-параметричного синтезу сервісних мережних систем з відкритою архітектурою за критеріями сервісної доступності та системної продуктивності: визначення та параметризація критеріїв, дослідження характеристик сервісної доступності та системної продуктивності в умовах масштабування мережних платформ;

6. Розроблення та моделювання методів забезпечення функціональної стійкості телекомунікаційних сервісних платформ: дослідження сучасних систем виявлення та запобігання функціональним втручанням, розроблення методу мігруючого мережного екрану, дослідження методів оптимального управління процесами міграції ресурсів в гетерогенних сервісних системах;

7. Оптимізація конвергованих ресурсів мережно-залежних рівнів гетерогенних розподілених сервісних систем: дослідження ефективності

структуро-генного балансування навантаження у транспортних платформах сервісних мережних систем, розроблення та моделювання методів ресурсного розподілу на основі теорії нечітких множин;

8. Дослідження особливостей трансформації архітектури телекомунікаційних сервісних платформ для застосування в критично важливих системах національного масштабу: вдосконалення протокольних засобів мережного рівня для спеціалізації гетерогенних сервісних мережних платформ, особливості адаптації IaaS для організації масштабованих мереж цивільного та спеціального призначення, голографічний опис функціональних метаданих мережної системи, дослідження особливостей скоординованої фіксації метаданих у мережних системах національного рівня.

Об'єктом дослідження є процес синтезу розподілених сервісних мережних систем.

Предмет дослідження: методи синтезу масштабованих телекомунікаційних сервісних платформ національного сегменту на основі відкритої архітектури.

Методи дослідження. В процесі досліджень використано такі теоретичні засади, як теорія систем масового обслуговування (для дослідження імовірно-часових характеристик телекомунікаційних сервісних платформ), теорія відкритих мереж Джексона (для дослідження процесів функціонування мережних платформ на основі відкритої сервісної архітектури), теорія оптимізації і теорія випадкових графів (для визначення критеріїв синтезу сервісних мережних платформ), теорія телекомунікаційних систем і теорія ієрархічних систем (для загального теоретичного обґрунтування результатів дисертаційної роботи), теорія марковських процесів (для дослідження процесів обслуговування навантаження в гетерогенних сервісно-орієнтованих платформах), а також методи математичного та комп'ютерного моделювання, нечіткої математики (для оптимізації розподілу ковергованих мережних ресурсів у гетерогенних сервісних платформах), метод Ватутіна (для

оцінювання ступеню паралельності структури), метод експертних оцінок (для оцінювання якості синтезованого рішення в поточних умовах функціонування).

Наукова новизна отриманих результатів.

1. Вперше запропоновано загальні принципи та структурно-організаційну модель трансформації телекомунікаційних сервісних платформ національного сегменту глобальної інформаційної інфраструктури на основі хмарних технологій, яка відрізняється від відомих урахуванням міжоператорської та крос-платформної конвергенції ресурсів в межах єдиної мережної політики під егідою DaaS концепції, що надало змогу пришвидшити процеси утворення національного хмарного простору.

2. Набула подальшого розвитку модель живучості складних мережних систем Додонова-Ланде шляхом урахування у компонентах її адитивного ймовірнісного представлення розв'язків модифікованої формули Норрса відносно ймовірності втрати запиту для заданих статистичних параметрів навантаження розпаралелених, послідовних та транзитних обробників (компонентів платформи), що дала змогу дослідити сервісну доступність при масштабуванні заданих сегментів телекомунікаційних сервісних платформ.

3. Вперше запропоновано методологію синтезу масштабованих телекомунікаційних сервісних платформ, яка, на відміну від відомих, враховує особливості адаптації їх SaaS, PaaS та IaaS реалізацій за критеріями сервісної (компонентної) доступності та системної продуктивності на основі доведення оптимальності структурної композиції у співвідношенні розпаралелених та послідовних компонент за принципом «золотого січення» ($\sim 0,6/0,4$), що дало змогу провести трансформацію та покращити ключові технічні параметри ряду мережних платформ національного рівня.

4. Вперше запропоновано структурно-функціональну модель мігруючого мережного екрану, яка, на відміну від відомих, передбачає реплікацію та міграцію компонентів телекомунікаційної сервісної платформи, які забезпечують збір статистичних даних про мережну активність для виявлення її

аномалій, що дало змогу забезпечити блокування або фільтрацію небажаних інформаційних потоків, інформаційної присутності.

5. Вперше запропоновано голографічну модель представлення часо-частотних параметрів або мережних метаданих гетерогенної мережної платформи, яка використовує принципи цифрової голографії для компактного числового представлення інтенсивності службових та інформаційних потоків навантаження, яка, на відміну від відомих, надає змогу відновлення їх розподілу за умов втрати частини даних голографічного представлення (образу).

6. Набула подальшого розвитку модель розподілу конвергованих ресурсів мережно-залежних рівнів гетерогенної сервісної платформи, яка, на відміну від відомих, базується на застосуванні положень нечіткої математики, зокрема методів оброблення трикутних нечітких чисел, що дало змогу уникнути двозначності при обґрунтуванні розв'язків завдань ресурсної оптимізації, які передбачають агрегацію складної, ієрархічної множини взаємопов'язаних критеріїв.

7. Удосконалено модель диференційованого обслуговування сегментом телекомунікаційної сервісної платформи двопріоритетного навантаження на основі рівнянь статистичної рівноваги для марковського процесу, що описується чотиривимірним вектором, яка, на відміну від відомих, враховує ресурсні обмеження та особливості дообслуговування навантаження різних груп користувачів, що дало змогу оптимізувати використання системної пропускної спроможності шляхом вибору порогового обсягу мережних ресурсів, доступних для обслуговування непріоритетних користувацьких запитів.

Практичне значення одержаних результатів. Основним практичним результатом дисертації, який одержаний на основі проведених теоретичних досліджень, є розроблена методологія синтезу телекомунікаційних сервісних платформ національного масштабу, як сукупність методів підвищення їх продуктивності та компонентної (сервісної) доступності, а також підтримання

функціональної стійкості з урахуванням особливостей реалізації національного сегменту глобальної інформаційної інфраструктури на основі хмарних технологій. При цьому, протягом 2014-2016 років проведено трансформацію мультисервісної телекомунікаційної платформи ПАТ «Укртелеком», на рівні IaaS реалізації одержано позитивний приріст продуктивності на 58% (з 198 до 314 Гбіт/с) та компонентної (сервісної) доступності на 1,3% (з 0,986 до 0,999); на рівні реалізації PaaS одержано позитивний приріст продуктивності на 35% (з 210 до 299 Гбіт/с) та сервісної доступності на 0,1% (з 0,99909 до 0,99999). Забезпечено сервісну доступність службової телекомунікаційної сервісної платформи ДПСУ на рівні не менше 0,99999, як PaaS реалізації на основі мережної інфраструктури ПАТ «Укртелеком».

У межах запропонованої методології використано наступні практичні особливості розроблених методів і моделей:

1. Розроблено метод мігруючого мережного екрану, який враховує загрози поширенню даних та порушення функціональної стійкості телекомунікаційної сервісної платформи, зокрема найбільш імовірні стратегії втручання в її роботу, підтримує її стійке функціонування шляхом багатофакторного статистичного аналізу мережної активності, зокрема фільтрування трафіку та блокування небажаних точок інформаційної (PoIP) та міжоператорської (PoP) присутності (відповідних мережних інтерфейсів, портів, окремих інформаційних потоків).

2. Запропоновано метод диференційованого обслуговування користувачів, який, шляхом оптимізації часу доступу до сервісної платформи неперіоритетними користувачами, дає змогу підвищити її добову системну продуктивність до 16%, а також удосконалено протокольні засоби сервісної мережної інфраструктури, які дають змогу підвищити якість потоків даних реального часу шляхом контролю та зменшення наскрізних затримок обслуговування пріоритетних пакетів у 2-7 разів. Для верифікації одержаного результату розроблено і апробовано моделі генератора трафіку, віртуалізованого програмного маршрутизатора з можливістю розпаралелення оброблення потоків навантаження за концепцією NFV, що, окрім цього, дало

змогу більш точно визначати статистичні параметри навантаження, зокрема параметр Херста.

3. Запропоновано нові підходи до аналізу та збору великих обсягів функціональних мережних метаданих. А саме, запропоновано розглядати їх, як цілісну сутність шляхом цифрового голографічного представлення мережної структури та множини її функціональних властивостей. Узагальнено теоретико-прикладні засади створення телекомунікаційної сервісної платформи національного масштабу для фіксації метаданих щодо комунікаційної активності абонентів рухомого зв'язку, з дотриманням принципів масштабованості в рамках глобальних комунікаційних процесів.

4. Запропоновано для гетерогенних телекомунікаційних сервісних платформ використовувати метод динамічної корекції маршрутних метрик шляхом наскрізного структурного трасування, що дало змогу підвищити доступність сервісних вузлів у хмарній системі до 4-10%, а також метод розподілу конвергованих ресурсів мережно-залежних рівнів гетерогенної сервісної платформи (наприклад безпроводного доступу) на основі застосування теорії нечітких множин, що дає змогу приймати обґрунтовані рішення щодо проведення процедур вертикального хендвера, базуючись на групі QoS-залежних критеріїв у амбівалентних ситуаціях.

Основні результати дисертаційної роботи використано і впроваджено:

– у ТзОВ СП «Мікро-код» Лтд (Україна-Канада) під час розроблення пропозицій щодо створення магістральних телекомунікаційних сервісних платформ з відкритою архітектурою, а також при розробленні систем фіксації метаданих щодо комунікаційної активності абонентів рухомого зв'язку;

– у Львівській філії ПАТ «Укртелеком» (керуючій філії Західного макрорегіону) для підвищення ефективності обслуговування навантаження користувачів при масштабуванні розподілених ЦОД сервісних мережних систем, а також при упровадженні методів підтримки їх функціональної стійкості;

– у ПП «Цифрові технології» (м. Львів) для покращення часових показників якості обслуговування користувачького навантаження у процесі надання розподілених хмарних сервісів, а також для підвищення коефіцієнта доступності композитних додатків, які реалізуються на основі масштабованих сервісних мережних систем;

– у навчально-науковому процесі кафедри телекомунікацій Національного університету «Львівська політехніка» для модернізації курсів лекцій з дисциплін «Телекомунікаційні та інформаційні мережі, ч.1», «Системне програмування інфокомунікацій»; для створення нових курсів лекцій з дисципліни «Розподілені сервісні системи та Cloud-технології», «Інтернет речей та повсюдний комп'ютинг».

Особистий внесок здобувача. Основні наукові результати дисертаційної роботи отримано автором самостійно. У працях, опублікованих у співавторстві, авторові належать: у роботах [2, 25, 55, 62, 75, 121, 227, 230, 231] – теоретичні основи побудови ефективних телекомунікаційних сервісних платформ національного сегменту глобальної інформаційної інфраструктури, зокрема у [26, 49, 55, 76, 161, 223, 225, 226] – результати моделювання їх функціональних характеристик; у роботах [116, 117, 218, 224, 228] – аналіз та розроблення сучасних методів забезпечення функціональної стійкості сервісних мережних систем, зокрема у [17] – метод та структурно-функціональна модель мігруючого мережного екрану, а у [219, 220] – методи фіксації мережних метаданих; у роботах [56, 62, 139] – загальний аналіз методів моделювання телекомунікаційних сервісних платформ; у [136] – голографічна модель телекомунікаційної системи; у працях [75, 83, 97, 161, 199, 229] – результати досліджень методів підвищення ефективності опрацювання навантаження в сервісних мережних платформах, зокрема у [76, 77, 83, 94, 199] – математичні моделі, результати моделювання; у роботах [126, 232] – математична модель ресурсної оптимізації з використанням методів теорії нечітких множин і результати моделювання; у роботах [26, 152, 223, 230, 233, 234] – методологічні основи структурно-параметричного синтезу масштабованих сервісних мережних платформ; у роботах [49, 75, 76, 94, 138] – моделі та результати

моделювання характеристик телекомунікаційних сервісних платформ з відкритою системною архітектурою; у праці [131] – результати експериментального статистичного дослідження мультисервісного навантаження в гетерогенній корпоративній мережній системі, а у [135] – аналіз стратегій міграції віртуальних машин у сервісній мережній платформі; у роботі [228] – математична модель параметрів поширення оптичного сигналу.

Результати спільних наукових праць було використано у дисертаційних роботах таких співавторів, як Стрихалюк Б.М. [235] (для дослідження критеріїв та варіантів здійснення міграції віртуальних машин у гетерогенних сервісно-орієнтованих телекомунікаційних мережах), Самер Мохамед Мустафа Аввад [236] (для моделювання процесів обслуговування навантаження в опорно-транспортній підсистемі мереж мобільного зв'язку 3-4 поколінь), Добуш Ю.Д. (для дослідження ефективності використання концепції відкритої сервісної архітектури в системах електронного урядування, а також загроз функціонуванню цих систем з погляду вразливостей телекомунікаційної інфраструктури) [237], Бешлей М.І., який використав розроблені автором методи оптимізації мережних ресурсів на основі методів нечіткої математики для апробації алгоритму вертикального хендвера [243].

Апробація результатів дисертації. Основні наукові результати і положення дисертації представлені, доповідались та обговорені на 18-ти міжнародних і державних науково-технічних конференціях та наукових семінарах: Міжнародних науково-технічних конференціях «Сучасні проблеми радіоелектроніки, телекомунікацій, комп'ютерної інженерії» (м. Львів-Славське, 2012, 2016 рр.); Міжнародних науково-технічних конференціях «Досвід розробки та застосування приладо-технологічних САПР в мікроелектроніці». (м. Львів-Поляна, 2011, 2015 рр.); Міжнародній науково-технічній конференції «Проблеми телекомунікацій - 2016» ПТ-16 (м. Київ, 2016 рр.); Міжнародній науково-технічній конференції «Информационные проблемы теории акустических, радиоэлектронных и телекоммуникационных систем» IPST-2012 (м. Алушта, 2012); Міжнародних науково-технічних конференціях «Сучасні інформаційно-комунікаційні технології» (м. Ялта,

2011 р., м. Київ, 2015 р.); Науково-практичних конференціях «Сучасні проблеми телекомунікацій і підготовка фахівців в галузі телекомунікацій – 2012, 2013» (м. Львів, 2012, 2013 рр.); XIII Міжнародній науково-технічній конференції «Вимірювальна та обчислювальна техніка в технологічних процесах» (м. Одеса, 2014); The 2014 IEEE International Black Sea Conference on Communications and Networking (IEEE BlackSeaCom 2014) (Odessa, Ukraine – Chisinau, Moldova, 2014); The 2015 Second International Scientific-Practical Conference Problems of Infocommunications Science and Technology (PIC S&T) (Kharkiv, Ukraine, 2015); Міжнародній конференції з інформаційно-телекомунікаційних технологій та радіоелектроніки IEEE (УкрМіКо'2016/UkrMiCo'2016) (м. Київ, 2016); 2nd International IEEE Conference on Advanced Information and Communication Technologies-2017 (м. Львів, 2017). Крім цього, дисертаційна робота у повному обсязі представлена на наукових семінарах кафедри телекомунікацій Національного університету «Львівська політехніка».

Публікації. За результатами досліджень, які викладені у дисертаційній роботі, опубліковано 40 наукових праць, серед них статей у наукових фахових виданнях – 23 (всі статті у науковій періодиці, що входить до міжнародних наукометричних баз різного рівня, включаючи Scopus, Index Copernicus, Google Scholar тощо), у збірниках матеріалів і тез доповідей міжнародних та всеукраїнських конференцій – 16, з них індексованих у наукометричній базі Scopus – 10.

Структура та обсяг роботи. Робота складається з переліку умовних скорочень, вступу, шести розділів, висновків, списку використаних джерел і чотирьох додатків. Загальний обсяг роботи складає 416 сторінок друкарського тексту, із них 14 сторінок вступу, 308 сторінок основного тексту, 120 рисунків, 17 таблиць, список використаних джерел із 243 найменувань, 4 додатки на 28 сторінках. Додатки містять обрані початкові коди розробленого програмного забезпечення, акти впровадження результатів дисертаційної роботи, а також список наукових праць автора.

РОЗДІЛ 1

Аналіз методів побудови сервісних мережних систем

1.1. Аналіз особливостей створення масштабованих сервісних мережних систем.

Сукупність установ, відомств та підприємств – основа економічного зростання України – зазнає активних інтеграційних процесів у глобальну інформаційну інфраструктуру. Пов'язані з відповідними бізнес-процесами (інформаційними процесами) сервісні мережні системи визначають акценти та пріоритети у реалізації актуальних соціальних, комерційних, оборонних, урядових програм тощо. Більшість державних і комерційних установ на сьогодні перебувають у стані динамічної конвергенції своїх інформаційно-комунікаційних систем задля розширення переліку послуг і сервісів, що надаються. Розвиток сервісної мережної інфраструктури для них є критично важливим завданням у світлі підтримки ефективності та конкурентоздатності на світовому рівні. Високоструктурованим, вертикально інтегрованим, багаторівневим організаціям, діяльність яких тісно пов'язана з інформаційними технологіями, електронними сервісами та телекомунікаціями все важче скорочувати час на їх модернізацію задля відповідності вимогам, що постійно зростають, особливо у випадку масштабованих рішень. Відповідями на всі перераховані виклики стало масове впровадження хмарних технологій, зокрема сторонніми операторами, проте проблематика побудови національного сегменту сервісних мережних систем, внаслідок специфічних вимог до його керованості, безпеки, а також технічної й економічної ефективності приводить до необхідності розв'язання низки складних взаємопов'язаних завдань, яким, власне і присвячена дана дисертаційна робота. Одним з основних функціональних елементів сервісної мережної інфраструктури є шар програмного забезпечення згідно моделі SaaS. Принциповою відмінністю моделі SaaS від попередніх (Hosted Applications та Application Service Provider (ASP)) є те, що отримується саме послуга та інтерфейс (призначений для

користувача або програми), тобто деяка функціональність без жорсткої прив'язки до способу її реалізації, як правило – розподіленого або хмарного [1]. Для оптимізації інфокомунікаційних процесів на основі сервісних мережних систем усередині організацій та відомств на сьогодні розроблено доволі значну кількість застосувань (рис 1.1). Як можна бачити, на практиці сучасні сервісні мережні системи охоплюють надання користувачам (організаціям чи фізичним особам) більшості існуючих інфокомунікаційних технологій у вигляді електронних послуг на основі мереж доступу (або ж IaaS) всіх можливих видів. Ефективне управління такими сервісними мережними системами, зокрема їх платформами є окремою важливою науковою задачею і у даному розділі, відповідно до обраної спеціальності, розглядається стисло.



Рис. 1.1. Інфокомунікаційні засоби та послуги, як продукт сервісної мережної системи сучасних розподілених підприємств та відомств [2].

Рівень моделі SaaS охоплює програмне забезпечення електронних послуг, яке використовує засоби рівня PaaS, що фізично розташовується на основі операторських рішень, зокрема – у рамках моделі IaaS. У національному сегменті сервісних мережних систем технічні параметри сервісної доступності та продуктивності безпосередньо впливають на ефективність інфокомунікаційної складової при наданні споживачам, таким як підприємства, відомства, групи окремих осіб, відповідних електронних послуг. Користувачі електронних сервісів є учасниками процесу їх одержання та, відповідно,

інформаційного обміну. Взаємодія та інфокомунікації – дві основні проблемні області, що стосуються діяльності розподілених суб'єктів народного господарства, а також забезпечення надання різного роду електронних сервісів, які націлені на індивідуальне використання. Очевидно, що розгортання операторами сучасних інфокомунікаційних засобів та оптимізація телекомунікаційних платформ підвищують ефективність управління та функціонування сервісних мережних систем, особливо для випадку оброблення інформації у реальному часі, а також дозволяють суб'єктам господарювання та операторам інфокомунікацій розв'язувати поставлені перед ними завдання на якісно новому рівні, впроваджуючи масштабовані розподілені обчислення для надання новітніх електронних сервісів.

Тим не менше, володіння покращеними засобами інфокомунікацій та взаємодії у розподілених системах не дає гарантій зростання продуктивності організаційних систем. Найбільш суттєві труднощі, з якими зустрічаються організації, що впроваджують згадані технології можна сформулювати наступним чином:

- Управління інфокомунікаційними технологіями. Є частиною теорії менеджменту інформаційних ресурсів підприємств у галузі економіки. В рамках даної спеціальності важливим є аспект виносу обчислювальних потужностей та засобів до сторонніх виконавців, наприклад – інфокомунікаційних провайдерів хмарних систем. Але такі системи за визначенням є гетерогенними: технології взаємодії на основі аудіо/відео-зв'язку та передавання даних різного пріоритету історично надавались розрізненими мережними платформами, чого, де-факто не допускають у сучасних конвергентних телекомунікаційних системах. А це, у свою чергу, викликає ризики зменшення системної продуктивності – середовище взаємодії суб'єктів господарювання стає незручним, громіздким, тобто – неефективним.

- Забезпечення взаємодії в рамках інфокомунікаційних систем у реальному часі. Розвиток ІР-технологій приводить до значного підвищення ефективності

діяльності споживачів, але взаємодія через інфокомунікаційні системи реального часу між групами користувачів досі стикається з обмеженнями, які стають особливо відчутними при трансформації неспеціалізованих сервісних мережних систем у спеціалізовані (зокрема відомчі) програмно-апаратні комплекси. Позитивні тенденції у розв'язанні даного питання виникають при впровадженні технологій повсюдного комп'ютингу, а також внаслідок наскрізного проникнення IP-телефонії через усі рівні сервісних мережних систем. Для досягнення максимальної ефективності своєї діяльності, кінцеві користувачі повинні чітко координуватися в рамках розподіленої сервісної інфраструктури (локалізація кореспондента, доступність тих чи інших послуг у реальному часі) [2-6].

1.1.1. Проблематика ефективного управління розподіленими сервісними платформами

У даному розділі визначимо основні вимоги до управляючих систем розподілених сервісних мережних платформ. Мережні системи суб'єктів господарювання, як правило складаються з мережного обладнання різного виду: маршрутизаторів, мостів, комутаторів, концентраторів тощо, які взаємодіють із зовнішнім або частково внутрішнім середовищем сервісних мережних систем. Цей підхід на сьогодні отримав загальну концептуальну назву Cloud Enabled Networking (CEN). Витіснення власного фізичного обладнання з мереж операторським відбувається, починаючи з 2015 року у рамках концепції Cloud Based Networking (CBN). Все обладнання сервісних мережних платформ взаємопов'язане через різноманітні топологічні конфігурації в межах операторських мереж або мереж підприємств. Система управління сервісними платформами повинна бути здатною автоматично визначати всі мережні пристрої та володіти інформацією про її структуру. Насправді, базова топологічна структура сервісних мережних систем не зазнає різких змін, якщо вони не перебувають у стані розвитку, проте, якщо ми переходимо до CBN концепції, то вона стає динамічною у межах взаємодії з

операторським обладнанням, зокрема – через мережу доступу. Всі структурні (в т.ч. топологічні) зміни повинні фіксуватися відповідними системами управління через мережний моніторинг [7-8]. Наступним відкритим питанням є *масштабоване* впровадження новітніх розподілених онлайн-електронних сервісів, які неминуче призводять до виникнення *загального протиріччя* щодо впровадження повсюдного комп'ютингу при одночасному скороченні споживання обчислювальних ресурсів хмарних сервісних мережних систем і розширенні переліку та обсягу задач оброблення інформації, що повинні розв'язуватись у рамках надання розподілених сервісів. Виявляється, що методологія, інструменти, навички і процеси, які використовувались для управління сервісними мережними системами (застосуваннями, платформами, інфраструктурою) протягом багатьох років стають *неефективними*.

Отож, веб-системи наступного покоління виявляються складними, зокрема в аспекті управління ними. В загальному, вони містять велику кількість взаємопов'язаних, гетерогенних компонентів: веб-вервери, Java та .NET сервери застосувань, сервери для оброблення сервісних запитів та взаємодії з СУБД, пакетні застосування, такі як Siebel, Oracle та SAP, а також серверні платформи, наприклад IBM MQ, CICS, Tuxedo, різноманітні види баз даних. Складнощі посилюються розробницькими ініціативами, що стосуються веб-сервісів та сервісно-орієнтованих архітектур (SOAs), бізнес процесів та сучасних інтеграційних технологій, а також систем управління якістю ITIL та Six Sigma. Такий рівень складності формується безпосередньо більше, ніж 25 нормами щодо організації та функціонування конкретної реалізації мережної архітектури, а також структурних параметрів розподіленої сервісної платформи (Enterprise distributed service platform). Сучасні методологічні засоби не можуть забезпечити достатній рівень її функціональної стійкості або ж якості управління нею з метою оптимізації продуктивності [9-12].

На сьогодні, кількість пропозицій інноваційних послуг, які спрямовані на підтримку та зростання середнього доходу від одного користувача (ARPU)

продовжує збільшуватися. Такі пропозиції, зокрема, включають конверговані сервіси (мультисервісні телекомунікаційні послуги), телеголосування, мікро-платежі, збалансоване самообслуговування користувачів електронними сервісами (наприклад – в системах електронного урядування), прогнозування потреб користувачів тощо. У середовищах сервісних мережних платформ наступного покоління оператори пропонують OSS/BSS застосування та засоби, що послуговуються стандартизованими елементами програмного забезпечення, використовуючи готові комерційні пакетні пропозиції апаратних та програмних рішень (COTS). Надання електронних сервісів та взаємодія сервісних елементів відбувається зазвичай на основі IP-базованих, стандартизованих мережних застосувань та операторської інфраструктури. Такі технології, як J2EE,.NET, SIP, JSLEE, SOA, а також онлайн веб-платформи використовуються все ширше, дозволяючи реалізовувати новітні мережні сервіси та застосування, які адаптуються під кожного окремо взятого користувача (див. рис. 1.2).

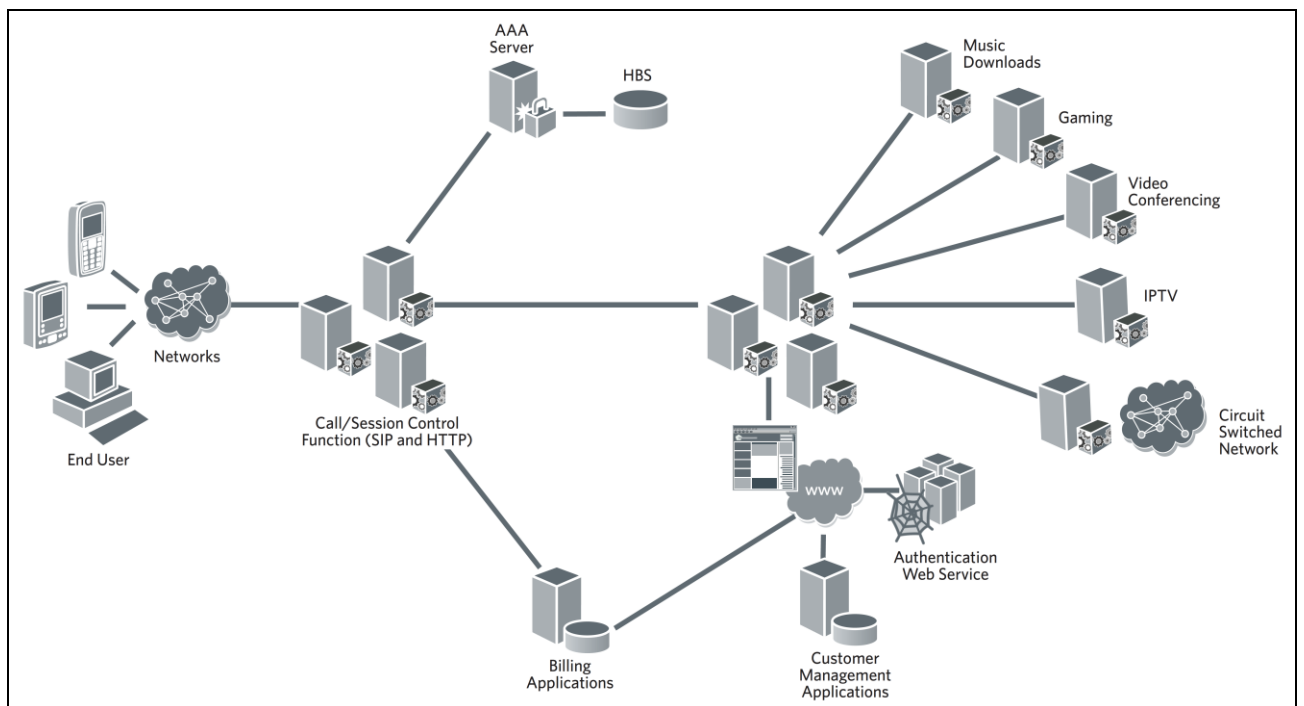


Рис. 1.2. Сервісна мережна архітектура для реалізації нового покоління електронних сервісів у моделі SaaS [2].

1.1.2. Особливості реалізації та моніторингу телекомунікаційних сервісних платформ національного сегменту

На першому етапі розбудови власної сервісної мережної інфраструктури більшість країн, що розвиваються застосовують модель, яка представлена на рис. 1.3. Можна говорити про реалізації ієрархічної сервісної системи, що зводиться до використання розподіленої мережі доступу (сервіси віддаленого доступу) та центральної системи оброблення даних (ЦОД). У деяких країнах, зокрема Україні, площин, на яких реалізують ЦОДи – багато, вони належать різноманітним державним відомствам або операторам інфокомунікацій. В інших країнах Азії, близького Сходу, Африки – подібні системи суворо ієрархічні з міркувань національної безпеки або протидії теористичним загрозам [13].



Рис. 1.3. Ранній розвиток національної сервісної мережної інфраструктури [13].

Як можа побачити з рис. 1.3 та 1.4 типово використовувалось обладнання комутаторів 3Com 3300 та маршрутизатори серії Cisco 2600.

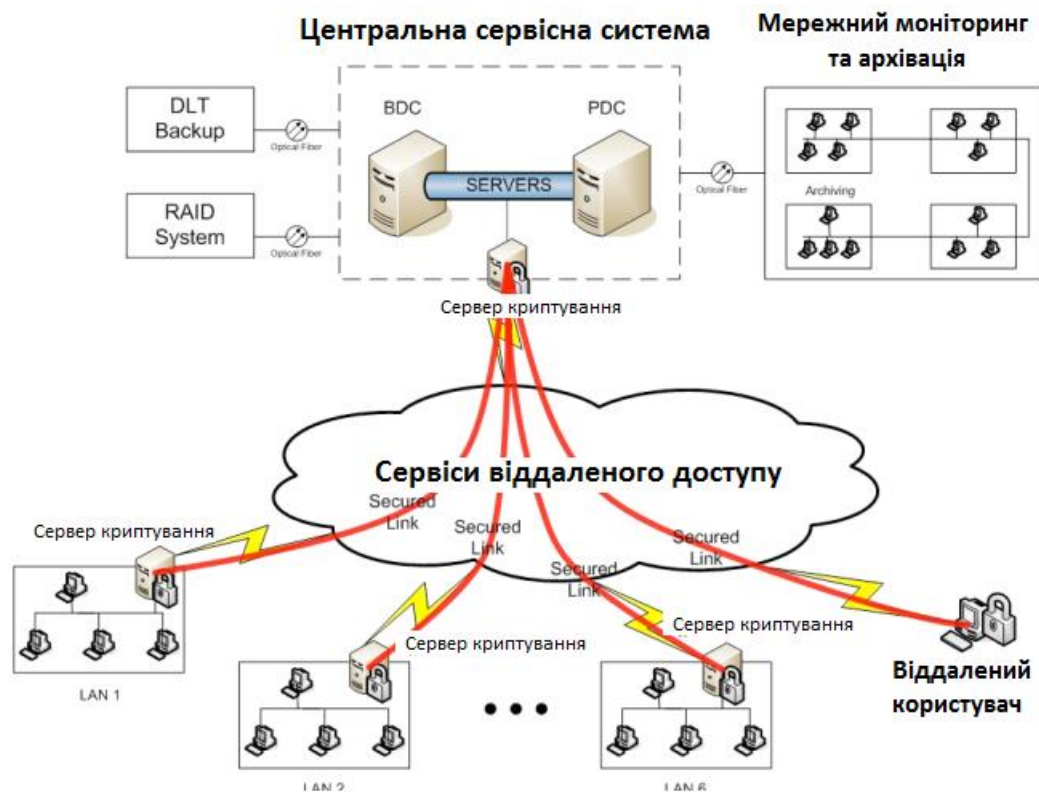


Рис. 1.4. Еволюція розвитку національної сервісної мережної інфраструктури у безпековому аспекті. Накрізне застосування шифрування [13].

US Department of Homeland Security протягом останнього десятиліття підтримував національні проекти з оптимізації управління ланцюгом поставок апаратно/програмних засобів мережної кібербезпеки на основі використання рішень виду COTS, підтримуючи національного виробника США Проте, варто відзначити позицію індустрії програмного забезпечення, що вказує на ще більшу загрозу порушення або втручання щодо даного ланцюга та відображена, зокрема фірмою Gartner і SANS Institute.

Аналіз мережних потоків у системах рис. 1.3-1.4 (NSA), виконується в обладнанні, що займається моніторингом Internet трафіку, застосовуючи принципи законного перехоплення.

Розроблене для моніторингу інтенсивності, обсягів та інших параметрів навантаження, з метою виключення негативних впливів на сервісну мережну систему, воно засовується, як правило, у інтересах спеціалізованих державних відомств.

У країнах Африки, Азії та Близького сходу і до сьогодні успішно застосовується принцип мінімізації числа з'єднань із глобальною мережною інфраструктурою. В країнах Європи та США це здійснити неможливо, тому обсяги інвестицій у кібербезпеку щороку зростають. Дані системи безпеки, як правило, є прозорими для користувачького трафіку.

Типове підключення системи моніторингу національного сегменту сервісних мережних систем відбувається через не менше, ніж 1 Gbit/s Ethernet оптичні підключення до комутатора CISCO Catalyst 6000 та головного маршрутизатора серії не нижче CISCO 7500, використовуючи головний та резервний канали з метою запобігання відмова у передаванні інформації та відмова обладнання (рис. 1.5) [228].

У цей же час, відповідним обладнанням збираються метадані сервісної мережної системи, які називають «атрибути», причому з інформаційних потоків, які передаються за усіма протоколами, що підтримуються. Відповідне програмне забезпечення американських виробників носить назву CAPI-FM. Для кожного відомого протоколу інтерес представляють кілька ключових атрибутів, наприклад:

- SMTP: відправник, одержувач, тема, ключові слова, тип додатків, ...
- GTP (мобільне тунелювання) L2TP (тунелювання фіксованих комп'ютерних мереж VPN): IMSI, MSISDN, номер, що викликається (called ID), тощо;
- WSP: Агент, контент тощо;
- HTTP: сервер, URI, агент, тощо;
- Radius: користувач, IP адреса тощо;
- Webmail: користувач, IP, тема, ключові слова тощо.

Звичайно важливим є те, щоб перераховані атрибути піддавались моніторингу та фіксації у режимі реального часу для всіх потоків зовнішнього трафіку в національній мережній сервісній системі. Затримка представлення повинна сягати не більше кількох секунд. Вони утворюють собою аналог CDR -

детального звіту про дзвінки, що зберігається у тій самій СУБД, що і весь пов'язаний потік трафіку.

Названа база даних містить дві менших за обсягом: база даних CDR та база даних усіх пов'язаних потоків трафіку. Фільтрування та моніторинг трафіку відбувається на основі зазначених атрибутів, а за необхідності – відбувається реконструкція всього об'єму інформаційного обміну, наприклад електронної пошти з вкладеннями, сесії VoIP, чату тощо.

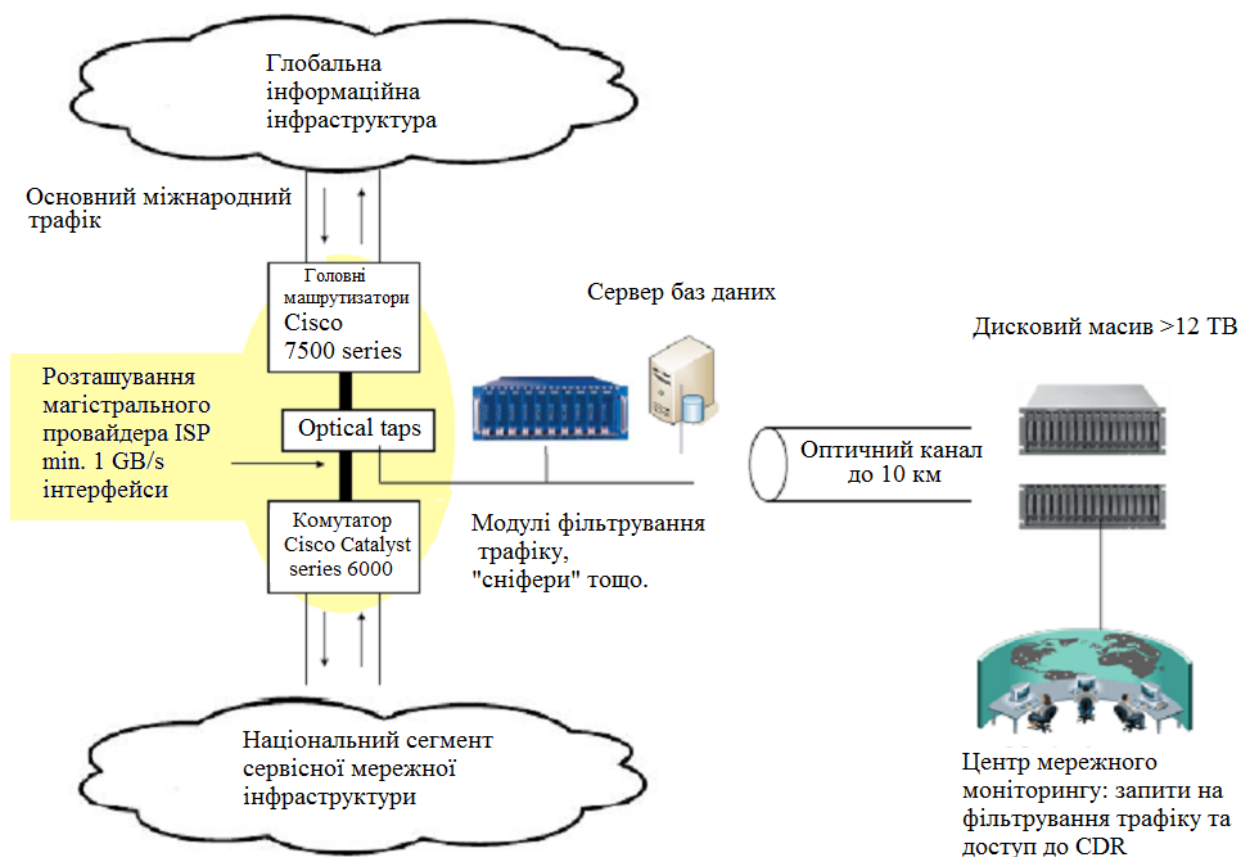


Рис. 1.5. Архітектура типової транзитної ланки національного сегменту сервісної мережної інфраструктури.

У базах даних може зберігатися, для прикладу, кількадекільні обсяг трафіку (рис. 1.5).

Всі реконструкції потоків відбуваються у центрах моніторингу мережі, в програмних модулях (транскодувальні модулі), тип яких залежить від типу потоку, що опрацьовується.

При відновленні, для прикладу, змісту електронного листування відповідний транскодувальний модуль використовує програмне забезпечення для опрацювання трафіку за протоколами: SMTP; POP3; IMAP; webmail (найбільш часто використовувані, google, yahoo, etc.).

Найбільш часто використовувані VoIP та Chat протоколи/застосування:

- Стандартизовані (H323, SIP, MGCP...);
- Функціональні (msn, yahoo, paltalk, vctocall, vctophone тощо.).

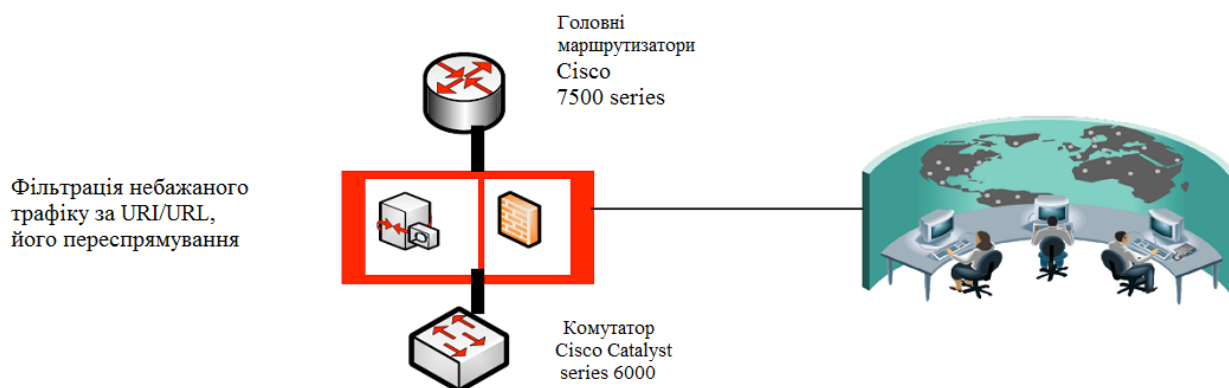


Рис. 1.6. Підсистема мережного моніторингу трафіку типової транзитної ланки національного сегменту сервісної мережної інфраструктури.

Підсистема моніторингу трафіку типової транзитної ланки національного сегменту сервісної мережної інфраструктури (рис. 1.6) підключається до центрів мережного моніторингу трафіку, звідки відбувається все керування. Налаштування процесів мережного моніторингу, виділення небажаної мережної активності відбувається за вказівкою зацікавлених державних органів, вони можуть динамічно оновлюватись у разі необхідності. Типова схема підключення національного сегменту сервісної мережної інфраструктури країн Африки/Азії (на прикладі Лівії) [13] представлена на рис. 1.7.

сервісу (зокрема сервісною доступністю) набуває характеру наукової проблематики у час, коли інфокомунікаційні оператори переходять до мереж наступних поколінь, які є конвергованими, програмно-базованими. Деякі основні вимоги до середовища управління сучасними інфокомунікаційними мережними системами, що забезпечують його ефективність були класифіковані автором у табл. 1.1. Найбільш важливі цілі управління продуктивністю цих систем, а також пов'язані з ними проблемні питання є наступними [2]:

- Оптимізація застосувань з підтримки користувачів – ціль для забезпечення достатнього рівня підтримки користувачів, оскільки вона є одним з елементів «першого враження» від взаємодії з сервісною мережною системою. Розміщення даних застосувань у колл-центрі або ж на порталі самообслуговування. Ефективне обслуговування запитів користувачів та проведення пов'язаних транзакцій вимагає одержання необхідної інформації у режимі реального часу від багатьох джерел (елементів сервісної мережної системи) для створення всієї повноти інформаційної взаємодії та більш повного їх інформування. При цьому, електронна послуга має надаватись без значних затримок. Будь-яке падіння продуктивності або сервісної доступності застосувань сервісної мережної системи, що виконують покладені на них функції призведуть до зменшення загальної системної продуктивності, рівня задоволеності користувачів, а також, у багатьох випадках, - до зменшення доходів відповідних суб'єктів господарювання та мережних операторів.

- Гарантії сервісу. Мережні платформи наступного покоління, а також пов'язані застосування в рамках моделі SaaS орієнтуються на застосування програмно-базованих сервісних платформ (SDPs) та мультимедійної підсистеми на основі Інтернет-протоколу (IMS) як частини NGN. Інфокомунікаційні оператори та сервісні провайдери потребують нових засобів для управління складними програмними платформами всередині інтегрованої сервісної

мережної системи, в той час як ІТ-індустрія потребує гарантій підтримки OSS/BSS на рівні, що відповідає вимогам обслуговування в реальному часі.

- Оптимізація підсистем OSS/BSS – OSS та BSS підсистеми повинні бути готовими відповідати вимогам реального часу, що визначаються мережами наступного покоління, але вони також повинні бути готовими працювати в умовах інших супутніх викликів ІТ індустрії. Швидке вдосконалення моделей здійснення оплати та нарахувань за одержані послуги, а також розвиток прогнозування системних вимог, які поєднуються зі значним зростанням кількості користувачів чинять додаткові навантаження на існуючі сервісні мережні системи.

- Забезпечення доступності інформаційних порталів (або агрегаторів навантаження) та внутрішніх інформаційних шин – зростаючи, інфокомунікаційні мережні оператори застосовують інтеграцію власних та партнерських платформ, SOA та веб-застосувань для підтримки запитів користувачів, обсяги яких постійно зростають. Утворені системи потребують проактивних управлінських ресурсів, які уможливають проактивне виявлення, локалізацію та подолання проблем із продуктивністю обслуговування користувацького навантаження.

- Відповідність вимогам угод про рівень якості обслуговування (SLAs) – комерційні взаємовідносини та регуляторні потреби потребують доволі суворих вимог, які закріплюються в SLA операторів сервісних мережних систем. Неможливість дотримання вимог даних угод викликає втрати комерційних вигод та репутації.

Без деталізованого мережного моніторингу та реагування на мережні загрози додержання SLAs ставиться під загрозу, навіть за умов застосування проактивного мережного управління, оскільки останнє потребує відносно значних проміжків часу для подолання виявлених проблем [14-16].

Талиця 1.1. Основні вимоги до середовища управління сучасними інфокомунікаційними мережними системами.

Системи, що розглядаються	Інтеграція процесів та рекомендовані підходи	Традиційне спрямування та планування потужностей
Системи, що орієнтовані на кінцевого споживача	Моніторинг реального часу	Експертні системи
Веб-застосування	Сервіс 24 × 7	Професійні системи
Портали підприємств /відомств	Низькі накладні витрати	Освітні системи
Сервери застосувань	Інформування про події	-
Інтеграція ПЗ проміжного шару (middleware)	Системний менеджмент, інтеграція платформ	-
Сервісно-орієнтовані архітектури (SOAs) Системи підтримки; Індивідуальні транзакції	Налаштовувані, інтуїтивно зрозумілі робочі столи (електронні робочі кабінети)	-

Приклад застосування підходів до управління мережною продуктивністю, який охоплює перераховані у табл. 1.1. системи; причому ці підходи забезпечують прозорість для запитів та транзакцій користувачів у інтегрованому мережному середовищі представлено на рис. 1.8.

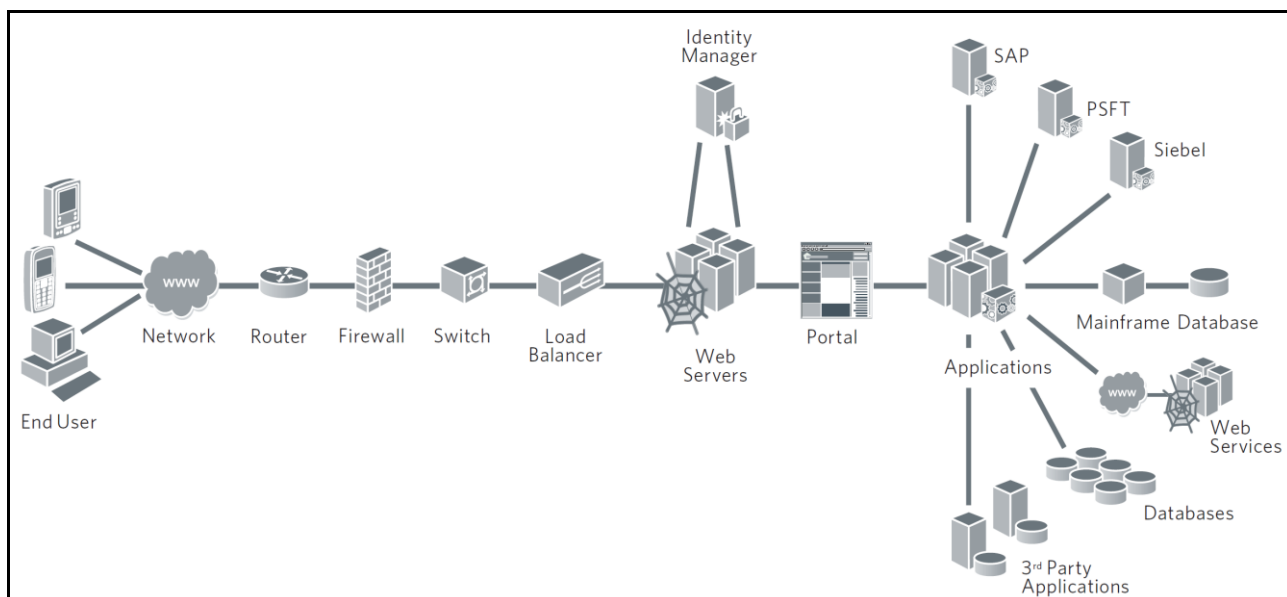


Рис. 1.8. Приклад сервісної мережної системи із застосуванням підходів до управління системною продуктивністю [2].

1.2. Визначення вимог до сучасних сервісних мережних систем національного сегменту.

Хмарні обчислювальні середовища та сервіси на їх основі пропонують безпрецедентну економію коштів, вдосконалений обмін інформацією та ефективність функціонування сервісної мережної інфраструктури. Відповідно, використання таких рішень дозволяє підвищити ефективність сервісів національного мережного сегменту. Таким чином, розроблення архітектури масштабованих сервісних мережних систем є ключовим аспектом, який безпосередньо формуватиме перевагу національних електронних сервісів, як державного, так і приватного секторів. Актуальність досліджень у даному напрямі підтверджується швидким розвитком комерційних технологій, які роблять процес впровадження хмарних технологій простішим, безпечнішим, а також значно продуктивнішим за критеріями прозорості, інтегрованості, розширення (масштабованості), якості сервісу. Впровадження хмарних сервісів державними та приватними операторами розподілених сервісних платформ потребує консолідації потреб у хмарних сервісних технологіях, а також узгодження тарифів на їх використання державними наглядовими органами, наприклад НКРЗІ України. Очевидно, що розробники хмарних сервісних

рішень повинні мати у своєму розпорядженні інструментарій для підтримування сервісної доступності та якості, базуючись на необхідних технічних та цільових параметрах. Дана публікація має на меті запропонувати архітектурні особливості реалізації хмарних сервісних технологій, які, зокрема, використовують існуючі приватні хмарні структури, для підтримки урядових та державних сервісних систем при значному зниженні рівня капітальних затрат, за умов підтримки необхідного рівня безпеки.

В сучасних соціально-політичних, а також економічних умовах, враховуючи розвиток нових мережних та інформаційних технологій, на перший план виходить проблематика впровадження повсюдного комп'ютингу, що має на меті скорочення споживання обчислювальних ресурсів для розв'язання більш широкого кола задач оброблення інформації в рамках надання необхідних розподілених сервісів. Не применшуючи вагу державних наглядових органів у процесі мережних перетворень, варто відзначити, що скорочення бюджетного фінансування потребує перегляду підходів до створення та модифікації сервісної мережної інфраструктури з метою підвищення її ефективності та безпеки, особливо в межах національного мережного сегменту [17].

Результатом цих перетворень виступає об'єднаний інформаційний простір (Joint Information Environment), як надійне та робастне середовище швидкісного доступу до даних, а також обчислювальних ресурсів, що не прив'язане до місця розташування споживачів тих чи інших сервісів.

Світовий досвід вказує на те, що хмарні платформи та сервіси дозволяють забезпечити підвищені можливості для швидкого розвитку сервісних застосувань у всіх галузях народного господарства України, в тому числі за рахунок множинного перевикористання сервісних застосувань та їх компонентів різними державними та недержавними організаціями. Спеціалізованими напрямками досліджень у даному контексті їх використання, окрім кібербезпеки, є методи забезпечення гарантованості інформації (Information assurance [18]), яка включає захист цілісності даних, доступність

даних та відповідних інформаційних сервісів, аутентифікаційні задачі та конфіденційність даних користувачів. Очевидно, такі методи повинні включати використання фізичних, технічних, а також адміністративних засобів. Цей методологічний аспект однаковою мірою стосується тих даних, що передаються, а також даних, які знаходяться на зберіганні. Важливими питаннями є також забезпечення системної адаптивності [19], неперервності функціонування (належного рівня сервісної доступності), функціональної стійкості, ефективності (продуктивності) впровадження сервісів, управління міграцією сервісів та даних, подолання залежності від мереж доступу, що, зокрема, є тактичним завданням сучасних безпроводних технологій доступу. Цікавим також є обслуговування користувачів у режимі перервного підключення.

Для подолання зазначених викликів та розв'язання окреслених задач необхідна синхронізація зусиль операторів телекомунікацій, інфокомунікаційних провайдерів (сервісних операторів), шляхом консолідації їх дата-центрів (ЦОД), а також проектних організацій під егідою державних наглядових органів, які в кінцевому результаті приведуть до вироблення спільної політики ефективного впровадження хмарних технологій, тобто створення необхідної методології відповідно до галузевих чи загально суспільних потреб. Такі заходи дозволять уникнути впровадження непродуктивних обчислювальних та мережних потужностей.

Досвід американських державних організацій свідчить, що у випадку призначення в хмарній системі кількох ЦОД у якості ядра, їх функціональність можливо поширити на іншу частину системи, поступово змінюючи її архітектуру, сервісні компоненти та оптимізуючи відповідні внутрішні процеси інформаційного обміну, що підвищить інтеоперабельність елементарних сервісних застосувань в ЦОДах та у всій мережній системі в цілому [20]. Крім того, такий підхід дозволяє розділити моделі застосування сервісів та передавання даних для різних за необхідним рівнем безпеки типів інформації: незахищених даних (Non-secure Internet Protocol Router Network), захищених

даних на основі відповідних протоколів безпечного передавання (Secure Internet Protocol Router Network), а також інформації з обмеженим доступом, що має піддаватися додатковим засобам захисту (Top Secret Sensitive Compartmentalized Information) в межах виділеної мережної інфраструктури [21].

Основною умовою впровадження хмарних технологій у національному сегменті сервісної мережної інфраструктури, на думку автора, є узгодження політики розподіленого використання сервісних компонентів різних сервіс-провайдерів за критеріями безпеки, якості, сервісної доступності. Виходячи з вище викладеного, можливо виділити наступну сукупність заходів із адаптації хмарних систем в національній сервісній мережній інфраструктурі:

1. Початкове впровадження хмарних сервісів: визначення стратегії та шляхів ефективного розвитку, користувацької бази, сфер застосування (державні та комерційні сервіси, зокрема e-government);

2. Оптимальна консолідація національних ЦОД: віртуалізація та консолідація даних і сервісних компонентів застосувань;

3. Впровадження консолідованої національної хмарної мережної інфраструктури: інтеграція багатоператорського середовища в рамках консолідації ЦОД, оптимізація надання розподілених сервісів через створену інфраструктуру в рамках прийнятої політики розподіленого використання сервісних компонентів, постійне оновлення сервісних та технологічних компонентів системи;

4. Підвищення ефективності надання хмарних сервісів: процес виводу сервісних компонентів на обслуговування до сторонніх операторів, підтримка комерційних сервісів, розширення переліку пропонованих мережних сервісів та обсягів їх надання, контроль з боку наглядових органів (НКРЗІ України).

Метою даного дослідження є пошук шляхів оптимальної консолідації для своєчасних трансформацій єдиного національного інформаційного простору України. На думку автора, забезпечення можливостей впливу на дані процеси з боку державних наглядових структур є критично важливим для України [234].

1.2.1. Загальні принципи трансформації сервісних мережних систем України на основі хмарних технологій

Впровадження хмарних технологій передбачає надання найбільш інноваційних, ефективних та безпечних інформаційних та інфокомунікаційних сервісів для забезпечення прозорого впровадження повсюдного комп'ютингу в національному мережному сегменті під необхідним контролем державних наглядових органів.

За визначенням Національного Інституту Стандартів та Технології (NIST), хмарні обчислення представляють собою модель неспеціалізованого мережного доступу на вимогу до сукупності конфігурованих обчислювальних ресурсів. Такими ресурсами виступають: мережі, сервери, дискові системи, застосування та сервіси. Загальноприйнята таксономія моделей, які використовуються для впровадження та надання хмарних послуг користувачам (рис. 1.9) включає три основні: Software as a Service (SaaS), Platform as a Service (PaaS), а також Infrastructure as a Service (IaaS) [22, 234].

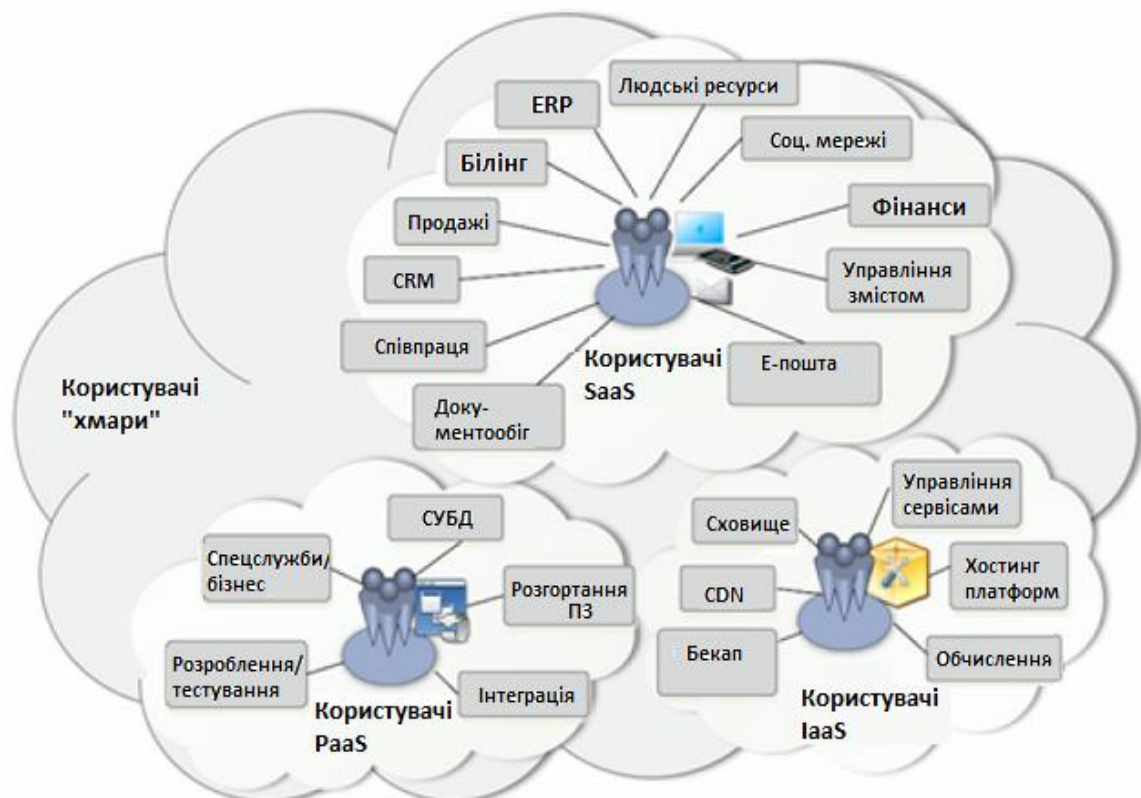


Рис. 1.9. Приклади сервісів, що доступні користувачам хмарної мережної системи [25].

Загальною особливістю цих моделей є фокусування на забезпеченні (підтримці та наданні) інформаційних технологій, як сервіса, що надається сервіс-провайдерами для споживачів. Взаємодія між останніми традиційно відбувається на основі IP-мереж. Зусилля державних наглядових органів повинні бути спрямовані на просування хмарних технологій для їх успішного використання національними споживачами та формування стійкого інтересу для інвестування в дану галузь ІТ як з боку держави, так і з боку комерційних організацій.

Основні переваги хмарних обчислень (ефективність, швидкодія, інновації) зведені до табл. 1.2.

Підсумовуючи наведене у табл. 1.2, можна стверджувати, що:

- консолідація хмарних систем є однією з ключових задач, яка приводить до економії капіталовкладень множини користувачів мережних сервісів, знижує вартість експлуатації неефективно розподілених та громіздких платформ надання сервісів. Крім того, практично «миттєва» масштабованість сучасних хмарних рішень дозволяє надавати послуги в обсязі, який необхідний користувачам тут і зараз, який, власне, і стане предметом фінансування в разі потреби. Чим ефективнішим є менеджмент сервісних мережних рішень, тим більшою буде економічна доцільність впровадження хмарних технологій, зокрема розроблення програмного забезпечення для нових хмарних застосувань;

- оперативний глобальний доступ до критично необхідної інформації в умовах високої доступності та оптимальної надмірності хмарного «повсюдного комп'ютингу» дозволяє підвищити опірність сервісної мережної інфраструктури до кризових ситуацій різного роду, зберігаючи неперервність системного функціонування;

- зменшення часу, який необхідно витратити на розповсюдження інформації користувачам системи в умовах її постійного масштабування можливо реалізувати на основі паралельності збору, оброблення та зберігання великих обсягів даних об'єднаними хмарними мережними системами, що

неможливо здійснювати за іншими підходами в сучасній галузі інфокомунікацій;

Таблиця 1.2. Основні переваги від впровадження хмарних обчислень.

Ефективність	Швидкодія	Інновації
Використання основних засобів – обчислювальних серверних потужностей на рівні більше 60-75% (існуючі системи – менше 30%)	Одержання сервісів від довірених сервіс-провайдерів інфокомунікацій вже і зараз (не потрібно роками будувати дорогу інфраструктуру)	Зміщення акцентів з управління основними засобами на управління сервісами (осучаснено управлінський підхід)
Підвищений ступінь агрегації вимог, пришвидшена консолідація хмарних систем (існуючим системам притаманне надлишкове дублювання серверних потужностей, розділені потоки запитів)	Практично миттєве нарощення і скорочення потужності сервісних мережних систем (на відміну від традиційних підходів, де потрібні місяці)	Підвищення рівня виробничої та організаційної культури (реформування державного управління, підвищення ефективності керування інформаційними потоками, електронне урядування)
Підвищення продуктивності розроблення та впровадження застосувань, вдосконалення управління мережними термінальними пристроями (на відміну від існуючих систем)	Більш швидка реакція на сучасний розвиток потреб державного та приватного секторів народного господарства (наприклад впровадження технологій IoT)	Покращена адаптація мережних сервісів до нових технологій (наприклад – термінальних пристроїв та гнучких мережних рішень)

- хмарні технології уможливають постійний моніторинг процесів надання мережних сервісів з боку державних наглядових органів, проте все ж виникають питання, що пов'язані з ефективною реалізацією безпеки національного мережного сегменту;

- додатковою перевагою впровадження хмарних технологій стає уніфікація доступу до сервісів на основі спрощення ідентифікації юридичних та фізичних осіб в єдиній аутентифікаційній системі національного рівня;

- взаємне об'єднання мережних і обчислювальних потужностей та системна консолідація ЦОД приводитиме до зменшення системних неоднорідностей в точках операторської присутності і, як наслідок, – зменшеної гетерогенності хмарних систем.

Під час трансформації сервісних мережних систем України на основі хмарних технологій виникають п'ять основних категорій організаційно-технічних задач, які повинні бути розв'язані, а саме:

1. Трансформація управлінської культури. Встановлення наглядового контролю з боку державних органів України для супроводу впровадження хмарних технологій у рамках національного сегменту сервісних мережних систем: визначення ключових осіб, їх повноважень, переліку заходів, в тому числі освітнього характеру.

2. Забезпечення функціональної стійкості, інформаційної гарантованості та безпеки. Впровадження політики безпеки щодо контролю над діяльністю хмарних сервісів з боку уповноважених органів у реальному часі, що дозволить виявляти мережні атаки, несанкціоноване втручання в роботу хмарних сервісних систем, проводити системну діагностику та виконувати відповідне реагування на виявлені загрози. Дана задача ставить питання щодо напрацювання офіційного документа, що характеризує політику національної безпеки в сфері інформаційно-телекомунікаційних систем хмарних платформ надання сервісів. Вагомого значення також набуває захист критичної мережної інфраструктури, який, по суті, визначається ступенем режимності об'єктів, які містять обладнання хмарних систем, а також методами

доступу відповідальних працівників до відповідних об'єктів (карткова, двофакторна ідентифікація тощо) і внутрішнього хмарного середовища.

3. Подолання тактичної мережної залежності «останньої милі».

Надання мережних сервісів у тому обсязі, наскільки це дозволяє смуга пропускання мережі доступу, враховуючи можливість проходження деяких операцій без гарантованого підключення, а також в умовах перервних мережних з'єднань.

4. Придбання сервісів та подолання фінансових труднощів.

Фінансування хмарної інфраструктури для надання сервісів за принципом оплати лише затребуваних обсягів послуг. Формування ядра ЦОД для створення та поширення сервісних компонентів з метою економії часу та витрат на впровадження нових сервісів, більш гнучке управління ними. Слід передбачити відмову від фінансування недовантажених та малопродуктивних мережних сервісних компонентів. Контрактна операторська взаємодія B2B і G2B для забезпечення цілісності даних в хмарному середовищі та можливості їх міграції.

5. Міграція даних, сервісів та функціональна прозорість. В рамках розв'язання даної задачі слід передбачити варіативність представлення інформації для її використання на множині різнорідних сервісних платформ, з метою застосування новітніх підходів до оброблення та аналізу даних, отриманих, в тому числі, за рахунок законного перехоплення. Застосування загальнозживаних стандартів перенесення даних, а також дотримання правових норм, зокрема законодавства, що пов'язане із захистом персональних даних [23].

1.2.2. Етапи впровадження хмарних технологій у національному сегменті сервісної мережної інфраструктури

Очевидно, що будь-які трансформації у складних системах не є миттєвими. Не виключення – і трансформації мережного середовища в напрямку утворення хмарної платформи надання сервісів. Передача мережної інфраструктури до

сфери відповідальності провайдерів інфокомунікацій є ефективним рішенням, яке дозволить загострити увагу персоналу, що відповідає за програмне забезпечення не на експлуатації апаратних засобів, які підтримують та надають обчислювальні потужності, а на створенні сертифікованих програмних продуктів для модифікованого мережного середовища. Хмарне мережне середовище (див. рис. 1.10) національного сегменту сервісних мережних систем, за умови дотримання єдиних стандартизованих вимог до впровадження операторського обладнання, є надійною основою для підтримки концепції повсюдного комп'ютингу в різних галузях народного господарства України, а також побудови захищених відомчих інформаційно-телекомунікаційних систем [25].



Рис. 1.10. Хмарне середовище національного сервісного мережного сегменту.

Це середовище (рис. 1.10) містить у своєму складі аналог грид-інфраструктури, що об'єднує компоненти контролю та безпеки, комерційні обчислювальні платформи та точки операторської присутності, партнерські мережі та мережі державних органів.

Розкриємо детальніше етапи впровадження хмарної інфраструктури, які частково вже були нами згадані вище.

1. Початкове впровадження хмарних сервісів: визначення державної стратегії, управлінської структури та шляхів ефективного розвитку, аналіз та розширення користувачької бази, сфер застосування (державні та комерційні сервіси, зокрема e-government).

Основною трудностю впровадження хмарного середовища на національному рівні є необхідність визначення сфер відповідальності державних органів та відомств, а також ключових осіб, що контролюють процеси впровадження національних сервісних систем, міжвідомчу взаємодію та мають достатній набір повноважень для здійснення професійної діяльності у сфері розроблення та реалізації відповідних нормативних документів. Підзвітність таких осіб повинна визначатися актами НКРЗІ. Необхідною виявляється зміна традиційного підходу-парадигми надання послуг, що привнесе інноваційні технології взаємодії суспільства та організацій, враховуватиме специфіку їх діяльності для максимізації системної емерджентності під час реалізації бізнес-процесів, що стають більш уніфікованими, інтегрованими та координованими в дата-центричному мережному середовищі. Стимулювання використання спільного мережного середовища для застосування моделі хмарних обчислень зменшить потреби організацій у специфічній технічній підтримці та виділених фахівцях, зокрема зі сфери системного адміністрування.

Важливим питанням є наукове обґрунтування необхідної системної продуктивності або системної ємності [24], від чого напряду залежатиме необхідний (і достатній) обсяг інвестицій, результати вибору альтернативного системного виконання, її архітектури, відповідного комплексу сервісних компонентів та обсягу послуг сервісної платформи інфокомунікаційного оператора.

Отже, по-перше зменшуються витрати на процес техобслуговування, що передається операторам інфокомунікацій на контрактній основі; по-друге заміщується фінансування основних засобів для розподілених обчислень фінансуванням, що породжується споживанням та наданням відповідних

інфокомунікаційних сервісів у хмарній мережній інфраструктурі; по-третє використання єдиного хмарного середовища викликає потребу у нових підходах до контактування та бюджетування, які приводять до суттєвої економії капіталовкладень та є більш адаптивними, реалізуючи принцип «плати за те, що спожив».

Таким чином, дослідження у порушеній автором проблематиці стосуються одночасно трьох галузей науки: технічної (превалює), державного управління та економічної.

Цікавими є також: соціологічний аспект, який пов'язаний безпосередньо зі споживанням інфокомунікаційних сервісів зацікавленими особами та їх групами, а також методологічний аспект підготовки фахівців на керівні посади, що будуть наділені відповідними компетенціями з оцінювання, підвищення ефективності та планування розвитку хмарного середовища за вищезгаданими загальними критеріями.

2. Оптимальна консолідація національних ЦОД на основі стандартизованих програмних платформ та групи дата-центрів ядра хмарного середовища, що спрощує адміністрування національного сегменту системи, дозволяє відповідну віртуалізацію та консолідацію даних і сервісних компонентів застосувань; крім того зменшується площа потенційних втручань у роботу системи, зокрема різного роду мережних атак.

Стратегія впровадження хмарного середовища в національному мережному сегменті передбачає розміщення ключових сервісних компонентів та даних у ЦОД ядра для їх захисту та контролю відповідних інформаційних потоків. Це дозволить не лише зменшити завантаженість надлишкових периферійних обчислювальних ресурсів, а і підвищити коефіцієнт утилізації власне задіяного програмного забезпечення, інтегрованість програмних платформ за умов постійного моніторингу їх функціонування відділом оперативного системного адміністрування. Стандартизація процесів надання послуг у різних дата-центрах оптимізує внутрішні бізнес-процеси їх

функціонування в загальному. Як наслідок – вища продуктивність ЦОД, менші ймовірності мережних атак за рахунок вдосконалення процесів управління. Слід віддавати перевагу централізації дата-центрів у захищених об'єктах, на противагу розвитку периферійних обчислювальних потужностей. При утворенні нових застосувань або при їх міграції до новостворених ЦОД, властивості мережного середовища дозволять застосуванням мігрувати групами, використовуючи так звані «прив'язані» дані, що будуть автоматично переміщуватись за носіями туди, де вони необхідні. Такий підхід також уможливорює проведення ефективної оперативної діяльності в інформаційному просторі. Концепція «віртуального робочого столу» значно пришвидшує оперативність надання існуючих ресурсів для нових груп користувачів, які користуються єдиним інформаційним середовищем хмарної інфраструктури, не прив'язуючись до їх тактичних параметрів та географічного розміщення.

3. Впровадження консолідованої національної хмарної мережної інфраструктури: інтеграція багатоператорського середовища в рамках консолідації ЦОД, оптимізація надання розподілених сервісів через створену інфраструктуру в рамках прийнятої політики розподіленого використання сервісних компонентів.

Відомою перевагою хмарного середовища є той факт, що воно легко адаптується до деструктивних впливів [26], оскільки апаратна або функціональна відмова одного або кількох вузлів практично не впливає на опірність та функціонування хмарної системи, а саме загальну інформаційну (сервісну) доступність, при цьому ймовірність перебування всієї системи у непрацездатному стані є дуже низькою. Безпека даних та застосувань в єдиному інформаційному середовищі зворотно-пропорційно залежать від складності хмарної системи, а отже прямо пропорційно – від ступеня консолідації та стандартизації програмно-апаратних засобів платформ надання розподілених сервісів. ЦОДи ядра єдиного інформаційного простору хмарного середовища потребують реалізації хмарних функцій шарів IaaS, SaaS, PaaS та функцій кешування (віртуальної реплікації контенту). За такої умови система

володітиме високою масштабованістю (як програмною, так і обчислювальною). Така масштабованість в процесі переходу від традиційної до хмарної сервісної інфраструктури (рис. 1.11) є життєво необхідною в плані утримання основних сервісів і їх супутніх інформаційних потоків під контролем державних наглядових органів, а також для постійного їх вдосконалення на програмно-технологічному рівні, що значно впливає на ресурсозатратність системи [25].

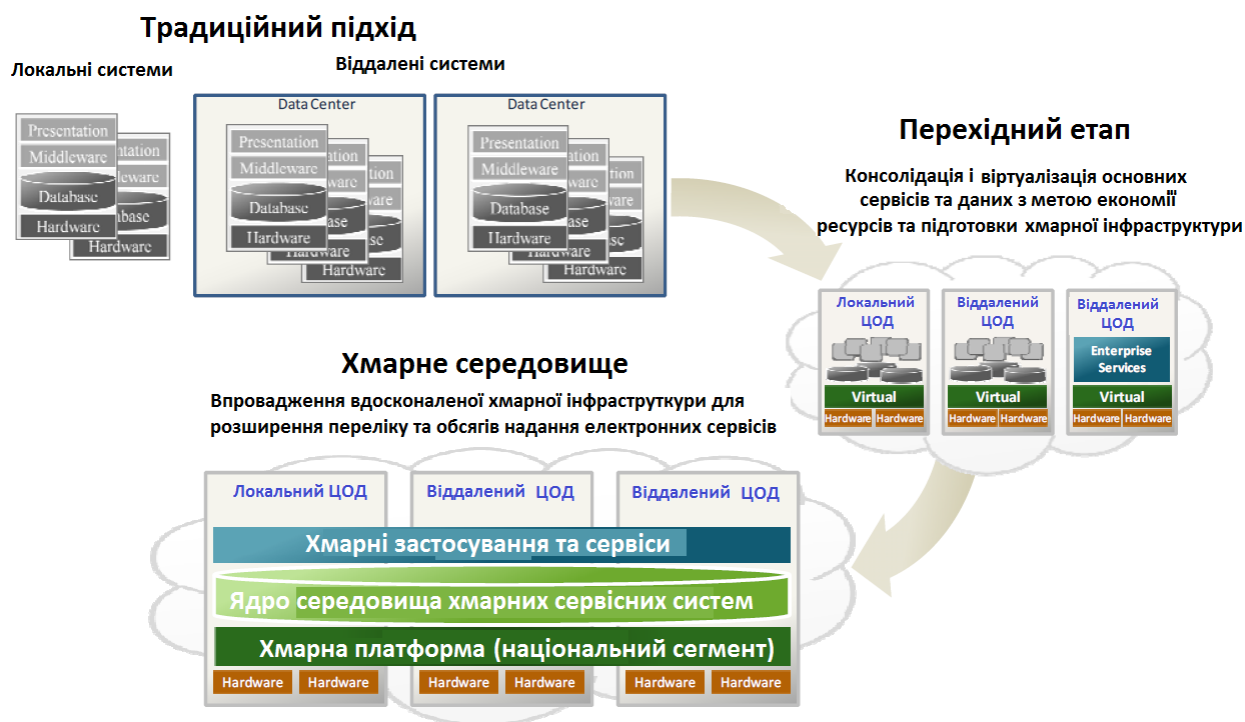


Рис. 1.11. Консолідовані ЦОДи формують основу національного сегменту єдиної хмарної інформаційної платформи [25].

Наглядові органи можуть приймати участь у розподілі навантаження хмарної платформи, формуванні переліку сервісів та контролі за їх наданням, а також їх відповідності (відповідності сервісних компонентів) вимогам гарантованості інформації, зокрема щодо її безпеки та надійності передавання і зберігання. Такий моніторинг повинен бути неперервним, що дозволить оперативно реагувати на потенційні кіберзагрози [17], зокрема загрози конфігурації системи, її телекомунікаційній та обчислювальній складовим.

Варто також акцентувати увагу на дата-центричному аспекті формування хмарної інфраструктури. Стандартизацією форматів представлення даних світове співтовариство розробників хмарних платформ приводить до висновку

про необхідність надання двох основних категорій електронних послуг: операційних сервісів та інформаційних сервісів. До операційних сервісів функціонально відносяться всі три шари IaaS, SaaS, PaaS в контексті технологічної підтримки інформаційного процесу. До інформаційних сервісів фахівці NIST відносять функції шарів SaaS та PaaS. Також примітним є виділення концепту DaaS (Data as a Service), що стосується оброблення так званих даних виду «big data», а також надання доступу до метаданих хмарної системи. Тут слід прокоментувати щодо традиційних сховищ даних у мережі. Вони, де-факто, перестають справлятися з обсягами інформації, поступаючись no-SQL хмарним рішенням DaaS (Google's Big Table, Apache's Hadoop/HBase, Erlang Mnesia тощо). І справа не лише у великих обсягах неструктурованих даних, або слабо структурованої інформації, яку важко обробляти традиційними інструментами, аналізувати, передавати тощо. Справа у безпрецедентній масштабованості і продуктивності хмарних рішень, яка приводить до нової якості таких систем – міжхмарної функціональної прозорості. Все це, очевидно, відбувається за рахунок підвищеного рівня стандартизованості, стійкості та функціональності відповідних програмно-апаратних засобів, незалежно від мети їх застосування, що, в свою чергу, у перспективі дозволяє міжхмарний обмін застосуваннями та інформацією за умови сумісності відповідних середовищ.

4. Підвищення ефективності надання хмарних сервісів: процес виводу сервісних компонентів на обслуговування до сторонніх операторів, підтримка комерційних сервісів, розширення переліку пропонованих мережних сервісів та обсягів їх надання, контроль з боку наглядових органів (НКРЗІ України).

Зусилля регулюючих органів у сфері впровадження хмарних технологій в Україні повинні бути спрямовані на розв'язання таких основних завдань:

- підтримка централізованого управління та функціональної прозорості для всіх хмарних систем національного сегменту сервісної мережної інфраструктури;

- сприяння остаточному перенесенню послуг групи «Triple Play» на IP платформу;

- впровадження та розширення ідентифікаційних сервісів для користувачів електронних сервісів України.

Разом з цим, автору видається доцільним коротко охарактеризувати ризики, що супроводжують новітні трансформації в інформаційно-телекомунікаційному просторі країни. Очевидно, що кібератаки на мережні системи на сьогодні найчастіше є дуже добре спланованими та агресивними. Тому, природно, слід визначити, що комерційні застосування, які експлуатуються операторами інфокомунікацій самостійно, на перших етапах повинні працювати з інформацією, використання якої супроводжується низькими ризиками, оскільки в разі втрати чи витоку вона не чинитиме істотного негативного ефекту на функціонування відповідних суб'єктів господарювання.

З іншого боку, якщо інформація є критично важливою, то її захист потребуватиме спеціальних програмних та апаратних засобів, які, в свою чергу, використовують певний обсяг обчислювальних ресурсів хмарної системи.

1.3. Порівняльний аналіз розподілених архітектур телекомунікаційних сервісних платформ.

У процесах створення технологій надання послуг в мережі наступного покоління бере участь низка організацій зі стандартизації та консорціумів розробників, які об'єднують інфокомунікаційних операторів та виробників програмно-апаратних засобів для телекомунікаційних мереж. Серед найбільш важливих та впливових слід відзначити таких, як Parlay/OSA, OSA, TINA, JAIN Eurescom Project P909, PINT / SPIRITS, а також SPAN [27-39].

Розроблювані даними групами технології надання послуг тісно пов'язані з такими поняттями, як прикладний програмний інтерфейс (API) і сторонні оператори послуг. Інтерфейс програмування додатків – це спосіб, що дозволяє

деякому фрагменту ПЗ звертатися до іншої програми за отриманням деякого сервісу. Це може бути надання доступу до даних або виконання конкретної операції [40]. Історія API розпочалася зі створення TAPI і TSAPI, які були розроблені в 1993-1994 роках фірмами Microsoft і Nowell [27, 41 - 43]. Основними завданнями даних інтерфейсів є організація взаємодії між різними програмними компонентами для надання ряду телефонних послуг. Але, в той же час, на базі цих технологій було можливе створення і більш складних систем, таких, як операторські центри та системи інтерактивної взаємодії з абонентами. Саме ці інтерфейси визначили розвиток технологій. А також - поява нового учасника телекомунікаційного ринку - стороннього провайдера послуг. Даний провайдер послуг повністю звільняється від однієї з найістотніших частин в організації будь-яких телекомунікаційних послуг - реальної взаємодії з елементами мереж. За рахунок відкритого інтерфейсу (в OSA), що йому надається, він здатен управляти мережними елементами, навіть не заглиблюючись у реальні технології надання сервісів. Протоколи взаємодії з мережевими елементами приховані від стороннього оператора, що особливо важливо, якщо в організацію послуги залучені різні мережі, і коли розробленням послуг повністю займаються його розробники. Якби вони займалися вивченням досить складних мережних протоколів, а вже потім реалізовували функціональності сервісів, то їх продуктивність праці була б на надзвичайно низькому рівні. Досить згадати стандарт ASN.1, який використовується, зокрема, в IP-телефонії (SIP+H.323), але конкретне застосування його при створенні власних апаратно-програмних засобів є надзвичайно дорогим або трудомістким.

Таким чином, системи з використанням API інтерфейсів дозволяють використовувати ресурси гетерогенних мереж і відокремити галузь розроблення послуг від області їх застосування, що не тільки розширює кількість послуг, але і значно скорочує час їх впровадження. Серед мережних сервісів, які можуть бути доступні стороннім операторам - послуги управління викликом, локалізації мобільного абонента, доступності терміналу абонента,

відправлення різного роду повідомлень, e-mail, USSD-послуги тощо. Особливість цього підходу полягає у створенні архітектури, за допомогою якої існуючі та інноваційні послуги стануть доступними для використання сторонніми операторами сервісних мережних систем [44-45].

Розглянемо типову сервісну мережну систему на базі Parlay/OSA API з точки зору моделі обслуговування користувацьких запитів (програмно-прикладних викликів необхідних процедур у відповідних сервісних елементах), функціональної площини сервісів і відкритої системної архітектури.

Для мереж PSTN, мобільних мереж зв'язку та IP-мереж модель обслуговування запитів (викликів) з використанням систем Parlay/OSA API може бути представлена, як базовий процес оброблення запитів мережею та процес їх оброблення сервісною логікою Parlay (рис. 1.12).

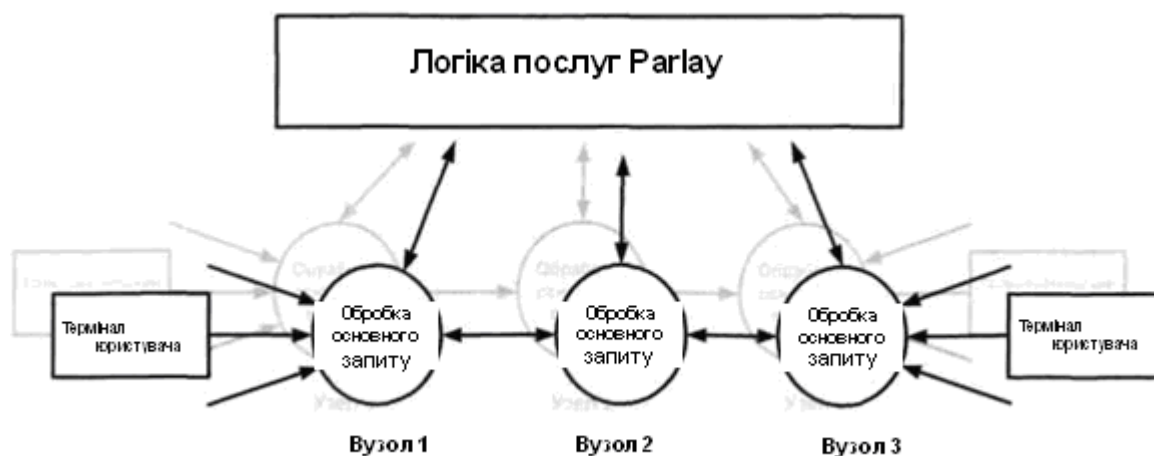


Рис. 1.12. Узагальнена модель обслуговування запитів відповідно до логіки Parlay/OSA.

З точки зору функціональної площини надання сервісів (рис. 1.13), система Parlay API подібна на IN. Для Parlay/OSA систем можливо визначити такі ключові об'єкти:

- Базовий процес оброблення запитів;
- SCF - функціональні компоненти управління сервісами;

- Точки ініціалізації та завершення надання сервісу.

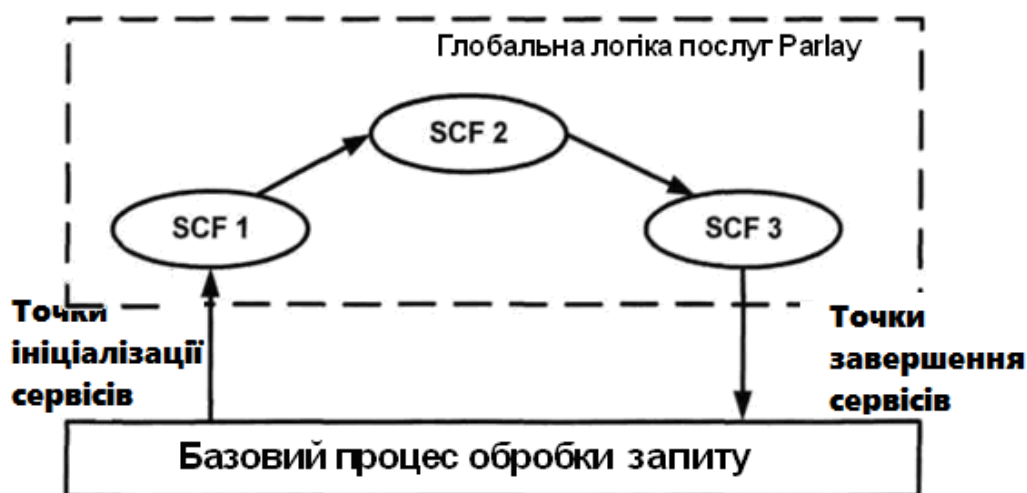


Рис. 1.13. Функціональна площина реалізації сервісів Parlay API.

Функціональні компоненти сервісів реалізуються на основі серверів послуг Parlay API, які підтримують елементарні сервісні компоненти, що можуть бути задіяні при обслуговуванні запитів в необхідній послідовності, визначеній логікою надання сервісу.

На рис. 1.14 представлено узагальнену відкриту сервісну мережну архітектуру з використанням інтерфейсів Parlay API. Основними елементами представленої функціональної моделі є шлюз Parlay/OSA, прикладні застосування і мережні ресурси.

Відкрита сервісна архітектура Parlay API дозволяє надавати мережні послуги сторонніх додатків (в тому числі тих, якими володіють інші оператори) за допомогою адаптованого прикладного програмного інтерфейсу. Основним модулем шлюзу Parlay API є базовий сервер послуг (позначений на рис.1.14 framework), до функцій якого належить авторизація, доступ користувачів та тарифікація використання серверів послуг [46-49]. Для забезпечення виконання цих та інших завдань у Parlay API включений ряд окремих інтерфейсів, класифікація яких представлена на рис. 1.15:

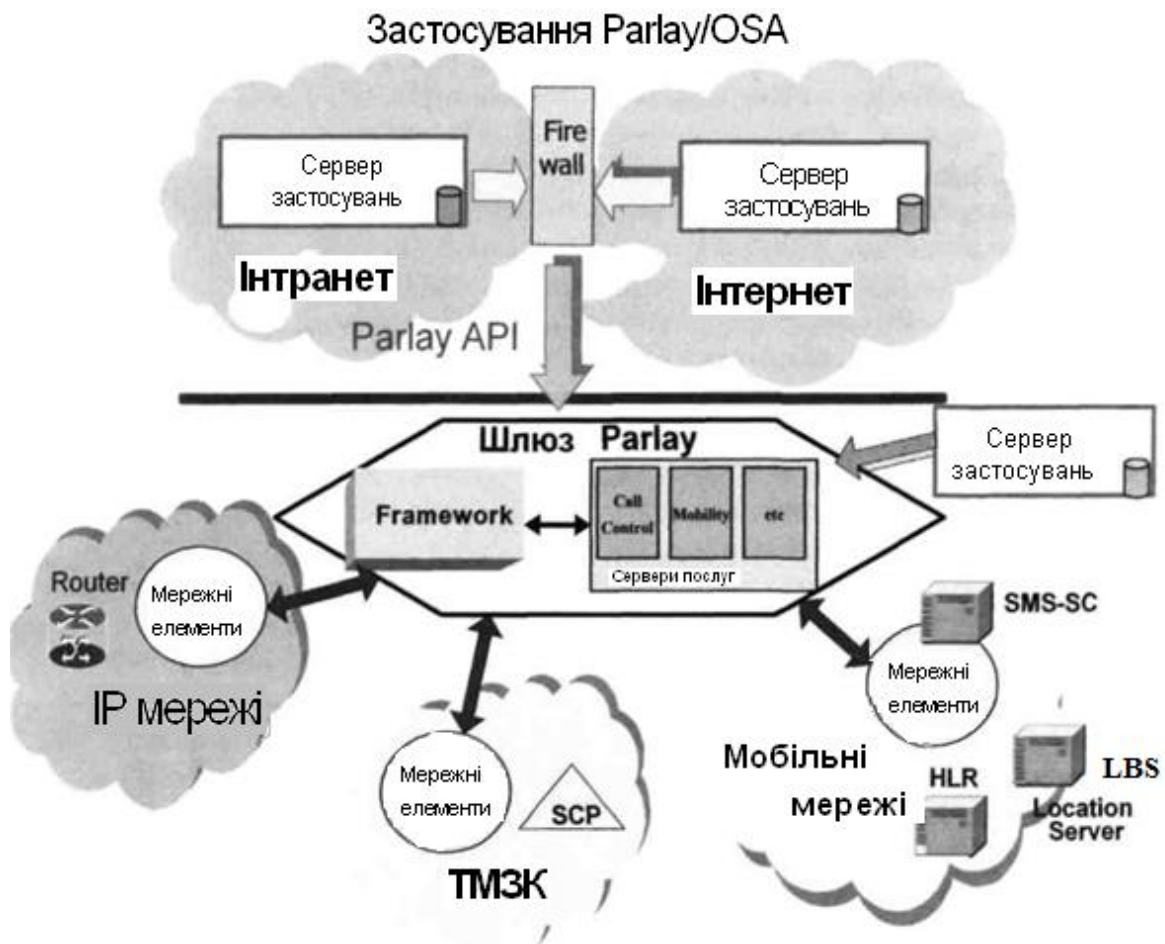


Рис. 1.14. Загальна архітектура надання послуг з використанням Parlay API.

Клас 1. До нього належать інтерфейси між застосуваннями (елементарними сервісними компонентами) і базовим сервером послуг. Ці інтерфейси забезпечують механізми авторизації, доступу користувачів та тарифікацію використання ними електронних сервісів.

Клас 2. Спеціалізовані інтерфейси між застосуваннями і сервісними вузлами (серверами послуг), через які сервісні застосування взаємодіють.

Клас 3. Інтерфейси між базовим сервером послуг Parlay/OSA та сервісними вузлами (серверами послуг), які забезпечують використання обладнання різних виробників.

Клас 4. Інтерфейси між оператором і базовим сервером послуг, які забезпечують оператору управління налаштуваннями сервісів, що надаються користувачам.

І фаза розроблення Parlay API присвячена інтерфейсам між користувачами і серверами послуг (сервісних застосувань) Parlay (інтерфейси 2 на рис. 1.15), а також

базовим сервером послуг (інтерфейси 1 на рис. 1.15).

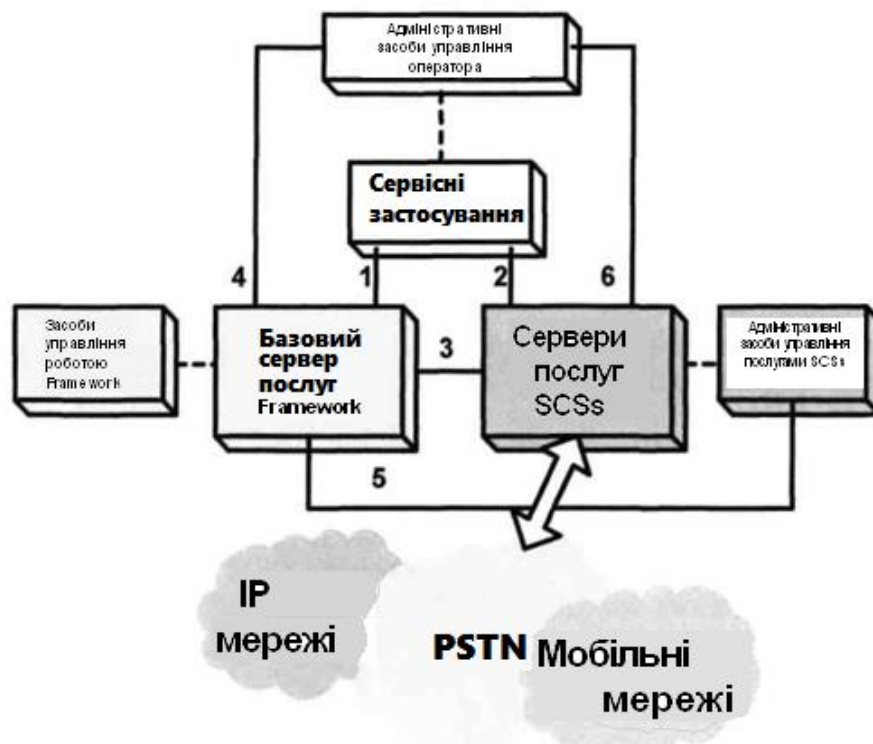


Рис. 1.15. Класифікація відкритих сервісних інтерфейсів Parlay API.

У II фазі були додані інтерфейси для підтримки функцій адміністрування – інтерфейси 4 і 6 на рис 1.15, а також для функцій підтримки сервісів на основі Parlay сторонніми операторами - інтерфейси 3 і 5. Такої ж структури дотримуються й подальші версії.

У такій функціональній моделі Parlay / OSA вже можна виділити наступні елементи: застосування (applications), сервісні вузли – сервери застосувань (application servers), масштабовані сервери послуг (service capability servers). Атрибутом серверів послуг є функціональні можливості серверів послуг (SCF - service capability features). Рис. 1.16 представляє описану структуру.

У третій фазі розвитку Parlay представлено такі функціональні можливості масштабованих серверів послуг (SCF) (кожному SCF відповідає нормативний документ у специфікаціях [50]):

1. Call Control. Функції управління з'єднаннями (простий зв'язок, конференц-зв'язок).
2. User Interaction. Функції взаємодії з користувачем (програвання підказок,

надсилання SMS).

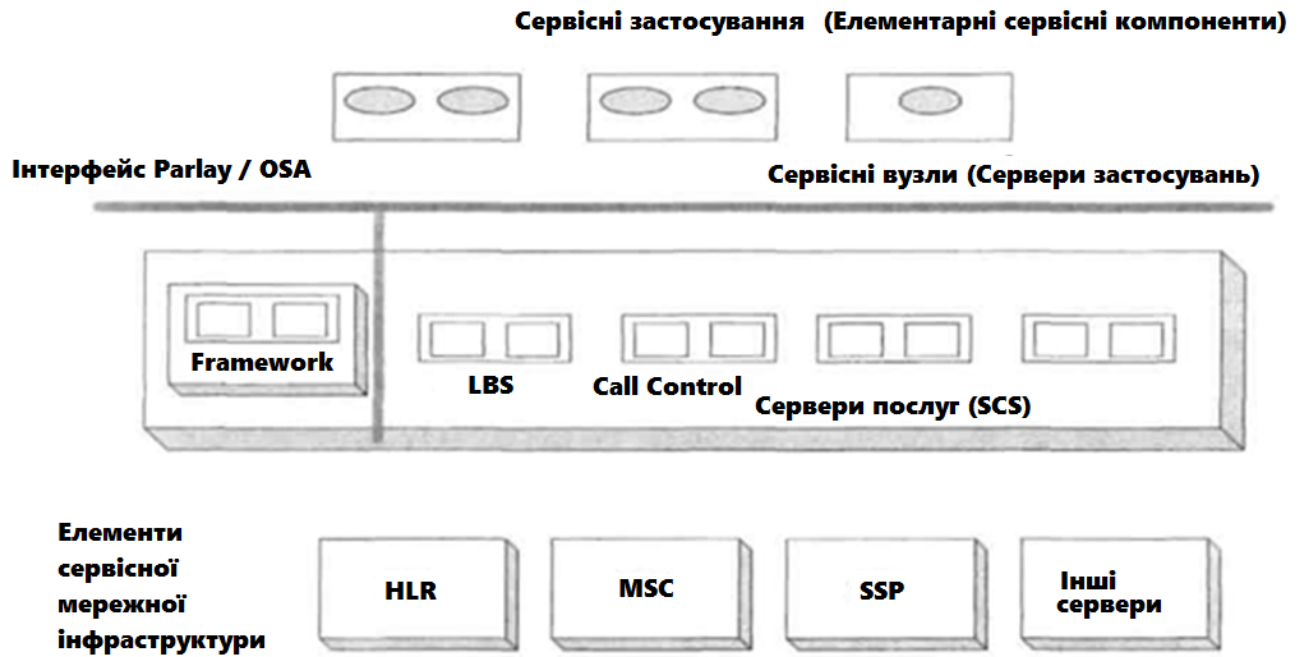


Рис. 1.16. Елементи функціональної моделі Parlay / OSA.

3. Mobility SCF або User location / User status. Опції одержання локалізаційної інформації про користувача та даних про стан його терміналу.

4. Terminal capabilities. Опції отримання інформації про можливості терміналу користувача.

5. Data Session Control. Функції управління сеансом передавання даних.

6. Generic Messaging. Функції роботи з поштовою скринькою (e-mail), в томсу числі голосовою поштою. Використовуються для прийому, передавання та зберігання інформації.

7. Connectivity Management. Функції забезпечення функцій якості сервісу QoS (Quality of Service).

8. Account management. Функції управління рахунками користувачів.

9. Content based charging. Опції тарифікації користування сервісами.

З усього перерахованого вище можливо зробити висновок, що запропонована відкрита сервісна архітектура для розроблення та надання інфокомунікаційних сервісів є однією з найбільш ефективних і зручних як для мережних операторів, так і для сервіс-провайдерів і кінцевих користувачів – юридичних або фізичних осіб, що взаємодіють за допомогою своїх кінцевих пристроїв в рамках концепції повсюдного

комп'ютерингу. Однак, жодні технічні рішення не бувають абсолютними, оскільки, наприклад, універсальність API-інтерфейсів Parlay/OSA може призводити (і зазвичай призводить) до погіршення ймовірно-часових характеристик (ЙЧХ) сервісної мережної системи у порівнянні з індивідуально розробленими та налаштованими для конкретного інфокомунікаційного оператора і для конкретної програмно-апаратної платформи електронними сервісами. Більш прогресивні технічні принципи вимагають значних комунікаційних ресурсів, а це означає, що є важливо досліджувати ЙЧХ платформ надання інфокомунікаційних послуг із застосуванням відкритих API-інтерфейсів, що і було зроблено у розділі 3.1 даної дисертаційної роботи. Більш того, у подальших дослідженнях буде показано, що ЙЧХ систем на базі відкритих API-інтерфейсів залежать від цілого ряду факторів (параметрів трафіку послуг, архітектури сервісної платформи, алгоритмів реалізації сервісів тощо), що робить проведені в наступних розділах роботи дослідження дуже важливими при побудові масштабованих сервісних мережних систем.

1.4. Характеристика та обґрунтування критеріїв оптимального вибору телекомунікаційних технологій шарів: доступу, агрегації, ядра.

У мережному контексті при побудові масштабованих сервісних систем широка множина інфокомунікаційних ресурсів та їх резервів реалізується, як деякий підвид grid-системи, що є інтегральною основою застосування хмарних технологій. Існуючі технологічні компоненти, які працюють в рамках розподілених хмарних платформ дозволяють гнучко надавати послуги для невеликих бізнес клієнтів та цілих транснаціональних корпорацій, причому управління потоками запитів бере на себе сама хмарна система [51]. Таким чином, актуальними є завдання управління продуктивністю сервісних хмарних платформ, такі як оптимізація процесів надання сервісів [52]. Враховуючи розроблення нових платформ надання сервісів (SDPs), які призначені для обслуговування навантаження від множини мереж доступу різного виду з метою надання комерційних електронних послуг, таких як голосові комунікації, передавання даних, широкосмугове мовлення та сервіси мережного управління,

причому з використанням всіх типів користувацького термінального обладнання [53], виникає концепція «Service storm» («Сервісний шторм»). Дана концепція виносить на перше місце модель PaaS, тобто сервісних платформ, які полегшують та пришвидшують гнучке розроблення та впровадження комерційних електронних сервісів на основі використання розробниками технологій відкритого коду [54], використовуючи взаємопідключення серверів, мережного обладнання та СУБД, що працюють під управлінням програмного забезпечення, як правило рівня middleware. У PaaS цим самим забезпечується безпечна взаємодія застосувань, які підтримують більшість відомих бізнес-процесів. Для забезпечення обслуговування цих процесів з відмінною якістю необхідно використати ефективні підходи з прогнозування, економічного позиціонування та гнучкого масштабування SDP реалізацій PaaS моделі, відповідно до потреб ринку. Традиційні підходи до управління потоками та системною продуктивністю стають неефективними. Необхідно не лише забезпечувати якість сервісу та відповідні показники QoS, але й робастність сервісної мережної системи, її технічну ефективність. Даний розділ роботи присвячено визначенню переліку ключових технічних параметрів SDP, які є необхідними для забезпечення ефективності її функціонування в рамках додержання укладених угод SLAs.

Сервісні мережні системи, в рамках парадигми інформаційної взаємодії бізнес-процесів, формують нові принципи організації розподілених мережних сервісних платформ. Зокрема, одним із важливих їх прикладних застосувань у сфері народного господарства є системи електронного урядування, що забезпечують гнучку інформаційну взаємодію державних структур, у відповідності до потреб населення держави. Як вже було зазначено, для того, щоб найбільш повно відчувати структурно-функціональні переваги застосування розподілених (хмарних) платформ надання послуг на основі потужних апаратних засобів (серверних систем), необхідним є забезпечення заданого рівня якості обслуговування у межах сервісної платформи для адекватного оброблення кожною СМО або ж MeMO свого потоку запитів-завдань під

управлінням відповідної сервісної програмної архітектури. Принципи побудови та розрахунку відкритих інтерфейсів у межах сервісної архітектури докладно досліджено у 3-му розділі даної дисертаційної роботи.

1.4.1. QoS і підходи до управління потоками завдань у сервісній мережній платформі.

Будь-яка архітектура, що реалізується у формі сервісної мережної платформи породжує задачі управління потоками завдань. Існує декілька *параметрів-критеріїв*, забезпечення яких є необхідним для дотримання рівня якості сервісу у відповідності із домовленими технічними специфікаціями.

Одним з них є *час затримки потоку завдань*, що складається з часу розподілу потоку при його маршрутизації у розподіленій сервісній структурі та часу оброблення запиту в СМО сервера застосувань (або MeMO серверів, на яких розміщено елементарні сервісні компоненти), яка його приймає на обслуговування в рамках одного з етапів оброблення метазапиту з базового серверу послуг. Подібні задачі управління потоками вивчались у численних роботах, таких як [55-57]; аналіз функціонування сервісних інтерфейсів був виконаний [58-60], разом із розглядом основних архітектурних концепцій для розподілених сервісних платформ, зокрема в рамках концепції технологічної сервісної шини.

Наступна задача полягає у забезпеченні необхідного рівня *функціональної стійкості та інфраструктурної надійності*. Мережі з комутацією пакетів гарантують, що при коректному обранні параметрів інфраструктури, що реалізується на основі них, апріорі досягається деякий обумовлений рівень надійності. Це може бути підтверджене ранніми дослідженнями US DARPA [61], але основною задачею є гарантування функціональної сервісної надійності шляхом забезпечення коректної параметризації сервісних програмно-прикладних серверних вузлів. Сервісні вузли є подібними до вузлів управління та маршрутизації потоків завдань. Вони також мають, як і будь які інші СМО, буфери, що технологічно обмежені за об'ємом. Ієрархічна структура сервісних

мережних платформ викликана вимогами високої масштабованості та диверсифікації функціонального доступу, агрегації потоків навантаження, а також завданням розподілу мультисервісного контенту. Прямим наслідком використання такого виду структур є диференціація властивостей мережного трафіку на кожному з рівнів мережної моделі. Відповідно, параметри сервісних вузлів платформи PaaS повинні дещо відрізнитись від параметрів вузлів інфраструктури доступу IaaS з метою забезпечення відповідних параметрів якості сервісу: *системної продуктивності та сервісної доступності*. Тому завдання вибору (розрахунку) цих параметрів є вагомою при забезпеченні сервісною архітектурою необхідного рівня якості сервісу.

Зрозуміло, що мережі з комутацією пакетів є основою для будь-якої сервісної інфраструктури, принаймні на найближчу осяжну перспективу. Однією з основних проблем управління потоками завдань у мережах з пакетною комутацією є складність забезпечення можливості гарантування затримки передавання інформаційних потоків запитів в процесі їх оброблення, тоді як число запитів користувачів до серверів послуг, що особливостями свого структурного розташування зумовлюють створення потоків, зростає експоненційно із розвитком мережної інфраструктури.

Для випадку мультисервісного трафіку важливим є дослідження його *статистичних властивостей*, які впливатимуть на необхідні вимоги до механізмів гарантування функціональної якості сервісу, що надається застосуваннями у деякому інформаційному потоці запитів. І ці параметри також мають бути прийняті у якості базових в процесі планування мережних ресурсів.

Для опрацювання ситуацій, коли затримки обслуговування потоків завдань, і, відповідно, затримки, що зумовлені самими завданнями в обслуговуючих пристроях на їх сервісних інтерфейсах будуть перевищувати допустимі (у випадку недостатньої кількості ресурсів) в умовах зростання кількості користувачів ми можемо визначити два основних шляхи:

- використання більш швидкої сервісної інфраструктури та більш продуктивних сервісних інтерфейсів, що не завжди, як правило, є економічно-виправданим;

- використання альтернативних конфігурацій (архітектур) сервісних мережних платформ PaaS (або ж SaaS в межах ЦОД) для оброблення потоків завдань, що, в загальному, враховуючи достатню кількість сервісних інтерфейсів можуть забезпечити наскрізну затримку опрацювання запитів користувачів та функціональні показники у відповідності до заданих норм.

Такі принципи організації управління потоками завдань та конфігураціями розподілених сервісних мережних платформ можуть бути отримані за допомогою спеціальних алгоритмів маршрутизації потоків завдань, або іншими словами - алгоритмів управління цими потоками. Цей підхід потребує дослідження мережної інфраструктури сервісної платформи з урахуванням її структурної моделі, або топологічних властивостей організації розміщення сервісних вузлів (серверів прикладних програм) під управлінням базового (шлюзового) сервера послуг. При просторовому розміщенні сервісних вузлів у просторі та їх конфігуруванні, як правило, повинні формуватись недовантажені ділянки з меншими затримками опрацювання потоків задач [55-57]. Таким чином, процеси розподілу і оброблення зазначених потоків необхідно дослідити більш детально.

1.4.2. Особливості використання ресурсів телекомунікаційної сервісної платформи мультисервісними потоками.

Розглянемо більш детально проблематику використання ресурсів сервісної мережної платформи для кожного з вищенаведених параметрів якості обслуговування. Узагальнена модель розподілу трафіку показана на рис. 1.17. Даний рисунок демонструє формування мультисервісного потоку пакетів та його оброблення у сервісному вузлі мережної інфраструктури сервісної платформи.

Кожне застосування користувача генерує впорядковану послідовність пакетів з рівними пріоритетами обслуговування. Агрегування цих впорядкованих послідовностей у єдиний мультисервісний потік відбувається на наступному етапі. Пріоритети обслуговування в цьому потоці вже є різними. Узагальнений потік має доволі стохастичний характер за характером застосувань, що його формують. Проте, сучасні сервісні мережні системи застосовують принципи розпаралелення для оброблення кількох запитів одночасно.

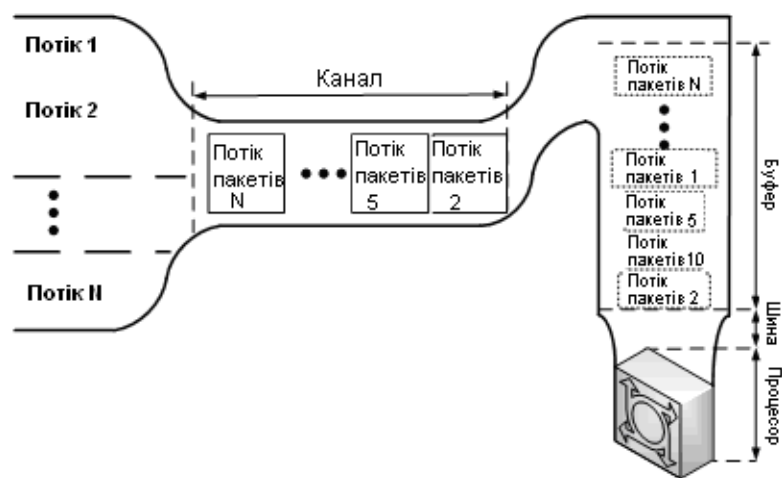


Рис. 1.17. Модель розподілу мультисервісного трафіку в SDP.

Сервісний вузол надає необхідні ресурси для гарантування якості сервісу при обробленні мультисервісних потоків. Таким чином, дана модель може бути застосована для постановки задачі визначення загальної необхідної кількості застосувань, що оброблятимуть мультисервісний потік запитів, або, за умови фіксованої кількості застосувань, вона може дати відповідь на питання про кількість потоків, що може бути оброблена деяким сегментом SDP. Пропонується розглядати окремо різні режими формування мультисервісних потоків. Перший нагадує віртуальну комутацію каналів. Він представлений на рис. 1.18. Агрегований потік є результатом послідовного використання ресурсів кожним диференційованим потоком. Дана система обслуговування є безпріоритетною по відношенню до різних пакетів і вони втрачаються лише у критичних (аварійних) ситуаціях.

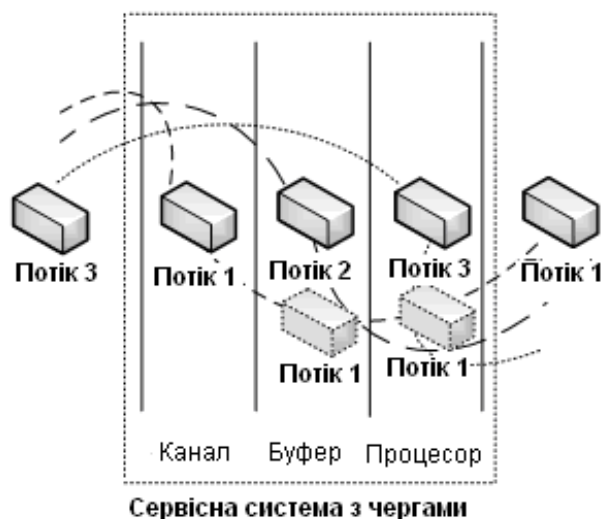


Рис. 1.18. Формування мультисервісного потоку в SDP у режимі віртуальних каналів.

Другий режим представляє ситуацію одночасної генерації пакетів користувацькими застосуваннями та їх об'єднання у єдиному потоці. У цьому випадку різні пакети деякого сервісного запиту можуть використовувати різні ресурси сервісного вузла одночасно (див. рис. 1.19). Представлений процес є абсолютно стохастичним. Тому задача гарантування параметрів якості обслуговування тут є складною.

Варто зауважити, що параметри якості сервісу для трафіку мають бути забезпечені вибором відповідної структурної та функціональної конфігурації параметрів сервісної мережної платформи та її окремих сервісних вузлів, які можуть розгортати, для прикладу, деяку множину віртуальних машин.

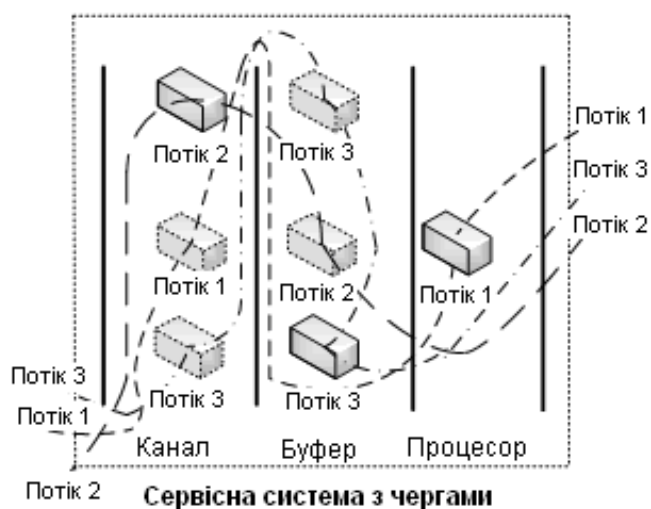


Рис. 1.19. Паралельна генерація пакетів та їх об'єднання в єдиний агрегований потік у межах SDP.

1.4.3. Підходи до моделювання та параметризації мережної інфраструктури сервісної платформи.

Мережна платформа сервісної інфраструктури в загальному базується на принципах магістралей та ієрархій, з метою мінімізації обміну сервісними потоками у просторово-розподіленій структурі, що може призвести до погіршення якості їх обслуговування елементами з обмеженою кількістю ресурсів. Таким чином, сервісна інфраструктура має бути спроектована для максимізації ефективності дорогого транспортного сегменту сервісної платформи, який повинен використовуватись максимально ефективно.

Сервісна мережна інфраструктура, або ж мережна платформа можуть бути формалізовані у вигляді граф-моделі на основі матриць суміжності, як мережі зв'язків між сервісними вузлами (у PaaS), а в загальному - між сервісними інтерфейсами та транзитними вузлами для обміну потоками завдань (у IaaS) [62].

Отже, одним з найбільш важливих завдань подальших досліджень є визначення основних параметрів сервісної мережної системи на основі структурного моделювання її основних обслуговуючих шарів та їх оптимізація для забезпечення показника якості обслуговування за критеріями: часу розповсюдження та обслуговування потоків завдань із врахуванням прогнозного рівня завантаження ресурсів сервісної інфраструктури та їх реальних показників, статистичних параметрів навантаження; а також цільових рівнів системної продуктивності та узагальненої сервісної доступності.

1.5. Висновки до 1-го розділу.

1. Будь-яка сервісна мережна система вимагає оптимізації за критеріями продуктивності та сервісної доступності, а також часу розповсюдження та обслуговування потоків завдань, із врахуванням статистичних параметрів навантаження, реалізуючи архітектуру телекомунікаційних систем SDP з розпаралеленим обробленням потокового трафіку різних видів, зокрема з використанням принципів NFV. Аналіз проблематики ефективного управління

системами такого роду викриває протиріччя щодо впровадження повсюдного комп'ютингу при одночасному скороченні споживання обчислювальних ресурсів хмарних телекомунікаційних платформ і розширенні переліку та обсягу задач оброблення інформації, що повинні розв'язуватись в рамках надання розподілених сервісів. Виявляється, що методологія, інструменти, навички і процеси, які використовувались для управління сервісними мережними системами (застосуваннями, платформами, інфраструктурою) протягом багатьох років стають неефективними. А відмови інфокомунікаційної сервісної мережної системи призводять до нищівних наслідків для користувачів, підприємств, державних відомств, національної економіки. Розв'язання сформульованого протиріччя є ключовим на думку багатьох науковців, створюючи передумови для підвищення якості сервісу, безпеки та продуктивності масштабованих телекомунікаційних сервісних платформ, особливо враховуючи специфіку їх національного сегменту. Отже, наукова проблема розроблення методологічного забезпечення синтезу телекомунікаційних сервісних платформ національного рівня для оптимального впровадження концепції повсюдного комп'ютингу (розподілених обчислень) із заданими рівнями якості сервісу, продуктивності та функціональної стійкості, є актуальною і своєчасною.

2. У розділі показано, що створення хмарного середовища в національному сегменті сервісної мережної інфраструктури є фундаментальним аспектом подальшого стратегічного розвитку інфокомунікаційного простору України. Адже передумовою ефективного розвитку електронних сервісів є сукупність організаційних заходів, які спрямовані на консолідацію апаратно-програмних засобів з метою створення масштабованої за обчислювальною потужністю хмарної системи на основі гетерогенної мультиоператорської платформи, що поєднується високим рівнем функціональної прозорості (в перспективі - до міжсистемного або «міжхмарного»). Створення єдиного інформаційного середовища хмарної сервісної мережної системи передбачає дата-центричну модель (в перспективі DaaS), яка містить ядро на основі довірених ЦОД, котрі

володіють необхідним рівнем захищеності та функціональності, поширюючи відповідну політику на всі об'єднані ЦОД різних операторів хмарної мережної системи в рамках національного сегменту за рахунок інтеперабельності, яка дозволяє надавати послуги в обсягах, що необхідні саме тут і зараз, шляхом реплікації та міграції відповідних сервісів і пов'язаних даних (в тому числі міжоператорської та крос-платформної). Хмарна інфраструктура потребує неперервного моніторингу, оперативного системного адміністрування, а її розвиток – ефективного державного нагляду з боку контролюючих органів, зокрема в галузі мережної безпеки, наприклад НКРЗІ.

3. Для більш ефективного масштабування хмарної мережної системи необхідно користуватись послугами сторонніх інфокомунікаційних операторів, що дозволяє оперативно нарощувати необхідні обчислювальні потужності відповідно до поточних потреб, але потребує вироблення нормативних та регулятивних документів. Також потребують подальшого дослідження методи оцінювання та підвищення параметричних показників ефективності масштабованих хмарних сервісних систем. Необхідним є врахування новітніх інфокомунікаційних технологій, що дозволяють адаптувати системну архітектуру до надання більших обсягів та різновидів послуг у безпечному сегменті національної сервісної мережної інфраструктури, що пов'язане, зокрема, з реалізацією концепції IoT.

4. Перспективна архітектура мереж наступного покоління (NGN) передбачає створення телекомунікаційної сервісної платформи з відкритим інтерфейсним винесенням функціональності послуг в граничні вузли мережі, створенням спеціальної підсистеми управління послугами у вигляді окремої мережної підсистеми, а також розширенням номенклатури інтерфейсів для підключення устаткування різних (конкуруючих) постачальників послуг. Відкриті інтерфейси, що найбільш активно розвиваються останнім часом надають змогу розгортання та розвитку інфокомунікаційних сервісів, які складають основу відомчих та бізнес порталів, а також добре зарекомендували

себе у реалізації концепцій надання державних послуг фізичним та юридичним особам.

5. Сервісні мережні системи створювались як новий клас інфокомунікаційних рішень із забезпеченням можливості взаємодії з існуючими мережами. З іншого боку, вони потребують вивчення питання формування точок присутності на існуючих операторських мережах зв'язку, а рівно і використання та модернізації існуючих транзитних мереж доступу для організації підключення до сучасних гетерогенних мережних платформ. Таку тенденцію, зокрема, демонструють оператори хмарних систем, наприклад, Google, який орендує для надання сервісів в Україну власні міжнародні канали. Особливістю сучасних послуг, що надаються телекомунікаційними сервісними платформами, є їх незалежність від способу доступу, що вивело мережі доступу в самостійний клас мереж зв'язку.

6. Системи управління телекомунікаційними сервісними платформами повинні будуватися за тими ж основними принципами, що і самі мережі, тобто мати модульну архітектуру з використанням відкритих інтерфейсів між модулями. При цьому, створення мереж такого виду вимагає формування узгодженої технічної політики, розробки питань мережної безпеки, які регламентуються основними нормативними документами, що визначають надання електронних сервісів державними структурами, що пов'язано з наявністю великого числа конкуруючих і не до кінця розроблених стандартів. Розроблені на сьогодні концептуальні положення визначають перелік і етапи виконання завдань формування національної нормативно-технічної бази, включаючи їх практичне опрацювання в рамках окремих НДР і пілот-проектів. Доцільним також є перехід до горизонтальної системи регулювання, як до механізму, що дозволяє врахувати особливості надання різних послуг в неоднорідних мережах. У якості першочергових завдань, що відносяться до регламентації процесів надання послуг в розподілених сервісних мережних системах, доцільно розглянути питання реалізації механізмів підвищення якості

реалізації універсальної послуги, послуг приєднання та забезпечення мережної безпеки при наданні користувачам сервісів доступу та передавання мультисервісних даних (в рамках надання відповідних інфокомунікаційних послуг). Актуалізується проблематика синтезу програмно-прикладних сервісних платформ національного рівня конфігуруванням структури та параметризацією апаратних і програмних компонентів масштабованих мережних рішень, приймаючи до уваги оптимізацію інфокомунікаційних процесів взаємодії серверів послуг/сервісних застосувань (на рівнях SaaS, PaaS, IaaS) при наданні послуг через відкриті системні інтерфейси за критеріями якості сервісу (з урахуванням сервісної доступності), системної продуктивності та функціональної стійкості.

7. У розділі розглянуто відкриту сервісну архітектуру систем для розроблення та надання інфокомунікаційних послуг на базі Parlay/OSA, що є однією з найбільш ефективних і зручних як для мережних операторів, так і для операторів послуг і кінцевих користувачів – юридичних або фізичних осіб, що взаємодіють за допомогою своїх кінцевих пристроїв в рамках реалізації концепції повсюдного комп'ютингу.

8. Описано основні залежності між параметрами розподіленої сервісної платформи та показниками якості обслуговування у ній. Виконано аналіз різних режимів формування мультисервісних потоків запитів і їх вплив на QoS. Ефективне та правильне конфігурування телекомунікаційної сервісної платформи (як відповідних фізичних інтерфейсів, так і розподілу сервісних потоків) може бути реалізоване шляхом розрахунку її необхідних параметрів на основі структурно-функціональних та математичних моделей сегментів розподіленої сервісної мережної інфраструктури, що дозволить оптимізувати показники якості сервісу, запобігати відмовам у обслуговуванні, наприклад, типу DoS в умовах інтенсивного зростання числа користувачів.

РОЗДІЛ 2

Моделювання імовірно-часових характеристик телекомунікаційних сервісних платформ

2.1. Дослідження методів підвищення продуктивності розподілених сервісних мережних систем.

Злиття послуг фіксованого та мобільного зв'язку в єдиній конвергентній мережній платформі, швидке поширення електронних послуг, зокрема в рамках концепції повсюдного комп'ютингу практично на всі галузі народного господарства висунуло надконвергентний принцип «одна людина - один термінал», який швидко еволюціонує в Інтернет речей, *англ.* Internet of Things (IoT). Проблема конвергенції (взаємопроникнення) мобільних і фіксованих мереж, а також мереж передавання даних в рамках реалізації хмарних обчислювальних та телекомунікаційних сервісів, стала підґрунтям для появи цілої палітри сучасних інфокомунікаційних платформ, яка успішно розвивається, охоплюючи все нові функціональні області, включаючи визначення місцеположення (LBS) і мобільну комерцію, як частину парадигми електронного бізнесу [64-66].

Відповідно до [64], сучасна конвергенція мереж пов'язана із забезпеченням мережних і сервісних можливостей, що не залежать від технології доступу. Це не обов'язково передбачає фізичну конвергенцію мереж і визначає розвиток ринку мережних можливостей та відповідних стандартів. Набір стандартів може бути використаний для впровадження ряду мережних послуг через фіксований або мобільний доступ до відповідних операторських мереж, мереж загального користування або приватних мереж [67].

Архітектура надання послуг абонентам в умовах конвергенції мережних систем (на типовому прикладі мереж мобільного зв'язку) містить чотири рівні [68]: рівень користувача, рівень інформаційної мережі (ІМ), рівень мережі сигналізації (МС) і рівень формування послуги з використанням відповідних сервісних систем та баз даних:

- На рівні користувача здійснюється взаємодія користувачів з відповідними телекомунікаційними мережами;

- На рівні ІМ стаціонарні та мобільні мережі з'єднуються спільними інформаційними каналами, утворюючи конвергентну сервісну мережну систему;

- Їх взаємодія при встановленні з'єднань, підтримці інформаційних потоків забезпечується на рівні МС;

- Надання сервісів здійснюється на рівні формування послуг.

Традиційно, в сучасних умовах оператори інфокомунікацій після якомога більш широкого охоплення аудиторії користувачів, фокусують свою увагу на додаткових послугах, використовуючи для цього всі існуючі технічні можливості та ресурси, зокрема концепцію інтелектуальних мереж (Intelligent Network- IN) [69]. Для інтелектуальних мереж (IN) був розроблений протокол користувача інтелектуальної мережі INAP. Він визначає процедури взаємодії модуля управління послугами (SCP) з модулем комутації послуг (SSP), і з модулем зберігання даних для послуг (Service data point - SDP) [70]. При застосуванні концепції IN до телекомунікаційних сегментів хмарних сервісних систем забезпечення збереження профілю послуг пов'язане з рядом труднощів.

По-перше, на відміну від традиційних мереж зв'язку, в платформах хмарних сервісів точки надання сервісу і профіль послуг, як правило, не є статично заданими, а визначаються динамічно при підключенні користувача. Інтелектуальні та функціонально-параметричні можливості «домашнього» і «гостьового» сегментів доступу хмарних сервісних систем можуть виявитися різними, що, швидше за все, позначиться на переліку та на характеристиках послуг, які зможуть бути запропоновані користувачеві, що перемістився в «гостьовий» сегмент системи, зокрема з використанням мережі рухомого доступу. По-друге, в процесі обслуговування запитів користувача може брати участь більше, ніж одна інтелектуальна сервісна мережна платформа.

Ефективність будь-якої розподіленої сервісної мережної системи характеризується великим числом критеріїв. Це ускладнює розв'язання задачі

оптимізації використання мережних ресурсів у загальному випадку і дослідження впливу окремих критеріїв на загальний результат.

Для оцінки ефективності використання мережних ресурсів, як правило, користуються двома критеріями:

- Якість обслуговування Q , що може виражатися як імовірністю відмов, так і іншими інтегральними характеристиками;

- Прибутковість сервісної мережної системи P , що являє собою різницю вартості наданих послуг і витрат (інтегральна системна продуктивність).

Якість обслуговування по суті є інтегральною властивістю мережі, при якій вона зберігає здатність надавати набір послуг у відповідності до умов, які визначені угодою SLA про необхідний рівень сервісу (тобто – потенційною можливістю мережі забезпечувати задані експлуатаційні характеристики). З метою кількісного оцінювання показника якості обслуговування можна використати деякий коефіцієнт Ψ . При перевантаженні мережі службовим трафіком (сигнальними повідомленнями), який необхідний для надання сервісів, коефіцієнт Ψ знижується, а при перевантаженні мережної системи породженими інформаційними потоками – збільшується. Для стійкої роботи сервісної мережної системи цей коефіцієнт не повинен значно змінюватися, тобто якість обслуговування можливо оцінити ступенем його флуктуацій (чим нижче флуктуації Ψ , тим краще):

$$Q = 1 - \frac{|\Delta\Psi|}{\Psi}. \quad (2.1)$$

При цьому інтегральну системну продуктивність, тобто прибуток сервісної мережної системи можливо визначити, як різницю доходів від користувацької бази і витрат на обслуговування та залучення нових користувачів.

Фізичний зміст коефіцієнта Ψ з (2.1) – це відношення середньої тривалості зайняття каналних ресурсів сервісної мережної системи до середнього часу очікування надання сервісу. Коефіцієнт Ψ можливо визначити експериментально для конкретної мережі, задавшись відповідно до норм SLA максимально допустимим часом очікування надання сервісу, а також

визначивши експериментально середню тривалість зайняття каналних ресурсів сервісної мережної системи. У загальному випадку значення коефіцієнта Ψ залежить від багатьох факторів: повної інтенсивності вхідного навантаження; його розподілу між вузлами обслуговування (зокрема, перекосу навантаження); середньої тривалості зайняття каналних ресурсів під час обслуговування користувачів; імовірності зайнятості (недоступності) серверних систем, зокрема некоректного опрацювання запитів; існування супутникових ланок в мережній платформі та інших.

Очевидно, що підвищення якості обслуговування користувачів приводить до необхідності збільшення витрат операторів сервісних мережних систем і, як наслідок, до зниження прибутковості мережі. Тобто, розглянуті критерії є взаємно суперечливими, що приводить до багатокритеріальної (векторної) задачі їх оптимізації [71]. Таким чином, в подальшому з метою спрощення міркувань пропонується прийняти якість обслуговування на рівні не нижче допустимого, що є характерним для більшості сучасних телекомунікаційних мереж хмаринкових сервісних систем внаслідок використання множини спеціальних технологій [72]. Найбільш суттєвим технічним показником ефективності в такому випадку виступає мережна продуктивність.

Мета даного розділу роботи – проаналізувати методи покращення основного показника ефективності сервісних мережних систем, а саме їх продуктивності. У відповідності до поставленої мети, в роботі визначаються найбільш оптимальні підходи, що їх можливо застосовувати у хмарних сервісних системах, які останнім часом зазнають стрімкого функціонального та структурного масштабування.

2.1.1. Аналіз існуючих методів підвищення продуктивності телекомунікаційних сервісних платформ.

Як вже було наголошено, основною характеристикою будь-якої мережі зв'язку, як системи розподілу інформації, є ефективність її функціонування. Основними критеріями ефективності телекомунікаційної системи з технічної

точки зору визначимо її продуктивність і пропускну здатність. Дамо їх аналітичне визначення. Згідно [68] під пропускну здатністю мережі зв'язку розуміємо

$$D = \sum_{\forall i,j} c_{ij} l_{ij},$$

де c_{ij} - номінальна пропускну здатність лінії в біт / одиницю часу, або Ерл при заданій якості обслуговування; l_{ij} - довжина лінії в м.

Під продуктивністю телекомунікаційної мережі зазвичай розуміємо навантаження, що обслужене одиницею довжини мережі за певний час:

$$\Pi = \sum_{\forall s,t} V_{st} l_{st} / T ,$$

де V_{ij} - обсяг переданих (обслужених) за час T повідомлень (в бітах або Ерл) між пунктами a_s і a_t ; l_{st} - довжина найкоротшого шляху між цими пунктами (в м). Час T вибирається залежно від поставленого завдання, аналогічно – міра довжини.

Звичайно при розрахунках необхідної продуктивності обладнання використовується його пропускну здатність в ГНН. З погляду ефективності роботи мережі нас цікавить середньодобова пропускну здатність, при цьому для її підвищення необхідне «часове розмиття» коефіцієнта концентрації навантаження. Нагадаємо, що під коефіцієнтом концентрації навантаження розуміється відношення навантаження, пропущеного мережною системою в ГНН до загальнодобового навантаження [71]: пропускну здатність мережі може бути оцінена в ГНН, або за добу. Існують також методики, що ґрунтуються на тривалих проміжках часу оцінювання навантаження. У даній роботі під пропускну здатністю хмарної сервісної мережної системи розуміється навантаження, обслужене мережею за добу із заданою якістю. Одним із показників, що характеризує ступінь завантаженості обладнання сервісної платформи протягом доби, є коефіцієнт концентрації навантаження [72, 74], який визначає ступінь концентрації навантаження в ГНН $k_{ГНН} = u_{ГНН} / u_{ДОБ}$, де $u_{ГНН}$ - величина навантаження за ГНН; $u_{ДОБ}$ - величина навантаження за добу. Величина даного коефіцієнта в основному залежить від структурного складу

користувачів системи і лежить в межах 0,09-0,15. Для того, щоб необхідні обсяги та продуктивність обладнання системи були мінімальними, а його завантаження - рівномірним, величина коефіцієнта концентрації повинна бути мінімальною.

Можна зробити висновок, що чим більш рівномірною є зміна коефіцієнта $k_{ГНН}$ протягом доби, тим вищою є пропускна здатність сервісної мережної системи.

Основні методи підвищення середньодобової пропускної здатності для сучасних сервісних мережних систем показані на рис. 2.1 [68, 73].

Перший метод заснований на тому факті, що в більшості мережних систем ГНН для різних категорій користувачів не збігаються. Тому в цих мережах часто застосовують балансування якісного складу користувачів різних категорій, яких обслуговують тими ж самими мережними сегментами. Для хмаринкових сервісних систем та їх телекомунікаційних платформ поділ користувачів на категорії поки не є вираженим. Спроби здійснити бізнес експлуатацію хмаринкової сервісної системи на сьогодні відбулися де-факто в компанії Google, проте в країнах, які розвиваються великого успіху даний підхід поки що не набуває. Якщо для мереж рухомого зв'язку в даний час навантаження в ГНН розраховується за питомим інформаційним навантаженням, однаковим для всіх користувачів (0,015 Ерл), то для хмаринкових сервісних систем такий підхід не завжди може принести адекватні результати, потребуючи додаткових міркувань, вхідних даних і більш складних розрахунків.

Другий метод - пільгові тарифи - застосовується в мережах зв'язку, де практикується погодинна оплата використання ресурсів для вирівнювання коефіцієнта концентрації навантаження протягом визначених часових інтервалів.

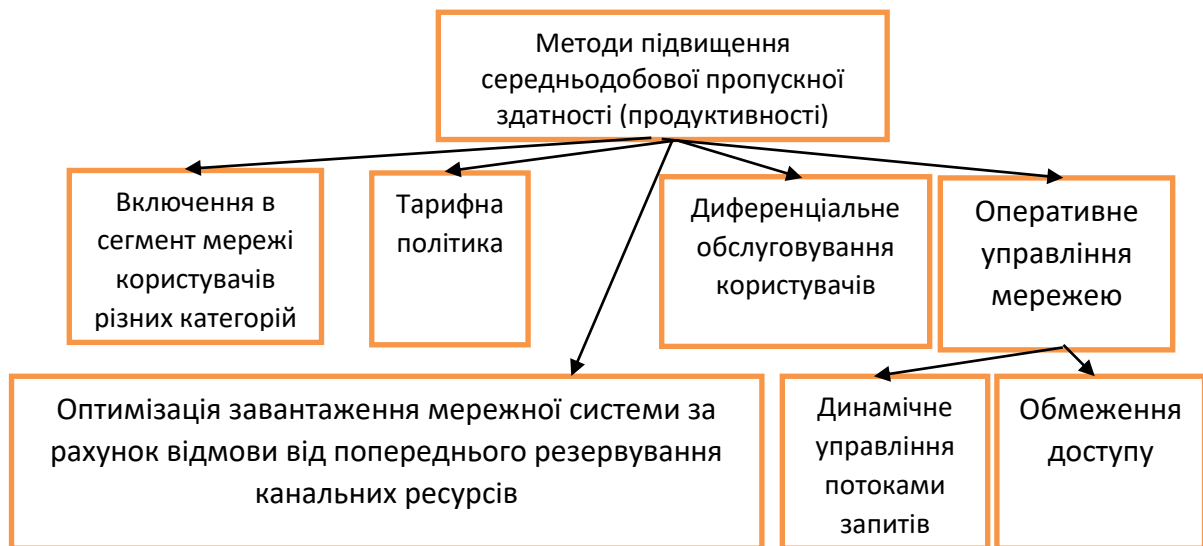


Рис. 2.1. Методи підвищення пропускної здатності в сервісних мережних системах [75].

Третій метод - диференційоване обслуговування користувачів, тобто виділення категорій користувачів, обслуговування яких відбувається з підвищеною якістю, раніше знаходив своє застосування в телеграфії (термінові телеграми) і на міжміській телефонній мережі (терміновий виклик з 3-х кратною оплатою) при напівавтоматичному встановленні з'єднання. В даний час цей спосіб може знайти широке застосування в хмаринкових сервісних системах за допомогою надання користувачам різних рівнів обслуговування (функціональних можливостей, пріоритетів і т.д.), тим самим, знижуючи взаємний вплив користувачів різних категорій. При цьому, у відповідності до угоди про рівень обслуговування SLA за певну щомісячну плату встановлюється певний обсяг послуг, а за перевитрату може стягуватися додаткова оплата. При введенні певних обмежень, як правило, оператори вимушені запропонувати користувачам додаткові можливості.

При розподілі користувачів за категоріями, відповідно до створюваного ними навантаження, повинні бути враховані специфічні види послуг, які пропонуються для кожної категорії [24]:

1. Категорія «традиційних» користувачів характеризується малою інтенсивністю запитів (для прикладу, один запит від одного користувача в ГНН) і великою середньою тривалістю зайняття каналних ресурсів мережі під

час обслуговування. Для даної категорії користувачів не є характерним використання додаткових сервісів. Коефіцієнт Ψ для даної категорії становить близько 300.

2. Категорія «бізнес» користувачів. Вона характеризується меншою тривалістю зайняття каналних ресурсів мережі під час обслуговування, але більшим числом запитів (приблизно 3 запити в ГНН). Для даної категорії є характерним активне використання додаткових сервісів. Коефіцієнт Ψ для даної категорії користувачів становить близько 150.

3. Категорія «економних» користувачів. Поява даної категорії обумовлена тарифною політикою телекомунікаційних операторів. Для цієї категорії є характерними дуже низька середня тривалість зайняття каналних ресурсів мережної системи під час обслуговування і дуже висока інтенсивність запитів. Особливістю даної категорії є те, що для опису розподілу тривалості зайняття каналних ресурсів запитами таких користувачів експоненціальний закон, що може бути використаний для інших категорій, не підходить. Тому приймається, що тривалість зайняття каналних ресурсів такими користувачами рівномірно розподілена на інтервалі від десяти до п'ятнадцяти секунд. Для категорії «економних» користувачів є характерним активне використання чатів. Ця категорія користувачів в основному створює службовий трафік, тому коефіцієнт Ψ для неї становить близько 15 [74, 75].

Метод диференційованого обслуговування користувачів є доволі перспективним, оскільки не вимагає підвищення продуктивності програмно-технічних засобів сервісної мережної платформи. Тим не менше, виходячи з аналізу літературних джерел, можна зробити висновок про необхідність проведення докладних чисельних досліджень щодо його застосування, зокрема комп'ютерного моделювання [75].

Четвертий метод полягає в тому, що відмова від попереднього резервування каналних ресурсів в телекомунікаційній платформі сервісної мережної системи дозволяє обслуговувати більшу кількість запитів, ніж у випадку виконання такого резервування. Якість обслуговування таких запитів,

зокрема тривалість їх оброблення при цьому змінюється незначно [76].

Зокрема, за результатами моделювання спостерігається підвищення продуктивності сервісної мережної системи за обслугованим навантаженням трафіку запитів. Зокрема, при інтенсивності вхідного навантаження на сервісну мережну систему 17-20 тис. зап./с. відповідний виграш становить 16-22%, при цьому середній час тривалості сесій клієнтів у сервісній мережній системі збільшується в середньому на 5 с. при інтенсивності навантаження більше 20 тис. зап./с [77].

Проте, даний метод є менш ефективним при обмеженій продуктивності програмно-технічних засобів сервісної мережної платформи, а також в умовах значних навантажень на хмарну сервісну систему.

П'ятий метод застосовується для боротьби з перевантаженнями. Це оперативне управління мережею, яке, в свою чергу, припускає динамічне управління потоками інформації та обмеження доступу користувачів в мережу. При цьому розрізняють методи локального і глобального управління. Глобальне управління передбачає обмеження загального числа запитів до сервісної мережної платформи або динамічне управління маршрутизацією в рамках застосування масштабованої PaaS моделі. Можливе використання комбінації обох прийомів.

Застосовують також локальне управління, відповідно до якого обмежується або загальна кількість запитів до сегментів сервісної мережної платформи, або обсяг мережних ресурсів, що виділяються різним категоріям користувачів.

2.2. Моделювання процесів обслуговування потоків запитів у розподіленій сервісній мережній платформі.

У розподілених сервісних мережах виникають ситуації, коли багатошляхова маршрутизація трафіку стає чи не єдиним засобом розв'язання проблеми його гіперагрегації трафіку, разом – зниження внутрішньо

системних відмов у обслуговуванні, а також – підвищення зовнішньо-системних показників якості сервісу. Проте, складність подібних алгоритмів розподілу навантаження, їх адаптації до поточних умов функціонування розподіленої мережної інфраструктури спонукає дослідити дисципліну обслуговування запитів всередині сервісних мережних систем більш докладно. Випадок існування резервного маршруту/маршрутів видається тривіальним лише з точки зору структурної інтерпретації, проте вже нескладні розрахунки свідчать, що імовірно-часові характеристики процесів обслуговування пов'язаних запитів і потоків є складнопрогнозованими. Більше того, недостатньо опрацьованим є апарат для аналітичних досліджень подібних імовірнісних явищ. Враховуючи те, що обсяги трафіку, які обслуговуються розподіленими сервісними системами вражають навіть спеціалістів, актуальними є задачі моделювання та оптимального розподілу їх мережних ресурсів. До такого трафіку відносять відеоконференції, відео на замовлення, “важкі” обчислення та бізнес за концепціями “повсюдного комп'ютингу”, а також m-business [65, 66, 78, 79]. Більшість трафіку потребує резервування пропускної здатності для гарантування належної якості обслуговування клієнта. Очевидно, що алгоритми розподілу потокового навантаження в сервісних мережних системах можуть враховувати дану потребу під час маршрутизації [80, 81]. Проте ефективність (за критерієм системної продуктивності) тієї чи іншої дисципліни обслуговування запитів та пов'язаного з ними характеру розподілу навантаження з розподіленою просторовою структурно-математичною моделлю сервісної мережної системи на сьогодні не узгоджували, а це дозволило б запропонувати моделі та методи отримання імовірно-часових характеристик потокового трафіку запитів для різних методів його обслуговування.

Зокрема, відповідно до рекомендації MCE-T Q.764 [82], при передаванні через мережу сигналізації ЗКС № 7 початкового адресного повідомлення (IAM) в системі рухомого зв'язку 4G LTE, одночасно відбувається резервування каналних ресурсів мережі транспортної підсистеми. Аналогічні по суті дії

можуть передбачатися при обслуговуванні сервісною мережною системою мультимедійного контенту множини клієнтів у реальному часі [81].

На рис. 2.2 наведено блок-схему сегменту розподіленої сервісної мережної системи з різними можливими маршрутами пересилання сервісного трафіку між вузлом субсистеми А та вузлом субсистеми В.

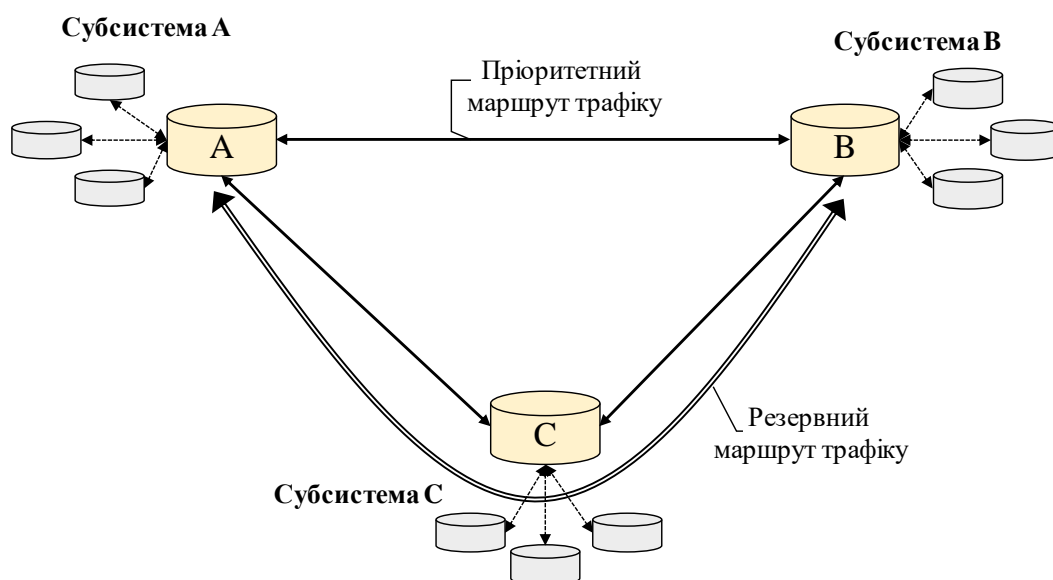


Рис. 2.2. Функціональна блок-схема сегменту розподіленої сервісної мережної системи з двома можливими маршрутами пересилання сервісного трафіку [83].

Очевидно, що не всі зарезервовані з'єднання всередині сервісної мережної платформи завершуються передаванням потоків корисного навантаження. Кожна сервісна мережа характеризується коефіцієнтом використання ресурсів. Звичайно, збільшення кількості непродуктивних та відхилених *потоків запитів* призводить до неефективних витрат телекомунікаційних ресурсів сервісної мережної платформи, а отже і зниження її системної продуктивності за обслугованим корисним навантаженням.

Одним зі способів підвищення ефективності сервісної мережної системи, зокрема її телекомунікаційної компоненти за рахунок виключення непродуктивних витрат комунікаційних ресурсів є відмова від попереднього резервування каналної ємності між сервісними підсистемами (вузлами, серверами) до встановлення відповідних потоків даних. Звичайно, набір мережних протоколів, які для цього слід використовувати потребує певних

модифікацій, наприклад відмови від застосування протоколів, які побудовані на зразок RSVP. Тим не менше, необхідним видається дослідження ймовірнісно-часових характеристик сервісної мережної системи за умови застосування різних підходів до резервування каналної ємності її телекомунікаційної платформи. Слід мати на увазі, що гарантування якісних показників обслуговування, зокрема за часткою невдало обслужених потоків трафіку, або ж потоків, які були обслужені недостатньо якісно є пріоритетним завданням при побудові відмовостійких розподілених сервісних мережних систем.

Метою даного розділу є розроблення функціональної і структурно-математичної моделей обслуговування потоків запитів на сегменті розподіленої сервісної мережної системи, що включає в себе об'єднання декількох систем масового обслуговування.

Інтуїтивно зрозуміло [84, 85], що для надання гарантій встановлення потоків запитів і результируючих потоків даних між елементами сервісної мережі, необхідно ввести поріг завантаження гарантованого каналного ресурсу відповідного визначеного пріоритетного маршруту трафіку в телекомунікаційній системі (див. рис. 2.2), при досягненні якого встановлювати з'єднання з використанням мережних ресурсів резервних маршрутів. На резервних маршрутах, враховуючи їх більшу фізичну довжину, існуватиме можливість здійснення резервування комунікаційних ресурсів.

2.2.1. Постановка задачі побудови математичної моделі обслуговування потоків запитів у телекомунікаційній сервісній мережній системі.

Розглянемо сегмент сервісної мережної системи, представлений на рис. 2.2 [83]. Для потоків запитів, що надходять від вузлів субсистеми А є два можливих варіанти встановлення маршрутів до вузлів субсистеми В. Перший варіант (заздалегідь визначений пріоритетний маршрут трафіку) передбачає встановлення прямого маршруту, а другий варіант (резервний маршрут трафіку) передбачає в нашій моделі встановлення шляху через транзитний маршрутизатор субсистеми С, тобто потоки запитів проходять за шляхом А-С-В. Більша

кількість резервних маршрутів може бути математично зведена до одного шляхом узагальнення відповідних ділянок (А-С і С-В) та трафіку інших субсистем (як субсистеми С), проте це призвело б до значного ускладнення моделі рис. 2.2, тому в даній роботі такий варіант спеціально не розглядається.

Уявімо ситуацію, коли на пріоритетному маршруті трафіку запитів загальний обсяг каналного ресурсу дорівнює N , на частині резервного маршруту трафіку запитів від субсистеми А до субсистеми С досяжний обсяг ресурсу – L_1 , а на його частині від субсистеми С до субсистеми В – L_2 . Слід врахувати, що ми розглядаємо сервісну мережену систему, в якій на ресурс з обсягом L_2 додатково поступатимуть також потоки запитів від субсистеми С до субсистеми В.

Відмова від попереднього резервування каналної ємності між сервісними підсистемами передбачається на пріоритетному маршруті трафіку на час встановлення з'єднання для потоків запитів та відповідного трафіку і (для розмовних викликів, наприклад у платформах 4G-LTE) – на час очікування відповіді абонента, або серверної системи, що викликається. При цьому із загального ресурсу каналної ємності N на пріоритетному маршруті трафіку встановимо поріг на рівні каналного ресурсу K , причому нехай $K = N - M$. Величину K будемо називати порогом гарантованого ресурсу каналної ємності в сервісній мереженій системі. Очевидно, що регулювання його величини можна використовувати для мінімізації втрат при обслуговуванні потоків запитів та підтримання в нормі якісних показників роботи розподіленої системи в цілому. Величина M характеризуватиме величину каналних ресурсів, які використовуються до фактичного досягнення заданого порогу гарантованого ресурсу каналної ємності в сервісній мережній системі.

Зробивши такі визначення та застереження, розглянемо три основні сценарії щодо проходження потоків трафіку в процесі встановлення з'єднань між субсистемами А і В сервісної мережної системи.

Сценарій 1. Якщо при надходженні запиту на передавання потоку від субсистеми А до субсистеми В через пріоритетний маршрут трафіку частина величини каналного ресурсу M виявиться вільною та достатньою, то відповідний інформаційний потік буде передаватись з використанням пріоритетного маршруту

трафіку.

Обслуговування інформаційного потоку сервісною мережною системою може характеризуватися двома фазами [86, 87]. Відповідно до пропонованої моделі, перша фаза - це очікування відповіді від сервісної служби в підсистемі В. Якщо мова йде про реагування абонента на виклик, то очікуються його дії. Канальні ресурси не займаються, а запит від серверів підсистеми А реєструється, очікуючи на обслуговування. Для мереж мобільного зв'язку передавання інформації про встановлення з'єднання може також здійснюватися через MAP підсистему сигналізації ЗКС №7.

Після відповіді сервісної служби або абонента, що запитується або викликається в підсистемі В починається друга фаза обслуговування запиту. Власне, розмовний канал або передавання даних потребують передавання деяких обсягів інформації, тобто встановлення інформаційного потоку, якому доступний весь обсяг ресурсів величиною N . Якщо перед початком другої фази обслуговування весь каналний ресурс величиною N виявляється зайнятим, то автоматично обирається резервний маршрут трафіку запитів. Звичайно, в такому випадку, за відсутності вільних каналних ресурсів на хоча би одній частині резервного маршруту, виникає відмова у обслуговуванні запиту сервісною мережною системою навіть при вдалій генерації відповідного потоку від сервісних вузлів підсистеми В.

Якщо запит в підсистемі В під час свого оброблення привів до досягнення тривалості тайм-ауту, то такий запит залишає систему масового обслуговування (СМО) необслуженим, не зайнявши жодних каналних ресурсів інформаційної мережі.

Сценарій 2. Якщо при надходженні запиту від вузлів підсистеми А на пріоритетному маршруті трафіку зайнята величина каналного ресурсу, що перевищує M , то запит відразу прямує на обслуговування, використовуючи резервний маршрут. Слід врахувати, що, використовуючи каналний ресурс першої частини резервного маршруту А-С (L_1), може не виявитись достатнього каналного ресурсу (L_2) в його другій частині, оскільки на маршрут С-В також надходять запити

від субсистеми В. У результаті також може виникати відмова у обслуговуванні запиту.

Сценарій 3. Якщо при надходженні запиту від вузлів субсистеми А на пріоритетному маршруті трафіку зайнята величина каналного ресурсу, що перевищує M , а на резервному маршруті обсяг задіяного каналного ресурсу досягає L_1 (або L_2), то цей запит отримає відмову в обслуговуванні.

Отже, потрібно побудувати математичну модель описаної СМО і за допомогою дослідження цієї моделі визначити оптимальні значення для її структурних параметрів: обсяг каналних ресурсів на кожному з маршрутів; поріг гарантованого ресурсу каналної ємності, його співвідношення з каналною ємністю N на пріоритетному маршруті трафіку, при якому ймовірність відмови у обслуговуванні запиту буде мінімальною (тобто слід підібрати оптимальне значення каналного ресурсу M); ймовірність відмови у обслуговуванні запиту, якщо в момент його приходу на пріоритетний маршрут трафіку було зарезервовано каналну ємність K , а за час оброблення її витратили інші запити відповідними інформаційними потоками і початковий запит отримає відмову.

Крім того, потрібно розробити алгоритм та його програмну реалізацію для обчислення ймовірності блокування запитів на отримання потоків трафіку через пріоритетний та резервний маршрути досліджуваної СМО сегменту сервісної мережної платформи.

2.2.2. Побудова структурно-математичної моделі обслуговування потоків запитів у телекомунікаційному сегменті сервісної мережної системи.

Для повного опису системи масового обслуговування з очікуванням необхідно описати імовірнісні процеси, що описують вхідний потік запитів на обслуговування, структуру обслуговуючих пристроїв і дисципліну обслуговування [88]. У загальному випадку вхідний потік запитів описується розподілом ймовірностей проміжків часу між сусідніми запитами, який позначимо наступним чином: $A(t) = P(t - \text{час між}$

послідовними запитами), де A – певна подія.

Зазвичай передбачають, що проміжки часу між послідовними запитами є незалежними і рівномірно розподіленими випадковими величинами [89].

Другою величиною, яку треба описати, є час обслуговування. Розподіл цієї величини позначимо так: $B(x) = P(x - \text{тривалість обслуговування})$.

Тривалістю обслуговування вважаємо проміжок часу, протягом якого запит знаходиться в обслуговуючому пристрої СМО сегменту сервісної мережної платформи.

Як правило, для опису структури обслуговуючого пристрою і дисципліни обслуговування використовують такі параметри: ємність пам'яті, в якій накопичуються запити, що очікують обслуговування (іноді передбачається, що обсяг пам'яті це нескінченна величина) і число доступних обслуговуючих пристроїв [89].

Важливою характеристикою СМО для нашої структурно-математичної моделі є дисципліна обслуговування, що визначає порядок вибору запитів з черги для обслуговування [90]: обслуговування заявок в порядку їх надходження (FCFS – first come first serve), обслуговування заявок у зворотному порядку надходжень (LCFS – last come first serve) і випадковий вибір заявок для обслуговування (RANDOM). Звичайно, якщо вхідні заявки розрізняються за групами і встановлюється деякий пріоритет обслуговування для цих груп, то говорять про пріоритетну дисципліну обслуговування [89].

Крім того, СМО може враховувати такі явища, як відкликання запитів з черги, перехід запитів з однієї черги до іншої, затримку запитів перед входом їх у чергу та інші.

Вказавши характеристики СМО, необхідно визначити показники ефективності роботи сервісної мережної системи, які будуть отримані в результаті аналізу її роботи.

Основні позначення:

λ_1 – інтенсивність вхідного потоку запитів від підсистеми А;

λ_2 – інтенсивність вхідного потоку запитів від підсистеми С;

μ – інтенсивність обслуговування запитів від підсистем А і С на пріоритетному та резервному маршрутах в сервісній мережній системі;

q – імовірність того, що запит від підсистеми А або С не буде оброблений підсистемою В (не утворить результуючого потоку трафіку в мережній системі);

π_{11} – імовірність того, що потік трафіку за запитом від підсистеми А буде заблокований на пріоритетному маршруті;

π_{12} – імовірність того, що потік трафіку за запитом від підсистеми А буде заблокований на пріоритетному маршруті після того, як буде згенерований підсистемою В внаслідок обслуговування запиту;

π_2 – імовірність того, що потік трафіку за запитом від підсистеми А буде заблокований на першій частині резервного маршруту трафіку (А-С);

π_3 – імовірність того, що потік трафіку за запитом від підсистеми А буде заблокований на другій частині резервного маршруту трафіку (С-В);

$\frac{1}{\mu_0}$ – середній час очікування обслуговування в підсистемі В запитами від підсистем А і С ;

μ_0 – параметр експоненційної функції розподілу $F(x)=1-e^{-\mu_0 x}$, $x > 0$, за допомогою якої моделюється час очікування обслуговування підсистемою В запитів від підсистем А і С.

Необхідно звернути увагу на те, що визначення величин каналних ресурсів (N, M, K, L₁, L₂) передбачає їх дискретний характер, зокрема з технологічних міркувань – при резервуванні й утворенні відповідних інформаційних потоків (віртуальних каналів) на практичному мережному обладнанні (маршрутизатори, серверні платформи), а також з математичних, оскільки до складу більшості класичних

розрахункових співвідношень теорії СМО входить поняття факторіалу. Розрахункову величину окремих потоків користувачів необхідно оцінювати, виходячи із прогнозованого набору послуг системи та конкретного типу мережного обладнання телекомунікаційної платформи.

В даній роботі була розроблена структурно-математична модель обслуговування потоків запитів на сегменті розподіленої сервісної мережної системи, що включає в себе об'єднання декількох СМО, та представлена у вигляді узагальненої блок-схеми на рис. 2.3.

Передбачається, що вхідні запити субсистем А і С утворюють пуасонівські потоки заявок з інтенсивностями λ_1 та λ_2 відповідно.

Тривалість обслуговування користувацьких запитів на маршрутах А-В і А-С-В прийнята експоненційно розподіленою з параметром розподілу μ . Тривалість очікування обслуговування запиту моделюється за допомогою одного обслуговуючого пристрою з нескінченною чергою очікування та випадковою дисципліною обслуговування. Передбачається, що дана тривалість також має експоненційний розподіл зі значенням параметра $\mu_0 \gg \mu$.

Всі ймовірності блокувань, які можуть відбуватися в розробленій СМО сервісної мережної системи позначені в моделі різними індексами. Відтак, першою цифрою в індексі позначаємо номер (частину) маршруту, на якій виникає блокування.

- Індекс 1 – маршрут А-В (з канальним ресурсом N);
- Індекс 2 – маршрут А-С (з канальним ресурсом L_1);
- Індекс 3 – маршрут С-В (з канальним ресурсом L_2), причому з вхідним потоком запитів від субсистеми С і вихідним потоком запитів з маршруту А-С розглянутої СМО.

Головними параметрами, що потребують дослідження та моделювання є ймовірності блокувань пов'язаного трафіку запитів, що надходять у СМО $\pi_{11}, \pi_{12}, \pi_2$ та π_3 .

Зважаючи на складність даної СМО її дослідження проводилося поетапно.

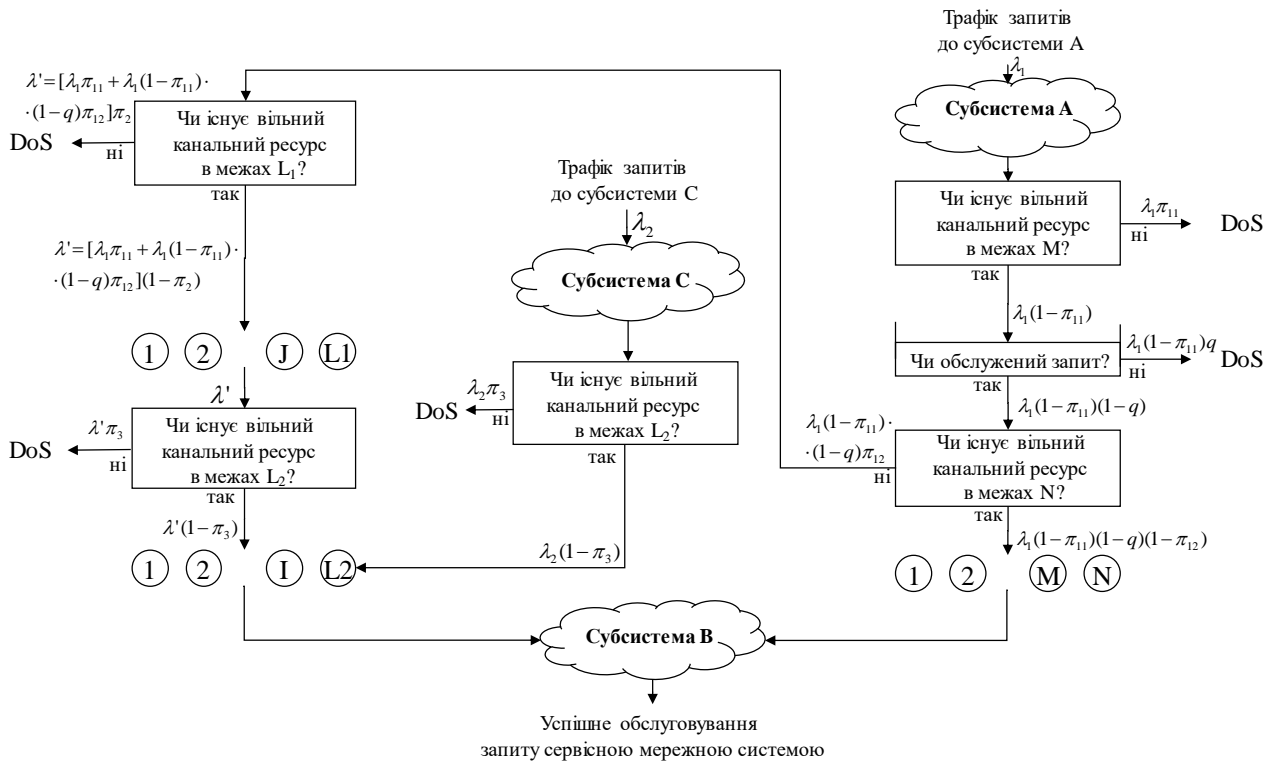


Рис. 2.3. Структурно-математична модель обслуговування потоків запитів на сегменті розподіленої сервісної мережної системи [76].

Оскільки самі шукані ймовірності блокування результируючих потоків запитів π_{11} , π_{12} , π_2 і π_3 беруть участь у перерозподілі цих потоків між ланками СМО (наприклад, чим більше ймовірність того, що трафік запиту від субсистеми А буде блокований на пріоритетному маршруті після свого обслуговування субсистемою В, тим частіше такі запити будуть потрапляти на резервний маршрут). Це стосується, зокрема, генерації сервісною мережною системою «важкого» мультимедійного контенту «на вимогу». Для їх обчислення доцільно застосовувати ітераційний алгоритм, оскільки в даний час не існує достатньо розробленого методу побудови математичних моделей аналогічних СМО і точних аналітичних формул для обчислення їх характеристик.

Розглянемо можливості обслуговування інформаційних потоків між субсистемами А і В (рис. 2.3). Якщо кількість задіяних мережних ресурсів на пріоритетному маршруті не досягла порогового значення М, то утворений потік

продовжує обслуговуватися за даним маршрутом. Така подія відбувається з імовірністю $1 - \pi_{11}$.

Якщо потік на пріоритетному маршруті не застане вільних ресурсів в межах величини M , тоді він з імовірністю π_{11} автоматично переспрямовується на резервний маршрут для дообслуговування. Обслуговування запиту відбувається двома фазами. Перша фаза передбачає оброблення запиту в субсистемі B , друга – передавання результуючого інформаційного потоку.

Фаза 1. Очікування завершення оброблення запиту субсистемою B моделюється за допомогою СМО з одним обслуговуючим пристроєм і з нескінченною чергою очікування, причому дисципліна обслуговування обрана випадковою. При цьому каналні ресурси де-факто не використовуються, а запит потрапляє в чергу очікування завершення оброблення (число запитів, що очікують у моделі необмежене). Передавання інформації про встановлення з'єднання у системах мобільного зв'язку здійснюється по мережі сигналізації ЗКС №7 в частині MAP.

З імовірністю q може відбутися така подія, як блокування запитів на маршрутах внаслідок того, що запити від субсистеми A залишають систему, не дочекавшись обслуговування (субсистемою B), причому так і не зайнявши жодних каналних ресурсів розподіленої сервісної мережної системи.

Фаза 2. З імовірністю $1-q$ субсистемою B буде оброблено запит субсистеми A та відповідний результуючий потік вимагатиме проходження через телекомунікаційну платформу. Даний потік потрапляє на пріоритетний маршрут з каналним ресурсом N , причому частина цього ресурсу буде вільною для того, щоб обслужити потік з імовірністю $1 - \pi_{12}$, тобто обслуговування запиту у такому разі відбувається успішно.

Можливе виникнення ситуацій, при яких за час оброблення запиту субсистемою B весь каналний ресурс на пріоритетному маршруті із залишкової величини вище порогу гарантованого ресурсу каналної ємності K був використаний на обслуговування інших запитів і при генеруванні потоку щодо даного запиту на пріоритетному маршруті не виявиться вільних каналних ресурсів. У цьому випадку

трафік запиту автоматично перенаправляється на резервний маршрут для дообслуговування.

Якщо запит, який надходить у СМО від субсистеми А застане вільні каналні ресурси в межах L_1 і достатню кількість каналних ресурсів в межах L_2 , то він вважається успішно опрацьованим і відповідний трафік передаватиметься резервним маршрутом у рамках сервісної мережної системи.

За відсутності вільних каналних ресурсів, запит зазнає відмови у обслуговуванні.

Розглянемо тепер можливі варіанти проходження трафіку запитів на маршруті субсистема С - субсистема В. Новий запит від субсистеми С надходить у СМО субсистеми В, що моделюється одним обслуговуючим пристроєм із нескінченною чергою очікування і випадковою дисципліною обслуговування. Отже, моделюється очікування оброблення трафіку запиту від субсистеми С до субсистеми В.

Якщо з імовірністю q субсистема В не обробить запиту від субсистеми С (не відбудеться з'єднання з абонентом, не буде згенерований відповідний сервісний трафік), то запит покине нашу модель СМО, не справляючи на її параметри впливу.

Відповідно, якщо з імовірністю $1-q$ запит від субсистеми С буде обслужений субсистемою В, то трафік буде вдало обслуговуватися за даним маршрутом С-В. При цьому, якщо трафік, що буде згенерований субсистемою В застане з імовірністю $1-\pi_3$ необхідний каналний ресурс в рамках L_2 , то трафік такого запиту буде успішно обслужений. У випадку, якщо трафік запиту від субсистеми С, який згенерований субсистемою В застане з імовірністю π_3 всі каналні ресурси L_2 зайнятими, то запиту буде відмовлено в обслуговуванні.

Таким чином, в даному розділі роботи побудовано структурно-математичну модель обслуговування трафіку запитів в розподіленій сервісній мережній системі, яка утворює собою об'єднання декількох СМО. Також наведений опис функціональної відповідності між функціональною (рис. 2.2) і структурно-математичною моделями (рис. 2.3) розглянутого сегменту розподіленої сервісної

мережної системи.

Був докладно описаний процес обслуговування та маршрутизації трафіку запитів від субсистем сервісної мережної системи при надходженні до змодельованої СМО.

Запропоновані та описані основні параметри розглянутої СМО, оцінку яких необхідно отримати при розробленні алгоритму обчислення ймовірності блокування трафіку запитів в досліджуваній СМО, зокрема в умовах відмови від попереднього резервування каналної ємності між сервісними підсистемами [94].

2.3. Дослідження імовірнісних характеристик трафіку магістральної мережі на прикладі опорно-транспортної підсистеми RAN LTE

Тенденції розвитку мереж мобільного зв'язку в сукупності з новими якісними та кількісними вимогами користувачів сервісних мережних систем обумовлюють зростаючу роль транспортної підсистеми (ВН - backhaul) на рівні радіодоступу (RAN – Radio Access Network) [81, 91, 92]. Вже сьогодні такі провідні компанії як Alcatel Lucent, NSN, Huawei, Ericsson та Cisco розробляють нові стандарти оптичного та безпроводного зв'язку для ВН [93, 228], що покликані підвищити ємність, масштабованість та доступність ресурсів транспортних компонентів сервісних мережних систем, зберігаючи низький рівень затримки, засоби підтримки мультисервісного трафіку та його диференціації за рівнями QoS. У той же час, відкритими залишаються питання дослідження імовірнісних характеристик трафіку та маршрутизації в таких системах. Розглянемо їх на базі сучасної магістральної мережної архітектури безпроводного сегменту сервісних мережних систем [77].

На рис. 2.4 зображена типова узагальнена архітектура RAN платформи, що складається з опорних станцій та точок доступу. Опорні станції формують макрокоміркове покриття, за їх допомогою забезпечується під'єднання точок доступу сервісних мережних систем до ядра мережі. За необхідності, вони

виконують ряд функцій управління, залежно від ступеня централізованості RAN [95]. Точки доступу приєднуються до опорних станцій та, разом з користувачами, які обслуговуються безпосередньо, формують вхідне навантаження, рівень якого може суттєво варіюватись впродовж доби.

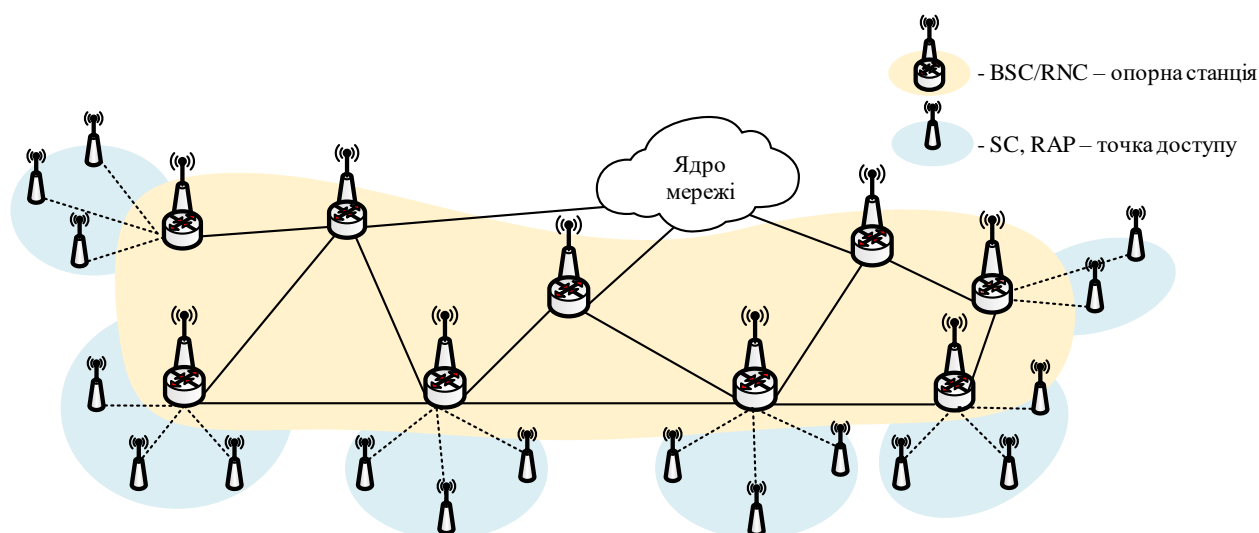


Рис. 2.4. Узагальнена архітектура RAN безпроводного сегменту телекомунікаційних сервісних платформ (у рамках LTE) [77].

Транспортна підсистема повинна ефективно адаптуватись до змін навантаження, розподіляючи каналні ресурси на кожному з маршрутів у відповідності до вимог рівня агрегації та поточних характеристик ВН сервісних мережних систем.

Метою даного розділу є розроблення структурно-математичної моделі обслуговування потоків запитів у сегменті сервісної мережної системи на прикладі транспортної підсистеми RAN у мережі мобільного зв'язку наступного покоління (в рамках LTE).

2.3.1. Постановка задачі математичного моделювання процесів обслуговування трафіку в розподіленій сервісній мережній архітектурі.

В роботі [76] було побудовано математичну модель обслуговування трафіку запитів в розподіленій сервісній мережній системі, яка утворює собою об'єднання декількох СМО. Також наведений опис функціональної

відповідності між структурно-функціональною (див. рис. 2.5) і структурно-математичною [76], рис. 2.3 моделями розглянутого сегменту розподіленої сервісної мережної системи [83].

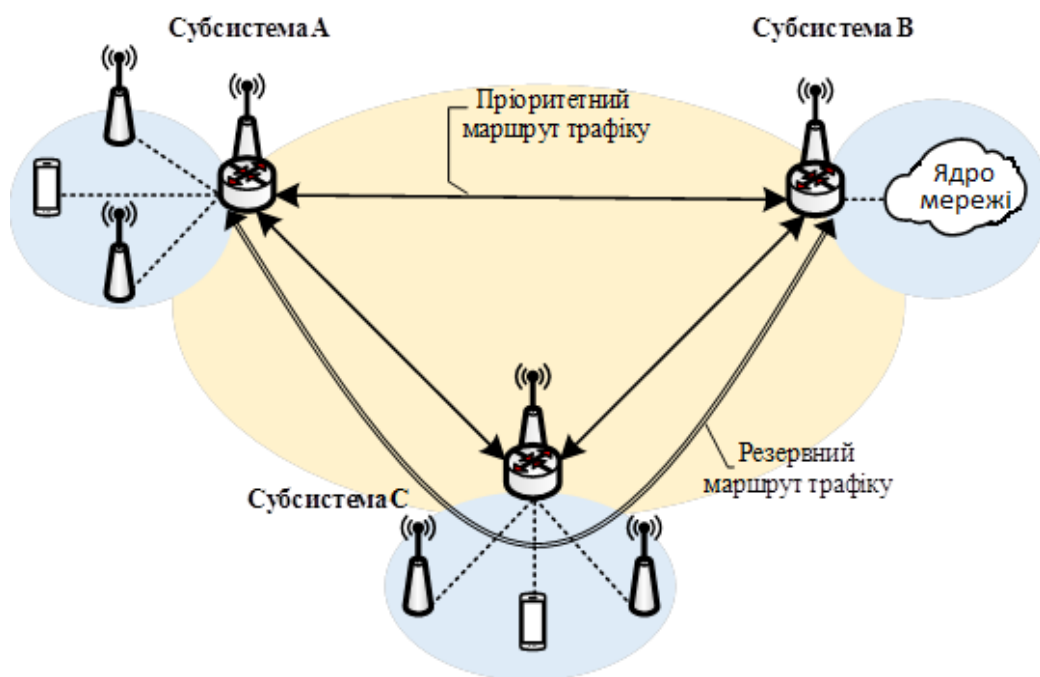


Рис. 2.5. Структурно-функціональна модель сегменту розподіленої мережної підсистеми 5G RAN з двома можливими маршрутами пересилання трафіку запитів [77].

Для спрощення побудови математичної моделі розглянемо транспортну підсистему RAN на прикладі трьох субсистем, одна з яких (B) має пряме під'єднання до ядра мережі, а інші виконують функції агрегування та ретрансляції трафіку.

У роботі [76] був докладно описаний процес обслуговування та маршрутизації трафіку запитів від субсистем сервісної мережної системи при надходженні до змодельованої СМО.

Були запропоновані та описані основні параметри розглянутої СМО, оцінку яких необхідно отримати при розробленні алгоритму обчислення ймовірності блокування трафіку запитів в досліджуваній СМО, зокрема в умовах відмови від попереднього резервування каналної ємності між сервісними підсистемами.

Виконаємо дослідження імовірності блокування трафіку запитів у розподіленій

сервісній мережній системі, що досліджується.

Остаточно, приймемо такі основні позначення:

λ_1 – інтенсивність вхідного потоку запитів від субсистеми А ВН RAN;

λ_2 – інтенсивність вхідного потоку запитів від субсистеми С ВН RAN;

μ – інтенсивність обслуговування запитів від субсистем ВН RAN А і С на пріоритетному та резервному маршрутах в сервісній мережній системі;

q – імовірність того, що запит від субсистеми ВН RAN А або С не буде оброблений субсистемою В (не утворить результуючого потоку трафіку в мережній системі);

π_{11} – імовірність того, що потік трафіку за запитом від субсистеми А ВН RAN буде блокований на пріоритетному маршруті;

π_{12} – імовірність того, що потік трафіку за запитом від субсистеми А ВН RAN буде блокований на пріоритетному маршруті після того, як буде згенерований субсистемою В внаслідок обслуговування запиту ядром мережі;

π_2 – імовірність того, що потік трафіку за запитом від субсистеми А ВН RAN буде блокований на першій частині резервного маршруту трафіку (А-С);

π_3 – імовірність того, що потік трафіку за запитом від субсистеми А ВН RAN буде блокований на другій частині резервного маршруту трафіку (С-В);

$\frac{1}{\mu_0}$ – середній час очікування обслуговування в субсистемі В ВН RAN запитами від субсистем А і С ;

μ_0 – параметр експоненційної функції розподілу $F(x)=1-e^{-\mu_0 x}$, $x > 0$, за допомогою якої моделюється час очікування обслуговування субсистемою В ВН RAN (ядром системи мобільного зв'язку) запитів від субсистем А і С.

Необхідно звернути увагу на те, що визначення величин каналних ресурсів (N , M , K , L_1 , L_2) у [76] передбачає їх дискретний характер, зокрема з технологічних

міркувань – при резервуванні й утворенні відповідних інформаційних потоків (віртуальних каналів) на практичному мережному обладнанні (маршрутизатори, серверні платформи), а також з математичних, оскільки до складу більшості класичних розрахункових співвідношень теорії СМО входить поняття факторіалу. Розрахункову величину окремих потоків користувачів необхідно оцінювати, виходячи із прогнозованого набору послуг системи та конкретного типу мережного обладнання телекомунікаційної платформи.

Отже, потрібно побудувати математичну модель описаної СМО сервісної мережної системи і за допомогою дослідження цієї моделі визначити оптимальні значення для її структурних параметрів: обсяг каналних ресурсів на кожному з маршрутів; поріг гарантованого ресурсу каналної ємності, його співвідношення з каналною ємністю N на пріоритетному маршруті трафіку, при якому ймовірність відмови у обслуговуванні запиту буде мінімальною (тобто слід підібрати оптимальне значення каналного ресурсу M); ймовірність відмови у обслуговуванні запиту, якщо в момент його приходу на пріоритетний маршрут трафіку було зарезервовано каналну ємність K , а за час оброблення її витратили інші запити відповідними інформаційними потоками і початковий запит отримує відмову.

Слід врахувати, що, використовуючи каналний ресурс першої частини резервного маршруту А-С (L_1), може не виявитись достатнього каналного ресурсу (L_2) в його другій частині, оскільки на маршрут С-В також надходять запити від субсистеми С. У результаті також може виникати відмова у обслуговуванні запиту.

Реалізуємо нашу математичну модель наступним чином.

1. Обчислюємо ймовірність блокування трафіку запиту від субсистеми А на пріоритетному маршруті А-В до ядра мережі ВН RAN за формулою:

$$\pi_{11} = E_{\rho = \frac{\lambda_1}{\mu}}(M) = \frac{\rho^M}{\sum_{i=0}^M \frac{\rho^i}{i!}}. \quad (2.2)$$

2. Обчислюємо ймовірність блокування трафіку запиту від субсистеми А на

пріоритетному маршруті А-В після того, як він отримає підтвердження обслуговування від мережного ядра ВН RAN субсистеми В за формулою:

$$\pi_{12} = E_{\rho = \frac{\lambda_1(1-\pi_{11})(1-q)}{\mu}}(N) = \frac{\rho^N}{\sum_{i=0}^N \frac{\rho^i}{i!}}. \quad (2.3)$$

Для обчислення імовірності блокування трафіку запиту від субсистеми А на першій частині резервного маршруту трафіку (А-С) (імовірності π_2) і на другій частині резервного маршруту трафіку (С-В) (імовірності π_3) проведено розрахунок параметрів СМО, до якої входять два потоки викликів і яка володіє канальними ресурсами L_1 і L_2 , відповідно.

Для обчислення ймовірностей π_2 і π_3 введемо двовимірний випадковий процес $(\xi(t), \eta(t))$, де $\xi(t)$ – кількість запитів від субсистеми А (назвемо їх запитами першого типу), що знаходяться на обслуговуванні в СМО в момент часу t , а $\eta(t)$ – кількість запитів від субсистеми С (назвемо їх запитами другого типу), що також знаходяться на обслуговуванні в СМО в момент часу t . Загальне число запитів, що знаходяться на обслуговуванні в СМО в будь-який момент часу t , дорівнюватиме сумі числа запитів першого і другого типів, тобто $\zeta(t) = \xi(t) + \eta(t)$. Простір станів цього процесу записується таким чином:

$$S = \{(i, j) | i = \overline{0, L_2}, j = \overline{0, L_1}, i + j \leq L_2\}, L_2 < L_1. \quad (2.4)$$

Граф інтенсивностей переходів описаного випадкового процесу подано на рис. 2.6. При цьому, стаціонарна ймовірність перебування випадкового процесу в стані (i, j) може бути подана, як:

$$P_{(i,j)} = P\{\xi(t) = i, \eta(t) = j\}. \quad (2.5)$$

Відповідні імовірності визначаються за допомогою сформованої системи рівнянь глобального балансу для випадкового процесу $(\xi(t), \eta(t))$ (див. рис. 2.6), яка записується наступним чином:

$$\begin{cases} p_{(0,0)}(\lambda_1 + \lambda_2) = \mu p_{(1,0)} + \mu p_{(0,1)}, i = 0, j = 0; \\ p_{(0,j)}(j\mu + \lambda_1 + \lambda_2) = \lambda_2 p_{(0,j-1)} + \mu p_{(1,j)} + (j+1)\mu p_{(0,j+1)}, i = 0, j \neq 0, j \neq L_1; \\ p_{(0,L_1)}(\lambda_1 + L_1\mu) = \lambda_2 p_{(0,L_1-1)} + \mu p_{(1,L_1)}, i = 0, j = L_1; \\ L_2\mu p_{(L_2,0)} = \lambda_1 p_{(L_2-1,0)}, j = 0, i = L_2; \\ p_{(i,0)}(i\mu + \lambda_1 + \lambda_2) = (i+1)\mu p_{(i+1,0)} + \mu p_{(i,1)} + \lambda_1 p_{(i-1,0)}, j = 0, i \neq L_2; i \neq 0; \\ p_{(L_2-j,j)}(j\mu + (L_2 - j)\mu) = \lambda_2 p_{(L_2-j,j-1)} + \lambda_1 p_{(L_2-j-1,j)}, j > 0, i + j = L_2. \end{cases} \quad (2.6)$$

Розв'язуючи систему рівнянь (2.6) і використовуючи умову нормування

$$\sum_{(i,j) \in S} p_{(i,j)} = 1, \quad (2.7)$$

отримуємо шукані значення ймовірностей $p_{(i,j)}$. За їх допомогою та за наступними формулами (2.8-2.9) визначаються шукані ймовірності. Таким чином:

$$\pi_2 = \sum_{(t,L_1) \in S, t=0, L_2-L_1} p_{(t,L_1)}, \quad (2.8)$$

$$\pi_3 = \sum_{(t,L_1) \in S, i+j=L_2} p_{(i,j)} \quad (2.9)$$

Розв'язання системи рівнянь (2.6) реалізовано програмно методами Гаусса та Крамера [95]. Причому, в результаті експериментів було встановлено, що використання методу Гауса для вирішення системи рівнянь (2.6) є більш ефективним, у порівнянні з методом Крамера за часом обчислень приблизно на 12%.

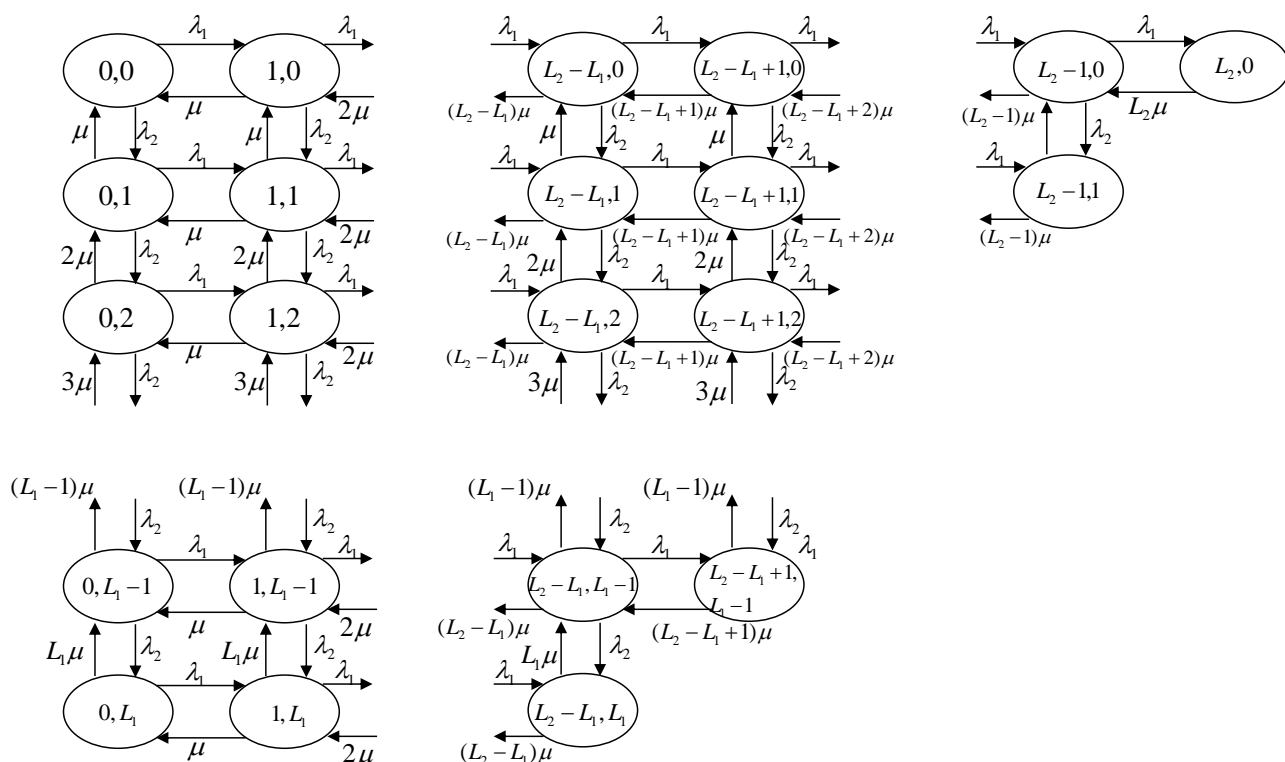


Рис. 2.6. Граф інтенсивностей переходів випадкового процесу $(\xi(t), \eta(t))$ [77].

Отриманий в результаті роботи програми масив розв'язків системи (2.6), тобто значень $p_{(i,j)}, (i, j) \in S$ був використаний для обчислення ймовірностей блокування трафіку запитів π_2 і π_3 за формулами (2.8) і (2.9) відповідно.

Величина π_2 – імовірність блокування трафіку запиту від підсистеми А на першій частині резервного маршруту трафіку (А-С) у ВН RAN. Отож, число запитів на обслуговування (з'єднання) першого типу від підсистеми А має використати каналний ресурс L_1 (відповідний буфер СМО заповнений), а імовірність такої події – $p_{(1,L_1)}$. Оскільки число запитів першого типу на обслуговуванні може бути будь-яким у межах каналного ресурсу від 0 до L_2-L_1 (більше бути не може, оскільки каналний ресурс рівний L_2 , а величина ресурсу L_1 вже зайнята обслуговуванням запитів від підсистеми А), то при обчисленні імовірності блокування викликів π_2 підсумовування за i ведеться у межах, вказаних у формулі (2.8).

Величина π_3 – імовірність блокування трафіку запиту від підсистеми А на

другій частині резервного маршруту трафіку (С-В) ВН RAN. Запити на обслуговування першого і другого типу зможуть використовувати каналний ресурс з величиною L_2 (величина доступного каналного ресурсу другої частини резервного маршруту), отже, будь-який новий запит, що входить в СМО буде блокований. Тому ймовірність π_3 є сумою всіх ймовірностей $p_{(i,j)}$ для станів процесу $(\xi(t), \eta(t))$, за умови коли $\zeta(t) = i + j = L_2$.

Таким чином, в даному розділі розроблено метод та описано алгоритм, який дозволяє обчислювати імовірності блокування трафіку запитів у розподіленій сервісній мережній системі з використанням математичного апарату теорії систем масового обслуговування та випадкових процесів. Отримані результати дозволили розробити програму мовою програмування C ++, яка дозволяє автоматизувати проведення розрахунків досліджуваної системи масового обслуговування (див. Додаток А).

Розроблена математична модель обслуговування запитів у розподіленій сервісній мережній системі максимально наближена до реальних умов і максимально повно відображає всі аспекти її роботи. При цьому, природно, не вдалося уникнути деяких спрощень для того, щоб розроблена математична модель піддавалася простому аналітичному дослідженню, а процеси, що відбуваються в ній логічно пов'язувалися між собою.

2.3.2. Дослідження процесів потокового резервування у розподіленій сервісній мережній архітектурі шляхом моделювання процесів обслуговування користувацьких запитів.

Відповідно до рекомендації MCE-T Q.764 [82], при передаванні через мережу сигналізації ЗКС № 7 початкового адресного повідомлення (IAM) в системі рухомого зв'язку 4G LTE, одночасно відбувається резервування каналів зв'язку в інформаційній мережі транспортної платформи. Те саме стосується оброблення потоків трафіку користувацьких запитів, які, для прикладу, відносяться до отримання та оброблення контенту в сервісних мережних

системах.

Результати досліджень, що подані нижче були виконані на основі комп'ютерного моделювання [96] та із застосуванням алгоритмів, що викладені у даному розділі та роботі [76]. Було досліджено ефективність застосування дисциплін обслуговування потоків запитів за умов резервування та за умов відсутності резервування каналних ресурсів в розподілених сервісних мережних системах. Дослідження проводилися в кілька етапів.

На етапі 1 було досліджено залежність показника відмов в сервісній мережній підсистемі ВН RAN від інтенсивності запитів, що до неї надходять для випадків попереднього резервування та відмови від резервування каналних ресурсів розподіленої телекомунікаційної платформи. Результати проведених досліджень представлені на рис. 2.7 [83, 97] нижче.

Таким чином, при відмові від апріорного резервування каналних ресурсів, виграш за продуктивністю обслуженого сервісною мережною системою навантаження у 16-22% спостерігається вже при 17-20 тис. зап./с.

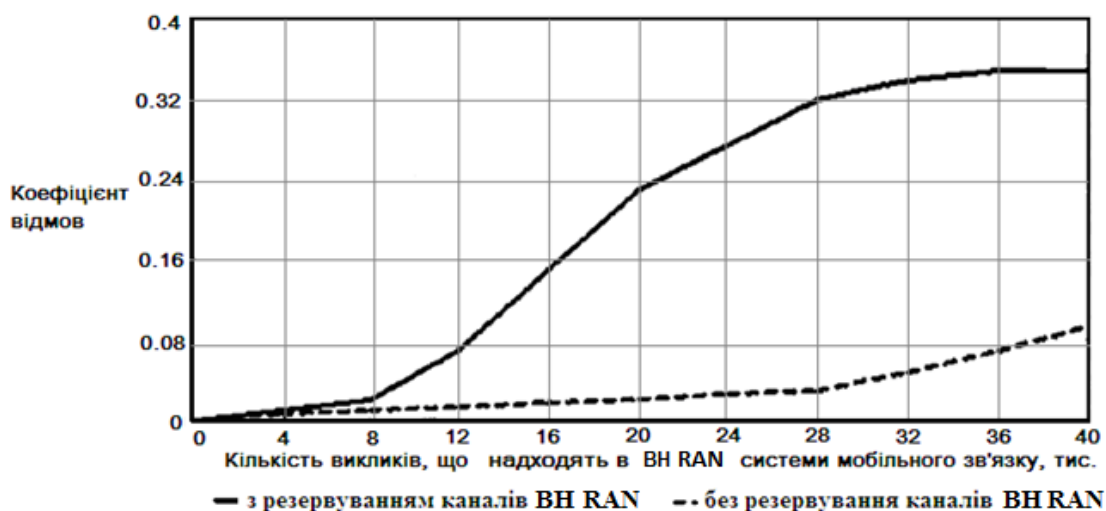


Рис. 2.7. Залежність показника відмов в сервісній мережній підсистемі ВН RAN, що моделюється від інтенсивності запитів, які до неї надходять (зап./с.)

Етап 2. За умов резервування каналних ресурсів телекомунікаційної підсистеми при зростанні інтенсивності запитів середня тривалість сесій при використанні клієнтами сервісної мережної підсистеми ВН RAN починала зменшуватися (внаслідок великої кількості відмов) (див. рис. 2.8), а за

відсутності резервування ця тривалість продовжувала збільшуватися, вказуючи на потенціал до збільшення системної продуктивності.

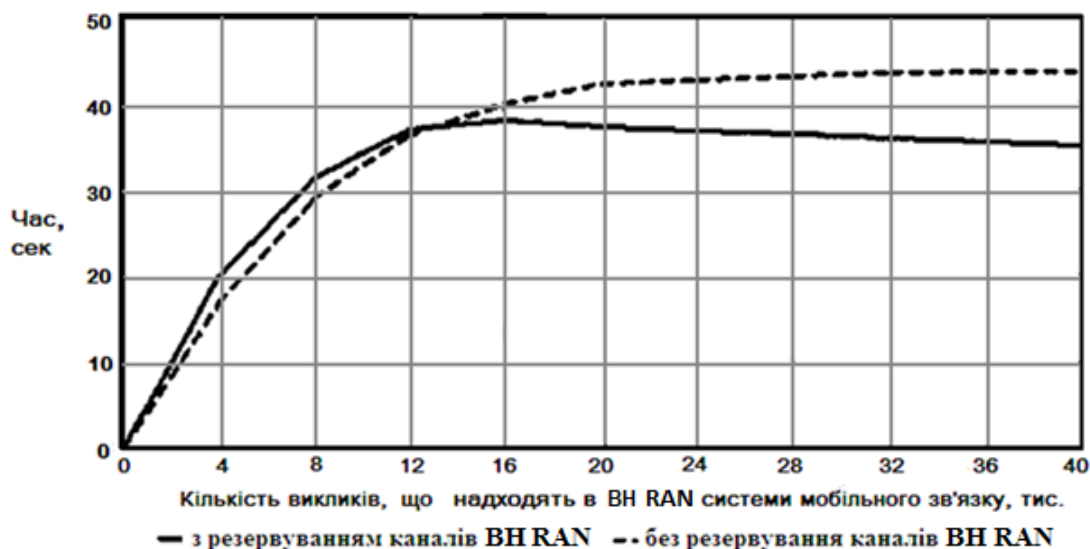


Рис. 2.8. Залежність середньої тривалості сесій клієнтів у сервісній мережній підсистемі ВН RAN, що моделюється від інтенсивності запитів, які до неї надходять (зап./с.)

На етапі 3 досліджувалася тривалість обслуговування запитів для випадків попереднього резервування та відмови від резервування каналних ресурсів розподіленої телекомунікаційної платформи сервісної мережної підсистеми ВН RAN. Результати проведених досліджень представлені на Рис. 2.9 [83, 97].

При попередньому резервуванні каналних ресурсів розподіленої телекомунікаційної платформи сервісної мережної підсистеми ВН RAN, середня тривалість обслуговування запитів, які надходять у сервісну мережну систему залишалася приблизно постійною. Спочатку даний показник незначно збільшився, внаслідок зростання навантаження, а потім зменшився, внаслідок зростання показника втрат (відмов у обслуговуванні користувачьких запитів), які з'явилися при обмеженні навантаження на сервісну мережну систему.

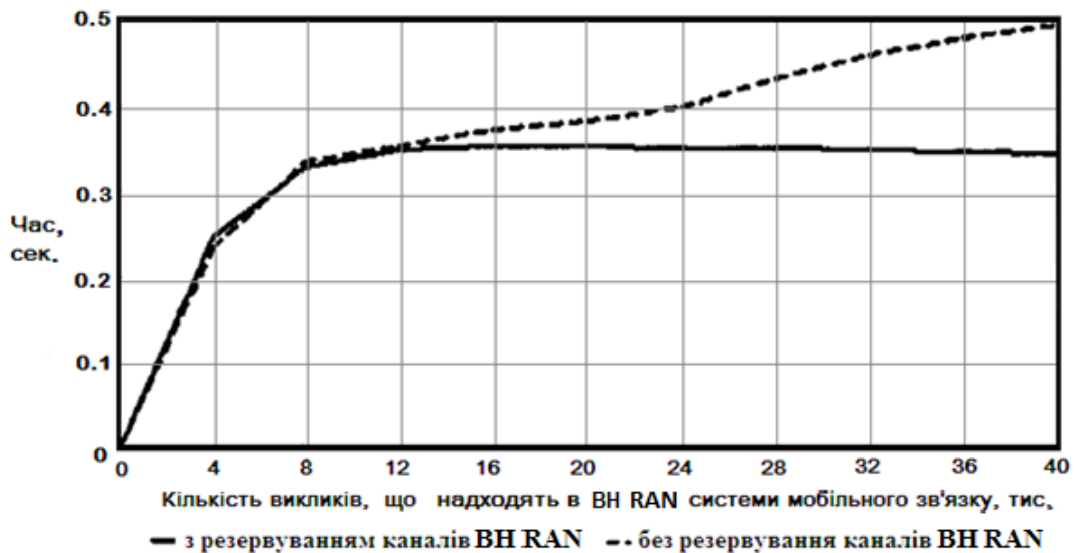


Рис. 2.9. Залежність середньої тривалості обслуговування запитів, які надходять у сервісну мережну підсистему ВН RAN, що моделюється від інтенсивності запитів, які до неї надходять (зап./с.)

2.4. Моделювання процесів диференційованого обслуговування користувачів хмарних сервісних платформ

На підставі застосування розглянутого в [75] методу диференційованого обслуговування різних категорій користувачів за допомогою імітаційного комп'ютерного моделювання проведемо дослідження для отримання оцінки якісних показників функціонування телекомунікаційних платформ хмарних сервісних мереж.

Мета даного розділу – визначення потенційних можливостей підвищення ефективності хмарних сервісних мережних систем (а саме – їх продуктивності) за рахунок обслуговування другорядних за пріоритетом запитів з негарантованою якістю.

Для досягнення поставленої мети необхідно запропонувати математичну модель обслуговування запитів сервісною мережною системою при диференційованому обслуговуванні запитів двох потоків. Запити першого потоку є пріоритетними в обслуговуванні і для їх обслуговування доступні всі

ресурси мережі. Крім того, передбачається, що ці запити можуть стосуватись додаткових сервісів, які надаються за більш високою вартістю, тобто, теоретично є більш ефективними. Оскільки відмова в обслуговуванні пріоритетних запитів призводить автоматично до втрати і додаткового ефекту, ймовірність втрат таких запитів через недостатню пропускну спроможність мережної системи повинна бути мінімальною.

Групи користувачів, які не відносяться до «бізнес» категорії, наприклад «економні» – не пред'являють високих вимог до якості сервісів, для них більш значущою є вартість сервісів, що надаються [75]. Тому для них надаються, в основному, вільні від обслуговування пріоритетних запитів користувачів мережні ресурси. Для таких запитів (другого потоку) характерне зайняття мережного ресурсу на більш короткий час і значна ймовірність відмов через відсутність вільного для їх обслуговування ресурсу мережі. У зв'язку з цим необхідно передбачати ефект, що пов'язаний з повторними спробами отримати доступ до ресурсів.

Таким чином, виникає досить складний вхідний потік запитів, у якому присутні: потік первинних пріоритетних запитів, потік запитів на додаткові сервіси, який, в загальному випадку, залежить від потоку вихідних запитів, потік низькопріоритетних запитів, а також потік повторних запитів. Безпосередній розрахунок такої моделі надходження запитів є складним навіть у припущенні, що обидва вхідні потоки є найпростішими, а тривалість обслуговування запитів сервісами – експоненційна. Як показано в [98], марковський процес, який виникає при цьому та описує стани елементів мережної системи, є чотиривимірним. Враховуючи те, що хмарна мережна система містить у своєму складі обслуговуючі пристрої, які можна вважати ланками великої ємності, де одночасно можуть обслуговуватися тисячі запитів, розрахунок подібної моделі на сучасних ЕОМ виконати важко, оскільки число станів всієї змодельованої системи буде значно більшим, ніж 10^9 .

В даному розділі роботи запропоновано удосконалення моделі

диференційованого обслуговування запитів, що дозволяє отримати ефективний метод розрахунку пропускної спроможності сервісної мережної системи, а також вибору порогового значення навантаження, після досягнення якого обслуговуються тільки високопріоритетні запити.

Теоретичні результати досліджень великих систем [99, 100] дають підстави вважати, що в міру збільшення ємності обслуговуючої ланки мережі зростає і кількість змін її станів за кінцевий проміжок часу, що, в свою чергу, позитивно впливає на збільшення точності наближеної моделі.

2.4.1. Математична модель диференційованого обслуговування користувачів.

Предметом подальших досліджень буде модель процесів обслуговування двох потоків запитів сервісною мережною системою, що володіє величиною каналного ресурсу ν , при цьому для запитів другого потоку доступні тільки мережні ресурси величиною k , $0 \leq k \leq \nu$. Запити з першого потоку утворюють пуасонівський потік інтенсивності λ_1 , і займають будь-який вільний каналний ресурс на час тривалості обслуговування, що має експоненційний розподіл з параметром μ_1 . Після завершення обслуговування запит може з імовірністю a продовжити обслуговування, тобто отримувати додатковий сервіс. Тривалість додаткового обслуговування має експоненціальний розподіл з параметром μ_s . У тому випадку, коли запит не надходить на обслуговування, він не може отримати і додатковий сервіс. Запити з другого потоку утворюють пуасонівський потік інтенсивності λ_2 і займають будь-який доступний їм каналний ресурс мережної системи на час тривалості обслуговування, що має експоненціальний розподіл з параметром μ_2 . Для запитів з другого потоку надання додаткових сервісів не передбачене. У випадку зайнятості всіх доступних каналних ресурсів запит другого потоку стає джерелом повторних запитів з імовірністю H , $0 < H < 1$, і інтенсивністю μ_r .

Структурно-параметрична модель обслуговуючого пристрою на основі ланки сервісної мережної системи (фактично – ланка відкритої MeMO Джексона) приведена на рис. 2.10. Відмічені канали, що доступні запитам другого потоку та показано формування потоку повторних запитів у разі відмови у обслуговуванні через зайнятість всіх доступних каналних ресурсів в межах величини k . Показано можливість додаткового обслуговування запитів першого потоку з імовірністю a у разі завершення основної фази обслуговування.

Модель описується марковським процесом, стани якого представляються чотиривимірним вектором (i_1, i_2, i_3, j) , де i_1 – каналний ресурс, зайнятий обслуговуванням запитів першого потоку, i_2 – каналний ресурс, зайнятий додатковим обслуговуванням запитів першого потоку при наданні додаткових сервісів, i_3 – каналний ресурс, зайнятий обслуговуванням запитів другого потоку, j – кількість джерел повторних запитів другого потоку. Множина можливих станів такої моделі подається як:

$$S = \{(i_1, i_2, i_3, j) : i_1 + i_2 + i_3 \leq v, 0 \leq i_1 + i_2 \leq v, 0 \leq i_1 \leq v, 0 \leq i_2 \leq v, 0 \leq i_3 \leq k, j \geq 0\}, (2.10)$$

де v – загальна величина каналного ресурсу мережної системи, k – величина каналного ресурсу, доступного для запитів другого потоку.

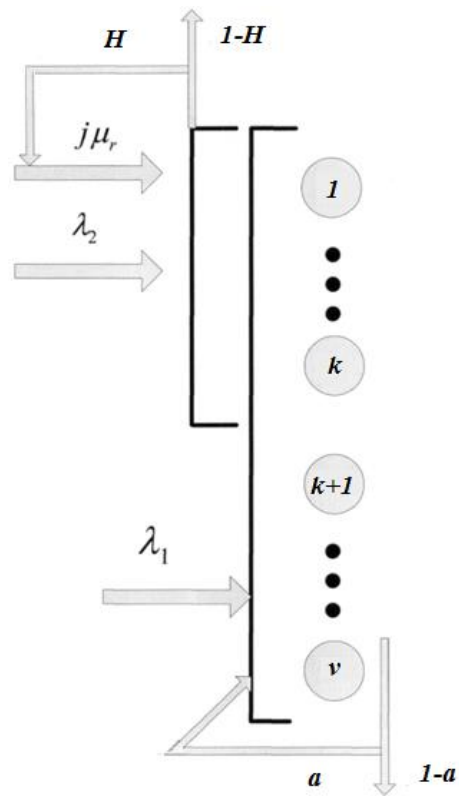


Рис. 2.10. Структурно-параметрична модель обслуговуючого пристрою на основі ланки сервісної мережної системи з диференційованим обслуговуванням запитів користувачів.

Виходячи з (2.10) та рис. 2.10, узагальнене рівняння статистичної рівноваги для такого процесу має наступний вигляд:

$$\begin{aligned}
 &P(i_1, i_2, i_3, j)(\lambda_1 + \lambda_2 + j\mu_r + \mu_1 i_1 + \mu_5 i_2 + \mu_2 i_3) = \\
 &P(i_1 - 1, i_2, i_3, j)\lambda_1 + P(i_1, i_2, i_3, j - 1)\lambda_2 + \\
 &+ P(i_1, i_2, i_3 - 1, j + 1)(j + 1)\mu_r + \\
 &+ P(i_1 + 1, i_2, i_3, j)(i_1 + 1)\mu_1(1 - a) + \\
 &+ P(i_1, i_2 + 1, i_3, j)(i_2 + 1)\mu_5 + P(i_1, i_2, i_3 + 1, j)(i_3 + 1)\mu_2,
 \end{aligned} \tag{2.11}$$

якщо виконуються такі умови:

$$i_1 + i_2 + i_3 < k, \quad i_1 > 0, \quad i_2 > 0, \quad i_3 > 0. \tag{2.12}$$

Рівняння (2.11) було отримано стандартним способом прирівнювання

інтенсивностей виходу і входу елемента СМО в стан [241]. У лівій частині рівняння наведено інтенсивність виходу зі стану за рахунок, відповідно, надходження запиту першого потоку, надходження запиту другого потоку, надходження повторного запиту другого потоку, завершення обслуговування запиту першого потоку, завершення додаткового обслуговування запиту першого потоку, завершення обслуговування запиту другого потоку. Введені обмеження (2.12) на змінні означають, що у разі приходу нового запиту він потраплятиме на обслуговування. Доданки у правій частині рівняння відповідають за інтенсивність входу в стан обслуговування. Вони послідовно відображають наступні події: зміна стану за рахунок надходження на обслуговування нового запиту першого потоку, зміна стану за рахунок надходження на обслуговування нового запиту другого потоку, зміна стану за рахунок надходження на обслуговування нового повторного запиту другого потоку (а оскільки в цих випадках величина зайнятих ресурсів не може бути рівною нулю, то повинні виконуватися співвідношення з умов (2.12)), звільнення обслуговуючих мережних (канальних та сервісних) ресурсів, зайнятих обслуговуванням запиту першого потоку, без подальшого дообслуговування, звільнення ресурсів, зайнятих обслуговуванням запиту першого потоку з подальшим дообслуговуванням, звільнення ресурсів, зайнятих дообслуговуванням запиту першого потоку і звільнення ресурсів, зайнятих обслуговуванням запиту другого потоку (первинного або повторного, оскільки в даному випадку процеси обслуговування є однаковими).

2.4.2. Аналіз результатів імітаційного моделювання процесів диференційованого обслуговування користувачів.

На основі узагальненого та часткових випадків розглянутої наближеної моделі (2.11) з урахуванням умов (2.12) та їх модифікацій виконано імітаційне статистичне комп'ютерне моделювання для розрахунку характеристик процесів диференційованого обслуговування користувачів сервісною мережною

системою з використанням засобів MATLAB та методів Монте-Карло.

Виконаємо дослідження ефективності введення динамічного управління [75], спрямованого на обмеження доступу до мережі запитів користувачів другого потоку в моменти, коли ресурси системи навантажено вище деякої порогової величини k . Узагальнену схему реалізації алгоритму моделювання наведено на рис. 2.11. Її було реалізовано програмно у фреймворку Qt5.2.

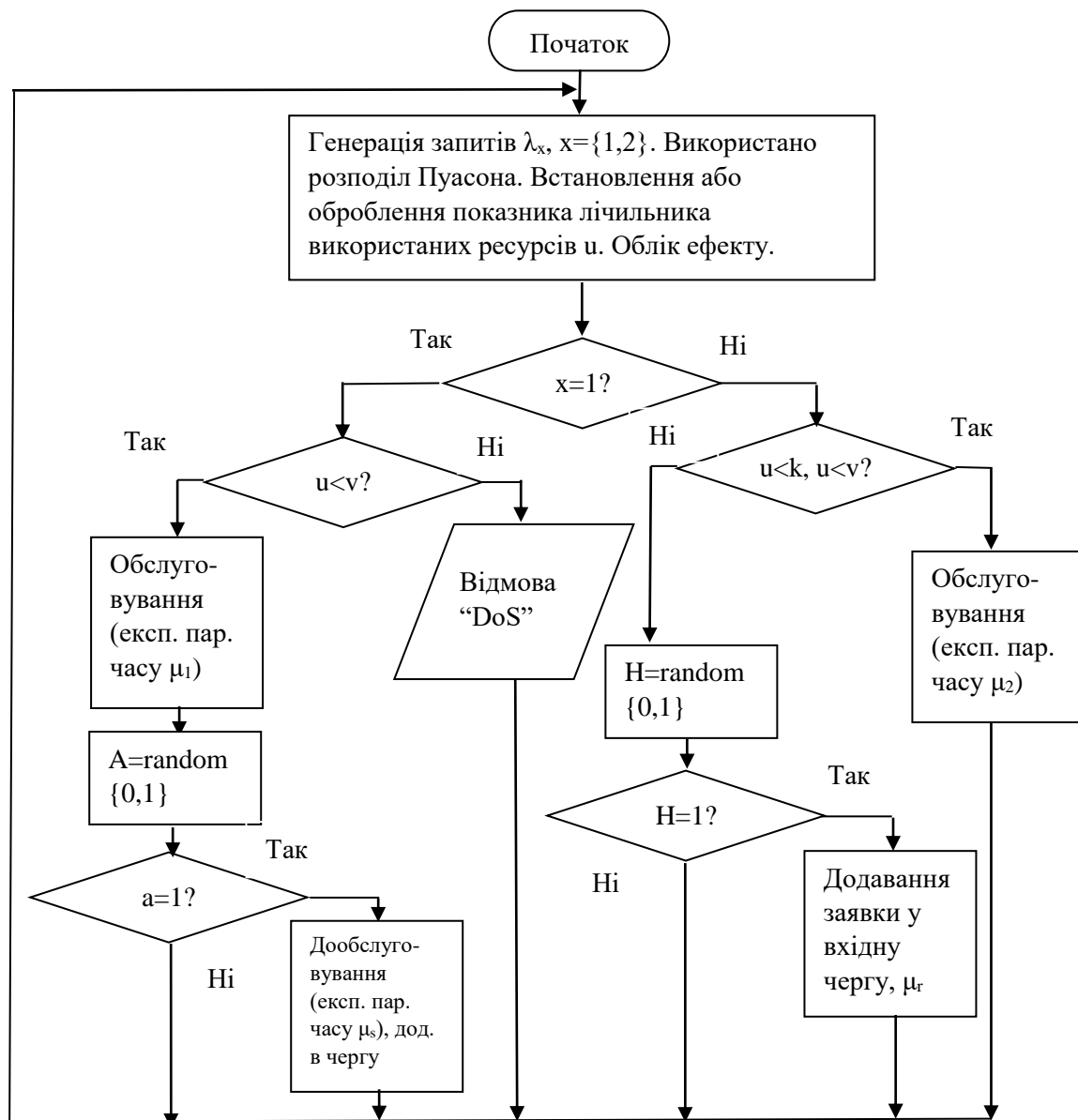


Рис. 2.11. Узагальнена схема реалізації алгоритму моделювання методу диференційованого обслуговування користувачів.

Вибір даної порогової величини здійснюється виходячи з вимог максимізації продуктивності хмарної сервісної мережної системи. При цьому

можливі різні види функціоналу якості роботи мережної системи: в одному випадку можна враховувати тільки продуктивність, позначимо її R , у другому – дохід мережі, який позначимо P , що виникає коли відраховуються непродуктивні ресурсні витрати, пов'язані з очікуванням надання сервісу. Тривалість очікування, в свою чергу, залежить від числа запитів, які надійшли в систему, але не залежить від тривалості їх обслуговування. Зрозуміло, що при малих значеннях непродуктивних ресурсних втрат у мережній системі різниця $R-P$ змінюється на незначну величину, що не впливає на якісну картину системної ефективності. При великих втратах виникає велике число невдалих спроб обслуговування, що може істотно змінити ситуацію. Як впливає з наведених нижче чисельних прикладів, в деяких випадках при неправильному регулюванні доступу до мережної системи обслуговування запитів другого потоку може не тільки не збільшити продуктивність, але й істотно її зменшити.

Передбачаємо, що мережна система спроектована для обслуговування запитів першого потоку в ГНН з необхідною якістю, однак через нерівномірності навантаження частина системного обладнання простоє, тому допускається обслуговування запитів другого потоку з обмеженим доступом до сервісної мережної хмари та з негарантованою якістю обслуговування, тобто для запитів другого потоку втрати не нормуються. Остання обставина дозволяє розглядати різні ситуації, коли втрати запитів другого потоку можуть бути дуже великими, а сама інтенсивність запитів другого потоку регулюється лише практичною доцільністю користування мережними сервісами з великими втратами, але з відносно низькими тарифами на обслуговування. При таких припущеннях різниця між R і P може бути досить значною, що може динамічно впливати на якісну картину обслуговування сервісною мережною системою і, відповідно, впливати на вибір значення k , при якому забезпечується максимальна продуктивність, як основний цільовий експлуатаційний показник мережної системи.

У міру зростання навантаження, що створюється низькопріоритетними

запитами, оператор може нарощувати пропускну здатність сервісної мережної системи, що дозволяє обслуговувати такі запити з кращою якістю і / або пропонувати частині користувачів інші тарифні плани, які гарантують певні параметри якості обслуговування (сервіси з гарантованою якістю обслуговування) [100]. Такий підхід дозволяє плавно здійснювати зміни у тарифній політиці в міру зростання навантаження зі збереженням якості обслуговування існуючих користувачів із заданою якістю та проводити нарощування пропускну здатності під уже сформовані потоки навантаження, що, в свою чергу, дозволяє будувати більш точні прогнози щодо необхідних програмно-апаратних мережних ресурсів і скоротити кількість обладнання мережної системи, яке використовується неефективно.

Наведемо результати розрахунків, які пов'язані з вибором значення k , при якому забезпечується максимізація функціоналів R – системної продуктивності і P - доходу мережі. Розрахунки проводилися при наступних вихідних даних: $\lambda_1 = 100$, $c_1 = 2$, $c_2 = 1$, $c_s = 3$, $\mu_1 = 1$, $\mu_2 = 5$, $\mu_s = 1$, $a = 0.5$, $\alpha = 0.01$, $v = 200$.

Вибрані значення параметрів створюють навантаження на сервісну мережну систему запити першого потоку в 150 Ерл, яке може бути обслужене сервісами системи з мінімальними втратами. Розрахунки проводилися при різних значеннях інтенсивності λ_2 ; її конкретні значення наведені в описах відповідних графіків з результатами розрахунків.

Розглянутий приклад повинен відповідати випадку максимального ефекту, пов'язаного з обслуговуванням запитів другого потоку, оскільки при подальшому зростанні інтенсивності запитів другого потоку має відбуватися зменшення продуктивності за рахунок зростання кількості необслужених запитів другого потоку. Отже, на рис. 2.12 наведено графіки R і P при сумарному навантаженні 350 Ерл, що відповідає значним перевантаженням сервісної мережної системи. У цьому випадку, при $k = 0$ значення функціоналу R все ще рівне 349,99 і відповідає обслуговуванню лише запитів першого потоку. Значення функціоналу P є істотно меншим і рівне 298,49, що набагато менше, ніж при відсутності запитів другого потоку, коли значення функціоналу

R було б, очевидно, рівне 348,5. Максимальне значення функціоналу R досягається вже при $k = 192$ і стає рівним 409,22, що дещо більше, ніж у попередньому випадку. Значення P досягає максимуму при $k = 193$ і рівне 367,82, що вже набагато менше, ніж у попередньому випадку. Далі відбувається спадання значень R і P через зростання втрат запитів першого потоку і при $k = v$, що відповідає відсутності регулювання доступу до ресурсів мережі, вони досягають свого мінімального значення, рівного 313,43 для R і 291,21 для P . Отже, продуктивність за рахунок обслуговування запитів другого потоку збільшиться на 59,23, а прибуток з урахуванням ресурсних витрат на очікування надання мережних сервісів збільшиться тільки на 19,32, при правильному управлінні доступом до ресурсів мережі (ефективному балансуванні навантаження в мережній хмарі PaaS).

При відсутності зазначеного регулювання потокового навантаження, а також при відсутності його балансування, дохід виявиться вже негативним, тобто збитки складуть 57,28. Таким чином, при відсутності диференційованого регулювання доступу до мережної системи при зростанні чисельності запитів другого потоку мережна система починає нести прямі збитки, причому при врахуванні ресурсних витрат на очікування надання мережних сервісів вони виявляються найбільш значними. За умов правильного регулювання доступу користувачів до системи її ефективність зберігається, проте відбувається її значне зменшення при врахуванні ресурсних витрат.

Для розрахунків мережної ефективності використовуються питомі продуктивність і дохід мережної системи, що припадають на одиницю її каналних (обслуговуючих) ресурсів.

При проектуванні сервісних мережних систем розрахунок пропускної спроможності проводиться виходячи з навантаження в ГНН. Оскільки ми розглядаємо одночасне обслуговування запитів декількох потоків, то їх ГНН не обов'язково повинні збігатися. Більше того, в аналізованих нами випадках передбачається, що запити першого потоку – це запити бізнес-користувачів, для яких характерні денні ГНН, а запити другого потоку – це запити користувачів,

для яких більш характерні вечірні ГНН (для прикладу – звичайне населення) [75]. Оскільки при проведенні мережею політики забезпечення користувачам, які формують другий потік запитів якості обслуговування, виходячи з загального навантаження на мережну систему, для них вигідним є використання мережних сервісів, а отже і відповідних ресурсів мережної системи в той час, коли активність користувачів, які формують перший потік запитів є низькою. Це характерно, наприклад, для ситуації, коли запити другого потоку формує молодь, тип активності якої припадає на пізній час, функціонально – на популярні мережні сервіси, коли потік запитів бізнес-користувачів вже невисокий. Цим самим, запитам другого потоку забезпечуються прийнятна якість обслуговування і одержується вища продуктивність мережі за рахунок більш повного використання її ресурсів.

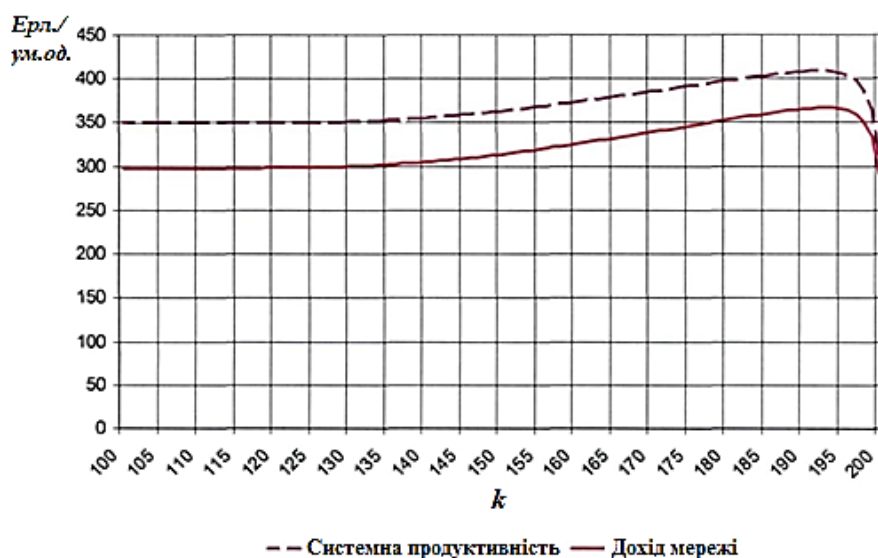


Рис. 2.12. Продуктивність і дохід мережної системи при $\lambda_2 = 1000$.

Розглянемо три випадки профілювання ГНН сервісної мережної системи за часом доби. Перший – коли добові профілі навантаження від груп користувачів збігаються (рис. 2.13), другий – коли у першій групі користувачів денні ГНН, а у другій – вечірні (рис. 2.14), а також третій випадок, коли користувачі, що формують запити другого потоку вибирають, в основному, час, під час якого бізнес-користувачами використовується найменше сервісів (рис. 2.15). Забезпечити таке профілювання оператор сервісної мережної системи зможе за

рахунок правильної маркетингової політики при встановленні тарифів, орієнтованих на користувачів другого пріоритету, саме тих, які орієнтуються не на тривалість отримання сервісів, зокрема на обсяг наданої послуги, а на факт отримання сервісів, як таких. Прикладами таких підходів є тарифи операторів мереж мобільного зв'язку, що застосовуються, зокрема, в нічний час, коли вартість послуг фактично не залежить від тривалості з'єднання. А при включенні в тариф вартості спроби з'єднання, як це практикується, наприклад, в США, можна забезпечити стимулювання абонентів мобільного зв'язку підлаштуватися під профіль добового навантаження на мережі, тобто реалізувати доволі ефективний з погляду системної продуктивності третій сценарій (див. рис. 2.15). Подібні маркетингові стратегії використовуються операторами хмарних сервісних мережних систем [65-66]. У відповідності до одержаних результатів, щодо низькопріоритетних абонентів рекомендується виконувати процедури вертикального хендоверу для переведення їх на обслуговування до платформ, у яких існують невикористані мережні ресурси. Наприклад, відбувається примусове переключення «економних абонентів» 3-4G на 2-2,75G сегмент мережі мобільного зв'язку, при цьому «бізнес»-абоненти одержують весь високошвидкісний ресурс для якісного надання базових та додаткових видів сервісів.

Отже, для кожного описаного вище випадку профілювання ГНН сервісної мережної системи наведемо графіки профілів добового навантаження, які для запитів першого потоку однакові, а для другого – змінюються. На цих графіках представимо також результати розрахунку ефективності функціонування мережної системи (її продуктивності). При виборі значення порогу k використовувався підхід, коли якість послуг для запитів першого потоку в ГНН гарантувалася на заданому рівні. Значення інших параметрів наступні: $H = 0.8$, $c1 = 3$, $c2 = 1$, $cs = 5$, $\mu r = 1$, $\mu1 = 1$, $\mu2 = 0.5$, $\mu s = 0.5$, $a = 0.5$, $\alpha = 0.1$, $v = 300$. Тривалості сеансів користування мережними сервісами у «економних» користувачів і у бізнес-користувачів при моделюванні приймалися однаковими.

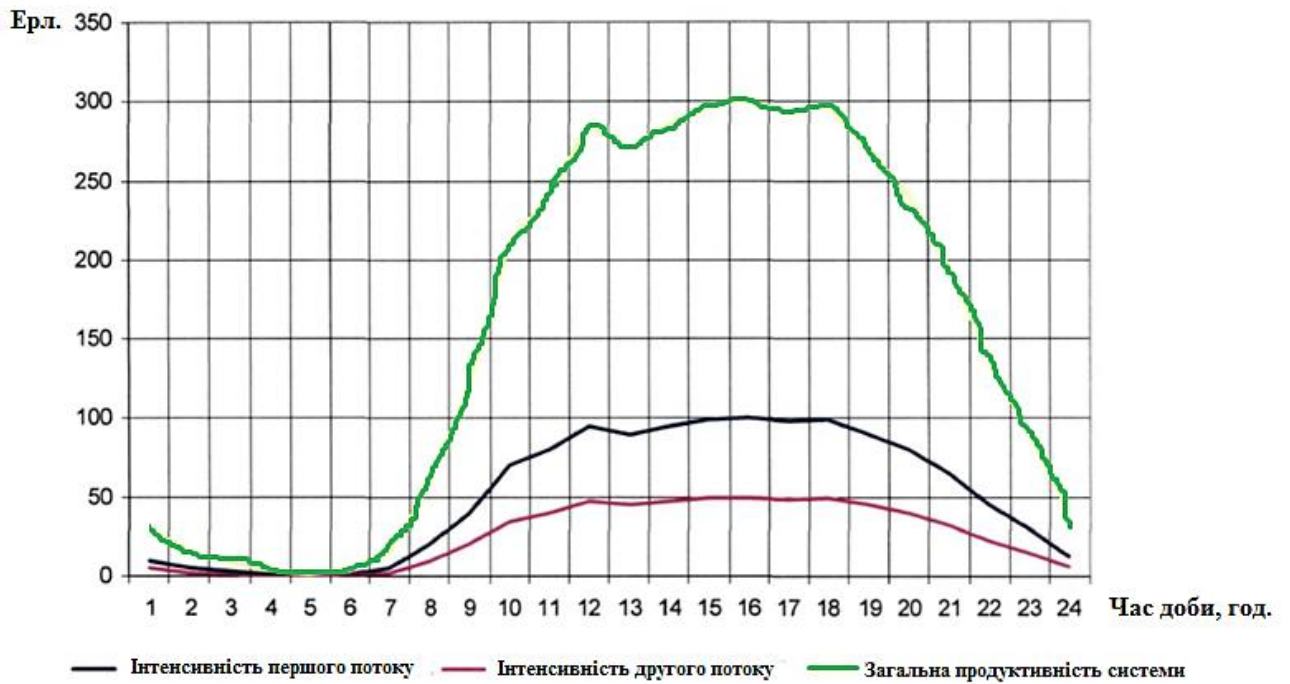


Рис. 2.13. Профіль розподілу добової продуктивності при співпадінні профілів навантаження бізнес- і «економних» користувачів.

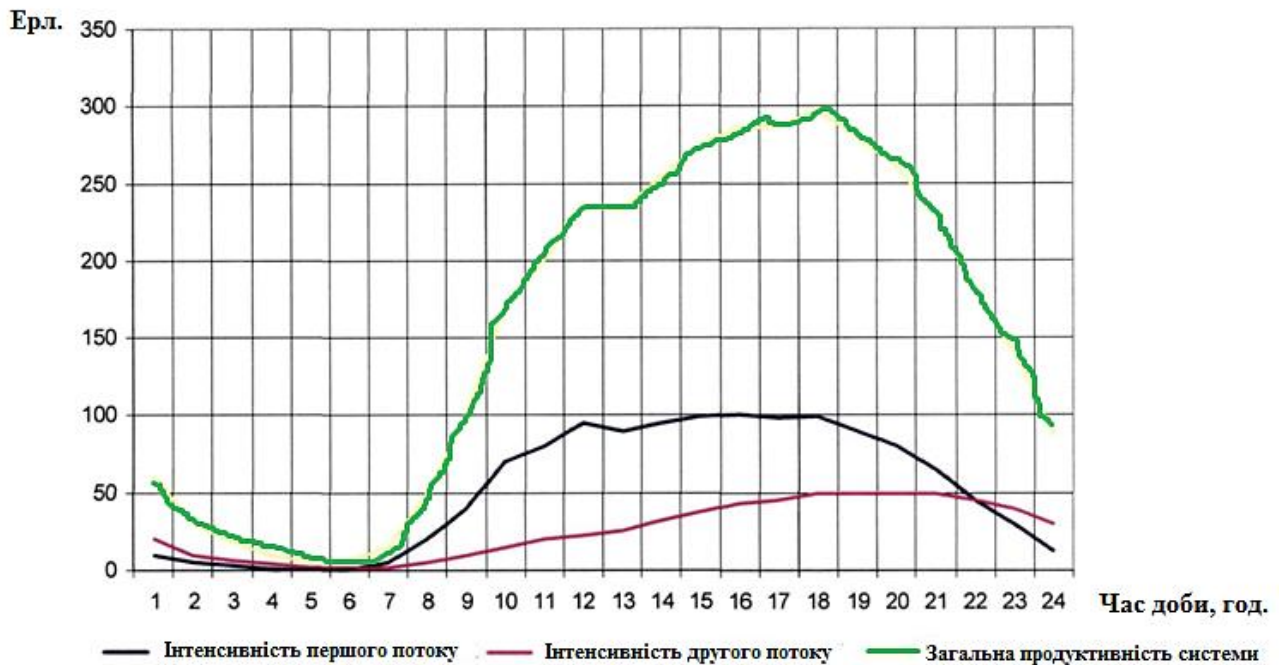


Рис. 2.14. Профіль розподілу добової продуктивності при неспівпадінні профілів навантаження бізнес- і «економних» користувачів.

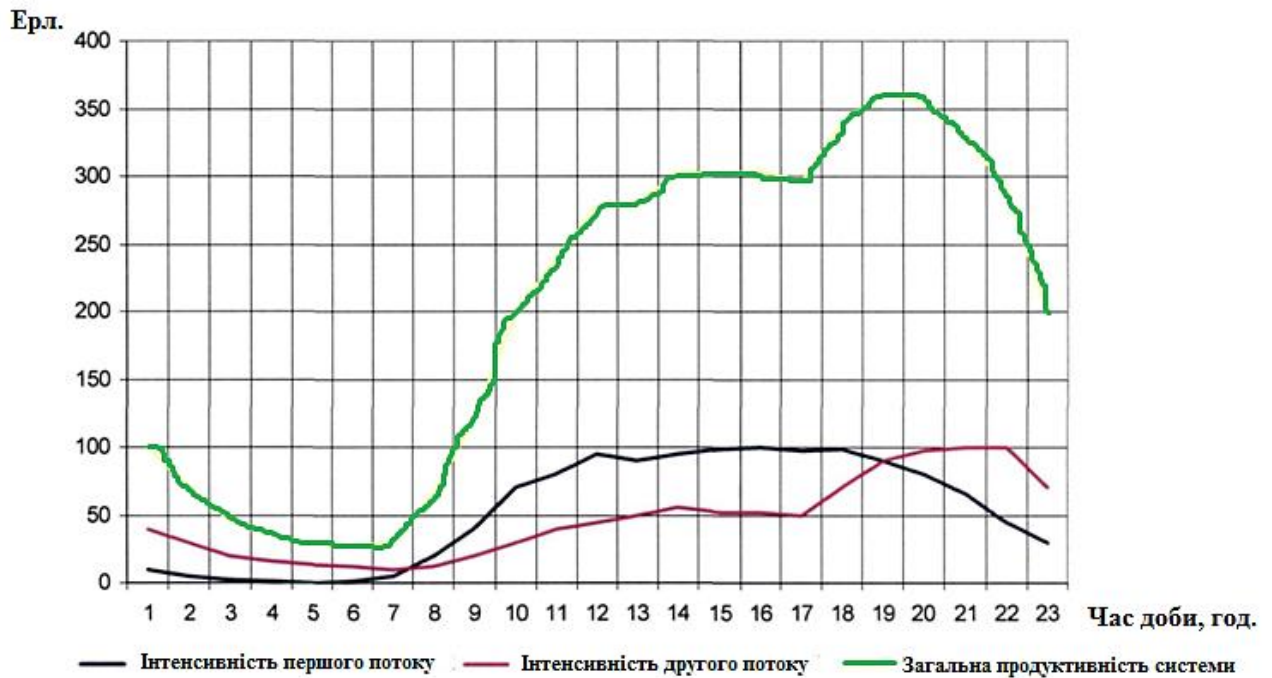


Рис. 2.15. Профіль розподілу добової продуктивності при найбільш оптимальному виборі часу використання мережних сервісів «економними» користувачами.

2.5. Висновки до 2-го розділу.

1. Аналіз існуючих методів підвищення продуктивності телекомунікаційних платформ хмарних сервісних систем показав, що, окрім застосування динамічного управління маршрутизацією в рамках масштабованої PaaS моделі, найбільш перспективними та доцільними до застосування є: метод диференційованого обслуговування користувачів, оскільки він не вимагає підвищення продуктивності програмно-технічних засобів сервісної мережної платформи, а також залишається ефективним в умовах підвищених навантажень на хмарну сервісну систему; метод адаптивного резервування ресурсів сервісної мережної платформи, що дозволяє користуватись багатошляховою маршрутизацією і уникати непродуктивних витрат мережних ресурсів магістральної мережної системи. Дослідження імовірно-часових характеристик мережної системи на основі відкритої архітектури, що пов'язане

з використанням обох методів потребує подальших досліджень, зокрема проведення комп'ютерного моделювання, що буде зроблено у 3-му розділі цієї дисертаційної роботи.

2. У розділі висловлено та доведено гіпотезу про те, що із урахуванням існування в телекомунікаційній платформі сервісної мережної системи достатньої кількості альтернативних маршрутів для обслуговування потокового трафіку запитів, доцільно відмовитися від попереднього резервування каналних ресурсів під час реалізації адаптивних методів управління потоками (ресурсного резервування). Розроблено структурно-функціональну та структурно-математичну моделі процесів обслуговування запитів у сервісній мережній системі. Параметризовано імовірності блокування запитів при використанні багатошляхової маршрутизації потокового трафіку запитів. Побудовано та описано граф переходів для такого випадкового процесу. Запропоновано математичну модель та загальний алгоритм обслуговування запитів без попереднього резервування мережних ресурсів сервісної платформи, які дозволяють оптимізувати їх використання за критерієм системної продуктивності під час оброблення потоку користувацьких запитів. Розроблено алгоритм обчислення імовірностей блокування запитів при використанні багатошляхової маршрутизації їх потокового трафіку, що може бути застосований при моделюванні транспортної підсистеми мобільних мереж четвертого та п'ятого покоління, як безпроводного сегменту сучасних сервісних мережних систем. Створено програмне забезпечення, що дозволяє проводити обчислення цих імовірностей (див. додаток). Адаптивне резервування каналних ресурсів в телекомунікаційній платформі сервісної мережної системи дозволяє обслуговувати більшу кількість запитів з якістю, зокрема тривалістю їх оброблення, що не зазнаватиме значних коливань. Відтак, за результатами моделювання спостерігається підвищення продуктивності сервісної мережної системи за обслуженням навантаженням трафіку запитів. Зокрема, при інтенсивності вхідного навантаження на сервісну мережну систему 17-20 тис. зап./с. відповідний виграш становить 16-22%, при цьому

середній час тривалості користувацьких сесій у сервісній мережній системі збільшується на 5 с. при інтенсивності навантаження більше 20 тис. зап./с.

3. Пропонується при проектуванні телекомунікаційних платформ хмарних сервісних систем виділяти і враховувати різні категорії користувачів, яким надаються різні пріоритети обслуговування, функціональні сервісні можливості, мінімальна гарантована якість сервісу тощо. При розподілі користувачів хмарних сервісних систем за категоріями відповідно до параметрів створюваного ними навантаження, необхідно враховувати інформацію про надання їм специфічних видів додаткових послуг. Проведені дослідження показують, що відсутність пріоритетів у обслуговуванні користувачів хмарних сервісних мережних систем не тільки не забезпечує задовільну якість обслуговування запитів бізнес-користувачів, але й не дозволяє підвищити ефективність використання додаткових мережних ресурсів за рахунок обслуговування запитів другого потоку від «економних» користувачів. Більше того, за відсутності диференційованого регулювання потокового навантаження, а також при відсутності його балансування, сервісна мережна система стає дотаційною. Оптимізація функціоналу системної продуктивності шляхом вибору порогу обсягу мережних ресурсів, які дозволяється виділяти під обслуговування непріоритетних користувацьких запитів, а також шляхом профілювання ГНН сервісної мережної системи дозволяє отримувати стійкий додатковий приріст продуктивності при невеликих перевантаженнях мережної системи. Однак, при виникненні великих навантажень низькопріоритетними запитами, якість обслуговування запитів пріоритетного потоку може стати незадовільною, а системна продуктивність – спадати. Варто зазначити, що можливо забезпечити вигреш за піковою добовою системною продуктивністю до 16% для випадку оптимізації часу доступу до сервісів непріоритетними користувачами (див. рис. 2.12-2.14). Детальніше методи розподілу ресурсів гетрогенних мереж зв'язку буде розглянуто у 5-му розділі цієї роботи.

4. Вибір порогу обсягу мережних ресурсів, які дозволяється виділяти під обслуговування неперіоритетних користувачьких запитів з метою створення функціональної переваги користувачів бізнес-сегменту фактично забезпечує задані параметри якості обслуговування потоку пріоритетних запитів, в тому числі – при високих навантаженнях, які створюються низькопріоритетним потоком запитів, що будуть зазнавати погіршення якості сервісу. Показники ефективності хмарних сервісних мережних систем при цьому погіршуються незначно. При зростанні інтенсивності навантаження низькопріоритетного потоку запитів мережний оператор може поступово змінювати політику, пов'язану з їх обслуговуванням, виходячи зі своїх інтересів: можливо нарощувати пропускну здатність (обсяг мережних ресурсів) і розглядати такі запити не як додаткове навантаження, а як основне з відповідним вибором пріоритету в його обслуговуванні і оптимізацією тарифної політики. Це дозволить операторам поступово та якісно нарощувати клієнтську базу і проводити більш точне прогнозування розвитку хмарних сервісних мережних систем.

5. На підставі розгляду методів підвищення продуктивності телекомунікаційних платформ хмарних сервісних систем, які базуються на диференційованому обслуговуванні користувачів та адаптивному резервуванні ресурсів сервісної мережної платформи впливає, що існує необхідність проведення подальших досліджень за допомогою імітаційного комп'ютерного моделювання з метою оцінювання і підвищення якісних показників функціонування та оптимізації розподілених мережних платформ сервісно-орієнтованої архітектури, зокрема показників сервісної доступності в умовах масштабування.

РОЗДІЛ 3

Дослідження телекомунікаційних сервісних платформ з відкритою архітектурою

3.1. Дослідження ефективності застосування відкритої архітектури у телекомунікаційних платформах національного масштабу на прикладі Parlay/OSA.

У цьому розділі продовжуємо розгляд сервісних платформ масштабованої мережної інфраструктури для надання інфокомунікаційних послуг, який частково було розпочато в розділі 1.3 із аналізом особливостей застосування методів ефективного управління трафіком запитів у другому розділі. Даний розділ присвячено дослідженню моделей і методів визначення статистичних характеристик сервісних вузлів телекомунікаційних платформ із використанням інтерфейсів відкритої сервісної архітектури Parlay API [49].

Відомо, що коефіцієнт доступності послуг інтелектуальної мережі повинен підтримуватись на рівні 99,999% [70]. Такі жорсткі вимоги щодо доступності не є обов'язковими для всіх електронних сервісів, які надаються з використанням відкритих інтерфейсів, але все ж є важливим, щоб сервіс-провайдери мали можливість підтримувати заданий SLA рівень якості послуг.

Доступність може бути визначена як відсоток часу, протягом якого система є працездатною і виконує свої функції відповідно до специфікацій [49, 101], іншими словами сервісна доступність – це імовірність того, що запит користувача буде успішно опрацьований сервісною мережною системою (одним з її електронних сервісів) в деякий момент часу. Доступність сервісної мережної системи залежить від її надійності, здатності до відновлення (оптимальної реконфігурації) та засобів технічного обслуговування. Надійність сервісної мережної платформи можна визначити, як здатність системи виконувати свої завдання за передбачуваний час при роботі в певних умовах [102]. Надійність телекомунікаційних сервісних платформ також тісно

пов'язана з такими поняттями, як функціональна стійкість, відмовостійкість і відновлюваність. Для тестування сервісних систем за даними параметрами створені спеціальні методики, що передбачають перевірку їх роботи в умовах різної завантаженості. Для тестування в рамках SaaS моделі, а саме перевірки працездатності логіки застосувань, серверів послуг (Application Servers) необхідно використовувати деякі системи моделювання [103-106].

Консорціум Eurescom визначає наступні характеристики ефективності систем класу Parlay / OSA: продуктивність, затримка запитів і час відповіді. Системна продуктивність визначається кількістю запитів, оброблених сервісними вузлами системи за деякий проміжок часу. Затримка запитів - це середній час передавання вхідних користувацьких запитів шлюзом Parlay. А час відповіді визначається швидкістю реагування системи на запити [107].

Визначимо функціональні моделі платформ Parlay API для централізованого і розподіленого варіантів відкритої архітектури. На їх основі далі будуються математичні моделі цих систем і обчислюються ймовірностно-часові характеристики, такі як середня кількість запитів у сервісній мережній системі, середній час затримки запиту в системі, а також їх залежності від інтенсивності вхідного навантаження, кількості серверів послуг та сервісних застосувань або композитних сервісів, які взаємодіють із базовим сервером послуг OSA.

Як було представлено на рис. 1.15, основними елементами відкритої сервісної архітектури систем виду Parlay є базовий сервер послуг та сервери послуг – прикладних сервісних застосувань. Як єдиний логічний елемент, сервер послуг може бути реалізований на базі декількох фізично незалежних модульних платформ [48, 101, 102, 108, 109]. Наприклад, одна його частина може бути частиною HLR або ж Mobile switching centre server, а інша – сервера, який здійснює білінг. Якщо сервер послуг повністю зосереджений на одному вузлі, то він повинен обмінюватися з вузлами мережі (наприклад - HLR і т.п.) за відповідними протоколами (наприклад - MAP, CAMEL і т.п.). Дана можливість

визначає дві основні архітектури надання мережних сервісів із використанням програмних інтерфейсів OSA виду Parlay: з централізованими серверами послуг (рис. 3.1) і розподіленими (рис. 3.2) [49].

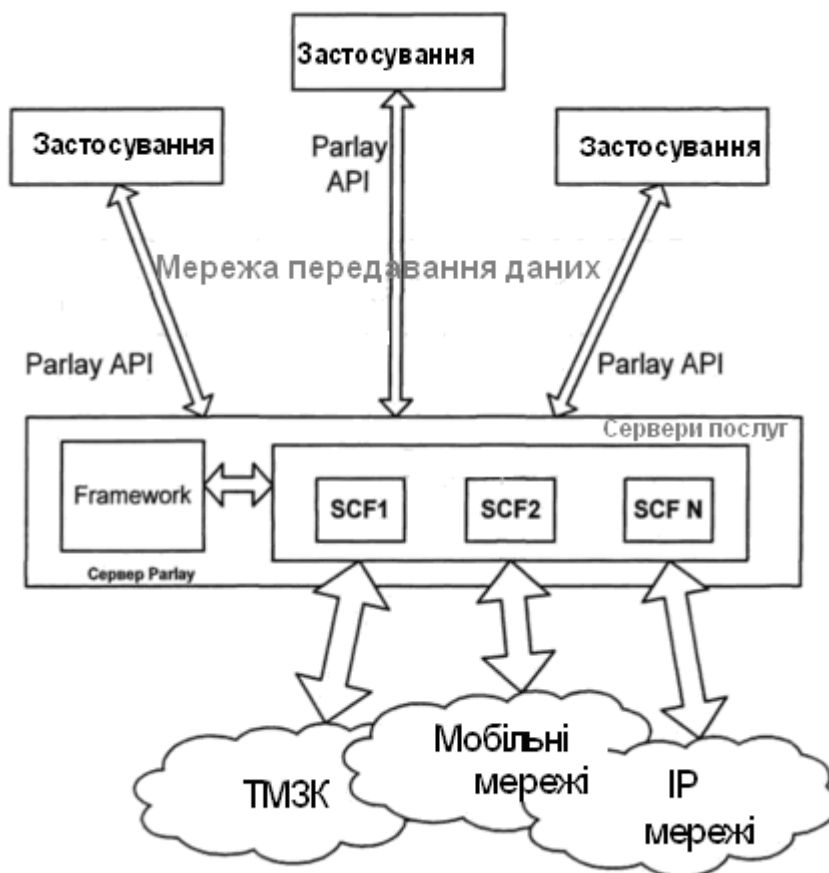


Рис. 3.1. Функціональна модель централізованого варіанту відкритої сервісної архітектури на базі системи Parlay/OSA [49].

Отже, централізований варіант побудови сервісного вузла (рис. 3.1) передбачає створення виділених серверів послуг SCF, які взаємодіють з мережними елементами з використанням існуючих протоколів. На відміну від цього варіанту, відкрита розподілена архітектура використовує функціональні можливості елементів мережі (мережної платформи згідно моделі PaaS) із використанням програмних інтерфейсів Parlay/OSA. Це передбачає, що елементи телекомунікаційної мережної платформи сервісної системи підтримують згадані інтерфейси (рис. 3.2).

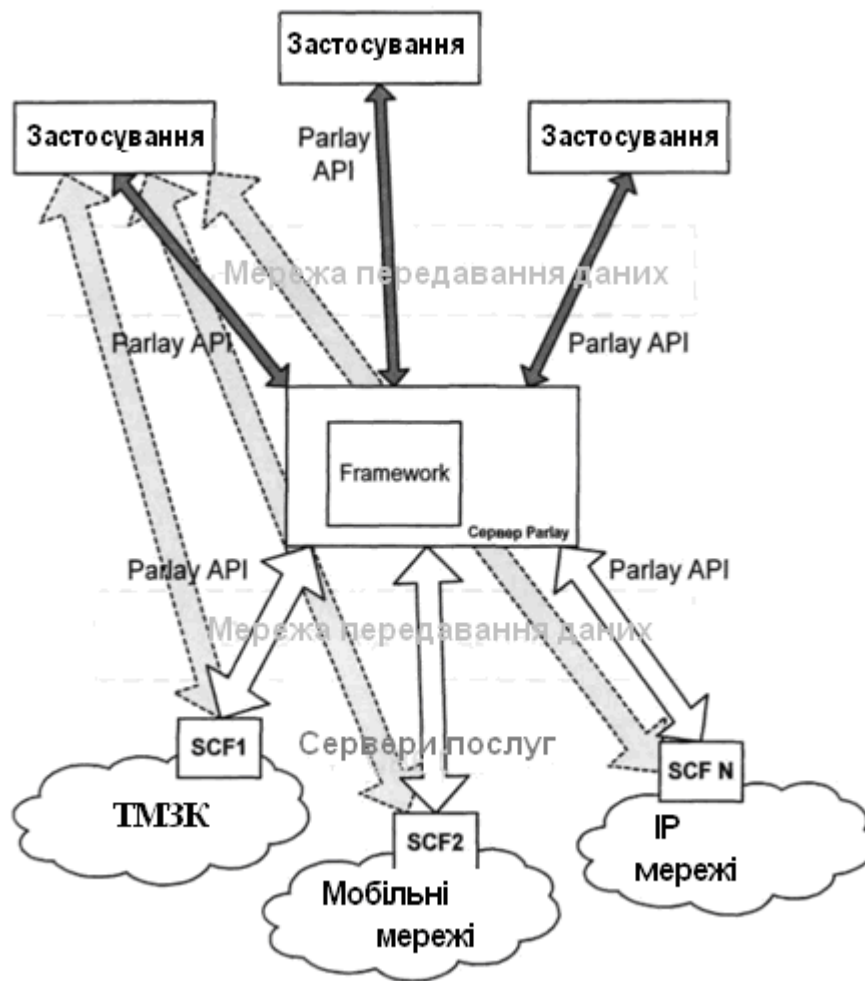


Рис. 3.2. Функціональна модель розподіленого варіанту відкритої сервісної архітектури на базі системи Parlay/OSA.

Таким чином, при розподіленому варіанті побудови (рис. 3.2), функціональні завдання сервісної мережної системи зводяться до функцій базового сервера послуг, тобто аутентифікації та авторизації, забезпечення можливості пошуку і використання серверів послуг (а також відповідних комплексних сервісів) та інших функцій, пов'язаних, зокрема, з обліком використання ресурсів системи. Варіант рис. 3.2 значно простіший з точки зору побудови, але, в той же час, передбачає більш суттєві вимоги до мережних елементів PaaS. При побудові мережі з нуля такий варіант може виявитись кращим, ніж централізований (рис. 3.1). Проте, очевидно, що у випадку впровадження подібної системи на існуючій мережі сервіс провайдера, більш економічним виявляється централізований варіант.

Об'єктами функціональних моделей, які представлені на рис. 3.1 і рис. 3.2 є:

- Джерела запитів користувачів відповідних інфокомунікаційних мережних систем;
- Інфокомунікаційні мережі, зокрема в рамках IaaS моделі (ТМЗК, мобільні та IP мережі, IN, зокрема національний сегмент мережі Інтернет – інфокомунікаційної сервісної інфраструктури);
- Шлюз послуг (наприклад, на основі Parlay API), що включає базовий сервер послуг та сервери послуг/сервісних застосувань або ж комплексних сервісів, включно з електронними послугами систем загальнодержавного значення;
- Відповідні програми-сервісні застосування;
- Мережна платформа сервісної системи, що об'єднує основні її об'єкти, пов'язуючи визначені мережні інтерфейси.

Основні відмінності між централізованим і розподіленим варіантами відкритої сервісної архітектури систем, які реалізують інтерфейси Parlay API, викликані розташуванням функціональних можливостей серверів послуг. Одним із завдань подальшого дослідження є порівняння характеристик двох описаних варіантів системи із відкритою сервісною архітектурою і надання рекомендацій щодо їх ефективного застосування.

3.1.1. Математичне моделювання PaaS, як відкритої системної архітектури.

При побудові математичної моделі системи з відкритою архітектурою, взявши за основу Parlay API (рис. 3.3-3.4) в даному дослідженні враховувалося наступне:

- Система Parlay API складається з ряду незалежних об'єктів: базового сервера послуг, серверів послуг/сервісних застосувань, сервісних застосувань і мережної платформи передавання даних;
- Під вимогами будемо розуміти потоки користувацьких запитів, які надходять від великої кількості джерел і мають показниковий розподіл інтервалів часу надходження;

- Для взаємодії між об'єктами моделі сервісної платформи з відкритою архітектурою, як правило, використовується мережа передачі даних за технологіями Ethernet, як найбільш поширеними і такими, що відповідають вимогам щодо швидкості передавання інформаційних потоків;

- Запити в систему можуть надходити безпосередньо на сервісні застосування (наприклад, запити, ініційовані самими застосуваннями або ті, які надходять через мережу Інтернет від інших (авторизованих) сервісних мережних систем) і/або на сервери застосувань;

- При взаємодії сервісного застосування та базового сервера послуг можливий запит на повторне оброблення вимоги (що часто трапляється у MeMO і передбачається теорією відкритих мереж Джексона), тобто, наприклад, вимога про встановлення IP з'єднання двох абонентів VoIP, що не зареєстровані на єдиному сервері, надходить на сервісне застосування, а процедура їх авторизації може передбачати декілька етапів.

Для аналізу відкритої системної архітектури, з урахуванням зазначених вище особливостей, може бути використана структурно-параметрична модель, представлена на рис. 3.3.

Цією моделлю представлена відкрита сервісна мережна система з використанням технології Parlay API із централізованими серверами послуг/сервісних застосувань, що об'єднує k серверів послуг/сервісних застосувань. У загальному випадку базовий сервер послуг координує надання сервісів різними застосуваннями, на які надходять запити з інтенсивностями $\gamma_1, \gamma_2, \dots, \gamma_n$. Інтенсивності оброблення запитів, які надходять застосуваннями, засобами мережної платформи, базовим сервером послуг і серверами послуг/сервісних застосувань позначені μ_{ap} , μ_{eth} , μ_{fw} і μ_{scs} , відповідно. Інтенсивності надходження запитів до системи через сервери застосувань позначені r_1, r_2, \dots, r_n , відповідно.

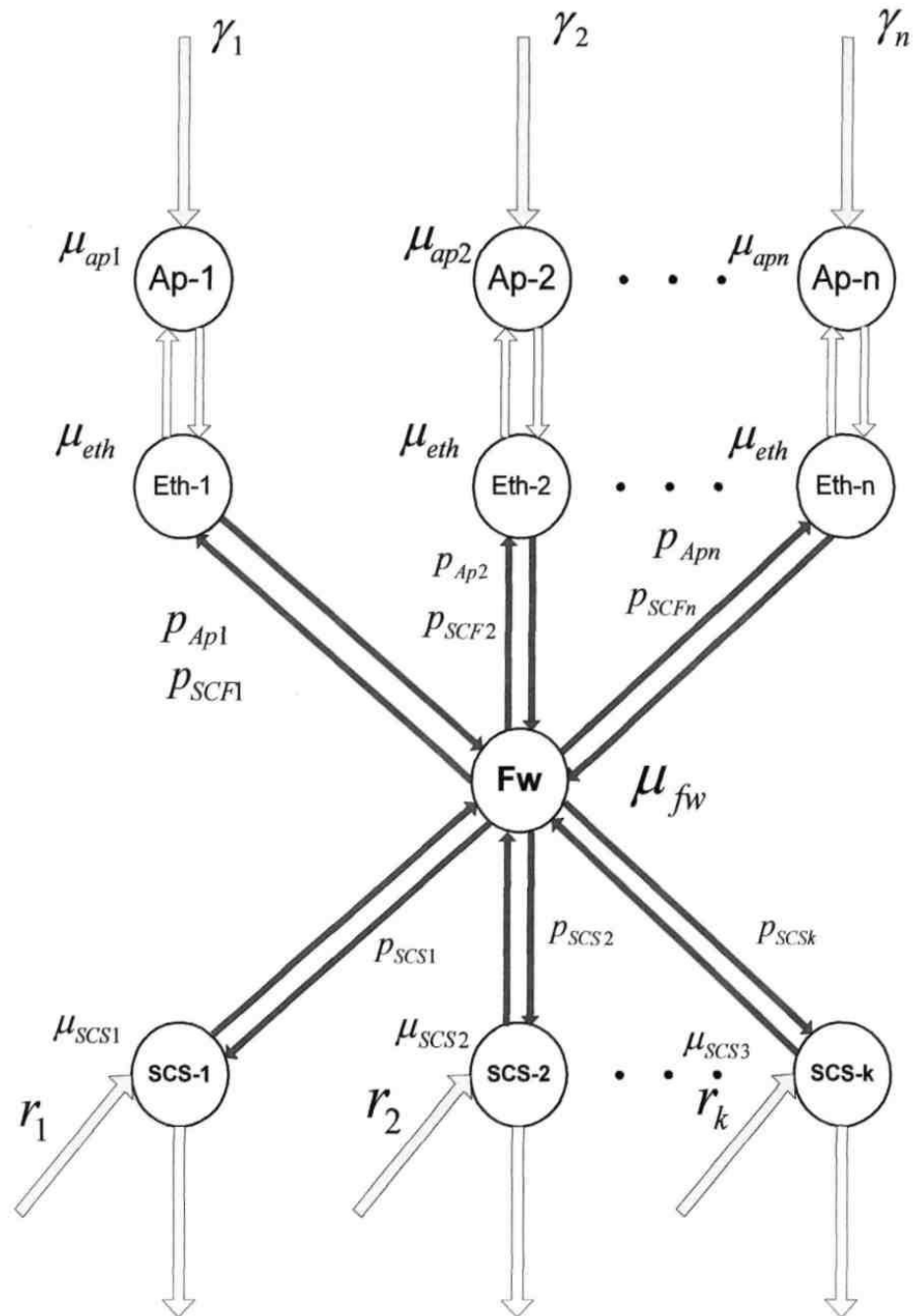


Рис. 3.3. Структурно-параметрична модель СМО відкритої сервісної платформи з централізованим сервером послуг/сервісних застосувань.

Імовірності того, що запити надійдуть на певні сервери послуг/застосувань, позначені $p_{scs1}, p_{scs2}, \dots, p_{scsk}$, а імовірності того, що після обслуговування на базовому сервері послуг запити знову надійдуть на сервери застосувань - $p_{Ap1}, p_{Ap2}, \dots, p_{Apn}$. Відповідна ймовірність визначається типом сервісів, сервісними застосуваннями, що використовуються, алгоритмами аутентифікації користувачів тощо.

Структурно-параметрична модель відкритої сервісної платформи з розподіленими серверами послуг/сервісних застосувань на прикладі Parlay API представлена на рис. 3.4. Дана модель відрізняється від моделі рис. 3.3 тим, що необхідно окремо враховувати потребу у передаванні даних через мережну платформу між базовим сервером послуг і серверами послуг/сервісних застосувань, які реалізовані безпосередньо в фізично рознесених мережних елементах сервісної платформи і, отже, не можуть взаємодіяти з базовим сервером послуг через внутрішні високошвидкісні інтерфейси.

Оскільки одним з дослідницьких завдань даної роботи є аналіз зміни ПЧХ сервісного вузла PaaS при використанні прикладного програмного інтерфейсу (на прикладі Parlay API), то необхідно розглянути математичну модель сервісного вузла [49], у якого область реалізації не виділена в окрему площину, тобто здійснена на серверній частині. Для того, щоб проводити порівняння близьких за використовуваними технологіями сервісних платформ згідно моделей, представлених на рис. 3.3 - 3.4, розглянемо також структурно-параметричну модель класичного сервісного вузла (рис. 3.5).

У структурно-параметричній моделі, представленій на рис. 3.5, процеси взаємодії сервісного вузла (SN) та інших мережних елементів є аналогічними процесам взаємодії серверів послуг/сервісних застосувань через базовий сервер послуг у моделі рис. 3.3, але логіка послуг/застосувань тут реалізується в центральному вузлі SN так само, як і системні функції координації, що відповідають за взаємодію всіх об'єктів сервісної мережної системи. Отже, SN має одночасно відповідати за процеси оброблення користувачьких запитів, комунікаційні процеси, процеси балансування навантаження тощо, що, у загальному, чинить значний стримуючий ефект на показники його продуктивності та доступності.

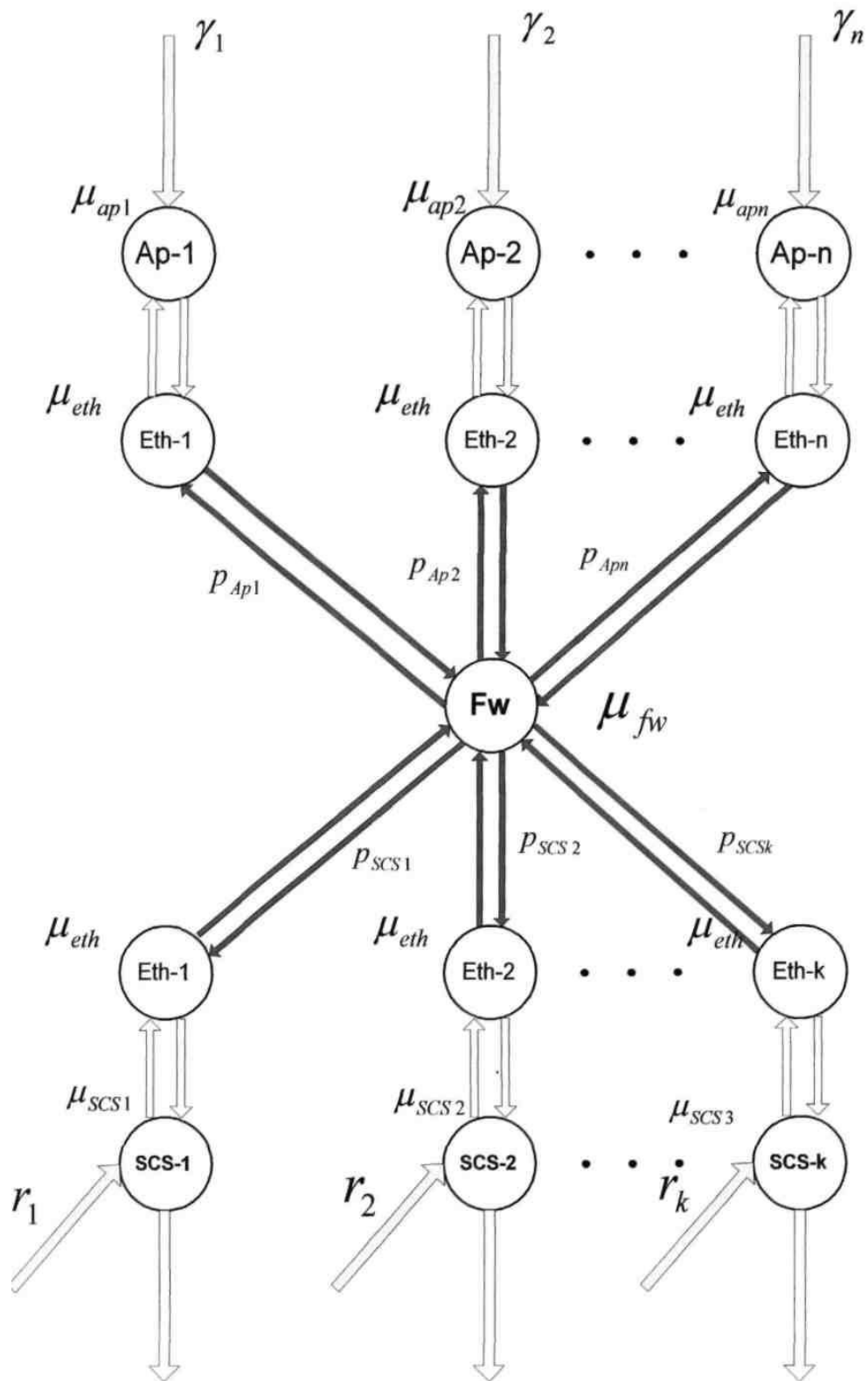


Рис. 3.4. Структурно-параметрична модель СМО відкритої сервісної платформи з розподіленими серверами послуг/ сервісних застосувань (оптимізована архітектура з підтримкою розпаралелення оброблення даних).

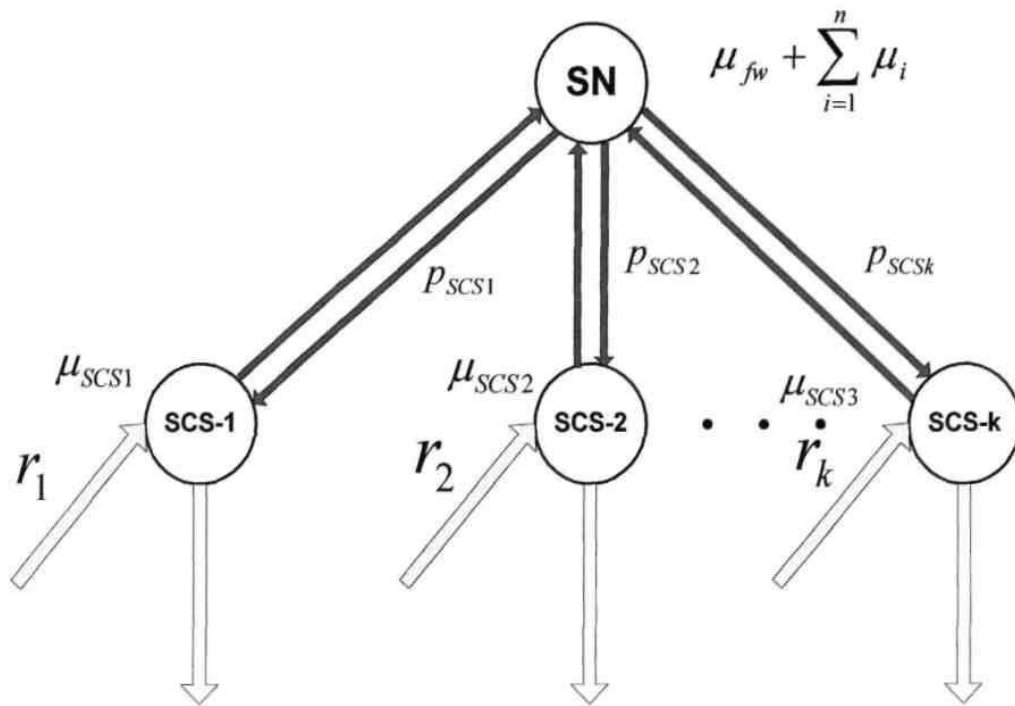


Рис. 3.5. Структурно-параметрична модель СМО сервісної платформи на основі вузла послуг (сервісного вузла SN) без API/OSA інтерфейсу.

3.1.2. Аналітичне дослідження статистичних характеристик телекомунікаційних сервісних платформ на основі відкритої системної архітектури.

Розглянуті у розділі 3.1.1 структурно-параметричні моделі (рис. 3.3 - 3.5) представляють собою скінченну кількість обслуговуючих вузлів, між якими циркулюють користувачькі запити, що переходять відповідно до маршрутної матриці мережної платформи з одного вузла в інший. У відкритій сервісній платформі вимоги можуть надходити з зовнішніх джерел, а також залишати систему після завершення обслуговування. Така система називається відкритою мережею масового обслуговування (MeMO). Якщо в момент надходження запиту всі обслуговуючі пристрої сервісного вузла зайняті, то запит займає місце в черзі буфера, де очікує деякий час початку обслуговування. При цьому запити, як правило, обслуговуються в порядку їх надходження. Під сервісним вузлом нашої системи в рамках PaaS на основі Parlay API будемо розуміти систему масового обслуговування, що складається з l однакових пристроїв ($1 < l < \infty$) і буфера з об'ємом C ($0 \leq C \leq \infty$)

запитів.

Для дослідження характеристик відкритих мереж масового обслуговування застосуємо методи складання рівнянь локального балансу, відповідно до теорії відкритих мереж масового обслуговування Джексона, яка передбачає можливість урахування процесів дообслуговування запитів [110].

При цьому, згідно спільних досліджень у [237], будемо вважати, що:

M - загальна кількість об'єктів сервісної мережної системи, що включає в себе базовий сервер послуг (який утворює Parlay framework), сервери застосувань, а також мережі передавання даних обраної мережної платформи;

$\mu_i(n_i)$ - Загальна інтенсивність обслуговування запитів у i -му об'єкті моделі (l_i - загальна кількість обслуговуючих пристроїв у заданому сервісному вузлі). У випадку, коли інтенсивність обслуговування запитів не залежить від кількості запитів у системі (відсутність масштабування), загальна інтенсивність обслуговування будь-якого об'єкта сервісної системи може бути визначена виразом:

$$\mu_{ш}(n_i) = \begin{cases} n_i \cdot \mu_i, & 0 \leq n_i \leq l_i \\ l_i \cdot \mu_i, & n_i > l_i, \quad i = \overline{1, M} \end{cases}, \quad (3.1)$$

де λ_i - загальна інтенсивність надходження запитів у i -ий об'єкт моделі;

$\lambda(N)$ - загальна інтенсивність надходження запитів до сервісної платформи (в загальному випадку ця інтенсивність залежить від кількості запитів у сервісній системі мережній Parlay API);

$n_i(t)$ - кількість запитів, які перебувають у i -ому об'єкті моделі в момент часу t ;

Введемо в розгляд багатовимірний випадковий процес $N(t) = \{n_1(t), n_2(t), \dots, n_M(t)\}$, і позначимо через:

$$P(n, t) = P\{k_1(t) = n_1, n_2(t) = n_2, \dots, n_M(t) = n_M, t\}$$

ймовірність того, що в момент часу t сервісна мережна система знаходиться в стані (n_1, n_2, \dots, n_M) . При цьому нехай маршрут переходу повідомлення з одного мережного об'єкта PaaS в інший задається матрицею маршрутів P . Таким

чином, P - ймовірність того, що повідомлення, яке йде від i -го об'єкта мережної системи надійде в j -ий. Очевидно, що при цьому виконується рівність

$$\sum_{j=0}^M P_{ij} = 1 \quad (i = 0, 1, \dots, M).$$

За проміжок часу Δt можливі наступні переходи у станах мережних об'єктів:

- Поява нового запиту на одному з об'єктів сервісної мережної системи;
- Запит залишає об'єкт сервісної мережної системи;
- Запит передається на обслуговування від одного об'єкта в інший;
- Не відбувається змін.

Таким чином, ймовірність того, що сервісна мережна система буде перебувати в стані $\{n_1, n_2, \dots, n_M\}$ в момент часу $t + \Delta t$, може бути представлена рівнянням (3.2):

$$\begin{aligned} P(n_1, n_2, \dots, n_M; t + \Delta t) = & \sum_{i=1}^M P(n_1, n_2, \dots, n_{i-1}, n_i - 1, n_{i+1}, \dots, n_M; t) \cdot \Lambda(N-1) \cdot P_{0,i} \cdot \Delta t + \\ & \sum_{j=1}^M P(n_1, n_2, \dots, n_{j-1}, n_j + 1, n_{j+1}, \dots, n_M; t) \cdot \mu_j(n_j + 1) \cdot P_{j,0} \cdot \Delta t + \\ & \sum_{i=1}^M \sum_{j=1}^M P(n_1, n_2, \dots, n_{i-1}, n_i - 1, n_{i+1}, \dots, n_{j-1}, n_j + 1, n_{j+1}, \dots, n_M; t) \cdot \mu_j(n_j + 1) \cdot P_{j,i} \cdot \Delta t + \\ & + P(n_1, n_2, \dots, n_M; t) \cdot \left(1 - \Delta t \sum_{j=1}^M (\Lambda(N) + \mu_j(n_j)) \right) \end{aligned} \quad (3.2)$$

Розділимо обидві частини виразу (3.2) на Δt і перейдемо до границі при $\Delta t \rightarrow 0$, при цьому отримаємо систему диференціальних рівнянь Колмогорова:

$$\begin{aligned} \frac{d}{dt} \{P(n_1, n_2, \dots, n_M; t)\} = & \sum_{i=1}^M P(n_1, n_2, \dots, n_{i-1}, n_i - 1, n_{i+1}, \dots, n_M; t) \cdot \Lambda(N-1) \cdot P_{0,i} + \\ & + \sum_{j=1}^M P(n_1, n_2, \dots, n_{j-1}, n_j + 1, n_{j+1}, \dots, n_M; t) \cdot \mu_j(n_j + 1) \cdot P_{j,0} + \\ & + \sum_{i=1}^M \sum_{j=1}^M P(n_1, n_2, \dots, n_{i-1}, n_i - 1, n_{i+1}, \dots, n_{j-1}, n_j + 1, n_{j+1}, \dots, n_M; t) \cdot \mu_j(n_j + 1) \cdot P_{j,i} + \\ & + \left(\sum_{j=1}^M P(n_1, n_2, \dots, n_M; t) \cdot (\Lambda(N) + \mu_j(n_j)) \right) \end{aligned} \quad (3.3)$$

Остаточно, розглянемо розв'язок системи (3.3) у *стаціонарному* режимі.

Прирівнюючи до нуля похідні в лівій частині цієї системи рівнянь, отримуємо наступну систему рівнянь:

$$\begin{aligned}
 & \sum_{j=1}^M P(n_1, n_2, \dots, n_M; t) \cdot (\Lambda(N) + \mu_i(n_j)) = \\
 & = \sum_{i=1}^M P(n_1, n_2, \dots, n_{i-1}, n_i - 1, n_{i+1}, \dots, n_M; t) \cdot \Lambda(N - 1) \cdot P_{0,i} + \\
 & + \sum_{j=1}^M P(n_1, n_2, \dots, n_{j-1}, n_j + 1, n_{j+1}, \dots, n_M; t) \cdot \mu_j(n_j + 1) \cdot P_{j,0} + \\
 & \sum_{i=1}^M \sum_{j=1}^M P(n_1, n_2, \dots, n_{i-1}, n_i - 1, n_{i+1}, \dots, n_{j-1}, n_j + 1, n_{j+1}, \dots, n_M; t) \cdot \mu_j(n_j + 1) \cdot P_{j,i}
 \end{aligned} \tag{3.4}$$

З метою спрощення запишемо систему (3.4) в компактнішому вигляді:

$$\begin{aligned}
 & \sum_{j=1}^M P(n) \cdot [\Lambda(N) + \mu_i(n_j)] = \\
 & = \sum_{i=1}^M P(n - 1_i) \cdot \Lambda(N - 1) \cdot P_{0,i} + \sum_{j=1}^M P(n + 1_j) \cdot \mu_j(n_j + 1) \cdot P_{j,0} + \\
 & + \sum_{i=1}^M \sum_{j=1}^M P(n - 1_i + 1_j) \cdot \mu_j(n_j + 1) \cdot P_{j,i}
 \end{aligned} \tag{3.5}$$

де 1_i і 1_j - вектори, у яких i і j координати відповідно рівні 1, а інші - нулю.

За фізичним змістом, ліва частина виразу (3.5) представляє собою інтенсивність переходів зі стану n , а права – швидкість переходів у цей стан.

Враховуючи, що:

$$\lambda_i = \lambda_{0,i} + \sum_{j=1}^M \lambda_j \cdot P_{j,i}, \quad i = 1, 2, \dots, M, \tag{3.6}$$

введемо поняття коефіцієнтів передавання e_i таких що $\lambda_i = e_i \cdot \Lambda(N)$ Тоді систему рівнянь (3.6) можна переписати в наступному вигляді:

$$e_i = P_{0,i} + \sum_{j=1}^M e_j \cdot P_{j,i}, \tag{3.7}$$

де $P_{0,i}$ - імовірність того, що в цей вузол надійде запит із зовнішнього джерела.

Представимо формулу (3.7) в наступному вигляді:

$$1 = \frac{\sum_{j=1}^M e_j \cdot P_{j,i}}{e_i - P_{0,i}} = \sum_{j=1}^M \frac{e_j}{(e_j - P_{0,i})} \cdot P_{j,i} = \sum_{i=1}^M \frac{e_i}{(e_j - P_{0,j})} \cdot P_{i,j} \quad (3.8)$$

Підставляючи одержані співвідношення у (3.5) маємо:

$$\begin{aligned} & \sum_{j=1}^M \sum_{i=1}^M \frac{e_i}{(e_j - P_{0,j})} \cdot P_{i,j} \cdot P(n) \cdot (\Lambda(N) + \mu_j(n_j)) = \\ & = \sum_{i=1}^M \sum_{j=1}^M \frac{e_j}{(e_i - P_{0,i})} \cdot P_{j,i} \cdot P(n-1_i) \cdot \Lambda(N-1) P_{0,i} + \\ & + \sum_{j=1}^M \sum_{i=1}^M \frac{e_i}{(e_j - P_{0,j})} \cdot P_{i,j} \cdot P(n+1_j) \cdot \mu_j(n_j) \cdot P_{j,0} + \sum_{i=1}^M \sum_{j=1}^M P(n-1_i + 1_j) \cdot \mu_j(n_j) \cdot P_{j,i} \end{aligned} \quad (3.9)$$

Очевидно, що дане співвідношення виконується за умови рівності:

$$\begin{aligned} & \frac{e_i}{(e_j - P_{0,j})} \cdot P_{i,j} \cdot P(n) \cdot (\Lambda(N) + \mu_j(n_j)) = \frac{e_j}{(e_i - P_{0,i})} \cdot P_{j,i} \cdot P(n-1_i) \cdot \Lambda(N-1) P_{0,i} + \\ & \frac{e_i}{(e_j - P_{0,j})} \cdot P_{i,j} \cdot P(n+1_j) \cdot \mu_j(n_j) \cdot P_{j,0} + P(n-1_i + 1_j) \cdot \mu_j(n_j) \cdot P_{j,i} \end{aligned} \quad (3.10)$$

або

$$\begin{aligned} P(n) = & P(n-1_i) \cdot \frac{\Lambda(N-1)}{(\Lambda(N) + \mu_j(n_j))} \cdot \frac{e_j (e_j - P_{0,j})}{e_i \cdot (e_i - P_{0,i})} \cdot \frac{P_{j,i}}{P_{i,j}} \cdot P_{0,i} + \\ & + P(n+1_j) \cdot \frac{\mu_j(n_j)}{(\Lambda(N) + \mu_j(n_j))} \cdot P_{j,0} + P(n-1_i + 1_j) \cdot \frac{\mu_j(n_j)}{(\Lambda(N) + \mu_j(n_j))} \cdot \frac{P_{j,i}}{P_{i,j}} \cdot \frac{(e_j - P_{0,j})}{e_i} \end{aligned} \quad (3.11)$$

З рекурентного виразу (3.11) випливає, що:

$$P(n) = \frac{\Lambda^*(N)}{G(N)} \cdot \prod_{i=1}^M Z_i(n_i), \quad (3.12)$$

де

$$\Lambda^*(N) = \prod_{i=1}^M \Lambda(i-1) \text{ при } M=1,2,\dots, \text{ а}$$

$$Z_i(n_i) = \frac{e_i^{n_i}}{\prod_{j=1}^{n_i} \mu_i(j)},$$

є нормалізуючою константою, визначеною з умови нормування $1 = \sum_{n \in S(N,M)} P(n)$. Через

$S(N, M)$ позначено множину M -вимірних векторів з невід'ємними цілочисельними координатами:

$$S(N, M) = \left\{ n; n_i \geq 0, \sum_{i=1}^M n_i = N \right\}.$$

Причому, якщо інтенсивність вхідного потоку запитів в модельовану PaaS не залежить від кількості запитів, які перебувають у сервісній мережній системі і дорівнює $\Lambda(N) = \Lambda^{n_i}$, то вираз для $\Lambda^*(N)$ набуває такого вигляду:

$$\Lambda^*(N) = \prod_{R=1}^M \Lambda(R-1) = \prod_{i=1}^M \Lambda^{n_i},$$

а формула (3.12):

$$P(n) = \prod_{i=1}^M P_i(n_i), \quad (3.13)$$

де $P_i(n_i)$ - стаціонарна ймовірність того, що в i -му сервісному вузлі, який розглядається ізольовано, знаходиться n_i вимог:

$$P_i(n_i) = P_i(0) \cdot \Lambda^{n_i} \cdot Z_i(n_i). \quad (3.14)$$

Формули (3.12) і (3.13) є основними для дослідження характеристик відкритих сервісних мережних систем, зокрема таких, що реалізуються на основі інтерфейсів Parlay API.

Таким чином показано, що рішення (3.14) для відкритої сервісної мережної системи має мультиплікативну форму, яка допускає декомпозицію системи на окремі вузли. Даний результат представляється нетривіальним, тому що потоки у відкритих мережах масового обслуговування з довільною матрицею не є пуассонівськими [111 - 113].

Таким чином, у цьому розділі були одержані аналітичні вирази для знаходження основних показників якості функціонування системи на базі відкритих сервісних інтерфейсів, представленої у вигляді відкритої однорідної експоненційної мережі масового обслуговування Джексона. Формули (3.12) - (3.14) дозволяють визначити ймовірність знаходження сервісних вузлів системи в заданому стані, а також математичні очікування числа запитів і середній час перебування запитів у сервісних

вузлах сервісної платформи. Перелічені результати можуть бути отримані при відомих інтенсивностях обслуговування запитів у вузлах сервісної системи (результати досліджень характеристик відкритої сервісної платформи на базі Parlay API приводяться в розділах 3.1.3-3.1.5 цієї роботи) і за визначеної маршрутної матриці сервісної мережної платформи, тобто при відомих ймовірностях переходів запитів між сервісними вузлами, що підтримують відповідні сервісні застосування [114, 115].

3.1.3. Залежності базових характеристик опрацювання запитів від параметрів телекомунікаційної сервісної платформи.

Як вже було зазначено, основними характеристиками досліджуваної сервісної мережної системи є середня кількість запитів в системі, а також середня тривалість обслуговування запитів, яка на пряму характеризує її продуктивність. Розглянемо експериментальні залежності цих характеристик від параметрів сервісної мережної платформи, до яких слід віднести:

- кількість сервісних застосувань;
- інтенсивність надходження запитів на сервісні застосування ззовні;
- кількість серверів послуг/сервісних застосувань та їх функціональних компонент;
- інтенсивність надходження запитів на сервери послуг ззовні;
- ймовірність повторного обслуговування запитом сервісним застосуванням після обслуговування на базовому сервері послуг тощо.

Таким чином, відповідні експериментальні дослідження та оцінювання основних параметрів сервісної мережної платформи здійснювалися згідно з наведеними у попередньому розділі формулами (3.12) – (3.14).

3.1.3.1. Залежність характеристик сервісної мережної платформи від кількості реалізованих комплексних сервісів.

У даному підпункті наведено графіки, що показують зміни характеристик сервісної мережної платформи при збільшенні кількості сервісних застосувань або комплексних сервісів, які реалізуються на її основі. Розглянута система

включає 5 різних серверів послуг/сервісних застосувань, до яких можуть звертатися користувачі та інші застосування для виконання своїх запитів. Розглядається два різновиди організації надання комплексних сервісів, що визначаються різними ймовірностями $p_{\text{Арі}}$, а саме – ймовірностями виникнення необхідності повторного обслуговування запиту деяким сервісним застосуванням.

Суцільною лінією на рис. 3.6 представлена залежність кількості запитів у сервісній мережній системі від кількості сервісних застосувань, при ймовірності необхідності повторного обслуговування запиту деяким сервісним застосуванням $p_{\text{Арі}} = 0,1$ (рис. 3.6 – Parlay-1). Друга залежність побудована для $p_{\text{Арі}} = 0,5$ (рис. 3.6 – Parlay-2). При цьому вважається, що навантаження між застосуваннями розподіляється рівномірно. Інтенсивність надходження запитів на сервісні застосування не дорівнює нулю, а інтенсивність надходження запитів на сервери послуг/сервісних застосувань залишається постійною. Розрахунки проводилися відповідно до формули (3.14).

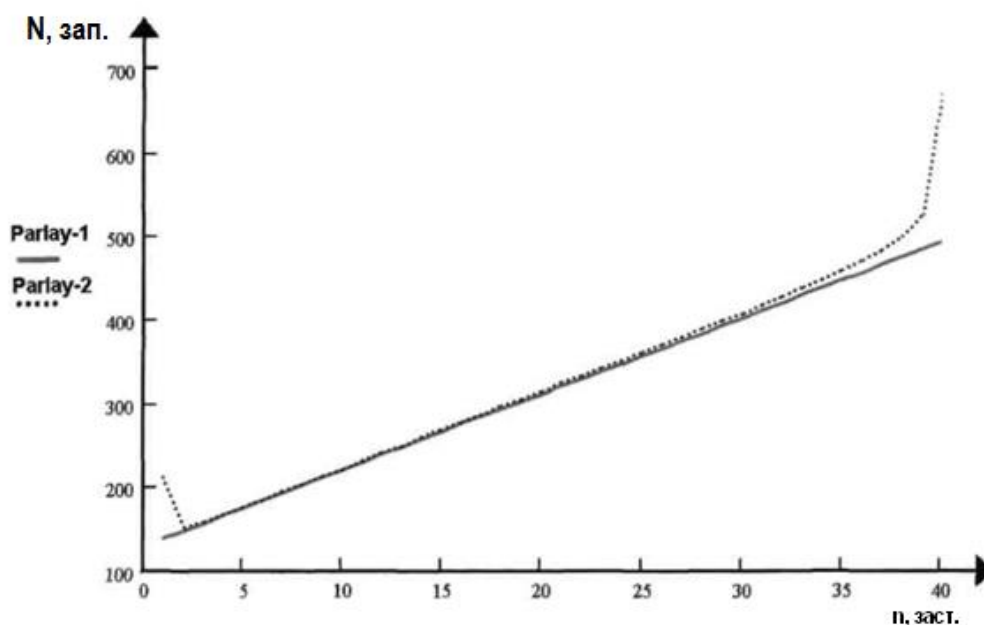


Рис. 3.6. Залежність середньої кількості запитів у сервісній мережній системі від кількості реалізованих у ній комплексних сервісів [49].

Як видно з графіка, що представлений на рис. 3.6, при функціонуванні

одних і тих самих комплексних сервісів, характеристики сервісних мережних систем із різною імовірністю повторного обслуговування запитів сильно розрізняються. Це пов'язано з тим, що при роботі деякого одного сервісу в сервісній мережній системі все навантаження, що надходить на сервери послуг, обробляється одним сервером застосувань і при ймовірності $p_{\text{Арі}}$ рівній 0,5, коефіцієнт використання такого сервера близький до 1. При збільшенні кількості комплексних застосувань, які реалізуються в досліджуваній PaaS, наведені характеристики практично не відрізняються. Одержані залежності підтверджено експериментально. Відбувається зменшення середнього часу перебування запитів у системі (рис. 3.7), до того ж збільшується загальна інтенсивність надходження вимог до системи за рахунок збільшення числа доступних сервісних застосувань, а коефіцієнт їх використання зменшується, тому що навантаження на сервери застосувань не зростає.

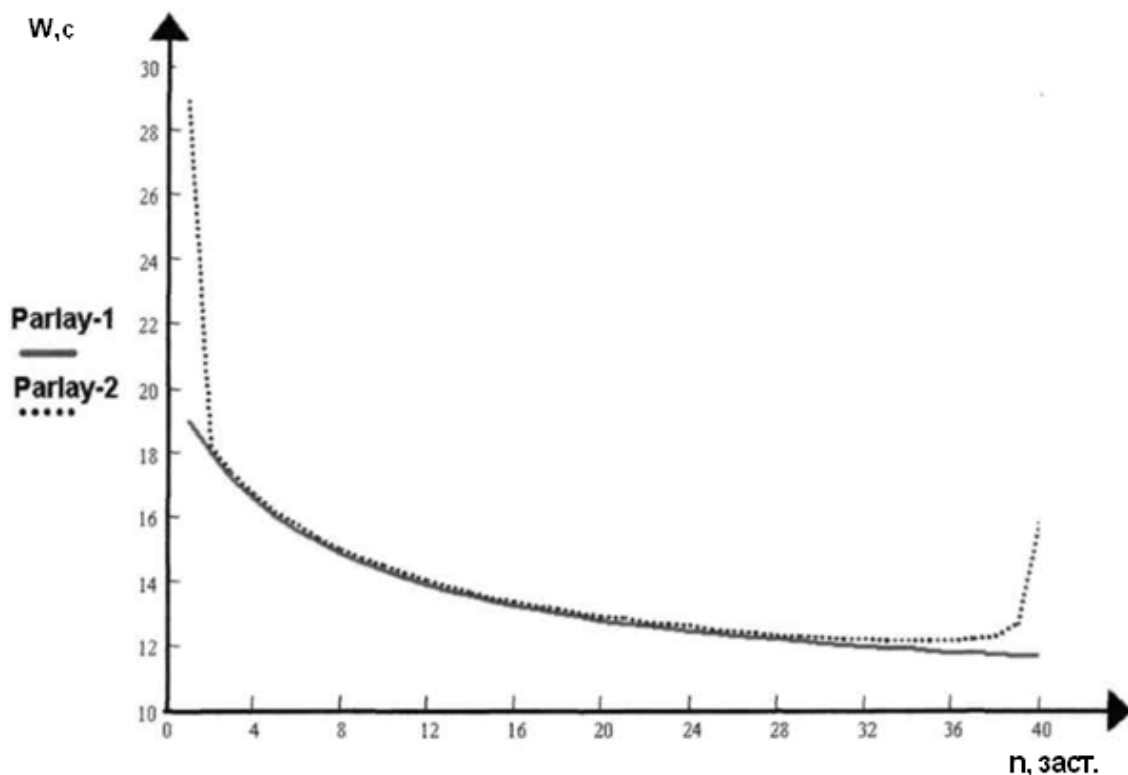


Рис. 3.7. Залежність середнього часу обслуговування запитів у сервісній мережній системі від кількості реалізованих у ній комплексних сервісів [49].

Покращення характеристик сервісної мережної системи відбувається до тих пір, поки загальне вхідне навантаження запитів не призводить до перевантаження базового сервера послуг (сервісної мережної платформи Parlay/OSA). Як видно з графіка (рис. 3.7 – Parlay-2), для $P_{\text{Api}} = 0,5$ це відбувається при одночасному функціонуванні близько 40 комплексних сервісних застосувань.

3.1.3.2. Залежність характеристик сервісної мережної платформи від кількості серверів послуг/сервісних застосувань.

Аналогічно до залежності середньої кількості запитів у системі від кількості комплексних сервісів, які нею підтримуються, залежність, що представлена на рис. 3.8, носить практично лінійний характер, і наведені функції відрізняються при великих значеннях кількості серверів послуг.

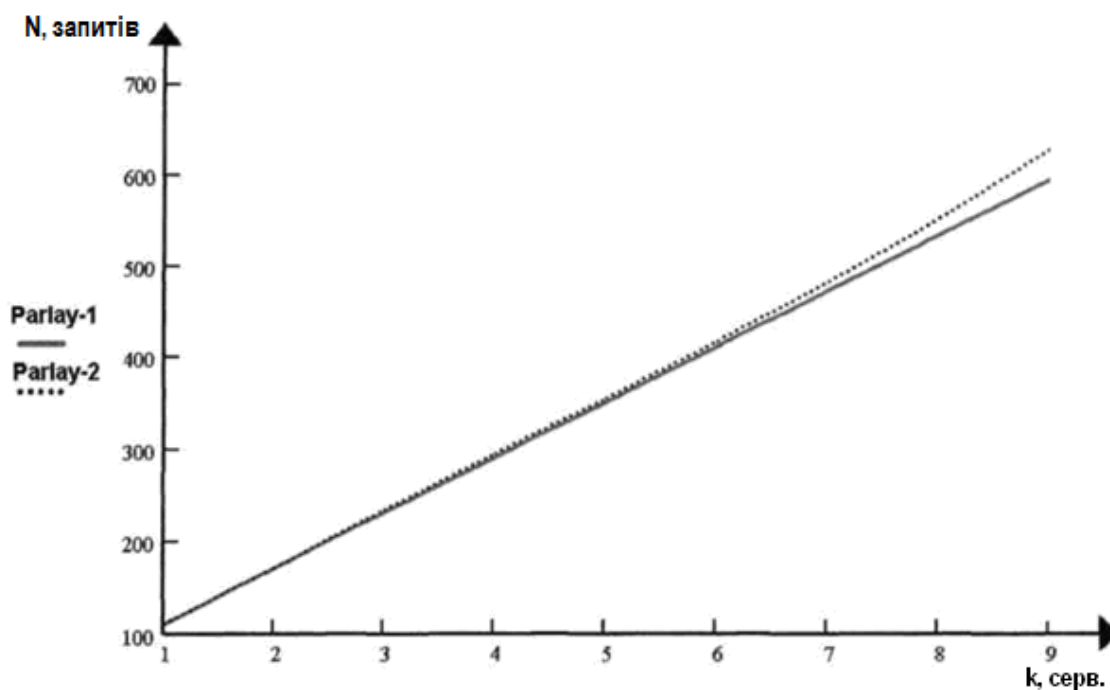


Рис. 3.8. Залежність середньої кількості запитів у сервісній мережній системі від кількості серверів послуг/сервісних застосувань [49].

Величина середнього часу перебування запитів у сервісній мережній системі, в основному, визначається під час експериментів тривалістю обслуговування запитів на серверах послуг, але, у сервісних мережних платформах з великою кількістю серверів послуг значну затримку починають вносити комплексні сервіси, телекомунікаційна мережна система сервісної платформи і базовий сервер послуг (рис. 3.9).

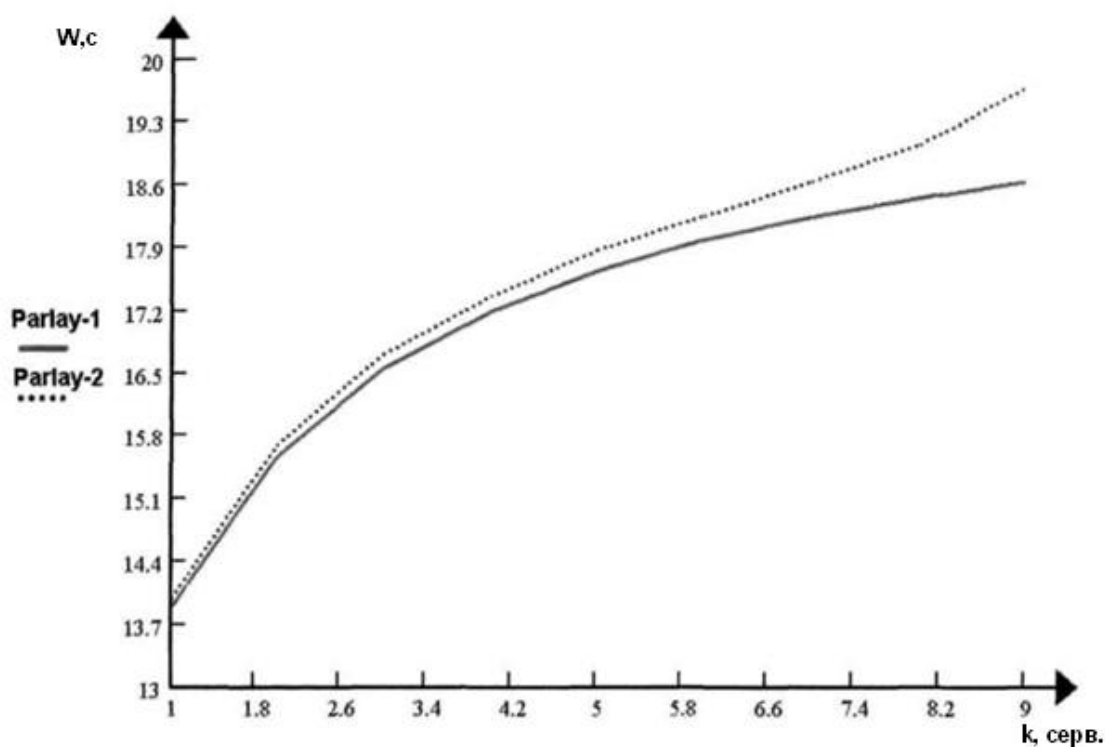


Рис. 3.9. Залежність середнього часу обслуговування запитів у сервісній мережній системі від кількості серверів послуг/сервісних застосувань [49].

Значне збільшення часу перебування запитів на опрацюванні у сервісній мережній системі відбувається за умови, коли коефіцієнт використання одного з об'єктів в PaaS наближається до 1. На графіку рис. 3.9 при 9 серверах послуг (тобто $k = 9$) коефіцієнт використання базового сервера послуг стає рівним 0,91, а відповідного сервера застосувань - 0,8, що показує - в цій конфігурації сервісна мережна система працює в неоптимальному режимі, внаслідок чого різко зростає середній час обслуговування запитів.

3.1.3.3. Залежність характеристик сервісної мережної платформи від інтенсивності надходження запитів на сервери застосувань.

Залежності характеристик сервісної мережної системи від інтенсивності надходження запитів на сервери застосувань, які представлені на рис. 3.10 - 3.11 схожі на графіки, наведені в розділі 3.1.3.2, оскільки характеристики сервісної платформи визначаються, в основному, інтенсивністю надходження запитів до системи, а не кількістю серверів застосувань.

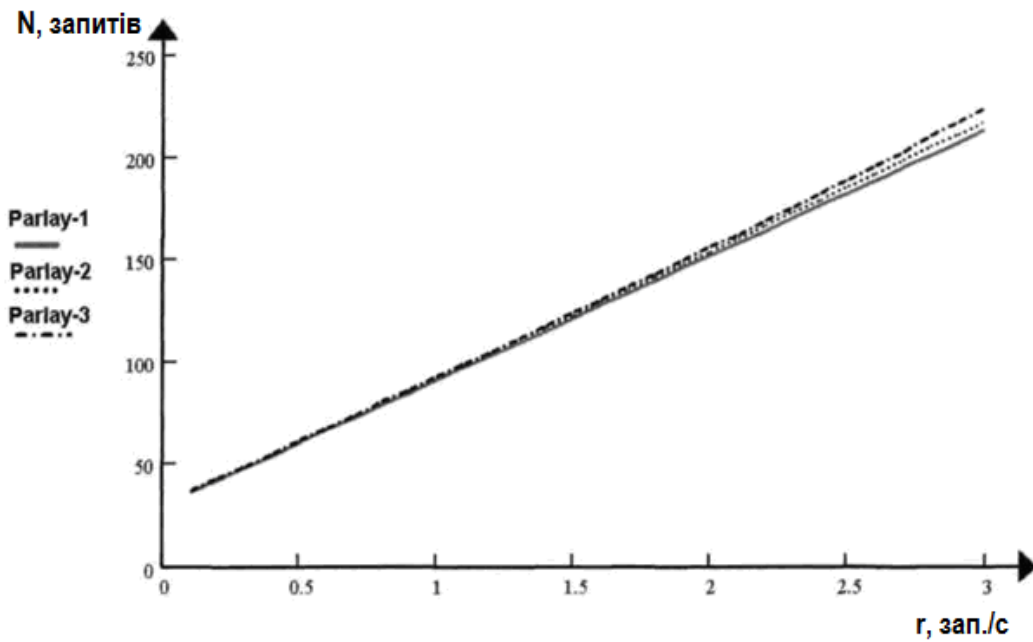


Рис. 3.10. Залежність середньої кількості запитів, що перебувають у сервісній мережній системі від інтенсивності надходження запитів на сервери послуг (серверів застосувань - 3; комплексних сервісів - 3; інтенсивність надходження запитів на комплексні сервіси 1; $\mu_{ap} = 10$; $\mu_{eth} = 50$; $\mu_{fw} = 50$; $\mu_{scs} = 0.1$; кількість обслуговуючих пристроїв досліджуваного сегменту PaaS SCS-100).

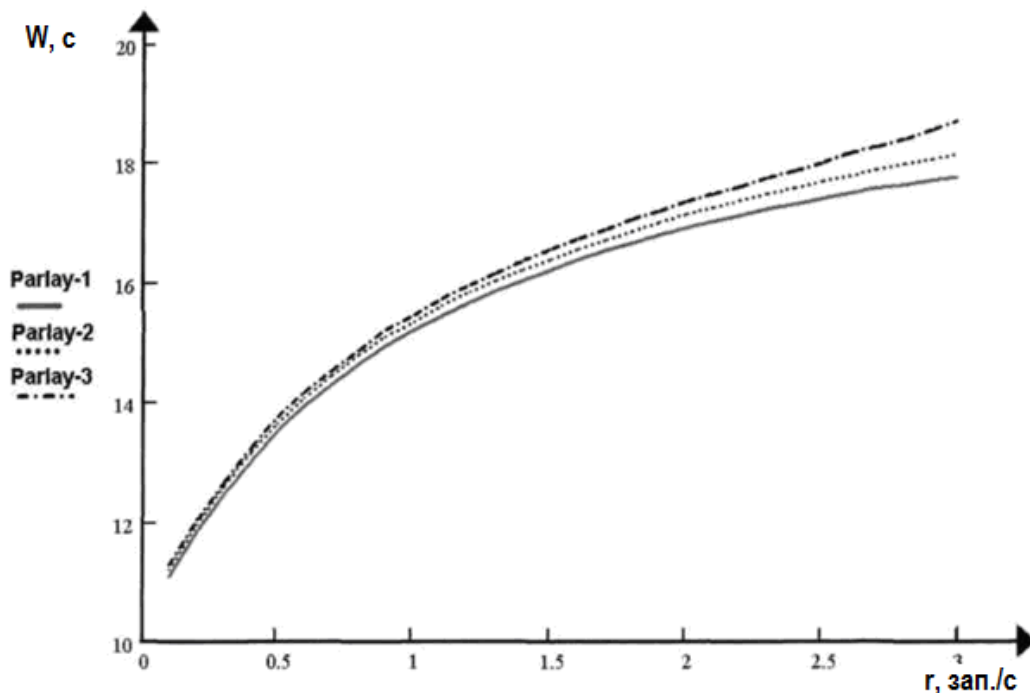


Рис. 3.11. Залежність середнього часу обслуговування запитів у сервісній мережній системі від інтенсивності надходження запитів на сервери послуг(застосувань) (серверів застосувань - 3; комплексних сервісів - 3; інтенсивність надходження запитів на комплексні сервіси 1; $\mu_{ap} = 10$; $\mu_{eth} = 50$; $\mu_{fw} = 50$; $\mu_{scs} = 0.1$ кількість обслуговуючих пристроїв досліджуваного сегменту PaaS SCS-100).

3.1.3.4. Залежність характеристик сервісної мережної платформи від ймовірності повторного обслуговування запитів сервісними застосуваннями.

У даному підпункті представлені залежності характеристик сервісної мережної системи від ймовірності повторного дообслуговування запитів комплексним сервісом на деякому сервері застосувань, яка пропорційна кількості послідовних попередніх етапів перед фінальним обслуговуванням запитів, пов'язаних з авторизацією, пошуком і вибором функціональних компонентів комплексних сервісних застосувань (див. рис. 3.12).

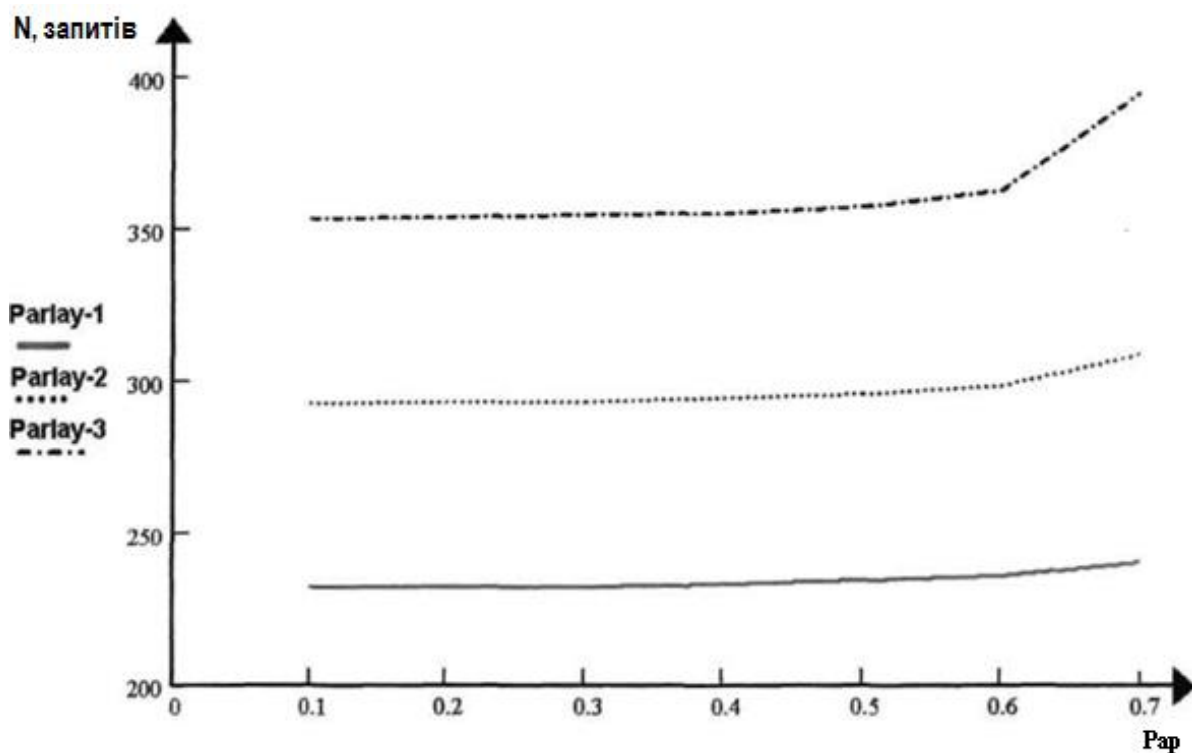


Рис. 3.12. Залежність середньої кількості запитів, що перебувають у сервісній мережній системі від ймовірності повторного дообслуговування запитів сервісними застосуваннями.

Криві на рис. 3.10-3.13, які позначено Parlay-3 побудовані розрахунково та експериментально для випадку класичного сервісного вузла без застосування відкритої сервісної системної архітектури виду Parlay. На рис. 3.12 видно, що виграш за продуктивністю по кількості запитів, які перебувають у сервісній мережній платформі від застосування відкритої сервісної архітектури складає до 17%.

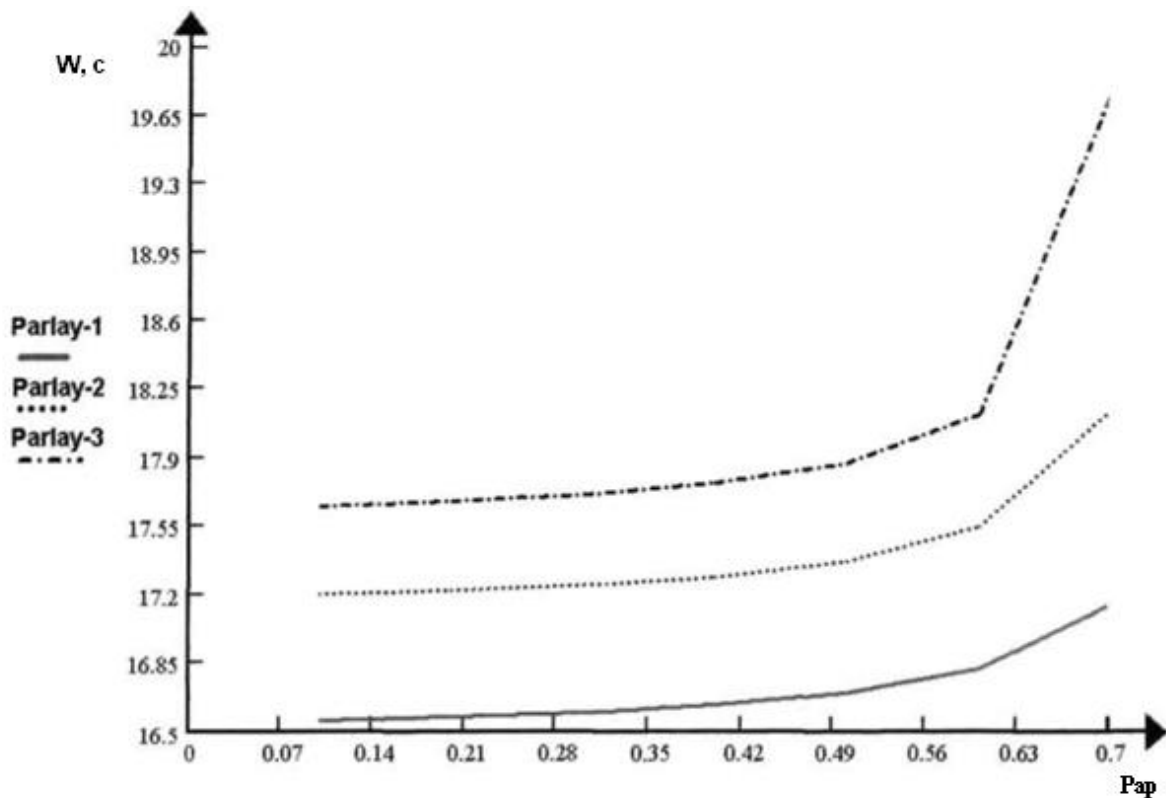


Рис. 3.13. Залежність середнього часу обслуговування запитів у сервісній мережній системі від ймовірності повторного дообслуговування запитів сервісними застосуваннями.

Як видно з графіків, які представлено на рис. 3.12 та рис. 3.13 характеристики залишаються практично постійними на ділянці ймовірності повторного дообслуговування запитів сервісними застосуваннями від 0,1 до 0,5. Подальші зміни характеристик на практиці сильно залежать від параметрів сервісної мережної платформи, тобто від кількості серверів послуг і комплексних сервісів, які вони надають. З рис. 3.13 видно, що виграш за продуктивністю по тривалості оброблення запитів, які перебувають у PaaS від застосування відкритої сервісної архітектури виду Parlay складає від 3% при найпростіших запитах до сервісної мережної платформи до 10% при опрацюванні складних запитів. Отримані в дисертації результати узгоджуються із результатами експериментальних досліджень, проведених, зокрема, у ЦОД Львівської філії ПАТ «Укртелеком» та на обладнанні ТзОВ СП «Мікро-код» із середньоквадратичним відхиленням залежностей менше 5%.

3.1.4. Порівняльний аналіз характеристик відкритої сервісної платформи та класичного сервісного вузла.

Для того, щоб порівняти підходи до побудови сервісних мережних систем, а саме на основі класичного вузла послуг IN та відкритої сервісної платформи (на прикладі системи Parlay API), використовувалися створені у розділі структурно-параметричні та математичні моделі (рис. 3.1-3.5) і проводились експерименти на реальному обладнанні, зокрема у ТзОВ СП «Мікро-код». При цьому, з точки зору сервісної платформи, тобто серверів послуг, обидва підходи абсолютно ідентичні за обчислювальними ресурсами (здіяно однакову кількість серверів послуг із однаковою кількістю сервісних застосувань) [49]. Звичайно, відразу робимо очевидний висновок про те, класичний сервісний вузол важко піддається масштабуванню за своєю архітектурою [114, 115].

Основна ж відмінність даних підходів полягає в тому, що в класичному підході логіка послуг реалізується в єдиному базовому сервері послуг, а у відкритій сервісній платформі – на серверах послуг/сервісних застосувань. Тому середній час оброблення запитів, що надходять на базовий сервер послуг (у системі з Parlay API), є значно меншим, ніж середній час оброблення запитів сервером у класичному сервісному вузлі. Середній час обслуговування запиту може бути визначено статистично в результаті експериментів.

При розгляді характеристик цих систем враховувалося, що середній час обслуговування запиту на базовому сервері OSA Parlay дорівнює 5 мс, а на сервісному застосуванні – 50 мс. Якщо вважати, що послуги, які надаються системами є однаковими по суті, тоді середня тривалість обслуговування запиту в класичному сервісному вузлі приблизно дорівнює тривалості обслуговування запиту сервісним застосуванням через відкритий сервісний інтерфейс. Припустимо також, що за рахунок збільшення продуктивності сервера послуг/сервісних застосувань ця тривалість була знижена до 40 мс.

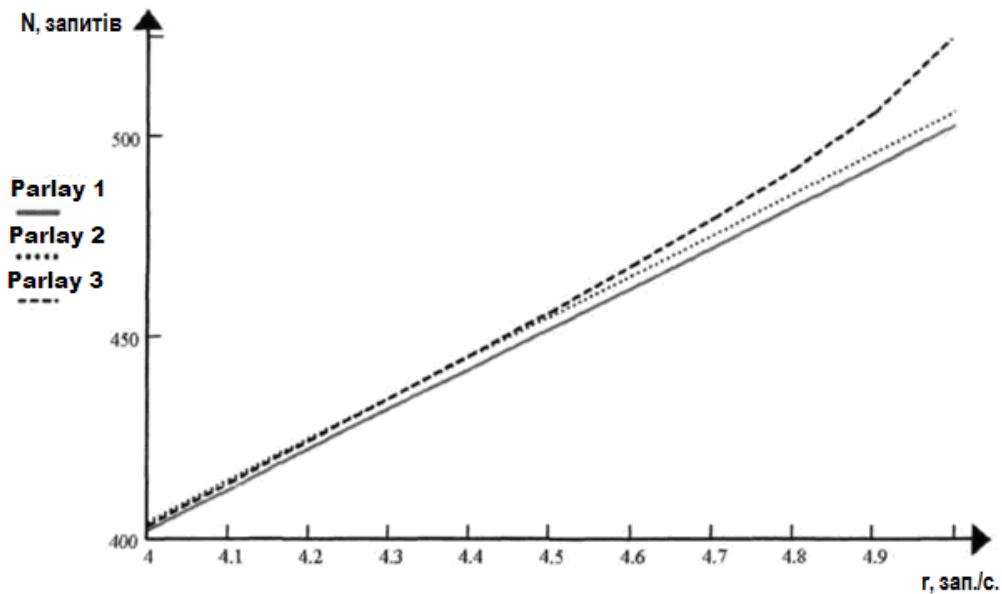


Рис. 3.14. Залежність середньої кількості запитів у сервісній мережній платформі від інтенсивності надходження запитів на сервери послуг [49].

На рис. 3.14 представлено залежності середньої кількості запитів в системі від інтенсивності їх надходження. Суцільною лінією на рис. 3.14 представлена залежність кількості запитів в системі від кількості сервісних застосувань, при ймовірності необхідності повторного обслуговування запиту деяким сервісним компонентом $p_{AP1} = 0,1$ (залежність Parlay-1). Точкова залежність побудована для $p_{AP1} = 0,5$ (залежність Parlay-2). Третя залежність – Parlay-3 - для класичного сервісного вузла (без застосування відкритої системної архітектури).

Бачимо, що наведені залежності мають лінійний характер, поки інтенсивність надходження запитів до сервісної платформи не досягає 4,7 - 4,8 зап. / с. При великих значеннях інтенсивності для класичного сервісного вузла різко зростає середня кількість запитів, що перебувають у сервісній мережній системі. Це пов'язано з наближенням коефіцієнта утилізації ресурсів сервера послуг до 1, що, відповідно, і впливає на збільшення середньої тривалості перебування запитів в системі (рис. 3.15).

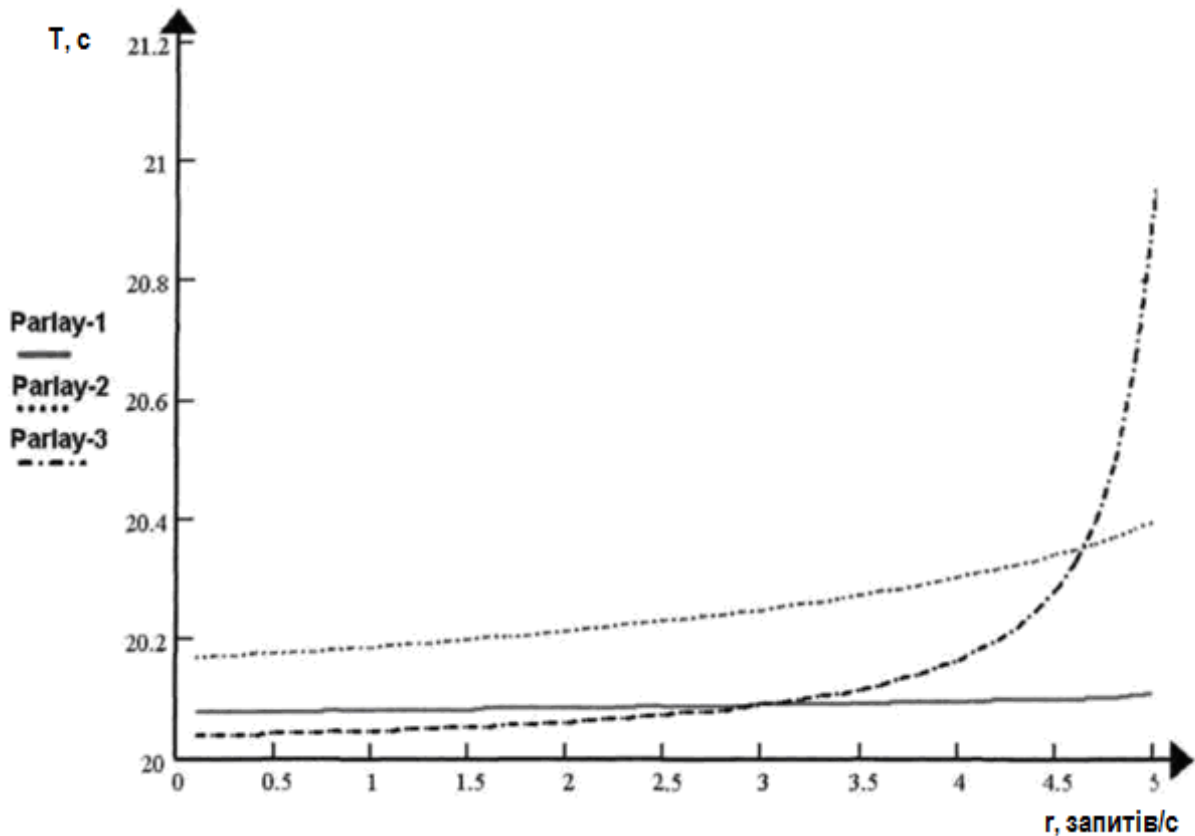


Рис. 3.15. Залежність середньої тривалості перебування запитів в PaaS від інтенсивності їх надходження на сервери послуг/сервісних застосувань [49].

Як можна бачити з рис. 3.15, при невеликих навантаженнях середня тривалість перебування запиту в класичному сервісному вузлі є меншою, ніж для OSA сервісних систем. Але при збільшенні навантаження на сервісну платформу в деяких точках залежностей відбувається перетин характеристик, і системи з відкритою системною архітектурою стають більш ефективними. Це пов'язане з тим, що реалізацією послуг в цих системах займається не один сервер сервісного вузла, а ряд незалежних (як правило - фізично розподілених серверних систем, які підтримують сукупність сервісних застосувань, що оптимізовані під роботу з певними типами електронних послуг.

На наступному рис. 3.16 представлено залежності середньої тривалості перебування запитів на обслуговуванні в сервісній системі від кількості серверів послуг/застосувань. Ці залежності показують, зокрема, *наскільки та чи інша архітектура PaaS є масштабованою*. З рис. 3.16 видно, що при невеликій

кількості серверів послуг характеристики класичного сервісного вузла є кращими, але при збільшенні кількості серверів послуг середня тривалість перебування запиту в сервісній платформі починає різко збільшуватися і вже при 5-8 серверах послуг характеристики SN стають значно гіршими [49].

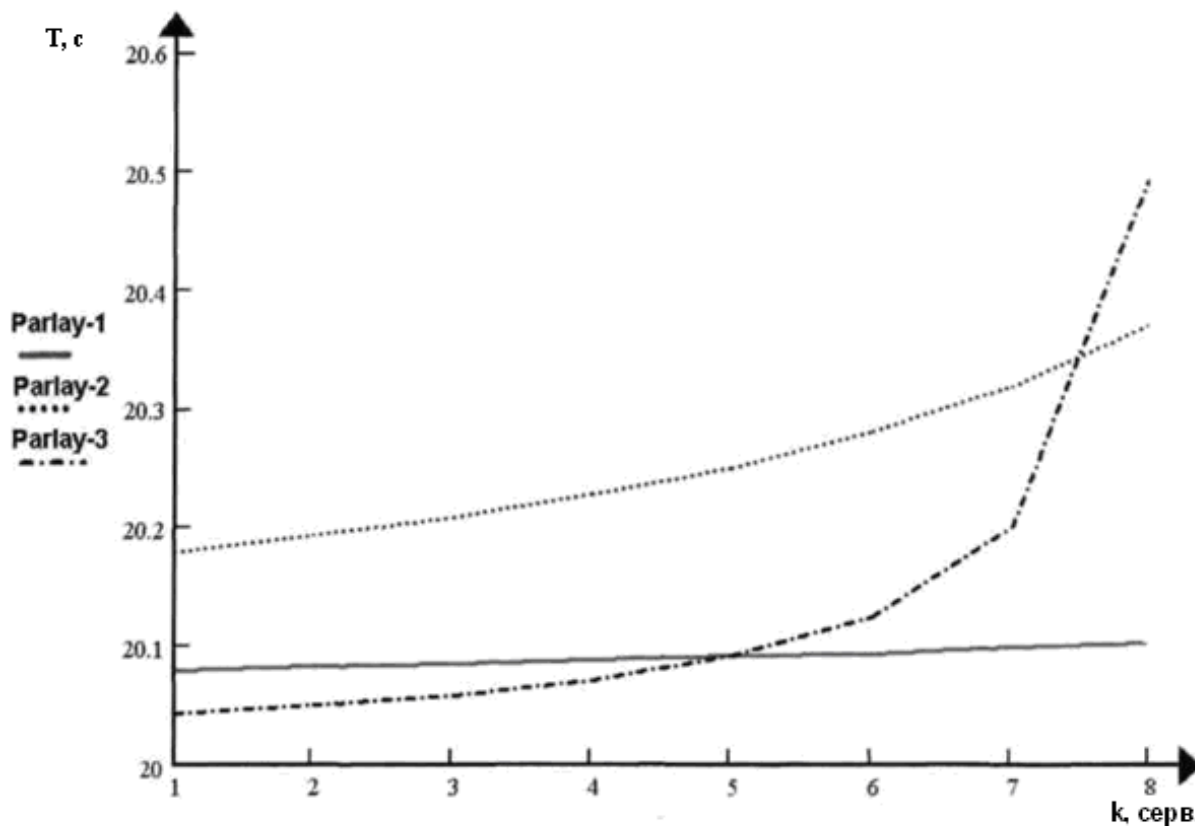


Рис. 3.16. Залежність середньої тривалості перебування запитів в PaaS системі від кількості серверів послуг / сервісних застосувань [49].

Різде збільшення тривалості перебування запиту в сервісній мережній системі пов'язане з перевантаженням основного сервера SN. Для того, щоб класичний сервісний вузол зміг працювати з великою кількістю віртуальних серверів послуг, необхідно значно збільшувати його продуктивність, однак це не є найбільш ефективним рішенням з точки зору мережної архітектури та масштабованості. Адже продуктивність обчислювальних ресурсів сучасних серверних систем є величезною, проте все ж обмеженою.

3.1.5. Порівняльний аналіз характеристик відкритих сервісних платформ розподіленої та централізованої архітектури.

Основна відмінність відкритих сервісних платформ розподіленої та централізованої архітектури полягає в тому, що при розподіленому підході до реалізації PaaS моделі вводяться додаткові ділянки мереж передавання даних, які повинні враховуватися в процесі оброблення запитів. Структурно-параметрична модель відкритої сервісної платформи з розподіленими серверами послуг/сервісних застосувань (тобто оптимізована архітектура з підтримкою розпаралелення оброблення даних) представлена на рис. 3.4.

На рис. 3.17 і 3.18 представлено залежності середньої тривалості перебування запитів у сервісній мережній платформі від інтенсивності надходження запитів на сервери послуг/сервісних застосувань. Перші криві представлено для розподіленої архітектури надання електронних сервісів при коефіцієнті використання ресурсів мережної платформи між базовим сервером послуг і серверами послуг/сервісних застосувань не більше 0,25.

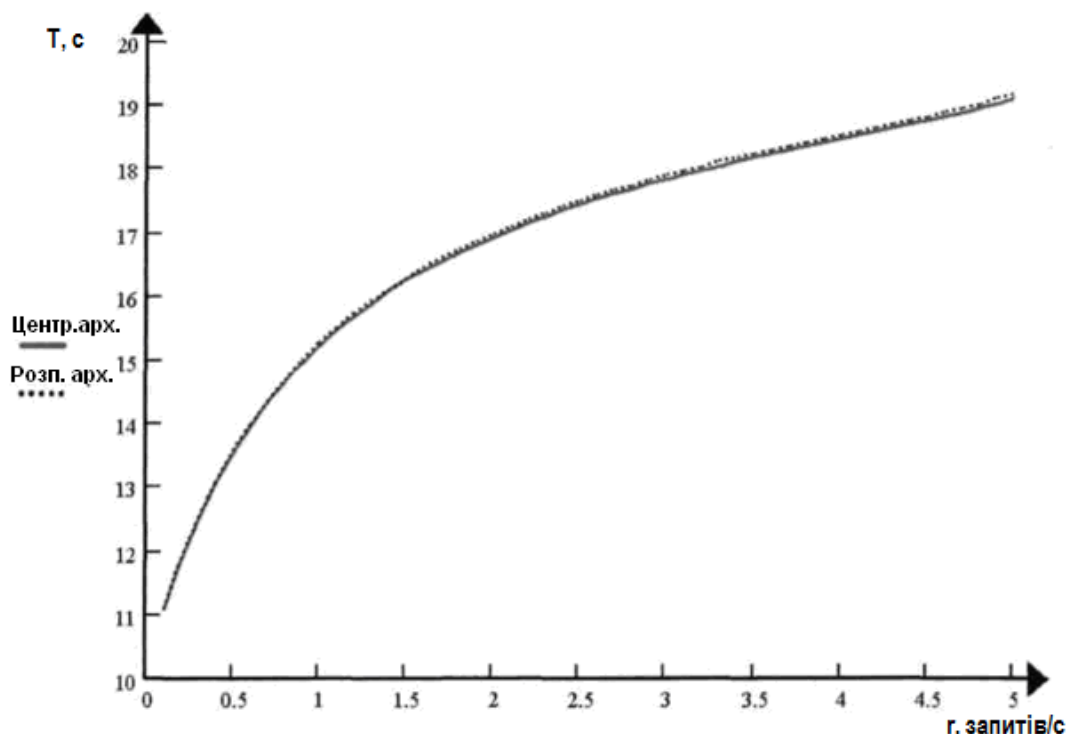


Рис. 3.17. Залежність середньої тривалості перебування запитів в PaaS системі від інтенсивності їх надходження (низький коефіцієнт використання мережної платформи, випадок реалізації розподіленої архітектури).

На рис. 3.18 коефіцієнт використання мережі передавання даних значно вище, а саме – 0,5-0,9. З представлених кривих видно, що при досить невисоких коефіцієнтах використання ресурсів мережної платформи, характеристики систем на основі різної архітектури практично не відрізняються. Це пов'язано з тим, що додаткова ділянка мережі передавання даних не вносить додаткових затримок в у процес оброблення користувацьких запитів.

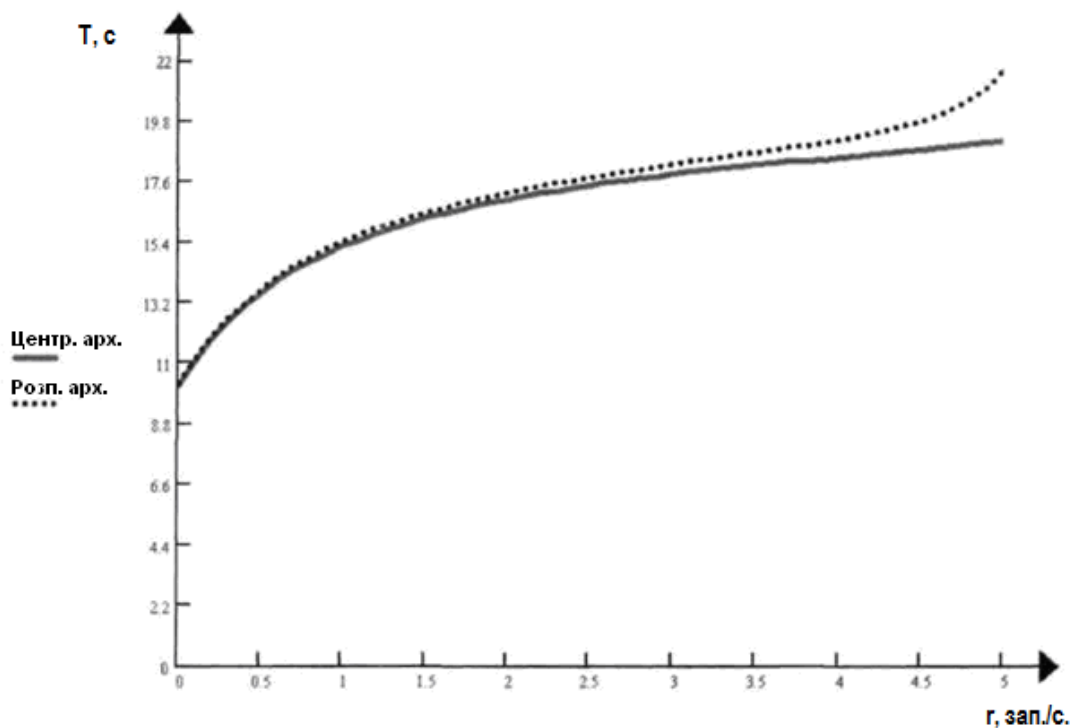


Рис. 3.18. Залежність середньої тривалості перебування запитів в PaaS системі від інтенсивності їх надходження (високий коефіцієнт використання мережної платформи, випадок реалізації розподіленої архітектури).

Одержані в цій дисертації результати узгоджуються із результатами експериментальних досліджень у ЦОД Львівської філії ПАТ «Укртелеком» із середньоквадратичним відхиленням залежностей не більше 5%, крім цього були одержані й опубліковані на основі науково-технічної співпраці з Українсько-канадським СП у формі ТЗОВ «Мікро-код» ЛТД, зокрема в рамках спільних наукових досліджень та експериментів з к.т.н. Добушем Ю.Д., у якості технічного директора названого підприємства. Наведені в дисертації відомості підтверджено відповідними актами, що додаються до роботи.

3.2. Аналіз недоліків сервісних мережних систем з відкритою архітектурою, характеристика їх функціональної стійкості.

Застосування інфокомунікаційних технологій при передаванні, обробленні та зберіганні персональних даних громадян, управлінської та іншої, як правило, мультимедійної інформації міністерств та відомств в Україні, як правило, стикається з низкою специфічних загроз – в основному щодо безпеки інформації та несанкціонованого доступу до неї, окремою гілкою яких є порушення функціональної стійкості телекомунікаційних сервісних платформ, які здійснюють вищеназвані дії. У даному розділі надамо стислу класифікацію та аналіз моделей таких загроз у контексті розгляду принципів побудови телекомунікаційних платформ, зокрема згідно архітектурної моделі IaaS при реалізації мережної інфраструктури національного сегменту сервісних систем з метою визначення завдань для спеціалістів в галузі захисту інформації, які потребують рішення у подальшому [116, 117].

3.2.1. Класифікація загроз обробленню даних в інфокомунікаційній площині сервісних платформ національного масштабу.

Отже, загрози утворюються внаслідок існування типових сценаріїв можливих дій порушників (атак), що описують послідовність (алгоритм) дій груп та окремих порушників, способи їх дій на кожному етапі порушення функціональної стійкості сервісних мережних систем. Не будемо зупинятися на класифікації типів порушників, оскільки їх діяльність може мотивуватися ситуативно, а також дане питання не відноситься до заявленої наукової спеціальності. Натомість, мета даного розділу дисертації – дослідити можливі інфокомунікаційні загрози функціонуванню телекомунікаційних сервісних платформ, зокрема їх національного сегмента в Україні та запропонувати загальні методи протидії таким загрозам [116].

Оскільки для реалізації інфокомунікаційної системи сервісної мережної платформи, що функціонує в захищеному режимі і реалізує сценарій «комп'ютер-комп'ютер», як правило, пропонується використовувати

можливості операційних систем (наприклад ОС Windows), апаратні можливості сучасних ПЕОМ та можливості розподілених обчислювальних інфраструктур, розглянемо можливі види атак порушника та використання специфічних йому засобів. Аналіз проведемо шляхом визначення найбільш важливих, з точки зору безпеки, ділянок у інфокомунікаційній сервісній платформі. Не розглядатимемо атаки безпосередньо на операційні системи, оскільки дослідження їх уразливостей виходить за рамки спеціальності дисертаційного дослідження. Врахуємо також, що атаки на різні типи даних та елементи мережної платформи в цілому аналогічні атакам на мультимедійні інформаційні потоки [116], при цьому реалізація інфокомунікаційної інфраструктури сервісних систем передбачає мультисервісний документальний обмін.

Спрощена модель передавання даних через IP-мультисервісну мережу в захищеному від несанкціонованого доступу (НСД) режимі представлена на рис. 3.19.

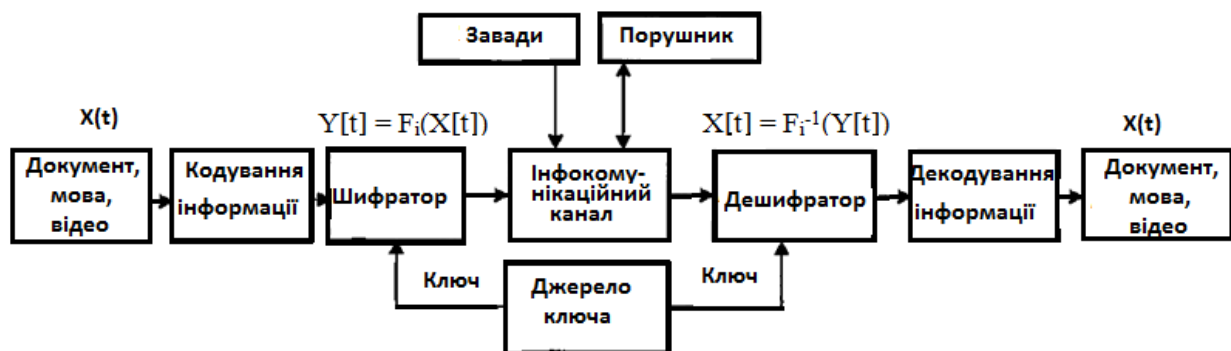


Рис. 3.19. Спрощена модель передавання даних у сервісній мережній системі в захищеному від несанкціонованого доступу режимі.

Під математичною моделлю мережної атаки, структурно-функціонального впливу будемо розуміти її формалізований опис, побудований з точки зору прийнятої моделі захищеності. В даному дослідженні приймемо до уваги ймовірнісну та теоретико-ігрову моделі захищеності та мережних атак. У рамках ймовірнісної моделі значущою буде виступати ймовірність запобігання атаці системою захисту XaaS, ймовірність її виявлення та локалізації за допомогою спеціалізованих мережних архітектур, методів та системних засобів

[17], або, з іншого боку, імовірність успішного завершення атаки. Ця ймовірність в загальному випадку буде залежати від часу і становитиме суть моделі атаки. Перерахованим в даній роботі видам функціональних загроз відповідають дві математичні моделі: модель перебору і модель перевірки [161].

Загрози, які пов'язані з перевіркою деякого числа варіантів критично важливих параметрів безпеки інфокомунікаційної сервісної системи, можна описати моделлю перебору. Типовим прикладом таких атак є характерна для більшості сучасних мережних систем, у тому числі і для систем національного сегменту сервісної мережної інфраструктури, атака підбором паролю або ключа (атаки типу А7, див. табл. 3.1). В табл. 3.1 для зручності кожному типові атаки привласнено індекс, що складається з префікса «А» і номера (див. табл. 3.1).

Атаки, засновані на помилках (недоліках) в системі безпеки сервісних мережних платформ і їм подібні, можна описати за допомогою моделі перевірки. Такі атаки використовують уразливість системи захисту, перевіряючи єдиний варіант – наявність або відсутність даної уразливості, тому:

$$p(t) = \begin{cases} 1, \text{ якщо уразливість існує;} \\ 0, \text{ якщо уразливості немає.} \end{cases} \quad (3.15)$$

Отже, доволі проста узагальнена математична модель виду (3.15) відображає більшість існуючих на даний час атак (А1-А6, А8-А10), оскільки під поняття вразливості підпадають як помилки (недоліки) в системі безпеки, так і помилки адміністрування сервісних мережних систем [116, 118].

З точки зору теоретико-ігрової моделі ключове значення має вплив, який заподіюється застосуванням тієї або іншої мережної атаки і ймовірність запобігання цій атаці різними методами захисту та протидії задля забезпечення функціональної стійкості сервісної мережної платформи. Вплив є основною характеристикою при описі відповідних різновидів атак з позицій цієї моделі. Проблема полягає в тому, що оцінити системний вплив та можливий збиток

буває досить складно, а самі оцінки, як правило, виявляються частковими і суб'єктивними, тому поширити їх на всю множину застосування сервісної інфокомунікаційної платформи, захищеної від несанкціонованого доступу, виявляється проблематично [119]. Логічним виходом у даній ситуації є відмова від ранжування і прийняття всіх різновидів існуючих атак рівно небезпечними.

При аналізі вразливостей захищеної сервісної інфокомунікаційної системи виділимо атаки, засновані не на помилках в її програмному забезпеченні, які розробник системи може де-факто виправити за лічені дні, а на концептуальних властивостях функціонування реалізацій системної архітектури.

Табл. 3.1. Можливі мережні атаки на сервісну інфокомунікаційну платформу.

Індекс	Вид мережної атаки та можливі причини
A1	Доступ до інформації в обхід інфокомунікаційної сервісної системи, в обхід ОС і в обхід ПЕОМ (недоліки в організаційних заходах із захисту від несанкціонованого доступу, недбальство/саботаж причетних осіб або шпигунська діяльність)
A2	Доступ до інформації в обхід власне сервісної мережної платформи (причини аналогічні пункту A1)
A3	Отримання інформації впровадженням «закладок» в модулі введення / виведення документальної/мультимедійної інформації ОС (наприклад, у Windows - DirectSound) (недоліки в організаційних заходах із захисту від несанкціонованого доступу, цілеспрямована діяльність групи осіб з метою несанкціонованого доступу до інформації, недоліки системи мережної безпеки)
A4	Отримання інформації впровадженням «закладок» у модулі компресії / декомпресії ОС та стороннього програмного забезпечення (як для мультимедійної так і для документальної інформації) (причини аналогічні пункту A3)
A5	Отримання ключа та / або інформації, що передається впровадженням «закладок» у програмні модулі захисту від несанкціонованого доступу ОС та стороннього програмного забезпечення для шифрування (цілеспрямована діяльність групи осіб з метою несанкціонованого доступу до інформації, недоліки системи мережної безпеки)

A6	Збір паролів вірусною програмою виду «Троянський кінь» (причини аналогічні пункту A5)
A7	Перехоплення пакетів з даними (виконується групою осіб через підключення до інфокомунікаційних каналів сервісної мережної платформи, атака неефективна в разі стійких алгоритмів шифрування, цифрового підпису та спеціальної розподіленої архітектури передавання /зберігання інформації) – див. розділи 4.2-4.3 цієї роботи.
A8	Нав'язування користувачеві сервісної мережної системи неправдивого повідомлення (причини та коментар аналогічні пункту A7)
A9	Відмова в обслуговуванні (DoS, атака виконується на визначені заздалегідь інформаційні ресурси сервісної мережної системи групою осіб через використання розподілених підконтрольних мереж типу «бот-нет», що виконують розсилання екстремально великої кількості запитів до серверів інфокомунікаційної системи, призводячи до їх перевантаження та/або недоступності) – див. розділи 4.2-4.3 цієї роботи.
A10	Підміна програмного забезпечення інфокомунікаційної сервісної системи (причини аналогічні пунктам A1, A3) – див. розділи 4.2-4.3 цієї роботи.

Атаки типів A7-A10 передбачають доволі серйозні втручання у функціонування сервісної мережної системи та потребують реалізації цілого ряду організаційних заходів, які пов'язані з її архітектурою. Детальніше дані питання розглядаються, як це було зазначено у табл. 3.1, у розділах 4.2-4.3 цієї дисертації. Розроблення методів підтримки функціональної стійкості сервісних мережних платформ є окремим завданням даної дисертаційної роботи, проте значна частина тих засобів, які стосуються безпосередньо інформаційної безпеки повинна бути розроблена фахівцями з відповідної спеціальності.

Розглянуті окремі типи мережних атак не завжди можуть привести порушника до позитивного для нього кінцевого результату, тому активність

порушника в загальному випадку може складатися з деяких послідовностей атак, які залежать як від цілей порушника, так і від його можливостей. Можливі варіанти послідовностей застосування атак складають стратегії дій порушника. У кожній конкретній атакуючій дії може бути реалізована тільки одна з можливих стратегій. Для аналізу загроз захищеності сервісної мережної інфраструктури системи велике значення має розуміння взаємозв'язків між елементами цієї множини – можливими стратегіями дій порушника і складовими діями його атак. Найбільш зручним способом відображення і дослідження цих взаємозв'язків є граф, що пояснюється такими особливостями стратегії дій порушника, як спрямованість та спільність складових елементів мережної атаки.

Коротко розглянемо стратегії дій порушника, спрямовані на НСД до інформації або на порушення функціональної стійкості інфокомунікаційної системи сервісної мережної платформи. Граф можливих стратегій дій порушника представлений на рис. 3.20.

На рис. 3.20 елементи A_i позначають види мережних атак, S_j – проміжні результати (S_0 відповідає початковому стану, S_1 відповідає стану, коли порушникові відомий ключ доступу), НСД і DOS (відмова у обслуговуванні внаслідок перевантаження запитами сервісної платформи, що виникає, в тому числі, й для інших корисувачів) – позначають результати дій порушника.

При визначенні якості захисту сервісної мережної системи нас цікавить максимальна серед усіх можливих стратегій дій ймовірність успіху, тобто критичний шлях графу. Після евристично-структурного аналізу моделей рис. 3.20 та табл. 3.1 можливо визначити, що найбільш ймовірними та успішними, а також і актуальними в Україні стратегіями дій порушника (див. рис. 3.20 і табл. 3.1) є три наступні: A7-S1-НСД; A7-S1-A8-НСД; A9-DOS. Однак імовірність успіху зазначених стратегій дій (A7-S1-НСД або A7-S1-A8-НСД) за прийнятний час є низькою при виборі стійкої сервісної мережної архітектури з надійним шифруванням.

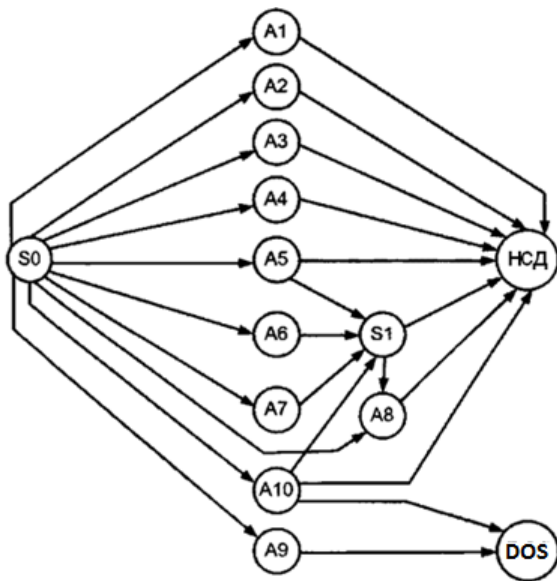


Рис. 3.20. Граф можливих стратегій дій порушника [116].

розосередженими по різних сегментах мережної платформи – наприклад створив «бот-нет») [17].

Після проведеного розгляду можливих загроз поширенню даних та функціональній стійкості в сервісній мережній платформі у вигляді аналізу можливостей атак з метою отримання НСД або блокування роботи такої системи, стає актуальною та зрозумілою необхідність запропонувати і проаналізувати відповідні узагальнені контрзаходи та методи для подальшого опрацювання методології запобігання подібним загрозам спеціалістами в галузі захисту інформації. Таким чином, у табл. 3.2 виділимо 4 основні групи методів та заходів (М1-М4) запобігання атакам, наведеним в табл. 3.1.

При аналізі якості захисту реальної інфокомунікаційної сервісної системи до уваги необхідно приймати адміністративні, організаційні та інженерно-технічні методи, а також використання додаткових програмних або апаратних засобів захисту, спеціалізованих мережних екранів. Найбільше значення при цьому будуть мати засоби захисту від атак, що входять до стратегій дій порушника, яким не запобігають відповідні засоби власне сервісної системи: *обмеження* фізичного доступу в приміщення, де розташовані серверні блоки;

Нажаль, для загальнодоступних мереж національного рівня критичний шлях A9-DOS завжди має ймовірність успіху, яка дорівнює 1, на підставі чого можна прийти до висновку, що забезпечити якіснї та доступне надання електронних послуг через сервісну інфокомунікаційну систему, не використовуючи додаткові методи захисту, важко (особливо у випадку якщо порушник володіє значними технічними засобами,

Табл. 3.2. Узагальнені методи та заходи запобігання атакам на сервісні мережні платформи.

Індекс	Опис
М1	<p>Організаційні та інженерно-технічні методи, спрямовані на забезпечення надійного захисту технічних приміщень сервісних мережних платформ проти фізичного проникнення в приміщення випадкових осіб, здатних принести записуючі або радіопередавальні пристрої, а також заходи спрямовані на нейтралізацію радіопередавальних або записуючих пристроїв; пріоритетне використання захищених баз даних і мереж урядового зв'язку.</p>
М2	<p>Використання лише сертифікованого програмного забезпечення, якісний антивірусний захист, здатний запобігти зараженню програмного забезпечення шкідливими троянськими програмами, несанкціонованому мережному доступі до ПЕОМ, <i>мережних платформ</i>, а також обмеження прав звичайних користувачів у частині встановлення та оновлення програмного забезпечення, зміни мережних параметрів. Організаційні та інженерно-технічні методи, у напрямку на забезпечення цілісності комп'ютерного обладнання та обмеження доступу в приміщення і фізичного доступу до серверів, у тому числі жорстка регламентація порядку роботи на комп'ютерах системи, порядку їх ремонту, заміни і т.д.</p>
М3	<p>Обмеження завантаження альтернативних операційних систем, щоб запобігти, для прикладу, заміні бібліотеки <code>advapi32.dll</code>, що здійснює перевірку цифрового підпису модулів захисту даних в ОС Windows.</p>
М4	<p>Використання методів і режимів шифрування в яких неможлива або не має сенсу маніпуляція блоками шифрованих даних; виконання дій з додавання до кожного пакету з відкритою інформацією деяких даних, які характеризують унікальність пакету, наприклад час і / або порядковий номер пакету, <i>використання цифрових підписів усіх документів</i>, використання захищеної розподіленої мережної архітектури всіх баз даних, <i>спеціальних мережних екранів</i>.</p>

обмеження фізичного доступу до серверних систем; *запобігання* фізичному доступу до мережної інфраструктури (платформи); *використання* сертифікованого програмного забезпечення; *обмеження* використання засобів мережного і локального адміністрування; *наявність* розгорнутого плану дій з протидії атакам виду DoS «Відмова в обслуговуванні». При цьому необхідне використання спеціальної серверної та мережної архітектури (фільтрація та законне перехоплення трафіку) та інтелектуального серверно-шлюзового програмного забезпечення, що визначатиме характер і походження «шкідливих» запитів та відкидатиме їх з метою мінімізації навантаження на сервісну мережну платформу.

При використанні для оцінки теоретико-ігрової моделі, якість захисту можна оцінити, як відношення кількості передбачених політикою безпеки атак до загальної кількості можливих атак на сервісну мережну систему, однак така оцінка в класичному формулюванні теоретико-ігрової моделі можлива тільки в статичному режимі і не є такою показовою, як ймовірнісна.

3.2.2. Оцінювання ефективності захисту мультисервісних інфокомунікаційних систем в національному сегменті сервісної мережної інфраструктури.

Дослідження будь-якої складної інфокомунікаційної системи включає в себе комплекс питань, пов'язаних з вибором методології дослідження; дослідженням програмної та телекомунікаційної архітектури, програмної сервісної платформи; застосуванням методів оцінки якості програмних застосувань, гнучкості реалізації і тестування функціонального змісту системи; формуванням вимог рекомендаційного характеру, орієнтованих на підвищення якості функціонування реалізованої сервісної мережної платформи [117]. Важливим є дослідження структури систем подібного класу з метою виявлення загальних елементів структури, вироблення єдиних вимог до їх реалізації. Це дає можливість виконати дослідження з позицій універсального підходу, що дозволить використовувати єдині методи для побудови цілого класу

стандартизованих на державному рівні систем.

Як вже стало зрозуміло, основним методом структуризації в нашому дослідженні є системний метод, який є основою теорії системного аналізу. У системно-структурному методі акцент переважно робиться на дослідженнях внутрішньої структури системи, внутрішніх зв'язків, тоді як системний підхід, крім цього, передбачає дослідження поведінки системи та її елементів залежно від зв'язків із зовнішнім середовищем, від походження ситуації, в яку потрапляє система. Важливою рисою системно-структурного методу є те, що він разом із розглядом структурних зв'язків розглядає і структуру функцій сервісної мережної системи.

Дослідити структуру складних мультисервісних мережних систем можна з використанням двох підходів: інформаційного та функціонального [117, 120]. Інформаційний підхід передбачає аналіз на основі розгляду транспортних потоків даних, що циркулюють між елементами інфокомунікаційної системи в її мережній платформі, у той час як функціональний ґрунтується на розгляді різноманітних зв'язків усередині системного комплексу, виділяючи в окремі одиниці функціонально завершені компоненти [116].

Функціональний підхід. Функціональна схема повинна відображати загальну структуру захищеної інфокомунікаційної платформи передавання даних у інфраструктурі сервісних мережних систем у вигляді множини завершених елементів, що реалізують певні функції в рамках вимог, які пред'являються до систем зв'язку для оперативного обміну повідомленнями різного типу (наприклад, документальними або мультимедійними), а також надають різні додаткові діагностичні або сервісні можливості. Деталізація функціональної схеми передбачає врахування конкретної програмно-апаратної платформи, на базі якої будується реалізація, що накладає свій відбиток на структуру зв'язків і набір функціональних компонентів, присутніх у структурній схемі. *Функціональна схема захищених інфокомунікаційних систем зв'язку* для реалізації, наприклад, концепції державних електронних сервісів, зокрема в рамках електронного урядування повинна передбачати високий

рівень надійності роботи, регламентувати допустимі часові затримки інформації, ступінь захисту від НСД, визначати програмно-апаратні середовища оброблення і передавання даних.

Структурно інфокомунікаційні системи зазначеного типу складаються з наступних підсистем (рис. 3.22):

- введення-виведення звукового і відео сигналу, зображень, зокрема документів та іншої важливої інформації (для забезпечення мультисервісного документообігу);
- цифрової обробки зображень, звукового і відео сигналу (компресія і шифрування документів та мультисервісних інформаційних потоків);
- серверної інфраструктури, баз даних та відповідних систем управління базами даних і взаємодії між ними;
- управління, візуалізації і реєстрації статистичної та діагностичної інформації, що відображають процес функціонування системи;
- телекомунікаційних мережних інтерфейсів відповідних платформ.

Компоненти підсистем, які відповідають за оброблення інформації, що надходить до сервісної мережної системи, зберігається в ній, опрацьовується та виводиться користувачам, створюються на основі програмного забезпечення сертифікованих розробників, яким комплектується більшість робочих станцій інфокомунікаційної системи в залежності від їх призначення та функціональності.

Забезпечення ефективного функціонування телекомунікаційних інтерфейсів у конвергентній інфокомунікаційній системі визначає як якість отриманого цифрового каналу передавання даних (у IP-мережі), так і економічний ефект від застосування технологій і рішень сервісних мережних систем національного масштабу.

Інформаційний підхід. З точки зору формалізації структури та інформаційних потоків захищеної інфокомунікаційної сервісної системи більш універсальним є інформаційний підхід, оскільки він надає можливість кількісно і якісно проаналізувати та представити внутрішню структуру зв'язків сервісної

мережної системи на основі графоаналітичних методів, а також визначити найбільш важливі, з точки зору безпеки, ділянки.

Особливістю систем, що досліджуються нами, як і багатьох інших сучасних інфокомунікаційних систем є модульність. Використання при розробці програмного забезпечення програмної архітектури заснованої на динамічному підключенні компонентів і модулів, у тому числі вбудованих в ядро ОС, дозволяє вже на рівні загального проектування архітектури неспеціалізованих національних сервісних мережних систем збільшити надійність, а також спростити розробку, тестування і налагодження створюваного програмного забезпечення. На рівні експлуатації спрощується оновлення відповідних модулів системи.

3.2.3. Критерії оцінювання ефективності реалізації інфокомунікаційної системи передавання даних для сервісної мережної інфраструктури національного масштабу, що функціонує в захищеному режимі.

Для складних інформаційних розподілених апаратно-програмних систем практично неможливе вироблення якого-небудь єдиного сукупного критерію, тому оцінка ефективності може бути проведена на підставі дослідження декількох груп часткових показників [117], вага яких може бути різною у кожному конкретному випадку [116]. Оцінка за кожним частковим показником виводиться за деякою уніфікованою шкалою.

У якості таких груп автором були обрані наступні групи часткових показників:

1. Якісні показники (М), що характеризують суб'єктивні результати вимірювання та оцінювання якості поширення даних на основі оцінок окремих експертів. Вони характеризують ефективність та ступінь відповідності системи в цілому встановленим при проектуванні вимогам.

2. Технологічні показники (Т), що характеризують якість програмних рішень із загальних позицій сучасної технологічної бази. Для систем реального часу такими показниками можуть бути коефіцієнти використання ЦП (T_1) і

мережних ресурсів системи (T_2), простота і функціональність налаштування параметрів системи (T_3), оперативність відображення необхідної статичної та динамічної інформації (T_4), надійність функціонування (T_5), можливість динамічного нарощування функціональних можливостей щодо алгоритмів компресії (T_6) і захисту інформації (T_7), наприклад, шляхом використання кодеків та / або алгоритмів для захисту від несанкціонованого доступу на основі апаратних інтерфейсів і модулів для захисту від несанкціонованого доступу операційної системи.

3. Показники, що характеризують якість захисту інформації (K): стійкість захисту пакетів даних - алгоритм шифрування (K_1), сукупна довжина ключа шифрування (K_2), алгоритм хешування (K_3), довжина криптоставки (K_4), простота і безпека розповсюдження ключів (паролів) для захисту від несанкціонованого доступу (K_5), можливість вести контроль і налаштування режимів захисту від несанкціонованого доступу трафіку IP-телефонії (K_6), можливість використання сертифікованих СБУ алгоритмів і модулів захисту від несанкціонованого доступу для того, щоб офіційно застосовувати системи електронного документообігу, цифрових репозиторіїв та IP-телефонії в органах державної влади і силових відомствах (K_7).

4. Показники, що характеризують сукупну складність реалізації програмного забезпечення (Q), що включає в себе: алгоритми компресії зображень, мови та відео (Q_1), захисту даних (Q_2), формування і обробки IP-пакетів (Q_3) та їх передачі / прийому через IP-мережі (Q_4), алгоритми керування обслуговуванням з'єднання, тобто прийняття рішень про те, яким чином має бути встановлена комунікація між користувачами (Q_5).

5. Економічні показники (E), що характеризують витрати, пов'язані із забезпеченням необхідних функціональних характеристик, які складаються з вартості проектування і розробки програмного забезпечення (E_1), мінімально необхідної конфігурації апаратних засобів (E_2) та вартості експлуатації функціональних підсистем (наприклад, підсистеми IP- телефонії) (E_3).

У підсумку загальний критерій оцінювання ефективності K_E захищеної

мультисервісної інфокомунікаційної системи передавання даних для інфраструктури «електронного урядування», набуде вигляду функції п'яти змінних:

$$K_E = (M, T, K, O, E).$$

3.2.4. Забезпечення якості обслуговування та оптимізація бізнес-процесів у розподілених телекомунікаційних системах на основі сервісно-орієнтованої архітектури.

Сучасні бізнес-процеси неодмінно передбачають використання Інтернету та інформаційних технологій. Бізнес все більше залежить від цих технологій, і з їхнім розвитком цей взаємозв'язок лише розширюється та поглиблюється. З'являються нові можливості щодо створення інноваційних послуг та сервісів для користувачів. Спрощуються та оптимізуються процеси управління бізнесом, що в результаті дає змогу істотно знизити вартість послуг для кінцевих користувачів і разом з тим збільшити доходи від ведення бізнесу.

Будь-яка велика компанія має власну корпоративну мережу, яка з'єднує між собою комп'ютери, сервери, принтери, сканери тощо і є закритою для зовнішньої мережі Інтернет. Це означає, що ніхто не може отримати доступ до її ресурсів, окрім працівників цієї компанії. На серверах корпоративної мережі встановлено програмне забезпечення, яке централізує управління мережею і дає змогу здійснювати контроль за всіма пристроями та користувачами, що працюють в мережі, реалізує зв'язок з базою даних для проведення аутентифікації та авторизації користувачів. На межі між корпоративною мережею та мережею Інтернет встановлюють сервери для забезпечення доступу до корпоративної мережі з інших мереж. Як правило, на цих серверах встановлюють спеціалізоване програмне забезпечення, яке відповідає за безпеку корпоративної мережі і дає змогу працівникам компанії без будь-яких проблем отримати доступ до ресурсів та інформації в корпоративній мережі з будь-якого місця і в будь-який час, навіть якщо вони перебувають поза межами

корпоративної мережі. У той же час, програмне забезпечення на цих серверах блокує проходження несанкціонованого трафіку в корпоративну мережу або підключення до неї сторонніх користувачів з метою отримання доступу до закритої інформації компанії [121].

Технології та методи побудови корпоративних мережних платформ є стандартизовані, а тому не викликають значних проблем під час розгортання корпоративних мереж. Набагато складнішим процесом є розроблення програмного забезпечення, яке реалізувало би всю необхідну функціональність. Основною проблемою, що стала на шляху побудови розподіленої системи, є сильна залежність програмних компонентів системи від мови програмування, на якій їх реалізують, та платформи, для якої вони створюються. Проблему відсутності стандартизованих інтерфейсів для взаємодії між такими компонентами та методики управління розподіленою системою сервісних застосувань довгий час вирішували за допомогою різноманітних технологій, які хоч і давали певний результат, проте робили створення такої системи надто складним процесом, а експлуатацію – проблематичною. У результаті необхідно було витратити набагато більше коштів на підтримування нормального робочого стану такої системи. Сьогодні вирішення цієї проблеми отримало інший підхід, який реалізують за допомогою технології веб-сервісів.

3.2.4.1. Аналіз технології веб-сервісів.

Технологія веб-сервісів привела до революції у створенні розподілених систем. Веб-сервіс – це функціональний компонент, можливості якого доступні для використання через Інтернет. Перевага веб-сервісів над іншими технологіями полягає в тому, що вони не прив'язані ні до однієї апаратної платформи, операційної системи чи мови програмування [122].

Для спілкування між собою веб-сервіси використовують текстові повідомлення на основі технології XML. Веб-сервіси дають змогу створювати складні апаратно розподілені програмні комплекси для розв'язання

різнопланових задач, потребуючи від розробника мінімум часу та зусиль.

Веб-сервіс є компонентом сервісно-орієнтованої архітектури. Як вже було зазначено, сервісно-орієнтована архітектура – це підхід до створення програм, який базується на використанні розподілених, слабо пов'язаних між собою компонентів, які взаємодіють один з одним за допомогою стандартизованих протоколів та інтерфейсів. Програмні комплекси такого виду, зазвичай, представлені набором веб-сервісів, що спілкуються між собою за допомогою протоколу SOAP. Цей протокол використовується для передавання повідомлень у форматі XML і може працювати поверх будь-яких протоколів прикладного рівня, наприклад: SMTP, FTP, HTTP, HTTPS тощо. Взаємодія SOAP з кожним з цих протоколів має свої особливості, проте, зазвичай, для комунікації використовується HTTP. Використання SOAP для передавання повідомлень збільшує їхній обсяг та зменшує швидкість оброблення, а тому часто здійснюють пряму передачу XML-повідомлення за допомогою HTTP із заданими параметрами.

Адресація веб-сервісів забезпечується за допомогою текстового рядка у форматі URI. Ця адреса може бути отримана з реєстру веб-сервісів UDDI. Під час розгортання веб-сервісу вся необхідна інформація про нього заноситься в UDDI. Ця інформація є описовою і використовується для знаходження сервісу та його адресації клієнтськими додатками (див. рис. 3.21).

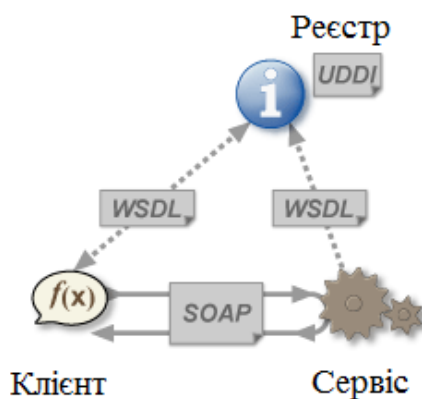


Рис. 3.21. Механізм публікації, пошуку та звертання до веб-сервісу [121].

У випадку першого звертання до веб-сервісу клієнтська програма отримує

від нього файл у форматі WSDL, що містить опис функцій, які може виконувати сервіс. На рис. 3.21 представлено механізм публікації, пошуку та звертання до веб-сервісу.

Веб-сервіси є компонентами мережі Інтернет, і аналогічно до інших програмних додатків їхнім розробникам доводиться вирішувати певні проблеми, які постають під час проектування, розгортання та функціонування веб-сервісу, а саме: забезпечення замовленої через SLA якості сервісу для кожного клієнта індивідуально, системної продуктивності сервісу (ефективності використання апаратних ресурсів), стійкості до відмов та перевантаження (функціональної стійкості рівня моделі SaaS та сервісної доступності), ефективності роботи сервісу. В умовах використання веб-сервісів за допомогою безпроводних мереж зв'язку гостро постає ще й проблема обмеженої пропускної здатності, оскільки використання текстових повідомлень у форматі XML обумовлює значну надлишкову інформацію. Такі повідомлення в умовах переходу стільникових операторів до обслуговування мультисервісного трафіку можуть істотно впливати на ефективність функціонування всієї системи.

Ще одним з недоліків веб-сервісів є їхня швидкодія. Використання повідомлень у форматі XML значно впливає на швидкість роботи сервісу через процес аналізу такого повідомлення, який є тривалим та вимагає потужніших, ніж зазвичай, апаратних ресурсів. Саме на цьому етапі обслуговування клієнтських заявок дуже часто виникають перевантаження, оскільки користувачькі запити мають великий обсяг. Ускладнює ситуацію ще й використання у запитах складних структур даних, зокрема таких, як масиви.

3.2.4.2. Характеристика якості обслуговування веб-сервісами.

Характеристики обслуговування запитів веб-сервісами мають відповідати певним вимогам, що дадуть змогу забезпечити задовільний рівень обслуговування запитів, як правило, прописаний в SLA. Зазвичай, у випадку складних бізнес-процесів кількість веб-сервісів, які будуть задіяні в процесі

обслуговування запиту, їхня різноманітність, цільове призначення та характеристики можуть по різному впливати на якість обслуговування клієнта. Кожний веб-сервіс у процесі обслуговування може по різному впливати на якість обслуговування конкретного запиту залежно від свого поточного завантаження, стану завантаження апаратних ресурсів сервера, продуктивності, ефективності та доступності необхідних ресурсів для виконання операцій. Таким чином, сумарний вплив всіх веб-сервісів на якість обслуговування запиту можна виразити формулою:

$$QoS_S = \frac{\sum_{i=1}^n QoS_i}{n}, \quad (3.16)$$

де QoS_S - показник якості обслуговування запиту під час проходження по конкретному маршруту сервісних застосувань, що складається з визначеної наперед кількості веб-сервісів n у сервісній мережній платформі;

QoS_i – показник середньої величини якості обслуговування на визначеному проміжку часу. Цю величину можна виразити такою залежністю:

$$QoS_i = \frac{\sum_{j=1}^m QoS_j(t)}{m}, \quad t \in (t_1; t_2), \quad (3.17)$$

де $QoS_j(t)$ – якість обслуговування конкретного запиту користувача, який надійшов на обслуговування на i -ий веб-сервіс у момент часу t , що належить проміжку часу від t_1 до t_2 .

Під час аналізу якості обслуговування запиту для кожного можливого маршруту маршруту сервісних застосувань можна спостерігати той факт, що якість обслуговування для кожного з них є різною. Отже, постає питання про

вибір оптимального маршруту маршруту сервісних застосувань для спрямування запиту. Цією проблемою займаються багато науковців, які вже мають серйозні напрацювання у її вирішенні [122]. Розроблені алгоритми та механізми вибору оптимального маршруту оброблення навантаження запитів дають змогу збалансувати навантаження та забезпечити ефективніше (з вищою продуктивністю) функціонування системи разом із підвищенням її прибутку.

Алгоритми знаходження оптимального шляху для направлення запитів на опрацювання можуть динамічно вибирати в процесі обслуговування той чи інший веб-сервіс на певному етапі проходження маршруту. Більшість алгоритмів реалізується за допомогою спеціального веб-сервісу або брокера. Брокер здійснює моніторинг стану завантаження всіх веб-сервісів і таким чином визначає оптимальні шляхи для проходження тих чи інших запитів за певним пріоритетом. Як і в кожній інформаційній технології, бажання здійснити пріоритезацію для підвищення якості обслуговування через деякий час призводить до збільшення кількості користувачів з вищим пріоритетом до такого обсягу, що зумовлює повторне виникнення проблеми перевантаження для користувачів з вищим пріоритетом та необхідності більш глибокої пріоритезації. Подальше збільшення кількості користувачів або ж обсягів вхідного навантаження у сервісній мережній системі лише погіршить ситуацію.

3.2.4.3. Забезпечення якості обслуговування веб-сервісами за допомогою методу поліваріантного доступу.

Розглянемо відносно просту розподілену сервісну мережну систему, яка реалізує три бізнес-процеси, що описують найпростіший онлайн-магазин. Реалізація цих бізнес-процесів здійснюється частково за допомогою одних і тих самих веб-сервісів. Граф маршрутів проходження запитів між веб-сервісами (сервісними застосуваннями) для трьох бізнес-процесів відображено на рис. 3.22.



Рис. 3.22. Граф маршрутів проходження та оброблення запитів для трьох бізнес-процесів [121].

На графі рис. 3.22 позначено три онлайн-магазини – 1, 2 та 3. Веб-сервіси магазинів 1 і 2 співпрацюють з виробником товарів 4, а веб-сервіс магазину 3 співпрацює з виробником товарів 5. Обидва виробники зберігають вироблений товар на складі 8. Доступ до інформації про кількість та наявність товару на складі того чи іншого виробника надає веб-сервіс 8. Виробники товарів користуються різними службами доставки, що мають власні веб-сервіси (6 та 7) для оброблення запитів. Виробник 4 встановив нижчу вартість товару, ніж виробник 5 за рахунок зменшення витрат на виробництво та використання послуг служби доставки 6, які є дешевшими, ніж у служби доставки 7. Крім того, якість обслуговування в цього виробника вища, в результаті чого йому вдалося здобути більшу частину ринку продажів. Більшість онлайн-магазинів використовують сервіси виробника 4 для здійснення продажів та отримання вищого прибутку.

Перший бізнес-процес передбачає надходження запиту від клієнта до онлайн-магазину 1. Після аутентифікації та авторизації онлайн-магазин здійснює запит до веб-сервісу виробника 4, отримує список товарів, що пропонуються виробником та їхні характеристики, і відправляє цей список користувачу. Клієнт визначився з необхідним йому товаром і, вибравши опцію «Купити», відправив запит до онлайн-магазину. Магазин перенаправив відповідний запит про замовлений клієнтом товар до виробника 4. Виробник, пересвідчившись, що замовлений товар є на складі, та отримавши інформацію

від служби доставки 6 про вартість доставки, відправляє остаточну інформацію, в якій зазначена кінцева вартість товару, до онлайн-магазину. Після цього клієнт здійснює процедуру оплати за товар в одному з банків за допомогою сервісу онлайн-банкінгу, який реалізується веб-сервісами 9 та 10. За такими ж самим схемами працюють бізнес процеси 2 та 3. Проте, на відміну від першого та другого магазинів, третій онлайн-магазин, для прикладу, користується сервісами виробника 5.

Зазвичай, апаратних та програмних ресурсів веб-сервісу виробника 4 достатньо для забезпечення прийняттого рівня обслуговування для всіх запитів. Проте, внаслідок очевидних переваг, все більше магазинів починають використовувати сервіс виробника 4. Більше того, на ринку з'явився новий товар, який бажає отримати значна частина користувачів. У результаті стрімкого збільшення попиту кількість запитів, що обробляються веб-сервісом, також значно збільшилася, а якість обслуговування почала погіршуватися. У багатьох онлайн-магазинів є домовленості з декількома виробниками товарів про користування їхніми послугами, що дає їм змогу вибирати між сервісом того чи іншого виробника. Відповідно до алгоритмів вибору оптимального шляху проходження та оброблення сервісного запиту частина запитів з онлайн-магазинів 1 та 2 може бути перенаправлена до веб-сервісу виробника 5. Оскільки веб-сервіс виробника 5 не є настільки завантаженим, то це дасть йому змогу отримати більший дохід від збільшення кількості користувачів, знизити вартість товару та підвищити лояльність клієнтів до себе.

Для виробника 4 така ситуація призведе до значних фінансових втрат та погіршення його становища на ринку. Вирішенням цієї проблеми для виробника 4 є використання методу поліваріантного доступу. Цей метод використовує спеціальний сервіс для моніторингу стану веб-сервісів та завантаження апаратних ресурсів пристроїв, на яких ці веб-сервіси встановлено. У разі виникнення перевантаження одного з веб-сервісів метод поліваріантного доступу приймає рішення про створення ще однієї копії перевантаженого веб-сервісу на додатковому обслуговуючому пристрої

(реплікація на деякому сервері застосувань) [123]. Реплікація веб-сервісу здійснюється за допомогою технології адаптивної міграції веб-сервісів. Метод поліваріантного доступу можна застосовувати за допомогою брокера, який реалізує алгоритми маршрутизації запитів по шляхах за оптимальним критерієм рівня якості обслуговування. У випадку застосування методу поліваріантного доступу топологія графу логічних зв'язків між веб-сервісами для описаної вище моделі зміниться, що відображено на рис. 3.23.

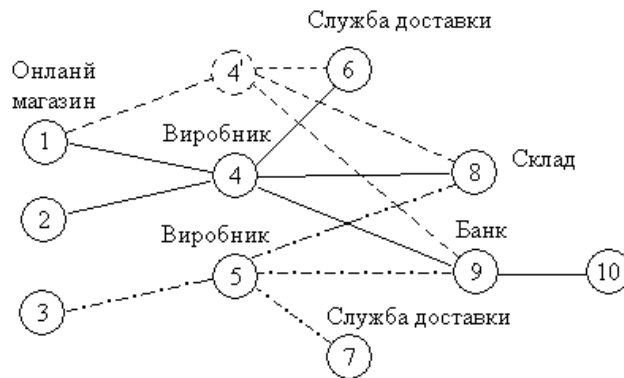


Рис. 3.23. Граф маршрутів проходження та оброблення запитів для трьох бізнес-процесів після застосування методу поліваріантного доступу [121].

Завдяки застосуванню брокером методу поліваріантного доступу утворилися два ідентичних веб-сервіси: 4 та 4'. Вони розташовані на різних серверах і обслуговують всі запити, які направлені до виробника 4. Брокер, застосовуючи алгоритми маршрутизації запитів, здійснює балансування навантаження між цими веб-сервісами. Виробник 4, у такому разі, хоч і змушений використовувати додаткові апаратні ресурси, за які йому потрібно додатково платити, все ж зможе зберегти лояльність клієнтів та забезпечити відповідну якість обслуговування, утримавши та навіть покращивши свою позицію на ринку. Додаткові витрати на оренду апаратних ресурсів ще одного сервера без проблем покриваються за рахунок істотного зростання доходів від продажів.

3.3. Експериментальні дослідження статистичних параметрів та характеристик інформаційних потоків в гетерогенних телекомунікаційних мережах.

Сучасні розподілені сервісно-орієнтовані мережі є складними гетерогенними системами. В основі більшості з них на сьогодні лежать так звані хмарні технології. Більшість телекомунікаційних мереж (ТКМ) є гетерогенними, тобто складаються із різноманітних програмно-апаратних засобів під керуванням різних операційних систем, та забезпечують споживачам широкий спектр інформаційних послуг. Це стає суттєвою перешкодою для досягнення необхідної якості обслуговування, зокрема дотримання часових вимог, для багатьох інформаційних систем та сервісних мережних платформ критичного застосування [124, 125].

Моделювання складних сервісних систем відбувається із застосуванням множини методів, в основі більшості з яких лежить теорія випадкових процесів у поєднанні з теорією телетрафіку. Із урахуванням властивості розподіленості, в таких системах особливого значення набувають методи керування інформаційним трафіком. Ефективне використання мережних ресурсів означає правильний їх розподіл, збільшення кількості послуг, відповідно – збільшення прибутку провайдера чи збільшення вигоди користувачу мережі за рахунок зростання ключових показників системної продуктивності та сервісної доступності.

Останні дослідження властивостей інформаційних потоків в гетерогенних телекомунікаційних системах показали, що використання моделей самоподібних процесів дозволяє більш точно описувати трафік, що передається в даних системах.

Оскільки в пакетному трафіку різних мереж було виявлено властивість самоподібності, виникла проблема побудови моделей, які могли б достатньо точно описати такий трафік або застосувати вже відомі моделі для опису подібних трафіків, що, зокрема, характерні для сервісів різного роду. Під час

дослідження та вивчення різних властивостей і характеристик систем передавання інформації виникає завдання побудови моделей вхідного трафіку, характеристики яких були б найближчими до характеристик реальних потоків даних заданого роду.

Характерною особливістю гетерогенних мереж можна вважати великі обсяги інформації, що циркулює в мережі та високі імовірно-часові вимоги до її передавання. В умовах істотного збільшення обсягів інформації у гетерогенних мережних системах особлива роль приділяється вдосконаленню й розробці нових технологій передавання та розподілу інформації, що забезпечують оперативність обміну на основі інформаційних технологій теорії масового обслуговування та методів фрактального аналізу. Традиційні методи розподілу мережних ресурсів припускають згладжування трафіка інформаційних потоків на основі статистичного мультиплексування. Існуючі методи керування перевантаженнями, які використовувались на критичних ділянках, також не враховують властивостей трафіка гетерогенних мереж [126]. Ця обставина визначає необхідність удосконалення класичного математичного інструментарію аналізу характеристик потоків, прогнозування навантаження та синтезу розподілених сервісних мережних систем для підвищення оперативності передавання інформації та її подальшого оброблення.

Таким чином, завдання підвищення оперативності передавання інформації в умовах збільшення її обсягів на основі розроблення математичних моделей і методів дослідження передавання інформаційних потоків в гетерогенних мережах має важливе науково-практичне значення та є актуальною. В загальному випадку, трафік деякої послуги представляється у вигляді випадкового процесу. Практичне використання такого методу опису є складним оскільки відсутній математичний апарат, що забезпечує оцінку параметрів якості нестационарного навантаження загального вигляду. Проте знання характеристик трафіку користувачів, який передаватиметься по мережі, є

неодмінною умовою для проектування будь-якої складної розподіленої гетерогенної мережної системи [127].

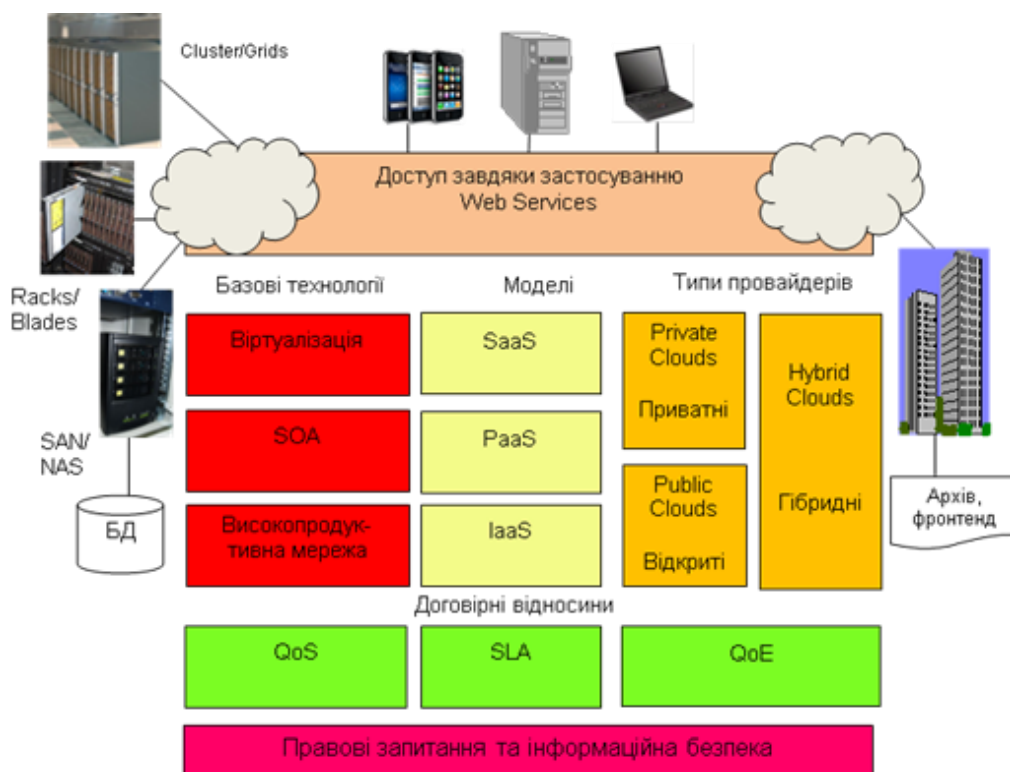


Рис. 3.24. Структура гетерогенної хмарної сервісної системи.

На рис. 3.24 ілюстративно зображено всі позитивні властивості, якими володіють гетерогенні Cloud-системи у порівнянні зі звичайною ІТ-системою. Важливо не забувати і про параметри надання сервісів у таких системах. Найважливішими критеріями щодо використання хмарних сервісів виступають функції, які відповідають за знання характеристик та параметрів трафіку на основі яких розробляються моделі забезпечення гарантованої якості їх надання.

3.3.1. Загальна характеристика досліджуваних мережних потоків.

Опис і аналіз інформаційних потоків сучасних гетерогенних мережних систем ускладнюється такими причинами:

- широкий діапазон швидкостей передавання інформаційних потоків;
- різноманітні статистичні властивості мультимедійних інформаційних потоків;

– велика різноманітність мережних конфігурацій, множина технологій і протоколів передавання;

– багаторівневе оброблення повідомлень, унаслідок чого якість обслуговування виявляється залежною від декількох рівнів оброблення.

В даній роботі аналізувався реальний трафік корпоративної мережі із використанням пріоритезації потоків навантаження [128]. В досліджуваній мережі існували групи користувачів, які прагнули отримати різнотипні сервіси з найкращою якістю, та мережеве обладнання, маршрутизатори, комутатори, серверні ферми, щоб надати зазначені сервіси та транспортувати дані до кінцевого користувача. Для того, щоб реально оцінити можливість якісного обслуговування мультисервісної мережної системи та вплив методів обслуговування різних типів потоків, дослідження проведено при одночасній наявності всіх мережевих потоків, утворених множиною користувачів.

Отже, кожен кінцевий користувач бажає отримати наступні мережні сервіси:

- Відео конференцв'язок із іншими користувачами (Skype);
- Голосовий зв'язок (IP-телефонія або VoIP);
- Під'єднання до мережної відео трансляції (IPTV);
- Перегляд онлайн відео (VoD);
- Інтернет-серфінг (Web Data);
- Високошвидкісне завантаження вибраного файлу із локального файлового сховища (Web Download).

Для захоплення, запису та аналізу мережного трафіку використано утиліту сніфер, а саме програмне забезпечення Wireshark Version 1.10.11, кінцевим результатом якої є створений дамп всіх мережевих пакетів присутніх на порті обслуговуючого пристрою за період спостереження. В даному дослідженні період запису рівний 2 хвилини. Цей параметр вибрано таким, виходячи з міркувань, який об'єм даних наявна обчислювальна техніка зможе обробити. Очевидно, що тривалі спостереження є досить ресурсоємними і потребують високих обчислювальних затрат. Отриманий дамп проаналізовано та визначено

наявність шести мережевих потоків, що відповідають кожній з бажаних послуг кінцевих користувачів або, сервісам, які надаються мультисервісною гетерогенною мережною системою (див. табл. 3.3).

Таблиця 3.3. Основні параметри мережних потоків кожного типу трафіку.

Тип трафіку	Протокол	Сер. довжина пакета L, байт	Смуга пропускання C, Кбіт/с	Пріоритет
SKYPE	RTSP	1370	3820	2
IPTV	UDP	1429	6044	4
Інтернет дані	HTTP	1514	7436	6
IP-телефонія	RTP	206	181	3
Відео за запитом (VoD)	TCP	666	1354	5
Службові дані	-	66	50	1
Загальний потік	-	1300	19122	-

На основі аналізу результатів проведених досліджень [129, 130] запропоновано класифікацію типів трафіку за сервісами і виконано підбір кожному типу сервісу таких статистичних законів розподілу навантаження, яке ним створюється, що дозволяють найбільш повно описати поведінку трафіку на конкретному рівні моделі IETF.

Для опису трафіку в гетерогенних IP-мережах найбільш широко застосовується розподіл Парето. Крім того, для трафіку певних сервісів обмежено використовуються розподіли Вейбулла, логнормальний і пуассонівський. Важливо відзначити, що розподіл Парето, як і розподіл Вейбулла і логнормальний, відноситься до розподілів з важким «хвостом» і володіє нескінченною дисперсією в діапазоні $1 < a < 2$, де показник a характеризує «важкість» «хвостів» розподілу і визначає пачкову структуру процесу. Такі процеси відносяться до самоподібних процесів. Таким чином, поведінка трафіку IP-мережі характеризується різними законами розподілу. В якості математичної моделі СМО може бути обрана система із загальними розподілами вхідного потоку і процесів обслуговування типу G/G/1. СМО типу G/G/1 є найбільш загальним випадком одноканальних систем масового обслуговування, в яку надходить довільний потік заявок загального вигляду з

функцією розподілу інтервалів між заявками $A(\tau)$. Тривалість обслуговування заявок в приладі розподілена за довільним законом $B(\tau)$. Завдання розрахунку систем виду $G/G/1$ для зазначених вхідних процесів і процесів обслуговування ускладнене тим, що дисперсії цих процесів є нескінченними.

Розрахунок таких систем вимагає задання конкретних законів розподілів, що не дозволяє отримати аналітичне рішення в загальному вигляді. Аналітичне рішення можливе лише для деяких розподілів, наприклад, експоненційного. Для більшості законів розподілів інтервалів між запитами, що надійшли до сервісної мережної системи і тривалостей їх обслуговування неможливо отримати точне рішення в аналітичній формі.

У той же час, на практиці при дослідженні реальних сервісних мережних систем рідко бувають відомі закони розподілів зазначених величин. Зазвичай, при описі процесів надходження запитів до системи і їх обслуговування в деяких приладах СМО обмежуються кількома моментами відповідних розподілів, найчастіше - двома першими моментами, які задаються у вигляді математичного очікування і середньоквадратичного відхилення або коефіцієнта варіації шуканої випадкової величини. Однак, при цьому виявляється неможливим отримання точного результату. Це обумовлено тим, що у випадку довільного (відмінного від найпростішого) потоку запитів, що надходять у систему, характеристики функціонування СМО, зокрема середній час очікування, залежать не лише від двох перших моментів, але і від моментів більш високого порядку - третього, четвертого і т.д. Причому ця залежність тим менша, чим вищим є порядок числового моменту.

Таким чином, всі результати, отримані в аналітичній формі при заданні інтервалів між заявками, що надійшли до сервісної мережної системи і тривалостями їх обслуговування двома першими моментами - середніми значеннями $a = 1/\lambda$ і $s = 1/\mu$ і коефіцієнтами варіації C_a і C_s , являють собою наближені залежності.

Завдяки результатам дослідження, маючи кількість всіх пакетів і довжину кожного пакета, можна побудувати графік розподілу кількості пакетів відносно часу дослідження, та відношення пропускної здатності (швидкості завантаження за одиницю часу) відносно часу дослідження. Через нерепрезентативність даних, вхідні значення для графіків не представлено. Задля збереження якості подання інформації, графіки наводяться в оригінальному вигляді, який отримується в програмі Wireshark, без умовних позначень осей абсцис та ординат, крім розмітки. Тривалість наведена у секундах, швидкість передавання – у бітах на секунду (bits per second).

Інтенсивність надходження переданої/отриманої інформації в бітах на секунду до часу тривалості досліду показано на рис. 3.25-3.29. Дослідження проводились в корпоративній мережі провайдерів НТЦ МТ Національного університету «Львівська політехніка», а також на мережних ресурсах Інтернет-провайдера Airbites у м. Львові.

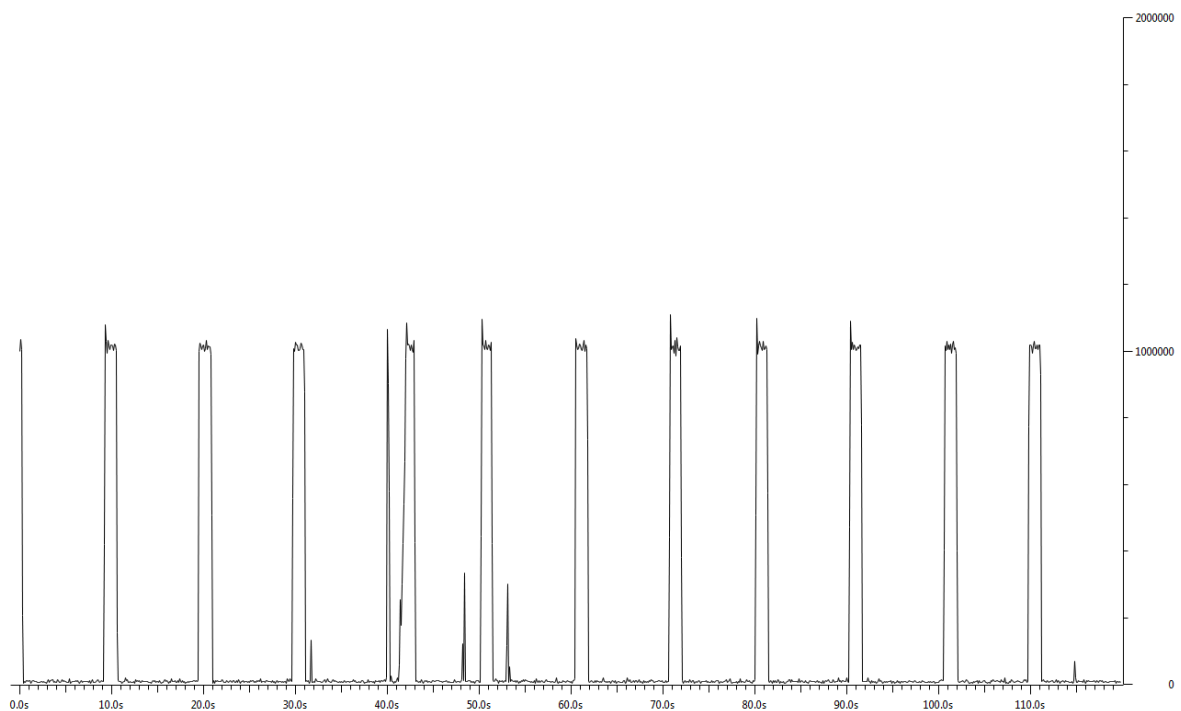


Рис. 3.25. Трафік при он-лайн перегляді відеофайлу.

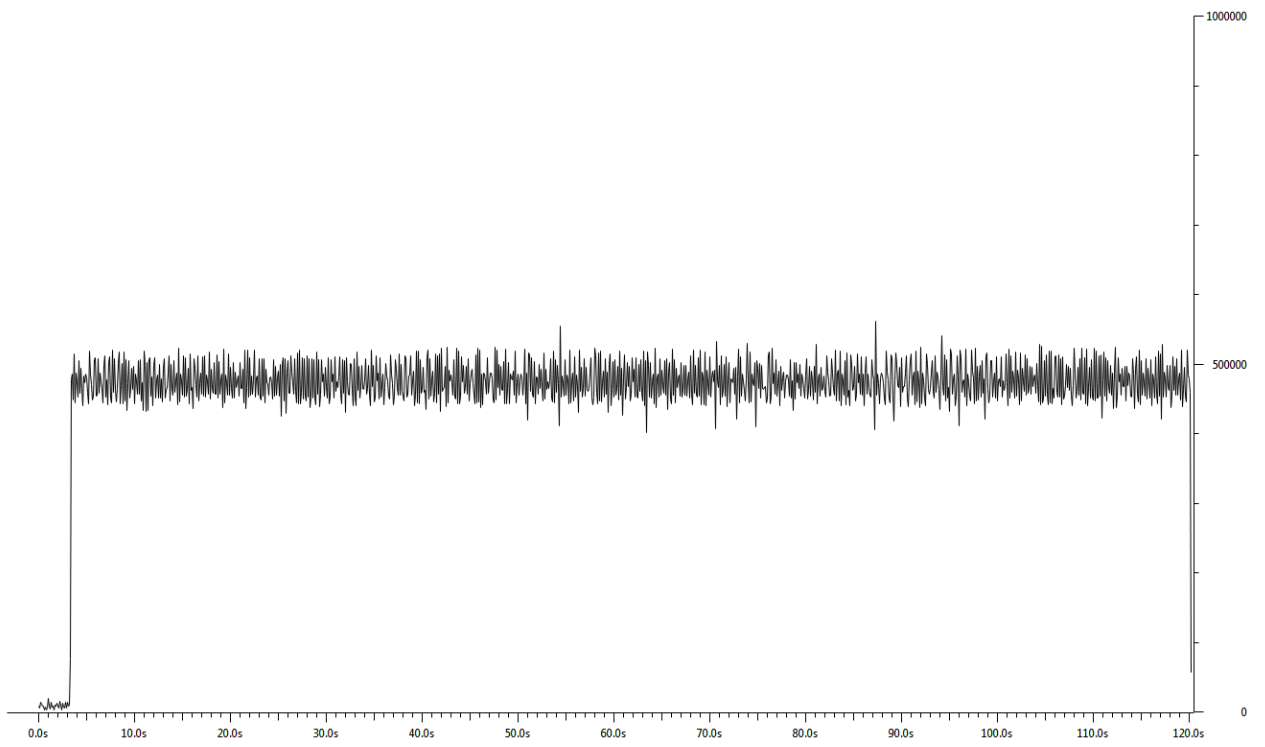


Рис. 3.26. Трафік при перегляді IPTV послуги.

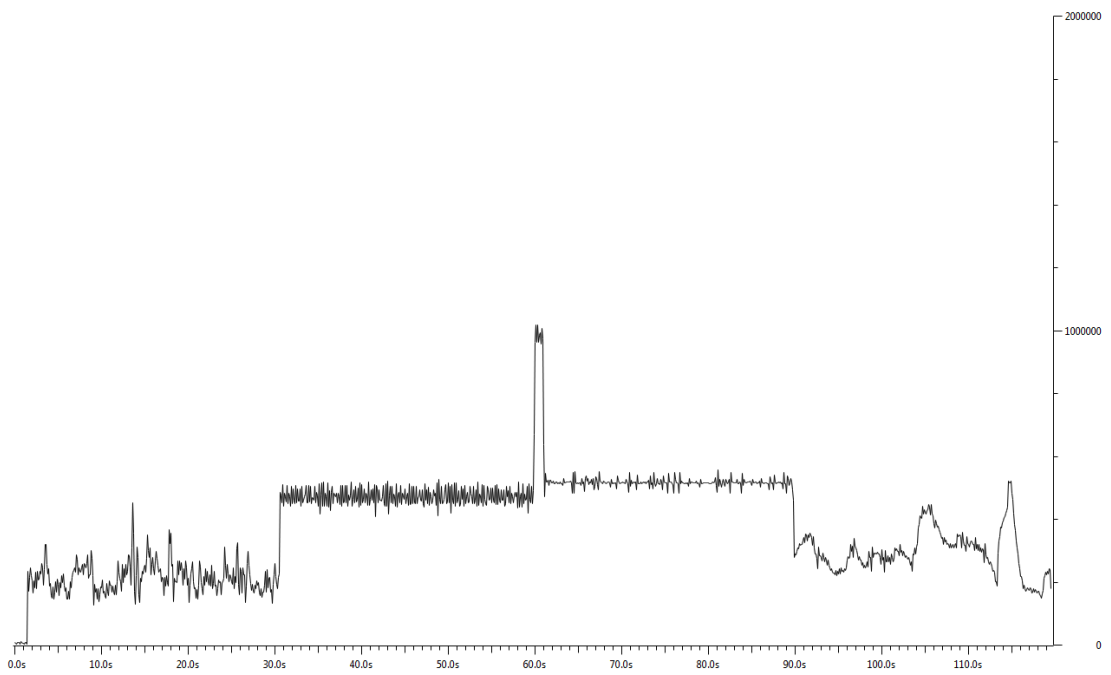


Рис. 3.27. Трафік при перегляді різних каналів IPTV послуги.

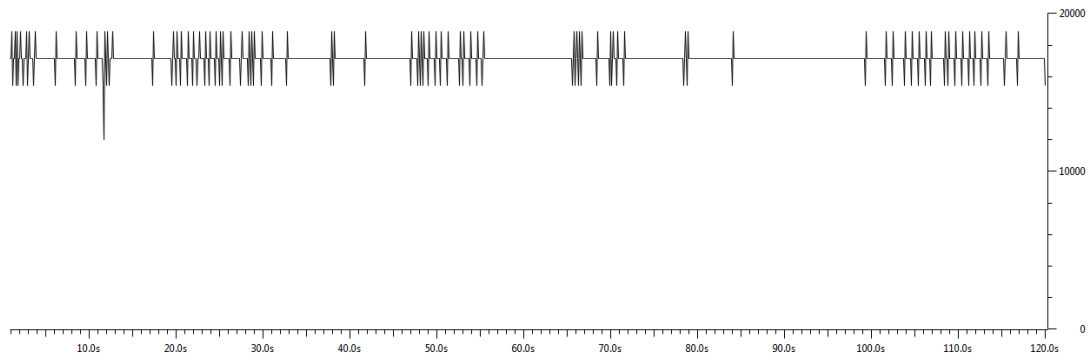


Рис. 3.28. Трафік при обслуговуванні з'єднань на основі послуги ІР-телефонії.

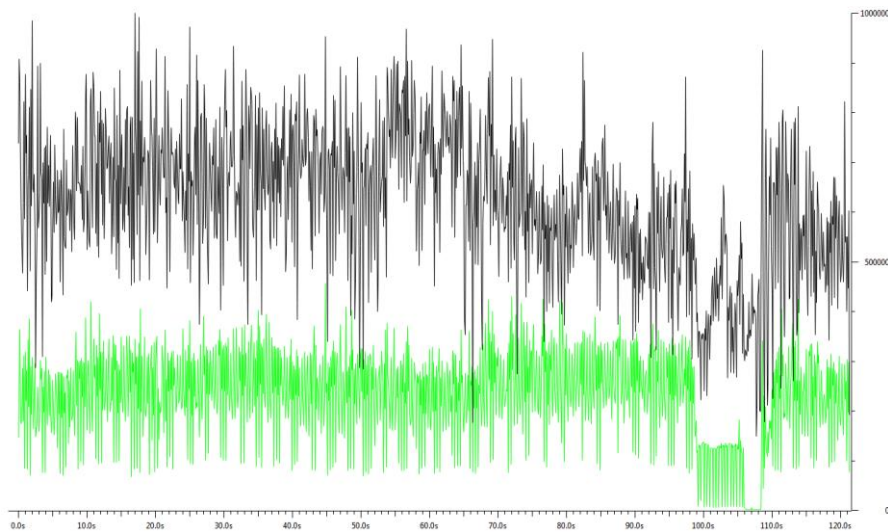


Рис. 3.29. Трафік сервісів SKYPE (світлішим) та IPTV (темнішим).

3.3.2. Підбір теоретичних законів розподілу і їх параметрів.

Для аналізу і вибору теоретичного розподілу, який найкраще характеризуватиме отриманий експериментальним шляхом розподіл, використаємо наступні закони розподілу:

Нормальний закон розподілу:

$$f(x) = \frac{1}{\sqrt{2\pi\sigma^2}} e^{-\frac{(x-m)^2}{\sigma^2}}. \quad (3.18)$$

$$F(x) = \frac{1}{\sqrt{2\pi\sigma^2}} \int_{-\infty}^{\infty} e^{-\frac{(x-m)^2}{\sigma^2}} dx. \quad (3.19)$$

Для даного розподілу $m = Mx$, а $\sigma^2 = S^2$.

Показниковий закон розподілу:

$$f(x) = \lambda e^{-\lambda x}. \quad (3.20)$$

$$F(x) = \begin{cases} 0, & x < 0 \\ 1 - e^{-\lambda x}, & x \geq 0 \end{cases}. \quad (3.21)$$

Параметр λ визначається як:

$$\lambda = \left| \frac{1}{M_x} \right|. \quad (3.22)$$

Розподіл Пуассона:

$$f(x) = \frac{\lambda^x}{x!} e^{-\lambda}, \quad (3.23)$$

$$F(x) = \frac{\Gamma(\lfloor k+1 \rfloor, \lambda)}{\lfloor k \rfloor!}, \quad (3.24)$$

де $\Gamma(x, y)$ - це неповна гама-функція та $\lfloor k \rfloor$ - це ціла частка.

Для даного розподілу $\lambda = Mx$.

Релеєвський закон розподілу:

$$f(x) = \frac{x}{\sigma^2} e^{-\frac{x^2}{2\sigma^2}}, 0 \leq x < \infty, \quad (3.25)$$

$$F(x) = 1 - e^{-\frac{x^2}{2\sigma^2}}, 0 \leq x < \infty. \quad (3.26)$$

Параметр σ визначається як:

$$\sigma = |M_x| \sqrt{\frac{\pi}{2}}. \quad (3.27)$$

Логнормальний закон розподілу:

$$f(x) = \begin{cases} \frac{1}{x\sigma\sqrt{2\pi}} e^{-\frac{(\ln x - \mu)^2}{2\sigma^2}}, & x > 0 \\ 0, & x \leq 0 \end{cases}, \quad (3.28)$$

$$F(x) = 0.5 - 0.5 \operatorname{erf} \left[\frac{\ln x - \mu}{\sqrt{2\sigma^2}} \right]. \quad (3.29)$$

Для агрегованого потоку навантаження характерною є статистична картина, що подана на рис. 3.30. Встановлено, що найбільш придатним законом статистичного розподілу для даного випадку є релеєвський. Для даного розподілу $\mu = Mx$, а $\sigma^2 = S^2$.

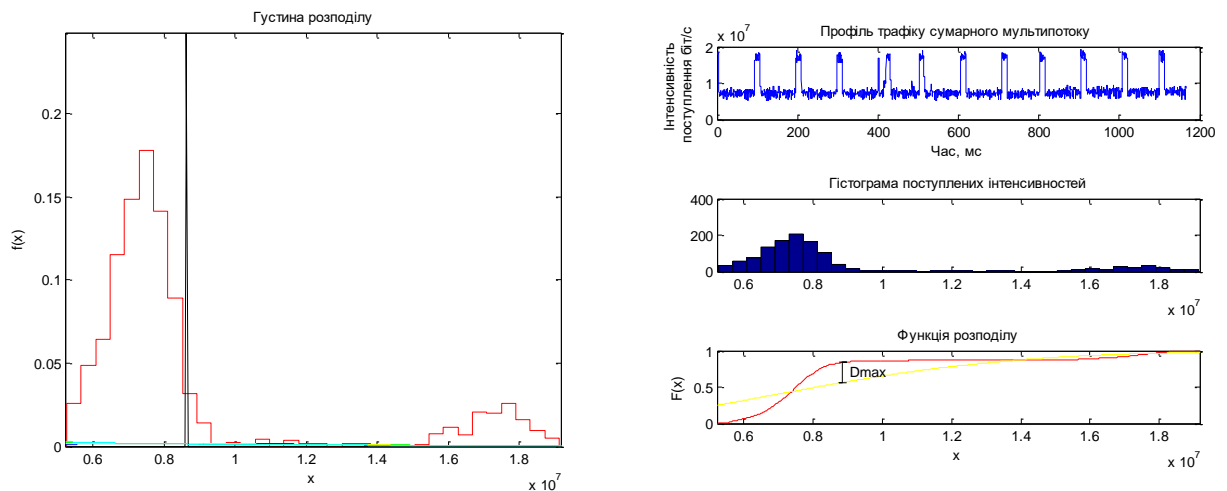


Рис. 3.30. Статистичний аналіз багатопотокового (агрегованого) трафіку.

З метою перевірки адекватності обраної статистичної моделі емпіричній вибірці висунуто статистичну гіпотезу H_0 про адекватність статистичної моделі обраній емпіричній вибірці. Для перевірки гіпотези використано статистичні критерії узгодженості Колмогорова, Пірсона та Колмогорова-Смірнова.

У табл. 3.4-3.6 наведено результати дослідження обраної вибірки інтенсивності мережного трафіку, а на рис. 3.30 наведено гістограму вибірки апроксимуючих кривих досліджуваних розподілів.

Таблиця 3.4. Результати перевірки статистичної гіпотези за допомогою критерію Колмогорова з параметром значущості $p=0,05$.

Статистичний розподіл	$\lambda_{кр.}$	$\lambda_{емп.}$	H_0
Нормальний	1,358	1,328	Приймається
Показниковий		1,323	Приймається
Пуассона		1,894	Відкидається
Релеєвський		1,635	Відкидається
Логонормальний		2,569	Відкидається

Таблиця 3.5. Результати перевірки статистичної гіпотези за допомогою критерію Колмогорова-Смірнова з параметром значущості $p=0,05$.

Статистичний розподіл	$K_{\alpha \text{кр.}}$	$K_{\alpha \text{емп.}}$	H_0
Нормальний	0,5	0,1931	Приймається
Показниковий		0,6071	Відкидається
Пуассона		0,7844	Відкидається
Релеєвський		0,4974	Приймається
Логонормальний		0,7103	Відкидається

Таблиця 3.6. Результати перевірки статистичної гіпотези за допомогою критерію Пірсона з параметром значущості $p=0,05$.

Статистичний розподіл	$\chi^2_{\text{кр.}}$	$\chi^2_{\text{емп.}}$	H_0
Нормальний	0,59	0,397	Приймається
Показниковий		5,206	Відкидається
Пуассона		6,028	Відкидається
Релеєвський		3,672	Відкидається
Логонормальний		2,631	Відкидається

В проведених дослідженнях для визначення ступеня самоподібності трафіку використовувався параметр Херста, який може приймати наступні значення:

- $0 \leq H \leq 0,5$ – випадковий процес, випадковий ряд, який не володіє самоподібністю;

- $H = 0,5$ – повністю випадковий ряд, аналогічний до випадкових зміщень частинки при класичному броунівському русі;

- $H > 0,5$ – процес, який володіє довготривалою післядією і є самоподібним.

Для оцінювання значень параметра Херста випадкового ряду існує багато методик. Найпростішою з них є RS-методика, яка, проте, має обмеження на застосування до процесів з малою дисперсією. Однак для потреб задач, вирішення яких пропонується в роботі, дана методика може бути використана.

Її суть полягає в наступному. Визначається математичне сподівання випадкового ряду X_k ($k=1..N$):

$$M_N = \frac{1}{N} \sum_{k=1}^N X_k \quad (3.30)$$

Визначається дисперсія вибірки:

$$S_N^2 = \frac{1}{N} \sum_{k=1}^N (X_k - M)^2 \quad (3.31)$$

Визначається інтегральне відхилення:

$$D_j = \sum_{k=1}^j X_k - jM, \quad j \in [1; N] \quad (3.32)$$

Визначається рознесення випадкового процесу:

$$R_N = \max_{1 \leq j \leq N} D_j - \min_{1 \leq j \leq N} D_j \quad (3.33)$$

На основі встановленого Херстом співвідношення:

$$\frac{R}{S} \approx \left(\frac{N}{2}\right)^H, \quad (3.34)$$

визначається параметр Херста H :

$$H = \frac{\log\left(\frac{R}{S}\right)}{\log\left(\frac{N}{2}\right)} \quad (3.35)$$

Узагальнюючи отримані результати для кожного типу трафіку за видами сервісу згідно (3.30-3.35) можливо розрахувати відповідні типові значення параметру Херсту за RS методикою, що подані в табл. 3.7 нижче [131].

Таблиця 3.7. Основні статистичні параметри мережних потоків для кожного типу трафіку телекомунікаційної платформи, що досліджувався.

Тип трафіку	Коефіцієнт варіації	Параметр Херста, H
SKYPE	0,200	0,513
IPTV	0,204	0,346
Інтернет дані	0,207	0,685
ІР-телефонія	0,370	0,981
Відео за запитом (VoD)	0,194	0,608
Службові дані	0,183	0,719
Загальний потік	0,39	0,639

3.4. Завдання оптимізації розподілу телекомунікаційних мережних ресурсів хмарних платформ для обслуговування сервісного навантаження із заданою якістю.

Структурно-функціональна цілісність сучасної хмарної парадигми організації мережних систем є дуже важливою для побудови масштабованих та надійних комерційних мережних інфраструктур, використовуючи SOA. Дедалі більше сервісних застосувань використовують зазначену концепцію сервісно-орієнтованої архітектури для того, щоб перебувати на очікуваному від них рівні ефективності у світі, де конкуренція визначає позиції ринкових гравців у сфері інфокомунікацій, а саме: електронного бізнесу, електронної комерції, особистих комунікацій, електронних фінансів та іншої діяльності [65, 132, 133]. Проте, згадані концепції мережних технологій з'явилися зовсім нещодавно. Внаслідок надзвичайно високої складності розроблення і проектування та високої вартості подібних мережних рішень, у даній роботі робиться спроба для розв'язання завдання розроблення загального аналітичного методу їх синтезу, керуючись структурними та функціональними оптимізаційними параметрами у рамках заданих обмежень для типових сервісних мережних платформ. SDP розглядаються автором на усіх трьох найбільш поширених рівнях модельних реалізацій, а саме IaaS, PaaS та SaaS. Як правило, перехід між рівнями IaaS та PaaS, а також між рівнями PaaS та SaaS якісно змінює показники функціонування сервісної мережної системи в бік покращення, в тому числі – в умовах її масштабування. Кожна нова мережна реалізація вищого рівня (сервісна надбудова) є покращеною або оптимізованою версією відповідної нижче розташованої мережної платформи.

Отже, на сьогодні обчислювальні сервіси на основі хмарних рішень, внаслідок непорівнянно вищої техніко-економічної ефективності широко розповсюджуються, використовуючи практично усі доступні ніші ІТ-ринку, надаючи бізнесу вищої ефективності та гнучкої масштабованості [133, 233].

Найбільш відомі рішення останніми роками були репрезентовані компаніями: Microsoft (Microsoft Azure), Google (Google Apps Engine), Amazon (Elastic CloudComputing, Simple Storage Service), IBM (Blue Cloud), Nimbus, Oracle та іншими. Приклад реалізації хмарної сервісної мережної платформи зберігання даних від Amazon представлено на рис. 3.31.

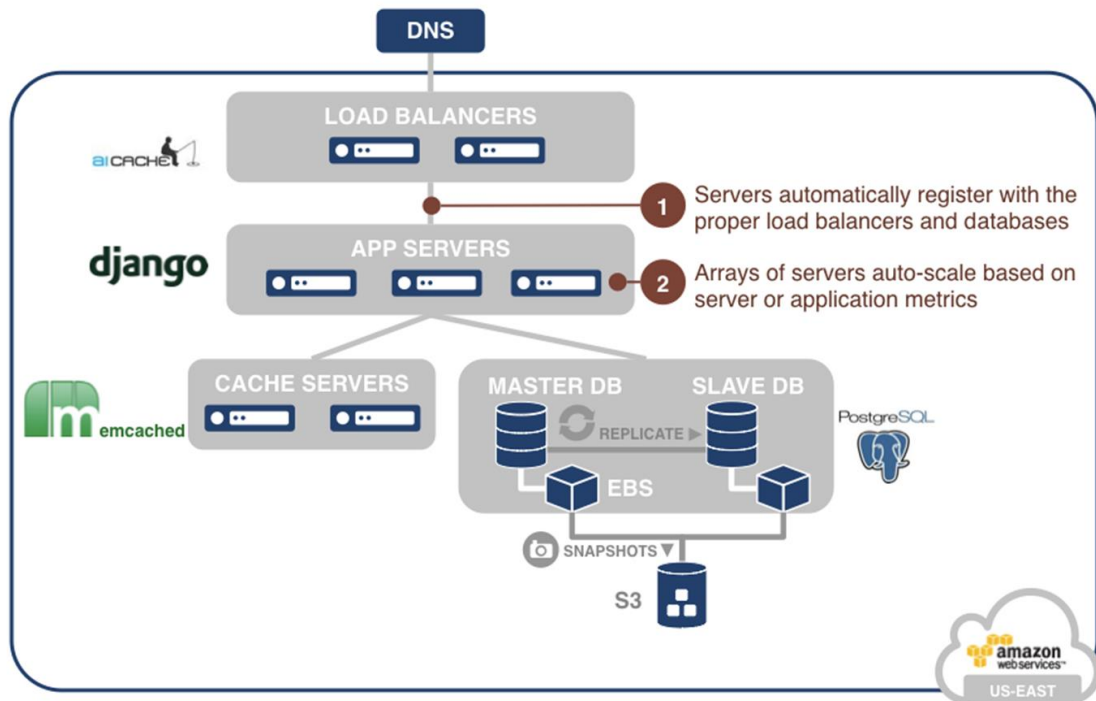


Рис. 3.31. Приклад сервісного мережного рішення «Elastic Cloud» від Амазон.

Окрім великих корпоративних хмарних рішень, сервіси хмарних обчислень надаються також невеликими компаніями. Доступні, часом безкоштовні рішення є поширеними на ринкових просторах, серед них: iCloud, Cloudo, FreeZoho, SalesForce тощо. Всі ці сервісні мережні рішення розрізняються сервісними моделями, що ними пропонуються, такими, як рівень SaaS (англ. software as a service), PaaS (англ. platform as a service), а також IaaS (англ. infrastructure as a service). Виникають також пропозиції виду HaaS (англ. hardware as a service). Незважаючи на розмаїття сервісних рішень (часто вживають поняття XaaS), для їх побудови використовують досить типові апаратні та програмні засоби, що лягають в основу більшості хмарних мережних систем. Ними, як набором віртуалізованих сервісних вузлів або віртуальних машин, які реплікуються при масштабуванні системи,

забезпечується функціонування цих систем у відповідності до сервісно-орієнтованої архітектури, що повинна бути реалізована. При цьому гнучко підтримується множина необхідних сервісів, у відповідності до узагальнених потреб користувачів. Відповідні апаратні та програмні засоби можуть виходити з ладу, працювати неправильно, наприклад, внаслідок збоїв різного роду. В процесі їх експлуатації, з певними ймовірностями, можливі погіршення показників якості та надійності їх функціонування, зокрема внаслідок процесів фізичної деградації. Для мінімізації впливу відмов обладнання та програмного забезпечення на відповідні загальносистемні показники, а також для зменшення тривалості періоду відновлення працездатності хмарної сервісної платформи застосовуються ті самі принципи, що і в галузі розподіленого оброблення даних (гаряче резервування (IaaS), перерозподілення потоків навантаження до інших обчислювальних потужностей (PaaS), міграція сервісних компонентів на інші серверні платформи (SaaS), тощо). Ці принципи орієнтовані на приховування від користувачів реального стану речей у сервісній мережній системі, зокрема щодо сервісної доступності. Для них створюється враження безвідмовного системного функціонування. Крім того, типова статистика відмов у хмарних реалізаціях SOA є досить цікавою (див. табл. 3.8) [134]. Це демонструє, що існуючі підходи до створення та підтримки високонадійних за функціонуванням хмарних сервісних систем (тобто підтримки високого рівня сервісної доступності) на сьогодні все ще потребують вдосконалення.

Розглядаючи ситуацію з даними табл. 3.8 більш глибоко, можна прийти до висновку, що наведена статистика свідчить не лише про тимчасову недоступність сервісів хмарних мережних систем. У випадку відмови сервісів Microsoft Sidekick були втрачені всі персональні дані їх користувачів [134], які, щоправда, згодом було відновлено, проте, все ж, не повністю.

Таблиця 3.8. Типова статистика відмов у хмарних сервісних системах [134].

№	Назва сервіс-провайдера	Сервіси, що були недоступними	Дата	Період недоступності, год.
1	Google	Gmail, Google Apps Engine	24.02.2009	2,5
2	Google	Google Search	31.01.2009	0,66
3	Google	Google Gmail	9.03.2009	22
4	Google	Google Network	14.05.2009	2
5	Amazon	Amazon Elastic Cloud Computing	11.06.2009	7
6	Amazon	Amazon Elastic Cloud Computing	9.12.2009	5
7	Amazon	Amazon Simple Storage Service	15.02.2008	2
8	Amazon	Amazon Elastic Cloud Computing	21.04.2011	27
9	Microsoft	Microsoft Azure	13-14.03.2008	22
10	Microsoft	Microsoft Hotmail	12.03.2009	5
11	Microsoft	Microsoft Sidekick	4.10.2009	144
12	Flexiant	FlexiScale	31.10.2008	18

Незважаючи на доволі значну кількість впроваджень різних рішень для підвищення рівня сервісної доступності, сервісні мережні системи все ще зазнають детального аналізу з метою пошуку «вузьких місць» їх реалізацій у SOA, що дозволить підвищити функціональну стійкість та надійність, рівень сервісної доступності, показники системної продуктивності [2, 62]. Актуальність згаданих питань на сьогодні залишається високою.

Приклад специфічного системного програмного коду для реалізації концептуальної моделі SaaS на основі деякої розподіленої сервісної платформи (наприклад, див. рис. 3.31) з використанням функціональної парадигми системного програмування мовою Erlang наведено у Додатку Б даної дисертаційної роботи. Зокрема показано:

- Послідовну компоненту початкового коду (її мінімізована реалізація займає близько 40% загального обсягу коду програмного модуля) – моделює мережний TCP шлюз (TCP gateway);
- Розпаралелену компоненту початкового коду (її мінімізована реалізація займає близько 60% загального обсягу коду програмного модуля) – моделює балансувальник сервера послуг (application server and RR balancer) за алгоритмом Round Robin;
- Просте сервісне застосування, що може реплікуватись у довільній доступній обчислювальній потужності розподіленої сервісної мережної платформи під управлінням вищезгаданого сервера послуг.

Як можна буде побачити далі у розділі 4.1, співвідношення 60% розпаралеленої компоненти програмного коду до 40% його послідовної компоненти є не випадковим і характеризує оптимальну структурну композицію системних програмних модулів у рамках побудови SaaS модельної реалізації деякої сервісної мережної системи за критеріями системної продуктивності та сервісної доступності.

В подальшому автор використовуватиме термін «структурний параметр» для означення кількісної структури елементарних сервісних компонентів (в рамках сервісної платформи деякого концептуального рівня або сервісного застосування) оптимально зкомпонованих у структурі віртуальних машин (або віртуалізованих мережних елементів), адже для опису структури хмарних сервісних систем неможливо застосувати типові топологічні чи архітектурні шаблони, а якщо це і можливо, то такі шаблони будуть надто узагальненими,

нечітко заданими, значно відрізняючись при спробах формалізації у термінах звичайних мережних систем різного виду. У загальному, топологія та структура сукупності віртуальних машини (VM) є динамічною, так само, як і сукупність сервісів та сервісних компонентів, що ними реалізується. VM піддаються процесам міграції в межах заданих сервісних платформ PaaS [135], а також реплікують елементарні сервісні компоненти у відповідності до поточного рівня потреб користувачів. Таким чином, можна стверджувати, що хмарна SOA одержує у своє розпорядження «купу» (англ. «heap») мігруючих ресурсів у середині сервісної мережної системи, яка є надзвичайно розподіленим об'єктом, реалізуючи власне платформу надання сервісів, тобто деяку SDP імплементацію. Ми можемо виокремити деякі специфічні групи сервісних компонентів, які використовуються для організації в рамках процесів оркестрування заданого комплексного сервісу, в умовах створення та впровадження деякого сервісного застосування або сервісу взагалі, що буде використовуватись користувачами SDP. Класифікація сервісних компонентів, як потоків завдань, які реалізуються процесорами сервісної мережної платформи у формі VM для SaaS моделі, або сукупності VM, яка підтримується процесорами серверних систем для PaaS моделі, або ж множини елементів PaaS, яка розміщується на деякій мережній (зокрема – віртуалізованій) інфраструктурі може бути виконана у відповідності до визначень закону Амдала (Amdahl's Law) [151, 230]. Таким чином, у загальному випадку, ми можемо виділити гіпервізори та інші сукупності елементарних сервісних компонентів (ESC) сервісної платформи або сервісного застосування, що функціонують послідовно (в послідовних сегментах застосувань) (α) в одну групу, а елементарні сервісні компоненти, що функціонують паралельно (у паралель одні з іншими, в паралельних сегментах застосувань) ($n - \alpha$) – в іншу, див. рис. 3.32. Тут і надалі параметр n означає загальну кількість ESC у деякій моделі сервісної мережної системи.

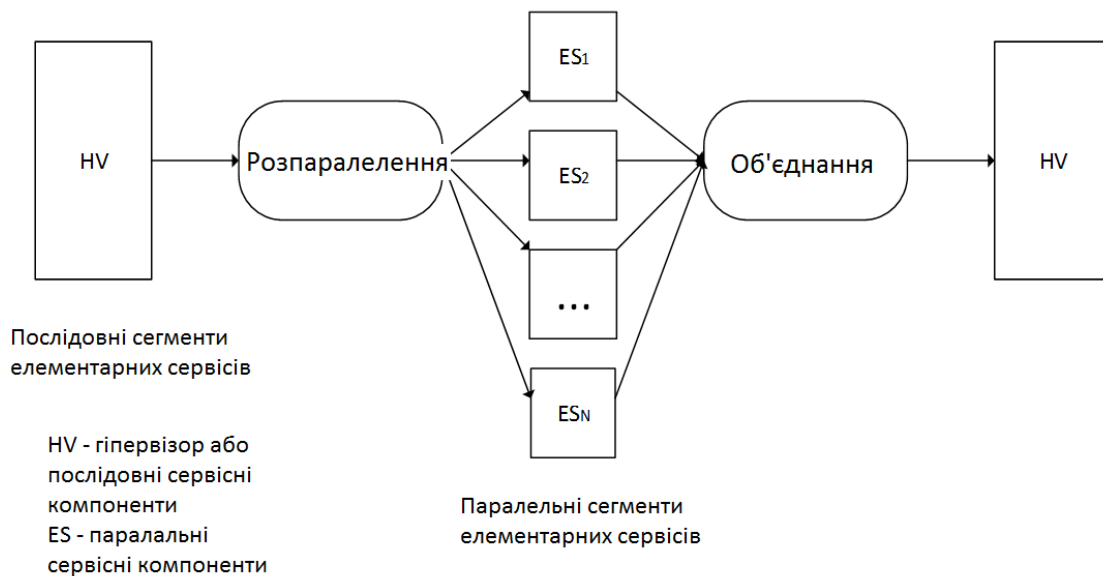


Рис. 3.32. Паралельні та послідовні сегменти застосувань, як варіант фрагменту елементарної сервісної структури в реалізації SOA.

Таким чином, завдання оптимального структурно-параметричного синтезу сервісних мережних платформ може бути зведене до завдання вибору їх оптимальних структурно-композиційних та функціональних параметрів у рамках деякої заданої архітектури виду SOA, а саме оптимального вибору кількості ESC для кожної з двох вище визначених груп у процесі їх комбінування та вбудовування в конкретну реалізацію SDP (рівня IaaS, PaaS або SaaS), див. рис. 6.18-6.21, рис. 4.13, 4.15. Нажаль, навіть у такій дещо спрощеній, на перший погляд, постановці питання, основні труднощі щодо розв'язання завдання оптимального структурно-параметричного синтезу вносяться перш за все браком знань про природу статистичних (ймовірнісних) процесів обслуговування трафіку структурою сервісних застосувань SDP, яка навантажена запитами користувачів на одержання сервісів заданого типу [136-139]. Функціональні властивості запитуваних сервісів повинні бути визначені статистично, тому найбільш вигідним, на думку автора, шляхом для їх опису є визначення статистичних параметрів навантаження користувацьких запитів, що їм притаманне та обслуговується синтезованою сервісною мережною платформою [131]. Параметр самоподібності трафіку Херста (Hurst) є доволі компактним та містким показником статистичної природи трафіку. Відповідно, у [131] та розділі 3.3 цієї дисертаційної роботи було проведено дослідження

статистичних властивостей та характеристик основних типів сервісного навантаження корпоративних мережних платформ (таких, як VoIP, VoD, IPTV Multicast, Web data тощо). Надалі, у наведеному в цій дисертації підході під терміном «функціональний параметр» автор буде мати на увазі попередньо експериментально (статистично) визначений та розрахований параметр Херста для відповідного типу сервісного навантаження, що має обслуговуватися хмарною сервісною платформою в рамках SOA. Також для цього навантаження будуть враховуватись його інтенсивність та коефіцієнт варіації.

Таким чином, для кожної синтезованої реалізації хмарної сервісної архітектури сервісна доступність буде представлена та розрахована для кожного функціонального сервісу, що надається SDP, так само, як і відповідний показник системної продуктивності. Кожна така реалізація хмарної сервісної архітектури володітиме власною структурною комбінацією ESC. Обидва згадані показники, а саме сервісна доступність та системна продуктивність були обрані автором, як критерії оптимального структурно-параметричного синтезу SDP.

У наступних розділах роботи автор спробує представити ці критерії у математичній формі для подальшого аналізу. Після цього, буде визначено всі параметри, які використовуються у математичних виразах критеріїв, для того щоб спростити завдання реалізації оптимального процесу синтезу шляхом математичного моделювання. Додатково приймається припущення, що реалізація транспортного шару SDP забезпечує оптимальне обслуговування сервісних мережних потоків при їх гнучкому перерозподілі [136].

3.4.1. Критерії оптимального структурно-параметричного синтезу та пов'язані з ними параметри.

Як відомо, найпростіша мережна структура (за топологією) є ненапрямленим (неорієнтованим) графом G із множиною вершин V та множиною ребер (дуг) E , які відносяться до мережних вузлів та каналів зв'язку, відповідно. Найпростішою моделлю структурної надійності інформаційних сервісних систем, або, якщо бути точнішим, їх доступності є імовірнісний граф

$(G; p)$ де $p = \{p(\varepsilon); \varepsilon \in E\}$. Вона може бути охарактеризована незалежним видаленням ребер (дуг) із G , $\varepsilon \in E$ з імовірністю $q(\varepsilon) = 1 - p(\varepsilon)$.

У деякій сервісній системі, доступність буде характеризуватися як живучість множини VM, яка реалізує задану послугу, або як здатність системи швидко і легко відновити нормальний режим роботи. Проте, ця концепція може бути описана, як здатність системи функціонувати протягом тривалого періоду часу з максимальною ефективністю, тобто надійно. Концепції сервісної доступності та живучості в теорії складних систем (наприклад, хмарних мереж) є взаємопов'язаними.

Найбільш важливим компонентом надійності хмарних систем є властивість сервісної доступності, що описує здатність мережної платформи зберігати працездатність безперервно в заданих умовах і протягом заданого інтервалу функціонування, та розраховується через живучість розподіленої сервісної реалізації, утвореної компонуванням (наприклад, у межах PaaS) сукупності VM, що використовуються для реалізації заданих комбінацій ESC.

Поєднання ESC утворює деякий комплексний сервіс або застосування, що безпосередньо його реалізує.

Властивості конкретного поєднання ESC суттєво впливають на сервісну доступність і загальну системну продуктивність.

Отже, для оцінки параметра сервісної доступності в хмарній сервісній системі, слід чітко розуміти, що топологія мережі є динамічною і постійно змінюється. У нашій моделі ми оцінюємо живучість сервісних мережних структур з точки зору ймовірності успішного з'єднання двох їх сегментів в наступний момент, тобто, того що буде організоване, щонайменше, одне ребро.

Це ребро є «ключовою ланкою» для з'єднання відповідних сегментів. З іншого боку, повинні також бути в працездатному стані ESC, тобто не перевантаженими і у змозі обробляти заданий потік запитів. Відповідні ймовірності залежать від імовірності відмови деякого шляху всередині сегмента сервісної системи (тобто, між компонентами всередині кожного сегмента має існувати принаймні один маршрут); імовірності відмови кожної

віртуальної машини, яка використовується деякою сукупністю ESC у будь-який заданий момент часу, а це означає, що наведені імовірності також залежать від ймовірності блокування запитів на ESC всередині кожного сегмента сервісної мережної системи.

У роботі [140] в рамках поняття живучості інформаційних систем розуміється здатність системи виконувати свої основні функції (принаймні, в межах допустимої втрати якості обслуговування) під впливом зовнішніх факторів. Це визначення близьке за змістом до визначення [141]. В роботі [142] це поняття визначається як властивість об'єкта, яка виражається як здатність виконати поставлене завдання під час дії несприятливого впливу на весь об'єкт або його окремі компоненти, зберігаючи в прийнятних межах функціональну продуктивність. Ці визначення звертають увагу на такі аспекти. Перший з них: живучість слід розглядати як внутрішню властивість системи, оскільки вона не залежить від умов її експлуатації, що виникають в будь-який заданий момент часу. Ця властивість їй належить постійно і до деякої міри несприятлива обстановка функціонування може скластися навіть при нормальних умовах експлуатації, оскільки час від часу відбуваються збої, які викликані виробничими дефектами, деградацією, збереженням системних компонентів тощо. Але в повному обсязі живучість системи піддається випробуванню зовнішніми впливами, які є неочікуваними в процесі її нормальної роботи. А такі впливи є важко прогнозованими, тому що вони створюють екстремальні умови експлуатації системи. Другий аспект: система підтримує не всі функції, які вона повинна виконувати в процесі нормальної роботи, а тільки основні функції, причому допускаючи іноді можливість зниження QoS. Зі збільшенням ступеня серйозності відхилень у експлуатації системи її слід піддавати оптимізації.

У дослідженнях живучості і доступності систем можна виділити ряд різних теоретичних підходів і, таким чином, застосування різних методів аналізу: теоретико-ігрових [143-144], імовірнісних [145], детермінованих [146, 147], графо-аналітичних [148, 149]. Імовірнісний і детермінований підходи є

найбільш розробленими для технічних цілей. Основні ідеї вищеперелічених методів були досить повно викладені в роботі [149].

Імовірнісні методи дослідження живучості засновані на припущенні про рівномірний закон розподілу несприятливих (шкідливих) впливів (НЕ) в рамках досліджуваної системи або на припущенні про той же самий обсяг або ефект від пошкоджень, що виникають після виникнення чи застосування того ж самого НЕ в будь-якому місці всередині системи.

Детерміновані методи дослідження живучості засновані на співставленні конкретних видів факторів НЕ і стійкості елементів системи та системи в цілому. У цьому напрямку існують два підходи: статичний і динамічний.

Графоаналітичні моделі характеризуються простотою, високою надмірністю. Вони традиційно використовуються в дослідженнях структурної надійності, при цьому вводиться поняття «руйнування». Систему, яка представлена у вигляді графа можна розглядати як знищену, якщо після видалення з неї вершин, одержуємо граф, що відповідає одній або декільком з наступних умов:

- Граф містить, щонайменше, два компонента;
- Немає спрямованих шляхів для даної множини вершин;
- Кількість вершин в найбільшому сегменті G менше деякого заданого числа;
- Найкоротший шлях став довшим, ніж деяке задане значення.

Відповідно, система розглядається як живуча, тобто сервісна мережна система вважається доступною при відсутності виконання цих умов. Така сервісна мережна система формується на відповідних ребрах, представлених ESC (SaaS), що не є перевантаженими запитами користувачів.

Завдання оптимального структурно-параметричного синтезу хмарної SDP реалізації може бути розв'язане шляхом оптимального вибору заданих вище параметричних показників для кожного впровадженого комплексного сервісного застосування; з міркувань спрощення визначимо, що вектор

$x_{opt} = (\alpha, n, H)$ повинен максимізувати наступну систему співвідношень, яка використовується для математичної формалізації критеріїв синтезу:

$$\begin{cases} x_{opt} = \arg \max P_A \{X(x_{opt}, t) \in D_x, \forall t \in [0, T]\}, \\ x_{opt} = \arg \max_{x_{opt} \in D_x} S_p(x_{opt}). \end{cases} \quad (3.36)$$

Тут $X(x_{opt}, t)$ є ймовірнісним процесом зміни параметрів вектора x_{opt} , функціонал $P_A(\bullet)$ відображає сервісну доступність, а $S_p(x_{opt})$ є функціоналом структурної продуктивності. D_x - це область допустимих розв'язків для параметрів вектора x_{opt} , T - час тривалості експлуатації для поточної реалізації SDP. Визначимо область допустимих розв'язків:

$$D_x = \{x \in R^3 : P_{Amin} \leq P_A(x) \leq 1\} \quad (3.37)$$

Тут P_{Amin} є мінімально допустимим значенням сервісної доступності у синтезованій SDP (або її конкретному взятому сегменті при декомпозиції).

Розв'язок для завдання (3.36) базується на аналізі співвідношень сервісної доступності та параметрів ESC, а також статистичних параметрів сервісного навантаження, що представлені узагальненим параметром Херста. Перший та другий статистичні моменти навантаження, яке обслуговується відповідним сервісом також є необхідними для проведення нашого дослідження та подальшого моделювання. Ці параметри можуть бути одержані як результат статистичного моделювання інтенсивності навантаження (трафіку) з відповідним параметром H [131, 137]. Множина внутрішніх параметрів вектора $x_{opt} = (\alpha, n, H)$ може бути представлена як точка всередині R^3 куба, а простір допустимих параметрів вектора x_{opt} додатково обмежується областю допустимих розв'язків D_x .

3.4.2. Розрахунок критеріїв у оптимізаційній задачі структурно-параметричного синтезу сервісної мережної системи.

Маючи внутрішні параметри SDP, можемо визначити, що [149, P.100-101]:

$$P_A(\bullet) = \frac{1}{N_0} \sum_{i=1}^{N_0} P_i(x, t)(N_0 - i), \quad (3.38)$$

де $N_0 = N(N-1)/2$, а N є кількістю сервісних вузлів у SDP, які агрегують відповідні сервісні компоненти ESCs, та якими підтримують обробники (наприклад, обробники у SaaS реалізації, розгорнуті на VM у деякій PaaS реалізації). В процесі досліджень виявлено, що тривіального розв'язання поставленої математичної задачі немає, тому вона була розбита на часткові підзадачі з використанням адитивного ймовірнісного представлення сервісної доступності Додонова-Ланде [149]:

$$P_i(x, t) = \sum_{i=0}^{\alpha} G_i^{E2}(x, t) + \sum_{i=\alpha+1}^n G_i^{E1}(x, t) + \sum_{i=n+1}^N G_i^P(x, t), \quad (3.39)$$

відповідно, використовуючи визначення [150] потоків Ерланга i -го порядку з післядією маємо:

$$G_i^{E1}(x, t) = \frac{(i\Lambda_i^{E1}(x))^i}{(i-1)!} t^{i-1} e^{-i\Lambda_i^{E1}(x)t}, \quad (3.40)$$

відповідно $\Lambda_i^{E1}(x) = \frac{h_1(x)\pi_1}{i(n-\alpha)}$, а $h_1 = \lambda p_1(x)$, тут і далі π_1 є усередненим значенням доступності VM для кожної *розпаралеленої* комбінації ESC у деякому сервісному вузлі SDP. Визначимо рівняння Норроса шляхом його перетворень наступним чином [137]:

$$p_1(x) = e^{\left[\frac{(1-H)^{2H} H^{-2H} \left(2^{-\frac{1}{2H}} \left(c_v(n-\alpha)^{\frac{1}{2}} \right)^{-H/2} B^{\frac{1}{H}-1} (C-\lambda/(n-\alpha)) \left(\frac{\lambda}{n-\alpha} \right)^{-H/2} \right)^{2H}}{(H-1)^2} \right]};$$

тут B є коефіцієнтом утилізації буфера ESC у момент часу t , H - параметр Херста для відповідного типу трафіку, що характерний для сервісу, який ми

досліджуємо, C середня інтенсивність оброблення трафіку запитів у ESC, λ - інтенсивність трафіку запитів, c_v - коефіцієнт варіації вхідного трафіку, обидва ці показники стосуються типу трафіку, що характерний для сервісу, який ми досліджуємо. Таким чином, використовуючи визначення потоків Ерланга i -го порядку запишемо:

$$G_i^{E2}(x, t) = \frac{(i\Lambda_i^{E2}(x))^i}{(i-1)!} t^{i-1} e^{-i\Lambda_i^{E2}(x)t}, \quad (3.41)$$

де $\Lambda_i^{E2}(x) = \frac{h_2(x)\pi_2}{i}$, а $h_2 = \lambda p_2(x)$, відповідно тут і далі π_2 є усередненим значенням доступності VM для кожної *послідовної* комбінації ESC у деякому сервісному вузлі SDP. Визначимо, шляхом використання трансформованого рівняння Норроса, наступне [137]:

$$p_2(x) = e^{-\left[\frac{(1-H)^{2H} H^{-2H} \left(2^{-\frac{1}{2H}} c_v^{-H/2} B^{\frac{1}{H}-1} (C-\lambda) \lambda^{-H/2} \right)^{2H}}{(H-1)^2} \right]};$$

та, відповідно, використовуючи визначення пуассонівського потоку, маємо [150]:

$$G_i^P(x, t) = \frac{(\pi_3 \lambda p_2(x))^i t^i}{i!} e^{-\pi_3 \lambda p_2(x)t}, \quad (3.42)$$

де π_3 є усередненою (фізичною для випадку PaaS-IaaS інтерпретації моделі) доступністю VM (або сервера для випадку PaaS-IaaS інтерпретації) у кожному сервісному вузлі *транспортної мережної підсистеми* SDP.

Отже у (3.39) перший і другий члени відносяться до опису доступності послідовних і паралельних сервісних компонентів, відповідно, а третій – характеризує доступність транзитних VM SDP. Таким чином, кожен наведений компонент виразу (3.39) враховує ступінь регулярності потоків відмов системи, що відчутно зростає у її паралельних і, особливо, у транзитних сегментах, зокрема – випадків її недоступності при перевантаженнях ТКСП, а також інші функціональні параметри. З цього ж випливає, що потік відмов мережного

обладнання ТКСП, наприклад на фізичному рівні, є практично регулярним із дуже низькою інтенсивністю.

Використовуючи (3.39-3.42), визначаємо статистичні властивості сегмента сервісної мережної системи у *стаціонарному* режимі функціонування для заданої конфігурації ESC та, відповідно, розраховуємо критерій сервісної доступності (3.38) для кожної заданої структури сервісних компонентів VM (та для визначеного типу сервісу) в процесі синтезу хмарної SDP (для прикладу, як PaaS). Використовуючи той самий набір параметрів вектора $x_{opt} = (\alpha, n, H)$, що використовується у (3.38), одночасно визначаємо коефіцієнт системної продуктивності, як значення другого критерію синтезу згідно закону Амдала, див. рис. 3.33 [151, 26]:

$$S_p(x) = \frac{1}{\alpha + \frac{1-\alpha}{n}}. \quad (3.43)$$

Отже, можливо визначати коефіцієнт структурної продуктивності системи, використовуючи (3.43) для заданої структурної комбінації ESC, досягаючи, таким чином, того, що розв'язки завдання синтезу (3.36) будуть послідовно ітеративно наближатися до оптимальних, див. рис. 6.18-6.21, рис. 4.13-4.15.

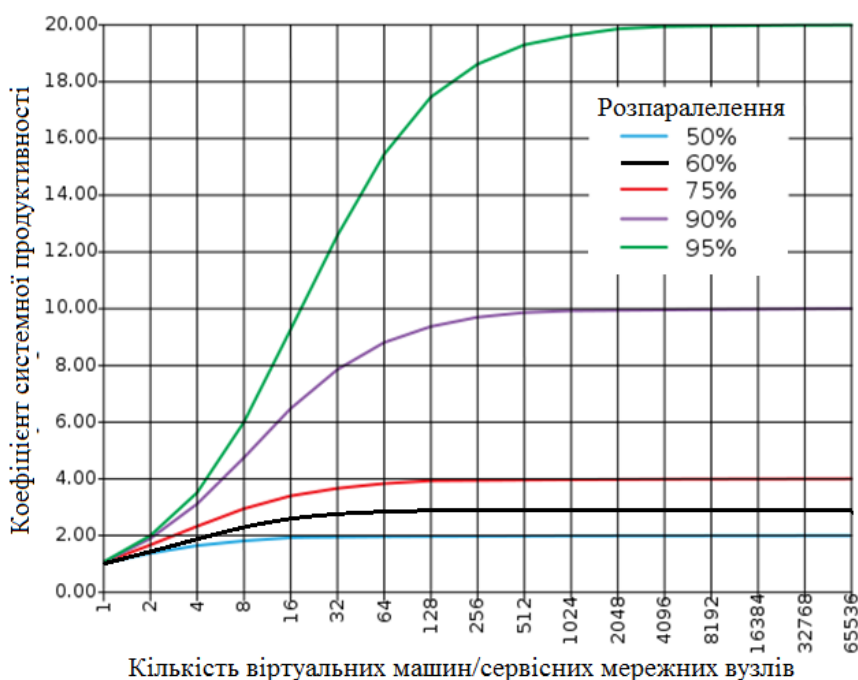


Рис. 3.33. Коефіцієнт системної продуктивності ТКСП (наприклад системи VM у PaaS модельній реалізації) відповідно до закону Амдала [151].

3.5. Висновки до 3-го розділу.

1. У даному розділі з використанням теорії відкритих мереж масового обслуговування Джексона і на базі побудованих структурно-параметричних та математичної моделей було досліджено найбільш поширені архітектури сервісних мережних платформ централізованої та розподіленої реалізації, як результат еволюції технологій інфокомунікаційних та інтелектуальних мереж, такий, що задовольняє вимогам відносно необхідних показників функціональності, швидкості розроблення сервісних компонентів та впровадження необхідних сервісів, а також продуктивності та ефективності масштабування. Проведено аналіз математичних підходів та моделі, які застосовуються для обчислення характеристик PaaS систем з відкритою сервісною архітектурою. Запропоновано шляхи оптимізації характеристик відкритих сервісних платформ та досліджено їх основні залежності при зміні вхідних параметрів. Виявлено, що середня тривалість оброблення вимог, які надходять на базовий сервер послуг (технології Parlay API), значно менше, ніж середня тривалість оброблення цих вимог єдиним фізичним сервером із віртуальними машинами в класичному сервісному вузлі (SN). Зменшення тривалості оброблення вимог в оптимізованій відкритій сервісній платформі складає від 3% у випадку найпростіших запитів до 10% при опрацюванні складних запитів. Середній виграш за системною продуктивністю, тобто за кількістю вимог, які перебувають на обробленні у сервісній платформі від застосування відкритої сервісної архітектури становить близько 17%, що свідчить про ефективність її застосування в умовах великих навантажень і масштабування для підтримки більшої кількості серверів послуг. Варто підкреслити, що сервісні інфокомунікаційні системи національного рівня повинні будуватися на основі сучасних телекомунікаційних платформ, з використанням високопродуктивних відкритих сервісних мережних архітектур.

2. Шляхом застосування структурно-функціонального моделювання виконано загальний аналіз загроз поширенню даних та функціональній стійкості у мультисервісних інфокомунікаційних системах, які реалізують

телекомунікаційну сервісну платформу національного сегменту глобальної інформаційної інфраструктури, зокрема в рамках реалізації концепції державного управління в інформаційному суспільстві – електронного урядування. Зазначені загрози визначено та класифіковано у вигляді множини можливих мережних атак гіпотетичного порушника. Охарактеризовано найбільш імовірні стратегії втручання в роботу захищених мультисервісних інфокомунікаційних систем. Запропоновано методичні рекомендації та визначено шляхи розроблення методології, що дозволить знизити вищезгадані ризики несанкціонованого доступу до захищеної інформації та порушення нормального функціонування мультисервісної інфокомунікаційної системи, а також визначено необхідність проведення подальших досліджень у галузі боротьби із навмисними перевантаженнями сервісної мережної інфраструктури та поширенням через неї небажаної інформації, що буде виконано у розділах 4.2-4.3 цієї дисертаційної роботи. Показано, що захищеність та функціональну стійкість сервісних мережних систем можна забезпечити тільки комбінацією технічних і організаційно-архітектурних методів та заходів із застосуванням додаткових технічних засобів захисту. Визначено загальний критерій ефективності захисту мультисервісних інфокомунікаційних систем в національному сегменті сервісної мережної інфраструктури. Подальше розроблення згаданих питань на основі наданих рекомендацій та підходів належить до галузі захисту інформації та лежить поза предметом дисертаційних досліджень.

3. Сучасні бізнес-процеси характеризуються широким використанням інформаційних технологій. Очевидно, що для їхньої реалізації використовують різноманітні програмні та апаратні рішення. Важливим компонентом при побудові сучасних сервісних мережних систем обслуговування є веб-сервіс. Завдяки своїй простоті, швидкості створення та незалежності від платформи і мови реалізації веб-сервіси можуть реалізувати складні бізнес-процеси, в яких беруть участь багато різних представників: як компанії, так і клієнти. У процесі інтенсивного розвитку електронної комерції розподілені системи на основі веб-

сервісів доцільно створювати відповідно до сервісно-орієнтованої архітектури. При великій кількості веб-сервісів, які беруть участь в обслуговуванні клієнта, постає питання забезпечення якості обслуговування клієнта. Для підтримання належного рівня якості обслуговування використовується брокер, який забезпечує маршрутизацію запитів, вибираючи оптимальний шлях за критерієм найвищого рівня якості обслуговування. У роботі запропоновано використовувати метод поліваріантного доступу для збільшення пропускної здатності веб-сервісу, що стає можливим завдяки його реплікації. Використовуючи метод поліваріантного доступу, брокер за допомогою алгоритмів маршрутизації запитів між сервісними вузлами зможе здійснювати динамічне балансування навантаження та підтримувати якість обслуговування клієнтів на високому рівні. Як результат, власник веб-сервісу забезпечить високий рівень якості обслуговування, підвищить ефективність, зокрема продуктивність сервісної мережної платформи, збереже своїх клієнтів і посилить позиції на ринку.

4. В даному розділі дисертаційної роботи проведено статистичне дослідження мультисервісного навантаження в гетерогенній корпоративній телекомунікаційній системі з метою аналізу показників його самоподібності для конкретних типів трафіку. Це, в свою чергу дозволить створювати та використовувати адекватні статистичні моделі для моделювання процесів передавання та оброблення інформаційних потоків, що відповідають заданим типам сервісу в гетерогенних сервісних мережних системах, застосовуючи їх усереднені статистичні параметри. Отримані результати дослідження допоможуть оцінити ефективність застосування спроектованої сервісної мережної системи для передавання мультисервісних даних заданого виду, виявити потенційні вузькі місця в гетерогенній хмарній системі з метою її модернізації та оптимізації, зокрема за критеріями системної продуктивності та сервісної доступності, сформулювати пропозиції щодо зміни топологій та архітектури різних сервісних шарів-моделей ХааS, в тому числі – програмної архітектури активного агрегуючого обладнання в рамках перспективної

реалізації NFV концепції та CBN; вони сприятимуть введенню в експлуатацію нових мережних технологій, а також дозволять покращити параметри мультисервісної мережної системи при мінімальних економічних затратах інфокомунікаційних сервіс-провайдерів.

5. У даному розділі дисертаційної роботи запропоновано критерії та обмеження для оптимального структурно-параметричного синтезу розподілених сервісних платформ на основі хмарних сервісно-орієнтованих архітектур, а саме – за сервісною доступністю та показником системної продуктивності шляхом розв’язання кількох взаємопов’язаних імовірнісно-статистичних задач. Запропонований метод синтезу дозволяє враховувати тип сервісного навантаження, поданий у статистико-аналітичній формі (інтенсивність, коефіцієнт варіації, параметр самоподібності Херста) для кожного комплексного сервісу, який потребує реалізації в рамках сервісної платформи, що синтезується, шляхом підбору структури її віртуальних машин комбінуванням розпаралелених та послідовних елементарних сервісних компонентів згідно заданої функціональності найбільш оптимальним чином. Із урахуванням результатів проведеного аналізу, відповідно до закону Амдала впливає доцільність архітектурної кластеризації сервісних мережних платформ, з метою спрощення широкосмугового доступу потоків навантаження (та управління ними) до віртуальних машин PaaS та, в загальному, внутрішньої структури хмарної сервісної системи, підтримуючи на заданому рівні загальну системну продуктивність.

Використано термін «структурний параметр (сервісної мережної системи)» для означення кількісної структури елементарних сервісних компонентів (в рамках сервісної платформи деякого концептуального рівня або сервісного застосування) оптимально зкомпонованих у структурі віртуальних машин (або віртуалізованих мережних елементів), адже для опису структури хмарних сервісних систем неможливо застосувати типові топологічні чи архітектурні шаблони, а якщо це і можливо, то такі шаблони будуть надто узагальненими, нечітко заданими, значно відрізняючись при спробах формалізації у термінах

звичайних мережних систем різного виду. Також застосовано термін «функціональний параметр (сервісної мережної системи)»: мається на увазі попередньо експериментально (статистично) визначений та розрахований параметр Херста для відповідного типу сервісного навантаження, що має обслуговуватися хмарною сервісною платформою в рамках SOA. Також для цього навантаження враховуються його інтенсивність та коефіцієнт варіації.

В цілому, запропоновані підходи дозволяють математично-обґрунтовано і алгоритмічно-орієнтовано описати процес структурно-параметричного синтезу ефективних розподілених сервісних платформ, а у процесі їх налаштування і експлуатації забезпечують можливість їх функціонування, як оптимального за сервісною доступністю та системною продуктивністю динамічного середовища з точки зору підтримки повноти спектру послуг і надійного оброблення пульсуючого навантаження мігруючих користувачів.

6. Запропоновані підходи більшою мірою стосуються опису квазістаціонарного або усталеного режиму функціонування телекомунікаційної сервісної платформи, проте, у разі застосування методів її динамічної оптимізації, для прикладу, будь-які збурення вхідного навантаження автоматично будуть приводити до його перерозподілу та, за потреби, можливого масштабування сервісної платформи в межах існуючих ресурсів. Питання моделювання показників сервісної доступності та дослідження ефективності масштабування сервісних мережних платформ винесені у наступний 4-ий розділ дисертаційної роботи.

РОЗДІЛ 4

Розроблення та моделювання процесів забезпечення функціональної стійкості телекомунікаційних сервісних платформ

4.1. Дослідження характеристик продуктивності та сервісної доступності розподілених сервісних мережних платформ у процесі їх структурно-параметричного синтезу.

Сучасна парадигма організації інфокомунікаційних систем для надання електронних сервісів передбачає поступову трансформацію традиційного підходу до побудови захищених приватних мереж, а також управління ними на основі використання загальнодоступних телекомунікаційних ресурсів. Очевидно, що активна участь у такому процесі приватних мережних операторів забезпечує утворення глобальної хмарної обчислювальної інфраструктури, серед якої необхідно виокремлювати її національні сегменти. Зазвичай у хмарному мережному середовищі традиційні функції та послуги, наприклад зв'язність (мережна доступність), безпека, мережне управління та моніторинг представляють у якості його невід'ємних сервісів, тобто сервісів самої хмарної інфокомунікаційної платформи. На сьогоднішній день відбуваються трансформації в хмарних мережних системах у рамках переходу від процесу мережної конвергенції та утворення сегментів виду Cloud-Enabled Networking (CEN) до єдиного мережного середовища Cloud-Based Networking (CBN). Перша категорія інфокомунікаційних систем CEN – переносить аспекти мережного управління, зокрема визначення функціональних політик безпеки та ін., в «хмару», проте залишає підтримування мережної доступності обладнання телекомунікаційної системи, потоковий менеджмент (маршрутизацію, комутацію та безпеку інформаційних потоків) на локальному рівні, як правило, реалізуючи ці функції апаратно, як у більшості сучасного мережного обладнання.

Впровадження сучасних широкосмугових мережних сервісів та, зокрема, концепції Internet of Things (IoT) значно змінює кут зору на сервіси та

інфраструктуру сервісних мережних систем, зміщуючи усі мережні функції адресації та управління потоками до сфери впливу хмарного середовища, нівелюючи потреби у локальному мережному обладнанні, що не є програмно-конфігурованим (SDN), або ж безпосередньо не забезпечує з'єднання з мережами зв'язку (Internet'ом). Дана категорія інфокомунікаційних систем - CBN зазнала розвитку в діяльності таких компаній, як Petrino та Aryaka [152, 153]. Пропонується визначення Network-as-a-Service (NaaS) для узагальнення наведених властивостей CBN інфокомунікаційних систем [154]. В роботах [155-158] розглядаються підходи до організації CEN систем, зокрема в частині оптимізації роботи відповідного телекомунікаційного обладнання. Концепції SDN, віртуалізації мережних функцій, як розподілених платформ, так і елементів сервісної мережної інфраструктури є базисом для опису та досліджень CBN сервісних систем [159]. В роботах [65, 160] виконані структурно-параметричні дослідження хмарних сервісних систем і отримані аналітичні залежності основних показників їх функціонування, а також якості сервісу (як деякої функції від джитера, часу затримки пакетів, пропускну здатності системи, ймовірності втрати пакетів). З метою виявлення можливостей покращення якості сервісу за рахунок підвищення показників доступності телекомунікаційних вузлів хмарної платформи на основі пропозицій [161] в дисертаційній роботі в розділі 5.1 промодельовано застосування запропонованого методу динамічної корекції маршрутних метрик шляхом наскрізного структурного трасування в масштабованих сервісних мережних системах. Для виконання синтезу ефективних систем надання електронних сервісів за критерієм сервісної доступності (яка враховує у собі показники надійності та живучості, а також інтегральної QoS), необхідно якісно дослідити числові характеристики доступності у хмарних сервісних системах. Для моделювання цих характеристик у даній роботі використано результати та функціональні залежності, що отримані в розділі 3.4 цієї дисертації [26]. Поєднання ж результатів, які пропонуються в даному розділі, робить можливим оцінювання альтернативних підходів щодо побудови сегментів хмарних

сервісних систем із необхідними параметрами для ефективного опрацювання стратегій їх розвитку та вдосконалення.

Метою даного розділу роботи є моделювання сервісної доступності хмарних сервісних систем для різних їх конфігурацій, характеристик трафіку та режимів роботи та дослідження ефективності їхмасштабування, а у розділі 5.2 цієї дисертаційної роботи подано результати оцінювання ефективності застосування запропонованого методу підвищення показників доступності вузлів хмарної мережної платформи.

4.1.1. Аналіз результатів моделювання функціональних характеристик масштабованих хмарних сервісних платформ

Структурно-функціональна цілісність сучасної парадигми хмарних мережних обчислень є важливою для побудови масштабованих та надійних сервісних платформ із використанням сервісно-орієнтованої архітектури (SOA). Існує багато застосувань, які використовують дану архітектурну концепцію для того, щоб стати ефективнішими у світі, де більших бізнес-процесів є паралельними: електронний бізнес, електронна комерція, персональний зв'язок та інші [65, 132-133] і подібні мережні концепти останніми роками набувають все більшого поширення. Внаслідок високої складності проектування, а також високої комерційної вартості таких мережних рішень в [26] автором було розроблено аналітичний метод синтезу з метою оптимізації структурних та функціональних параметрів із заданими обмеженнями для типових хмарних платформ надання сервісів (SDP).

Очевидно, що хмарні сервісні системи на сьогодні набули широкого поширення на ринку, роблячи електронний бізнес більш ефективним та масштабованим [132-133]. Найбільш відомими на ринку інфокомунікаційних систем є рішення від Microsoft (Microsoft Azure), Google (Google Apps Engine), Amazon (Elastic CloudComputing, Simple Storage Service), IBM (Blue Cloud), Nimbus, Oracle та інші (типовий приклад – див. рис. 3.31). Окрім великих корпоративних хмарних систем, хмарні обчислювальні сервіси надаються

також невеликими інфокомунікаційними операторами. Існують доступні або безкоштовні хмарні рішення, такі як iCloud, Cloudo, FreeZoho, SalesForce тощо. Всі вони відрізняються за переліком послуг, які ними пропонуються, а також – за типом (моделлю) сервісу, що ними надається: SaaS (software as a service – програмне забезпечення, як сервіс), PaaS (platform as a service – платформа, як сервіс), та IaaS (infrastructure as a service – інфраструктура, як сервіс). Для випадку завершеної трансформації інфраструктури від CEN до CBN парадигми, виділяють також HaaS (hardware as a service – обладнання, як сервіс). Незважаючи на різноманіття сервісів (котрі в загальному називають XaaS), існує кілька типових апаратних та програмних засобів, які використовуються в якості базису для побудови хмарних систем. Вони забезпечують функціонування системи, що побудована на основі SOA архітектури, будучи реалізованою, як множина віртуалізованих сервісних вузлів або віртуальних машин, що реплікуються задля масштабування та підтримки деякої множини електронних сервісів із гнучкістю та у відповідності до користувацьких потреб.

Апаратні та програмні засоби хмарної обчислювальної платформи часом можуть функціонувати нестабільно або ненадійно внаслідок своєї фізичної деградації або недосконалості, за деякими статистичними законами. Для мінімізації такої ймовірності і зменшення часу відновлення нормального процесу надання сервісів у хмарному обчислювальному середовищі необхідно застосовувати спеціальні принципи, більшість з яких є характерними для реалізації процесів розподіленого оброблення даних (резервування, паралелізація, перерозподіл обчислювальних ресурсів тощо).

Описані підходи націлені на часткове приховування від користувачів реальної ситуації щодо системної доступності з метою створення ілюзії безвідмовного функціонування розподіленої сервісної платформи. Незважаючи на це, існує статистика відмов хмарних платформ надання сервісів [162]. Вона свідчить, що можливі ситуації, коли використані у SDP рішення для забезпечення високої сервісної доступності стають неефективними. Аналізуючи глибше, можна також відмітити, що системна недоступність може

бути не єдиним наслідком відмов хмарних систем. У випадку відмови Microsoft Sidekick були втрачені персональні дані користувачів, які були згодом відновлені, але не повною мірою [162].

Незважаючи на високий рівень реалізації загальновідомих рішень для підвищення доступності в сервісних мережних системах, на сьогоднішній день хмарні системи все ще піддаються аналізу на вузькі місця в їх SOA, з метою підвищення надійності їх роботи, рівня сервісної доступності, системної продуктивності [2, 139]. Можна стверджувати, що актуальність досліджень за даною тематикою є доволі високою.

Отже, з метою виконання моделювання сервісної доступності в масштабованих хмарних сервісних мережах, визначимо в якості терміну «структурні параметри» кількісні показники щодо системи елементарних сервісних компонентів, які деяким чином сконфігуровані у структурі віртуальних машин на вузлах телекомунікаційної хмарної платформи. При цьому структура мережних з'єднань та фізична топологія мережі визначені нечітко, що є притаманним для хмарних систем, відрізняючи їх від традиційних мережних архітектур. В загальному, топологічна конфігурація віртуальних машин є динамічно-змінною, так само як і конфігурація пропонованої та запитуваної множини сервісів. Віртуальні машини мігрують та реплікують елементарні сервіси, як компоненти комплексних аплікацій (сервісних застосувань) у відповідності до розподілу запитів користувачів у системі. Тобто, сервісно-орієнтована архітектура (SOA) володіє сукупністю мігруючих ресурсів різного рівня всередині хмарної системи, яка є надзвичайно складним розподіленим об'єктом, утворюючи конкретну реалізацію платформи надання сервісів (SDP). Ми можемо виділити специфічні групи сервісних компонентів, що використовуються у процесі оркестрації, за рахунок якого комплексне застосування може бути використане користувачами SDP. Класифікація сервісних компонентів, як «тредів» або потоків, що реалізуються віртуальними машинами може бути прийнята у відповідності до визначень закону Амдала [151]. Таким чином, для нашої інтегральної моделі, яка описує стаціонарний

режим функціонування сервісної мережної системи, ми можемо виділити гіпервізори та інші послідовні за характером функціонування елементарні сервісні компоненти (ESC) сукупності сервісних застосувань (α) в одну групу, а також ESC, які функціонують, обслуговуючи потоки запитів паралельно – в іншу ($\eta = n - \alpha$), див рис. 3.32. Тут n - відображає загальну кількість елементарних сервісних компонентів.

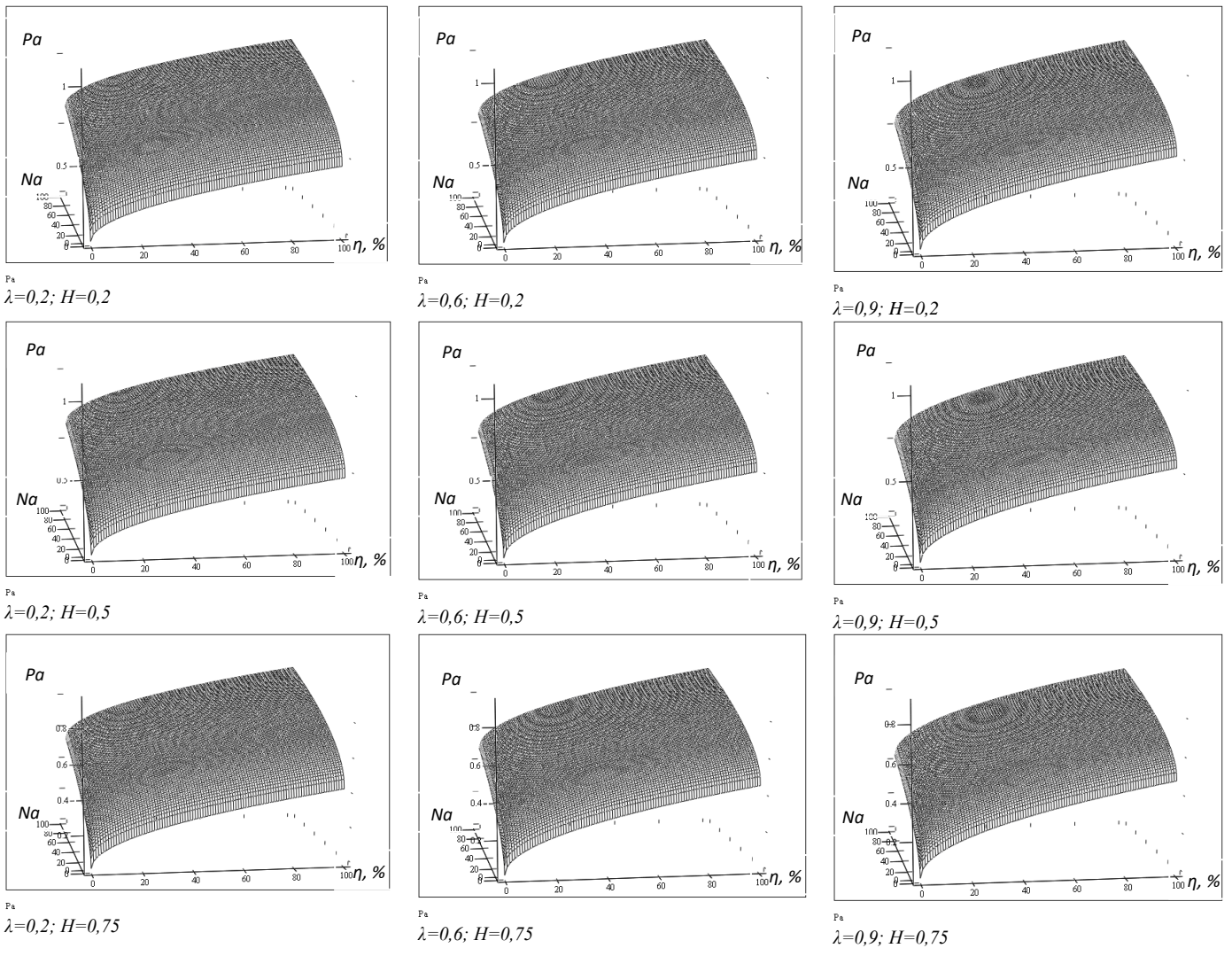
Таким чином, враховуючи нечітко задану та динамічно-змінну структуру хмарної мережної системи, задача її оптимального структурно-параметричного синтезу може бути зведена до вибору оптимального співвідношення кількості сервісних компонентів, які відносяться до різних визначених груп в рамках їх комбінованого поєднання при утворенні та вибудовуванні комплексних застосувань різного рівня у сервісно-орієнтованій архітектурі. На жаль, основні труднощі, що пов'язані з вирішенням цієї задачі вносяться браком досліджень щодо ймовірнісних процесів обслуговування трафіку розподіленими сервісними застосуваннями в системному аспекті, за умов варіації навантаження на SDP, що генерується запитами користувачів до сервісів різного виду [139, 160]. Функціональні властивості сервісів повинні розглядатись в термінах стохастичних процесів, враховуючи їх пряму залежність від статистичних властивостей навантаження, що обслуговується. Для характеризування статистичних особливостей трафіку навантаження на хмарну систему можна використати параметр самоподібності Херста. Відповідно, у розділі 3.3 цієї дисертації [131] визначено специфічні особливості таких типів трафіку, як VoIP, VoD, IPTV Multicast, Web-дані тощо. Отже, визначимо поняття «функціонального параметра» для відповідного виду сервісу, що має бути обслужений в хмарній платформі із SOA, як попередньо статистично визначеного та розрахованого параметра Херста, що відповідає специфічному для цього сервісу типу трафіку. Також враховуються інтенсивність навантаження та відповідний коефіцієнт варіації.

Отже, для кожної синтезованої реалізації хмарної архітектури відповідний показник узагальненої сервісної доступності може бути представлений та

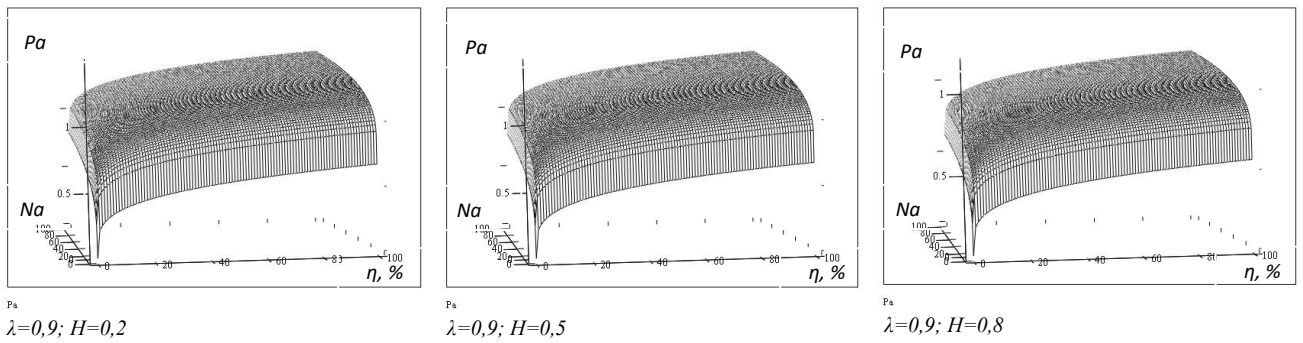
розрахований для кожного функціонального виду сервісу, що пропонується SDP, так само, як і показник відносної системної продуктивності рис. 3.33 для заданої структурної реалізації (комбінації) елементарних сервісних компонентів. Обидві зазначені показники обрані автором у якості критеріїв для оптимального структурного та функціонального синтезу платформ надання сервісів [26, 152, 223].

Далі наведемо результати моделювання сервісної доступності в масштабованій хмарній сервісній платформі, що виконане на основі чисельних розрахунків та апроксимації розв'язків аналітичних залежностей роботи [26] (рис. 4.1 а, б). Робимо припущення, що для випадку моделювання, результати якого представлено на рис. 4.1 а, реалізація обраного сервісного шару хмарної платформи відбувається без оптимального розподілу обробників навантаження сервісних потоків (міграції віртуальних машин PaaS або ESC SaaS); випадок, коли розподіл обробників навантаження сервісних потоків може бути адаптивно скоректований, у разі потреби, міграцією віртуальних машин або ESC [135], представлено на рис. 4.1 б. Процеси мірації віртуальних машин у сервісних мережних системах докладніше буде розглянуто у розділі 4.5 цієї дисертаційної роботи.

На рис. 4.1 а представлено випадок неоптимального конфігурування ресурсів хмарної мережної платформи (для прикладу, необхідний ресурс для обслуговування комплексних застосувань SaaS перевищує доступні ресурси віртуальних машин у вузлах сервісної мережної системи PaaS, що підтримують відповідні елементарні сервісні компоненти). Параметри навантаження λ (відносно до максимально можливого у %) та значення параметру Херста H для агрегованого вхідного трафіку вказані під відповідними залежностями. P_a – узагальнена сервісна доступність хмарної мережної платформи; η – частка ESC, які функціонують, обслуговуюючи потоки запитів паралельно, у відсотках; N_a – кількість сервісних вузлів у хмарній мережній платформі.



a)



б)

Рис. 4.1. Результати моделювання сервісної доступності в масштабованій хмарній сервісній платформі [152, 223].

На рис. 4.1 б представлено випадок адаптивного конфігурування ресурсів хмарної мережної платформи міграцією віртуальних машин (необхідний ресурс для обслуговування комплексних застосувань SaaS приблизно відповідає

доступним ресурсам віртуальних машин у вузлах сервісної мережної системи PaaS, що підтримують потрібну конфігурацію елементарних сервісних компонентів). Параметри навантаження λ (відносно до максимально можливого у %) та значення параметру Херста H для агрегованого вхідного трафіку вказані під відповідними залежностями. Pa – узагальнена сервісна доступність хмарної мережної платформи; η – частка ESC, які функціонують, обслуговуючи потоки запитів паралельно, у відсотках; Na – кількість сервісних вузлів у хмарній мережній платформі.

Аналізуючи результати, що подані на рис. 4.1 а та рис. 4.1 б, можна зробити висновок про закономірне поступове зниження сервісної доступності в хмарній мережній системі при зростанні навантаження до максимального, причому воно відбувається повільніше у реалізаціях системи, де частка паралельних елементарних сервісних компонентів, які функціонують, обслуговуючи потоки запитів, переважає над часткою послідовних. При більшій кількості сервісних вузлів у хмарній платформі, за умови збільшення частки розпаралелених елементарних сервісних компонентів, сервісна доступність зростає швидше. За її показниками, отриманими в процесі моделювання визначено, що в якості оптимального співвідношення η/α можна прийняти $60/40$. Вплив показника Херста на сервісну доступність якісно проявляється при його високих значеннях, вказуючи на те, що самоподібний трафік відчутно знижує її. Відтак, на рис.4.1 а видно, що в умовах дефіциту ресурсів або неоптимального конфігурування хмарної сервісної платформи, для *самоподібного* трафіку можливе погіршення даного показника в середньому від 15 % при $\lambda=0,2$ до 30% при $\lambda=0,9$. За умов застосування адаптивного конфігурування ресурсів хмарної мережної платформи з міграцією віртуальних машин (наприклад, в рамках оптимальної реалізації моделі PaaS), подібне зниження сервісної доступності не перевищить 5-10% (див. рис. 4.1 б), а при кількості сервісних вузлів більше 40 – стає невідчутним. Тобто, очікуваний ефект від оптимізації, або ж розбудовування архітектури сервісних мережних систем згідно моделі PaaS на основі деякої IaaS становить від 10 до 20%.

Відмітимо, що високими показниками самоподібності володіє трафік сервісів генерування інтернет даних (нереального часу) – $H \cong 0,685$, IP-телефонії – $H \cong 0,981$, відео за запитом (VoD) – $H \cong 0,608$, передавання службових даних – $H \cong 0,719$ [131, табл. 5].

Отже, в даному розділі виконано чисельне дослідження сервісної доступності розподіленої сервісної платформи, що працює у *стаціонарному* режимі. На основі одержаних результатів можливо виконувати ефективний синтез конфігурацій масштабованих хмарних сервісних систем із урахуванням типу та величини навантаження, що потребує обслуговування в рамках вибудовування відповідного сервісу з комбінуванням паралельних та послідовних елементарних сервісних компонентів задля досягнення найкращих показників продуктивності та системної працездатності (рівня сервісної доступності).

З урахуванням закону Амдала (рис. 3.33, крива 60% паралельності обробників) можна також постулювати, що кластеризація хмарних систем може досягати найбільшої ефективності для масштабу кластера близько 100 сервісних вузлів, що узгоджується з результатами моделювання сервісної доступності розподіленої сервісної платформи (рис. 4.1). Проте, збільшення розміру кластера хмарної платформи призведе до необхідності вдосконалення методів управління потоками, зокрема застосування модифікованих методів підвищення доступності її телекомунікаційних вузлів, наприклад шляхом структурно-генного динамічного балансування (див. розділ 5.1). Одержане композиційне співвідношення (55-65% паралельності обробників) також підтверджується результатами моделювання проф. Богатирьова В.А. у роботі [222] для випадку мінімізації часу перебування запиту у мережній системі.

Як правило, перехід між рівнями IaaS та PaaS, а також між рівнями PaaS та SaaS якісно змінює показники функціонування сервісної мережної ситеми в бік покращення, в тому числі – в умовах її масштабування. Кожна нова мережна реалізація вищого рівня (сервісна надбудова) є покращеною або оптимізованою версією відповідної нижче розташованої мережної платформи.

На базі розгляду запропонованих у розділі рішень, які відповідають заданим обмеженням щодо допустимості розв'язків системи критеріїв оптимального структурно-параметричного синтезу, а саме, приймаючи до уваги застосування закону Амдала для опису системної продуктивності з одної сторони, а також результати моделювання змін сервісної доступності системи розпаралелених сервісних обробників з іншої сторони, можливо прийти до висновків, що досягається підвищення ефективності реалізацій IaaS, PaaS та SaaS сервісних архітектурних моделей за вищезгаданими критеріями для заданого набору вхідних параметрів навантаження, з урахуванням можливостей застосування сучасного NFV підходу.

4.2. Аналіз сучасних підходів до виявлення та запобігання функціональним втручанням у розподілені мережні системи.

Починаючи з 2010-х років, розроблення сучасних телекомунікаційних засобів, таких як мережні екрани, а також підходів до підтримки функціональної стійкості сервісних мережних систем, які базуються на подібних засобах (виявлення та запобігання функціональним втручанням), послідовно переходить у русло створення сервісних систем, що орієнтовані на виявлення подібних втручань і підвищення рівня власної функціональної стійкості, безпечності мережних сегментів, особливо національного значення та стратегічного призначення [17, 189]. У загальному, периметри безпеки сучасних сервісних мережних систем представлено на рис. 4.2. Виділено: зовнішній мережний екран, системи мережної безпеки та безпеки даних користувачів, внутрішній мережний екран VPN (приватних сервісних мережних сегментів).

Підсистеми мережних екранів і виявлення функціональних втручань, як правило, об'єднують у мережні сегменти, що функціонують окремо (наприклад за технологіями LAN, WLAN, 2G-4G, LTE, NFC та Bluetooth) з можливістю взаємодії для покращення запобігання спробам зниження їх функціональної стійкості, що можуть бути як зовнішнього, так і внутрішнього походження.

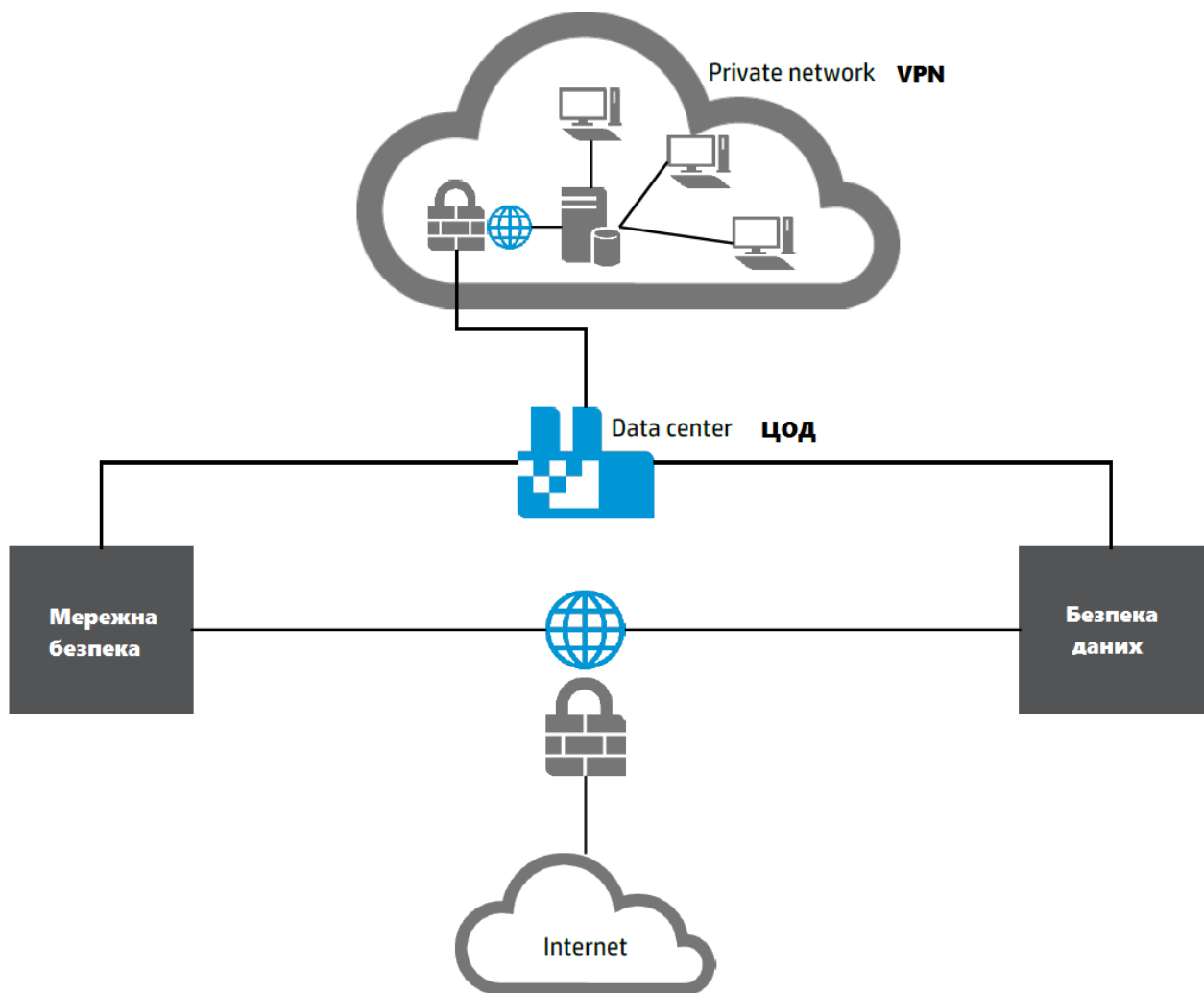


Рис. 4.2. Периметри безпеки сервісних мережних систем.

4.2.1. Особливості застосування мережних екранів.

Публічно доступні види сервісів (Web-сервери, FTP-сервери, файлообмінні платформи, веб-сервіси тощо) зазвичай розміщуються у так званій демілітаризованій зоні (DMZ) за активними мережними екранами. Демілітаризована зона (DMZ) — технологія забезпечення захисту інформаційного периметра мережної системи, при якій сервери, що відповідають на запити з внутрішньої мережі, знаходяться в особливому сегменті мережі (який і називається DMZ) та обмежені у доступі до основних сегментів мережі за допомогою мережного екрану, з метою мінімізувати негативний ефект при зламі одного з загальнодоступних сервісів, що

знаходяться в DMZ [66, 188]. Можливо розглядати різну функціональність мережних екранів за рівнями моделі ISO/OSI (див. рис. 4.3):

- PF – Packet Filters – Фільтрування пакетів (мережний рівень 3);
- CR - Circuit Relay – Фільтрування каналів (транспортний рівень 4);
- AG - Application Gateway – Шлюз застосувань (рівні 5-7 ISO/OSI).

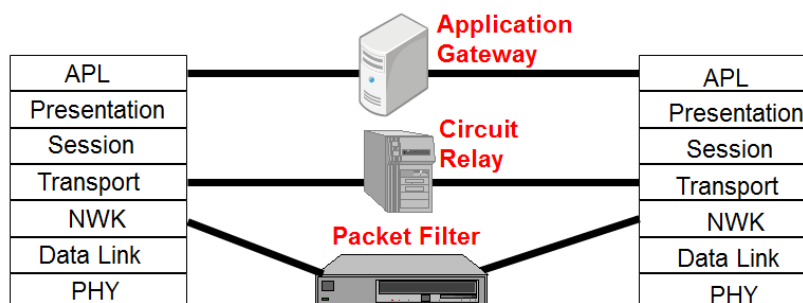


Рис. 4.3. Мережні екрани: особливості застосування на різних рівнях ISO/OSI.

Підсистема мережних екранів із множиною внутрішніх інтерфейсів у рамках DMZ сервісної мережної системи з підтримкою кількох публічних сервісів представлена на рис. 4.4.

Її основним завданням є блокування спроб порушення функціональної стійкості сервісних мережних систем на основі несанкціонованого доступу до VPN із використанням IP-адресації (PF, Фільтрування пакетів), TCP/IP-з'єднань для передавання потоків інформації (CR, Фільтрування каналів) або інформації, що передається в рамках взаємодії рівнів моделі ISO/OSI вище сеансового, тобто пов'язаної із сервісними застосуваннями (AG, Шлюз застосувань).

4.2.2. Порівняльний аналіз рівнів функціональності мережних екранів.

Як вже було зазначено, доступна функціональність мережних екранів може бути поділеною на такі концептуальні рівні: (PF, Фільтрування пакетів), (CR, Фільтрування каналів) та (AG, Шлюз застосувань). Інтегрована функціональність забезпечується гібридними концепціями мережних екранів, а саме, для прикладу, SIF – Stateful Inspection Firewall (технологія інспектування пакетів зі збереженням стану для перевірки вхідного навантаження на коректність) [163] від компанії Check Point Software Technologies.

Концепції виду PF та CR є доволі простими та ефективними у застосуванні. Концепція шлюзу застосувань (AG) або мережний екран прикладного рівня ISO/OSI, привносить більш вагомі переваги від застосування фільтрування навантаження: добре розпізнаються та аналізуються інформаційні потоки деяких застосувань, які утворені за такими мережними протоколами, як VPN, DNS, FTP, SMTP, POP3/IMAP, HTTP так само, як і їхніми безпечними версіями, наприклад HTTPS, SSH тощо. Для забезпечення можливості застосування технології Cloud Access Monitoring щодо віртуалізованих кластерів або сегментів сервісних мережних систем, власне мережних платформ, а також СУБД (VLAN, SAN/NAS) та сервісних вузлів (VMs, RAICs), так само як і тих, що реалізуються на основі SDN технології, застосовуються відповідні спеціалізовані типи мережних екранів.

Отже, починаючи з 2010-х років, впроваджується нове покоління мережних екранів на основі шлюзів застосувань. Це покоління передбачає більш глибоку та детальну перевірку інформаційних потоків на рівні протоколів прикладного рівня та базується на основі традиційних SIF рішень. Існуючі системи глибокого аналізу змісту пакетів можуть бути поділені на системи виявлення функціональних втручань, системи запобігання функціональним втручанням, системи з розширеною інтеграцією ідентифікаторів користувачів (ідентифікатор користувача прикріплюється до IP або MAC адреси з метою встановлення рівня загрози).

Окремим типом мережних екранів нового покоління є так звані Web Application Firewall (WAF). Захист відносно атак на подібні мережні екрани був докладно проаналізований та застосований у сервісному застосуванні "WAF Fingerprinting utilizing timing side channels" (WAFFle) [66, 163-165].

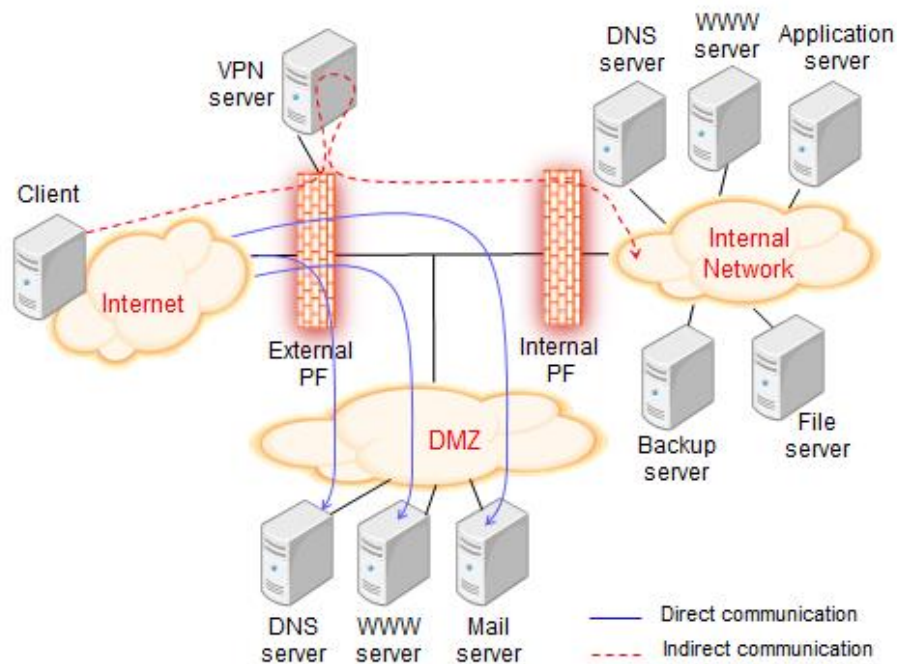


Рис. 4.4. Приклад сервісної мережної системи, що забезпечена від функціональних втручань застосуванням мережних екранів і підтримує мережні сервіси в рамках DMZ.

Для кращого розуміння варто зазначити: сучасний мережний екран є системним засобом безпеки, що захищає сервісний вузол мережної платформи, сукупність таких вузлів, або мережних підсистем від деструктивних впливів на функціональну стійкість, які виникають через спроби незаконного проникнення в інформаційні системи або небажану інформаційну активність. Проте, функціональність мережних екранів не є прямо орієнтованою на визначення зовнішніх мережних атак. У класичному розумінні, мережний екран використовує лише окремо взяті правила фільтрації навантаження при мережній комунікації. З метою визначення різних видів мережних атак використовуються певні модифікації модулів систем виявлення функціональних втручань і/або систем запобігання функціональним втручанням, які можуть також виступати засобами керування для відомих рішень на основі мережних екранів. Системи виявлення функціональних втручань спрямовані на підвищення рівня мережної безпеки, а системи запобігання функціональним втручанням є вдосконаленою версією попередніх і

спрямовані на підтримання функціональної стабільності мережних платформ у випадку виявлення негативних зовнішніх або внутрішніх втручань у їх роботу.

Таким чином, названі системи можуть виконувати роль модифікованих мережних екранів або, відповідно, бути окремими системними модулями, що працюють на досягнення поставлених безпекових завдань. Наступною модифікацією мережних екранів стало їх поєднання на основі SIF технології. Одержуємо мережні екрани виду SMLIF (Stateful Multilayer Inspection Firewalls). На думку фахівців відомої компанії Gartner Inc. (засн. 1979 року) перелік найбільш популярних SMLIF рішень можна представити наступним чином: AhnLab; Barracuda Networks; Check Point Software Technologies; Cisco; Dell SonicWALL; F5; Fortinet; Hillstone Networks; HP; Huawei; Intel Security (McAfee); Juniper Networks; Palo Alto Networks; Sangfor; Sophos; Stormshield; WatchGuard [164, 165].

Наведені рішення можуть застосовуватись у сервісних мережних системах при міжрівневій взаємодії та забезпечують їм непогану функціональну стійкість за допомогою застосування комбінованих правил фільтрації навантаження.

4.2.3. Технології подолання мережних екранів.

Advanced Evasion Technologies (AET) - технології подолання мережних екранів, які можуть наносити шкоду функціонуванню сервісної мережної системи безслідно та цілком анонімно. Таким чином, AET представляють собою нові виклики для мережної безпеки. На відміну від відомих методів втручання у роботу сервісних мережних платформ, AET поєднують і змінюють методи маскуванню під час мережних атак або від небажаного для системи безпеки (мережних екранів) коду. Такі підходи дозволяють проникати в захищену мережу без фіксації самого факту проникнення. Відповідно до сучасних оцінок, на сьогодні існує близько 2^{180} потенційних комбінацій методів класу AET. Це передбачає, зокрема, проникнення у мережну систему одночасно і узгоджено на кількох рівнях моделі ISO/OSI.

Насправді, відповідні системи запобігання функціональним втручанням Really IPS або Advanced Evasion Firewalls представляють собою доволі ефективні технології для боротьби з АЕТ. Вони передбачають комбінування шаблонів небажаної мережної активності одночасно на кількох рівнях моделі ISO/OSI, прикладом є АЕТ-Platform від Stonesoft: <http://evader.stonesoft.com>. Даний вид систем запобігання функціональним втручанням забезпечує комбінований захист: власне системою запобігання функціональним втручанням, антивірусами, мережними екранами, DMZ, зонуванням сервісної мережної системи (на захищені домени або сегменти). Впровадження подібних засобів є виправданим для великих компаній з розповсюдженою мережею структурних підрозділів та відділень.

Деякі з шаблонів небажаної мережної активності та пробування функціональної стійкості є наступними:

- На рівнях ISO/OSI 3, 4: перш за все відслідковуються можливості мережних атак на протоколи IP, TCP, UDP;

- На рівнях ISO/OSI 5-7: Протоколи прикладного рівня, такі як SMB та RPC є досить захищеними. Тому, по-друге, проводиться оцінювання внутрішніх загроз (див. розділ 3.2 цієї дисертаційної роботи);

- Після цього АЕТ може дослідити вразливості для інших протоколів, таких як IPv6, HTTP;

- Якщо АЕТ використовує HTTP (Port 80), то можливо обійти мережні екрани, вбудовуючи шкідливе програмне забезпечення в сервісну мережну систему поверх веб-трафіку. Тому, очевидно, існують АЕТ для веб-сервісів, веб-застосувань та хмарних обчислювальних середовищ, а це вказує на вкрай серйозний рівень загроз їх функціональній стійкості.

4.2.4. Об'єднані системи виявлення функціональних втручань.

Поширення систем виявлення функціональних втручань дозволяє оцінити потенціал щодо деструктивних впливів, спрямованих проти функціональної стійкості сервісних мережних систем різного виду. Системи виявлення

функціональних втручань підвищують безпеку оброблення даних на відміну від класичних мережних екранів, які самі по собі не є задовільним засобом підтримки функціональної стійкості в сучасних умовах.

Відповідно, системи запобігання функціональним втручанням (IPS) є вдосконаленими системами виявлення функціональних втручань, які забезпечують додаткову функціональність, яка націлена на виявлення та запобігання потенційним загрозам.

Тим не менше, обидва вищезгадані класи систем функціонують автономно. Вони не в змозі детектувати нові види мережних загроз, що з року в рік стають все більш складними. За їх допомогою можливо порушити функціонування дата-центрів, сервісних мережних систем в цілому, особливо таких систем, що працюють в режимі «24/7». Таким чином, об'єднання та інтеграція в рамках різних реалізацій систем виявлення функціональних втручань є надзвичайно важливою. Особливості систем виявлення функціональних втручань (IDS) нового типу представлено на рис. 4.5.

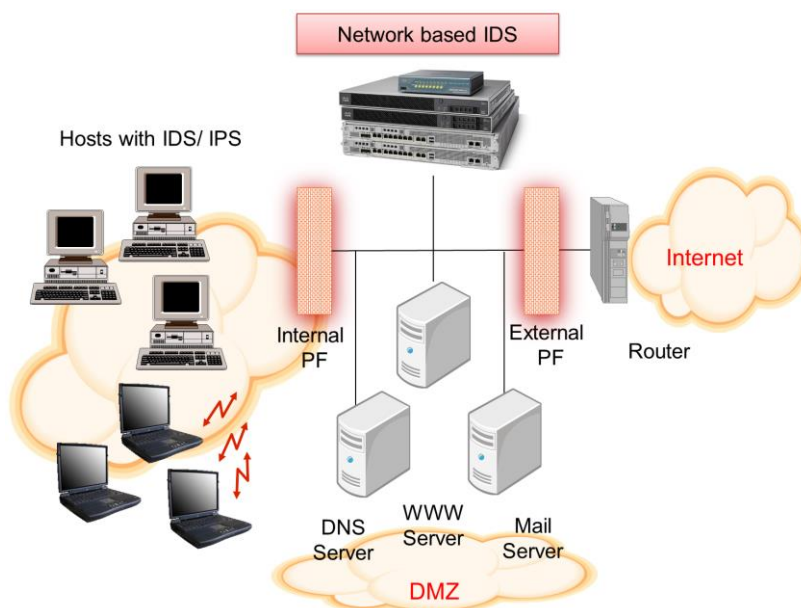


Рис. 4.5. Особливості об'єднаних систем виявлення функціональних втручань.

Спільна мережа виявлення функціональних втручань (CIDN) є наступним кроком розвитку об'єднаних IDS/IPS мережних систем, які сфокусовані на пошуку шляхів запобігання невідомим видам мережних загроз. against the unknown dangerous attacks. CIDN дозволяє (див. рис. 4.6) залученим IDS ділитись одержаними даними, досвідом та рішеннями щодо боротьби проти

спланованих мережних загроз функціональній стійкості сервісних мережних систем [166].

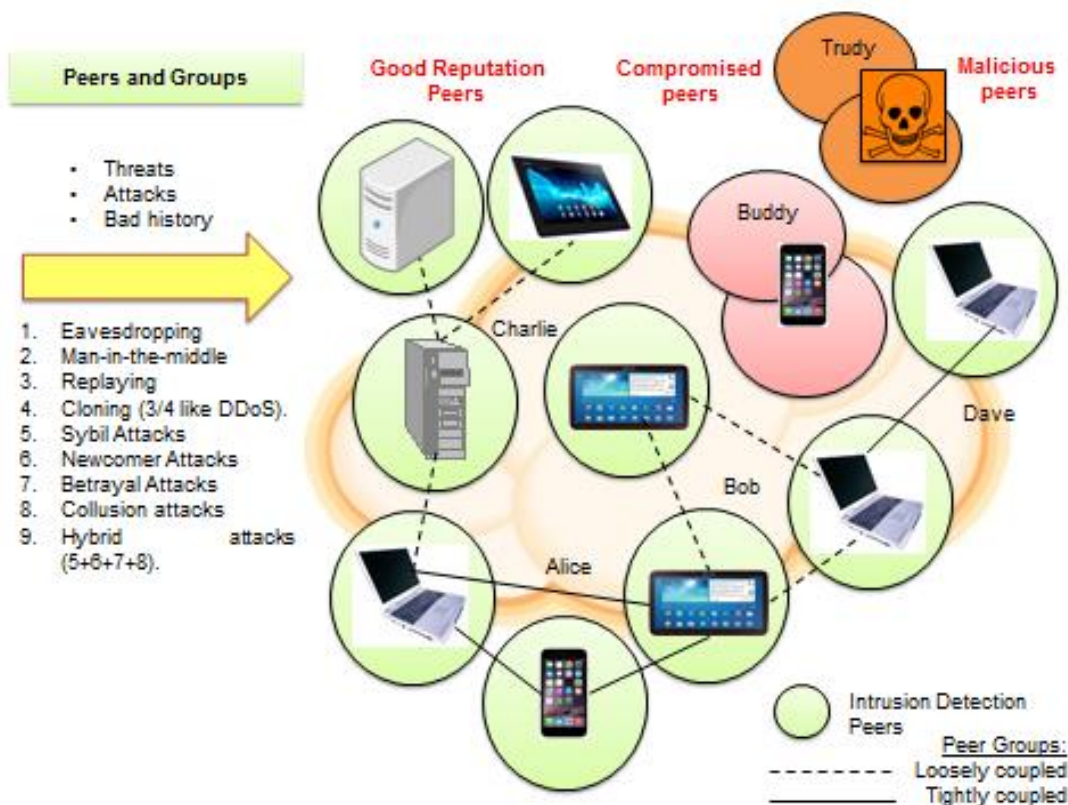


Рис. 4.6. Приклад взаємодії IDS в рамках CIDN.

Основні вимоги до розроблення CIDN та підтримування її функціональності є наступними: ефективна комунікація малого та середнього радіусу, живучість та сервісна доступність пірів (IDS) та каналів мережної платформи між ними, масштабованість та взаємна сумісність окремих IDS. Типова сервісна платформа, що реалізує CIDN концепцію може об'єднувати такі мережні технології як: LAN, WLAN, 2G-4G, інфраструктуру для NFC та Bluetooth.

Спільна мережа виявлення функціональних втручань складається з множини сервісних вузлів, деякі з яких мають вбудовані IDS, підключеного обладнання користувачів, а також встановлених мережних екранів для груп користувачів, які керовані адміністраторами Alice, Bob, Charlie, Dave. Зв'язки між цими групами є слабкими або тисними. Тим не менше, можливі внутрішні атаки на CIDN (користувач Trudy через Buddy).

Взаємодія через окремі пірингові системи (IDS-компоненти) стає більш ефективною в рамках упровадження CIDN.

Нажаль, CIDN може набути характеру мішені для атак на основі небезпечного програмного забезпечення. Таким чином, деякі небезпечні користувачі у рамках CIDN можуть скомпрометувати сегмент сервісної мережної платформи, порушуючи її функціональну стійкість та знижуючи ефективність IDS систем зсередини. Відповідно, доволі велика кількість завдань із дослідження проблематики CIDN все ще має бути розглянута в майбутньому [166], наприклад:

- Вибір сервісних вузлів для реалізації об'єднаної IDS та управління довірою в мережній системі;
- Концепції прийняття рішень в об'єднаній IDS (див. розділ 4.3 цієї роботи);
- Управління ресурсами в межах CIDN.

4.2.5. Особливості мережних загроз для CIDN.

Традиційні мережні загрози можуть значно скомпрометувати мережну безпеку всередині CIDN. Прості мережні атаки можна подати таким чином (рис. 4.6, 1-4 позиції списку): Eavesdropping (прослуховування трафіку), Man-in-the-middle (людина посередині, підміна), Replaying (імітація автентичності), Cloning (3/4 таких атак нагадують DDoS).

Більш складні внутрішні атаки на CIDN (рис. 4.6, 5-9 позиції списку), які можуть виникати несподівано з внутрішніх пірів мережної платформи, причому раніше нескомпрометованих, можна охарактеризувати наступним чином [166]:

Sybil-атака (атака Сибілли): розповсюдження великої кількості різних ідентифікаторів (фальшивих) від атакуючого піру; атака «новоприбульця»: атакуючий пір намагається стерти дані про свою компрометацію з інших вузлів мережної платформи; betrayal атака: механізм довіри в сервісній мережній системі, що є стійким до такого виду атаки має задовольняти виконанню наступної соціальної норми: «побудова надійного партнерства займає довгий

час, тоді як лише кілька неправильних вчинків руйнують довіру повністю». У випадку, коли довірені вузли починають діяти неприпустимо, довіра до них падає дуже швидко і система IDS приймає відповідні рішення, а от відновлення колишніх (очевидно, що статистичних) показників функціонування вимагає значного часу та є складним процесом; атака синдикату: виникає в умовах, коли група користувачів або атакуючих мережних вузлів узгоджено поєднує зусилля задля компрометації всієї сервісної мережної системи; гібридні атаки (рис. 4.6, позиції списку 5+6+7+8). Типова CIDN повинна забезпечувати необхідну сервісну функціональність для запобігання перерахованим видам загроз.

4.3. Концепції точок присутності й інформаційної присутності у відкритій функціональній моделі гетерогенної сервісної системи.

В сучасних хмарних сервісних системах не існує єдиного централізованого ЦОД. Це означає, що дані зберігаються, передаються та обробляються в хмарних серверних системах: а) розподілено; б) неузгоджено; в) окремими фрагментами у відповідності до запитів деякого програмного забезпечення під загальним контролем центру мережного моніторингу інфокомунікаційних операторів, які здають в оренду свої мережні ресурси для персонального, корпоративного або урядового використання та відповідних цілей. Природно, що мережні ресурси операторських мереж мають бути оптимізованими за ефективністю, утворюючи деяку мережну (фізичну) інфраструктуру, проте на сьогодні для користувачів хмарних сервісних систем ці питання відходять на другий план, оскільки мережні оператори комерціалізують свої технічні рішення у чіткій відповідності до бізнес-моделей, які мають на меті максимізувати кількість застосувань, що приносять прибуток. На перший план для оператора виходить власний прибуток та конкурентоздатність за якістю послуг. Тим не менше, багато країн у інтересах національної безпеки роблять спроби виділяти та аналізувати небажані інформаційні потоки в мережних системах інфокомунікаційних операторів, включаючи мережі їх технічних

партнерів, що може розглядатись як втручання до царини інформації, що може бути чутливою для деяких зацікавлених осіб, із відповідними юридично-політичними наслідками. З іншого боку, спробуємо проаналізувати, які технічні методи можливо застосувати для виявлення та локалізації такої активності у сервісних мережних системах національного сегменту, яка може бути потенційно шкідливою для національних інтересів. Як можна бачити з результатів, які були одержані у попередньому розділі 4.2, розв'язання даного завдання є далеко нетривіальним. IDS повинні володіти засобами для прийняття рішень щодо спроб порушень функціональної стабільності пов'язаних сервісних мережних платформ.

Таким чином, першочерговим є питання, як саме визначити мережні ресурси, що найбільш ймовірно використані або використовуються для дестабілізації функціонування сервісної мережної системи чи її окремих сегментів, зокрема у розумінні інформаційної атаки? Почнемо з умовної класифікації видів такої шкідливої діяльності:

- Перший її вид добре відомий під аббревіатурами – такими, як DoS, або DDoS (мережні атаки). Ці атаки на сьогодні досить широко використовуються для блокування цифрових ресурсів шляхом організації перевантаження деяких мережних інтерфейсів сервісних вузлів. Відповідно, продуктивність деяких ресурсів мережної системи падає практично до нуля. DoS можна легко ідентифікувати та локалізувати на більшості сучасних серверних платформ, але її розподілена версія (DDoS) є значно складнішою та добре спланованою активністю, що походить від мережних вузлів, які розподілені всередині/зовні мережної платформи, а також, як правило, використовуються в неавторизованому режимі генерування запитів до потрібного сервісу або їх множини, перебуваючи під контролем деякого мережевого програмного забезпечення (бот-нету).

- Другий вид шкідливої діяльності є більш складним, проте водночас більш важливим для зловмисника. Ним є заздалегідь сплановані медіа-вкиди, витоки інформації або дезінформації, в загальному – елементи пропаганди впродовж

інформаційної війни. Очевидно, що найбільш ефективним для інформатизованого суспільства інструментом війни в даному випадку виступає брехня.

Обидва зазначені види діяльності мають схожі риси щодо інформаційної орієнтованості, проте вони мають і значні відмінності. Вони є: а) розподіленими, як і хмарна сервісна система сама по собі; б) функціонують віддалено. Проте, з іншого боку, перший вид активності (мережні атаки), є глибоко технічним аспектом у сучасних телекомунікаційних системах, а другий її вид – безпосередньо пов'язаний із семантикою інформаційних потоків, які обробляються та поширюються у мережних системах для персонального використання, але у максимально можливому масштабі для глибшого соціального впливу.

Визначимо точки присутності – points of presence (POP) як точки через які два або більше різних мережних операторів (або мережних пристроїв) одержують взаємопідключення [17, 167], див. рис. 4.7.

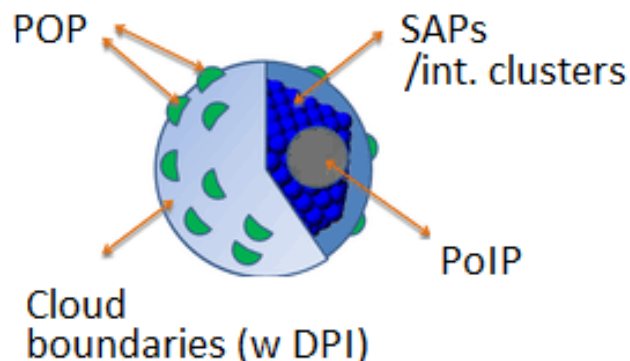


Рис. 4.7. Сферична концептуальна модель хмарних кластерів [17].

Зазначимо, що безпечна мережна архітектура хмарних сервісних систем, таких як сервісні системи національного сегменту хмарної інфраструктури, як правило, передбачає, що вона є ізольованою від інших зовнішніх мережних систем через застосування lawful interception, тобто технології та засобів законної фільтрації та перехоплення мережного трафіку у відповідних PoP.

Точки інформаційної присутності – Points of Information Presence (PoIP) можливо визначити, як одну або декілька областей у хмарній мережній системі, що пропускають вхідні або вихідні потоки трафіку в яких спостерігаються під

час фільтрування наперед визначні теги з вмістом, наприклад, небажаної інформації. Ця інформація, для прикладу, може становити загрозу національним інтересам. Технологія DPI використовується для визначення згаданих інформаційних потоків, маючи також можливості для фіксації множини внутрішніх мережних інтерфейсів сервісної мережної платформи, що їх одержували або генерували. Області з високою концентрацією таких мережних інтерфейсів були визначені автором як такі, що їх можна розглядати у якості відповідних PoIP для кожної заданої інформаційної активності, що зазнає моніторингу [17].

Як правило, відповідні PoP для зовнішнього або внутрішнього (міжсегментного) обміну трафіком повинні передбачати ізоляцію засобами фільтрування з DPI [168] після виявлення небажаних потоків трафіку, що адресовані до визначених PoIP/PoIPs. Концепція мігруючого мережного екрану – **migrating firewall (MF)**, що була запропонована автором, може бути розглянута як перспективна внаслідок власної гнучкості та можливості реплікації у необхідних сегментах або вузлах сервісної мережної системи під час локалізації та запобігання небажаній активності, що зменшує функціональну стійкість хмарної сервісної системи [17]. MF може коректувати правила фільтрації навантаження існуючими мережними екранами, контролювати процеси фільтрації навантаження, виконувати збір відповідної статистичної інформації. Згадана активність, зокрема, може виникати під час виявлення асиметрії потоків керування при запуску пірінгової «бот-нет» мережі, а також при симетричному транзиті сторонніх інформаційних потоків через сервісну мережну платформу (транзитна DoS схема, що призводить до недоступності деяких мережних інтерфейсів), при спробах локалізації небажаного контенту і/або програмного забезпечення в PoIP/PoIPs, що були виявлені під час DPI аналізу.

Застосування принципів MF дозволяє підвищити якість захисного оверлейного кількшарового «покриття» хмарної сервісної системи. Зокрема, це дозволить долати мережні атаки типу DoS/DDoS як зовнішнього, так і

внутрішнього походження, тому що граничні вузли сервісної мережної системи також підпадають під можливість реплікації сервісів MF, а це дозволяє, у випадку необхідності, ізолювати новоутворений (D)DoS “бот-нет”, при спробі розпочати відповідну деструктивну діяльність, яка, як правило, спрямована на пригнічення продуктивності та доступності деякої множини SAP. Додатково, при аномальному навантаженні мережних шлюзів SAP (що перебувають у процесі активного масштабування екземплярів комплексного сервісу або оркестрації ESC) та, одночасно, недовантаження відповідних сервісних компонентів, MF повинен визначити причини цієї ситуації. А саме – визначити перелік атакуючих вузлів, перевірити відповідні внутрішні потоки трафіку на присутність ознак пірингової структури і, у разі потреби, виконати ізолювання або зміну пріоритету відповідного навантаження (наприклад, надавши йому найнижчий можливий пріоритет). Потоки навантаження, що аналізуються методами DPI у граничних сервісних вузлах та містять ознаки передавання потоків команд до множини атакуючих вузлів всередині хмарної сервісної системи, після їх співставлення з розташуванням носіїв PoIP небажаного інформаційного контенту або активності, дозволять виявити та запобігти застосуванню навіть складних AET методів.

Підвищення функціональної стійкості архітектури сервісних мережних систем до зловмисних зовнішніх впливів на їх функціональну стабільність дозволить нівелювати наслідки від застосування мережних атак, а саме зниження кількості працездатних сервісних вузлів і, відповідно, обсягів загальних ефективних обчислювальних потужностей (див. рис. 3.33, 4.1), а отже – запобігти критичному зниженню рівня сервісної доступності.

Відповідно, Н.Ф. Казакова у своїх працях [169, 170] розглядає процеси когнітивного оброблення даних в ЦОД, які, за необхідності, можуть мігрувати до безпечних мережних сегментів хмарної сервісної системи, приховуючись від зовнішніх деструктивних впливів (див. рис. 4.8). Проте, можливості виявлення реплікованих ресурсів, які зазнали міграції є доволі високими, наприклад, на

основі емпіричного аналізу флуктуацій навантаження до реплікованих засобів оброблення даних.

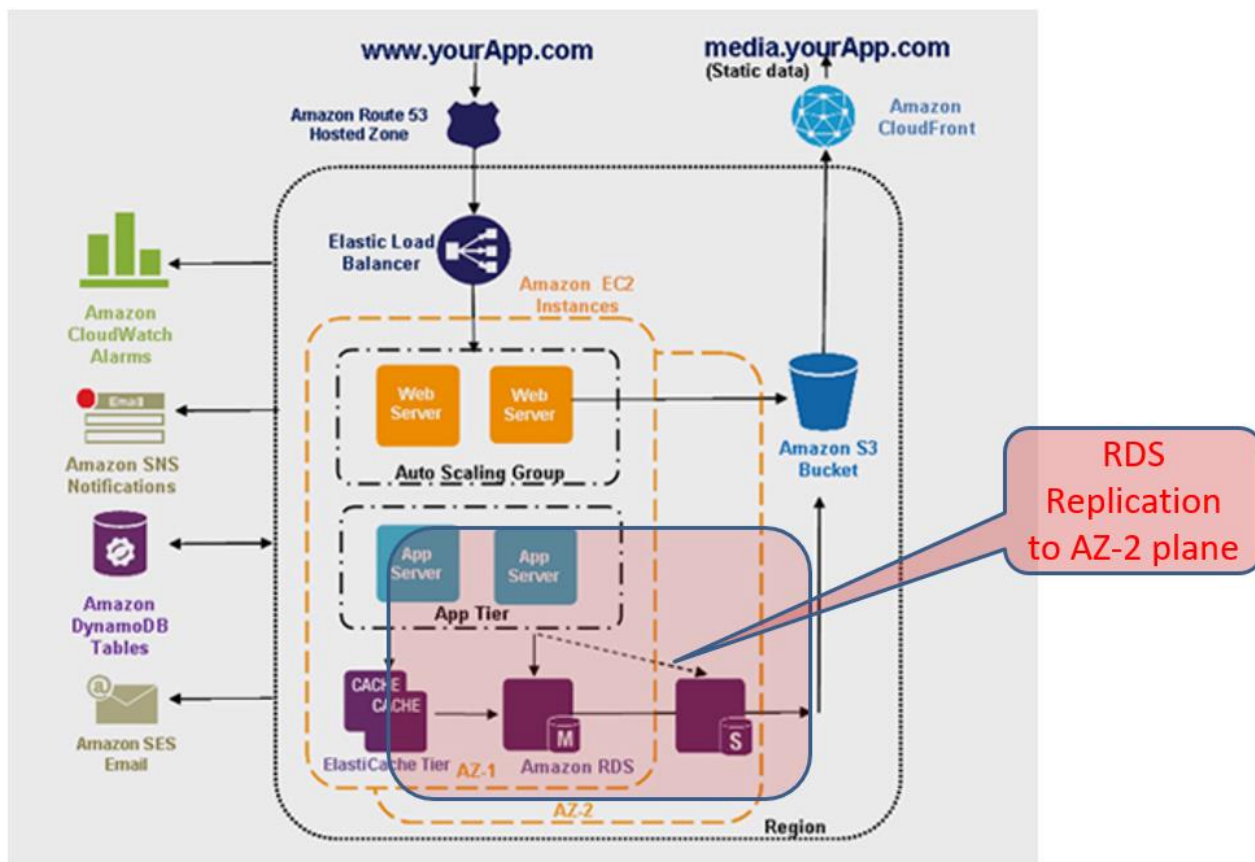


Рис. 4.8. Підхід на основі міграції ресурсів ЦОД у безпечні сегменти (AZ-2).

Також, можливо розглянути ідею міграції довірених потоків трафіку (див. рис. 4.9) серед спеціально надлишково утворених майже ідентичних із зовні віртуальних сервісних площин (віртуалізованих PaaS), що ускладнює зовнішнє втручання у функціонування сервісної мережної системи, підвищуючи її функціональну стійкість. Проте, такий підхід є технологічно (апаратно-програмно) ускладненим, вимагає детального аналізу мережних протоколів для забезпечення ефективного управління відповідними віртуалізованими SDP. Деструктивні впливи на таку систему стикаються з високою складністю виявлення конкретної віртуалізованої SDP, яка безпосередньо опрацьовує навантаження. Спроби виявлення можуть бути використані відповідною IDS сервісної мережної платформи для подальшого запобігання потенційним мережним атакам, зокрема, шляхом зміни робочої площини SDP PaaS.

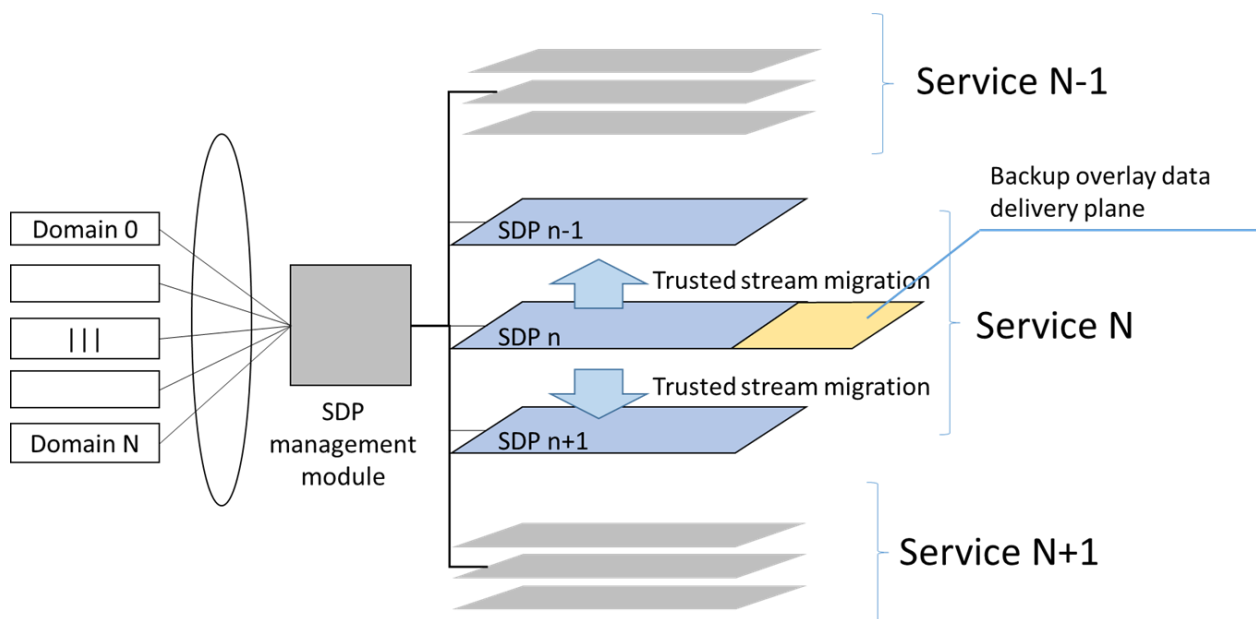


Рис. 4.9. Підхід на основі міграції довірених потоків трафіку серед спеціально утвореної множини квазі-ідентичних надлишкових віртуалізованих PaaS.

4.4. Розроблення методу та моделі мігруючого мережного екрану.

Запропонована автором концепція мігруючого мережного екрану (MF) вирізняється більшою компактністю рішення, відсутністю необхідності реплікацій та виділення потоків трафіку при міграції відповідної множини сервісів, а також є більш надійною, з погляду негарантованості мережної функціональної стабільності під час міграції або реплікації сервісів.

Очевидно, що MF повинен мати кількшарову оверлейну структуру. Рис. 4.7 демонструє, що границі хмарної сервісної системи мають засоби lawful interception, які реалізовані модулями DPI; фільтрація трафіку відбувається у всіх зовнішніх мережних інтерфейсах. Кількість таких граничних мережних інтерфейсів визначається архітектурою хмарної платформи, прийнятою політикою безпеки, її внутрішньою структурою та масштабованістю, розташуванням SAPs. Система фільтрації трафіку на основі DPI збирає статистику з потоків даних, а у подальшому ці статистичні дані обробляються та зберігаються у компактній формі, наприклад – із використанням голографічного представлення мережних метаданих [136]. В результаті, одержуємо номінальний статистичний профіль (NSP) стаціонарного режиму функціонування хмарної мережної системи, див. рис. 4.10.

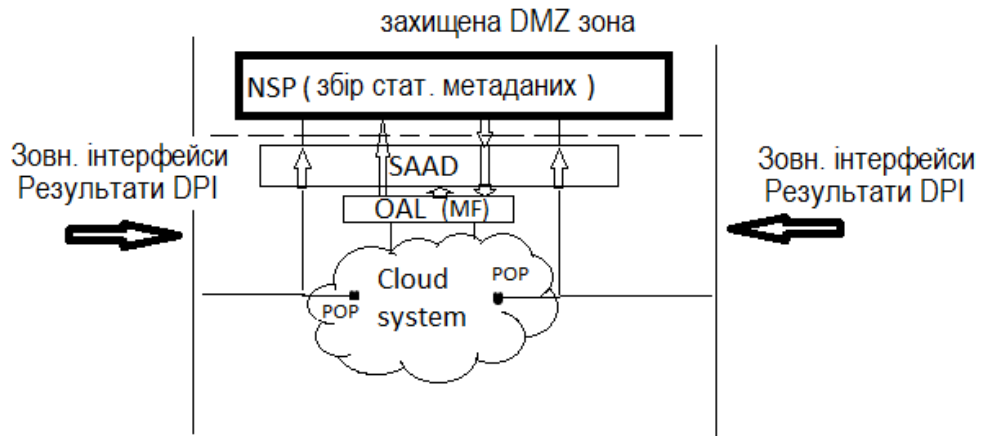


Рис. 4.10. Функціональна модель мігруючого мережного екрану (MF) [17].

NSP є специфічним верхнім шаром структури MF. Властивостями NSP відображаються особливості поведінки сервісної мережної системи у зовнішньому мережному середовищі. У відповідності до міркувань безпеки, NSP повинен бути розташованим у захищеному сегменті хмарної платформи (DMZ), ізольовано від зовнішніх та внутрішніх потоків даних, а процес формування даного профіля відбувається неперервно.

Шар, що є підлеглим до NSP відноситься до системи виявлення аномальної статистичної активності (SAAD). SAAD збирає та проводить первинне оброблення статистичних потоків даних безпосередньо від фільтруючої системи DPI. Його функціонування передбачає порівняння метаданих від NSP та поточного статистичного профілю системи, який виникає під час оброблення навантаження у сервісній мережній платформі. Отже, шар SAAD відслідковує аномальну активність, яка виникає відносно SAPs та має як зовнішнє, так і внутрішнє походження. SAAD встановлює також правила фільтрування навантаження з метою виявлення аномальної (або небажаної) інформаційної активності, виокремлюючи області PoIP за присутністю заданих ключових семантичних маркерів. Картина пірінгових атак будується за результатами аналізу внутрішньої міжпірінгової взаємодії та з урахуванням можливості її зовнішнього варіанту при керуванні кризь зовнішні границі сервісної мережної хмари. Оцінка обсягу параметрів, які потребують вимірювань може бути

прогнозована та розрахована на основі результатів [24], шляхом застосування експертної системи та методів регресивного аналізу.

Під управлінням SAAD розташований шар, який аналізує маркери згідно з правилами фільтрування, визначеними SAAD. Визначимо його, як безпосередню реалізацію мігруючого мережного екрану MF або як аналітичний оверлейний шар (OAL). OAL реалізується шляхом конкретних сервісних реплікацій для підтримування функціональності MF у потрібних сегментах сервісної мережної системи.

Впродовж нормального (стаціонарного) режиму функціонування сервісної мережної системи OAL періодично звітує до шару NSP, використовуючи ресурси SAAD, які виконують первинне оброблення та відбір одержаних повідомлень. Таким чином, у NSP накопичуються статистичні метадані щодо функціонування мережної платформи.

В процесі функціонування SAAD, виконується аналіз звітів від OAL шляхом узгодження одержаної інформації з даними від NSP та корекція роботи MF щодо правил фільтрації та відбору інформації. Надаються інструкції щодо реплікації та міграції груп сервісів, які підтримують OAL (MF) у відповідних мережних сегментах. Автор дозволить собі відмітити, що *результати* коректуючих впливів аналізуються в процесі неперервного формування статистичних метаданих безпосередньо у NSP (а не у SAAD, для забезпечення незалежності функціонування NSP). Після такої диференційної координації у відповідності до даних про номінальну статистику трафіку, що зберігаються у NSP, виробляються керуючі впливи щодо функціонування аналітичних алгоритмів SAAD та, за необхідності, активується захист сервісної мережної платформи. SAAD може приймати рішення про ізоляцію: а) зовнішніх мережних інтерфейсів сервісної платформи; б) обраних внутрішніх міжсегментних інтерфейсів. Обидва випадки є характерними для окремих груп мережних адрес щодо яких зафіксована аномальна активність або для потоків даних у яких визначені попередньо задані ключові семантичні маркери. Після цього визначається необхідність оптимізації сервісів, що підтримують MF та

засобів протидії деструктивним впливам, які використовуються. Вдало завершуючи пригнічення мережної атаки, OAL MF продовжує надавати первинні дані аналізу трафіку до SAAD, в подальшому відстеження статистичної ситуації у сервісній мережній системі продовжується за вищеописаним алгоритмом. Рішення щодо міграції сервісів, які підтримують MF можуть ухвалюватись на основі підходів із використанням нечіткої логіки [157] або результатів [65, 135, 171], на основі яких формуються критерії міграції. Як показав досвід [238], ймовірність виявлення складної аномальної мережної активності у випадку застосування подібних методів становить 90-98%, у залежності від особливостей ТК платформи та налаштувань системи.

4.5. Дослідження методів оптимального управління процесами міграції ресурсів в гетерогенних сервісних системах.

Всі основні тенденції розвитку інформаційних технологій, такі як хмарні обчислення базуються на великих та потужних обчислювальних системах. Постійно зростаючий попит на мережні сервіси, що надаються хмаринковими обчислювальними системами став причиною того, що компанії та постачальники ресурсів змушені будувати масштабні центри обробки даних, які функціонують на великих апаратних потужностях, а отже, споживають багато енергії. В 2006 році енергія, що була спожита галуззю ІТ в США становила близько 61 мільярдів кВт*год, що становило 1.5% всієї виробленої у світі електричної енергії, що відповідає 2% світового викиду оксиду вуглецю, а це, у свою чергу, еквівалентне сукупним викидам CO₂ авіаційної галузі. Причому, ці показники збільшуються приблизно удвічі кожні 5 років [172].

Протягом останніх кількох років відбувся значний прорив в контексті зменшення споживання енергії, в основному, за рахунок підвищення ефективності енергопостачального та охолоджувального обладнання в центрах оброблення даних сервісних мережних систем. Ще декілька років тому коефіцієнт ефективності використання енергії, який визначається як

відношення підведеної потужності до потужності, яка використана обчислювальними ресурсами центру обробки даних, лежав в межах між 2 та 3, а в даний час великі компанії, які спеціалізуються на хмарних обчисленнях досягають величин цього коефіцієнта менших за 1.1. Проте, все ще існує багато можливостей оптимізації самих обчислювальних ресурсів. Було підраховано, що сервери мережних платформ більшість часу працюють на 10-50% своєї повної потужності [173-174]. Таке низьке використання потужностей, зокрема, зумовлене доволі повільними флуктуаціями навантаження на віртуальні машини – центри обробки даних спроектовані так, щоб витримувати піки навантажень, хоча протягом довгих періодів часу навантаження є значно меншим [175, 176]. Оскільки, ввімкнений, але незадіяний сервер споживає близько 50-70% від тієї потужності, яку він споживає при повній власній завантаженості [177], стає очевидним, що значна кількість енергії споживається навіть при низькому завантаженні.

Для вирішення цієї проблеми може бути використана парадигма віртуалізації в рамках розв'язання завдань структурно-параметричної оптимізації при конфігуруванні віртуальних машин на відповідній сервісній мережній платформі. Такий підхід дає можливість консолідації навантаження, яке полягає в розміщенні максимальної кількості віртуальних машин на мінімальній кількості фізичних серверних систем [178]. Консолідація дозволить переводити незавантажені сервери в режим зниженого енергоспоживання або відімкнути їх взагалі (що приведе до економії енергії та скорочення експлуатаційних витрат), або ж використати ці системи для обслуговування додаткових навантажень (що приведе до зменшення капітальних витрат). Нажаль, ефективна консолідація віртуальних машин утруднена успадкованою складністю проблеми. Завдання оптимального призначення віртуальних машин серверам центру обробки даних є аналогом задачі «про упаковку в контейнери» недетермінованої поліноміальної складності, суть якої полягає в розміщенні змінного набору предметів у мінімальній кількості контейнерів із заданого набору. Дане завдання ускладнене двома обставинами: 1) призначення

віртуальних машин має враховувати декілька параметрів серверної системи сервісного вузла, наприклад параметри продуктивності процесорів (надалі CPU) і обсяг оперативної пам'яті (надалі RAM), а отже, внаслідок цього, задача стає «багатовимірним завданням про упаковку в контейнери»; 2) навіть при вдалому призначенні, віртуальні машини безперервно змінюють свої апаратні потреби, тобто попередня конфігурація їх призначення стає зовсім неактуальною вже за декілька годин.

Розглянемо підхід до консолідації віртуальних машин на основі вирішення описаного багатовимірного завдання, а саме представлений конкретним випадком, в якому віртуальні машини консолідується стосовно двох ресурсів серверної мережної платформи: продуктивності CPU і обсягу оперативної пам'яті RAM. Причому, віртуальні машини консолідується за допомогою двох типів імовірнісних методик-процедур – для їх призначення та міграції на інший сервісний вузол відповідно. Обидві методики-процедури націлені на підвищення рівня використання серверів та динамічну консолідацію навантаження з дотриманням відповідної якості обслуговування користувачів сервісних мережних платформ за умови мінімізації енергетичних витрат. Всі ключові операції покладені на окремі сервери, в той час, як менеджер або гіпервізор центру обробки даних повинен правильно поєднувати локальні структурно-параметричні конфігурації цих серверів. Метод, який лежить в основі цього підходу насамперед заснований на «мурашиних» алгоритмах, які спершу використовував Деньюберг [179], а потім і широке наукове співтовариство для моделювання поведінки мурашиних колоній та вирішення багатьох складних проблем розподіленого характеру. Характеристики, які надають мурашині алгоритми для даного підходу, роблять його ефективним та особливим по відношенню до інших рішень. Наведемо деякі з цих характеристик: 1) використання парадигми колективного інтелекту, яка дозволяє вирішувати складні проблеми за допомогою простих операцій, що виконуються великою кількістю автономних дійових осіб (в нашому випадку – окремих серверів на сервісних вузлах); 2) використання імовірнісної методики

в формі моделей поведінки реальних живих комах; 3) самоорганізаційна поведінка системи, яка гарантує, що призначення конфігурації віртуальних машин серверам динамічно адаптуватиметься до змінного навантаження.

З метою оцінювання ефективності запропонованого підходу за рівнем використання ресурсів розподіленої сервісної мережної системи, застосуємо два взаємодоповнюючих напрямки досліджень. Перший напрямок пропонує математичну модель, яка простежує еволюцію сервісної системи протягом певного часу базуючись на тому, що залучені в її описі змінні є неперервними. Така модель дозволяє нам перевірити поведінку хмарної сервісної платформи в умовах великої кількості різноманітних сценаріїв, просто змінюючи значення деяких її параметрів. Другий підхід складається з експериментальних дослідів, які виконуються в реальних центрах обробки даних. Ці два напрямки доповнюють один одного: удосконалена аналітична модель вводить деякі спрощення, але дозволяє дослідити систему на широкому діапазоні сценаріїв; з іншого боку, реальні експерименти не вносять ніяких спрощень, але в певній мірі обмежуються конкретною ситуативністю, що відчутно зменшує кількість сценаріїв тестування. Дослідження показали, що хмаринкова сервісна платформа розподіленого дата центру, що конфігурується на основі запропонованого підходу дозволяє досягати дуже хорошої консолідації, та плавно адаптується до можливих змін. Зрештою, для того щоб порівняти ефективність хмаринкової сервісної системи сконфігурованої за новим підходом з системами, які організовані згідно базового підходу, описаного в [172], а також для того щоб провести дослідження системної масштабованості автором використано спеціально підібраний симулятор [135].

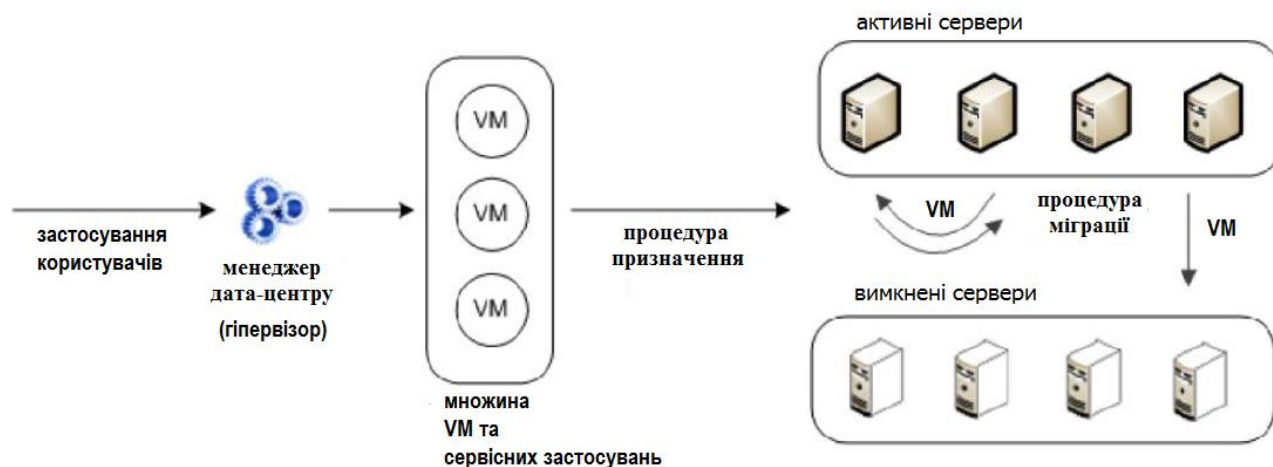


Рис. 4.11. Процедури призначення та міграції віртуальних машин VM в розподіленому хмаринковому центрі обробки даних сервісної мережної платформи [135].

Основною метою запропонованого підходу є динамічне призначення віртуальних машин серверним системам з метою зменшення енерговитрат (за рахунок консолідації віртуальних машин, що дає змогу помістити деякі сервери в енергозберігаючий режим), за умов підтримування аналогічної або навіть кращої якості сервісу. Основні процедури сценарію схематично зображено на рис. 4.11: запит сервісного застосування передається від користувача до менеджера (або гіпервізора) центру обробки даних, який обирає віртуальну машину, що підходить даному сервісному застосуванню на основі його системних потреб (показників CPU, RAM, обсягів вільного дискового простору), а також параметрів користувача, наприклад типу клієнтської операційної системи. Після цього віртуальна машина призначається одному з існуючих серверів за допомогою процедури призначення.

Основна ідея всього підходу полягає в тому, що сам сервер повинен вирішити: прийняти або ж відхилити призначену віртуальну машину. Таке рішення приймається на основі локальної інформації сервера – наприклад, інформації про поточне ресурсне завантаження CPU і RAM – і ґрунтується на методиці випробувань Бернуллі. Гіпервізор центру обробки даних сервісної мережної системи виконує лише координуючу роль, яка не потребує складних

централізованих алгоритмів для оптимальної реалізації процесів призначення віртуальних машин.

Навантаження, яке припадає на кожне сервісне застосування є динамічним, або, іншими словами, обчислювальні ресурси, які необхідні для правильної роботи такого сервісного застосування, змінюються з часом: наприклад, потреби щодо продуктивності CPU web-сервера залежать від навантаження запитів, яке формується пов'язаними користувачами. Таким чином, процес призначення віртуальних машин у потрібній конфігурації постійно контролюється і адаптується через процедуру їх міграції. Міграція віртуальної машини може бути вигідною, як у випадку, коли коефіцієнт використання обчислювальних ресурсів є надто малим, так і у випадку, коли коефіцієнт їх використання є надто високим (що може привести до ситуації перевантажень та порушення якості сервісу). Міграція також може виникати у розподіленій хмарній сервісній системі тоді, коли користувачі починають концентрувати навантаження на сервісній застосування у деякій її просторовій частині. Процедура міграції VM складається з двох етапів: на першому етапі сервер запитує міграцію віртуальної машини, на основі інформації про використання ресурсів його CPU/RAM. Метою наступного кроку є обрання сервера, який буде обслуговувати віртуальну машину, що мігрує за допомогою методів, подібних до тих, які використовуються при процедурі призначення.

Ефективність технології конфігурування хмаринкових сервісних систем оцінюється за допомогою таких критеріїв:

- Коефіцієнт використання обчислювальних ресурсів. З метою сприяння консолідації та енергозбереженню, сервер або повинен використовуватись майже на повну потужність, або ж знаходитись в режимі сну. Аналіз ступеню використання ресурсів CPU і RAM має на меті перевірку того, чи досягнута дана мета.

- Кількість активних серверних систем. Віртуальні машини повинні бути розміщені на найменшій можливій кількості активних серверів.

- Спожита потужність. Кінцевою метою є економія енергоресурсів, тому ми обчислюємо потужність, спожиту всім центром обробки даних сервісної мережної системи в різних режимах її завантаження.

- Частота міграцій та змін режимів роботи серверів. Міграція віртуальної машини викликає невелике зниження продуктивності сервісного застосування, що нею обслуговується. Час, який необхідний для того, щоб передати буфер пам'яті віртуальної машини з одного сервера на інший може варіюватися в межах від декількох секунд до кількох хвилин [180-181]. Під час такого періоду віртуальна машина є активною на сервері вузла походження. Протягом фактичного передавання функціональності віртуальної машини відбувається її простій, тривалість якого декілька мілісекунд. Аналогічно цьому, з метою ввімкнення/вимкнення сервера потрібні час та додаткова потужність. Тому, хоча міграції та зміни режимів роботи серверів і мають важливе значення для процесів консолідації віртуальних машин та зменшення споживаної потужності, важливим також є зменшення частоти їх виникнення. Ще важливішим є недопускання великої кількості міграцій віртуальних машин: асинхронна та поступова їх міграція є значно менш згубною, ніж паралельна міграція такої ж кількості віртуальних машин; наприклад, паралельні міграції можуть згенерувати трафік, який перевищить пропускну здатність каналів сервісної мережної платформи, а отже кардинально зменшаться сервісна доступність, системна продуктивність та якість сервісу.

Варто також відмітити ситуації, коли відбувається порушення угоди про рівень обслуговування (Service Level Agreement, SLA). Порушення угоди про рівень обслуговування може відбутися тоді, коли навантаження на деякі віртуальні машини зростає і серверні вузли, якими вони обслуговуються, стають перевантаженими. Появі такої ситуації можна запобігти шляхом своєчасного перенесення деяких віртуальних машин на інші, менш завантажені сервери. Цей критерій, відповідно до нещодавніх досліджень [135, 172], використовується для оцінки рівня QoS послуг, які пропонуються користувачам.

Кілька досліджень та експериментів, наприклад [177, 182], показали, що активний сервер з дуже низьким рівнем використання CPU споживає близько 50-70% тої потужності, яку він споживає при повній своїй завантаженості. Більше того, у випадку, коли використання CPU зростає, споживану потужність можна описати з похибкою меншою, ніж 10%, за допомогою лінійної функції його навантаження починаючи від потужності, яка відповідає стану бездіяльності до потужності, яка відповідає стану повного завантаження сервера [183, 184]. Хоча деякі дослідження вказують на більш точні нелінійні залежності [185], такі уточнення приносять мало практичної користі для досягнення поставлених цілей. Таким чином, в аналітичних та імітаційних експериментах, потужність, яка споживається одним сервером виражається як:

$$P(u) = P_{прост} + (P_{макс} - P_{прост})u \quad (4.1)$$

де $P_{макс}$ – потужність, яка споживається при повному завантаженні CPU, тобто коефіцієнт утилізації $u=1$, $P_{прост}$ – потужність, яка споживається тоді, коли сервер є активним, але в стані простою $u=0$. В експериментах, які проводяться в реальних центрах обробки даних сервісних мережних систем, споживана потужність безпосередньо відслідковується та вимірюється.

Як вже було зазначено, існує дві основні ймовірнісні процедури, на яких базується запропонований технологічний підхід, а саме процедури призначення та міграції VM. Основним критерієм розміщення віртуальних машин на серверах вузлів мережної платформи є наявні у них вільні ресурси CPU та RAM.

Процедура призначення VM виконується тоді, коли користувач своїми запитами запускає в центрі оброблення даних нове сервісне застосування. Отже, коли сервісне застосування вже пов'язане з відповідною віртуальною машиною, менеджер-гіпервізор центру оброблення даних мережної платформи повинен призначити дану віртуальну машину одному з її серверів. Менеджер, замість того, щоб самостійно прийняти рішення (що потребувало б застосування складних оптимізаційних алгоритмів), передає основну частину

цієї процедури самим серверам. Зокрема, він відправляє запрошення всім активним серверам, або тільки їх частині (в залежності від масштабу хмарної сервісної платформи та архітектури розподіленого центру оброблення даних). Воно полягає в команді перевірити, чи мають відповідні сервісні вузли можливість прийняти нову віртуальну машину. Кожен сервер приймає рішення щодо того, відхилити, чи прийняти запрошення і тим самим здійснює свій вклад до процесу консолідації навантаження на мінімально можливій кількості серверів. Запрошення повинно бути відхиленим, якщо сервер перевантажений або недостатньо завантажений з точки зору будь-якого з двох розглянутих критеріїв – рівнів доступних ресурсів CPU і/або RAM. У випадку перевикористання ресурсів, основною причиною відмови від запрошення щодо призначення VM є уникнення ситуацій перевантаження, яке може зменшити якість сервісу, що надається користувачам, а у випадку недовикористання ресурсів – сервер повинен відхилити запрошення, та, водночас, спробувати відмовитись від тих віртуальних машин, які на ньому працюють, оскільки йому варто перейти в режим сну для економії енергії. В іншому випадку, коли рівень використання обчислювальних ресурсів сервера є проміжним, він повинен прийняти запрошення на обслуговування нової віртуальної машини для покращення цільової консолідації.

Сервер приймає рішення на основі випробування Бернуллі. Імовірність успіху такого випробування рівна величині загальної функції ймовірності призначення, що, в свою чергу, визначається шляхом оцінювання функцій ймовірностей призначень для кожного розглянутого ресурсу. Нехай $0 \leq \chi \leq 1$ є відносним рівнем використання ресурсу (CPU або RAM), а T є максимальним дозволеним рівнем його використання (наприклад $T=0.8$ означає те, що рівень використання ресурсу не повинен перевищувати 80% величини ресурсу цього сервера). Тоді функція призначення рівна нулю, коли $\chi > T$, інакше вона обчислюється з використанням розподілу Бернуллі:

$$f(\chi, p, T) = \begin{cases} \frac{1}{M_p} \chi^p (T - \chi), & \text{якщо } 0 \leq \chi \leq T; \\ 0, & \text{якщо } T < \chi \leq 1; \end{cases} \quad (4.2)$$

де p є параметром розподілу, а знаменник M_p нормалізує максимальне значення до 1 і визначається як:

$$M_p = \frac{p^p}{(p+1)^{p+1}} T^{(p+1)}. \quad (4.3)$$

На рис.6.5 показано графік для функції призначення (4.2)-(4.3) з єдиним ресурсом для деяких значень p та $T=0.9$. Параметр p можна використовувати для зміни форми графіку функції. Справді, при $\chi=p/(p+1)T$ функція (4.2)-(4.3) дорівнює 1, і цей максимум наближається до T , якщо p зростає.

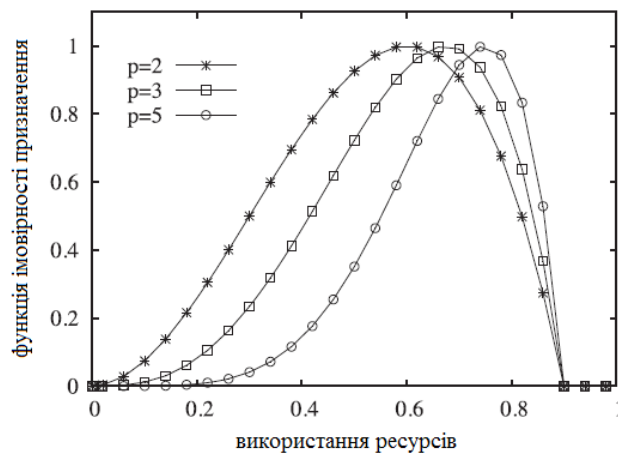


Рис. 4.12. Функція ймовірності призначення $f(\chi, p, T)$ для трьох різних значень параметру p і $T=0.9$ [135].

Значення даної функції рівне нулю, або є дуже низьким, коли обчислювальний ресурс сервісного мережного вузла або перевикористовується, або недовикористовується.

Нехай u_s та m_s є поточними рівнями використання ресурсів CPU та RAM деякої серверної системи s . Тоді загальна функція призначення VM буде дорівнювати добутку двох функцій призначення VM (4.2-4.3), в яких $\chi=u_s$ та $\chi=m_s$ відповідно. Нехай також, припустимо, що p_u та p_m є параметрами розподілу обчислювальних ресурсів сервісного мережного вузла, які розглядаються, а T_u та T_m – їх максимальними рівнями використання

відповідно. Тоді загальна функція призначення для серверної системи s , яку позначимо як f_s , буде виглядати як:

$$f_s(u_s, m_s, p_u, p_m, T_u, T_m) = f(u_s, p_u, T_u) * f(m_s, p_m, T_m) \quad (4.4)$$

Форма функції призначення VM, об'єднана з визначенням функцій за виразом (4.4) гарантує, що серверні системи повинні позитивно відповідати на запрошення прийняти віртуальну машину, коли рівень завантаження їх RAM та CPU є проміжним. А якщо один з їх ресурсів недо- або перевикористовується, то значення ймовірності, яке повертає функція (4.4), буде малим.

Схему реалізації процедури призначення віртуальної машини представлено на рис. 4.13.

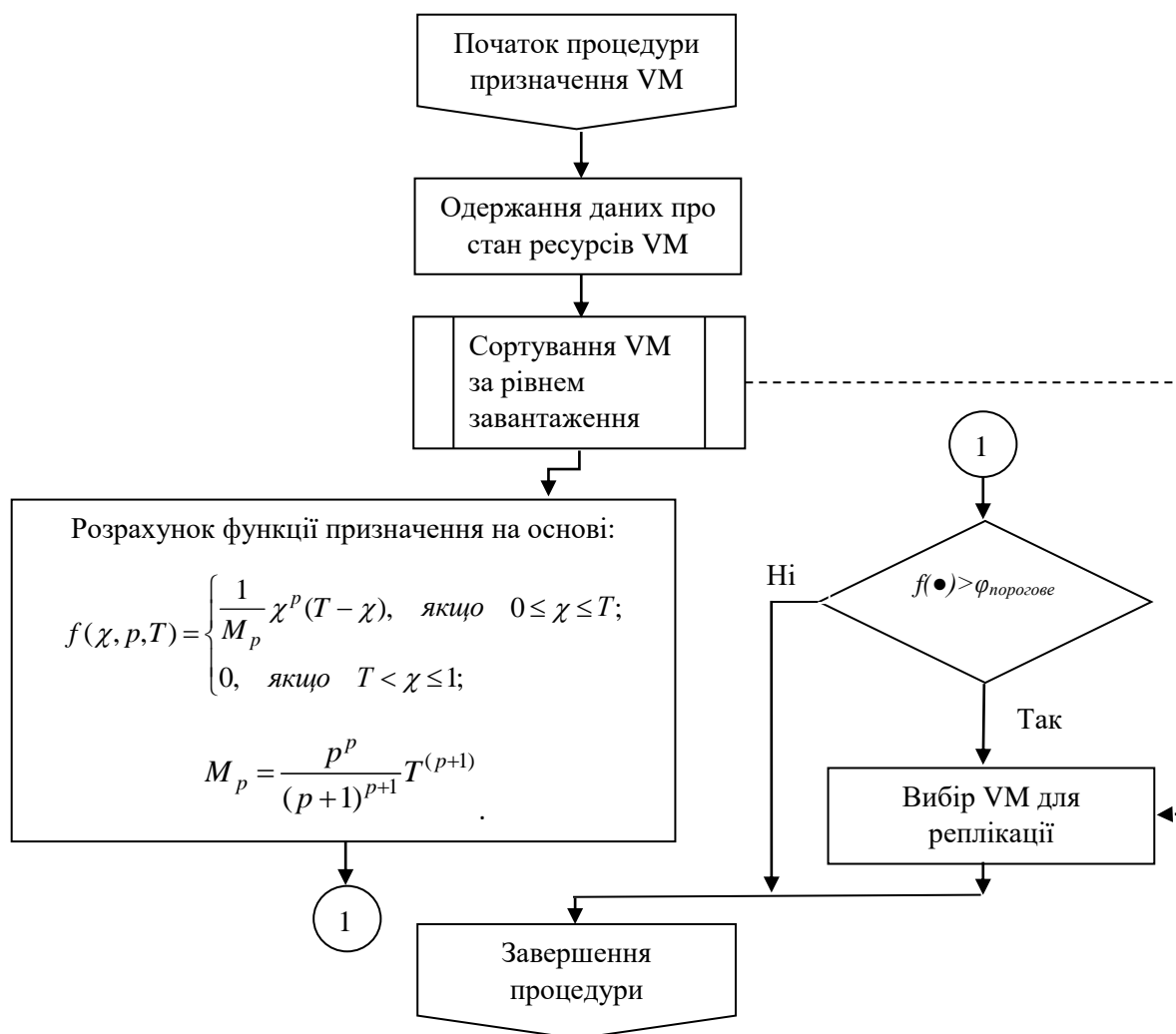


Рис. 4.13. Схема реалізації процедури призначення віртуальної машини: p – коефіцієнт стратегії призначення, T – допустимий рівень використання ресурсу, χ – відносний рівень використання ресурсу, ϕ – поріг прийняття рішення.

Якщо випробування Бернуллі пройдено успішно, то сервер повідомляє менеджера (гіпервізору) центру оброблення даних сервісної мережної системи про свою готовність обслуговувати нову віртуальну машину. Після цього, менеджер просто вибирає один з таких наявних серверів і призначає йому цю нову віртуальну машину. Для цього він може використати оцінки взаємопов'язаних параметрів серверів, обрані, зокрема, за принципами використання теорії нечітких множин [126]. Якщо ж немає жодного придатного сервера, тобто всі випробування Бернуллі пройшли невдало, то досить імовірно, що у всіх серверах один з двох ресурсів (CPU або RAM) близький до порогу використання. Таке зазвичай відбувається тоді, коли загальне навантаження збільшується настільки, що поточна кількість активних серверних систем у сервісній мережній платформі не є достатньою для підтримки такого навантаження [126, 135]. У такому випадку, гіпервізор виводить з режиму сну один з неактивних серверів та доручає йому обслуговування нової віртуальної машини. Якщо має місце випадок, коли немає сервера, який можна вивести з режиму сну, оскільки всі наявні серверні платформи вже є активними, то це означає, що всі вони разом узяті не в змозі обслуговувати таке навантаження навіть за умов його консолідації, а отже інфокомунікаційному оператору слід розглянути можливість встановлення нових серверів та провести масштабування сервісної мережної системи.

У випадку, коли віртуальні машини збільшують свої вимоги до використання ресурсів, серверна система може стати перевантаженою, що ймовірно призведе до подій, пов'язаних із порушенням угоди SLA, які, у свою чергу, негативно вплинуть на репутацію інфокомунікаційного оператора. В обох випадках, а саме недовикористання та перевикористання серверних систем, деякі віртуальні машини можуть вигідно мігрувати до інших серверів, для того щоб дати змогу виключити його, або зменшити його завантаженість.

Процедура міграції відбувається наступним чином. Кожна серверна система слідкує за рівнем використання своїх ресурсів CPU та RAM за допомогою бібліотек, які постачаються разом з інфраструктурою віртуалізації

(наприклад VMWare чи Hyper-V) і перевіряє, чи ці рівні лежать в межах попередньо визначених порогів – нижнього порогу T_n та верхнього порогу T_v . Коли такий стан речей порушується, сервер оцінює відповідну функцію ймовірності міграції та проводить випробування Бернуллі, імовірність успіху якого присвоюється значенню цієї функції. Якщо випробування пройшло вдало, то сервер запитує міграцію однієї зі своїх локальних віртуальних машин. Якщо χ означає рівень використання одного з обчислювальних ресурсів сервісного вузла (CPU чи RAM), то допоміжну функцію міграції пропонується визначити як:

$$f_{мігр}^n = \left(1 - \frac{\chi}{T_n}\right)^\alpha \quad (4.5)$$

$$f_{мігр}^v = \left(1 - \frac{\chi - 1}{1 - T_v}\right)^\beta \quad (4.6)$$

$$f_{мігр} = \begin{cases} \left(1 - \frac{\chi}{T_n}\right)^\alpha, & \text{якщо } \chi \leq T_n; \\ 0, & \text{якщо } T_n < \chi < T_v; \\ \left(1 - \frac{\chi - 1}{1 - T_v}\right)^\beta, & \text{якщо } \chi \geq T_v; \end{cases} \quad (4.7)$$

Функцію (4.7), графік якої представлено на рис. 4.14, сформовано таким чином, щоб викликати міграцію VM тоді, коли рівень використання їх обчислювальних ресурсів стає нижче заданих порогового рівня T_n або вище порогового рівня T_v , відповідно. Ці два види міграції в подальшому будуть називатись «низькою міграцією» і «високою міграцією». Форма графіків даних функцій міграції може бути скоректована за допомогою підбирання параметрів α та β , внаслідок чого можна буде сприяти чи запобігати міграціям. Дана функція є однаковою по відношенню до ресурсів CPU чи RAM, хоча параметри T_n , T_v , α та β можуть бути різними для цих двох видів ресурсних показників.

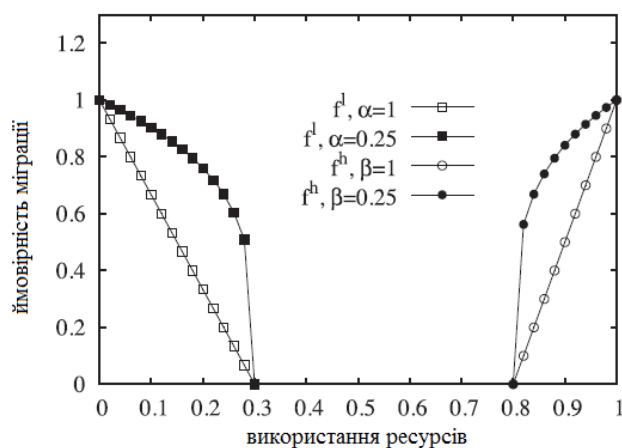


Рис. 4.14. Функції «низької» та «високої» міграції (позначені як f^l та f^h) для двох різних значень параметрів α та β . На цьому рисунку нижній поріг T_n рівний 0.3, а верхній поріг T_e рівний 0.8 [135].

На кожній наступній ітерації процесу підготовки до міграції VM, у випадку коли випробування Бернуллі завершилось успіхом (якщо є віртуальні машини з успішними випробуваннями згідно (4.7)), сервер повинен вибрати віртуальну машину для її міграції. У випадку «високої міграції» і $f_{мігр} > 0$ серверна система фокусується на перевикористаному ресурсі (CPU чи RAM) та розглядає віртуальні машини, для яких рівень використання даного ресурсу є вищим, ніж різниця між поточним рівнем використання серверною системою даного ресурсу та його пороговим значенням T_e . Після цього, одна з таких віртуальних машин вибирається випадковим чином для її міграції, оскільки це дозволить зробити меншим за порогове значення T_e рівень використання даного обчислювального ресурсу сервером. У випадку «низької міграції» і $f_{мігр} < 0$ вибір віртуальної машини для її міграції є цілком випадковим.

Процес вибору нової серверної системи гіпервізором сервісної мережної платформи, на якій розміщуватиметься віртуальна машина, що мігрує, подібний до процесу вибору віртуальної машини в процедурі призначення, лише з двома суттєвими відмінностями. Перша відмінність стосується випадку «високої міграції» в зв'язку з перевантаженням ресурсів і полягає в тому, що пороговий рівень T_e функції призначення встановлюється в значення, рівне $T_e = 0.9$ від рівня використання обчислювального ресурсу сервером, який ініціює процедуру міграції, і розсилається всім іншим серверам разом із запрошенням прийняти на обслуговування віртуальну машину. Це гарантує те, що віртуальна

машина мігрує до менш завантаженого сервера, а також дозволить уникнути багаторазових міграцій однієї і тієї ж віртуальної машини. Друга особливість стосується випадку «низької міграції». Коли немає сервера для обслуговування віртуальної машини, що мігрує, буде неприйнятним вмикати новий сервер для розміщення її на ньому – оскільки недоречно вмикати новий сервер для того, щоб інший сервер перевести в режим глибокого сну. В зв'язку з цим при «низькій міграції», коли немає іншого працюючого сервера для міграції, міграція віртуальної машини не відбувається взагалі.

Схему реалізації процедури міграції віртуальної машини представлено на рис. 4.15.

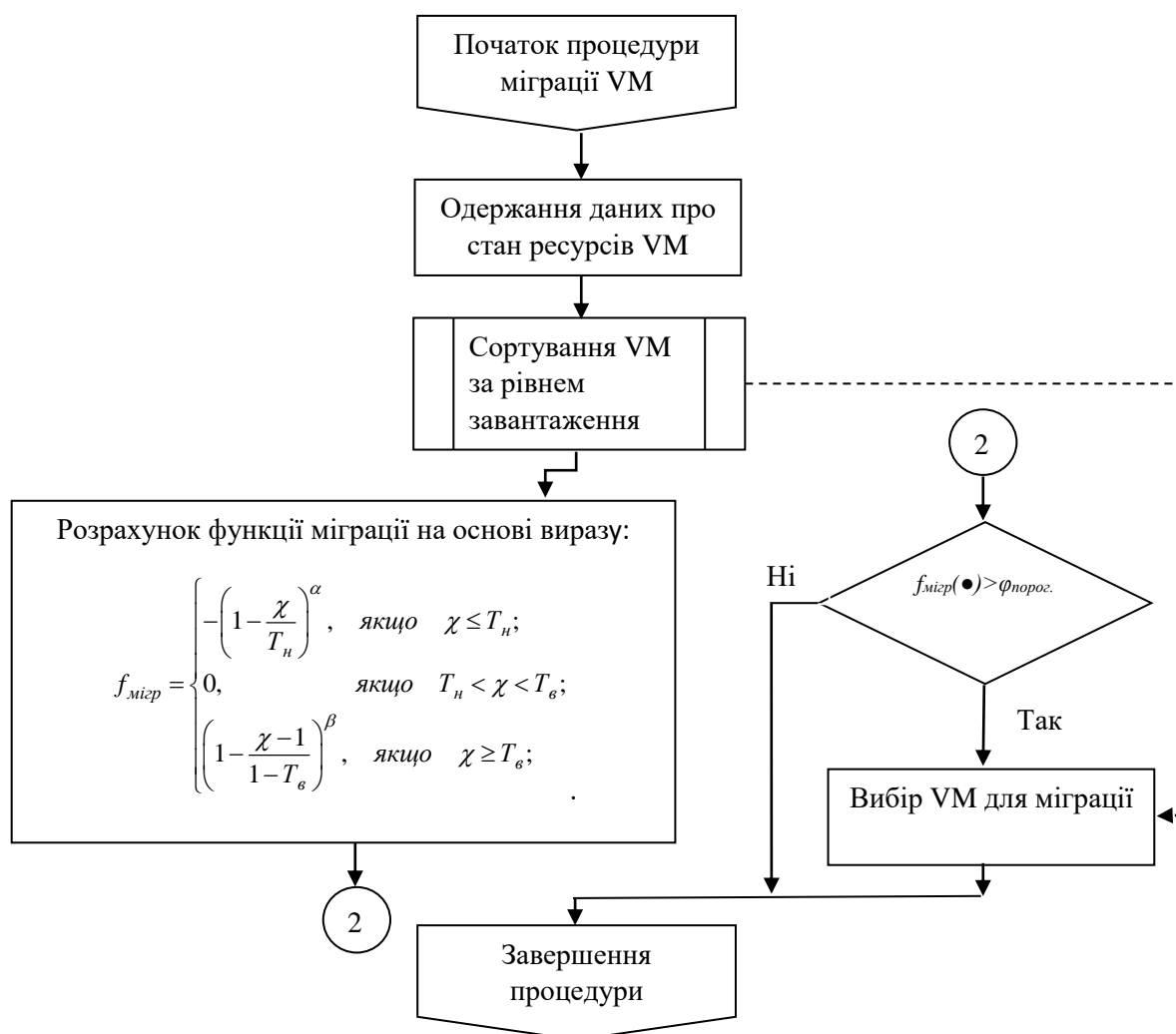


Рис. 4.15. Схema реалізації процедури міграції віртуальної машини: α , β – коефіцієнти вибору стратегії міграції, T_n , T_ϵ – нижній та верхній пороги використання ресурсів для ініціації процедури міграції віртуальної машини, відповідно, χ - відносний рівень використання ресурсу.

Варто відзначити, що запропонований підхід забезпечує поступовий та безперервний процес адаптивної міграції, в той час, як більшість інших нещодавно запропонованих методів міграції вимагають одночасної міграції великої кількості віртуальних машин.

Порогові значення, як правило, можуть задаватись адміністратором сервісної мережної системи, на основі попереднього аналізу показників дисперсії завантаженості віртуальних машин. Параметри форми залежностей рис. 4.12-4.14 дозволяють адміністратору сервісної мережної системи обирати між різними стратегіями консолідації (наприклад, консервативною, проміжною, агресивною). Більш агресивна стратегія дозволить перевести в режим сну більшу кількість серверів, водночас спричиняючи більший кількості міграцій. Вибір потрібної стратегії проводиться шляхом підбору значень параметрів залежностей рис. 4.12-4.14. Оскільки подальший аналіз стратегій консолідації дещо виходить за рамки даної дисертаційної роботи, представлені значення параметрів наведених залежностей відповідають проміжній стратегії консолідації. Очевидно, що для умов більш високої динаміки змін навантаження користувачів слід обирати більш агресивну стратегію консолідації віртуальних машин, а для випадку більшої динаміки просторової міграції користувачів відносно хмарної сервісної платформи, більш оптимальною стає стратегія міграції VM, що наближається до консервативної.

4.6. Висновки до 4-го розділу.

1. В даному розділі виконано чисельне дослідження сервісної доступності розподіленої сервісної платформи, що працює у стаціонарному режимі. На основі одержаних результатів можливо виконувати ефективний синтез конфігурацій масштабованих хмарних сервісних систем із урахуванням типу та величини навантаження, що потребує обслуговування в рамках вибудовування відповідного сервісу з комбінуванням паралельних та послідовних

елементарних сервісних компонентів задля досягнення найкращих показників продуктивності та системної працездатності (рівня сервісної доступності).

З урахуванням закону Амдала (рис. 3.33, крива 60% паралельності обробників) можна також постулювати, що кластеризація хмарних систем може досягати найбільшої ефективності для масштабу кластера близько 100 сервісних вузлів, що узгоджується з результатами моделювання сервісної доступності розподіленої сервісної платформи (рис. 4.1). Проте, збільшення розміру кластера хмарної платформи призведе до необхідності вдосконалення методів управління потоками, зокрема застосування модифікованих методів підвищення доступності її телекомунікаційних вузлів, наприклад шляхом структурно-генного динамічного балансування (див. розділ 5.1).

2. Загалом, у даній дисертаційній роботі була запропонована математична модель оптимального процесу синтезу для побудови:

- Структури програмного коду обробників сервісної мережної платформи з оптимізацією компонентної (функціонально-модульної) доступності та коефіцієнту системної продуктивності при їх розпаралеленні в рамках реалізації SaaS архітектури, зокрема при вибудовуванні балансуванням послідовно-паралельних ланок логіки процесів оброблення користувацького навантаження на основі деякої підпорядкованої платформи, як сервісу; співвідношення 60% розпаралеленої компоненти програмного коду до 40% його послідовної компоненти є не випадковим і характеризує оптимальну структурну композицію системних програмних модулів у рамках побудови SaaS модельної реалізації деякої сервісної мережної системи за критеріями системної продуктивності та сервісної доступності (див. Додаток Б);

- Системної конфігурації PaaS в рамках оптимізації її структурних та параметричних показників за критеріями системної продуктивності та сервісної доступності шляхом конфігурування розпаралелених сегментів множини віртуальних машин у процесі їх міграції серверними вузлами сервісної мережної платформи;

•Реалізації IaaS мережної архітектури за критеріями доступності мережних інтерфейсів телекомунікаційної платформи та коефіцієнта її системної продуктивності шляхом композиції множини розпаралелених віртуалізованих елементів активного мережного обладнання (наприклад – віртуальних маршрутизаторів у рамках застосування NFV, див. розділ 6.1 цієї дисертаційної роботи) та його послідовних мережних елементів (наприклад – комутаторів); окремі віртуалізовані маршрутизатори можуть одночасно обслуговувати диференційовані за пріоритетами та типами потоки трафіку.

3. Як правило, перехід між рівнями IaaS та PaaS, а також між рівнями PaaS та SaaS якісно змінює показники функціонування сервісної мережної системи в бік покращення, в тому числі – в умовах її масштабування. Кожна нова мережна реалізація вищого рівня (сервісна надбудова) є покращеною або оптимізованою версією відповідної нижче розташованої мережної платформи.

На базі розгляду запропонованих у розділі підходів, які відповідають заданим обмеженням щодо допустимості розв'язків системи критеріїв оптимального структурно-параметричного синтезу, а саме, приймаючи до уваги застосування закону Амдала для опису системної продуктивності з одної сторони, а також результати моделювання змін сервісної доступності системи розпаралелених сервісних обробників з іншої сторони, можливо прийти до висновків, що досягається підвищення ефективності реалізацій IaaS, PaaS та SaaS сервісних архітектурних моделей за вищезгаданими критеріями для заданого набору вхідних параметрів навантаження, з урахуванням можливостей застосування сучасного NFV підходу.

4. Підвищення функціональної стійкості архітектури телекомунікаційних сервісних платформ до зловмисних зовнішніх впливів на їх функціональну стабільність дозволить нівелювати наслідки від застосування мережних атак, а саме зниження кількості працездатних сервісних вузлів і, відповідно, обсягів загальних ефективних обчислювальних потужностей, а отже – запобігти критичному зниженню рівня сервісної доступності (див. рис. 3.33, 4.1).

Тому, розвиток мережних екранів, систем виявлення та запобігання функціональним втручанням у сервісні мережні платформи, а також об'єднаних систем виявлення функціональних втручань набуває все більшого значення у сучасному світі різноманітних інформаційних загроз. Такі підходи необхідно застосовувати при реалізації концепцій NFC та IoT (Internet of Things).

Мережні екрани та системи виявлення функціональних втручань поєднують основні гетерогенні мережні рішення глобальної інформаційної інфраструктури (LAN, WLAN, 2G-4G-LTE, NFC та Bluetooth) з можливістю об'єднання існуючих засобів мережної безпеки для запобігання внутрішнім та зовнішнім втручанням задля зниження загроз функціональній стійкості відповідних сервісних мережних систем. У даному розділі дисертаційної роботи виконано порівняння сучасних засобів мережної безпеки, враховуючи об'єднані системи виявлення функціональних втручань, за перспективами їх розвитку та удосконалення. Можна зробити узагальнення про те, що методи ухвалення та імплементації рішень для систем виявлення функціональних втручань вимагають подальшого вивчення.

5. У розділі обґрунтовано та розроблено концептуальні основи для архітектурної реалізації методу мігруючого мережного екрану та описано загальний алгоритм його функціонування. Будучи комплексною системою запобігання функціональним втручанням різного роду та складності, таке рішення може виступати у якості конкурентної багат шарової платформи для підтримування функціональної стійкості масштабованих сервісних мережних систем. Механізми захисту мігруючого мережного екрану розглянуто із використанням визначень семантичної інформаційної (PoIP) та технічної міжоператорської присутності (PoP).

6. Запропоновано структурно-параметричний підхід до оптимальної консолідації віртуальних машин на основі балансування кількох ресурсних параметрів серверних систем розподіленої мережної платформи, що, з одного боку, дозволяє підвищити енергоефективність хмарних центрів оброблення даних, а з іншого боку – їх адаптованість до динамічних змін навантаження на

сервісні застосування з боку користувачів, як просторово-номадичних, так і рухомих категорій.

Для оцінювання ефективності використання ресурсів розподіленої сервісної платформи пропонується застосування двох взаємодоповнюючих напрямів досліджень. Перший напрямок пропонує аналітичне моделювання для вивчення еволюції сервісної мережної системи протягом певного періоду часу, а другий – орієнтується на експерименти, які виконуються на основі реальних ЦОД сервісних мережних систем. Одержані залежності дозволяють визначити особливості структурно-параметричного конфігурування віртуальних машин в процесі їх динамічної міграції/реплікації або призначення в межах хмарних сервісних платформ з метою досягнення енергоефективності та дотримання належного рівня якості функціонування комплексних сервісних застосувань, що надаються, в умовах динамічних змін конфігурацій їх елементарних сервісних компонентів та флуктуацій користувацького навантаження. Запропоновано схеми реалізації процедур реплікації (призначення) та міграції віртуальних машин в заданих умовах функціонування телекомунікаційної сервісної платформи на рівні PaaS.

РОЗДІЛ 5

Розроблення методів оптимізації конвергованих ресурсів мережно-залежних рівнів гетерогенних розподілених сервісних систем

5.1. Розроблення методу динамічної корекції маршрутних метрик шляхом наскрізного структурного трасування.

Висловимо гіпотезу про те, що алгоритмічна реалізація методу [161] в процесі управління потоками буде ефективною для масштабованих та високонавантажених потоками запитів сервісних мережних систем. Очевидно, що будь-яка хмарна система володіє зовнішніми мережними інтерфейсами для обслуговування множини користувачів або взаємопід'єднання до інших мереж. Граничні маршрутизатори (Border gateways), як правило, реалізовані за підтримки Border Gateway Protocol (BGP). Враховуючи результати досліджень надійності маршрутизації, апаратних відмов, відмов ліній зв'язку транспортної телекомунікаційної підсистеми та проблем у роботі самого протоколу BGP, ми можемо розглядати невірне конфігурування маршрутизаторів та відмови BGP у якості домінуючих причин недоступності хмарних систем [187, 190]. Таким чином, використання відмовостійких підходів до конфігурування та підтримування BGP маршрутизації значно покращує хмарну доступність. На сьогодні якість телекомунікаційних засобів дозволяє не розглядати фізичні властивості елементів розподілених платформ надання сервісів. Власне, протокол маршрутизації BGP часто класифікується як протокол «вектора шляху», але інколи його розглядають також, як дистанційно-векторний. Оскільки він широко використовується для обслуговування потоків користувачів як всередині, так і зовні хмарної системи, повільна реакція на реструктуризацію мережі та відмови її елементів, а також, як наслідок, нестабільність логіки надання сервісів мають значний вплив на системну працездатність (робастність) та продуктивність. Подібний вплив має також його реакція на зміни у обсягах навантаження та структурі самої сервісної платформи [152, 186, 225, 229, 231].

Можна зробити висновок, що розроблення та імплементація методу, який забезпечує найбільш оперативне визначення структурних змін, а отже – і відмов мережних елементів, а також флуктуацій обсягів трафіку в системі, що призводять до його дизбалансування, - є логічним кроком до розвитку хмарних технологій. Це дозволяє уникнути надлишкового завантаження деяких вузлів хмарної сервісної системи, а отже – їх недоступності.

Для моделювання роботи алгоритму було визначено та формалізовано розподілену мережну систему з метою ефективного вирівнювання навантаження на сервісні вузли. Застосовано відомі алгоритми визначення внутрішніх та зовнішніх граней графу мережної системи [191]. В результаті, всі граничні вузли увійшли до відповідних множин вершин, причому вершини зовнішніх граней були виділені окремо для відділення внутрішніх системних неоднорідностей. Відзначимо, що вхідними даними для коректної роботи алгоритмів [191] є застосування планарного графу, зведення до якого можливо виконати на основі результатів, як отримано у [192]. Після таких дій, можливо встановити вагові коефіцієнти маршрутних метрик всередині хмарної мережної системи рівними 1.0 ($w = 1$) [224].

Таким чином, отримуємо множини вершин, які належать кожному з периметрів (або границь) хмарної мережної системи. Внутрішні грані (периметри) є структурно неоднорідними. Також вузли, що належать до внутрішніх границь системи є найближчими до ядра хмарної платформи та основних компонентів сервісів, які вона надає. Іншими словами, ці вузли найбільше піддаються перевантаженням або структурним змінам. Очевидно, що вузли, які належать до зовнішніх границь системи є об'єктами складних методів управління потоками, оскільки працюють, як шлюзи. Таким чином, існує можливість виникнення потенційно невикористаних мережних ресурсів, що мають бути розміщені між внутрішніми та зовнішніми границями хмарної системи. Відповідно, деякі обсяги потокового трафіку та сервісних компонентів можуть бути перенесені або піддаватись міграції від більш завантажених до менш завантажених сервісних вузлів. У випадку, коли виявляється аномальне

завантаження в структурі сервісної мережної системи у вузлах, що не належать її границям, для прикладу, внаслідок серйозних змін у логіці надання сервісів або відмов елементів мережної структури платформи надання сервісів, відповідні сервісні потоки також повинні мігрувати.

Приймаючи описану вище гіпотезу, для модельованої хмарної системи було обрано доступну вершину на зовнішній грані її графу. Після цього було застосовано наскрізне маршрутне трасування за принципом наступного стрибка в напрямі, що є протилежним до початкового вузла, який відповідає обраній вершині. Процес маршрутного трасування тривав, допоки не був досягнутий вузол, що належить зовнішній або внутрішній границі хмарної платформи.

В результаті цього, ми фіксуємо проходження за маршрутом R та його довжину L . Знаючи маршрут який було пройдено, зафіксувавши параметри завантаженості відповідних вузлів та каналів зв'язку, а також використовуючи його у зворотному напрямі, ми повертаємось назад до початкового вузла та одночасно коректуємо вагові коефіцієнти маршрутних метрик W у відповідних вузлах, які входили до складу останнього пройденого маршруту R , використовуючи метод модифікованого ковзного середнього з L , в якості довжини пройденого маршруту:

$$w_{new}^k = \begin{cases} \frac{2/L \times |L/2 - k| + (n-1) \cdot w_{old}^k}{n}, & \sum_{i=2}^{\lceil L/2 \rceil} (w_{old}^i - w_{old}^{i-1}) + \sum_{i=\lceil L/2 \rceil+1}^L (w_{old}^{i-1} - w_{old}^i) \leq \varepsilon; \\ \frac{(1 - (2/L \times |L/2 - k|)) + (n-1) \cdot w_{old}^k}{n}, & \sum_{i=2}^{\lceil L/2 \rceil} (w_{old}^i - w_{old}^{i-1}) + \sum_{i=\lceil L/2 \rceil+1}^L (w_{old}^{i-1} - w_{old}^i) > \varepsilon, \end{cases} \quad (5.1)$$

де k - є послідовним номером вузла у маршруті R ; w_{new}^k - є модифікованим ваговим коефіцієнтом відповідної маршрутної метрики; w_{old}^k - є його попереднім значенням; n - прийнято в якості значення згладжуючого інтервалу (встановлене рівним 3); ε - є пороговим значенням для процесу наскрізного

структурного маршрутного трасування (для моделювання прийнято значення 0,4) [161, 224].

5.2. Моделювання процесів гіперагрегації трафіку у транспортних платформах сервісних мережних систем.

Відзначимо, що алгоритмом маршрутизації інформаційних потоків передбачається, що кращий маршрут повинен мати меншу маршрутну метрику. Після повного виконання описаного циклу, який може бути реалізований централізованою імплементацією алгоритму, що схематично представлений на рис. 5.1, відбувається неперервне повернення на його початок і процес повторюється для іншого початкового вузла. Після деякої кількості ітерацій загальний структурний розподіл потоків у графі буде оптимізуватись у відповідності до оперативного балансування навантаження та структурних особливостей хмарної мережної платформи згідно системи співвідношень (5.1).



Рис. 5.1. Алгоритм коректування вагових коефіцієнтів маршрутних метрик для балансування сервісного навантаження за допомогою наскрізного структурного трасування в хмарній мережній платформі.

Моделювана хмарна мережна система досліджувалась із використанням системи MATLAB, а також засобів середовища Qt5.2 у двох варіантах

масштабу – для 50 та 100 сервісних вузлів. Результати моделювання представлено на рис. 5.2 а та рис. 5.2 б, відповідно.

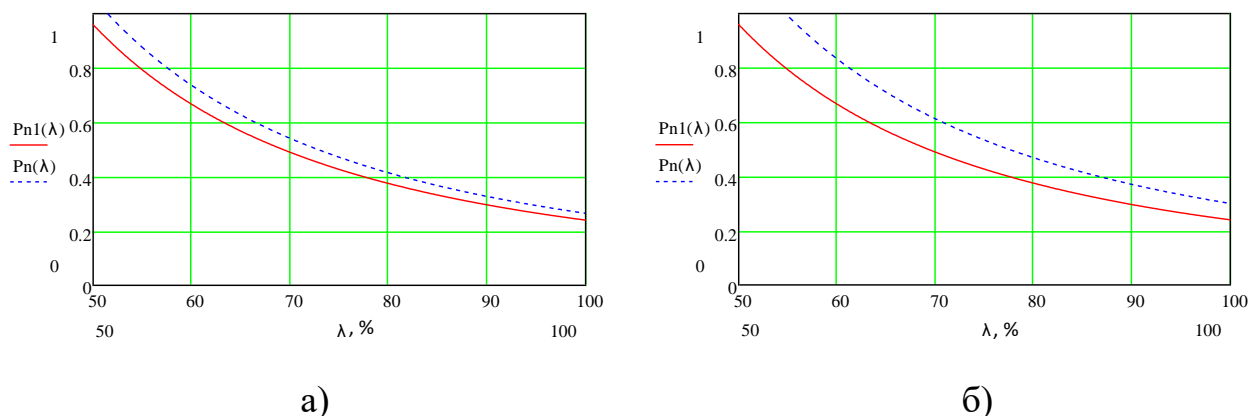


Рис. 5.2. Результати комп’ютерного моделювання ефективності застосування алгоритму динамічної корекції маршрутних метрик шляхом наскрізного структурного трасування в хмарній мережній платформі з а) 50 та б) 100 сервісними вузлами.

На рис. 5.2. λ – відносьне навантаження хмарної платформи у відсотках до максимального, P_n – доступність вузла телекомунікаційної хмарної платформи з дистанційно-векторною маршрутизацією, P_{n1} - доступність вузла телекомунікаційної хмарної платформи за умови застосування запропонованого алгоритму [224].

Як можна бачити з рис. 5.2, застосування запропонованого підходу та алгоритму пропонує нам оперативно і динамічно визначати структурно-топологічні зміни в хмарній сервісній платформі, а це, в свою чергу, дозволяє покращити балансування навантаження в сервісних вузлах, виконуючи плавну міграцію основних інформаційних потоків та, відповідно, сервісних компонентів за межі областей мережної системи із високим завантаженням і структурними неоднорідностями. Доступність сервісних вузлів у телекомунікаційній платформі підвищується до 4% у масштабі хмарної платформи в рамках 50 сервісних вузлів, при цьому динаміка покращення зростає до 10% у масштабі хмарної мережної платформи в рамках 100 сервісних вузлів [224, 229, 231].

5.3. Оптимізація протоколів маршрутизації та призначення мережних ресурсів на основі застосування методів нечіткої логіки за критеріями якості сервісу (приклад оптимізації процесів вертикального хендвера в гетерогенних безпроводних мережах).

На сьогодні розвиток телекомунікаційних рішень приводить до конвергенції різних мережних систем та методів мережного управління, відбувається стрімке зростання кількості технологій доступу, аналогічне зростання кількості мережних терміналів, які орієнтовані на широкі можливості отримання мережних послуг та електронних сервісів різного виду. В найближчій перспективі відбудеться інтеграція окремих мережних технологій в рамках єдиної гетерогенної мережної системи, більшість сегментів доступу якої будуть безпроводними [92, 126]. Сегменти цієї мережі поєднують різні мережні технології єдиною телекомунікаційною сервісною платформою, а кожна з окремо взятих систем працює на досягнення спільної мети – прокращення показників обслуговування користувачів у деякій зоні покриття. При цьому зони покриття різних безпроводних телекомунікаційних технологій перекриваються, створюючи можливості пошуку альтернативних способів підключення та одержання сервісів для мережних користувачів. Це дозволяє підвищити пропускну спроможність, якість сервісів, які надаються користувачам у якомога більшій зоні мережного покриття, знижуючи собівартість відповідних мережних послуг. У гетерогенних мережних системах наступного покоління, що підтримують мультисервісні та мультистандартні користувацькі термінали існуватиме можливість одержання доступу до мережної інфраструктури різних мережних операторів/провайдерів. У таких умовах постає необхідність підтримування гнучкої користувацької мобільності (зокрема в рамках реалізації концепції повсюдного комп'ютингу), що може бути забезпечена інтелектуальним вертикальним хендвером – технологією безперервного підтримування та передачі з'єднань на обслуговування від одної телекомунікаційної системи до іншої, використовуючи доступні мережні ресурси (див. рис. 5.3). Оптимізація процесів перемикання між такими

мережними системами може здійснюватись на підставі цілого набору критеріїв, що описують якість сервісу (QoS): мережної затримки, джиттеру, показників втрат пакетів (PER), пропускної спроможності мережної системи; QoE; пріоритетності обслуговування користувачів, швидкості їх переміщення, типу сервісу, рівня сигналу кожної окремо взятої мережі доступу, поєднання яких у процесі функціонування гетерогенної мережної платформи за деякими алгоритмами може суттєво впливати на якість мережних послуг для кінцевих користувачів та рівень їх задоволеності, а також на ефективність розподілу мережних ресурсів.

5.3.1. Метод інтелектуального вертикального хендовера на основі гетерогенної телекомунікаційної платформи.

Зростання складності телекомунікаційних систем, а також обсягів навантаження безпроводних мереж доступу приводить до інтенсифікації процесів координування їх функціонування в рамках гетерогенної телекомунікаційної платформи (включно з удосконаленням протоколів мережної взаємодії), одночасно породжуючи цілу множину нових завдань. Зокрема, до таких завдань відноситься завдання оптимального вибору системи доступу в режимі високого завантаження мережної платформи. Відповідно, метою його розв'язання є підвищення показників QoS безпроводних мережних систем [127] шляхом більш ефективного використання мережних та каналних ресурсів (зокрема, радіоресурсів) гетерогенної телекомунікаційної платформи, а також оптимізації процесів та процедур інтелектуального вертикального хендовера, базуючись на методах нечіткої логіки.

Запропонований у цій дисертаційній роботі підхід, у порівнянні з відомими [193], використовує теорію нечітких множин на основі трикутних нечітких чисел. Теорія нечітких множин є засобом розв'язання завдань з агрегування двозначних (амбівалентних), суб'єктивних та нечітких оцінювальних суджень про стан деякого часткового параметру або показника, що безпосередньо впливає на оптимальний вибір мережної системи доступу.

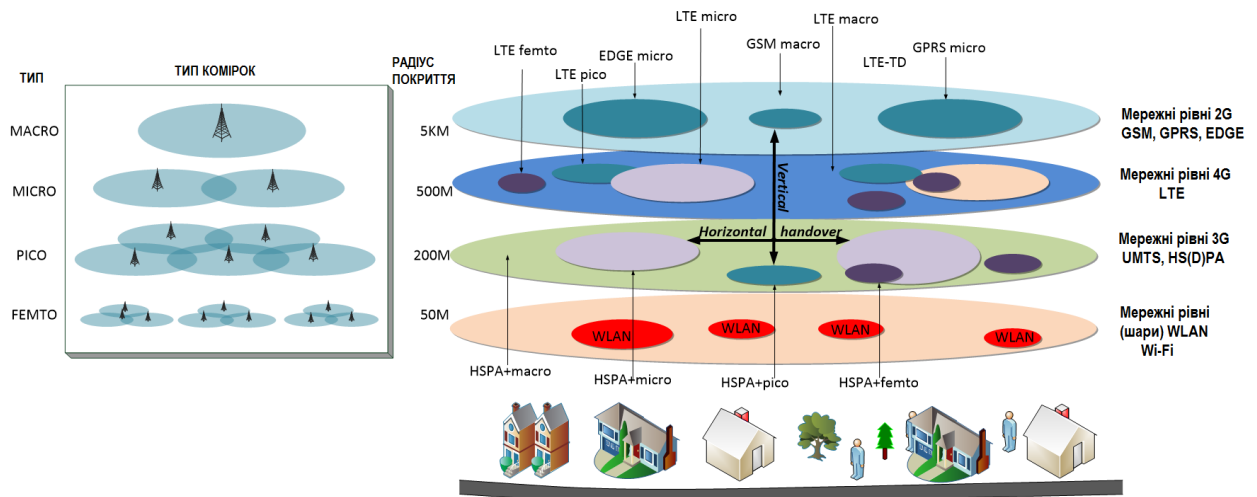


Рис. 5.3. Гетерогенна телекомунікаційна платформа, як взаємопоєднання мереж безпроводного доступу [126].

Використання класичної теорії множин є ускладненим у зв'язку із необхідністю поєднання всіх оцінок в єдиній результуючій, одержання якої за допомогою цих методів подекуди здійснити дуже важко. Більше того, нечіткі множини можуть ділити одержані результати за шкалою, що відповідає лінгвістичним термам, а це також може бути використаним для подальшого прийняття рішення. Використовуючи подібний підхід для побудови математичної моделі процесів призначення мережних ресурсів та, зокрема, вертикального хендовера, останній (підхід) стає кількісним, на відміну від існуючих суб'єктивних оцінювальних методів.

Для того, щоб розв'язати завдання ініціації перерозподілу мережних ресурсів у гетерогенній мережній платформі на основі виконання хендоверу, в цьому розділі роботи запропоновано централізовану реалізацію методів управління хендовером, які можуть опиратися на хмарні сервісні технології з використанням методів нечіткої логіки. Для виконання хендоверу пропонується використання принципів розпаралелювання обчислень на основі обраних кластерів сервісних мережних систем. Кожний інфокомунікаційний оператор може визначити відповідний кластер системи для цілей взаємointegraції у

єдиній гетерогенній мережній платформі. Іншим шляхом є використання сервісних моделей хмарних обчислювальних систем, їх взаємоп'єднання, а також розроблення власного системного програмного забезпечення та його запуск і підтримка на основі об'єднаної хмарної інфраструктури.

Це дозволить мережним операторам уникати значного зростання капітальних витрат вже у найближчому майбутньому. Такий підхід визначається необхідністю застосування складних методів передбачення та опрацювання для оптимального вибору обслуговуючої мережної системи і прийняття рішення щодо процедури хендовера, що може вимагати більшої тривалості оброблення, зважаючи на рівень обчислювальної продуктивності мережної системи та архітектуру програмного забезпечення. Зрозуміло, що рівень мобільності сучасних користувачів висуває критерій часу оброблення подібних запитів для прийняття відповідного рішення на перший план. Коли користувачі рухаються з вищою швидкістю і мають при цьому, для прикладу, активні мультимедійні сесії, надто висока тривалість обчислень для прийняття рішення про перерозподіл ресурсів мережно-залежних рівнів у гетерогенній платформі буде призводити до потенційного переривання сесій зв'язку, а також проблематичності щодо спроб їх відновлення. Використовуючи можливості та засоби хмарних сервісних платформ, можливо проводити подібні розрахунки в межах кількох мілісекунд та забезпечувати оптимальний вибір мережної системи для хендоверу в рамках, відповідно, перерозподілу загальносистемних ресурсів [194, 232].

Тому автором запропоновано алгоритм інтелектуального вертикального хендовера згідно рис. 5.4. Для його реалізації було встановлено необхідне програмне забезпечення на серверному кластері, що керує процесами ресурсної оптимізації (вертикального хендовера), які представлено на рис. 5.3.

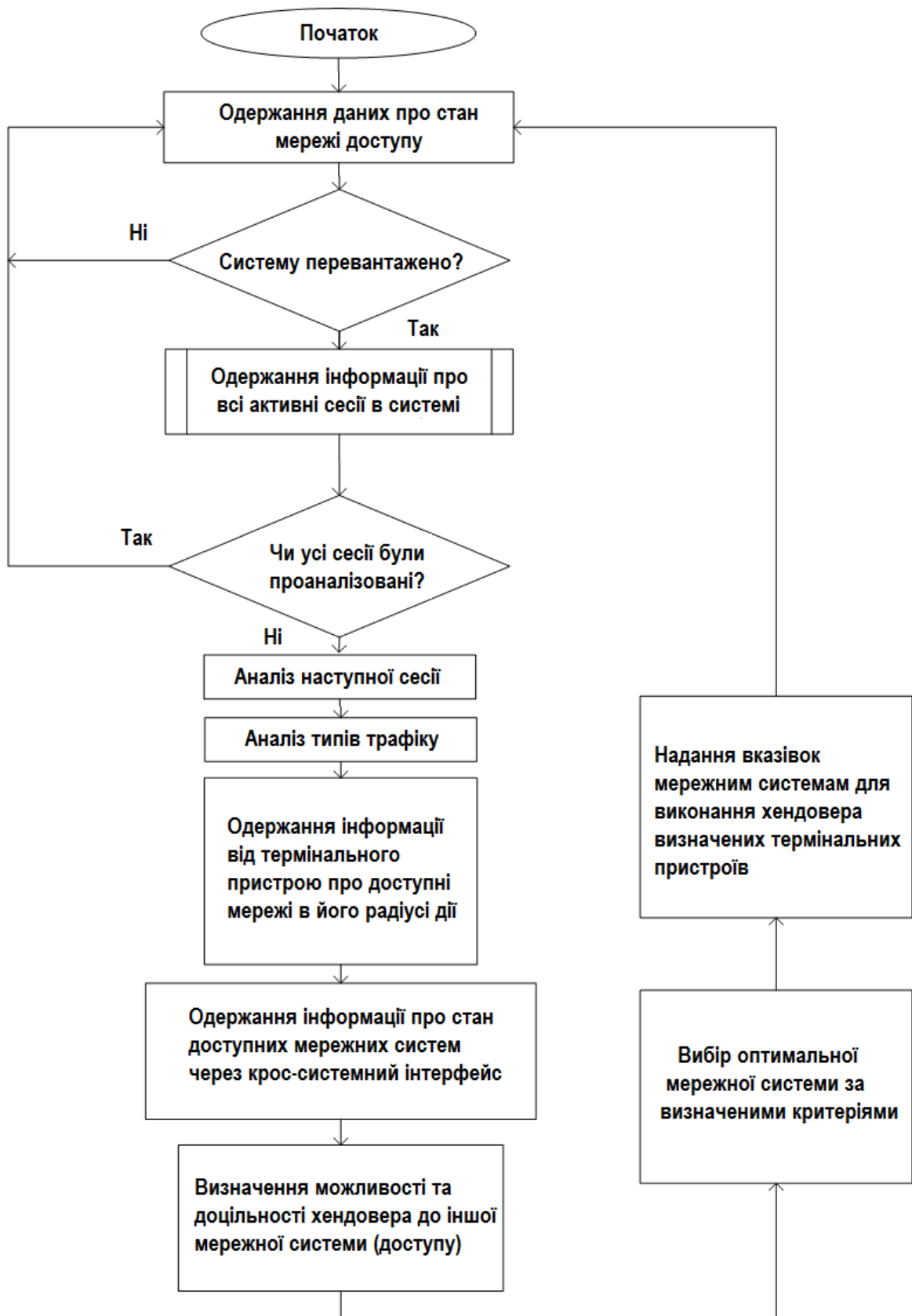


Рис. 5.4. Алгоритм ініціації перерозподілу ресурсів мережно-залежних рівнів на основі технології інтелектуального вертикального хендвера [232].

5.3.2. Багатокритерійний алгоритм вертикального хендовера користувачького навантаження.

Розглянемо основні типи трафіку та критерії хендовера. Рис. 5.5 описує різні типи трафіку та декілька обраних критеріїв хендовера, що використовуються у якості вхідних даних для цілої множини алгоритмів вертикального хендовера [195]. Ці критерії подано нижче:

Потужність прийнятого радіосигналу (RSS). Критерій є доволі простим у розумінні, впливає з відповідної фізичної величини, а також широко використовується для випадків горизонтального та вертикального хендовера. Його можливо легко визначити шляхом вимірювання рівня радіосигналу та співставлення його з еталоном. RSS безпосередньо впливає на QoS сервісних застосувань. Його значення є обернено-пропорційними до відстані між користуваьким терміналом та точкою безпроводного доступу, що аналізується. Флуктуації RSS можуть провокувати надмірну та/або недоцільну кількість реконфігурацій мережних ресурсів шляхом застосування процедур хендовера.

Доступна пропускна спроможність. Вимірюється у біт/с. Доступна пропускна спроможність використовується для визначення умов завантаження трафіком деякої мережної системи доступу, а також доволі точно описує своїм показником доступні мережні ресурси базової станції.

Тривалість мережних під'єднань. Це тривалість під'єднання термінального обладнання користувачів до відповідної мережі доступу. Вона залежить від розміщення та швидкості переміщення користувачького обладнання, що, в свою чергу, впливає на зміну показників RSS. Внаслідок різної площі покриття окремих систем доступу, об'єднаних гетерогенною безпроводною мережною платформою, оцінювання даного критерію є дуже важливим з метою: а) визначення умов перемикавання, досягнення яких вказує на необхідність хендовера, причому настільки вчасно, щоб уникнути погіршення показника QoS при обслуговуванні користувачів, а також неефективного використання (марнування) мережних ресурсів; б) зменшення кількості невдалих завершень процесів хендовера. Для прикладу, надто поспішний

хендовер від IEEE 802.11 WLAN до 3G безпроводної мережі [196] призведе до марнування значної кількості мережних ресурсів, які мають потенціал до використання. З іншого боку, затримки у хендовері між цими мережними системами призведуть до перебоїв у сеансі зв'язку, тому хендовер завершиться невдало. Очевидно, що такі статистичні показники, як середній час підключення до визначеної мережної системи доступу або середній час перемикавання (передачі) до неї на обслуговування деякого сеансу зв'язку можуть також бути використані в якості критеріїв для прийняття рішень щодо процедури хендовера.



Рис. 5.5. Типи трафіку та критерії прийняття рішень щодо хендовера.

Вартість. Користувачі можуть використовувати мережі доступу різних операторів у рамках єдиної гетерогенної мережної платформи, причому вартість послуг у таких мережах може різнитися. Тому, перевагу при хендовері слід надавати мережам, у яких вартість послуг є нижчою.

Параметри обслуговування трафіку. Для користувацького обладнання параметри обслуговування трафіку визначаються, як тривалість часового інтервалу між одержанням останнього пакету трафіку даних від старої мережі доступу і одержанням першого пакету трафіку даних від новопризначеної

мережі доступу після успішного виконання хендвера. Значення цього критерію суттєво коливаються для різних безпроводних технологій в межах гетерогенної мережної платформи.

Безпека. Деякі сервісні застосування вимагають захисту конфіденційності даних, що передаються та/або їх цілісності.

Споживана потужність. Процеси хендвера вимагають додаткових витрат енергії як для мережної платформи, так і для термінального обладнання користувача. Таким чином, якщо термінальне обладнання використовує джерело живлення з обмеженим запасом енергії, то перевага при хендвері надається мережним системам, які дозволять збільшити час роботи пристрою на одному заряді батареї.

Рівень мобільності користувача. Даний критерій є важливим фактором при прийнятті рішення щодо хендвера, оскільки від нього залежить час роботи користувача у межах покриття деякою безпроводною мережею доступу. Якщо користувач зазнає швидкого переміщення, то це може призвести до великої кількості надто поспішних хендверів між безпроводними мережами.

Для випадку обслуговування деякого кінцевого користувача можливо призначити пріоритетність критеріїв при винесенні рішення щодо виконання процедури хендвера. Порядок пріоритетності критеріїв, згідно запропонованого у даній дисертаційній роботі підходу, є наступним (критерії першого рівня): RSS, QoS, рівень мобільності користувача, мережна завантаженість, безпека, а також вартість; причому показникам RSS та QoS надано однакову пріоритетність, оскільки наша ціль полягає у максимізації рівня задоволеності кінцевого користувача якістю послуг, що надаються. Тим не менше, запропонований підхід передбачає можливість гнучкої пріоритезації, тому для певних категорій кінцевих користувачів зазначена вище пріоритетність критеріїв може зазнати змін. Схему розрахунку вагових коефіцієнтів для всіх чотирьох визначених на рис. 5.5 типів трафіку представлено на рис. 5.6. Таким чином, запропоновано поділити всі параметричні критерії на дві групи: QoS-залежні та такі, що залежать

безпосередньо від властивостей радіоінтерфейсу безпроводної мережної системи.

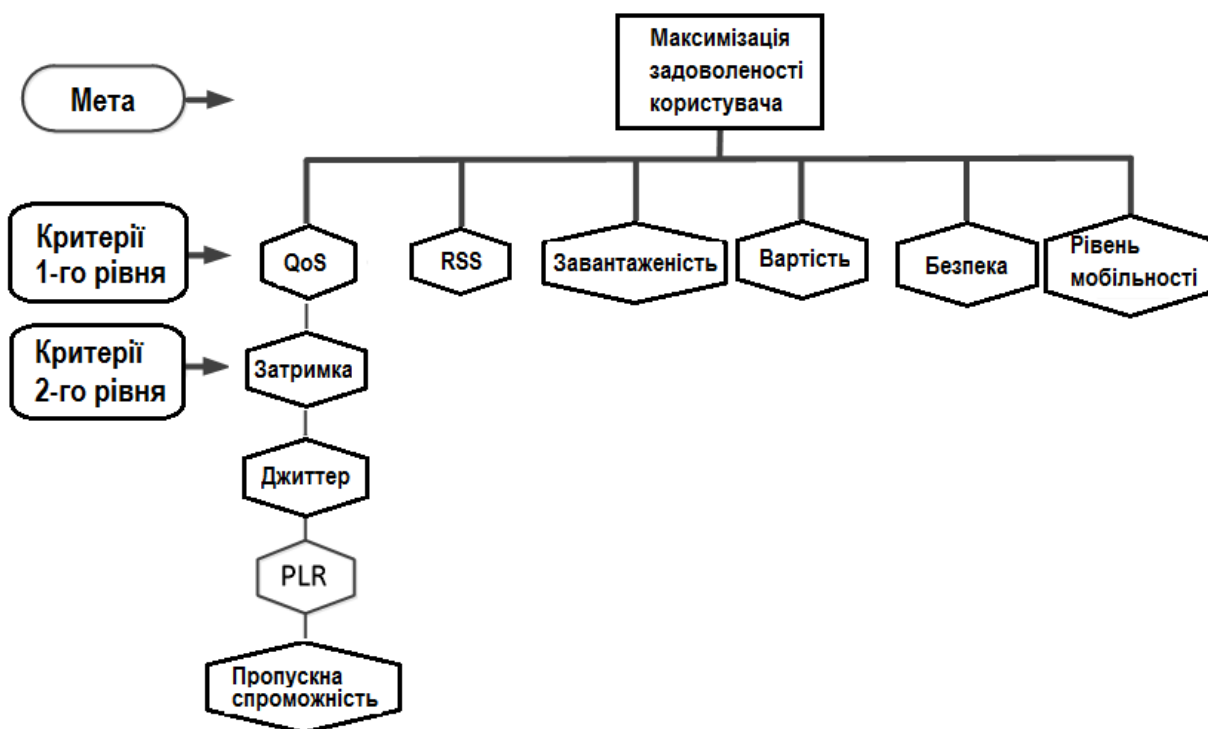


Рис. 5.6. Множина критеріїв для прийняття рішення щодо ініціалізації процесу вертикального хендвера.

Таблиця 5.1. Оцінки критерійних параметрів мережних систем для ініціалізації процесу хендвера за шкалою Лікерта.

Шкала	1	2	3	4	5	Min/Max показники
Завантаженість, [%]	70–100	50–70	40–50	30–40	0–30	0–100
Вартість	1–2	2–3	3–4	4–8	8–10	1–10
Безпека	1–2	2–4	4–6	6–8	8–10	1–10
Рівень мобільності, [км/год]	<120	80–120	60–80	40–60	0–40	0–160
Затримка, [мс]	<300	200–300	100–200	50–100	10–50	10–500
Джиттер, [мс]	<30	20–30	10–20	5–10	1–5	10–30
Коефіцієнт втрат пакетів (PLR), [%]	<8	6–8	4–6	3–4	1–3	1–8
Пропускна здатність, [Мбіт/с]	<0/1	0.1–10	1–50	50–100	100–200	0/1–200
RSS, [dBm]	< -110	-100 – -110	-90 – -100	-75 – -90	-55 – -75	-110 – -55

5.3.3. Моделювання процесу прийняття рішення щодо вертикального хендвера на основі використання нечіткої логіки.

Типова гетерогенна безпроводна мережна платформа забезпечує функціонування різних технологій доступу з різними параметрами та функціональними характеристиками. В загальному ці параметри неможливо порівнювати напряду (див. табл. 5.1). Таким чином, з метою їх нормалізації та агрегування в діапазоні $[0, 1]$ використовуються підходи нечіткої логіки [197].

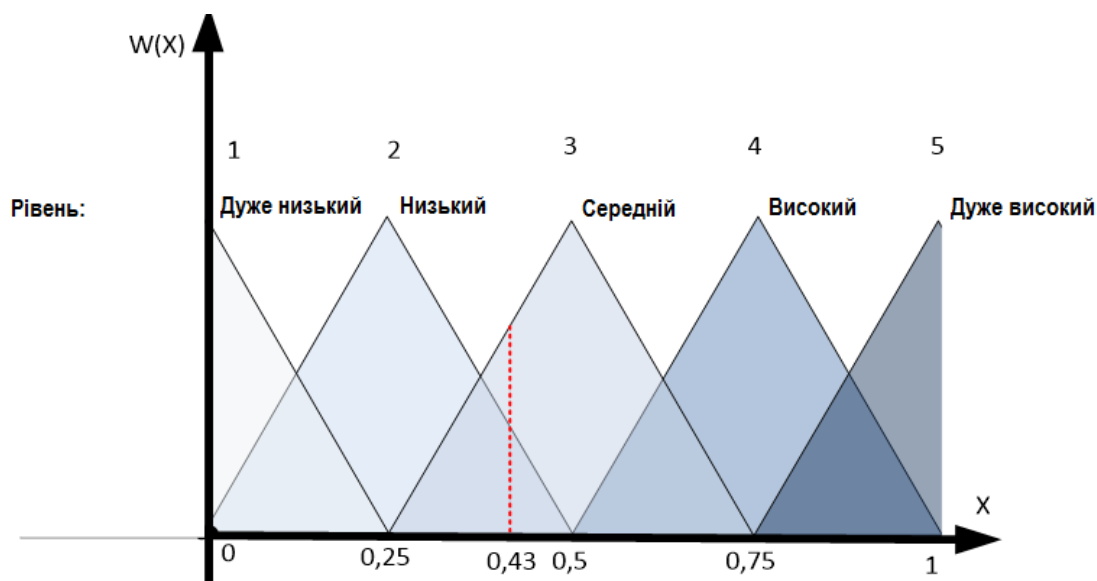


Рис. 5.7. Шкала оцінок та функції належності відповідних лінгвістичних термінів.

Після підготовки параметрів для виконання обчислень з метою прийняття рішення про інтелектуальний вертикальний хендвер, введемо шкалу ваги кожного критерію щодо ініціації хендвера у відповідності до шкали Лікерта (1 – не може бути застосований $(0,0,0.25)$, 2- можливо застосовувати $(0,0.25,0.75)$, 3 – середнього рівня, $(0.25, 0.5, 0.75)$, 4 – варто застосовувати $(0.5,0.75,1)$, 5 – необхідно застосовувати $(0.75,0.75,1)$) з урахуванням оцінок табл. 5.1. В дужках подані відповідні трикутні нечіткі числа. Також введемо п'ятирівневу шкалу лінгвістичних термінів для оцінювання рівня корельованості між відповідними показником стану мережної системи та критерієм (1 – “дуже низький”, 2 – “низький”, 3 – “середній”, 4 – “високий”, 5 – “дуже високий”), що дозволяє провести оцінювання значення рівня відповідного критерійного параметра за шкалою рис. 5.7.

Розглядаючи гетерогенну сервісну мережну систему, вважатимемо, що вона надає сім різновидів сервісу, таких як: передавання голосу (А), відеоконференцзв'язок (В), послуги IPTV (С), передавання даних через Internet (D), передавання інтерактивних даних (Е), передавання мультимедіа на вимогу (VoD)(F), послуги Voice over IP (G) через Internet.

Сформуємо емпіричні коефіцієнти ваги даних сервісів у відповідності до необхідної для задоволення користувачів якості сервісу в процесі забезпечення хендоверу, використовуючи вагові коефіцієнти B_1 , B_2 , B_3 та B_4 , які можуть набувати значень в діапазоні від 1 до 3, причому більше значення коефіцієнта означає більшу вагу заданого параметра якості сервісу для його відповідного виду (категорії послуг) (див. табл. 5.2).

Таблиця 5.2. Види сервісів та відповідні відносні вагові коефіцієнти якісних параметрів трафіку.

Параметри якості Види сервісу	PLR B_1	Затримка B_2	Джитер B_3	Пропускна здатність B_4
Передавання голосу	2	3	3	1
Відеоконференцзв'язок	2	3	3	2
Послуги IPTV	3	2	2	3
Передавання даних через Internet	3	1	1	1
Передавання інтерактивних даних	2	2	1	1
Передавання мультимедіа на вимогу (VoD)	2	2	2	3
Послуги Voice over IP	3	2	1	1

Визначимо також вплив зростання рівня завантаження мережної платформи (кожного її сегмента – безпроводних мереж доступу) на параметри, що визначають вибір відповідної мережної системи в процесі вертикального хендовера. Процес вибору найбільш оптимальної мережної системи буде

відбуватися в рамках взаємодії із системою моніторингу її завантаженості, використовуючи засоби для реалізації хмарних обчислень та методи нечіткої логіки.

Отже, введемо параметр завантаженості в якості коефіцієнта утилізації мережних ресурсів вузла мережної системи, що надає сервіс за деякою безпроводною технологією, а саме вагового коефіцієнта ρ_{mn} , який базується на поточному рівні навантаження вузла, причому m є номером вузла мережної системи доступу, що розміщується в зоні покриття мережної платформи, а n – типом технології безпроводного доступу у вузлі m . Прийmemo, що $n=1$ для технології LTE та $n=2$ для технології GSM. Відповідні вагові коефіцієнти технологічно-залежних параметрів для названих технологій подано у табл. 5.3.

Таблиця 5.3. Вагові коефіцієнти технологічно-залежних параметрів.

Технологія мережного доступу Параметри	GSM T ₁	LTE T ₂
Вартість	1	2
Безпека	1	2
RSS	2	2
Завантаження	2	1
Рівень мобільності користувачів	1	2

Після оцінювання параметрів мережного вузла, як результату процесу збору коефіцієнтів, що характеризують показники QoS (PLR, затримку, джитер, пропускну здатність), визначимо вплив рівня його завантаження по замовчуванню за допомогою вагових коефіцієнтів, які дорівнюють 0.5. Для випадку збільшення ваги параметра при збільшенні ρ_{mn} , вагові коефіцієнти відповідних параметрів з табл. 5.2 розраховуються у відповідності до правил із табл. 5.4 за формулою:

$$w\rho_{imn} = 0.5 + 0.5 \cdot \rho_{mn}, i = 1..4. \quad (5.2)$$

Для випадку зменшення ваги параметра при збільшенні ρ_{mn} , вагові коефіцієнти відповідних параметрів з табл. 5.2 розраховуються у відповідності до правил із табл. 5.4 за формулою:

$$wp_{imn} = 0.5 - 0.5 \cdot \rho_{mn}, i = 1..4, \quad (5.3)$$

де i є індексом QoS-пов'язаного параметру за порядком згідно табл. 5.2 (B_i), який використано у відповідному ваговому коефіцієнті wp_{imn} цього параметра, що, в свою чергу, приймається до уваги у процесі прийняття рішення щодо інтелектуального вертикального хендовера.

Таблиця 5.4. Вплив змін коефіцієнту завантаження мережних вузлів на вагові коефіцієнти їх QoS-пов'язаних параметрів.

Параметр моделі	Зміна завантаження	Зміна ваги
Джитер	Зростання $\rho \uparrow$	Зменшення \downarrow
Вартість	Зростання $\rho \uparrow$	Зростання \uparrow
Безпека	Зростання $\rho \uparrow$	Без змін \leftrightarrow
Рівень мобільності користувачів, [км/год]	Зростання $\rho \uparrow$	Зменшення \uparrow
Затримка, [мс]	Зростання $\rho \uparrow$	Зростання \uparrow
Коефіцієнт втрат пакетів [%]	Зростання $\rho \uparrow$	Зростання \uparrow
Пропускна здатність, [Мбіт/с]	Зростання $\rho \uparrow$	Зменшення \downarrow
RSS, [dbm]	Зростання $\rho \uparrow$	Без змін \leftrightarrow

Нарешті, вагові коефіцієнти w_{imn} одержуємо, як результат перемноження ваг згідно (5.2-5.3), отже ваговий коефіцієнт QoS-пов'язаного параметру для відповідного сервісу:

$$w_{imn} = wp_{imn} B_i, i = 1..4, \quad (5.4)$$

де B_i є ваговим коефіцієнтом QoS-пов'язаного параметру для відповідного типу сервісу, що запитується користувачем (див. табл. 5.2).

Після цього виконується нормалізація коефіцієнта w_{imn} :

$$W_{imn} = \frac{w_{imn}}{\sum_{i=1}^4 w_{imn}}, \quad (5.5)$$

Відповідно, розрахунок трикутних нечітких чисел для агрегованого оцінювання обраного мережного вузла доступу \tilde{Q}_{mn} виконується у відповідності до технології його безпроводної мережної системи, а також згідно оцінок значень критерійних параметрів для прийняття рішення щодо хендвера за шкалою, що наведена в табл. 5.1. Власне, сама процедура хендвера може привести до змін показників QoS для користувача, що обслуговується.

$$\tilde{Q}_{mn} = (q_1, q_2, q_3)_{mn} = \sum_{i=1}^4 (W_{imn} \times \tilde{L}_{imn}) \quad (5.6)$$

$$q_{jmn} = \sum_{i=1}^4 (W_{imn} \times l_{ijmn}) \quad (j=1,2,3; m=1,2,3; n=1,2), \quad (5.7)$$

де q_1, q_2, q_3 є нижнім рівнем узагальненої оцінки \tilde{Q} , її основним значенням та верхнім рівнем, відповідно, $\tilde{L}_{imn} = (l_{i1}, l_{i2}, l_{i3})_{mn}$ - трикутне нечітке число, що характеризує показник параметра мережного вузла за i -им критерієм, причому сам вузол належить безпроводній мережній системі в рамках гетерогенної мережної платформи з порядковим номером m та використовує n -ту технологію доступу (див. табл. 5.3). Тут l_{i1}, l_{i2}, l_{i3} - є нижнім рівнем лінгвістичної змінної, її основним значенням та верхнім рівнем, відповідно до формату трикутних нечітких чисел (Triangular Fuzzy Number [193]), див. шкалу рис. 5.7.

Після розрахунку значень параметрів вузла доступу у процесі оцінювання його ресурсів (для мережно-залежних рівнів) на основі зведення відповідних технічних показників з метою ухвалення оптимального рішення щодо процедури хендвера, при врахуванні поточного стану радіоінтерфейсів, найбільш пріоритетними виступають такі показники (табл. 5.3): RSS, завантаження, безпека, рівень мобільності користувача, вартість. Причому, за замовчуванням, дані параметри наділені ваговими коефіцієнтами, що дорівнюють 0.5.

Для випадку збільшення ваги та збільшення ρ_{mn} , результуюча вага параметра визначається у відповідності до правил табл. 5.4 та (5.2):

$$plp_{kmn} = 0.5 + 0.5 \cdot \rho_{mn} \quad (5.8)$$

Для випадку зменшення ваги та збільшення ρ_{mn} , результуюча вага параметра визначається у відповідності до правил табл. 5.4 та (5.3):

$$plp_{kmn} = 0.5 - 0.5 \cdot \rho_{mn}, \quad (5.9)$$

де k – порядковий номер параметра радіоінтерфейса plp_{kmn} , що приймається до уваги у процесі прийняття рішення щодо вертикального хендовера (див. параметри у табл. 5.3).

Результуюча вага pl_{kmn} одержується як результат перемноження оцінок параметрів, базуючись на даних щодо вагових коефіцієнтів з табл. 5.1 та вагових коефіцієнтів з табл. 5.3 для кожної технології безпроводного доступу:

$$pl_{kmn} = plp_{kmn} T_k, k = 1..5, \quad (5.10)$$

де k – порядковий номер параметра з (5.9), що приймається до уваги у процесі прийняття рішення щодо вертикального хендовера та T_k є ваговим коефіцієнтом для відповідних параметрів обраної технології безпроводного доступу (див. коефіцієнти технологічно-залежних параметрів у табл. 5.3).

Після цього необхідно виконати нормалізацію pl_{kmn} :

$$PL_{kmn} = \frac{pl_{kmn}}{\sum_{i=1}^5 pl_{kmi}}, \quad (5.11)$$

Відповідно, узагальнена оцінка обраного вузла доступу мережної системи \tilde{P}_{mn} розраховується у відповідності до технології, що у ній застосовується та парціальних оцінок параметрів, які базуються на інтерпретації вхідних даних на основі табл. 5.1. Вона якісно характеризуватиме радіоінтерфейс:

$$\tilde{P}_{mn} = (p_1, p_2, p_3)_{mn} = \sum_{i=1}^5 (PL_{kmi} \times \tilde{L}_{kmi}) \quad (5.12)$$

$$p_{jmn} = \sum_{i=1}^5 (PL_{k_{mn}} \times l_{kj_{mn}}), \quad (j=1,2,3; m=1,2,3; n=1,2), \quad (5.13)$$

де P_1, P_2, P_3 є нижнім рівнем узагальненої оцінки \tilde{P} , її основним значенням та верхнім рівнем, відповідно, $\tilde{L}_{k_{mn}} = (l_{k1}, l_{k2}, l_{k3})_{mn}$ трикутне нечітке число, що характеризує показник параметра мережного вузла за k -им критерієм, причому сам вузол належить безпроводній мережній системі в рамках гетерогенної мережної платформи з порядковим номером m та використовує n -ту технологію доступу (див. табл. 5.3). Тут l_{k1}, l_{k2}, l_{k3} є нижнім рівнем лінгвістичної змінної, її основним значенням та верхнім рівнем, відповідно до формату трикутних нечітких чисел (див. шкалу рис. 5.7.).

Агрегована оцінка мережного вузла доступу може бути визначена наступним чином:

$$\begin{aligned} \tilde{R}_{mn} &= (r_{1mn}, r_{2mn}, r_{3mn}) = \frac{1}{2} \times (\tilde{Q}_{mn} + \tilde{P}_{mn}) \\ &= \frac{1}{2} \times (q_{1mn} + p_{1mn}, q_{2mn} + p_{2mn}, q_{3mn} + p_{3mn}). \end{aligned} \quad (5.14)$$

Остаточно, проведемо дефазифікацію одержаного нечіткого (трикутного) числа (5.14) у відповідності до методу [193]:

$$R_{mn} = \frac{1}{3} \times \sum_{t=1}^3 r_{tmn}. \quad (5.15)$$

5.3.4. Моделювання процесів оптимального розподілу ресурсів у гетерогенній мережній платформі безпроводного доступу.

Імітаційне моделювання процесу обслуговування є необхідним розробнику відповідних математичних моделей для перевірки їх адекватності під час протікання процесів, які відбуваються в реальній системі. Найпростіший спосіб визначення характеристик сервісної мережної системи полягає в отриманні експериментальних даних, що стосуються процесу обслуговування. Аналіз отриманих даних дозволяє визначити, які параметри системи обслуговування

повинні бути змінені з метою підвищення якості сервісу, тобто як саме оптимізувати відповідні процеси.

Існуючі сервісні мережні платформи містять велику множину компонентів, причому кожен окремий компонент, як правило, являє собою складну підсистему, яка має свої параметри і характеристики. У загальному випадку, враховуючи системоутворюючі принципи, всі компоненти можуть впливати на системну якість обслуговування. Проте, характер цих впливів є важкопередбачуваним. Саме тому для створення адекватної моделі і проведення адекватної оцінки результатів моделювання необхідно максимально враховувати всі компоненти, які беруть участь в процесі обслуговування навантаження користувачів.

Велика кількість користувачів, сервісних застосувань і сесій, які генеруються цими застосуваннями, в загальному – їх різноманітність справляють значний вплив на характеристики обслуговування трафіку, що надходить у мережну платформу. Таким чином, для того, щоб промоделювати згадані процеси, необхідно застосовувати математичний апарат, який дозволить найбільш точно описати характеристики навантаження та властивості методів його опрацювання. Зрозуміло, що найефективнішим способом моделювання в такій ситуації виступає розроблення спеціалізованого програмного забезпечення.

Використовуючи програмну реалізацію імітаційної моделі, можна реалізувати не тільки всі необхідні функції моделювання, а й забезпечити належний контроль за його процесом. Програмне забезпечення дозволяє використовувати графічний користувацький інтерфейс, динамічно змінювати параметри моделі і, таким чином, оцінювати поведінку системи в конкретній ситуації, що може виникнути в реальній сервісній мережній платформі. Крім того, програмне забезпечення за допомогою графічного інтерфейсу дозволяє в режимі реального часу спостерігати за усіма параметрами моделі, що може виконуватись із використанням графіків, діаграм, списків і таблиць.

Для дослідження процесів функціонування мобільної мережної системи з високим рівнем мобільності користувачів необхідно розробити імітаційну модель з використанням великої кількості параметрів і характеристик, які дозволяють описати існуючі мережні технології, використовуючи, відповідно, математичні, прогностичні і оптимізаційні моделі. Таким чином, в даній роботі розроблено модель гетерогенної мережної платформи безпроводного доступу. Її структуру представлено на рис. 5.8.

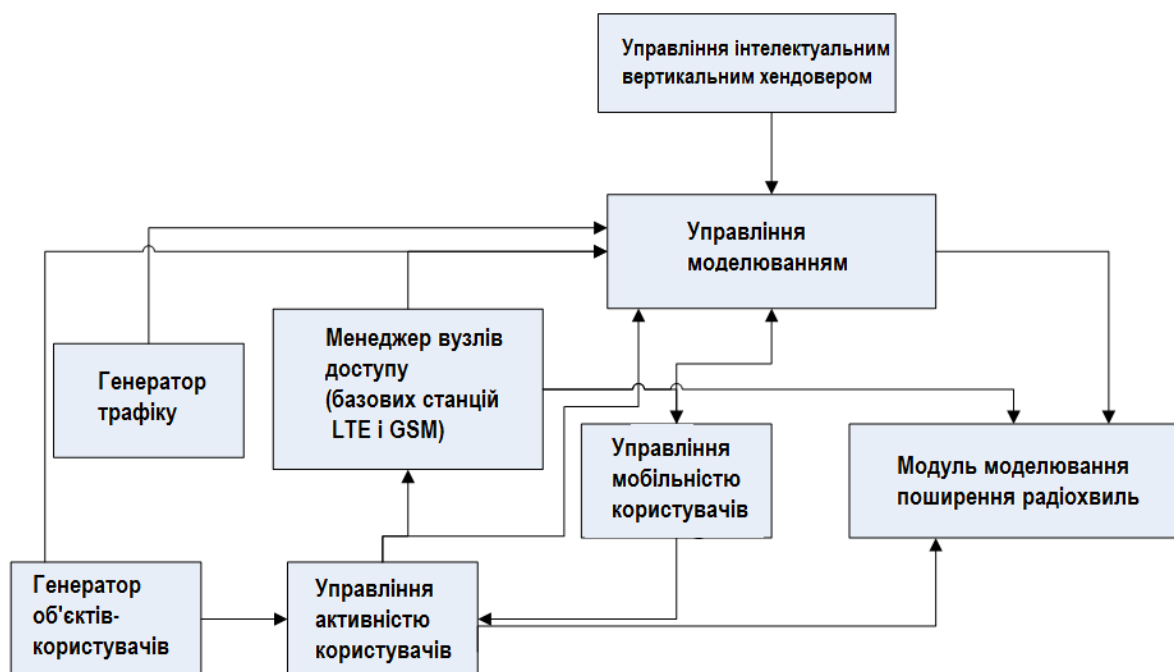


Рис. 5.8. Структурна схема імітаційної моделі гетерогенної мережної платформи безпроводного доступу.

Імітаційна модель містить блок моделювання поведінки користувачів, який включає в себе генерацію трафіку. Сформовані об'єкти-користувачі передаються «менеджеру користувачів». Якщо користувач тільки реєструється в мережі і не має активних сесій, що він відзначається в графічному інтерфейсі моделі, як товста сіра точка. Якщо користувач має активне з'єднання з мережею, тоді він відзначається кольоровою точкою з кольором в залежності від того, до якої мережної системи він підключений до: GSM - зелений колір, LTE - синій колір. Користувач в такій моделі представлений, як об'єкт з набором параметрів, таких як: тривалість активності, вектор руху, швидкість руху, місце перебування, відстань до базових станцій (мережних вузлів

доступу), рівень сигналу від кожної базової станції LTE і GSM (RSS) та інших додаткових параметрів, необхідних для функціонування моделі.

Швидкість переміщення користувача визначається за формулою:

$$V_{SPEED} = \frac{\sqrt{(x_i - x_{i-1})^2 + (y_i - y_{i-1})^2}}{\Delta\tau}, \quad (5.16)$$

Було запропоновано провести класифікацію швидкості користувачів для того, щоб записати зміни рівня сигналу базової станції під час спостереження і проводити прогнозування необхідності передавання обслуговування в іншу комірку на основі результатів прогнозування ймовірності напрямків руху користувачів.

В даній роботі розроблено оригінальне програмне забезпечення, яка дозволяє встановлювати довільний закон розподілу руху користувачів із різними швидкостями. Координати і параметри користувачів зберігаються в системі моніторингу та представляються відповідними масивами даних. Основні масиви даних моделі: координатний (x, y), швидкості переміщення (V_{SPEED} , м/с), рівень прийнятого сигналу RSS від сусідніх мережних вузлів доступу (базових станцій) ($n = 1, 2, 3$, див. рис. 5.9-5.13).

Дані до цього масиву записується щосекунди. Модуль управління активністю користувачів представляє собою масив, який зберігає призначені для користувача об'єкти і здійснює моніторинг діяльності кожного зареєстрованого в системі користувача. Якщо тривалість зберігання призначеного для користувача об'єкта в масиві вище, ніж середня тривалість сесії, яка був встановлена за допомогою генератора трафіку при створенні об'єкта користувача, тоді вважається, що користувач закінчив сесію і його об'єкт видаляється з масиву. Іншим важливим елементом моделі є блок, який відповідає за реалізацію математичної моделі поширення радіохвиль. Блок може інтегрувати до себе будь-яку модель і, таким чином, є універсальним, тобто дозволяє моделювати поведінки для різних систем безпроводного доступу з різними інтерфейсами радіозв'язку і у різних обставинах. Алгоритм цього блоку моніторить розташування користувачів і їх переміщення, на підставі чого

він обчислює рівні загасання сигналів від усіх базових станцій. У свою чергу, базова станція, яка також описується як об'єкт має свої власні параметри, такі як: висота розташування антен, потужність випромінювання сигналу, робоча частота, кількість антен і т.д.

Поширення сигналу і, відповідно, його загасання описується моделлю Окумура-Хата для міських умов, де ефект багатопроменевого поширення хвиль виявляється найбільшою мірою. Отже, розрахунок загасання в моделі для міських умов проводиться за формулою:

$$L_{[\text{dbm}]} = 69,55 + 26,16 \cdot \lg(f) - 13,82 \cdot \lg(h_{N[\text{m}]}) - a(h_0) + \left(\left[49,9 - 6,55 \cdot \lg(h_{N[\text{m}]}) \right] \right) \cdot \lg(d_{[\text{km}]}) \quad (5.17)$$

Важливе значення для проведення досліджень, описаних в даній роботі має блок, який відповідає за переміщення користувачів. Він використовує інтерфейс менеджера користувачів і, відповідно до закону розподілу броунівського руху, виконує зміни координат користувача з різними інтервалами і кількостями кроків, забезпечуючи, таким чином, моделювання руху користувачів [198]. Відповідно, блок поширення радіохвиль на кожному новому кроці моделювання обчислює загасання сигналу для користувача в новому розташуванні. Варто відзначити, що є такі користувачі, які не рухаються.

Для розроблення такого програмного забезпечення в даній роботі використовується мова програмування C ++, базуючись на середовищі розроблення Borland Builder C ++ 6.0. Головне вікно програми, що реалізує моделювання відповідно до створеної імітаційної моделі показано на рис. 5.9-5.13. Інтерфейс містить компонент для відображення використання трьох базових станцій типу GSM і трьох базових станцій типу LTE. Для кожної базової станції є графік у програмному інтерфейсі, який відображає зареєстрованих і активних користувачів. Для того, щоб порівняти продуктивність системи без інтелектуального вертикального хендвера і з ним, в програмну модель додано можливість відключення цього алгоритму.

5.3.5. Аналіз результатів моделювання.

Ґрунтуючись на запропонованих у даному розділі роботи рішеннях, а також використовуючи розроблену імітаційну модель, були одержані наступні результати (див. рис. 5.9-5.15 та табл. 5.5), причому найбільш оптимальний результат для виконання інтелектуального вертикального хендоверу (та перерозподілу мережних ресурсів гетерогенної мережної платформи) був одержаний для вузла доступу BS2 (мережна система LTE) (це показано на рис. 5.15). Результат для вузла доступу BS1 (мережна система LTE) є нижчим, хоча, згідно функції належності, належить до того ж самого лігвістичного терму «Високий». Таким чином, теорія нечітких множин кількісно демонструє різницю між якісно однорідними рішеннями оптимізаційної задачі розподілу конвергованих ресурсів мережно-залежних рівнів гетерогенних розподілених сервісних систем [126].

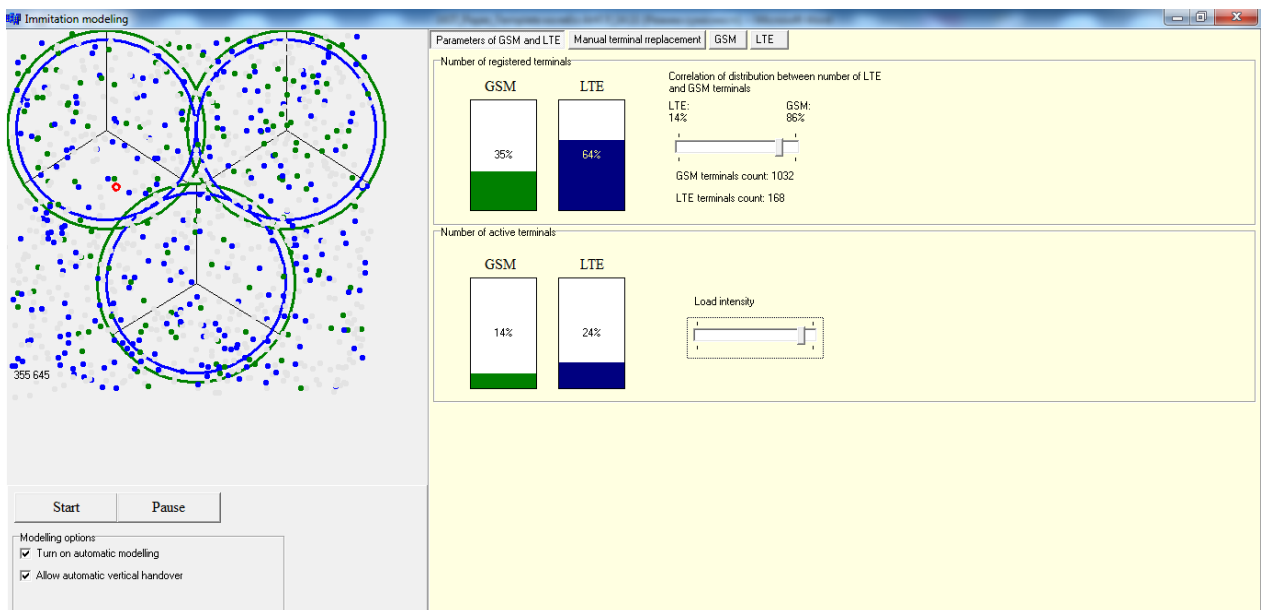


Рис. 5.9. Інтерфейс імітаційної програмної моделі гетерогенної мережної платформи з можливістю зміни рівня вхідного навантаження для LTE та GSM систем (представлено в умовах високого системного завантаження).

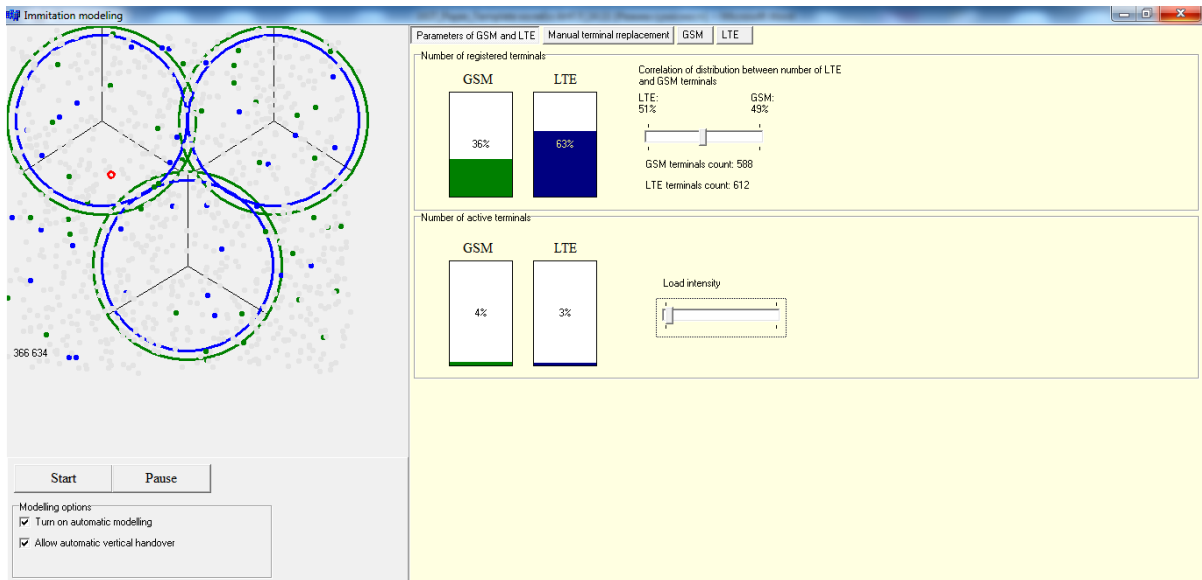


Рис. 5.10. Інтерфейс імітаційної програмної моделі гетерогенної мережної платформи з можливістю зміни рівня вхідного навантаження для LTE та GSM систем (представлено в умовах низького системного завантаження).

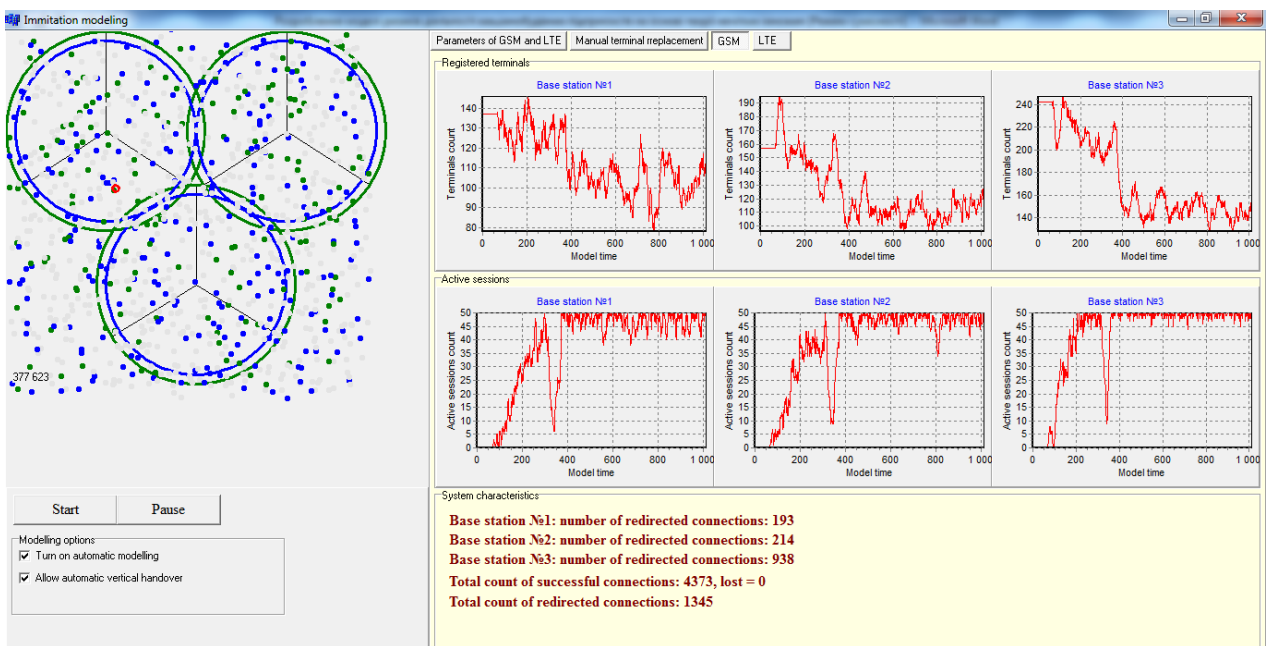


Рис. 5.11. Інтерфейс імітаційної програмної моделі гетерогенної мережної платформи на основі LTE та GSM систем, представлено моніторинг зареєстрованих та переключених груп користувачів у GSM комірках.

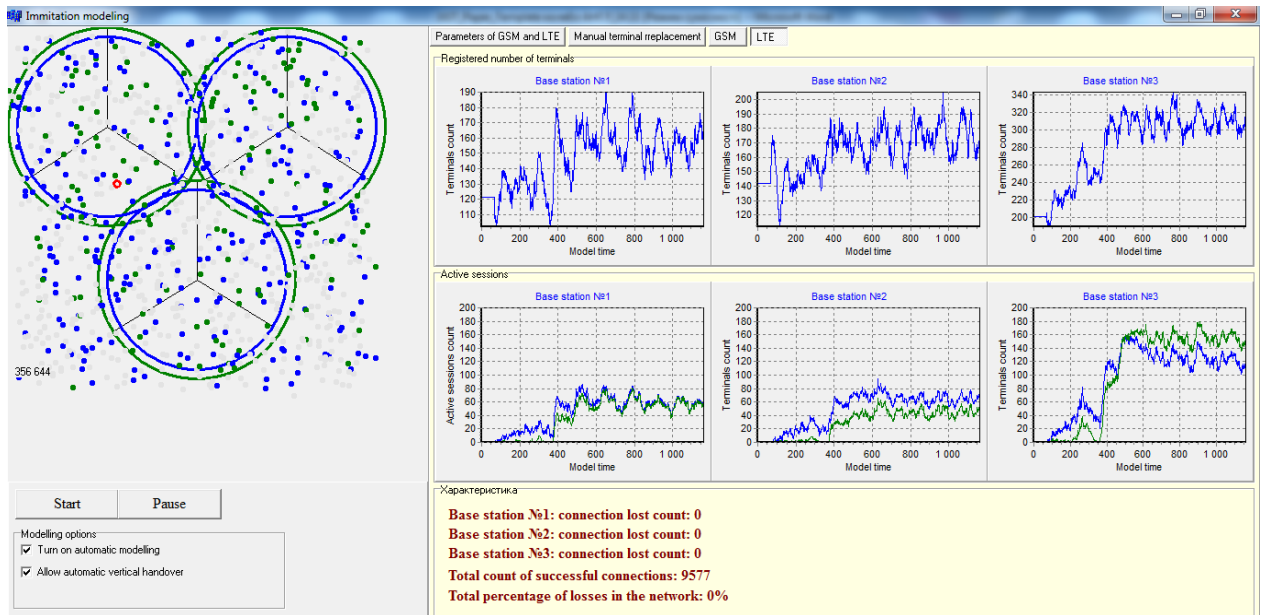


Рис. 5.12. Інтерфейс імітаційної програмної моделі гетерогенної мережної платформи на основі LTE та GSM систем, представлено моніторинг зареєстрованих та переключених груп користувачів у LTE комірках.

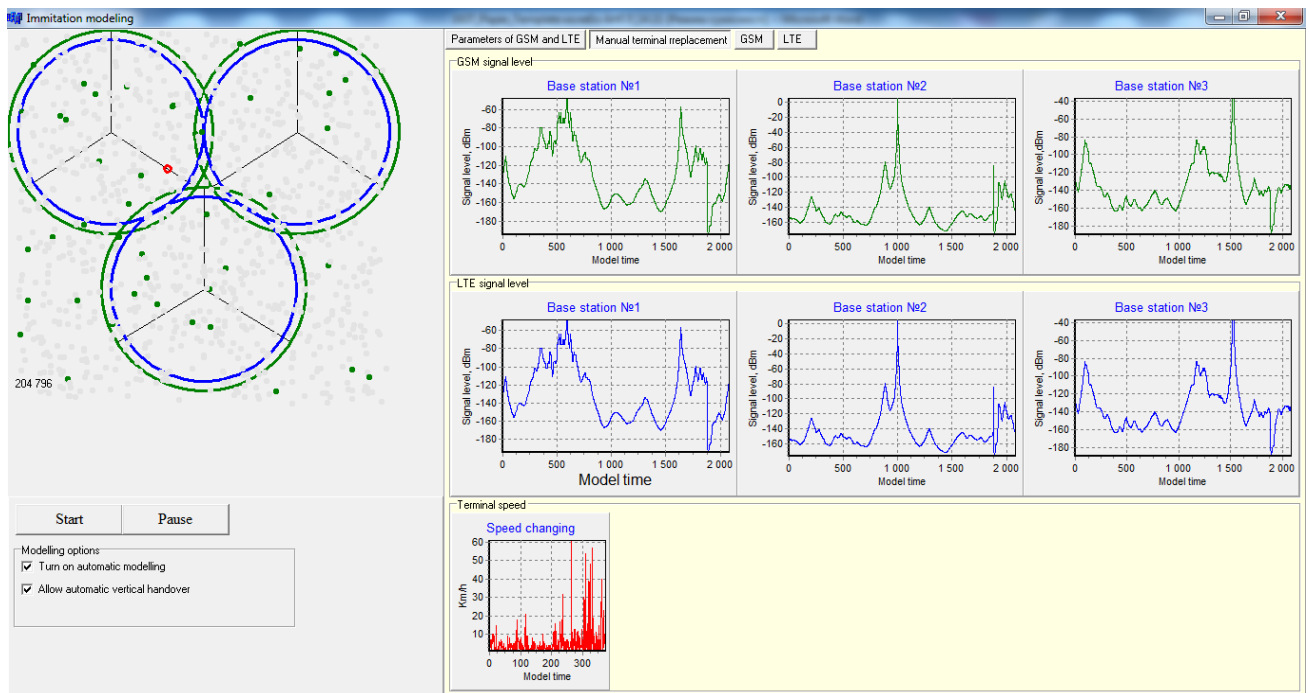


Рис. 5.13. Інтерфейс імітаційної програмної моделі гетерогенної мережної платформи на основі LTE та GSM систем, представлено моніторинг змін швидкості руху користувача (рівня його мобільності – червона точка, червоний графік), зміну загасання сигналу від призначеної базової станції впродовж часу спостереження у відповідних мережних комірках, при виконанні прогнозування щодо необхідності проведення вертикального хендвера.

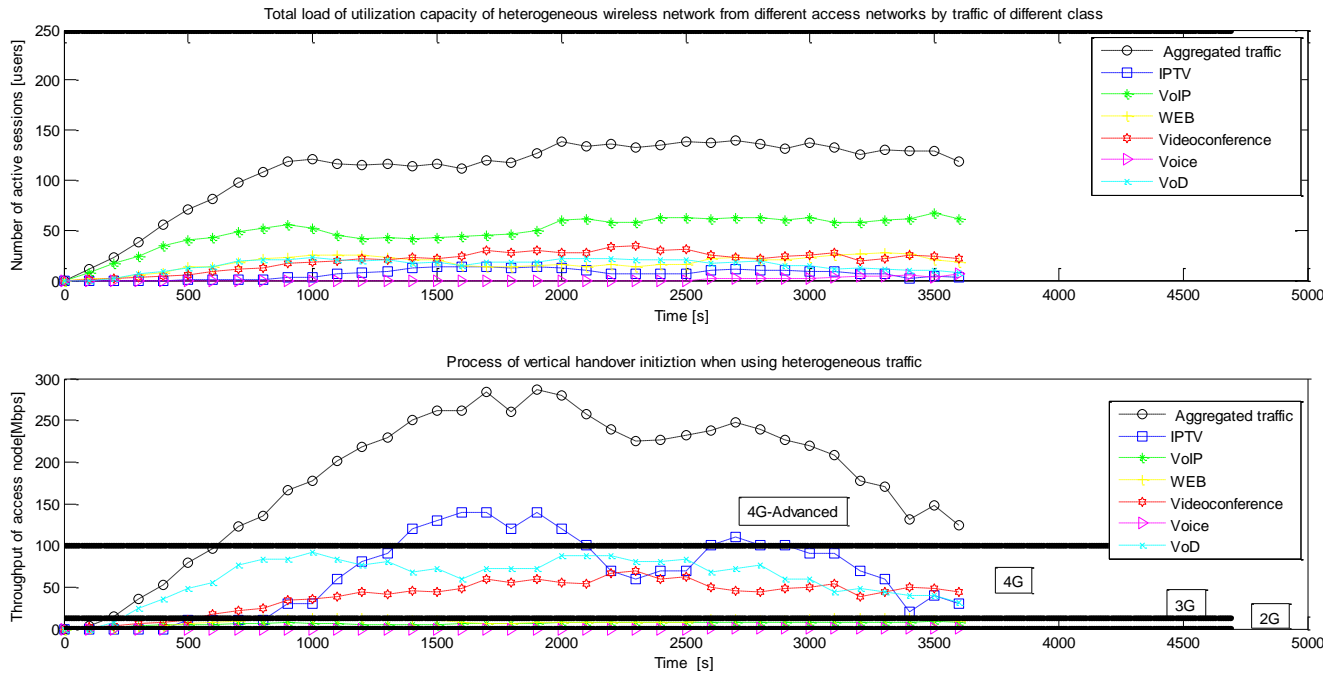


Рис. 5.14. Навантаження на гетерогенну мережну платформу від різних мережних систем доступу та поріг ініціювання інтелектуального вертикального хендовера.

Таблиця 5.5. Результати оцінювання на основі нечітких множин (трикутних нечітких чисел) для мережних вузлів доступу та їх дефазифікації (R_{mn}).

	BS1 (GSM) $\frac{1}{2} \times (\tilde{Q}_{mn} + \tilde{P}_{mn})$ (\tilde{R}_{mn})	BS2 (GSM) $\frac{1}{2} \times (\tilde{Q}_{mn} + \tilde{P}_{mn})$ (\tilde{R}_{mn})	BS3 (GSM) $\frac{1}{2} \times (\tilde{Q}_{mn} + \tilde{P}_{mn})$ (\tilde{R}_{mn})	BS1 (LTE) $\frac{1}{2} \times (\tilde{Q}_{mn} + \tilde{P}_{mn})$ (\tilde{R}_{mn})	BS2 (LTE) $\frac{1}{2} \times (\tilde{Q}_{mn} + \tilde{P}_{mn})$ (\tilde{R}_{mn})	BS3 (LTE) $\frac{1}{2} \times (\tilde{Q}_{mn} + \tilde{P}_{mn})$ (\tilde{R}_{mn})
Jitter	(0,2; 0,005; 0,005)	(0,2; 0,005; 0,005)	(0,105; 0,005; 0,005)	(0,2; 0,005; 0,005)	(0,15; 0,005; 0,005)	(0,105; 0,005; 0,005)
Packet Loss Ratio	(0,04; 0,053; 0,03)	(0,04; 0,053; 0,03)	(0,008; 0,053; 0,003)	(0,04; 0,053; 0,03)	(0,04; 0,053; 0,023)	(0,04; 0,053; 0,008)
Throughput	(0,15; 0,095; 0,075)	(0,1; 0,0095; 0,06)	(0,01075; 0,00 57; 0,1750)	(0,25; 0,195; 0,175)	(0,25; 0,0095; 0,175)	(0,01; 0,005; 0,175)
Delay	(0,105; 0,04)	(0,05; 0,105; 0,04)	(0,1; 0,105; 0,0055)	(0,1; 0,105; 0,04)	(0,1; 0,105; 0,0055)	(0,1; 0,105; 0,0055)
Cost	(0,0025; 0,0125; 0,01)	(0,0025; 0,0125; 0,01)	(0,006; 0,011; 0,001)	(0,0051; 0,0225; 0,01)	(0,006; 0,0225; 0,001)	(0,006; 0,006; 0,001)
Security	(0,0225; 0,0525; 0,15)	(0,0225; 0,0525; 0,07)	(0,00375; 0,05 375; 0,15375)	(0,0325; 0,0525; 0,25)	(0,0325; 0,075; 0,15)	(0,0375; 0,0525; 0,15)
Ms-Velocity	(0,032; 0,017; 0,12)	(0,032; 0,017; 0,02)	(0,0052; 0,012; 0,12)	(0,032; 0,017; 0,12)	(0,032; 0,012; 0,12)	(0,032; 0,012; 0,12)
RSS	(0,0125; 0,0875; 0,125)	(0,0625; 0,0375; 0,052)	(0,125; 0,0047 5; 0,0475)	(0,125; 0,2375; 0,225)	(0,1025; 0,2375; 0,225)	(0,125; 0,2375; 0,225)
Load	(0,00525; 0,00 525; 0,00525)	(0,00525; 0,00 525; 0,00525)	(0,00525; 0,00 525; 0,00525)	(0,00525; 0,00 525; 0,00525)	(0,00525; 0,00 525; 0,00525)	(0,00525; 0,00 525; 0,00525)
\tilde{R}_{mn}	(0,51475; 0,43 275; 0,56025)	(0,51475; 0,29 725; 0,29275)	(0,36895; 0,25 55; 0,516)	(0,78985; 0,69 275; 0,86025)	(0,71825; 0,52 475; 0,70975)	(0,46075; 0,48 125; 0,69475)
R_{mn}	0,502583333	0,36825	0,38015	0,78095	0,6509166	0,545583333

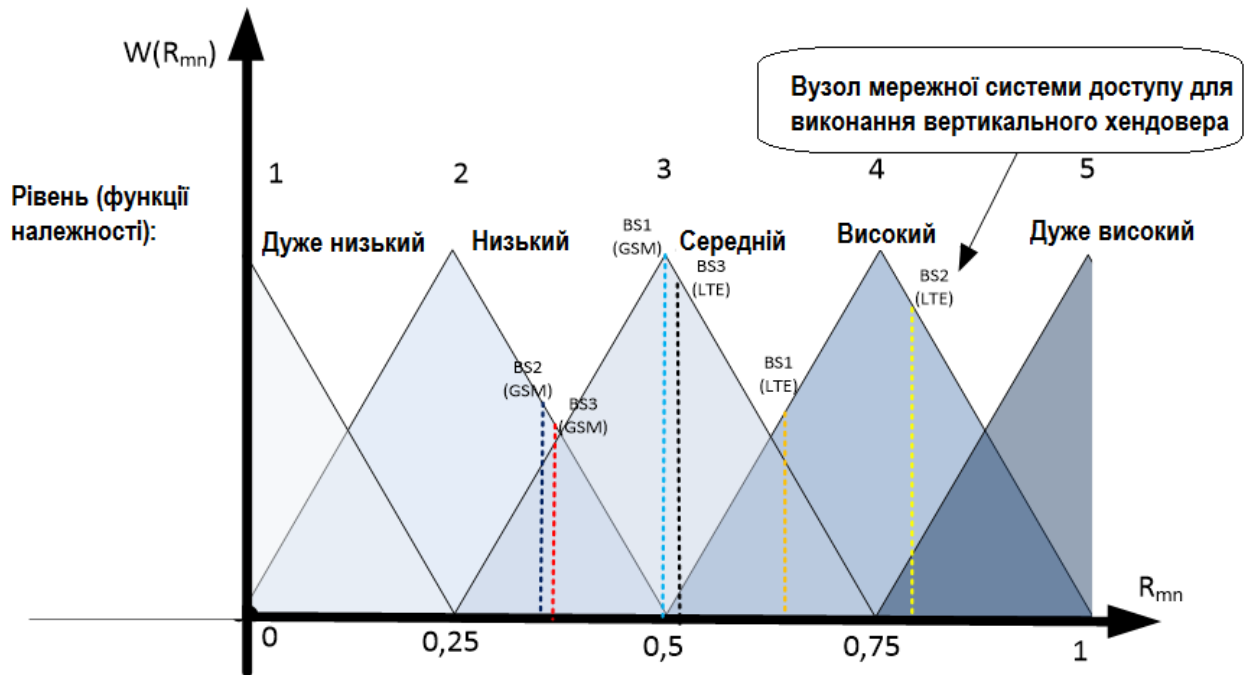


Рис. 5.15. Визначення оптимального вузла мережної системи доступу для виконання вертикального хендвера з використанням установленної шкали Лікерта.

5.4. Висновки до 5-го розділу.

1. Застосування запропонованого в розділі підходу та алгоритму динамічної корекції маршрутних метрик шляхом наскрізного структурного трасування пропонує нам оперативну і динамічно визначати структурно-топологічні зміни в хмарній сервісній платформі, а це, в свою чергу, дозволяє покращити балансування навантаження в сервісних вузлах, виконуючи плавну міграцію основних інформаційних потоків та, відповідно, сервісних компонентів за межі областей мережної системи із високим завантаженням і структурними неоднорідностями. Іншими словами – більш рівномірно розподілити обчислювальні та телекомунікаційні ресурси гетерогенних сервісних мережних платформ, особливо в умовах їх високого завантаження. Доступність сервісних вузлів у хмарній сервісній системі підвищується до 4% у масштабі хмарної платформи в рамках 50 сервісних вузлів, при цьому динаміка

покращення зростає до 10% у масштабі хмарної мережної платформи в рамках 100 сервісних вузлів.

2. У цьому розділі запропоновано покращувати якісні показники обслуговування користувачів гетерогенних телекомунікаційних платформ безпроводного доступу на основі більш ефективного використання їх телекомунікаційних та радіо-ресурсів, а також оптимізації процесів прийняття рішень про ресурсний перерозподіл, зокрема – в рамках процедури інтелектуального вертикального хендовера, що базується на використанні принципів хмарних обчислень, повсюдного комп'ютингу, застосовуючи математичний апарат нечітких множин. Показано, що теорія нечітких множин кількісно демонструє різницю між якісно однорідними рішеннями оптимізаційної задачі розподілу конвергованих ресурсів мережно-залежних рівнів гетерогенних розподілених сервісних систем.

3. Для розв'язання завдання прийняття оптимального за критеріями групи QoS рішення щодо процедури ресурсного перерозподілу при обслуговуванні користувачів мережних платформ безпроводного доступу було запропоновано централізований метод управління хендовером. Запропонований підхід дозволяє уникати двозначності у трактуванні нечітко заданих, двозначних та суб'єктивних суджень у процесі багатокритерійної оптимізації. Для дослідження процесів функціонування реальних гетерогенних мережних систем в умовах високої мобільності користувачів було розроблено програмну імітаційну модель, яка, в свою чергу, реалізує запропоновану в роботі математичну модель процесу прийняття рішення щодо вертикального хендовера на основі використання методів нечіткої логіки. Це дозволяє здійснювати налаштування великої кількості параметрів моделювання, використовуючи допоміжні математичні моделі, зокрема для опису та прогнозування процесів руху (мобільності) користувачів, а також поширення радіохвиль до їх термінального обладнання. Як було показано, вибір оптимального мережного вузла доступу на основі розв'язання багатокритерійного завдання прийняття рішення щодо хендоверу є нетривіальним, оскільки на результати цього розв'язання

впливають одночасно кілька динамічно-змінних і взаємопов'язаних факторів, тому їх агрегація згідно запропонованих у дисертаційній роботі підходів є необхідною.

4. У результаті моделювання процесів надання сервісів користувачам гетерогенної мережної платформи на базі розроблених моделей було досліджено випадок користування послугою «конференцзв'язок». Визначено оптимальну комірку гетерогенної мережної системи, що повинна прийняти на обслуговування заданого користувача на основі оцінювання характеристик та параметрів відповідного мережного вузла доступу з використанням методів теорії нечітких множин. Обґрунтовано вибір вузла радіодоступу LTE для задоволення запитів користувача щодо отримання сервісу заданого типу. У амбівалентній ситуації, коли користувач знаходиться на границі покриття комірки, запропоновані в дисертаційній роботі моделі та методи дали змогу прийняти обґрунтоване рішення щодо проведення процедури вертикального хендовера, базуючись на групі QoS-залежних критеріїв.

РОЗДІЛ 6

Дослідження особливостей трансформації архітектури телекомунікаційних сервісних платформ для застосування в критично важливих системах національного масштабу

6.1. Дослідження ефективності застосування вдосконалених протокольних засобів мережного рівня для спеціалізації гетерогенних сервісних мережних платформ.

У розділі 4.1 було показано, що в сервісних мережних системах оптимальне за критерієм сервісної доступності співвідношення між паралельними та послідовними сервісними компонентами деякого комплексного сервісу наближається за характером до «золотого січення» і складає приблизно 60/40% [152]. Поширюючи це структурне співвідношення на реалізації мережної системи згідно моделі виду «інфраструктура, як сервіс» (IaaS), можна зробити висновок, що оброблення мережного трафіку, як потоків пакетів повинне відбуватись у мережній інфраструктурі, у якій до 40 % обладнання має послідовний характер функціонування. Такий характер має пасивне комутаційне обладнання, що здійснює недиференційоване опрацювання потоків агрегованого навантаження. Інша частина обладнання для оброблення мережного трафіку (близько 60%) повинна носити характер розпаралелених обробників (віртуалізованих програмних маршрутизаторів), тобто забезпечувати виділення частини навантаження для диференційованого обслуговування в окремих компонентах, які функціонують паралельно або квазі-паралельно. Таким навантаженням є, зокрема, навантаження деяких потоків трафіку високого пріоритету. За рахунок окремого і паралельного в часі оброблення потоків пріоритетного трафіку та незначного погіршення часових параметрів обслуговування трафіку нереального часу (низького пріоритету), відбувається значне (у рази) покращення часових параметрів обслуговування цих виокремлених потоків. Це, зокрема, доведено і продемонстровано у [199].

Для технологічної зручності реалізації оброблення виокремлених високопріоритетних потоків навантаження, а також з метою уникнення взаємних впливів між окремими розпаралеленими компонентами при синтезі сервісної системи типу IaaS, необхідно виділити та реорганізувати відповідні програмно-апаратні ресурси у якості ізольованих віртуалізованих компонент системи (програмного маршрутизатора), що значно підвищить стабільність її функціонування. Ґрунтуючись на вдосконаленні процесів у мережно-залізничних рівнях, при дотриманні запропонованого чисельного співвідношення (60/40%) між паралельними та послідовними компонентами, які задіяні в архітектурі сервісної мережної системи, оптимально підвищується їх доступність, вивільняються та перерозподіляються буферні та обчислювальні системні ресурси, а отже синтезована мережна архітектура IaaS забезпечує відчутне зниження зваженої затримки передавання мережного трафіку, зокрема – за рахунок спеціалізованих потоків реального часу з високими пріоритетами, підвищуючи якість сервісу для критичних застосувань [226].

Агрегування потоків на послідовних ланках сервісної мережної системи після паралельних обробників не вносить глобального погіршення у якість сервісу IaaS, такі флуктуації параметрів QoS носять локальний характер на окремих мережних інтерфейсах, а в цілому, за рахунок ефектів синергізму та системної емерджентності, а також із урахуванням результатів вище перелічених публікацій, спостерігається загальносистемне покращення часових показників якості обслуговування трафіку, в залежності від наданих йому пріоритетів [226, 227].

Далі розглянемо підтверження висловлених тез дослідженням реалізації віртуалізованих протокольних засобів на основі програмних моделей маршрутизаторів, як активних мережних елементів, які забезпечують паралельне обслуговування потоків, щодо яких виконана диференціація за пріоритетами або ж іншими заданими параметрами, а також ефективність застосування подібної реалізації у спеціалізованих відомчих мережах інформаційного обміну.

Отже, одним із найбільш актуальних наукових завдань в галузі телекомунікаційних систем є передавання трафіку реального часу з дотриманням низки вимог щодо якості обслуговування. Проблематикою якості обслуговування науковці займаються з моменту появи та впровадження мультисервісних мереж [2, 139]. Це пов'язано з тим, що множина потоків даних передається по мережі, ресурси якої повинні бути розподілені між цими потоками за певною пропорцією. Оскільки дані, які підлягають передаванню, різні за своєю природою та важливістю, то необхідно мати механізми, які дають змогу розв'язувати завдання розподілу ресурсів оперативно, у відповідності до властивостей тих потоків, які передаються у конкретний момент часу через конкретні телекомунікаційні вузли. Такі механізми повинні базуватись на удосконалених методах розподілу ресурсів, що мають високу масштабованість, швидкодію, гнучкість, низьку операційну складність та ресурсоємність. Базова вимога до таких методів – можливість їх реалізації у вигляді програмних продуктів, які підлягають інтеграції у операційну систему вузлів телекомунікаційної мережі.

Мета даного розділу роботи полягає у створенні методів оброблення та пріоритезації трафіку для розгортання телекомунікаційних мережних систем інформаційного обміну регіонально-магістрального, корпоративного рівня, зокрема – у рамках побудови спеціалізованих відомчих мереж інформаційного обміну, шляхом зниження затримок при комутації/маршрутизації відповідних інформаційних потоків.

6.1.1. Практична реалізація модифікованого методу обслуговування черг на основі диференціації сервісів у моделі IaaS.

Поява мультисервісних мережних систем, виникнення нових властивостей мережного трафіку, необхідність забезпечення високої якості обслуговування різними категоріями сервісних застосувань визначають необхідність вдосконалення теорії управління трафіком мультисервісних мереж. Мережні пристрої не завжди в змозі адекватно реагувати на сплески інтенсивності

трафіку, які часто виникають в мережній платформі, це, в свою чергу, погіршує якість обслуговування потоків реального часу, а саме – збільшується затримка обслуговування окремих пакетів потоку навантаження, і, як наслідок, джитер. В результаті, для прикладу, відбувається завмирання відтворення аудіо- та відео мультимедійних даних на кінцевих пристроях користувачів. Ключовою функцією маршрутизаторів у процесі оброблення мультисервісного трафіку є вибіркоче обслуговування кожного потоку, відповідно до його пріоритету. Зрозуміло, що потокам реального часу надається найвищий пріоритет в обслуговуванні. Проте, дуже часто затримка передавання пакету від вузла відправника до вузла призначення може змінюватися залежно від подій в мережі, що не мають безпосереднього впливу на алгоритми пріоритетного або диференційованого обслуговування. Чим більше мережних пристроїв й окремо взятих мережних сегментів проходить пакет на своєму шляху, тим більшою буде результуюча варіація затримки. Проблема в тому, що існуючі алгоритми пріоритетного оброблення трафіку не беруть до уваги той факт, що затримка пакету на момент його прибуття в конкретний маршрутизатор вже досягнула критичного значення, а отже вони практично не здатні гарантувати вчасну доставку пакетів та усунення критичних флуктуацій у аудіо- та відео потоках даних (реального часу). Саме ця проблема і розглядається далі. Для її вирішення розроблено модель пріоритезації оброблення сервісного навантаження [200-203] та модифіковано алгоритм пріоритетного обслуговування трафіку в буферах маршрутизатора (рис. 6.1).

Пропонується для кожної зони пріоритетності буферного ресурсу встановлювати свій лічильник часу допустимої затримки пакетів, який, на основі аналізу 2⁵- 3=29 рівнів затримок $t_1, t_2, t_3, t_4, \dots, t_{29}$, маркуватиме пакети шляхом встановлення двох зарезервованих (невикористаних на мережному рівні для інформаційних потоків, особливо для протоколу реального часу UDP) останніх бітів у полі DSCP та бітів DS3-DS5 з урахуванням 3-ох комбінацій (високого, середнього та низького) рівня інтенсивності відкидання пакетів в алгоритмах WRED. Таким чином пакети, час затримки буферизації яких

досягнув критичного рівня $t_{29} = T_{\text{доп}} * 100\%$, отримують найвищий пріоритет обслуговування на всьому шляху передавання до пункту призначення (адресата) і не піддаються буферизації у вузлах. При цьому, кожному відліку лічильника затримки може бути призначена конкретна величина часу перебування пакету у вузлі. Це дає змогу визначити затримку пакетів з необхідною точністю, в залежності від умов функціонування домену мультисервісної мережної системи.

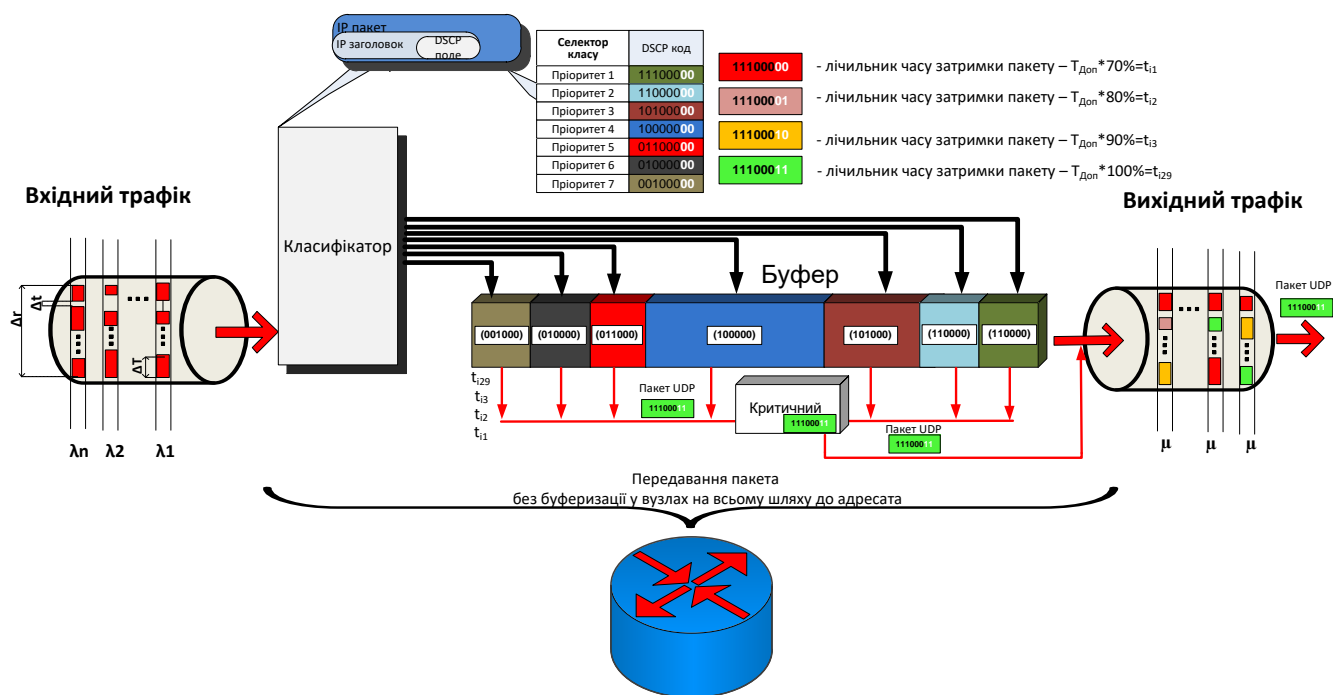


Рис. 6.1. Удосконалення процесу пріоритизації та обслуговування потоків в активному мережному пристрої (маршрутизаторі) сервісної платформи.

Перевага даної моделі у тому, що гарантується забезпечення якості надання послуг на всьому шляху передавання відповідних потоків пакетів за рахунок невикористаних ресурсів сервісів, які визнаються пріоритетними. Тим самим, незначно збільшуючи затримку високопріоритетних пакетів у допустимих або прийнятних межах, можна забезпечити гарантовану якість обслуговування для послуг з низьким пріоритетом, поточна затримка яких досягнула критичного рівня. Очевидно також, що можливо зменшити затримку деяких високопріоритетних інформаційних потоків та підтримати необхідний рівень якості сервісу за рахунок незначного, у допустимих межах, збільшення

затримки низькопріоритетних потоків, що є важливим для забезпечення оперативності передавання окремих спеціалізованих потоків даних реального часу.

Для того, щоб практично використовувати існуючі моделі мережної системи у багатьох випадках потрібна інформація про реальний перебіг інформаційно-обчислювального процесу надання сервісів. Подібна інформація необхідна і для того, щоб з більшою мірою вірогідності оцінювати якість проектних рішень, закладених при створенні обчислювальних пристроїв і розробці математичного забезпечення, а також – для вирішення проблем, пов'язаних із налаштуванням операційної системи мережних пристроїв у відповідності до конкретних умов експлуатації. Необхідну інформацію збирають за допомогою спеціальних засобів, які забезпечують вимірювання параметрів, що характеризують динаміку функціонування мережної системи у режимі нормальної експлуатації (див. рис. 6.2 в).

З цієї причини, у рамках дисертаційної роботи розроблено віртуальний програмний маршрутизатор з підтримкою диференціації обслуговування сервісних потоків (рис. 6.2 а). Розроблення здійснювалося з використанням середовища програмування Qt5.2, яке, в свою чергу, використовує мову програмування C++ (стандарт C++11, 2011р.). Основною перевагою цього середовища є те, що написаний у ньому код може бути скомпільований на різних апаратно-програмних архітектурах (наприклад Windows, Linux, Mac OS). В основу програмного маршрутизатора покладено технологію сокетів, які є програмними об'єктами операційної системи та містять атрибути IP адреси пристрою та TCP порту. Використовуючи API операційної системи, програмний маршрутизатор отримує сформований об'єкт сокету та використовує його для комунікації з іншими програмними маршрутизаторами (в тому числі – віртуалізованими реалізаціями, що функціонують паралельно), які встановлені на інших фізичних машинах у локальній мережі. Для генерації мультисервісного трафіку розроблено генератор, що також використовує сокети і дає змогу формувати трафік з довільними параметрами на основі

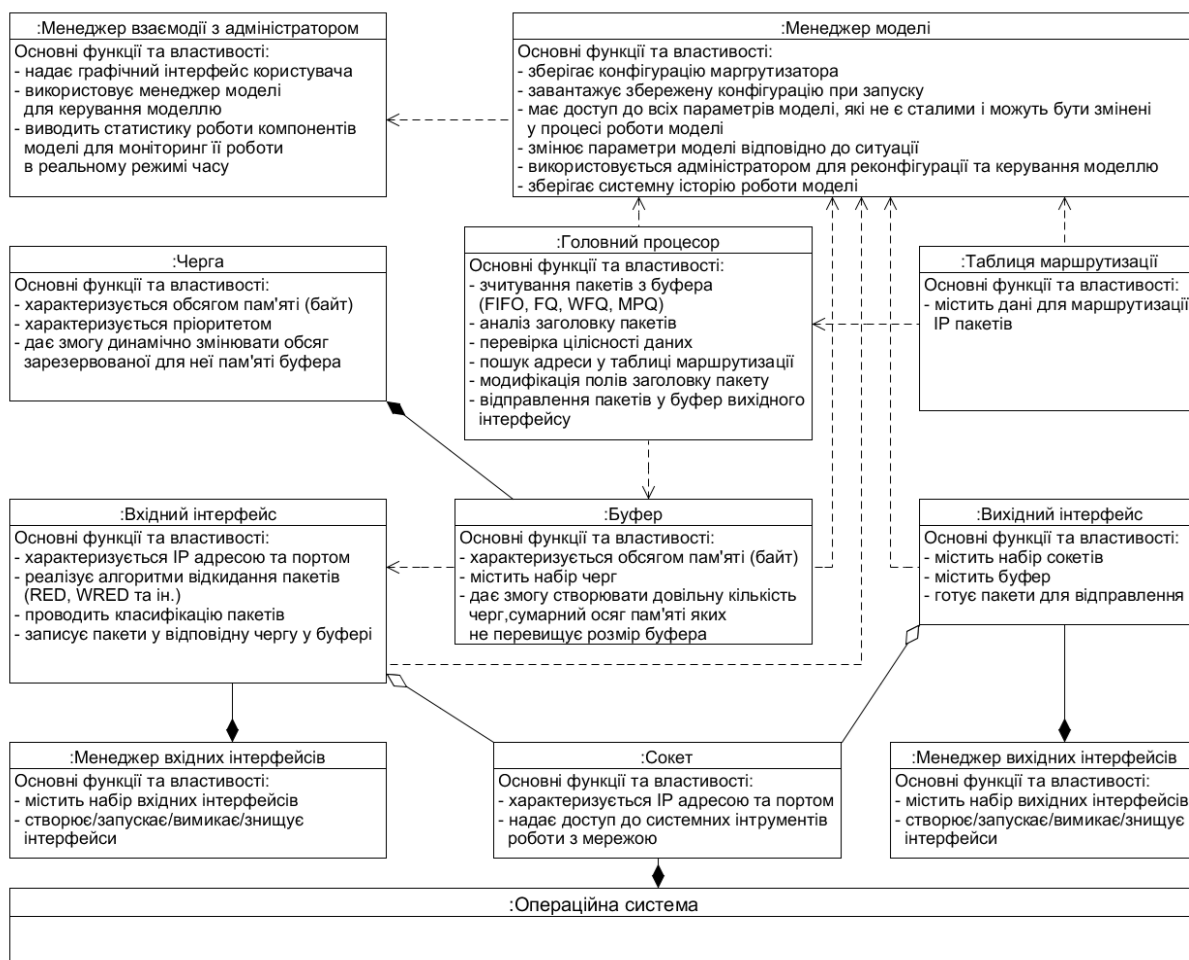
динамічного змішування потоків з різними статистичними характеристиками та вимогами до якості обслуговування (рис. 6.2 б), згідно [131].

У роботі проводився експеримент, який полягав у порівнянні характеристик обслуговування навантаження при застосуванні розробленої технології пріоритезації та оброблення пакетів у активних мережевих пристроях із характеристиками, що досягаються при обслуговуванні мультисервісного трафіку існуючим на ринку маршрутизатором компанії Cisco серії 2800. Було забезпечено та апробовано відповідність технічних характеристик програмного маршрутизатора та підтримку DSCP, проте внесено необхідні відмінності у алгоритми функціонування. Відповідно, на маршрутизаторах типу Cisco 2800 налаштовано алгоритм обслуговування черг WFQ, як один із широко розповсюджених алгоритмів із застосуванням класифікації пакетів в полі DSCP (рис. 6.2 г) [204].

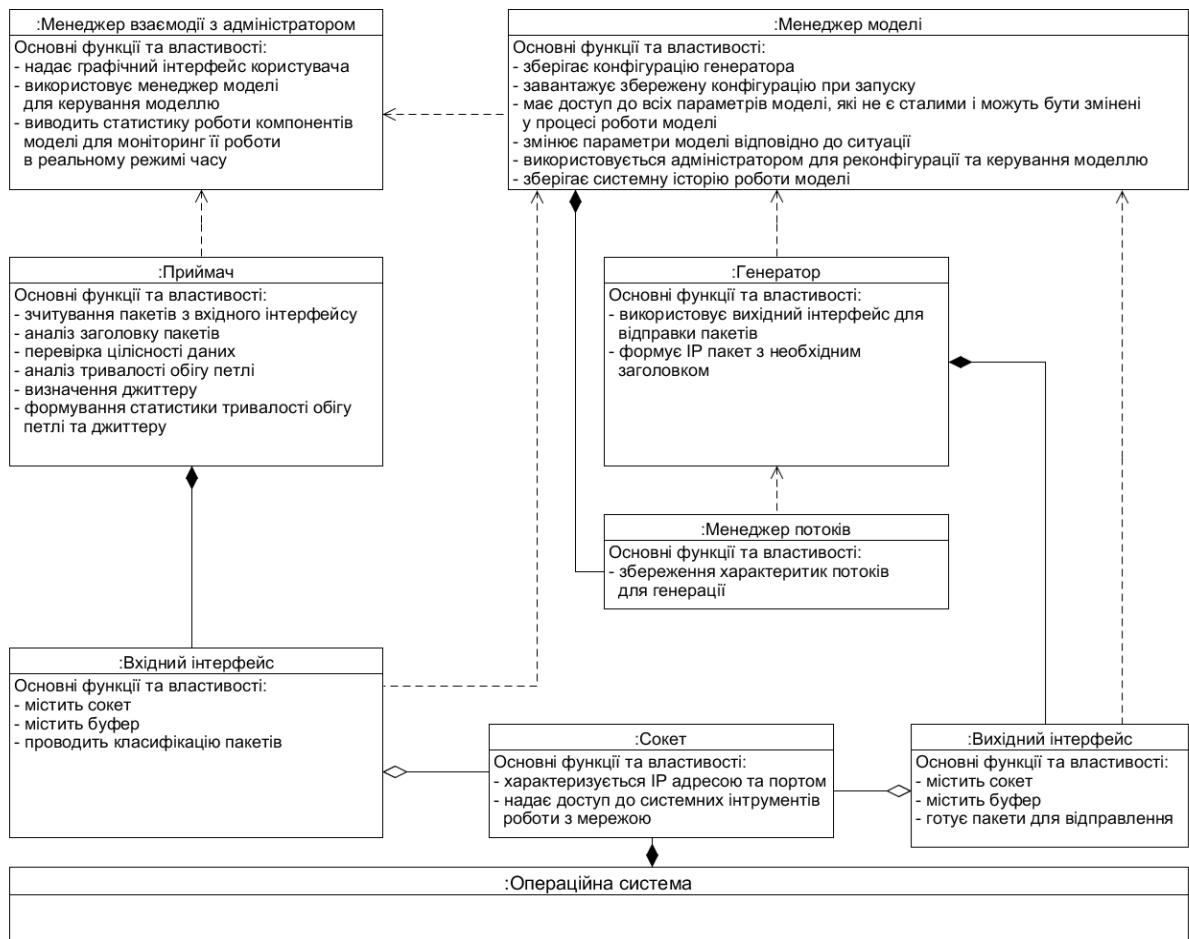
Наступним кроком після налаштування мережі з 3-ма маршрутизаторами була генерація агрегованого потоку. Для цього використано 4 персональні комп'ютери. На кожному із них встановлено генератор мультисервісного трафіку. Використано 24-ох портовий комутатор для агрегації потоків навантаження користувачів, що створювались 4-ма комп'ютерами. Отже, протягом 13 хвилин передавався трафік із 2-ох ПК для створення навантаження $\rho=0.45$, тобто мережний пристрій не був навантаженим настільки, щоб створювались черги із значними затримками при передаванні інформаційного потоку (через маршрутизатори). Для завантаження досліджуваного мережного пристрою на $\rho=0.7$ використано додатково ще 2 генератори (на основі ПК), що були включені в роботу вже після 13-ти хвилинного періоду спостереження.

На основі проведених досліджень було встановлено, що при передаванні інформаційних потоків навантаження в режимі реального часу на виході комутатора утворюється агрегований мультисервісний трафік, який надходить на інтерфейс маршрутизатора Cisco 2800 та проходить ще через 2 аналогічні маршрутизатори, які, в кінцевому результаті, створюють результуючу часову

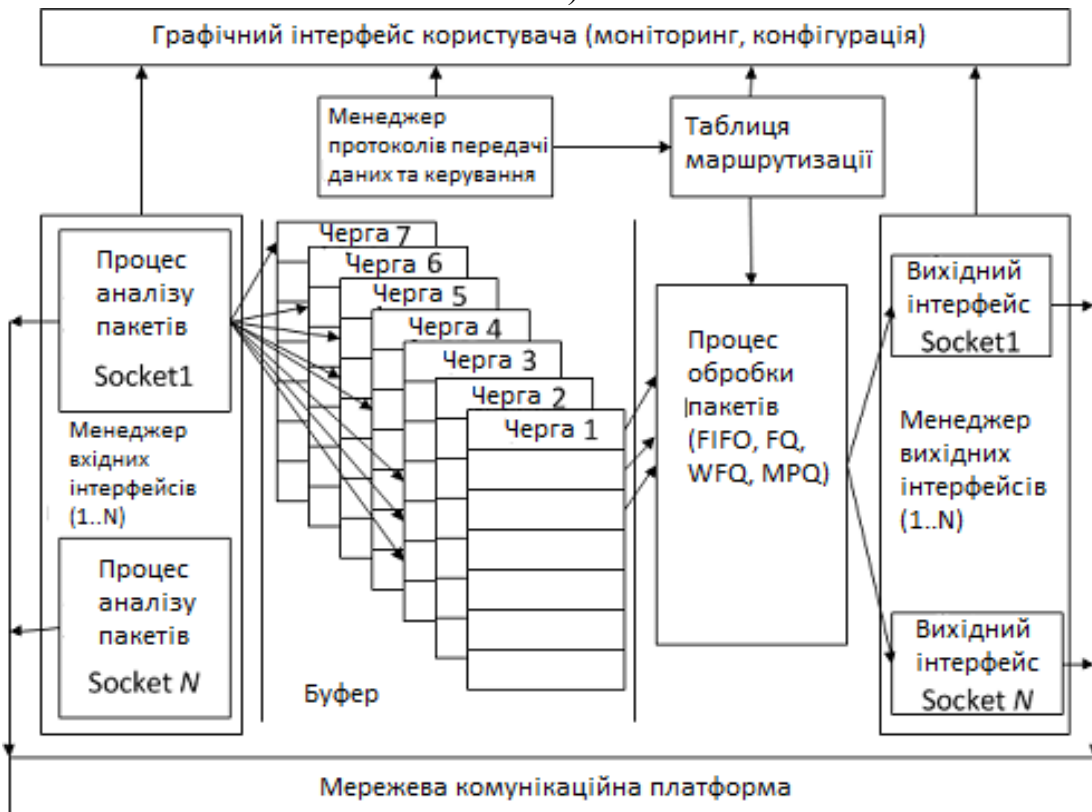
затримку інформаційних потоків. Для фіксації результатів експерименту та порівняння тривалості оброблення пакетів програмними та апаратними маршрутизаторами (в рамках експериментального підтвердження адекватності моделі обслуговування, що ними реалізується) побудовано графіки рис. 6.4 - рис. 6.8. Одержана експериментальним способом часова затримка, що внесена комутатором пакетів є сталою величиною і становить близько 50 мкс.



a)



б)



в)

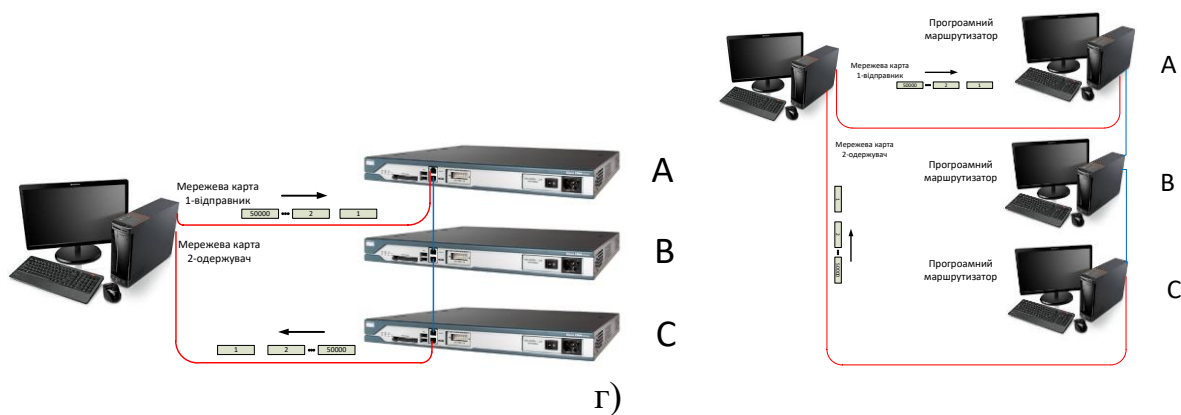


Рис. 6.2. UML-діаграма комп'ютерної імітаційної моделі програмного маршрутизатора (а) та генератора навантаження (б), структура розробленої мережної комунікаційної платформи (в), структурна схема дослідження характеристик програмних (ПК) та апаратних (Cisco серії 2800) маршрутизаторів (г).

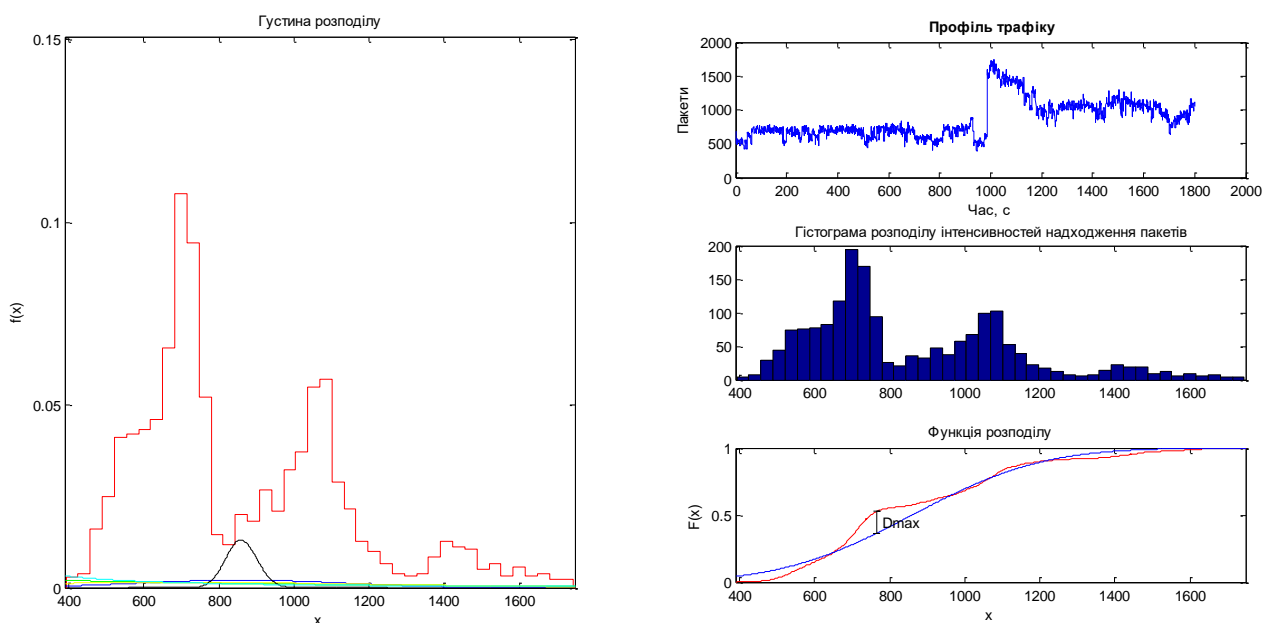


Рис. 6.3. Імовірно-статистичний аналіз вхідного навантаження експериментальної мультисервісної мережної системи.

На основі проведених досліджень доведено, що агрегований вхідний трафік експериментальної мультисервісної мережної системи, що створювався 4-ма генераторами є самоподібним з параметром Херста, близьким до одиниці ($H=0.971$), а це свідчить про неможливість точної апроксимації відповідного випадкового процесу аналітичними розподілами ймовірностей [131] (див.

рис. 6.3). Дана гіпотеза перевірена на основі проведення підбору аналітичного розподілу за критерієм Колмогорова. Найбільш адекватним для опису вхідного трафіку виявився нормальний розподіл [156].

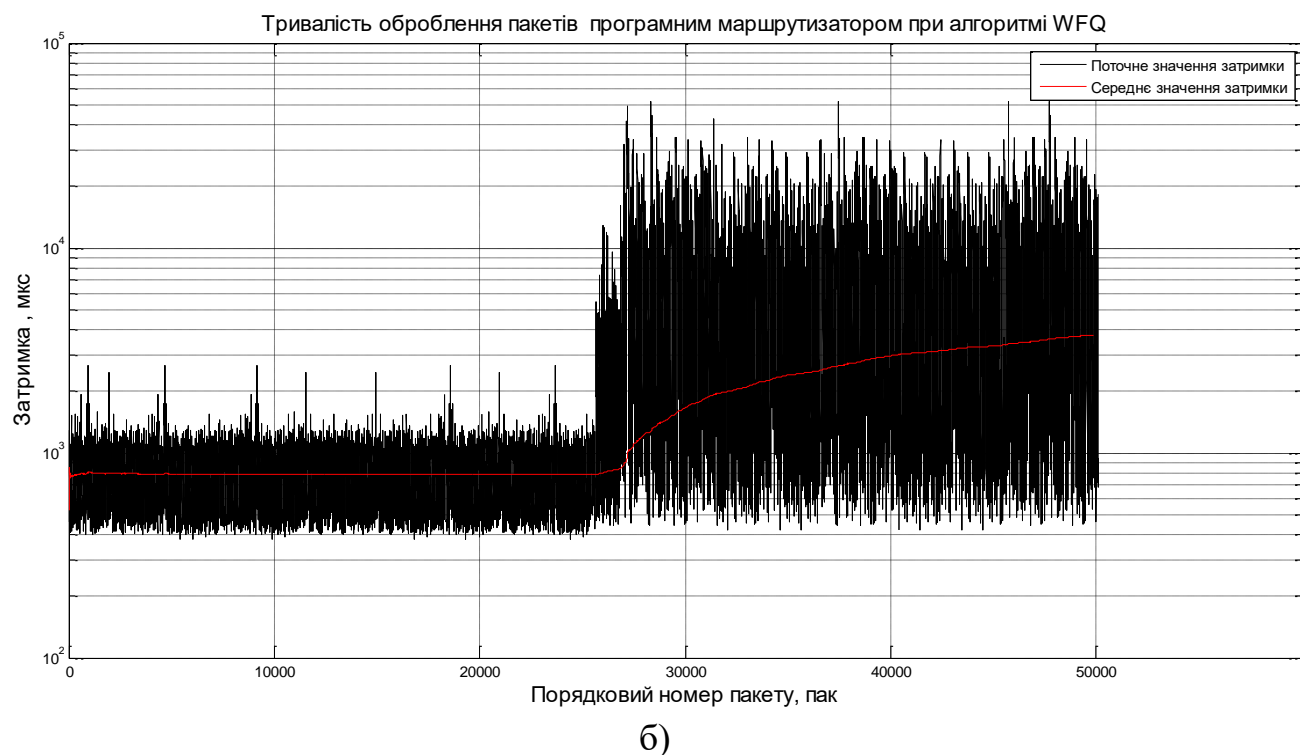
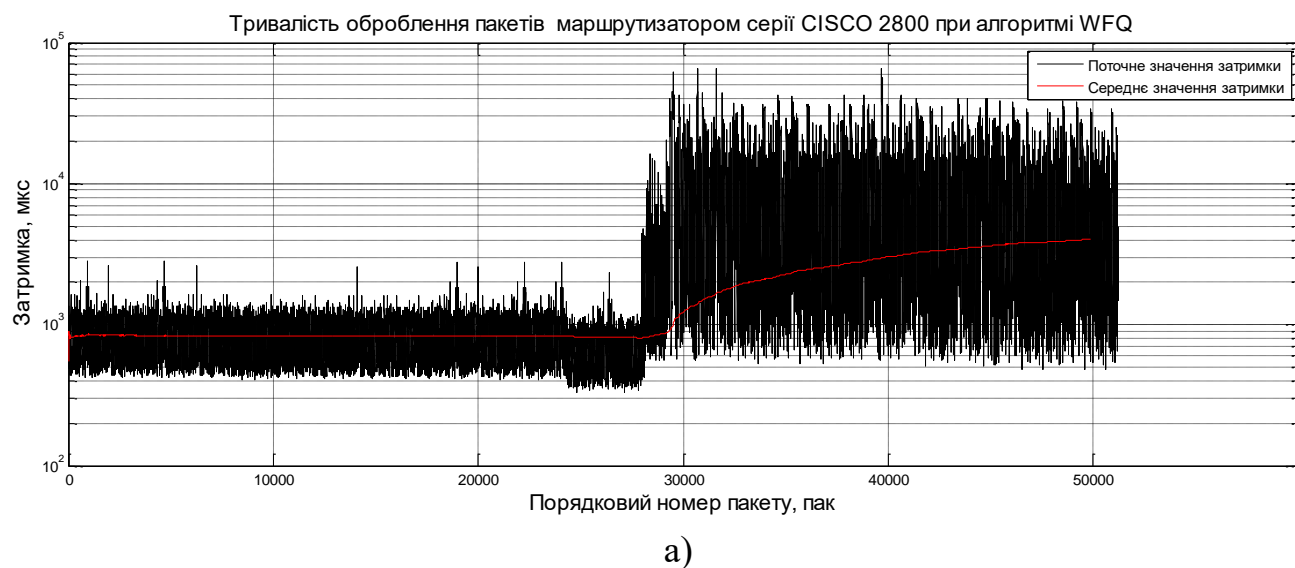


Рис. 6.4. Ряди значень тривалості затримок пакетів через комутатор і 3 апаратні (а) та програмні (б) (віртуалізовані) маршрутизатори.

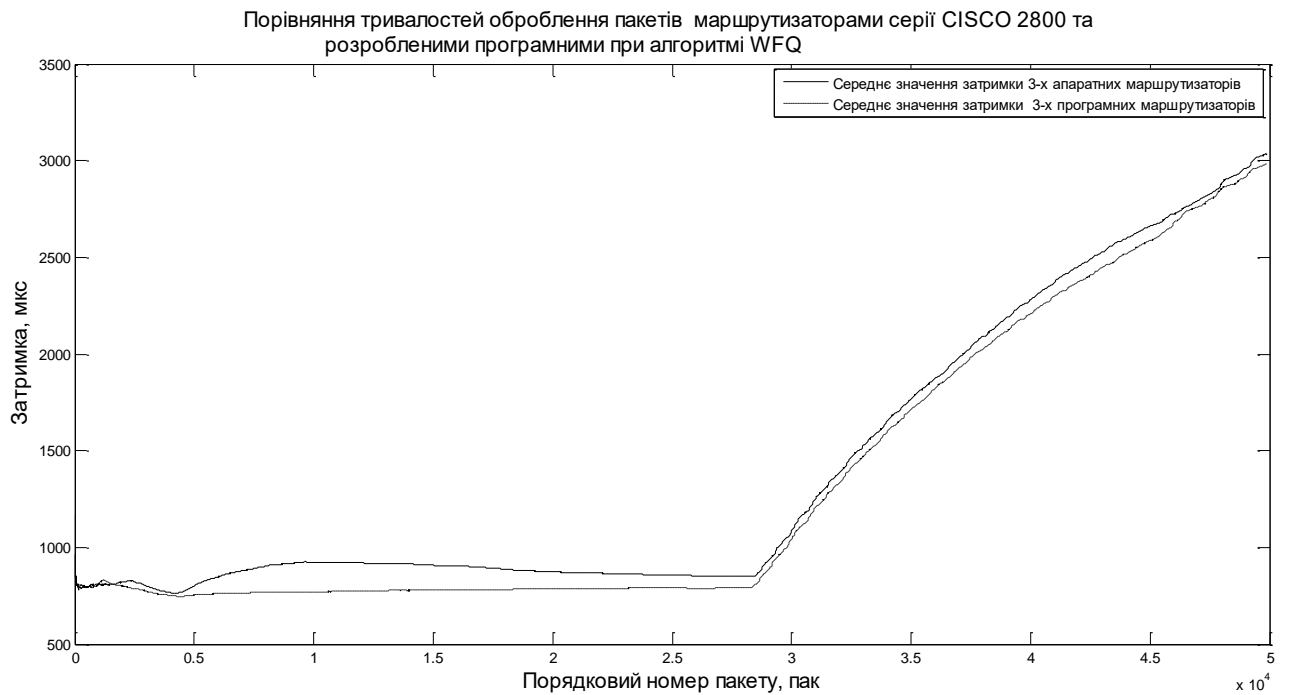


Рис. 6.5. Порівняння середніх значень затримок оброблення пакетів, внесених комутатором і 3-ма програмними та 3-ма апаратними маршрутизаторами.

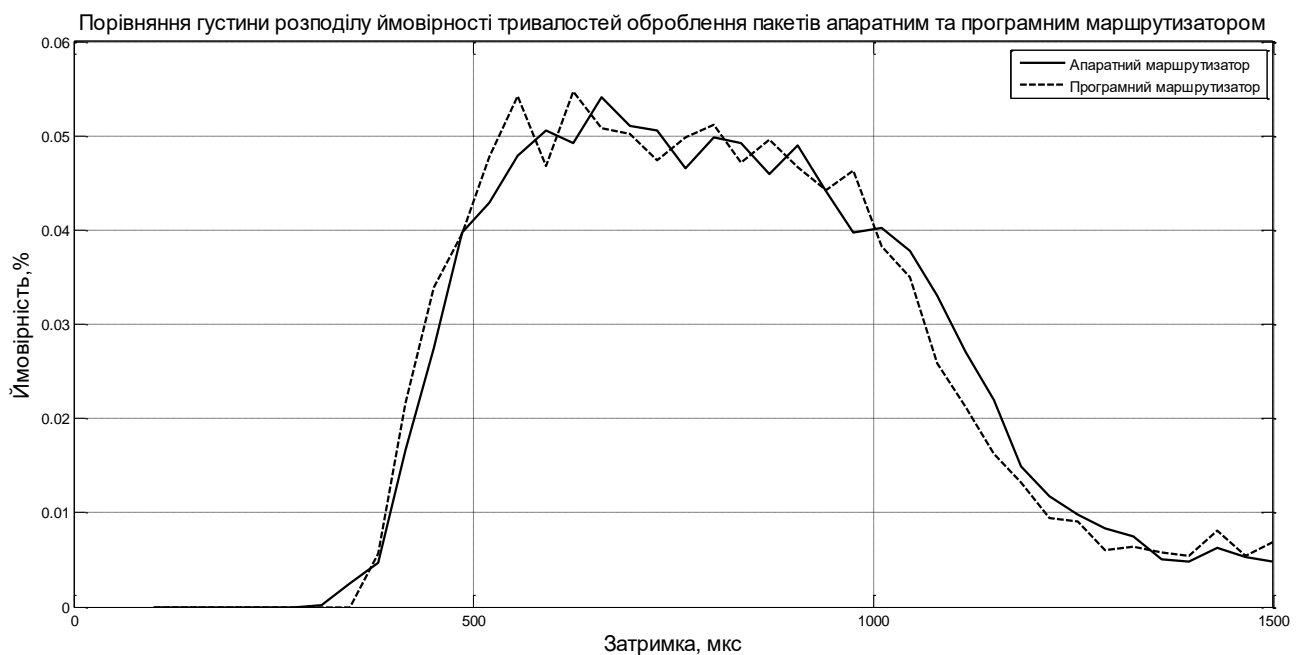


Рис. 6.6. Порівняння густини розподілу ймовірностей тривалості оброблення пакетів комутатором із 3-ма апаратними та 3-ма програмними (віртуалізованими) маршрутизаторами, протягом періоду 0...14 хв експерименту.

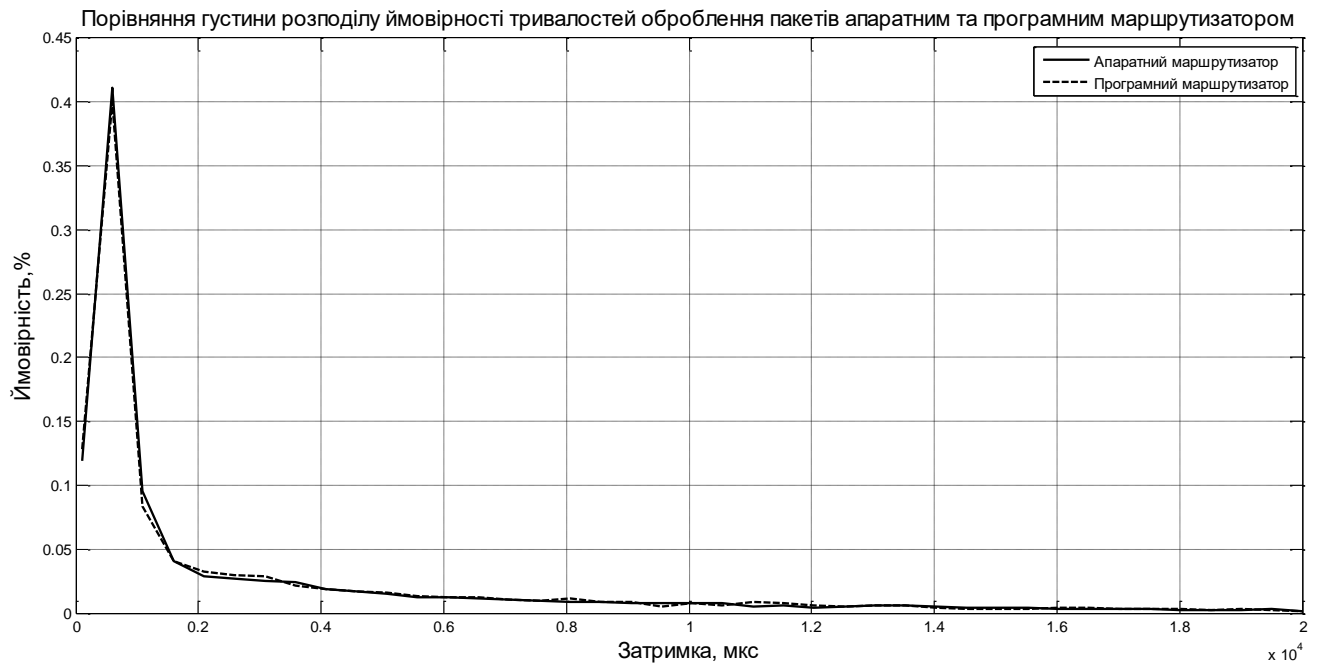


Рис. 6.7. Порівняння густини розподілу ймовірностей тривалості оброблення пакетів комутатором із 3-ма апаратними та 3-ма програмними (віртуалізованими) маршрутизаторами, протягом періоду 0...30 хв експерименту.

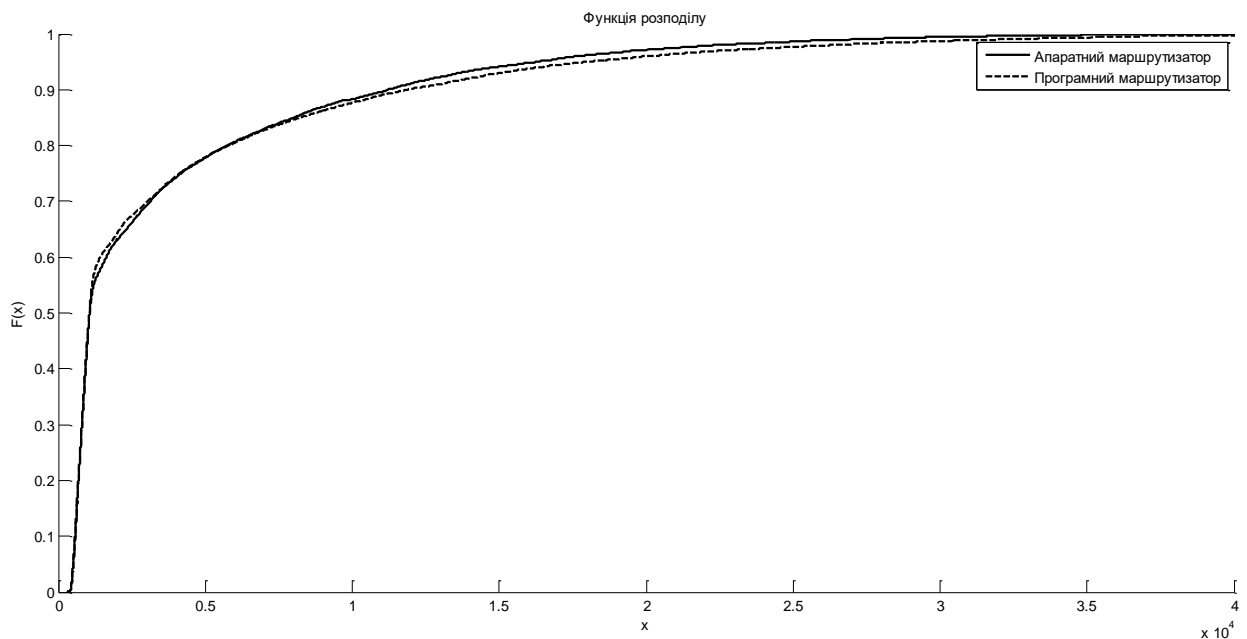


Рис. 6.8. Порівняння функцій розподілу ймовірностей тривалості оброблення пакетів комутатором із 3-ма апаратними та 3-ма програмними (віртуалізованими) маршрутизаторами, протягом періоду 0...30 хв експерименту.

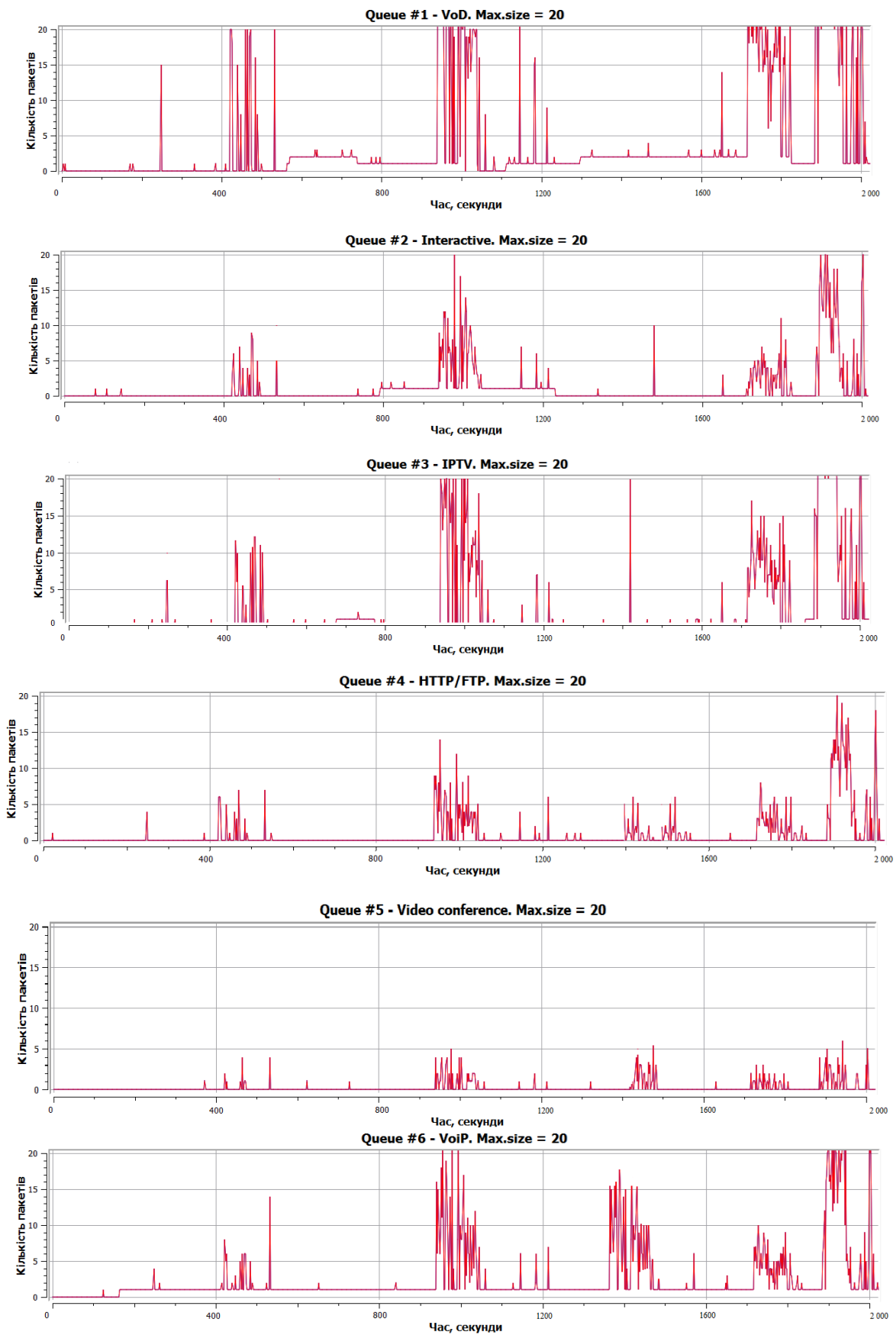


Рис. 6.9. Завантаженість буферів програмного (віртуалізованого) маршрутизатора протягом часу спостереження (використано алгоритм WFQ).

На основі аналізу результатів, представлених на рис. 6.9 бачимо, що після 13-ти хвилинного періоду спостереження завантаженість буферного простору маршрутизаторів пакетами сервісних інформаційних потоків різко зростає. Це пов'язано зі значним збільшенням обсягів вхідного навантаження на інтерфейсах програмного маршрутизатора. У загальному, середня кількість пакетів в буфері становить 105.

У результаті проведеного експерименту (зокрема, на основі даних рис. 6.3 - рис. 6.8) можна зробити висновок, що розроблений якісний програмний продукт (імітаційна комп'ютерна модель), придатний для моделювання маршрутизатора з алгоритмом, який використовує черги різної пріоритетності та який повністю відображає роботу реального маршрутизатора з похибкою отриманих результатів у 2 мкс, що, на думку автора, достатньо строго підтверджує адекватність розробленої моделі.

На рис. 6.10-6.11 показано тривалість затримки та джитер для потоку пакетів IPTV сервісу, який передається через канал мережної платформи, по якому проходить агрегований трафік. На першому етапі експерименту (0...13 хв) затримка і джитер потоку IPTV були мінімальними. На другому етапі (після 13 хв експерименту) затримки і джитер значно збільшилися за величиною (до десяти разів), що пов'язано зі значним збільшенням навантаження на активний мережний пристрій у якому за замовчуванням використовується алгоритм WFQ. Після другого етапу експерименту, при застосуванні у віртуалізованих мережних маршрутизаторах модифікованого у [199] алгоритму MPQ, було досягнуто зниження затримки і джитера трафіку IPTV сервісу до значень, які спостерігались в першій експериментальній фазі. Алгоритм MPQ використовується в умовах, коли потоки реального часу (в нашому випадку – сервіс IPTV), які є критичними до затримки, необхідно передати (обробити) з мінімальними її значеннями в умовах високого навантаження сервісної мережної платформи. Коли алгоритм MPQ (удосконалений у [199]) був вимкнений, черга для таких потоків не

використовувалась, але коли MRQ був застосований – її довжина почала зростати. Отже, на рис. 6.10 показано розподіл тривалості затримки пакетів для потоку навантаження IPTV сервісу протягом усієї тривалості експерименту [199, 205].

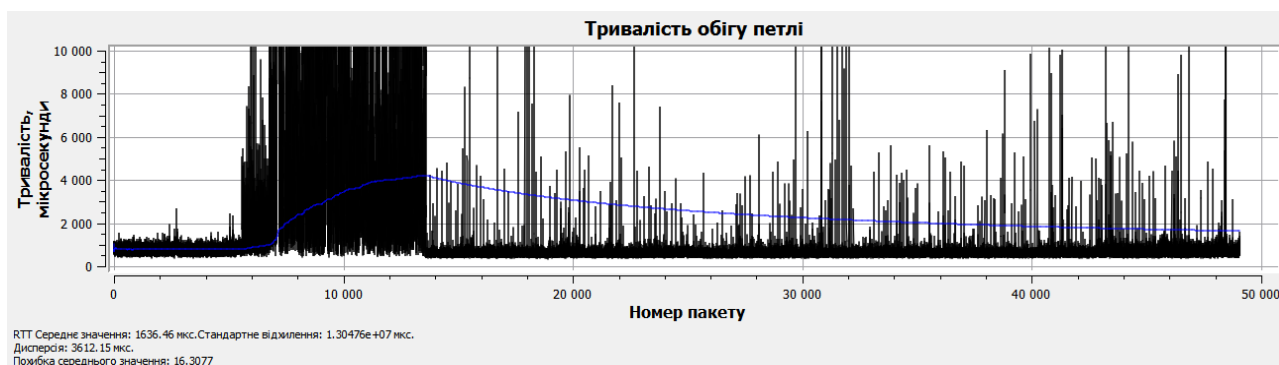


Рис. 6.10. Наскрізна затримка при передаванні трафіку IPTV сервісу через агрегуючий маршрутизатор без застосування MRQ та при його використанні.

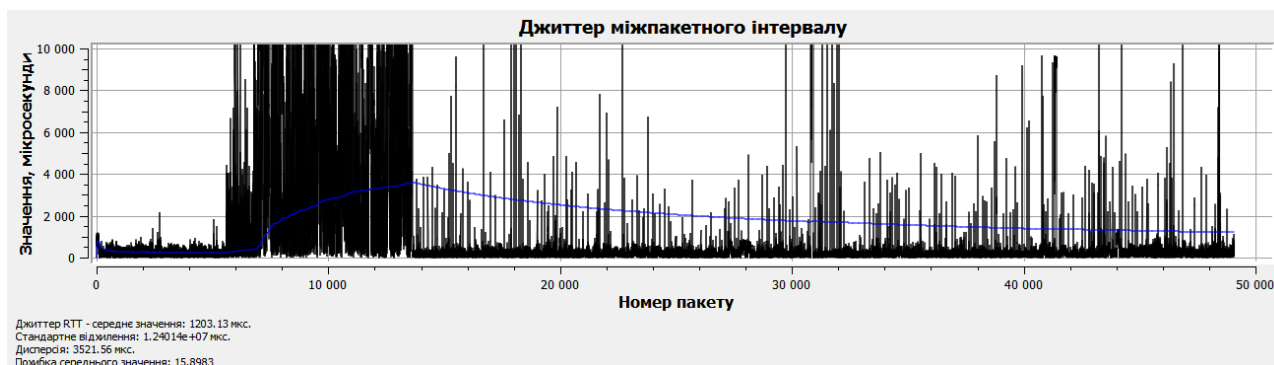


Рис. 6.11. Джиттер при передаванні трафіку IPTV сервісу через агрегуючий маршрутизатор без застосування MRQ та при його використанні.

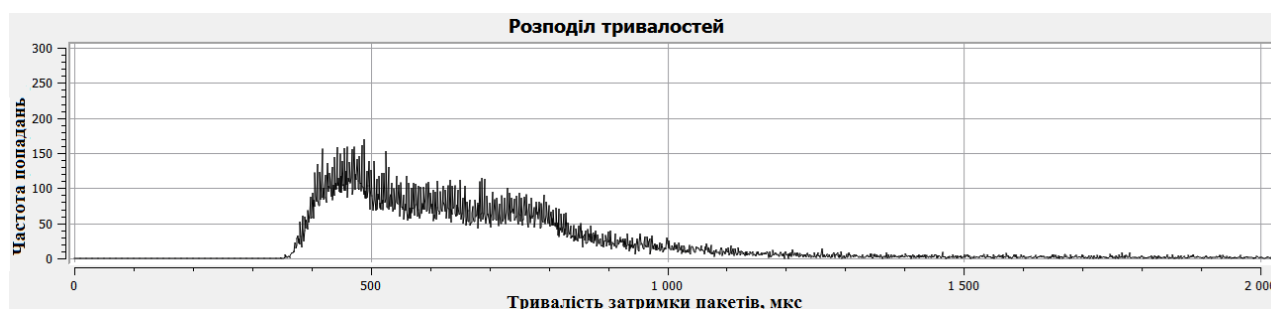


Рис. 6.12. Розподіл тривалостей затримки передавання пакетів.

Застосування розроблених моделей та алгоритмів покращення якості обслуговування потоків реального часу забезпечує підвищення рівня якості сервісу у мережі в ідеальних умовах до 5 разів. Такі оцінки можуть бути одержаними на основі визначення показника стабільності часових параметрів

якості, якими є джитер та тривалість затримки. Очевидно, що чим менші значення джитеру та тривалості затримки забезпечує метод гарантування якості обслуговування, тим вищою стає якість сервісу, що може бути досягнута в мережній системі. Для підтвердження ефективності розроблених моделей проведено дослідження тривалості затримки та джитеру у реальній мережі із застосуванням диференціації потоків сервісного навантаження та алгоритму керування чергами WFQ, а також із застосуванням удосконаленого алгоритму MRQ.

Для кількісної оцінки досягнутого ефекту запропоновано використовувати коефіцієнти, які визначаються відношеннями середнього джитера (6.1) та тривалості затримки (6.2) передавання пакетів трафіку при застосуванні WFQ і MRQ алгоритмів, відповідно:

$$K_t = \frac{T_{MPQ}}{T_{WFQ}}, \quad (6.1)$$

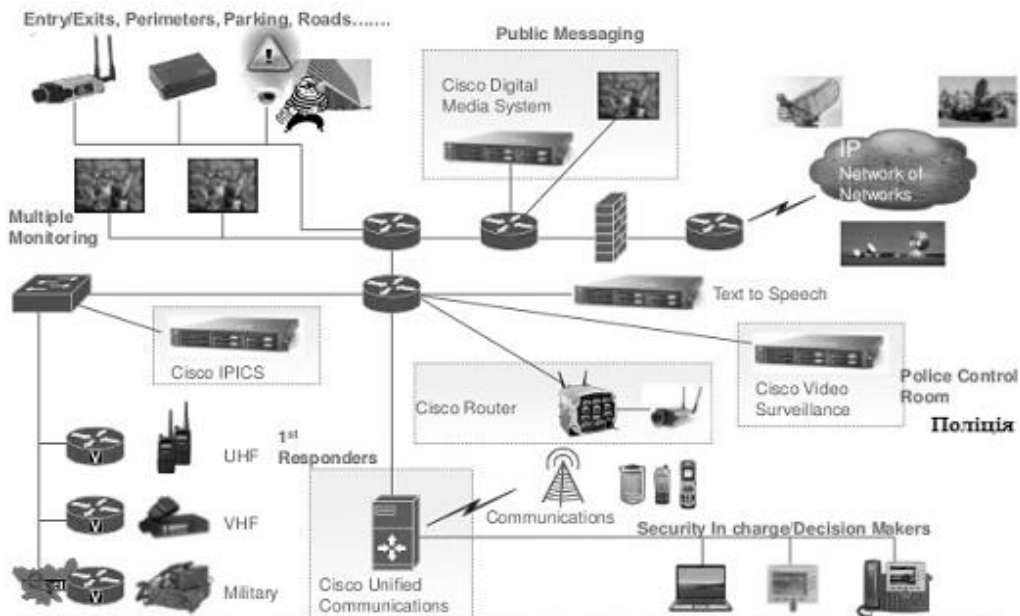
$$K_j = \frac{J_{MPQ}}{J_{WFQ}}. \quad (6.2)$$

Графіки, які демонструють час проходження пакетів трафіку (рис. 6.10) і джитер (рис. 6.11) дають змогу зробити висновок, що удосконалений алгоритм MRQ і спосіб визначення пріоритетів обслуговування сервісного навантаження дають змогу досягнути значного зниження джитера (до десяти разів) і стабілізувати часову затримку при обробленні пакетів маршрутизаторами на мінімально можливому рівні. Таким чином, якщо удосконалений MRQ встановлено на всіх маршрутизаторах мережної платформи, то рівень якості сервісу для поточкових сервісних застосувань в режимі реального часу може бути значно покращена.

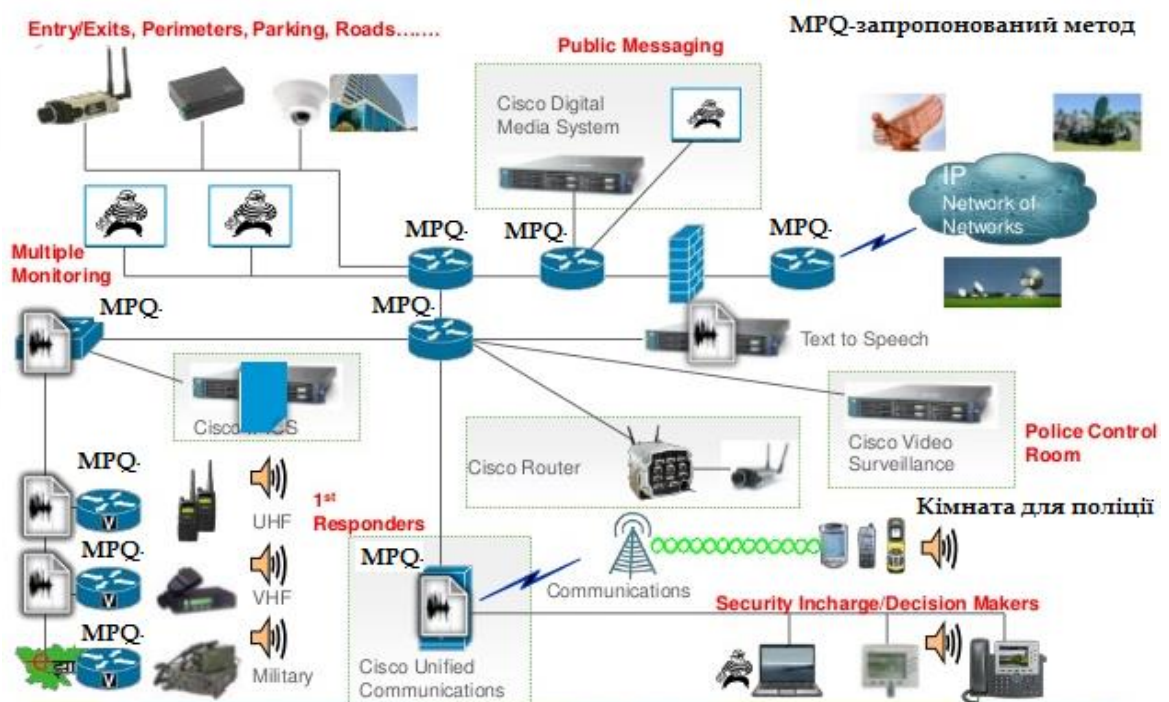
6.1.2. Вдосконалена телекомунікаційна платформа IaaS магістрального рівня з можливістю організації масштабованих мереж цивільного та спеціального призначення

Аналізуючи тенденції розвитку телекомунікаційних мережних платформ для сервісної інфраструктури спеціального призначення провідних країн світу [25, 204, 219], необхідно відмітити потребу формування єдиного адаптивного інформаційно-функціонального простору для оперативного керування, а також узгодження дій у кризових ситуаціях, у тому числі військово-політичних, економічних, техногенних, гуманітарних, екологічних, під час антитерористичних операцій і інших з використанням нових технологій, що, наприклад, забезпечить можливість стійкого та раціонального поєднання централізованого і розподіленого використання інформації на всіх рівнях управління (рис. 6.13).

В запропонованій концепції управління інформаційними потоками даних виникає можливість їх спрямування не за найкоротшими шляхами, що обчислені за допомогою традиційного протоколу маршрутизації, а через менш завантажені вузли й канали зв'язку. При правильному конфігуруванні потоків навантаження на всі фізичні канали зв'язку, маршрутизатори й комутатори [152, 157], а також застосовані методи і алгоритми обслуговування трафіку повинні бути збалансовані таким чином, щоб жоден із мережних компонентів не був недовантажений або перевантажений. Як результат, мережна платформа буде працювати більш ефективно, стабільно й передбачувано [199].



a)



б)

Рис. 6.13. Інформаційно-телекомунікаційна інфраструктура для цивільних і спеціальних цілей без застосування розробленого методу (система працює в критичних умовах – доставка повідомлень вчасно не виконана) (а) та із застосуванням запропонованого методу – оперативні повідомлення доставлено вчасно (б).

Даний підхід є актуальним для деяких державних структур, зокрема таких, як Міністерство оборони України та інших силових відомств при розв'язанні

задач підвищення оперативності доставки контенту, чутливого до часу (інформації керування, відеоспостереження, в т.ч. за периметром кордону, визначених об'єктів, зокрема в мережах радіорозвідки, ПВО-ПРО). Запропоновані рішення є також особливо актуальними для мереж, які потребують застосування ефективних методів шифрування, що створюють додаткові затримки у мережних вузлах. Описана технологія також дозволяє зберегти рівень якості надання заданого переліку мультимедійних сервісів за рахунок підвищення адаптивності транспортного сегменту телекомунікаційної IP-орієнтованої мережної платформи при оперативному розширенні зон покриття територій системами широкосмугового радіодоступу, зокрема при їх масштабуванні в польових та важкодоступних умовах за допомогою нестационарних або квазістационарних вузлів [206, 219].

6.2. Голографічна модель функціонального аналізу мережних систем.

На думку фізиків, у деякому просторовому об'ємі доволі чітко можливо уявити голографічну структуру та її властивості; більше того, щонайменше 50 років назад були успішно створені перші непогані зразки фотоголографічних об'єктів (рисуноків). Фотоголограма, для прикладу, може зафіксувати визначену множину амплітуд та фаз у деякій площинній проекції, що відбиває експонований тривимірний об'єкт, підсвічений когерентним джерелом випромінювання, на основі формування інтерференційної картини при взаємодії прямих та відбитих променів того ж самого джерела. Відповідне (лазерне) когерентне випромінювання має однакові часо-частотні характеристики, але на цільовій поверхні, що міститиме майбутню голограму інтерферує за рахунок різниці фаз, враховуючи амплітудні властивості проекції відбитих від експонованого об'єкта хвиль [207]. Для відновлення оптичного зображення початкового об'єкта, потрібне еталонне джерело (лазерного) когерентного випромінювання для підсвічування площинного голографічного

зразка, на якому записана відповідна голографічна картина. В принципі, можливо створити голограму для будь-яких хвиль [207, 208].

Також відомо [209-212], проте, нажаль, не так широко, що голографічна картина є неподільною за змістом щонайменше у вимірі $D-1$, маючи на увазі відображення об'єкта вимірності D . Це означає, що, маючи лише невелику частину записаного (площинного) голографічного зразка, ми в змозі відновити цілісну картину початкового експонованого об'єкта, проте з гіршою роздільною здатністю. Для прикладу, при голографічній реконструкції зображення, кожна окрема область площини фотографічного носія (пластини) містить цілісне зображення [209]. Очевидно, що описані вище принципи можуть бути застосованими до будь-якої голограми, що була створена на основі взаємодій хвильової природи відносно деякого заданого досліджуваного об'єкта. На думку автора, світова метамережа, що містить численні підмережі, впродовж свого існування забезпечує деякі періодичні, або ж у деякій мірі періодичні процеси, що пов'язані із розповсюдженням трафіка [136]. Розглядаючи взаємопоєднання вузлів, ці процеси можуть бути представленими, як множина хвильових функцій, виходячи, у загальному, з властивостей їх самоподібності (циклічності). Розповсюдження трафіка, зокрема реалізація сервісів його маршрутизації та перерозподілу є пульсуючими та, по суті, періодичними хвилевими процесами, що мають чітку фізичну природу своїх носіїв, що, з одної сторони, відмінна від природи світла чи акустичних хвиль, проте впровадження широкосмугових фотонних мереж дещо нівелює зазначене протиріччя. З іншої сторони, всі ці взаємопов'язані процеси можуть розглядатись у числовій формі, як похідні від структури деякого багатовимірною голографічного об'єкту. Відповідно, маючи математичний опис голографічної «картини» цих процесів, ми можемо відновити наперед задані пов'язані мережні метадані меншої вимірності для деякого скінченного проміжку часу, причому, навіть маючи лише частину голографічної «картини». Такими даними можуть бути мережні з'єднання в топологічному розумінні (як фізичні, так і віртуальні), розподіл значень обсягів трафіку в мережній системі

та його динаміка, прогнозована поведінка мережної системи (виходячи з більшої вимірності голографічних мережних метаданих і у випадку відомих параметрів, зокрема структури для модифікацій мережної платформи) тощо.

6.2.1. Голографічна модель мережної системи.

Мета даного розділу дисертаційної роботи – визначення методологічних принципів та підходів для узагальненого математичного опису мережних метаданих та їх відновлення (виділення) у цифровій формі відносно відповідних мережних структур на основі принципів цифрової голографії [213, 214].

Таким чином, необхідно розв'язати два важливих завдання. Перше має на меті створення голографічного опису часо-частотних мережних властивостей, а друге – розгляд методів оброблення існуючих мережних метаданих для оцінювання, прогнозування та виділення визначених властивостей мережної системи, що аналізується (розділ 6.2.2) та окремого її вузла (розділ 6.2.3).

Зрозуміло, що кожний мережний вузол повинен мати засоби для моніторингу і фіксації пов'язаних із його функціонуванням мережних метаданих. Це не обов'язково повинна бути інформація, що передається через мережу. Перш за все, слід розглядати властивості та динаміку трафіку у кожній точці мережної системи. По суті, ця інформація поділяється на службові мережні повідомлення, що оновлюють формальні представлення про поточну мережну структуру для цілей маршрутизації, а також деякий обсяг інформації, що описує часо-частотний характер міжвузлового навантаження. Відповідні модулі для проведення розрахунків, які пов'язані з формуванням вищенаведених даних повинні бути реалізованими щонайменше у кожному граничному вузлі мережної системи, та, як це зазвичай реалізується в парадигмі хмарних мережних систем, подібні модулі виконують заданий за глибиною аналіз процедур обміну сервісним навантаженням. Таким чином, слід описати сервісне навантаження в кожному з N мережних вузлів, що має порядковий номер z , використовуючи деякі комплексні змінні [214]. Для опису згаданих

параметрів у цих вузлах потрібно припустити, що відповідними вузлами формується багатошарова гіперструктура, а кожен з них має власну площину z , що агрегує параметризовані з'єднання від інших. Тобто, потрібно розглянути процеси передавання навантаження (його амплітуду і періодичні пульсації) для кожного дискретного шару мережного об'єкту. Іншими словами, кожен вузол буде мати власну передавальну площину з координатним номером z (див. рис. 6.14), а кожна окрема точка на цій площині описуватиме її (вузла) з'єднання з іншими площинами (вузлами) у термінах часо-частотних характеристик навантаження, використовуючи загальні наскрізні декартові координати $(x, y; z)$ для опису системних міжшарових взаємозв'язків при їх (шарів-вузлів) взаємному розміщенні в єдиному просторовому континуумі комплексного мережного об'єкта. Відповідно, комплексні часо-частотні змінні мережного об'єкта $O(x, y, z)$ можна розглядати, як комплексну інтенсивність трафіку $\lambda_{x,y,z}$ до відповідної точки обміну мережного шару (площини вузла) z з координатами $(x, y; z)$ на площині, від іншої точки обміну мережного шару (площини вузла), що розташований у тому самому континуумі з загальними наскрізними декартовими координатами. Оскільки згадані вище змінні є комплексними, то приймемо, що їх дійсна частина відображає інтенсивність службового трафіку (внаслідок його топологічно-залежного характеру відносно структури мережної системи), а уявна – використовується для опису обсягів трафіку між окремими мережними вузлами (внаслідок його наскрізного поширення через мережну структуру та періодичного характеру пульсацій). Використовуючи роботи [136, 214], запишемо віртуалізовану передавальну функцію (аналог ОТФ):

$$\begin{aligned} \aleph(k_x, k_y; z) = & \exp\left\{j \frac{z}{2k_0} (k_x^2 + k_y^2)\right\} \times \\ & \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} p_1(\tilde{x}, \tilde{y}) p_2\left(\tilde{x} + \frac{f}{k_0} k_x, \tilde{y} + \frac{f}{k_0} k_y\right) \\ & \times \exp\left\{j \frac{z}{f} (\tilde{x} k_x + \tilde{y} k_y)\right\} d\tilde{x} d\tilde{y}, \end{aligned} \quad (6.3)$$

де f є дистанційною метрикою мережної системи (прийнемо $f = N$), $k_0 = \frac{2\pi}{\lambda_{\max} f}$, а λ_{\max} - є константою, що відображає максимально можливу інтенсивність навантаження у лінії зв'язку між вузлами всієї мережної системи, що розглядається; $p_1(x, y)$ та $p_2(x, y)$ є функціями апертури для створення цифрового голографічного образу мережного об'єкта, відповідно: $p_1(x, y) = 1$ та $p_2(x, y) = \delta(x, y)$, які у складі (6.3) використовуються для синхронних розрахунків цифрового голографічного образу у модулях вузлів моніторингу і фіксації мережних потоків для одержання результуючої повної голографічної картини мережних функціональних метаданих.

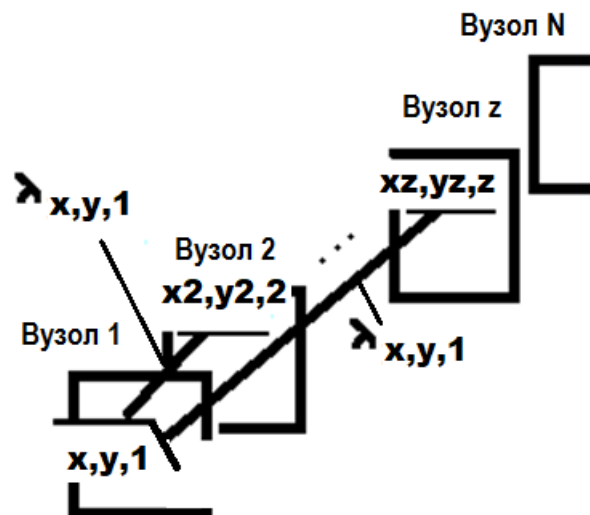


Рис. 6.14. Мережні вузли, як декартові площини у єдиному мережному просторовому континуумі. Показано зв'язки від Вузла 2 та Вузла z до Вузла 1.

Отже, після виконання відповідної фіксації процесів обміну даними в мережному об'єкті $O(x, y, z)$, необхідно розрахувати загальний просторовий імпульсний відклик мережної системи (у єдиному мережному просторовому континуумі), що розглядається по відношенню до всіх задіяних вузлів, користуючись (6.3) та використовуючи зворотне швидке перетворення Фур'є:

$$h(x, y; z) = \mathfrak{F}^{-1} \left\{ \mathfrak{S}(k_x, k_y; z) \right\}. \quad (6.4)$$

Після перетворень (6.3-6.4), одержаний опис функціональних мережних метаданих конвертується у компактну цифрову форму, а саме – комплексний голографічний цифровий масив виду (символ * означає двовимірну згортку):

$$g(x, y) = \sum_{i=1}^N \left(|O(x, y, f \cdot i)|^2 * h(x, y; f \cdot i) \right) \quad (6.5)$$

6.2.2. Визначення функціональних метаданих мережної системи на основі її цифрового голографічного представлення.

Відтак, у випадку часткової відмови мережної системи, узагальнена інформація про функціональні процеси, що в ній протікають може бути відновлена на вимогу, використовуючи хоча би частину голографічного представлення оцифрованих мережних метаданих (6.5). Розглянемо відновлення цілісної картини функціональних метаданих мережної системи на основі її цифрового голографічного представлення з використанням підходу до зворотної реконструкції зображень [215], причому верхній індекс ^{mod} використано для опису випадку, коли виконується прогнозування властивостей мережної системи при зміні умов її функціонування та/або структури. Використовуючи рівняння (6.5), конвертуємо 2D цифрове голографічне представлення $g(x, y)$ розміру $N \times N$ у вектор довжиною N^2 із застосуванням лексикографічного впорядкування. Відповідно, $|O(x, y, z)|^2$ стає ϕ_z . З метою прогнозування мережних властивостей, для нашого випадку, загальний просторовий імпульсний відклик *модифікованої* мережної структури у формі щонайменше частково наповненої модифікованої матриці H_z^{mod} розміром $N^2 \times N^2$ формується на основі $h^{\text{mod}}(x, y; z)$, що дає нам $H_z^{\text{mod}} \phi_z \sim |O(x, y, z)|^2 * h^{\text{mod}}(x, y; z)$ після лексикографічного впорядкування. Таким чином, (6.5) можна переписати, як:

$$g = H^{\text{mod}} \phi + \eta, \quad (6.6)$$

де η є вектором гаусівського шуму довжиною N^2 . Відповідно,

$$H^{\text{mod}} = [H^{\text{mod}}_1 \quad H^{\text{mod}}_2 \dots H^{\text{mod}}_z \dots H^{\text{mod}}_N] \text{ та } \phi = \begin{bmatrix} \phi_1 \\ \phi_2 \\ \vdots \\ \phi_N \end{bmatrix}.$$

Аналітичний розв'язок [216] можна представити, як:

$$\hat{\phi} = H^{\text{mod}T} (H^{\text{mod}} H^{\text{mod}T} + \mu 1)^{-1} g. \quad (6.7)$$

Тут, μ є лагранжіаном, а 1 – одиничною матрицею. У іншій формі цей розв'язок може бути представлений, як [214]:

$$\hat{\phi} = \arg \min \|H^{\text{mod}} \phi - g\|^2 + \mu \|g\|^2. \quad (6.8)$$

Де $\|\cdot\|$ описує квадратичну форму вектора, а член $\mu \|g\|^2$ - представляє параметри регуляризації у відповідності до термінів нечітко поставленої інверсної реконструктивної задачі.

Рішення (6.8) забезпечує прогнозування комплексних значень інтенсивності мережних потоків, їх розподілу (або одержання відновленої картини функціональних метаданих мережної системи, причому враховуючи внесення можливих оптимізацій у її структуру) у всій *модифікованій* мережній структурі, використовуючи попередньо сформоване базове цифрове голографічне представлення функціональних мережних метаданих об'єкту g та його відповідне, хоча би частково надане, модифіковане представлення h^{mod} .

6.2.3. Точкове відновлення функціональних мережних метаданих.

Для *часткового* відновлення функціональних метаданих мережної системи (щодо бажаного мережного вузла) потрібні відповідний номер площини-січення структури початкового мережного об'єкту z та проведення згортки цифрового представлення комплексних голографічних метаданих з узгодженим фільтром на передавальній площині вузла z . Узгоджений фільтр може бути

побудований на основі (6.4-6.5) як $h^*(x, y; z) = h(x, y; -z) = j \frac{k_0}{2\pi z} e^{\left(-j \frac{k_0}{2z}(x^2+y^2)\right)}$, причому $h^*(x, y; z) * h(x, y; z) = \delta(x, y)$ [214], після чого можливо записати розв'язок [136]:

$$\begin{aligned}
 g(x, y) * h^*(x, y; z_1) &= \sum_{i=1}^N \left(|O(x, y, z_i)|^2 * h(x, y; z_i) \right) \\
 &\quad * h^*(x, y; z_1) = |O(x, y, z_1)|^2 + \\
 &\quad + \sum_{i=2}^N |O(x, y, z_i)|^2 * h(x, y; z_i) * h^*(x, y; z_1).
 \end{aligned} \tag{6.9}$$

Використаємо перший член $|O(x, y, z)|^2$ як найбільш точну частину розв'язку (6.9), що містить відповідний мережний об'єкт із даними про просторовий розподіл функціональних властивостей мережної системи для обраного вузла (наприклад – про розподіл інтенсивностей потоків навантаження), що описані та відновлені для нього, як для невіддільної частини цілісної мережної платформи з використанням голографічних принципів. Другий член за характером відноситься до шуму голографічного дефокусування від інших компонентів мережної системи (відображає мережні потоки між вузлами). Його негативний вплив збільшується при відновленні мережних метаданих на основі використання лише частини цифрового голографічного представлення комплексних мережних метаданих, внаслідок його пошкодження або часткової втрати. Таким чином, перший член дає нам дійсну частину комплексного розв'язку (як правило - службовий трафік), а другий – уявну, що відображає пульсуючі мережні потоки між вузлами мережної структури (див. розділ 6.2.1). Прогнозування розподілу трафіку в процесі модифікацій мережної структури можливо реалізувати на основі використання рівняння (6.9) у спосіб, що розглянутий у розділі 6.2.2 в рамках розрахунку та використання імпульсного відклику модифікованої мережної структури $h^{\text{mod}}(x, y; z)$.

6.3. Метод скоординованої фіксації мережних метаданих телекомунікаційних платформ в центрах оброблення даних національного рівня

Володіння інформацією про активність абонентів телекомунікаційних мереж у глобальному аспекті з метою гарантування національної безпеки є прерогативою низки державних органів України [25]. Поділяючи глобальні телекомунікаційні мережі на фіксований та мобільний сегменти передавання даних, ми можемо констатувати, що мережі мобільного зв'язку мають вбудовані механізми для глобальної взаємодії в рамках розв'язання проблеми встановлення контролю за передаванням інформації з використанням відповідних персональних засобів зв'язку. Якщо фіксація метаданих з'єднань та документальна локалізація абонентів провайдерів фіксованого зв'язку згідно чинного законодавства України є функцією відповідних провайдерів, а отже може бути виконана через контроль у точках доступу провайдерів та точках обміну трафіком національного рівня (NAP, N(UA)-IX для мережі Інтернет), а також точках контролю мережі сигналізації (для ТМЗК – в рамках SCP/ISUP), то отримання інформації про абонентів мереж рухомого зв'язку є дещо складнішим. Умовно можна вважати задачі фіксації такої інформації поділеними на наступні дві категорії:

1. Фіксація метаданих щодо активності абонентів національних мереж мобільного зв'язку в національному та міжнародному роумінгу;

2. Фіксація метаданих щодо активності абонентів закордонних мереж мобільного зв'язку в гостьовому національному та міжнародному роумінгу.

Задачі першої категорії розв'язуються шляхом стандартних процедур обміну сигналізаційною інформацією оператором мобільного зв'язку через його контролери сигналізації (підсистема SS7 MAP) при шлюзових комутаційних станціях та реєстри HLR/VLR (для національного роумінгу) або лише реєстр HLR (у випадку міжнародного роумінгу) за принципом реєстрації комунікаційних подій, зокрема – оновлення місцезнаходження (LAI/MS Service Area). Активні комунікаційні події за участю абонента ефективно

фіксуються за посередництва підсистеми білінгу шлюзової комутаційної станції. Локалізація абонента у глобальному масштабі без явного застосування спеціальних заходів (наприклад супутникового радіомоніторингу території) можлива з точністю до зони обслуговування комутаційної станції. При цьому глобальний ідентифікатор абонента IMSI є відомим національному оператору мобільного зв'язку.

Реалізація задач другої категорії є легальною і найменш складною в національному роумінгу мереж мобільного зв'язку України після реєстрації в них абонентом іноземної мережі свого IMSI, а у глобальному ж масштабі може здійснюватися, наприклад, шляхом фіксації активності за даним IMSI серією спроб роумінгових запитів з метою отримання інформації MSRN до шлюзових комутаційних станцій потенційних країн перебування через шлюзову комутаційну станцію від імені реєстру HLR одного з національних операторів мобільного зв'язку. Отриманий MSRN свідчитиме про присутність абонента у роумінговій мережі іноземного оператора, який його надіслав. Щоправда, у подібних запитах може бути відмовлено, внаслідок налаштувань політики безпеки мережі сигналізації приймаючого оператора, а також у випадку, коли абонент потрапляє до супутникового роумінгу. У випадках, коли існує відносно необмежений доступ, або засоби для створення такого доступу по мережі сигналізації MAP до баз операторів HLR/VLR глобальної мережі рухомого зв'язку, існує й можливість безперешкодно створювати метасховища активності їх абонентів, включно з локалізацією їх комунікаційного обладнання. За-значимо, що США забезпечили собі оброблення всіх зовнішніх з'єднань, зокрема й Інтернет-трафіку в магістралях Австралія-Азія-Європа та Південна Америка-Європа потужностями відповідних підрозділів АНБ. Крім цього, Великобританія де-факто монополює трафік, що проходить у напрямку мережних систем країн Африки [217, 220]. Ці дані підтверджено також за результатами експериментальних досліджень, які були проведені шляхом виконання трасування маршрутів передавання пакетів у відповідних напрямках.

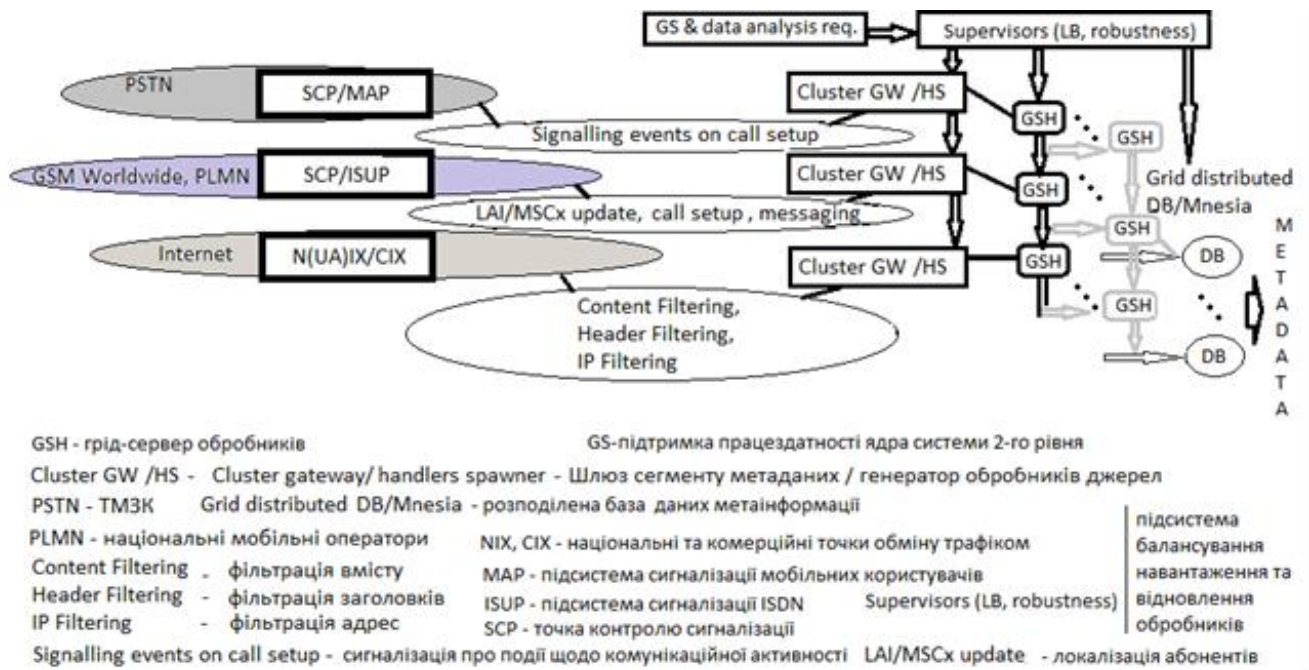


Рис. 6.15. Структурно-функціональна схема ЦОД сервісної мережної платформи фіксації комунікаційних метаданих мереж зв'язку [220] (SaaS).

Оцінимо обчислювальну складність для апаратної реалізації процесів фіксації метаданих щодо активності абонентів мереж зв'язку (рис. 6.15). Нехай в середньому у годину-пік активними є N абонентів мереж мобільного зв'язку, що підлягають моніторингу. Для оброблення подій кожного з них, необхідно створити у наведеній платформі для збереження метаданих щонайменше один «легкий» незалежний паралельний процес, який оброблятиме події та прийматиме рішення щодо внесення їх у бази даних.

Хмарне розпаралелення низькопрофільованого за функціями обчислювального навантаження передбачає використання технологій асинхронного обміну між процесами, загальна ефективна кількість яких на одне сучасне серверне ядро з M доступних може перевищувати 90 тисяч [221]. Отже, за умови використання, до прикладу, функціональної мови системного програмування розподілених обчислень Erlang, необхідно, за попередніми оцінками, $N \cdot (M \cdot 9 \cdot 10^4) - 1$ апаратних серверів. Для прикладу, якщо моніторинг відбувається у глобальному масштабі, то активними є приблизно $2,5 \cdot 10^9$ паралельних комунікаційних процесів мереж рухомого зв'язку [218, 220]. Це

дає нам, за умови використання прямої обробки RTMP повідомлень кожним згенерованим процесом, при числі ядер $M=8$, кількість необхідних серверів ЦОД сервісної мережної платформи фіксації всієї метаданих мереж зв'язку планети менше, ніж 3500 одиниць. Слід додати, що грид-мережа ЦОД в межах такої метабази має бути побудована виключно за оптичними технологіями з пропускними спроможностями не нижче рівня 10 Гбіт/с. Звідси стає зрозуміло, що в межах національної системи електрозв'язку України задача фіксації подібної метаданих мереж зв'язку в принципі не вимагає складних апаратних та часових ресурсів, за умови правильного вибору архітектури апаратно-програмної платформи, наприклад – шляхом реалізації архітектурного об'єднання кількох ЦОД на каналному рівні (рис. 6.16) [63]. Необхідні коефіцієнти доступності на рівнях PaaS, SaaS покращено до рівня 0,99999.

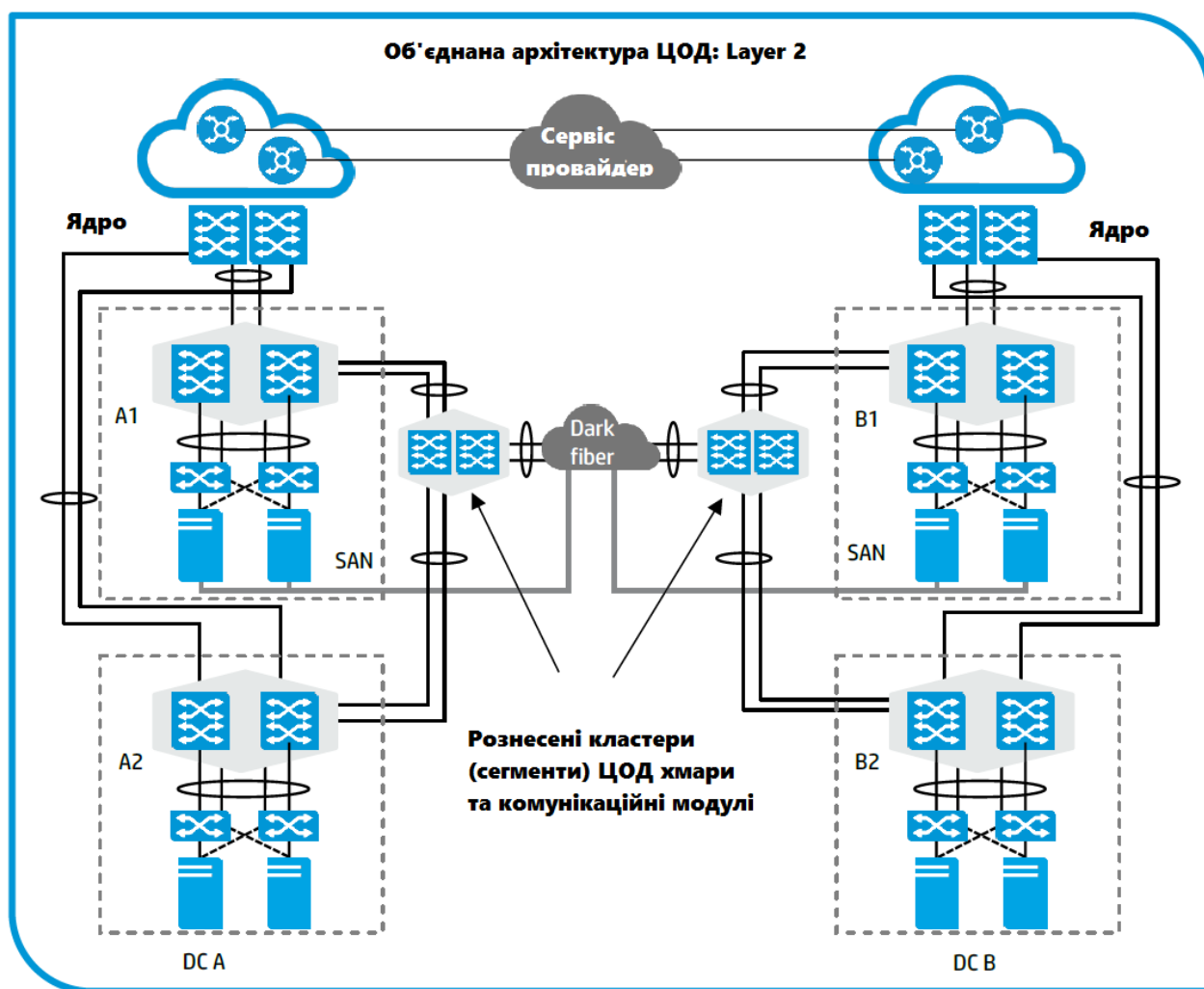


Рис. 6.16. Об'єднана архітектура ЦОД сервісної мережної платформи фіксації комунікаційних метаданих мереж зв'язку на рівні L2 (PaaS).

6.4. Узагальнена методологія синтезу телекомунікаційних сервісних платформ національного масштабу.

На основі проведених у дисертаційній роботі досліджень було сформовано низку методів, які умовно можна поділити на методи покращення параметрів ХааS реалізацій ТКСП та методи підтримки функціональної стійкості ТКСП (див. рис. 6.17). Функціональна стійкість представляється не кількісним критерієм, що, по суті, є похідним від критеріїв продуктивності та сервісної (або компонентної) доступності ХааS реалізації, що розглядається, при цьому визначаються правила сегментації та рекомендації щодо захисту ТКСП від функціональних впливів іззовні. Таким чином, у 1-6 розділах дисертаційної роботи сформовано та докладно розглянуто елементи методології синтезу телекомунікаційних сервісних платформ національного масштабу (див. рис. 6.17). На основі цих елементів, а також допоміжних методів та підходів, які виходять за рамки проблематики досліджень цієї дисертаційної роботи було сформовано ієрархічну методологію синтезу телекомунікаційних сервісних платформ національного масштабу (див. рис. 6.18). Вона, окрім зазначених на рис. 6.17 компонентів, включає також метод експертних оцінок, метод Ватутіна [239, 240] для розрахунку ступеню паралельності структури та/або алгоритму відповідного рівня сервісної реалізації ХааS на основі побудованої граф-моделі. Метод експертних оцінок передбачає агрегування одержаних в результаті застосування розробленої методології результатів для цілісного врахування досвіду фахівців у сфері ТКСП і особливостей їх прикладної реалізації під ті чи інші цілі (у поточних умовах функціонування).

Оскільки кожен рівень реалізації (та, відповідно, представлення) ХааS ТКСП вимагає більш детального розгляду, процедури адаптації рівнів реалізації телекомунікаційних сервісних платформ (SaaS, PaaS, IaaS) напрацьовано та детально представлено на рис. 6.19-6.21, відповідно у вигляді узагальнених стратегій адаптації. Адаптація IaaS рівня реалізації передбачає використання принципів та підходів до віртуалізації компонентів мережного обладнання з метою підтримування належного рівня QoS, основні особливості яких було детально розглянуто у дисертації Червенця В.В. [242].

Концепція	Національний сегмент глобальної інформаційної інфраструктури, як ТКСП, що оптимізується за продуктивністю, сервісною доступністю та функціональною стійкістю		
Принципи	Трансформація CEN →CBN	Впровадження «повсюдного комп'ютингу»	Масштабування ХааS архітектурних реалізацій
Моделі	Модель синтезу абстрактної реалізації ХааS (SaaS, PaaS, IaaS) платформ за критеріями продуктивності та сервісної доступності	Модель розподілу ресурсів у гетерогенних мережних системах на основі застосування методів нечіткої математики	Структурно-функціональна модель мігруючого мережного екрану
Методи покращення параметрів ХааS реалізацій	Метод диференційованого обслуговування користувачів	Метод оцінювання параметрів ХааS реалізації	Метод оптимізації розподілу ресурсів гетерогенних систем
	Метод оптимізації передавання пріоритетованого трафіку	Метод підвищення доступності вузлів шляхом наскрізного структурного трасування	Метод адаптивного резервування каналних ресурсів ТКСП
Методи підтримки функціональної стійкості ТКСП	Метод мігруючого мережного екрану	Метод фіксації метаданих мереж зв'язку	Метод голографічного представлення метаданих мереж зв'язку
	Методологія синтезу ефективних ТКСП		

Рис. 6.17. Елементи методології синтезу телекомунікаційних сервісних платформ національного масштабу.

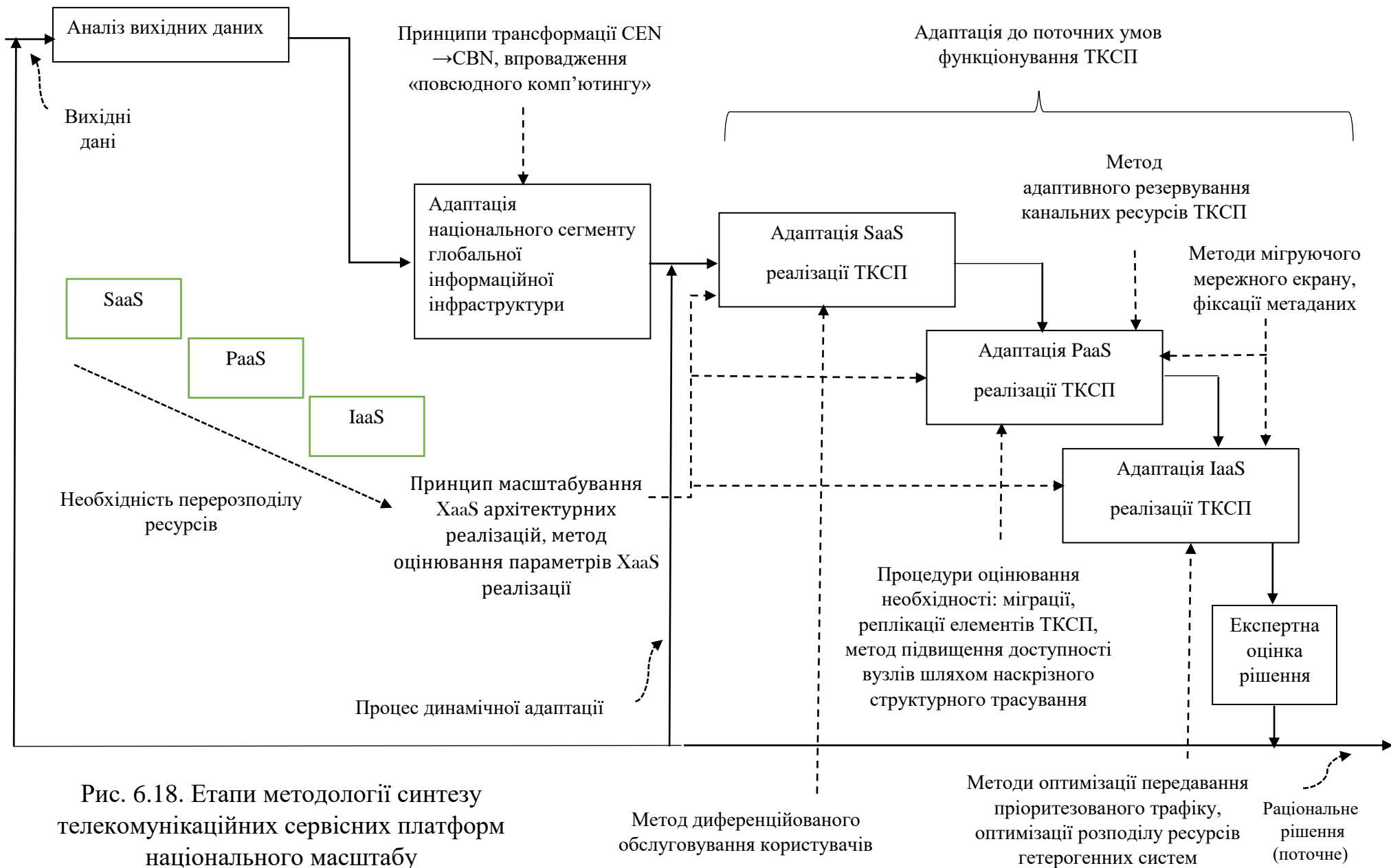


Рис. 6.18. Етапи методології синтезу телекомунікаційних сервісних платформ національного масштабу

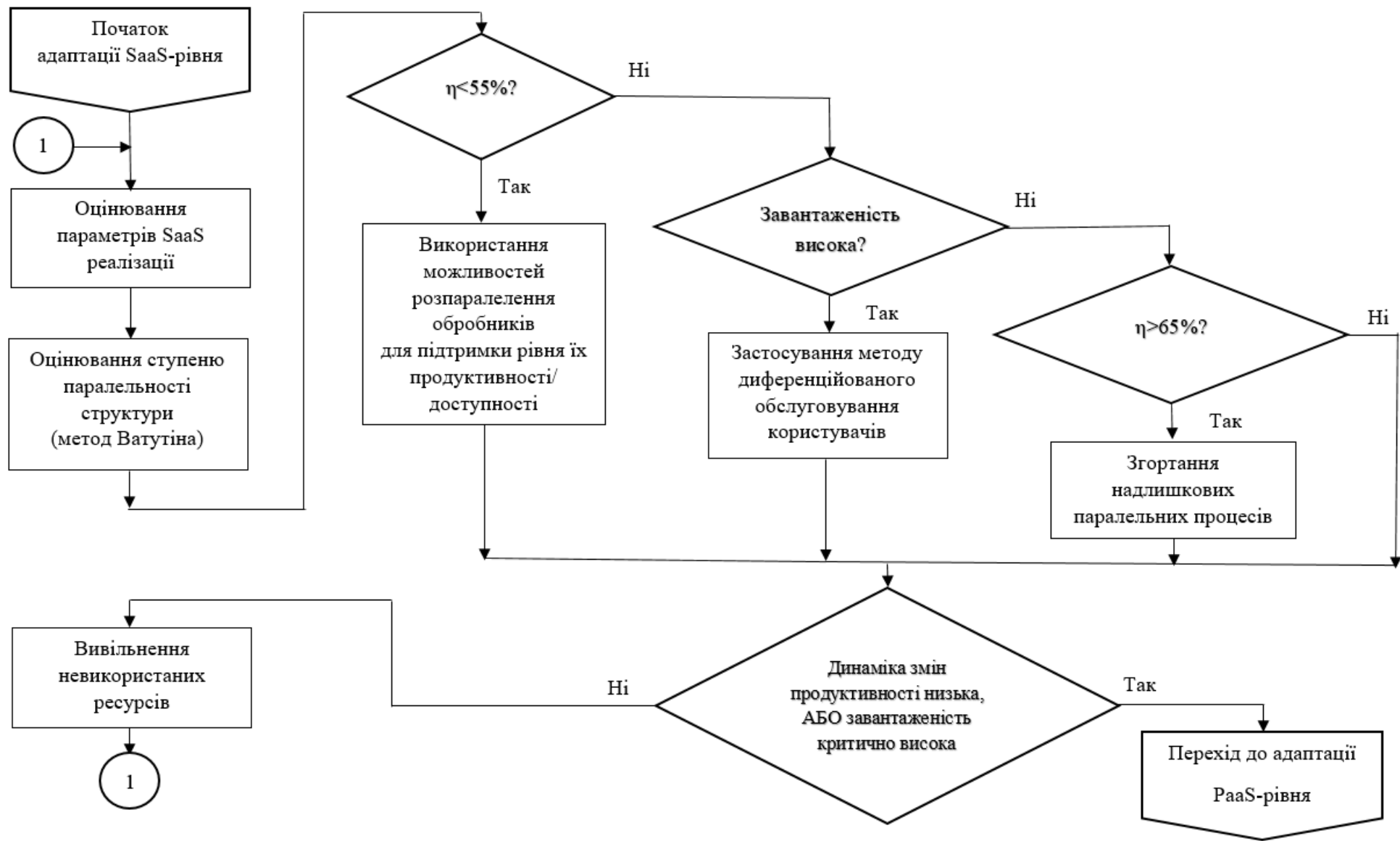


Рис. 6.19. Стратегія адаптації SaaS реалізації телекомунікаційних сервісних платформ.

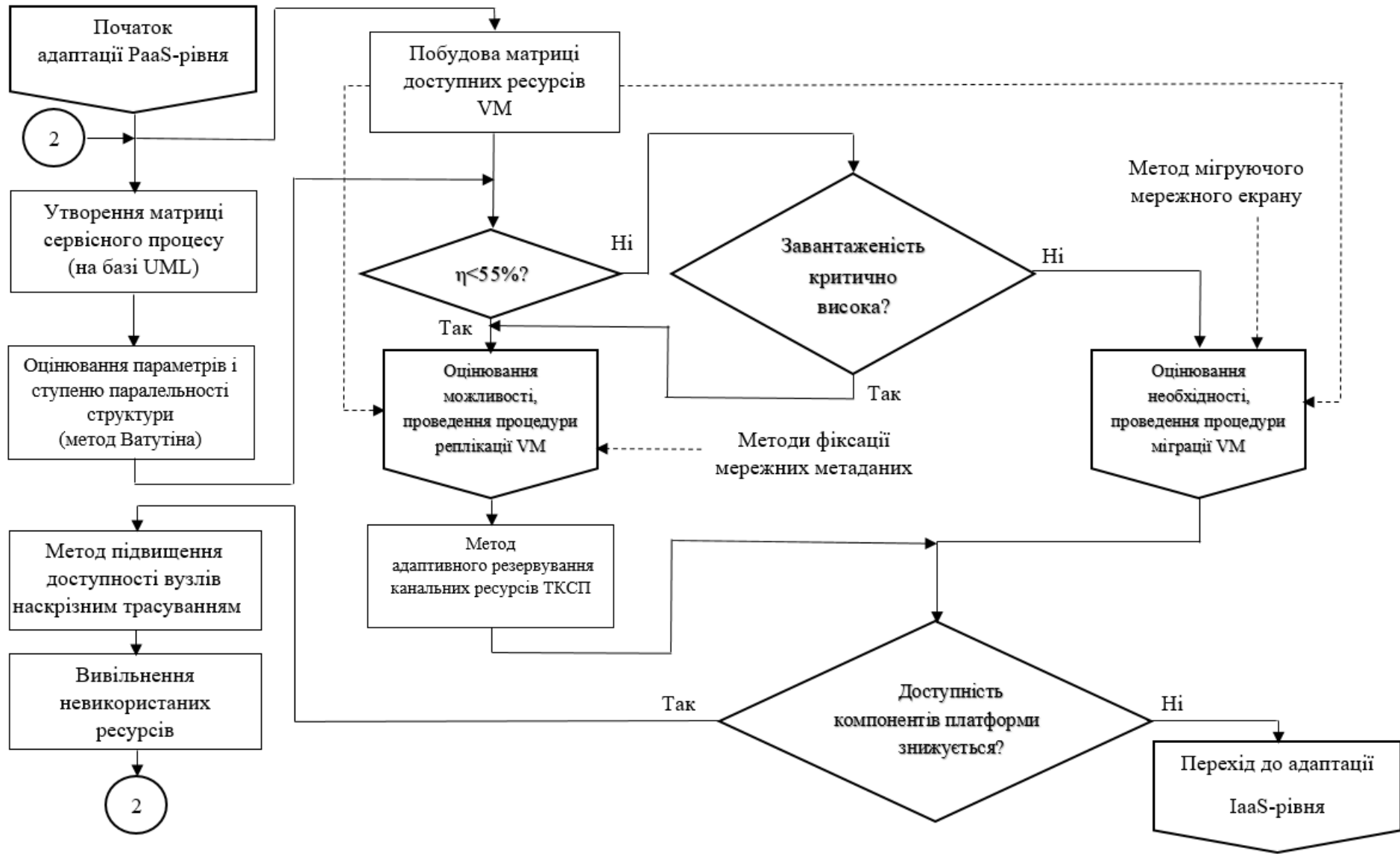


Рис. 6.20. Стратегія адаптації PaaS реалізації телекомунікаційних сервісних платформ.

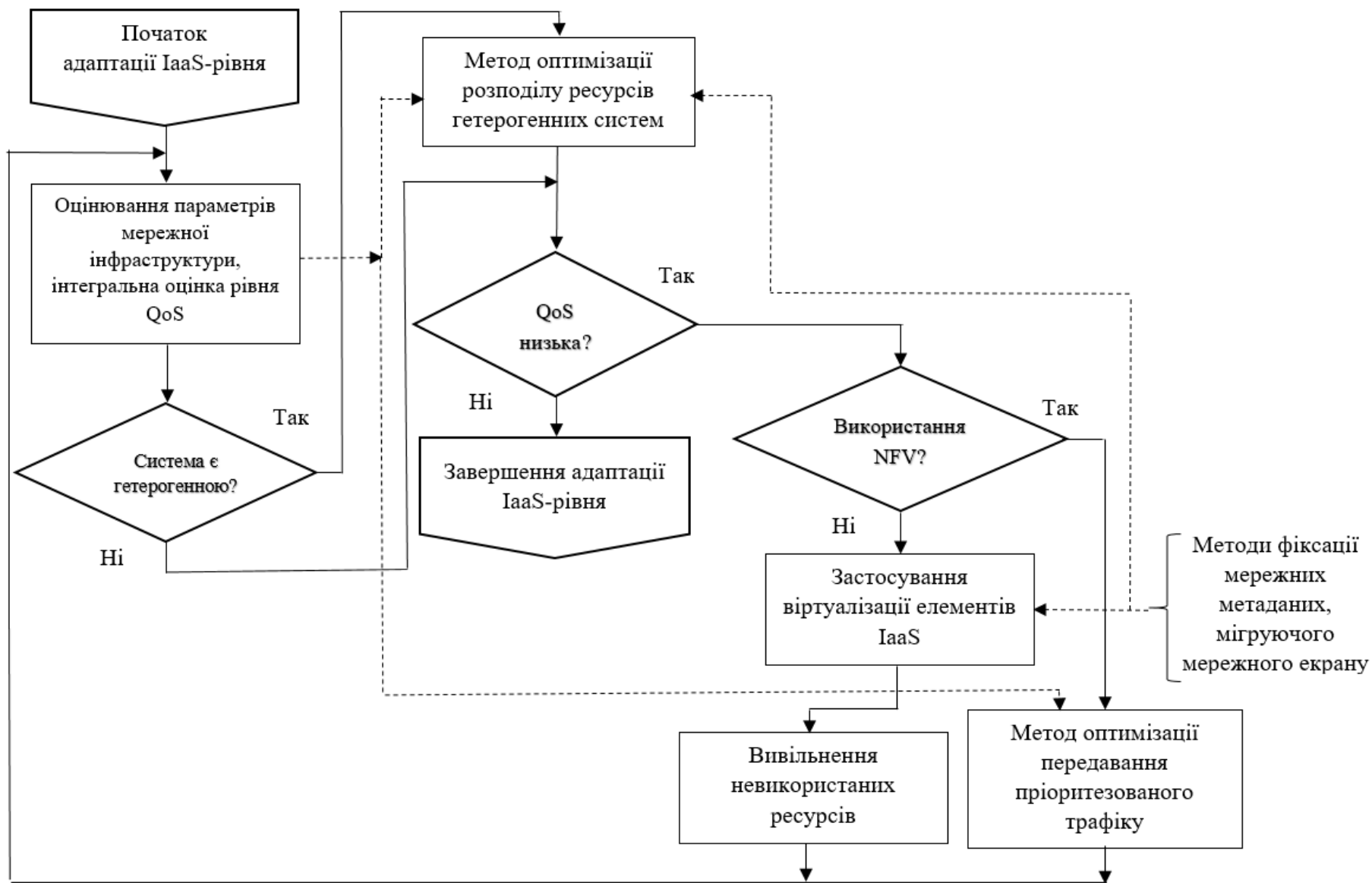


Рис. 6.21. Стратегія адаптації IaaS реалізації телекомунікаційних сервісних платформ.

На рис. 6.19 представлено стратегію адаптації SaaS реалізації телекомунікаційних сервісних платформ, за допомогою якої, зокрема, розроблено структурно-функціональну схему ЦОД сервісної мережної платформи фіксації комунікаційних метаданих мереж зв'язку [220] рис. 6.15. При цьому використовуються можливості розпаралелення обробників для підтримки рівня їх продуктивності/доступності та застосовано метод диференційованого обслуговування користувачів.

На рис. 6.20 представлено стратегію адаптації PaaS реалізації телекомунікаційних сервісних платформ, за допомогою якої, зокрема, розроблено об'єднану архітектуру ЦОД сервісної мережної платформи фіксації комунікаційних метаданих мереж зв'язку на рівні L2, а також оптимізаовано структуру ТКСП Держприкордонслужби, див. рис. 6.24 нижче. При цьому використовуються для підвищення продуктивності та сервісної доступності компонентів (VM) платформи метод адаптивного резервування каналних ресурсів ТКСП, метод підвищення доступності вузлів наскрізним трасуванням, враховано необхідність застосування методів мігруючого мережного екрану та методів фіксації мережних метаданих для забезпечення функціональної стійкості ТКСП. Процедури реплікації/міграції VM наведено у розділі 4.5.

На рис. 6.21 представлено стратегію адаптації IaaS реалізації телекомунікаційних сервісних платформ, з урахуванням якої, зокрема, розроблено методи 5 та 6 розділів цієї дисертаційної роботи, а саме метод оптимізації розподілу ресурсів гетерогенних сервісних систем на основі апарату нечіткої математики та метод оптимізації передавання пріоритезованого трафіку.

Адаптація SaaS та PaaS реалізацій передбачає застосування бібліотек для утворення інфраструктури віртуалізації, таких як VMWare та HyperV з метою ефективного програмного управління процедурами віртуалізації, реплікації, міграції віртуальних машин та, зокрема, віртуальних обробників навантаження.

З метою спрощення розрахунків сервісної доступності в рамках процесу структурно-параметричного синтезу (оцінювання параметрів структури) сервісної мережної системи, варто зазначити, що вирази (3.38-3.42) можливо апроксимувати наступним виразом (у припущенні обслуговування в ТКСП агрегованого мультисервісного трафіку):

$$P_A \approx e^{0.712d-4.955} \left(1 - (H - 0.2)^3\right) \left((1.6 + \lambda + H)N \right)^{1/d} + (2\eta(2.2 - \lambda))^{1/d}, \quad (6.10)$$

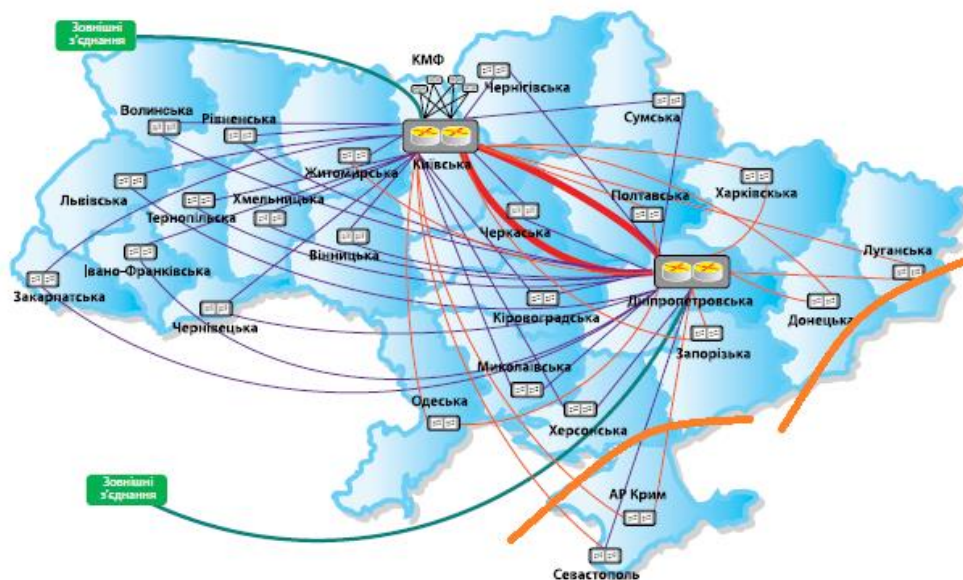
причому похибка апроксимації у граничних умовах складає не більше 2%. Позначення у (6.10) відповідають позначенням у (3.38-3.42), а коефіцієнт d характеризує ступінь оптимальності стратегії реплікації/міграції віртуалізованих компонентів у конкретній реалізації ТКСП, таким чином $d \sim 2$ приймається для консервативної стратегії реплікації/міграції (неоптимального

конфігурування динамічної ХааS реалізації), $d \sim 4$ – для умовно-оптимальної стратегії (адаптивного конфігурування ресурсів хмарної мережної платформи), λ – інтенсивність навантаження на ТКСП (нормована до максимально можливої), η – частка ESC, які функціонують, обслуговуючи потоки запитів паралельно.

6.4.1. Результати дослідження ефективності застосування методології синтезу ТКСП.

На рис. 6.22 представлено узагальнену схему мультисервісної пакетної мережі ПАТ «Укртелеком» (наведено з люб'язного дозволу цієї компанії). Протягом 2011-2016 років було проведено ряд досліджень, які стосувались оптимізації показників продуктивності та сервісної доступності відповідних IaaS та PaaS реалізацій. Застосовано розроблену методологію (рис. 6.17-6.21).

Отже, згідно запропонованої у розділі 6.4 методології синтезу телекомунікаційних сервісних платформ національного масштабу на потужностях ПАТ «Укртелеком» (див. рис. 6.22) було проведено послідовні трансформації щодо конфігурування магістрального комунікаційного обладнання компанії. При цьому враховано поступову переорієнтацію на проектування та запровадження IMS (IP Multimedia Subsystem) інфраструктури у регіональних філіях. Дослідження щодо надання сервісів у мультисервісній телекомунікаційній платформі та їх результати підтверджуються матеріалами акту впровадження результатів дисертаційної роботи.



Мережа: 30 вузлів магістральної IP/MPLS-мережі, з'єднані через DWDM

Пропускна здатність: вузли IP/MPLS мають швидкість 20 – 40 Гбіт/с

Обладнання: Juniper Networks, Cisco Systems та Huawei

Рис. 6.22. Приклад IaaS платформи, як мультисервісної пакетної мережі ПАТ «Укртелеком» для реалізації платформи національного масштабу (мережі обміну даними ДПСУ).

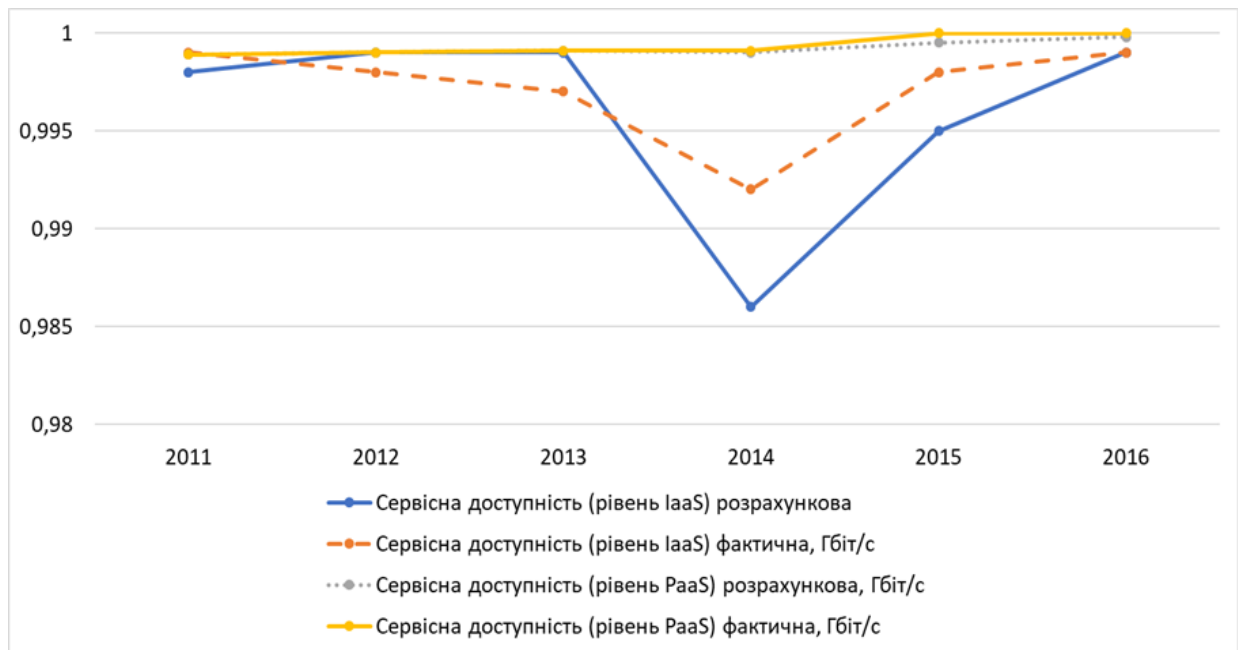
Дані моделювання за етапами трансформування мереж від CEN до CBN концепції, що виконані у середовищі Qt5.2 відносно ТКСП рис. 6.22 представлено у табл. 6.1 і табл. 6.2 та проілюстровано на рис. 6.23 а і 6.23 б, відповідно. Там же наведено для порівняння фактично досягнуті показники щодо функціонування телекомунікаційних сервісних платформ ПАТ «Укртелеком» на рівнях IaaS та PaaS. Похибка моделювання по відношенню до фактичних даних складає не більше 5-8%.

Таблиця 6.1. Порівняння прогнозованого та фактичного середньорічних показників продуктивності ТКСП ПАТ «Укртелеком».

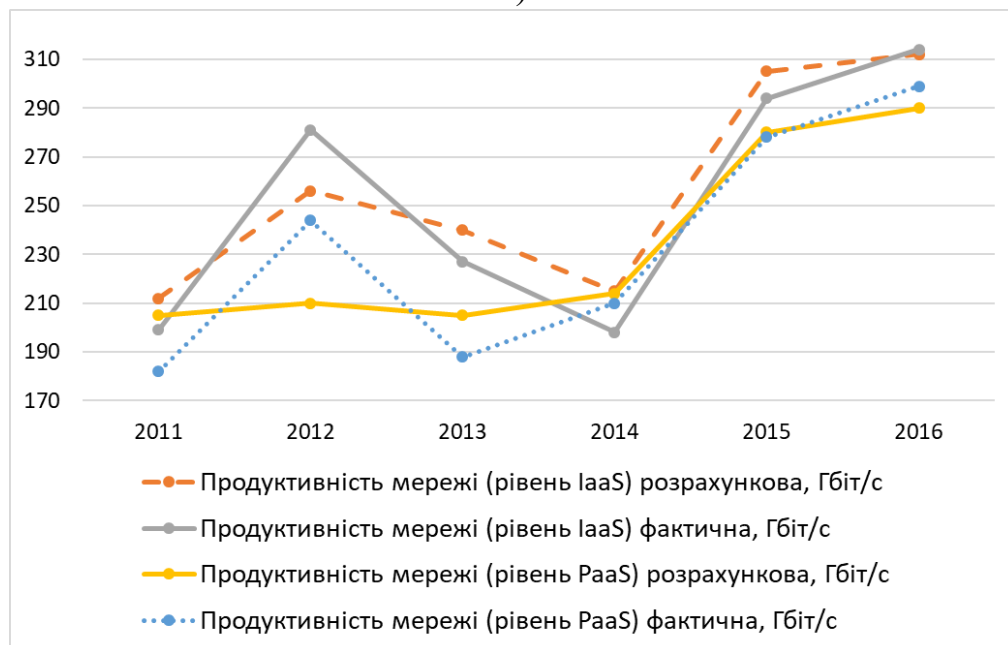
Період, рік	Продуктивність мережі (рівень IaaS) розрахункова, Гбіт/с	Продуктивність мережі (рівень IaaS) фактична, Гбіт/с	Продуктивність мережі (рівень PaaS) розрахункова, Гбіт/с	Продуктивність мережі (рівень PaaS) фактична, Гбіт/с
2011	212	199	205	182
2012	256	281	210	244
2013	240	227	205	188
2014	215	198	214	210
2015	305	294	280	278
2016	312	314	290	299

Таблиця 6.2. Порівняння прогнозованого та фактичного середньорічних показників сервісної доступності у ТКСП ПАТ «Укртелеком».

Період, рік	Сервісна доступність (рівень IaaS) розрахункова	Сервісна доступність (рівень IaaS) фактична, Гбіт/с	Сервісна доступність (рівень PaaS) розрахункова, Гбіт/с	Сервісна доступність (рівень PaaS) фактична, Гбіт/с
2011	0,998	0,999	0,9989	0,9989
2012	0,999	0,998	0,9990	0,9990
2013	0,999	0,997	0,9991	0,9991
2014	0,986	0,992	0,9990	0,99909
2015	0,995	0,998	0,9995	0,99999
2016	0,999	0,999	0,9998	0,99999



а)



б)

Рис. 6.23. Результати моделювання та фактичні показники середньорічної сервісної доступності (а) та продуктивності (б) ТКСП ПАТ «Укртелеком» за період 2011-2016 рр.

Наведені результати та методологія лягли також в основу трансформації інформаційно-комунікаційної PaaS сервісної платформи Державної прикордонної служби України (Рис. 6.24), як такої, що реалізується на основі IaaS ПАТ «Укртелеком» під егідою Держспецзв'язку. Застосування наведених у розділі 6.1 методів динамічної пріоритетизації при передаванні трафіку в цьому випадку є виправданим з метою підвищення оперативності передавання

чутливих до затримок службових даних. Рис. 6.24 сформовано на основі даних відкритих джерел [241].

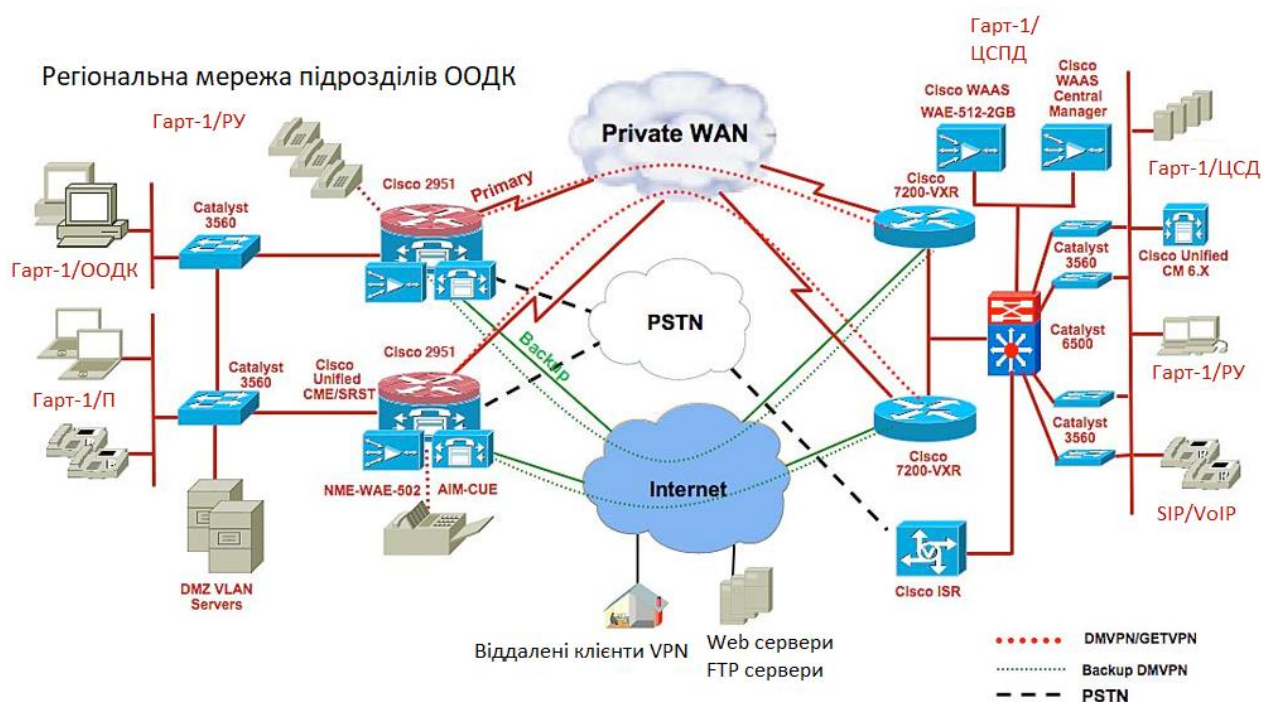


Рис. 6.24. Загальна блок-схема оптимізованої реалізації PaaS службової мережі ДПСУ, як телекомунікаційної сервісної платформи національного масштабу на основі IaaS платформи рис. 6.22. Фактично досягнуто рівень сервісної доступності 0,99999 (на рівні PaaS реалізації).

6.5. Висновки до 6-го розділу.

1. Для технологічної зручності реалізації процесів оброблення виокремлених високопріоритетних потоків навантаження, а також з метою уникнення взаємних впливів між окремими розпаралеленими компонентами при синтезі сервісної платформи типу IaaS, необхідно виділити та реорганізувати відповідні програмно-апаратні ресурси у якості ізольованих віртуалізованих компонент системи (програмного маршрутизатора), що значно підвищить стабільність її функціонування. Ґрунтуючись на вдосконаленні процесів у мережно-зелезних рівнях, при дотриманні запропонованого чисельного співвідношення (60/40%) між паралельними та послідовними компонентами, які задіяні в архітектурі сервісної мережної системи,

оптимально підвищується їх доступність, вивільняються та перерозподіляються буферні та обчислювальні системні ресурси, а отже синтезована мережна архітектура IaaS забезпечує відчутне зниження зваженої затримки передавання мережного трафіку, зокрема – за рахунок спеціалізованих потоків реального часу з високими пріоритетами, підвищуючи якість сервісу для критичних застосувань.

2. З метою забезпечення мінімального часу очікування високопріоритетних даних у маршрутизаторах телекомунікаційної сервісної платформи, в роботі удосконалено протокольні засоби сервісної мережної інфраструктури, зокрема метод обслуговування черг, який за рахунок зниження якості обслуговування потоків даних не реального часу, дає змогу зберегти необхідну якість обслуговування мультимедіа потоків реального часу, що набуває особливого значення в моменти перевантаження вузлів мережі. Новизна методу полягає в тому, що в ньому ведеться облік часу очікування пакету в чергах активного мережного обладнання, і, відповідно до цієї тривалості затримки, на транзитних маршрутизаторах пакет, «що спізнюється», може обслуговуватися з більш високим пріоритетом. Для тестування мережних пристроїв розроблено модель генератора трафіку, яка дає змогу без використання складних методів синхронізації виміряти затримку оброблення пакету маршрутизатором з точністю до 2 мкс. Точність розробленої моделі може бути суттєво покращеною без зміни її структури і алгоритму роботи. На основі детального аналізу принципів роботи апаратних маршрутизаторів фірми Cisco series 2800 розроблена та апробована адекватна модель віртуалізованого програмного маршрутизатора, що має масштабовану модульну архітектуру з можливістю розпаралелення. Також її новизна полягає у тому, що кожен з модулів може бути змінений без зміни архітектури всієї моделі маршрутизатора. Таким чином, розроблена модель може бути використана для тестування широкого спектру не тільки маршрутизаторів, але і й комутаторів. В результаті експерименту встановлено, що за рахунок використання модифікованого методу обслуговування черг та, відповідно, удосконалення процесів

обслуговування пріоритезованого трафіку вдалося покращити часові параметри якості обслуговування у 2-7 разів, у залежності від рівня завантаження вузлів мультисервісної мережної платформи.

3. Агрегування потоків навантаження на послідовних ланках сервісної мережної системи після паралельних обробників (віртуалізованих маршрутизаторів) не вносить глобального погіршення у якість сервісу IaaS, такі флуктуації параметрів QoS носять локальний характер на окремих мережних інтерфейсах, а в цілому, за рахунок ефектів синергізму та системної емерджентності, а також, із урахуванням результатів моделювання та експериментів у рамках цього дисертаційного дослідження, спостерігається загальносистемне покращення часових показників якості обслуговування трафіку, в залежності від наданих йому пріоритетів.

4. Запропоновано нові підходи до аналізу та збору великих обсягів функціональних мережних метаданих. А саме, запропоновано розглядати їх, як цілісну сутність шляхом цифрового голографічного представлення мережної структури та множини її функціональних властивостей. Підхід, що був запропонований, в цілому, добре співвідноситься з парадигмою хмарних мережних систем. Відповідно, запропоновано метод аналізу та прогнозування розподілу трафіку при модифікації мережної структури, або ж зміні умов її функціонування, з можливістю повузлового представлення мережних властивостей. Часткова втрата голографічного представлення функціональних мережних метаданих, що є доволі компактним способом їх зберігання, буде впливати лише кількісно на точність їх відтворення/прогнозування, але не на загальну якісну картину. Таким чином, голографічне представлення функціональних мережних метаданих дозволяє описати розподіл потоків службового трафіку у мережній структурі, а також відповідних наскрізних міжвузлових мережних потоків, як для всієї мережної системи в цілому, так і для окремо взятих її сегментів. На думку автора, запропоновані підходи є аналогічними за складністю до методів тензорного аналізу мережних систем

[56], проте дозволяють більш компактно описати цілісну множину взаємопідключених дискретних мережних об'єктів.

5. В даному розділі дисертаційної роботи узагальнено теоретико-прикладні засади створення сервісної мережної платформи національного масштабу для фіксації метаданих щодо комунікаційної активності абонентів рухомого зв'язку, з дотриманням принципів масштабованості в рамках глобальних комунікаційних процесів. Оцінено обчислювальну складність та архітектурні особливості сучасної розподіленої обчислювальної платформи для організації ЦОД, який може обробляти та зберігати згадану мережну метаінформацію. Показано, що створення подібної національної метабази даних в межах України не потребує значних обчислювальних та часових ресурсів, за умови правильного вибору архітектури апаратно-програмної платформи.

6. Запропоновано та описано узагальнену методологію синтезу телекомунікаційних сервісних платформ, описно процеси адаптації їх ХаaS реалізацій на рівнях SaaS, PaaS, IaaS. Приведено особливості стратегій адаптації зазначених реалізацій з урахуванням множини методів, які представлені у дисертаційній роботі. Представлено результати дослідження ефективності застосування запропонованої методології на прикладі телекомунікаційних сервісних платформ національного масштабу ПАТ «Укртелеком» (IaaS, PaaS) та ДПСУ (PaaS).

ВИСНОВКИ

В дисертаційній роботі розв'язано наукову проблему розроблення методологічного забезпечення синтезу телекомунікаційних сервісних платформ національного рівня для оптимального впровадження концепції повсюдного комп'ютингу (розподілених обчислень) із заданими рівнями якості сервісу, продуктивності та функціональної стійкості.

За результатами розв'язання поставленої проблеми можна зробити такі висновки:

1. На основі аналізу опублікованих праць та проведених теоретичних досліджень запропоновано формувати національний сегмент глобальної мережної інфраструктури, використовуючи телекомунікаційні сервісні платформи, які реалізують неперервний моніторинг, оперативне системне адміністрування і держнагляд, зокрема у галузі мережної безпеки, а отже володіють необхідними рівнями захищеності та функціональності. Будучи реалізованими у вигляді множини довірених ЦОД, які поширюють єдину мережну політику на всіх операторів інфокомунікацій, телекомунікаційні сервісні платформи національного мережного сегменту стають взаємоінтероперабельними, дозволяючи надавати послуги в обсягах, що необхідні у конкретні періоди часу для конкретних груп користувачів.

2. Виконано дослідження ефективності застосування групи методів підвищення системної продуктивності телекомунікаційних сервісних платформ, зокрема диференціації обслуговування користувачів (підвищення до 16%), адаптивного резервування мережних ресурсів сегменту мережної системи (покращення до 20%). Застосування відкритої (розподіленої) системної архітектури дозволяє підвищити продуктивність платформи за кількістю обслугованих вимог до 17% у порівнянні з їх обробленням у класичних (централізованих) серверних вузлах; крім того підвищується масштабованість сервісних мережних систем, а застосування методу поліваріантного доступу дало змогу збільшити пропускну здатність веб-сервісу, що реалізується на основі розподіленої мережної платформи.

3. Виконано експериментальне статистичне дослідження мультисервісного навантаження в гетерогенній телекомунікаційній мережній системі з метою

аналізу показників його самоподібності для окремих типів трафіку, показано, що основні типи навантаження мають доволі високий ступінь самоподібності, зокрема трафік сервісів генерування інтернет даних (нереального часу) – $H \cong 0,685$, IP-телефонії – $H \cong 0,981$, відео за запитом (VoD) – $H \cong 0,608$, передавання службових даних – $H \cong 0,719$.

4. Проведено визначення та загальний аналіз загроз поширенню даних та критеріїв функціональній стійкості у реалізаціях телекомунікаційних сервісних платформ національного сегменту глобальної інформаційної інфраструктури та відповідних підходів до протидії цим загрозам. Підвищення функціональної стійкості архітектури сервісних мережних систем до зловмисних зовнішніх впливів на їх функціональну стабільність дозволить нівелювати наслідки від застосування мережних атак, а саме зниження кількості працездатних сервісних вузлів і, відповідно, обсягів загальних ефективних обчислювальних потужностей, а отже – запобігти критичному зниженню рівня сервісної доступності. Тому розвиток технологій мережних екранів є необхідним рішенням. У роботі розроблено концептуальні основи для реалізації методу мігруючого мережного екрану та описано загальний алгоритм його функціонування. Таке рішення, на відміну від відомих, дозволяє уникати міграції обчислювальних ресурсів, є більш гнучким за рахунок статистичного виявлення аномальної мережної активності шляхом фільтрування трафіку, ізолювання точок небажаної інформаційної присутності, зокрема відповідних інформаційних потоків, контенту, портів, мережних інтерфейсів.

5. Запропоновано та промодельовано метод розподілу конвергованих ресурсів мережно-залежних рівнів гетерогенної сервісної платформи на основі застосування теорії нечітких множин, що дає змогу прийняти обґрунтоване рішення щодо проведення процедури вертикального хендвера, базуючись на групі QoS-залежних критеріїв у амбівалентній ситуації, наприклад, коли користувач знаходиться на границі покриття її комірок, а також метод динамічної корекції маршрутних метрик шляхом наскрізного структурного трасування в хмарних мережних системах (динаміка покращення сягає до 10% у масштабі кластера хмарної мережної платформи близько 100 сервісних вузлів). Показано, що така кластеризація хмарних систем дає змогу досягати

найбільшої ефективності, що узгоджується з результатами моделювання сервісної доступності та системної продуктивності телекомунікаційної сервісної платформи.

6. Запропоновано узагальнену методологію синтезу телекомунікаційних сервісних платформ національного масштабу за критеріями сервісної доступності та системної продуктивності. На основі доведення оптимальної структурної композиції у співвідношенні їх розпаралелених та послідовних компонент за принципом «золотого січення» ($\sim 0,6/0,4$) виконано експериментальну науково-виробничу трансформацію мультисервісних IaaS та PaaS мережних систем ПАТ «Укртелеком» за період 2011-2016 років. За останні два роки на рівні PaaS досягнуто 35% підвищення продуктивності, а на рівні IaaS – 1,3% підвищення рівня сервісної доступності (мале значення приросту рівня сервісної доступності відображає ступінь складності при його досягненні або підтримуванні на середньорічних показниках у змінних умовах експлуатації телекомунікаційних платформ). На рівні PaaS реалізації забезпечено показник середньорічної сервісної доступності 0,99999. Запропоновано та верифіковано протокольні засоби зменшення затримок передавання високопріоритетного мережного трафіку у 2-7 разів (у залежності від поточного рівня завантаженості ТКСП), що є зручними для імплементації NFV підходу щодо реалізації віртуалізованих розпаралелених обробників навантаження.

7. Запропоновано нові підходи до аналізу та фіксації великих обсягів функціональних мережних метаданих, розглядаючи їх, як цілісну сутність шляхом цифрового голографічного представлення мережної структури та множини її функціональних властивостей. Часткова втрата голографічного представлення функціональних мережних метаданих, що є доволі компактним способом їх зберігання, буде впливати лише кількісно на точність їх відтворення, але не на загальну якісну картину. Запропоновано теоретико-прикладні засади створення сервісної мережної платформи національного масштабу для фіксації метаданих щодо комунікаційної активності в ТКСП.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Програмне забезпечення, як послуга. // Матеріал з Вікіпедії (Вільної енциклопедії). [Електронний ресурс]. Режим доступу до сторінки: https://uk.wikipedia.org/wiki/Програмне_забезпечення_як_послуга
2. Demydov I. Enterprise Distributed Service Platform – Network Architecture and Topology Optimization / I. Demydov, M. Klymash, N. Kryvinska, C. Strauss // Int. J. Space-Based and Situated Computing. -2012. – Vol. 2. - № 1. - pp. 23-30.
3. Kerravala Z. Intelligent communications powers the next wave of productivity growth, Yankee Group Research. February, 2007. [Електронний ресурс]. Режим доступу до ресурсу: <http://www.yankeegroup.com> (accessed on 21/05/2011).
4. Kryvinska N. Managing an increased service heterogeneity in converged enterprise infrastructure with SOA / N. Kryvinska, L. Auer, C. Strauss // Int. Journal of Web and Grid Services (IJWGS). - 2008. - Vol. 4. - No. 4. - pp.440–460.
5. Converged intelligent network concept – joined future for telecommunications and the internet / N. Kryvinska, H.R. van As]// Proceedings of 7th Int. Conf. ICIN-2001, Bordeaux, France. - 01-04.10.2001. - pp.74–79.
6. End-to-end QoS monitoring tool development and performance analysis for NGN / C.C. Kim, S.C. Shin, S.Y. Ha, S.Y. Han, Y. Kim // Proceedings of APNOMS-06, LNCS, 27–29 September 2006. - Vol. 4238. - Busan, Korea.
7. Hong J.W. Enterprise network traffic monitoring, analysis, and reporting using web technology / J.W. Hong, S.U. Park, Y.M. Kang, J.T. Park // Journ. of Network and Systems Management. - 2001. - Vol. 9. - No. 1. - pp.89–111.
8. Bloomers J. Practical Planning for Network Growth. Upper Saddle River, New Jersey: Hewlett-Packard Professional Books, Prentice Hall PTR, 1996. – 400 p.
9. Managing application performance to achieve mission success, Technical paper from CA Wily Technology, 0108, February, 2008.

10. Leng B. Automating network configuration tasks using multi-level modeling / B. Leng, D.P. Weeks, M.K. Mahapatra // Bell Labs Technical Journal. – 2008.- Vol. 12. - No. 4. - pp. 83–102.

11. Yohanan G. Web services technologies in enterprise IT management / G. Yohanan, J. Hahn-Steichen // White paper from Intel Corporation, March, 2006. [Електронний ресурс]. Режим доступу: <http://www.intel.com/IT> (accessed on 21/05/2011).

12. Kumar B. Broadband Communications. New York: McGraw-Hill, 1995. – 513p.

13. Public Safety Systems And Passport Network of The Great Libyan Arab Jamahiriya. Homeland Security Program Technical Specification // 11 November 2006. – Washington: Homeland Security Office, 2006. – 62 p.

14. Optimizing telecommunications OSS/BSS and SDP deployments with application performance management, Solution brief from CA Wily Technology, 0807, 2007.

15. Hong J.W. Web-based intranet services and network management / J.W. Hong, J.Y. Kong, T.H. Yun, J.S. Kim, J.T. Park, J.W. Beak // IEEE Communications Magazine. - October, 1997. - Vol. 35. - No. 10. - pp.100–110.

16. Kang T.H. A seamless service management with context-aware handoff scheme in ubiquitous computing environment/ T.H. Kang, C.P. Hong, W.J. Jang, S.D. Kim // Proceedings of APNOMS-06, LNCS, 2006, 27–29 September. - Busan, Korea. - Vol. 4238.

17. Demydov I. Concept of the Migrating Firewall to Scalable Cloud Networks / Ivan Demydov, Orest Lavriv, Zenoviy Kharkhalis, Mohamed Mehdi El Hatri // Сучасні проблеми радіоелектроніки, телекомунікацій, комп'ютерної інженерії TCSET'2016 : матеріали XIII Міжнародної конференції, 23-26 лютого 2016, Львів, Славське, Україна / Міністерство освіти і науки України, Національний університет "Львівська політехніка". - Львів : Видавництво Львівської політехніки, 2016. – С. 643-645.

18. Information assurance. // Матеріал з Вікіпедії (Вільної енциклопедії). [Електронний ресурс]. Режим доступу до сторінки: https://en.wikipedia.org/wiki/Information_assurance

19. Стрихалюк Б. М. Структурний та функціональний синтез гетерогенних сервісно-орієнтованих телекомунікаційних мереж : автореферат дисертації на здобуття наукового ступеня доктора технічних наук : 05.12.02 – телекомунікаційні системи та мережі / Богдан Михайлович Стрихалюк; Міністерство освіти і науки України, Національний університет "Львівська політехніка". – Львів, 2015. – 40 с.

20. Federal Cloud Computing Strategy, Feb 2011. [Електронний ресурс]. Режим доступу до сторінки: <http://www.cio.gov/documents/Federal-Cloud-COMputing-Strategy.pdf>

21. DoD Cloud Computing Strategy. [Електронний ресурс]. Режим доступу до сторінки: <http://www.defense.gov/Releases/Release.aspx?ReleaseID=15435>

22. NIST Special Publications: [SP 500-292] NIST Cloud Computing Reference Architecture, September 8, 2011.

23. DoD Directive 4630.5: Interoperability of IT and NSS, May 5, 2004 [Електронний ресурс]. Режим доступу до сторінки: <http://www.dtic.mil/whs/directives/corres/pdf/463005p.pdf>

24. Домаскін О. М. Формалізація вимог користувачів до телекомунікаційних мереж : автореферат дисертації на здобуття наукового ступеня кандидата технічних наук : 05.12.02 – телекомунікаційні системи та мережі / Олег Михайлович Домаскін; Міністерство освіти і науки України, Національний університет «Львівська політехніка». – Львів, 2015. – 24 с.

25. Demydov I. Features of the cloud services implementation in the national network segment of Ukraine / I. Demydov, M. Klymash, M. Beshley, O. Shpur // Information and telecommunication science. К.: NTUU “KPI”, 2016. - No.1. - P. 31-38.

26. Demydov I. V. The structural-functional synthesis of cloud service delivery platform after service availability and performance criteria / I. V. Demydov,

В. М. Strykhalyuk, О. М. Shpur, Mohamed Mehdi El Hatri, Y. V. Klymash // Системы обработки информации. — 2015. — № 1. — С. 144-159.

27. Гольдштейн Б.С., Фрейнкман В.А. Call-центры и компьютерная телефония. - СПб.: БХВ - Санкт-Петербург, 2002. – 373 с.

28. Шнепс-Шнеппе М.А. Сети нового поколения NGN / М.А. Шнепс-Шнеппе // «Вестник связи». - 2002. - №7.

29. Шнепс-Шнеппе М.А. Как строить NGN: архитектура Parlay и Parlay-X / М.А. Шнепс-Шнеппе // «Вестник связи».- 2004. - №2.

30. Соловьев С.П. TINA - новая концепция построения сетей связи / С.П. Соловьев, М.А. Шнепс-Шнеппе // «Электросвязь». -1997. - №7.

31. Next Generation Voice Services - Open Solutions for the Next Generation Network. Intel Corporation, 2001.

32. An Introduction to Next-Generation Network Services. The Next Bug Opportunity on the Web. White paper. Intel Corporation, 2001.

33. Полканов Е.И. Открытые стандарты и технологии -катализатор развития сервисных платформ / Е.И. Полканов, В.В. Гамов // «Информ Курьер Связь». - 2004. -№ 2.

34. Jack Kozik, Igor Faynberg. On Opening PSTN to Enhanced Voice/Data Services - The PINT Protocol Solution // Bell Labs Technical Journal, 2000.

35. Christopher Bear, Warren A. Montgomery. Open, Programmable Network // Bell Labs Technical Journal, 2000.

36. Bjorkman N., Yong Jiang, Torbjorn Lundberg. The movement from monoliths to component-based network elements // IEEE Communications Magazine. January, 2001.

37. Чурбанов Д.В. Открытая сервисная архитектура OSA / Д.В. Чурбанов // «Сети и системы связи». - 2002. - №3.

38. G TS 129.128-x Universal Mobile Telecommunications System (UMTS): Open Service Access APIs.

39. ECMA Standard 179 - Services for Computer Supported Telecommunications Applications (CSTA) Phase I, June 1992.

40. Оринштейн Д. Прикладной программный интерфейс / Д. Оринштейн // "Computerworld". - 2000. - №9.
41. Иванова Т.И. Корпоративные сети связи. - М.: «Эко-Трендз», 2001. - 282 с.
42. Ричардсон Р. Тоновый набор для небольших компаний // LAN. -1996. - №7.
43. Коглер С. Д. СП: TAPI или TSAPI? / С.Д. Коглер // "Сети и системы связи". - 1996. -№4.
44. Parlay Group, Parlay X Web Services white paper, 2002.
45. Kocan Kristin F. Service Creation for Next-Generation Networks / F. Kocan Kristin, A. Montgomery Warren // Bell Labs Technical Journal. - 2002. - pp. 63-79.
46. Beddus Simon. Opening up networks with JAIN Parlay / Simon Beddus, Gary Bruce, Steve Davis // IEEE Communications Magazine. – May, 2000 – Vol. 38(4). -pp. 136 – 143.
47. Chaniotakis S. Emmanuel. External service provision in telecommunications networks using open interfaces / Emmanuel S. Chaniotakis, Andreas E. Papadakis, Iakovos S. Venieris // Computer Communications. - 2004. - Volume 27. - Issue 1. - pp. 1–12.
48. Yves De Serres Lawrence. Value-added services in the converged network / Lawrence Yves De Serres // IEEE Communications Magazine. - 2001. - Volume 39. - Issue 9. - pp. 146 – 154.
49. Добуш Ю.Д. Дослідження відкритих сервісних інтерфейсів Parlay в концепції «електронного урядування»/ Ю.Д. Добуш, І.В.Демидов, М.М. Климаш // Комп'ютерні технології друкарства: Зб. наук. пр. – Львів: Українська Академія Друкарства, 2012. – №28. – С. 170-186.
50. Рекомендации ETSI ES 201 915 Parlay версії 3. European Telecommunications Standards Institute, 2002.
51. Minor M. Adaptive workflow management in the cloud-towards a novel platform as a service / M. Minor, R. Bergmann, S. Görg // Proceedings of the ICCBR. – 2011. - pp.131–138.

52. Sung H.C. Adaptive service scheduling for workflow applications in service-oriented grid / H.C. Sung, S. Taeweon, C.Y. Heon // *Supercomput.* - 2010. - Vol. 52. – Issue 3. - pp.253–283.

53. Kuroyanagi K., Mori Y. Service delivery platforms for network operators / K. Kuroyanagi, Y. Mori // *Hitachi Review.* – February, 2009. - Vol. 58. – pp. 26–30.

54. Yu C.Z. Service storm: a self-service telecommunication service delivery platform with platform-as-a-service technology / C.Z. Yu, X. Liang, P.L. Xin, N.W. Xi, X.L. Xiao, H.S. Chang // *2010 IEEE 6th World Congress on Services.* – 2010. - pp.8–15.

55. Demydov I. Enterprise Distributed Service Platform – Network Architecture and Topology Optimization / Ivan Demydov, Mykhailo Klymash, Natalia Kryvinska, Christine Strauss // *Int. J. Space-Based and Situated Computing.* - 2012. - Vol. 2. - No. 1. - P. 23-30.

56. Klymash M. Traffic routing in telecommunication nets and its diakoptics representation / M. Klymash, B. Strykhalyuk, M. Kaidan, I. Demydov // *Computation Problems of Electrical Engineering.* –Lviv, 2011. - №1(1). – P.15-19.

57. Demydov I.V., Kryvinska N., Klymash M.M. An Approach to the Flexible Information/Service Workflow Managing in Distributed Networked Architectures / I.V. Demydov, N. Kryvinska, M.M. Klymash // *The International Workshop on Design, Optimization and Management of Heterogeneous Networked Systems (DOM-HetNetS'09), in conjunction with the 38th International Conference on Parallel Processing (ICPP-2009), September 22nd -25th, 2009.* - Vienna, Austria, 2009. - P. 236-242.

58. Kryvinska N. An Analytical Approach for the Modeling of Real-time Services over IP Network. / N. Kryvinska // *Elsevier Transactions of IMACS, Journal «Mathematics and Computers in Simulation».* – 2008. - Vol.79. - pp. 980-990.

59. Kryvinska N. Intelligent Network Analysis by Closed Queueing Models / N. Kryvinska // *Kluwer/Springer Journal «Telecommunication Systems».* – 2004. - Vol. 27(1). - pp. 85-98, ISSN: 1018-4864 (Print), 1572-9451 (Online).

60. Papazoglou Michael P. Service-Oriented Computing: a Research Roadmap / Michael P. Papazoglou, Paolo Traverso, Frank Leymann // International Journal of Cooperative Information Systems. – 2008. - Vol. 17. - No. 2. - P. 223–255.
61. Kleinrock L. An early history of the internet [History of Communications] / Leonard Kleinrock //IEEE Communications Magazine. – 2010. – Vol. 48. – Issue 8. – pp. 26-36.
62. Klymash M.M. Analysis of service workflows distribution and SDP parameters / M.M. Klymash, I.V. Demydov, O.A. Lavriv, Yu.D. Dobush// Системи обробки інформації. – Харків, 2012. – Вип. 6 (104). – С. 103-107.
63. HP FlexFabric Reference Architecture: Data Center Trends: A Hewlett Packard Technical white paper. - February, 2015. - [Електронний ресурс]. – Режим доступу до сторінки: <https://www.hpe.com/h20195/v2/getpdf.aspx/4AA5-6481ENW.pdf?ver=1.0>
64. Elloumi O. IoT/M2M from research to standards: the next steps (Part I) / O. Elloumi, J. Song, Y. Ghamri-Doudane, V.C.M. Leung // IEEE Communications Magazine — Communications Standards Supplement. – 2015. – Issue 9. – pp. 8-9.
65. Kryvinska N., Strauss C., “Conceptual Model of Business Services Availability vs. Interoperability on Collaborative IoT-enabled eBusiness Platforms”, in the “Internet of Things and Inter-cooperative Computational Technologies for Collective Intelligence”, book Ed.: N. Bessis and F. Xhafa, D. Varvarigou, R. Hill, and M. Li, the book series “Studies in Computational Intelligence”, (SCI-460), Springer-Verlag Berlin Heidelberg, 2013, ISBN: 978-3-642-34951-5, pp. 167-187.
66. Лунтовський А. О. Розподілені сервіси телекомунікаційних мереж та повсюдний комп'ютинг і Cloud-технології / А. О. Лунтовський, М. М. Климаш, А. І. Семенко. – Львів: Львівська політехніка, 2012. – 368 с.
67. Блэк Ю. Сети ЭВМ: протоколы стандарты, интерфейсы. - М: Мир, 1990. - 506 с.
68. Recommendation ETSI 3G TS 29.002 version 3.3.0. – ETSI, 1999. – 1226 p.
69. Q. 1711: Network functional model for IMT-2000 // Series Q: switching and signaling. – Geneva: ITU-T, 1999. – 67 p.

70. Q. 1208: General Aspects of the Intelligent Network Application Protocol // Series Q: switching and signaling. – Geneva: ITU-T, 1997. – 9 p.

71. Безир Х., Хойер П., Кеттлер Г. Цифровая коммутация. Перевод с немецкого под ред. В.В. Штрагера. - М.: Радио и связь, 1984. – 264 с.

72. Боккер П. ISDN. Цифровая сеть с интеграцией служб. Понятия, методы, системы. - М.: Радио и связь, 1991. - 304 с.

73. M.3010: Principles for a Telecommunications Management Network // Series M: TMN and Network Maintenance: International Transmission Systems, Telephone Circuits, Telegraphy, Facsimile And Leased Circuits. – Geneva: ITU-T, 2000. – 44 p.

74. E. 713 (10/92): Control Plane Traffic Modeling // Series E: Telephone Network and ISDN Quality of Service, Network Management and Traffic Engineering. – Geneva: ITU-T, 1993. – 10 p.

75. Демидов І. В. Аналіз методів підвищення продуктивності телекомунікаційних мереж хмарних сервісних систем / І. В. Демидов, Мухамед Мехді Ель Хатрі, Укаблі Юсеф // Телекомунікаційні та інформаційні технології. – 2016. – №1. – С. 41-47.

76. Демидов І. В. Моделювання процесів обслуговування потоків запитів у розподілених сервісних мережних архітектурах / І. В. Демидов, П. О. Гуськов, Мухамед Мехді Ель Хатрі // Наукові записки Українського науково-дослідного інституту зв'язку. – 2015. – №5(39). – С. 44-51.

77. Демидов І. В. Дослідження імовірнісних характеристик трафіку опорно-транспортної підсистеми мережі мобільного зв'язку / І. В. Демидов, М.М. Климаш, П. О. Гуськов, Мухамед Мехді Ель Хатрі // Наукові записки Українського науково-дослідного інституту зв'язку. – 2015. – №6(40). – С. 11-18.

78. Spillner Josef. Cloud Resource Recycling: An Addition of Species to the Zoo of Virtualised, Overlaid, Federated, Multiplexed and Nested Clouds / Josef Spillner, Andrii Chaichenko, Andrey Brito, Francisco Brasileiro, Alexander Schill//

SDPS Transactions: Journal of Integrated Design and Process Science (JIDPS). - 2014. – Issue 4. - Vol. 18/1. – pp. 5-19.

79. Corezoid: process engine. (Назва з екрану). – [Електронний ресурс]. Режим доступу: <https://new.corezoid.com/>

80. Лагутин В. С. Телетрафик мультисервисных сетей связи / В.С. Лагутин, С. Н. Степанов. – Москва : Радио и связь, 2000. – 320 с.

81. Климаш М. М. Дослідження особливостей розвитку архітектури та технологій WiMAX-орієнтованих інтегрованих радіомереж доступу 4G / М.М. Климаш, І. В. Демидов, Самер Аввад // Наукові записки Українського науково-дослідного інституту зв'язку. – 2008. – №4 (6). – С.37-47.

82. Q.764: Specifications of Signalling System No. 7 – ISDN user part // Series Q: switching and signaling. – Geneva: ITU-T, 1999. – 110 p.

83. Самер Аввад. Дослідження обслуговування трафіку на транзитній мережі оператора мобільного зв'язку / Самер Аввад, М. М. Климаш, І.В. Демидов, Б. В. Коваль // Наукові записки Українського науково-дослідного інституту зв'язку. – 2011. – №1 (17). – С. 51-55.

84. Бутрименко А. В. Система поиска оптимальных путей передачи сообщений / А. В. Бутрименко, В. Г. Лазарев // Проблемы передачи информации. – 1965. – Т.1. – С. 8-26.

85. Богомолова Н. Е. Метод повышения пропускной способности транзитной сети операторов сотовой подвижной связи / Н. Е. Богомолова, А.С. Крылов // Мобильные системы. – 2005. – № 9. – С. 14-18.

86. Протоколы и методы управления в сетях передачи данных. Под ред. Ф. Куо. – Москва : Радио и связь, 1985. – 120 с.

87. Чекмарев Е. В. Особенности системы сигнализации №7 для сетей подвижной связи. Подсистема MAP / Е. В. Чекмарев // Материалы курсов «Новые технологии связи». – Москва : НТЦ КОМСЕТ, 1996.

88. Лившиц Б. С. Теория телетрафика / Б. С. Лившиц, А. П. Пшеничников, А. Д. Харкевич. – Москва : Связь, 1979. – 224 с.

89. Вентцель Е.С. Теория вероятностей / Е. С. Вентцель. – Москва : Высшая школа, 2000. – 480 с.
90. Форд Л. Потоки в сетях ; перевод с англ. / Л. Форд, Д. Фалкерсон. - Москва: Мир, 1966. – 276 с.
91. Xiaohu Ge. 5G Wireless Backhaul Networks: Challenges and Research Advances / Xiaohu Ge, Hui Cheng, Mohsen Guizani, Tao Han // IEEE Network Magazine. USA: Institute of Electrical and Electronics Engineers. – 2014. – Vol. 28, no. 6. – P. 6-11.
92. M. Jo. A Survey of Converging Solutions for Heterogeneous Mobile Networks/ M. Jo, T. Maksymyuk, R.L. Batista, T.F. Maciel, A.L.F. de Almeida, M. Klymash // IEEE Wireless Communications. - 2014. – Vol. 21. - №8 . - P. 54-62.
93. Monica Paolini. Small-cell backhaul: Industry trends and market overview / Monica Paolini, Lance Hiley, Frank Rayal Senza Fili. – Senza Fili Consulting, 2013.
94. Демидов І.В. Моделювання процесів диференційованого обслуговування користувачів хмаринкових сервісних мережних систем / І. В. Демидов, Мухамед Мехді Ель Хатрі, Укаблі Юсеф // Наукові записки Українського науково-дослідного інституту зв'язку. – 2016. – №1(41). – с. 26-34.
95. Шварц М. Сети связи: протоколы, моделирование и анализ: в 2 - х частях. Ч.2 / М. Шварц. – М.: Наука, 1992. – 276 с.
96. Мышкис А. Д. Элементы теории математических моделей / А.Д. Мышкис. – 3-е изд., – Москва : КомКнига, 2007. – 192 с.
97. Samer Awwad. Traffic Design in 4G Broadband Backbone Nets / Samer Awwad, Mykhailo Klymash, Ivan Demudov // Матеріали 11-ї Міжнародної науково-технічної конференції «Досвід розробки та застосування приладотехнологічних САПР в мікроелектроніці». – Львів – Поляна, Україна, 2011. – P. 145 – 146.
98. Степанов С.Н. Численные методы расчета систем с повторными вызовами. -М.: Наука, 1983. – 230 с.

99. Лазарев В.Г., Лазарев Ю.В. Динамическое управление потоками информации в сетях связи. – М.: Радио и связь, 1983. — 235 с.

100. Применение дифференцированного обслуживания пользователей для повышения качества обслуживания в мобильных сетях / [Я.В. Чернушевич] // Труды конференции «Телекоммуникационные и вычислительные системы». Международный форум информатизации (МФИ-2004). - М.: МТУСИ, 2004. - С. 62.

101. ITU-T E.800, Terms and definitions related to quality of service and network performance including dependability, 1994.

102. Reibman L. Reliability Modelling: an Overview for System Designers / L. Reibman, M. Veeraraghavan // IEEE Computer. - Apr. 1991. – Vol. 24. – Issue 4. – pp. 49-57.

103. Leue Stefan. Specifying real-time requirements for SDL specifications - a temporal logic-based approach / Stefan Leue // Proceedings of the Fifteenth IFIP WG6.1 International Symposium on Protocol Specification, Testing and Verification XV. – London: Chapman & Hall, Ltd., 1996. – pp. 19-34.

104. Чурина Т. Г. Способ построения раскрашенных сетей Петри, моделирующих SDL - системы = Coloured Petri nets approach to the validation of SDL - specifications / Т. Г. Чурина. - Новосибирск : Ин-т систем информатики им. А. П. Ершова СО РАН, 1998. - 56 с. : ил.; 21 см.

105. Liu L. Modelling and analysis of the CES protocol of H.245 / L. Liu, J. Billington // Proceedings of the 3rd workshop and tutorial on practical use of coloured petri nets and the CPN tools (CPN'01). -Aarhus. – 2001. - pp. 95–114.

106. Burke P.J. The output of a queueing system // Operations Research. - 1956.- Vol. 4. - pp. 699-704.

107. Пинчук А.В. Предоставление новых услуг средствами компьютерной телефонии / А.В. Пинчук, В.А. Фрейнкман // Вестник связи. - 1999. - №9. – С. 75-79.

108. Khorasani Mehdi. Middleware in telecommunications // Lucent Technologies. 2000.

109. Рекомендації ETSI ES 202 915 European Telecommunications Standards Institute, 2002.
110. Jackson J.R. Networks of waiting lines. Operations Research. – 1957. - Vol. 5. – pp. 518-521.
111. Клейнрок Л. Теория Массового Обслуживания. - М.: «Машиностроение», 1979. - 432 с.
112. Клейнрок Л. Вычислительные системы с очередями. - М.: «Мир», 1979. – 595 с.
113. Вишнеvский В.М. Теоретические основы проектирования компьютерных сетей. - М.: «Техносфера», 2003. - 512 с.
114. Jackson J.R. Jobshop-like queueing systems / J.R. Jackson // Management Science. – 1963. - Vol. 10. - №1. -pp. 131-142.
115. Hsieh C. T. Two Classes of Performance Bounds for Closed Queueing Networks / C. T. Hsieh, Simon S. Lam // Performance Evaluation. – 1987. - Vol. 7. - No. 1. – pp. 3-30.
116. Добуш Ю.Д. Аналіз загроз передавання даних у системі «електронного урядування» та оцінка її ефективності / Ю.Д. Добуш, І.В.Демидов, М.М. Климаш // Вісник Державного університету інформаційно-комунікаційних технологій. – К., 2012. Т.10, №3. – С.29-36.
117. Добуш Ю.Д. Загрози поширенню даних в інфокомунікаційних системах «електронного урядування» / Ю.Д. Добуш, М.М. Климаш, І.В. Демидов // Матеріали Міжнародної науково-технічної конференції «Інформаційні проблеми теорії акустических, радіоелектронних і телекомунікаційних систем» (IPST-2012): Тезиси доповідей. – АР Крим, Алушта, 2012. – С.165-166.
118. Нопин С.В. Моделирование защиты речевой информации с помощью персонального компьютера. / С.В. Нопин, В.Г. Шахов // Омский научный вестник. – 2004. – №4(29). – С. 124-126.
119. Родионов Д. Е. Методика анализа защищенных систем IP-телефонии. Автореф. дис. .канд. техн. наук / Д. Е. Родионов//. – М., 1999. – 24 с.

120. Климаш М.М. Підхід до оцінки ефективності захищеної мультисервісної мережної системи передавання / М.М. Климаш, Ю.Д. Добуш // Матеріали 4-ої Міжнародної науково-технічної конференції «Проблеми телекомунікацій-2010» (ПТ-10): Збірник тез. – К.: НТУУ «КПІ», 2010. – С.31-32.

121. Климаш М.М. Забезпечення якості обслуговування та оптимізація бізнес-процесів у розподілених системах на основі сервісно-орієнтованої архітектури / М.М. Климаш, І.В. Демидов, М.О. Селюченко, І.Д. Орлевич // Радіоелектроніка та телекомунікації. Вісник Національного університету “Львівська політехніка”. – Львів, 2013. – №766. – С. 150-155.

122. Aramudhan M. A Study on Enhancing QoS Through Dynamic Service Prioritization in Web Services / M. Aramudhan, Rhymend V. Uthaiaraj // Asian Journal of Information Technology. - 2005. – Vol. 4. - №10. – P. 954-956.

123. Schmidt Holger. Adaptive Web Service Migration, in Distributed Applications and Interoperable Systems / Holger Schmidt, Rüdiger Kapitza, Franz J. Hauck and Hans P. Reiser // (DAIS '08), R. Meier and S. Terzis, LNCS, Oslo, Norway: Springer. -2008. – pp. 182-195.

124. Klymash M. Service Quality Oriented Method of Multiservice Telecommunication Networks Design / Mykhailo Klymash, Orest Lavriv, Bohdan Buhyl, Yuriy Danik // 11th International Conference Modern Problems of Radio Engineering, Telecommunications and Computer Science Dedicated to the 60th Anniversary of Radio Department at Lviv Polytechnic National University TCSET'2012. February 21-24, 2012 Lviv-Slavske, Ukraine. – Publishing House of Lviv Polytechnic. – P. 235-236.

125. Strykhalyuk B., Service provisioning by using a structure stability algorithm in a virtualized data center based on cloud technology // Bogdan Strykhalyuk, Olga Shpur, Andriy Masiuk // Computational Problems of Electrical Engineering. – 2014. – Vol. 4. - №1. – P.83-88.

126. Klymash M. A Novel Approach of Optimum Multi-criteria Vertical Handoff Algorithm for Heterogeneous Wireless Networks / M. Klymash,

B. Stryhaliuk, I. Demydov, M. Beshley, M. Seliuchenko // International Journal of Engineering and Innovative Technology (IJEIT). – November 2014. – Volume 4, Issue 4(5). – P. 42-52.

127. Beshley M. Research and Development the Methods of Quality of Service Provision in Mobile Cloud Systems / M. Beshley, T. Maksymyuk, B. Strykhaluk, M. Klymash // IEEE International Conference [Black Sea Conference on Communications and Networking (BlackSeaCom'2014)], May 27-30, 2014, Odessa, Ukraine. – 2014. – P. 165-169.

128. Klymash M. Model of network resources management on the basis of services priorities association / Mykhailo Klymash, Mykola Beshley, Orest Lavriv // Proceedings of international conference CADSM'2013. Polyana-Svalyava. – 2013. – P. 172-173.

129. Trang, D. D. Fractal Analysis and Modeling of VoIP Traffic // D. D. Trang, B. Sonkoly, S. Molnar// Telecommunications Network Strategy and Planning Symposium. 2004. - Issue №1. - P. 123-130.

130. Crovella, M. E. Self-similarity in world wide web traffic: Evidence and possible causes / M. E. Crovella, A. Bestavros// IEEE/ACM Trans. Networking - 1997. Vol. 5, № 6. - P. 835-846.

131. Стрихалюк Б.М. Дослідження статистичних параметрів та характеристик інформаційних потоків в гетерогенних мережах / Б.М.Стрихалюк, І.В. Демидов, В.І. Романчук, М.І. Бещлей // Наукові записки УНДІЗ. – 2014. – №6(34). – С. 82-92.

132. Kryvinska, C. Strauss, “Next Generation Networks - Service Delivery and Management”, Book, Electronic Business series, vol. 7, International Academic Publishers, Peter Lang Publishing Group, 2011; ISBN-978-3-631-60871-5; ISSN: 1868-646X.

133. N. Kryvinska, Converged Network Service Architecture: A Platform for Integrated Services Delivery and Interworking. Electronic Business series edited by C. Strauss, vol. 2, International Academic Publishers, Peter Lang Publishing Group, 2010; ISBN-13:978-3631595251; ISSN:1868-646X.

134. Witt Walter F. Keep Your Feet on the Ground When Moving Software into the Cloud / Walter F. Witt // International Journal of Digital Content Technology and its Applications. – 2010. – Volume 4. - Number 2. – P.10-17.

135. Стрихалюк Б.М. Структурно-функціональна оптимізація процесів міграції віртуальних машин в розподілених дата-центрах / Б.М. Стрихалюк, З.В. Хархаліс, І.В. Демидов // Комп'ютерні технології друкарства: збірник наукових праць. - 2014. - №32. - С. 69-81.

136. Demydov I. The Holographic Network Analysis / Ivan Demydov, Bohdan Strykhalyuk, Mykhailo Klymash // The 2014 IEEE International Black Sea Conference on Communications and Networking (IEEE BlackSeaCom 2014), Odessa, Ukraine – Chisinau, Moldova, May 27-30, 2014. – Chisinau:TUM, 2014. - pp. 66-68. - ACM ISBN: 978-1-4799-4067-7/14 (electronic).

137. Климаш М.М. Моделирование та прогнозування зайнятості буфера системи розподілу мультисервісного трафіка з використанням методу автозупинки [Электронный ресурс] / М.М. Климаш, О.А. Лаврів, Б.А. Бугиль, Р.І. Бак // Проблемы телекоммуникаций. – 2011. – № 2 (4). – С. 108 – 117. – Режим доступа к журн.: http://pt.journal.kh.ua/2011/2/1/112_klimash_buffer.pdf.

138. Бугиль Б.А. Підвищення ефективності розподілу ресурсів телекомунікаційної мережі шляхом зміни маршрутів передавання даних [Електронний ресурс] / Б.А. Бугиль, М.М. Климаш, О.А. Лаврів, І.В. Демидов // Проблемы телекоммуникаций. – 2012. – № 4 (9). – С. 32 - 44. – Режим доступа до журн.: http://pt.journal.kh.ua/2012/4/1/124_bugil_resource.pdf.

139. Demydov I. Analysis of service workflows distribution and service delivery platform parameters / Ivan Demydov, Orest Lavriv, Bohdan Buhyl, Yuriy Dobush, Mykhailo Klymash // Int. J. Services, Economics and Management. -2013. - Vol. 5. - No. 4. - P. 280-290.

140. Рябинин И. А. Теоретические основы проектирования ЭЭС кораблей. - Л.: ВМА, 1964.- 240 с.

141. Волик Б.Г., Рябинин И.А. Эффективность, надежность и живучесть управляющих систем // Автоматика и телемеханика. - 1984. - № 12.

142. Крапивин В.Ф. О теории живучести сложных систем. — М.: Наука, 1978. — 248 с.

143. Крапивин В.Ф. Теоретико-игровые методы синтеза сложных систем в конфликтных ситуациях. — М.: Сов. радио, 1972. — 192 с.

144. Рябинин И.А., Черкесов Г.Н. Логико-вероятностные методы исследования надежности структурно-сложных систем. — М.: Радио и связь, 1981. — 216 с.

145. Волик Б.Г., Рябинин И.А. Эффективность, надежность и живучесть управляющих систем. // Автоматика и телемеханика, 1984. — № 12. — С. 151-160.

146. Волик Б.Г. Надежность, эффективность и живучесть управляющих систем // Системы управления и их применение. — М.: Ин-т проблем управления, 1985. — С. 23-31

147. Гуляев В.А., Додонов А.Г., Пелехов С.П. Организация живучих вычислительных структур. — К.: Наук. думка, 1982. — 140 с.

148. Додонов А.Г., Кузнецова М.Г., Горбачик Е.С. Введение в теорию живучести вычислительных систем. — К.: Наук. думка, 1990. — 184 с.

149. А.Г. Додонов, Д.В. Ландэ. Живучесть информационных систем. — К.: Наук. думка, 2011. — 256 с.

150. Дещинський П. Ю. Дослідження впливу перевантаження мережі на живучість пірингової системи / П. Ю. Дещинський, Б. М. Стрихалюк, М. В. Кайдан // Радіоелектроніка та телекомунікації : [збірник наукових праць] / відповідальний редактор Б. А. Мандзій. — Львів : Видавництво Львівської політехніки, 2012. — С. 231–235. — (Вісник / Нац. ун-т "Львів. політехніка" ; № 738). — Бібліографія: 5 назв.

151. Amdahl G.M. The validity of the single processor approach to achieving large-scale computing capabilities. In Proceedings of AFIPS Spring Joint Computer Conference, Atlantic City, N.J., AFIPS Press, 1967.

152. Климаш М.М. Дослідження доступності у хмарних сервісних системах / М.М. Климаш, І.В. Демидов, Мохамед Мехді Ель Хатрі,

Ю.Л. Дещинський // Радіоелектроніка та телекомунікації. Вісник Національного університету «Львівська політехніка». – Львів, 2016. – №849. – С. 218-229.

153. https://en.wikipedia.org/wiki/Cloud-based_networking

154. https://en.wikipedia.org/wiki/Network_as_a_service

155. Климаш М.М. Підвищення якості обслуговування в конвергентних мобільних системах на основі платформи UMA-A [Електронний ресурс] / М.М. Климаш, М.І. Бешлей, Б.М. Стрихалюк, Г.В. Холявка // Проблеми телекомунікацій. – 2014. – № 1 (13). – С. 3 - 19. – Режим доступу до журн.: http://pt.journal.kh.ua/2014/1/1/141_klymash_uma.pdf.

156. Климаш М.М. Модель надання сервісів на основі методу адаптації логічної структури cloud-системи / М.М. Климаш, Б.М. Стрихалюк, О.М. Шпур, М.І. Бешлей // Наукові записки УНДІЗ. – 2014. – №5(33). – С. 27-36.

157. Beshley M. SOA quality management subsystem on the basis of load balancing method using fuzzy sets [Електронний ресурс] / М. Beshley, М. Klymash, В. Strykhalyuk, О. Shpur, В. Bugil, I. Kagalo // International Journal of Computer Science and Software Engineering (IJCSSE). – 2015. – Vol. 4. - Issue 1. – P.10-21. – Режим доступу: <http://ijcsse.org/published/volume4/issue1/p3-V4I1.pdf>. – Назва з екрану.

158. Климаш М. М. Узагальнений метод оптимізації структур телекомунікаційної мережі за критерієм ефективності розподілу її ресурсів [Електронний ресурс] / М. М. Климаш, Б. А. Бугиль // Системи обробки інформації. - 2013. - Вип. 7. - С. 72-78. - Режим доступу: http://nbuv.gov.ua/UJRN/soi_2013_7_20.

159. P. Barham, B. Dragovic, K. Fraser, S. Hand, T. Harris, A. Ho, R. Neugebauer, I. Pratt, and A. Warfield, “Xen and the art of virtualization,” in SOSP’03: Proceedings of the nine-teenth ACM symposium on Operating systems principles. New York, NY, USA: ACM, 2003, pp. 164–177.

160. Klymash M.M., “The simulation and provision of the buffer’s utilization in the multi service traffic distribution system using auto stopping technique”

[Electronic resource] / M.M. Klymash, O.A. Lavriv, B.A. Bugil, R.I. Bak // Problems of Telecommunications. – 2011. – № 2 (4). – P. 108 – 117. – The access mode to the issue: http://pt.journal.kh.ua/2011/2/1/112_klimash_buffer.pdf.

161. Demydov I. Dynamic Correction of Routing Metrics by Pervasive Structural Routing in the Scalable Distributed Service Networks / Ivan Demydov, Mohamed Mehdi El Hatri, Olga Shpur // Problems of Infocommunications Science and Technology (PIC S&T), 2015 Second International Scientific-Practical Conference, 13-15 Oct. 2015, Kharkiv, Ukraine. – P. 164-166.

162. Walter F. Witt Keep Your Feet on the Ground When Moving Software into the Cloud / Walter F. Witt // International Journal of Digital Content Technology and its Applications. – 2010. – Volume 4, Number 2. – P.10-17.

163. Firewall classification: [excITingIP.com](http://www.excitingip.com) (Online): <http://www.excitingip.com>

164. Greg Young. Hype Cycle for Infrastructure Protection, in Gartner Inc., 11 August 2015, Reg.-Nr. G00277614, P. 45.

165. Adam Hils, Greg Young, Jeremy D'Hoinne. Magic Quadrant for Enterprise Network Firewalls, in Gartner Inc., 22 April 2015, Reg.-Nr. G00263955, P. 30.

166. Carol Fung, Raouf Boutaba. Intrusion Detection Networks: A Key to Collaborative Security (ISBN-13: 978-1466564121). Auerbach Publications, 2013. - 261p.

167. Fernandes, James. Academic Dictionary of Internet. Isha Books, 2005. - p. 316. - ISBN 9788182052680.

168. Добуш Ю.Д. Розвиток інфокомунікаційної мережної інфраструктури для систем електронного урядування : автореф. дис. ... канд. техн. наук : 05.12.02 / Ю. Д. Добуш; Нац. ун-т "Львів. політехніка". - Л., 2013. - 20 с. - укр.

169. Казакова Н.Ф. Оцінка живучості систем моніторингу інформаційного простору [Текст] / Н. Ф. Казакова // Східно-Європейський журнал передових технологій. — 2012. — Т. 4, № 2(58). — С. 12—15.

170. Відновлення та оптимізація інформації в системах прийняття рішень [Текст]: підруч. для студ. вищ. навч. закл., які навч. за напрямом "Інформаційна

безпека" / В. Л. Баранов [та ін.] ; Державний ун-т інформаційно-комунікаційних технологій. - К. : ДУІКТ, 2009. - 132 с.: рис. - Бібліогр.: с. 118-126. - ISBN 978-966-2970-35-7.

171. N. Kryvinska, C. Strauss, L. Auer, "Demand on Computational Intelligence Paradigms Synergy - SOA and Mobility for the Efficient Management of Resource-Intensive Applications on Constrained Devices", Chapter 14, in the "Next Generation Data Technologies for Collective Computational Intelligence", book Ed.: N. Bessis and F. Xhafa, the book series "Studies in Computational Intelligence", (SCI-352), Springer-Verlag Berlin Heidelberg, 2011, ISBN: 978-3-642-20343-5, e-ISBN: 978-3-642-20344-2, pp. 357-382.

172. Beloglazov A. Energy-Aware Resource Allocation Heuristics for Efficient Management of Data Centers for Cloud Computing/ A. Beloglazov, J. Abawajy, R. Buyya // Future Generation Computer Systems. - 2012. - vol. 28. - No. 5. - pp. 755-768.

173. Barroso L.A. The Case for Energy-Proportional Computing / L.A. Barroso, U. Hölzle // IEEE Computer. -2007. - Vol. 40. - No. 12. - pp. 33-37.

174. Dasgupta G. Workload Management for Power Efficiency in Virtualized Data Centers / G. Dasgupta, A. Sharma, A. Verma, A. Neogi, R. Kothari // Comm. ACM. – 2011. - Vol. 54. -No. 7. - pp. 131-141.

175. Hosman L., Baikie B. Solar-Powered Cloud Computing Datacenters / L. Hosman and B. Baikie // IT Professional. – 2013. - Vol. 15. - No. 2. - pp. 15-21.

176. Aggar M. Developers, Developers, Developers: Engaging the Missing Link in It Resource Efficiency, technical report, The Green Grid, Mar. 2013.

177. Greenberg A. The Cost of a Cloud: Research Problems in Data Center Networks / A. Greenberg, J. Hamilton, D.A. Maltz, P. Patel // Proc. ACM SIGCOMM Computer Comm. Rev. – 2009. - Vol. 39. - No. 1. - pp. 68-73.

178. Cardosa M. Shares and Utilities Based Power Consolidation in Virtualized Server Environments / M. Cardosa, M.R. Korupolu, A. Singh // Proc. 11th IFIP/IEEE Integrated Network Management (IM '09), June 2009.

179. Deneubourg J.L. The Dynamics of Collective Sorting: Robot-Like Ants and Ant-Like Robots / J.L. Deneubourg, S. Goss, N. Franks, A. Sendova-Franks, C. Detrain, and L. Chretien // Proc. First Int'l Conf. Simulation of Adaptive Behavior on from Animals to Animats. – 1990. - pp. 356-363.

180. Hirofuchi T. A Live Storage Migration Mechanism over Wan for Relocatable Virtual Machine Services on Clouds/ T. Hirofuchi, H. Ogawa, H. Nakada, S. Itoh, S. Sekiguchi // Proc. Ninth IEEE/ACM Int'l Symp. Cluster Computing and the Grid (CCGrid '09). – May, 2009. - pp. 460-465.

181. Liu H. Performance and Energy Modeling for Live Migration of Virtual Machines / H. Liu, C.-Z. Xu, H. Jin, J. Gong, X. Liao // Proc. 20th Int'l Symp. High Performance Distributed Computing (HPDC '11). – June, 2011. - pp. 171-182.

182. Khosravi A. Energy and Carbon-Efficient Placement of Virtual Machines in Distributed Cloud Data Centers/ A. Khosravi, S. Garg, R. Buyya// Proc. 19th Int'l Conf. Parallel Processing (Euro-Par '13), 2013.

183. Mazzucco M. Maximizing Cloud Providers' Revenues via Energy Aware Allocation Policies / M. Mazzucco, D. Dyachuk, R. Deters // Proc. 10th IEEE/ACM Int'l Symp. Cluster Computing and the Grid (CCGrid '10), May 2010. - pp. 131-138.

184. Rivoire S. A Comparison of High-Level Full-System Power Models / S. Rivoire, P. Ranganathan, C. Kozyrakis // Proc. Conf. Power Aware Computing and Systems (HotPower '08), Dec., 2008.

185. Fan X. Power Provisioning for a Warehouse-Sized Computer / X. Fan, W.-D. Weber, L.A. Barroso// Proc. 34th Ann. Int'l Symp. Computer Architecture (ISCA'07), June 2007. - pp. 13-23.

186. Врублевський А. Р. Модифікація протоколу маршрутизації EIGRP на основі нечіткої логіки / А. Р. Врублевський, І.П. Лісовий // Моделювання та інформаційні технології. - 2014. - Вип. 73. - С. 215-220.

187. Лісовий І.П. Маршрутизація на основі нечіткої логіки за протоколом RIP / І.П.Лісовий, А.Р. Врублевський, Г.В. Пилипенко // Телекомунікаційні та інформаційні технології. – К.:Державний університет телекомунікацій. - 2015. – № 3 - С. 64-69.

188. Семко В.В. Модель управління захистом інформації в інформаційно-телекому-нікаційній системі / В.В. Семко, В.Л. Бурячок, С.В. Толюпа, П.М. Складанний // *Радіоелектроніка та телекомунікації : [збірник наукових праць]* / відповідальний редактор Б. А. Мандзій. – Львів : Видавництво Львівської політехніки, 2015. – С. 151–155.

189. Кривуца В. Г. Інфокомунікаційні мережі нового покоління: монографія / В.Г. Кривуца, Л. Н. Беркман, С. В. Толюпа; ред.: В. Г. Кривуца; Держ. ун-т інформ.-комунікац. технологій. - К. : ДУІКТ, 2012. - 286 с. - (Мережі майбутнього).

190. Andrei Agapi et al. Routers for the Cloud // *IEEE Internet Computing*. – 2011. – №11. - pp. 72-76.

191. Detecting all the faces and outside edge for planar graph (in Russian) [Electronic resource] // <http://e-maxx.ru/algo/facets>

192. Kurapov S.V., Kondratyeva N.A. The algorithm for graph planarity (in Russian) // *The Bulletin of Zaporizhzhya State University*. – 2001. - №1. – <http://web.znu.edu.ua/herald/issues/archive/articles/1615.pdf>

193. Zhao X. Developing Fuzzy Enterprise Risk Management Maturity Model for Construction Firms / Xianbo Zhao, Bon-Gang Hwang, A.M.ASCE, Sui Pheng Low // *Journal of construction engineering and management*. - September 2013. - №9. - pp. 1179-1189.

194. Kang J. Autonomic personalized handover decisions for mobile services in heterogeneous wireless networks / J. Kang, J. Strassner, S. Seo, J. W. Hong // *Computer Networks*. – 2011. - Vol. 55. – Issue 5/16. - pp. 1520-1532.

195. Smaoui I. Multi-criteria dynamic access selection in heterogeneous wireless networks / I. Smaoui, F. Zarai, R. Bouallegue, L. Kamoun // in *Wireless Communication Systems, 2009. ISWCS 2009. 6th International Symposium on*. – 2009. - pp. 338-342.

196. Mohamed L. A hybrid approach for network selection in heterogeneous multi-access environments / L. Mohamed, C. Leghris, A. Adib // *New Technologies*,

Mobility and Security (NTMS), 2011 4th IFIP International Conference on. – 2011. - pp. 1-5.

197. Vasu K. QoS aware fuzzy rule based vertical handoff decision algorithm for wireless heterogeneous networks / K. Vasu, S. Maheshwari, S. Mahapatra, C.S. Kumar // Communications (NCC), 2011 National Conference on. – 2011. - pp. 1-5.

198. Yang T. A fuzzy logic vertical handoff algorithm with motion trend decision / Tao Yang, Peng Rong // in Strategic Technology (IFOST), 2011 6th International Forum on. – 2011. - pp. 1280-1283.

199. Бешлей М. І. Розвиток методів передавання даних реального часу шляхом вдосконалення процесів пріоритезації потоків у маршрутизаторах / М. І. Бешлей, В. В. Червенець, І. В. Демидов, В. І. Романчук, О. М. Панченко // Системи обробки інформації. — 2016. — № 5. — С. 114-123.

200. Beshley M. Increasing the efficiency of real-time content delivery by improving the technology of priority assignment and processing of IP traffic / M. Beshley, M. Seliuchenko, O. Lavriv, V. Chervenets, H. Kholiavka, M. Klymash // Smart Computing Review, - 2015. - Vol. 5. - No. 2. – P.76-88.

201. Klymash. M.M. Model of Network Resources Management on the Basis of Services Priorities Association / M. Klymash, M. Beshley, O. Lavriv // Proceedings of XIIth International conference "The experience of designing and application of CAD Systems in microelectronics" CADSM'2013. (24-27 February, Lviv-Poljana, Ukraine), 2013.- P. 146-148.

202. Бешлей М. І. Розробка та впровадження нового алгоритму планування черг у мережах з диференціацією сервісів. / М. І. Бешлей, М.О. Селюченко, Р.С.Колодій // VIII Міжнародна науково-технічна конференція «Проблеми телекомунікацій» ПТ-2015: збірник матеріалів конференції (22-25 квітня 2015р., м. Київ, Україна), 2015 - К.: НТУУ «КПІ»– С. 119-121.

203. M. Seliuchenko, M. Beshley, O. Panchenko, M.Klymash, "Development of Monitoring System for End-to-End Packet Delay Measurement in Software-Defined Networks", Modern problems of radio engineering, telecommunications and

computer science Proceedings of the XIII th International Conference TCSET'2016(Lviv – Slavske, February 23–26), 2016. - P. 667-670.

204. Beshley M. Investigation the modified priority queuing method based on virtualized network test bed /M. Beshley, V. Romanchuk, M. Seliuchenko, A. Masiuk // Proceedings of XIIIth international conference”The experience of designing and application of CAD Systems in microelectronics” CADSM’2015 (24-27 February, Lviv-Poljana, Ukraine), 2015. - P. 1-4.

205. Klymash Mykhailo. System for Increasing Quality of Service of Multimedia Data in Convergent Networks / Mykhailo Klymash, Mykola Beshey, Bohdan Stryhaluk, Marian Seliuchenko // Problems of Infocommunications. Science and Technology. – IEEE First International Conference. Kharkiv, October 14-17, 2014. – P. 63-66.

206. Strykhalyuk B., Implementation of wireless heterogeneous network based on LTE core virtualization for military communication systems / B.Strykhalyuk, I.Kahalo, M.Brych, M.Beshley, M.Seliuchenko // Системи озброєння і військова техніка: наук. журнал - X: Харк. ун-т Повітр. Сил ім. Івана Кожедуба. - 2014. – №4(40). - С. 125-132.

207. <http://en.wikipedia.org/wiki/Holography>

208. Denisyuk, Yuri N. "On the reflection of optical properties of an object in a wave field of light scattered by it". Reports of Academy of Sciences of USSR. – 1962. -Vol. 144 (6). – P. 1275–1278.

209. http://en.wikipedia.org/wiki/David_Bohm#cite_note-holo-5

210. Bohm D., Aharonov Y. Discussion of Experimental Proof for the Paradox of Einstein, Rosen, and Podolsky, Phys. Rev. – 1957. - Vol. 108. - No. 4. - pp. 1070–1076.

211. Bohm David. A new theory of the relationship of mind and matter, Philosophical Psychology. – 1990. - Vol. 3. - No. 2. - pp. 271—286. - doi:10.1080/09515089008573004

212. Bohm D. Fragmentation and Wholeness, van Leer Jerusalem Foundation, Jerusalem, 1976.

213. Schnars U., Jüptner W. Digital Holography. Springer, 2005.
214. Lam E. Three-dimensional microscopy and sectional image reconstruction using optical scanning holography / E. Lam, X. Zhang, H. Vo, T.-C. Poon, G. Indebetouw // Applied Optics. – Vol. 48 (34). - H113–H119.
215. Zhang X. Fast iterative sectional image reconstruction in optical scanning holography / X. Zhang, E. Y. Lam, and T.-C. Poon // in OSA Topical Meeting in Digital Holography and Three-Dimensional Imaging, 2009.
216. Shen Y. Binary image restoration by positive semidefinite programming. Opt. Lett. – 2007. – Vol. 32. – P. 121–123.
217. Система PRISM: как АНБ следит за Интернетом // Система PRISM: как АНБ следит за Интернетом. Электронный ресурс. Режим доступа: <http://m.ichip.ru/stati/internet-i-seti/2013/08/sistema-prism-kak-anb-sledit-za-internetom>
218. Dobush Yu. Approach to Secure Distributed Data Storing by Quasi-Random FAT Network Mapping / [Yuri Dobush, Ivan Demydov] // Матеріали Міжнародної науково-технічної конференції «Сучасні проблеми радіоелектроніки, телекомунікацій, комп'ютерної інженерії». – Львів – Славське, Україна, 2012. – P. 335.
219. Добуш Ю.Д. Застосування широкосмугових бездротових мереж UMTS/3G для організації мереж моніторингу параметрів розподілених об'єктів / [Ю.Д. Добуш, І.В. Демидов] // Матеріали VII Міжнародної науково-технічної конференції «Сучасні інформаційно-комунікаційні технології» (COMINFO'2011-Livadia): Збірник тез. – К.: ДУІКТ, 2011. – С.154 -155.
220. Демидов І.В. Методи фіксації метаданих з'єднань глобальних мобільних телекомунікаційних мереж / І.В. Демидов, Ю.Д. Добуш // Всеукраїнська Науково-практична конференція „Сучасні проблеми телекомунікацій і підготовка фахівців в галузі телекомунікацій – 2013”. Матеріали конференції 30 жовтня - 2 листопада 2013 р. – Львів, 2013. – С.167-170.

221. Лапшин М. Высокая нагрузка на erlang-приложения: erlyvideo на гигабитном канале // Российские Интернет-технологии. Клуб профессионалов. Электронный ресурс. Режим доступа: <http://profyclub.ru/docs/298>.

222. Голубев И.Ю. Оптимизация распределения запросов в системе кластеров при сочетании аналитического и имитационного моделирования / И.Ю. Голубев, В.А. Богатырев // Научно-технический вестник информационных технологий, механики и оптики. – 2012. - №5(81). – С.79-83.

223. Demydov I. The Synthesis Methodology of Scalable Telecommunication Service Platforms / Ivan Demydov, Zenoviy Kharkhalis // 2nd IEEE International Conference on Advanced Information and Communication Technologies-2017 (AICT-2017): Conference Proceedings. – Lviv, 2017. – P. 199-203.

224. Demydov I. The Method of Improving the Availability at Cloud Service Systems / Ivan Demydov, Olga Shpur, Rakhman Lutfor, Yurii Deshchynskyi // Матеріали Міжнародної конференції з інформаційно-телекомунікаційних технологій та радіоелектроніки (УкрМіКо'2016/UkrMiCo'2016): Збірник тез. – К.: НТУУ «КПІ», 2016. – С. 446 - 448.

225. Demydov I. Methods of traffic load balancing in telecommunication networks / Ivan Demydov, Yasser Muayyad Al-Hayali // Науково-методична конференція «Сучасні проблеми телекомунікацій і підготовка фахівців в галузі телекомунікацій – 2012». Матеріали конференції 1-4 листопада 2012 р. – Львів, 2012. – С.28-30.

226. Demydov I. The Research of the Availability at Cloud Service Systems / I. Demydov, M. Klymash, Z. Kharkhalis, B. Strykhaliuk, P. Komada // Proceedings of SPIE: Photonics Applications in Astronomy, Communications, Industry, and High-Energy Physics Experiments, USA. – 2017. – Vol. 10445. – doi: 10.1117/12.2280885.

227. Demydov I. The Structural-Functional Synthesis of IoT Service Delivery Systems by Performance and Availability Criteria / Ivan Demydov, Yulia Klymash, Mykola Brych, Mykhailo Klymash // Internet of Things (IoT) and Engineering Applications (Canada). – May, 2017. – Vol. 2. – Issue 1. – P. 1-13.

228. Красько О. В. Аналіз параметрів оптичного сигналу в повністю оптичній мережі з комутацією за довжинами хвиль / О. В. Красько, І.В. Демидов, М. В. Брич // Вісн. Нац. ун-ту «Львів. Політехніка». - 2014. - № 796. - С. 140-146. - Бібліогр.: 23 назв. - укр.

229. Стрихалюк Б. Моделювання хмаринкової мережної системи у гіперболічних віртуальних координатах [Електронний ресурс] / Б. Стрихалюк, М. Климаш, І. Демидов // Комп'ютерні технології друкарства. - 2014. - № 32. - С. 3-19.

230. Демидов І.В. Доступність композитних застосувань у сервісно-орієнтованих системах / І.В. Демидов, О.А. Лаврів, О.М. Шпур, М.О. Селюченко // Вимірювальна та обчислювальна техніка в технологічних процесах: матеріали XIII Міжнародної науково-технічної конференції (6-12 червня 2014 р. м. Одеса). – 2014. - с.119-121.

231. Strykhalyuk B. Synthesis of distributed service-oriented structures cloud networks is based on algorithm for determining hyperbolic virtual coordinates / Bogdan Strykhalyuk, Olga Shpur, Ivan Demydov, Yulia Klymash // Proceedings of XIIIth international conference «The experience of designing and application of CAD Systems in microelectronics» CADSM'2015, 24-27 February, Lviv-Poljana, Ukraine. – 2015. - P. 231-235.

232. Demydov I. Mobility Management and Vertical Handover Decision in an Always Best Connected Heterogeneous Network / Ivan Demydov, Marian Seliuchenko, Mykola Beshley, Mykola Brych // Proceedings of XIIIth international conference «The experience of designing and application of CAD Systems in microelectronics» CADSM'2015, 24-27 February, Lviv-Poljana, Ukraine. – 2015. - P. 103-105.

233. Demydov I.V. The features of cloud service delivery platform structural-functional synthesis / I.V. Demydov, M.M. Klymash, O.M. Shpur, Z.V.Kharkhalis // Міжнародна науково-технічна конференція «Сучасні інформаційно-телекомунікаційні технології»: матеріали науково-технічної конференції (17-20 листопада 2015 р. м.Київ), Т.3 – К: ДУТ. – 2015. – С. 19-21.

234. Демидов І.В. Впровадження хмарних сервісних систем в національному мережному сегменті України / І.В. Демидов, О.М. Шпур // X Міжнародна науково-технічна конференція «Проблеми телекомунікацій» ПТ-2016: Збірник матеріалів конференції (19-22 квітня 2016р. м. Київ) - К.: НТУУ «КПІ», 2016. – С. 342-344.

235. Стрихалюк Б.М. Структурний та функціональний синтез гетерогенних сервісно-орієнтованих телекомунікаційних мереж: дис. ... д-ра техн. наук : 05.12.02 / М-во освіти і науки України, Нац. ун-т "Львів. політехніка" .- Львів, 2015 .-302 с.-(іл.) .-Бібліогр.: с. 284-302 (164 назви)

236. Самер Мохамед Мустафа Аввад. Оптимізація транспортних мереж і їх навантаження у системах мобільного зв'язку наступного покоління: дис. ... канд. техн. наук : 05.12.02 / М-во освіти і науки, молоді та спорту України, Нац. ун-т "Львів. політехніка" .-Л., 2011 .-140 с.-(іл.) .-Бібліогр.: с. 127-140 (161 назва)

237. Добуш Ю.Д. Розвиток інфокомунікаційної мережної інфраструктури для систем електронного урядування: дис. ... канд. техн. наук : 05.12.02 / М-во освіти і науки України, Нац. ун-т "Львів. політехніка" .-Львів, 2013 .-164 с.-(іл.) .-Бібліогр.: с. 147-161 (167 назв)

238. Stampar M., Fertalj K. Artificial intelligence in network intrusion detection // Information and Communication Technology, Electronics and Microelectronics (MIPRO), 2015 38th International Convention on, 25-29 May 2015, Opatija, Croatia. - 10.1109/MIPRO.2015.7160479.

239. Ватутин Э.И. Оценка степени параллелизма алгоритма с использованием матрицы отношений // Материалы IV международной научно-технической конференции «Современные инструментальные системы, информационные технологии и инновации». Ч. 2. Курск: изд-во КурскГТУ, 2006. - С. 135–139.

240. Ватутин Э.И. Определение степени параллелизма параллельной граф-схемы алгоритма // Интеллектуальные и информационные системы (Интеллект–2009). Тула: изд-во ТулГУ, 2009. - С. 24–26.

241. Клейнрок Л. Теория массового обслуживания. – М.: Машиностроение, 1979. – 432 с. (стор. 177-180).

242. Червенець В.В. Підвищення якості передачі потокового трафіку в мультисервісних мережах: дис. ... канд. техн. наук : 05.12.02 / М-во освіти і науки України, Нац. ун-т "Львів. політехніка" .-Львів, 2017 .-173 с.-(іл.) .- Бібліогр.: с. 151-166 (121 назва)

243. Бешлей М.І. Підвищення якості обслуговування пріоритетного трафіку реального часу у вузлах мультисервісної мережі: автореферат дисертації на здобуття наукового ступеня кандидата технічних наук : 05.12.02 – телекомунікаційні системи та мережі / Микола Іванович Бешлей ; Міністерство освіти і науки України, Національний університет "Львівська політехніка". – Львів, 2015. – 24 с. – Бібліографія: с. 15–19 (40 назв).

ДОДАТОК А. Початковий код програми для комп'ютерного моделювання процесів обслуговування запитів користувачів у ВН RAN безпроводного сегменту сервісної мережної системи.

Наведено алгоритм розрахунку імовірностей блокування на транзитних мережних ресурсах, зокрема резервного маршруту сегменту ТКСП. Програмний код реалізовано відповідно до запропонованих у дисертаційній роботі підходів та моделей. Він складається з трьох модулів:

1. Unitl.cpp – модуль основних обчислень;
2. Matrix.cpp – реалізація програмного класу Matrix;
3. Project.cpp – базова точка входу програми.

Програмний модуль Unitl.cpp

```
//-----  
#include <vcl.h>  
#pragma hdrstop  
#include "Matrix.h"  
#include "Unitl.h"  
#include <math.h>  
  
//-----  
#pragma package(smart init)  
#pragma resource "*.dfm" TForm1 *Form1;  
double dL1; //канальні ресурси А-С;  
double dL2; // канальні ресурси С-В;  
double dN; // канальні ресурси А-В;  
double dial; //інтенсивність вхідного потоку запитів від  
користувачів підсистеми А  
  
double dla2; // інтенсивність вхідного потоку запитів від  
користувачів підсистеми С  
  
double dmu; // інтенсивність обслуговування запитів від  
користувачів на кожній з ланок системи.  
  
double dq; // ймовірність того, що субсистема В не  
обслужить запит від субсистеми А.  
  
//-----
```

```

double Erlang(double n, double ro) { if(n == 0) return 1;
    double tmp er = ro*Erlang(n-1, ro); return
    tmp er/(n+tmp er);

//-----

// імовірність блокування запиту від субсистеми А на А-С.

double getP2(const Matrix *rez) { double sum = 0; for (int
    i = 0; i <= (dL2-dL1); i++)
    sum += rez->value(getIndex(i, dL1), 0); return
    sum;
}

//-----

// імовірність блокування запиту від субсистеми А на С-В.

double getP3(const Matrix *rez) { double sum = 0; for (int i
    = 0; i <= dL2; i++)
    for (int j = 0; j <= dL1; j++)
        if ((i + j) == dL2 ) sum += rez-
>value(getIndex(i, j), 0); return sum;
}

// Обчислюються наступні імовірності:
// 1. Імовірність блокування трафіку запиту від субсистеми
А на А-В.
// 2. Імовірність блокування трафіку запиту від субсистеми
А на А-В після його оброблення в субсистемі В.
void getАНР(double &p1 1, double &p12,
double q, double eps, double M, double N) {
    bool isfirst = true;
    do{
        if (isfirst) {
            p11 =Erlang(M,dla1/dmu); isfirst = false; } else
            {
                p11 = fabs(Erlang(N, dla1/dmu) - p12);
            }
        p12 = ErIang(N, (dla1*(1-p1 1)*(1-dq))/dmu );
    }
}

```

```

    } while (fabs(pl 1 + pl2 - Erlang(N, dla1/dmu)) >=
deps); }

//-----
// повернення кількості станів системи

int getValueState() { int res = 0;
    for (int i = 0; i <= dL2; i++) for (int j = 0; j <=
        dL1; j++) if(i+j<=dL2)res++;

    return res; }

//-----
// повернення індексу стовпчика матриці

int getlndex(int in, int jn) { int num = 0, rez = 0; for
    (int i = 0; i <= dL2; i++) for(int j = 0;j<=dL1;j++)
    if(i+j<=dL2){
        if(i = in && j =jn) rez = num; num++;
    }

    return rez; }

//-----

// ініціалізація матриці

Matrix * TForm1::init()

{
    int valuestate = getValueState();
    Matrix *sur = new Matrix(valuestate, valuestate);
    for (int i = 0, k = 0; i <= dL2; i++)
        for (int j = 0; j <= dL1; j++)
            if(i+j<=dL2){
                if(i = 0&&j = 0){
                    sur->value(k, getIndex(i, j)) = -
                        (dla1+dla2); sur->value(k, getIndex(i+1,
                            j)) = dmU; sur->value(k, getIndex(i, j+1))
                            = dmU;
                }

                if(i = 0&&j!=0&&j !=dL1){ sur->value(k,
                    getIndex(i, j)) = -(j*dmU + dla1 + dla2);

```

```

        sur->value(k, getIndex(i, j-1)) = dla2;
        sur->value(k, getIndex(i+1, j)) = dmdu;
        sur->value(k, getIndex(i, j+1)) =
            (j+1)*dmdu;
    }

    if(i = 0&&j = dL1) {
        sur->value(k, getIndex(i, j)) = -
            (dla1+j*dmdu); sur->value(k, getIndex(i, j-
            1)) = dla2; sur->value(k, getIndex(i+1, j))
            = dmdu;
    }

    if (i = dL2&&j==0) {
        sur->value(k, getIndex(i, j)) = -i*dmdu;
        sur->value(k, getIndex(i-1,j)) = dla1;
    }

    if (i = 0 &&i!=dL2 &&i!=0) {
        sur->value(k, getIndex(i, j)) = -(i*dmdu +
            dla1 + dla2); sur->value(k, getIndex(i+1,
            j)) = (i+1)*dmdu; sur->value(k, getIndex(i,
            j+1)) = dmdu;
    }

        if (i >0&&i+j = dL2) {
            sur->value(k, getIndex(dL2-j, j)) = -(j*dmdu
+ (dL2-j)*dmdu);
            sur->value(k, getIndex(dL2-j, j-1)) =
            dla2; sur->value(k, getIndex(dL2-j-1,
            j)) = dla1;
        }

    if (i != 0 && j != 0 && i + j != dL2) {
        sur->value(k, getIndex(i, j)) = -(dla1 +
i*dmdu + dla2 + j*dmdu);
        sur->value(k, getIndex(i, j-1)) =
            dla2; sur->value(k, getIndex(i-1, j))
            = dla1; sur->value(k, getIndex(i+1,
            j)) = (i+1)*dmdu;
        sur->value(k, getIndex(i, j+1)) =
            (j+1)*dmdu;
    }
    k++;
    for (int j = 0; j < getValueState(); j++)

```



```

        sur->value(0,j)= 1;
        return sur; }

//-----
fastcall TForm 1: :TForm 1 (TComponent*
    Owner) : TForm(Owner)
{ }

//-----

// Закриття програми

voidfastcall TForm 1 "Button 1Click(TObject *Sender)
{
    Close();
}

//-----

// виконання перевірки введених значень

voidfastcall TForm1::Button3Click(TObject *Sender)
{

try{
    dL1 =L1->Text.ToDouble(); } catch (EConvertError &e) {
    Application->MessageBoxA(
        MB_OK+MB_ICONSTOP); return;
    }

try{
    dL2 = L2->Text.ToDouble(); } catch (EConvertError &e) {
    Application->MessageBoxA( ,
        MB_OK+MB_ICONSTOP);
    return;

if(dL2<=dL1){ Application->MessageBoxA(,
        MB_OK+MB_ICONSTOP); return;

} try{

    dN = N->Text.ToDouble(); } catch (EConvertError &e) {

    Application->MessageBoxA(

```

```

MBOOK+MBICONSTOP); return;
}

try{
    dM = M->Text.ToDouble(); } catch (EConvertError &e)
{Application->MessageBoxA( MB_OK+MB_ICONSTOP); return;
} if(dN<=dM){

Application->MessageBoxA(, MB_OK+MB_ICONSTOP); return;

} try{

    dial = la1->Text.ToDouble(); } catch (EConvertError &e) {
Application->MessageBoxA(,
                        MB_OK+MB_ICONSTOP); return;

} try{

dla2 = la2->Text.ToDouble(); } catch (EConvertError &e) {
Application->MessageBoxA( MB_OK+MB_ICONSTOP); return;

try{
    dmU = mu->Text.ToDouble(); } catch (EConvertError &e) {
Application->MessageBoxA( MB_OK+MB_ICONSTOP);
return;
} try{

    dq = q->Text.ToDouble(); } catch (EConvertError &e)
{Application->MessageBoxA(MB_OK+MB_ICONSTOP); return;

} try{

    deps = eps->Text.ToDouble();

catch (EConvertError &e) { Application->MessageBoxA(
MB_OK+MB_ICONSTOP); return;

} Matrix *work = init();

Matrix leftteil(work->getRow(), 1), result;
leftteil.value(0,0)=1;

//      result.setForm(ProgressBar1);

```

```

result.operator=(work->Gauss(leftteil));

p2->Caption = getP2(&result); p3->Caption =
getP3(&result); double pi11 = 0, pi12 = 0; getAHP(pi11,
pi 12, dq, deps, dM, dN); p 11 ->Caption = pi 11; p12-
>Caption = pi12; delete work;
}
//-----

```

Програмний модуль Matrix.cpp

```

#include "Matrix.h"
#include <iostream.h>
#include <math.h>
#include "Unit1.cpp"

// ініціалізація матриці

Matrix::Matrix(int row, int col)
{
    this->row = row;
    this->col = col;

    for (int i = 0; i < row; i++) {

        single_vector vec; for(int
        j = 0; j < col; j++)
        vec.push_back(0);
        element.push_back(vec);
    }

// Вивід матриці

void Matrix::print()
{
    cout <<endl;
    for (double vector::iterator i = element.begin(); i !=
    element.end(); i++) {

```

```

        for (single vector::iteratorj = i->begin(); j != i-
>end(); j++)
            cout<< *j << "    ";
        cout<< endl;
    }
    cout << endl;
}

// параметри оператора присвоювання

Matrix &Matrix::operator= (Matrix &Obj) {

if (this = &Obj) return
    *this; row = Obj.row;

    col = Obj.col; element =
    Obj.element;

    return *this; }

// звернення до елемента матриці

double &Matrix::value (int index 1, int index2)
{
    return element[index1][index2];
}

// звернення до елемента матриці без можливості змін

const double &Matrix::value (int index 1, int index2) const
{
    return element[index1][index2];
}

// параметри оператора додавання

Matrix Matrix::operator+ (Matrix &Obj)

    if (this->row != Obj.row || this->col != Obj.col) {
        cout<<"Error: 'Matrix Matrix::operator+ (Matrix
&Obj)'" << endl; return Matrix();
    }

    Matrix newObj = Obj;
    for (int i = 0; i < this->row; i++)

```

```

        for (int j = 0; j <this->col; j++)
            newObj.value(i, j) += this->value(i, j);

    return newObj; }

// параметри оператора множення

Matrix Matrix::operator* (Matrix &Obj)
{
    if (this->col != Obj.row) {
        cout<< "Error: 'Matrix Matrix-operator* (Matrix
            &Obj)'" << endl; return Matrix();

        Matrix newObj(row, Obj.col); for(int i = 0; i < this-
            >row; i++) for(int j = 0; j<Obj.col;j++)
                for(int k = 0; k < this->col; k++)
                    newObj.value(i, j) += this->value(i, k)*Obj.value(k, j);

        return newObj; }

    // параметри оператора віднімання

Matrix Matrix-operator- (Matrix &Obj)
{
    if (this->row != Obj.row || this->col != Obj.col) {

cout << "Error: 'Matrix Matrix::operator- (Matrix &Obj)'"
<< endl;

return Matrix(); }

    Matrix newObj = Obj;
    for (int i = 0; i < this->row; i++)
        for (int j = 0; j < this->col; j++)
            newObj.value(i, j) = this->value(i, j);

    return newObj; }

// обчислення оберненої матриці

Matrix Matrix::operator~ ()

{
    Matrix Obj(this->row, this->col),
        tempObj(this->row, 2*this->col);
    for(int i = 0; i < this->row; i++)

```

```

        for(int j = 0; j < this->col; j++)
            tempObj.value(i, j) = this->value(i, j);
for(int i = 0; i < this->row; i++)
    for(int j = this->col; j < 2*this->col; j++)
        if((i+this->col)==j)
            tempObj.value(i, j) = 1;

for(int i = 0; i < this->row; i++) {

    int ki = i;
    while((tempObj.value(ki, i) == 0) && (ki != this->row)) { for(int kj = i; kj < 2*this->col;
        kj++) {
            double tmp = tempObj.value(ki, kj);
            tempObj.value(ki, kj) = tempObj.value(i, kj);
            tempObj.value(i, kj) = tmp;

        }

        ki++;

    }

    for(ki = i+1; ki < this->row; ki++) {
        double kof = tempObj.value(ki,
            i)/tempObj.value(i, i);
        for(int kj = i; kj < 2*this->col; kj++)
            tempObj.value(ki, kj) -=
                kof*tempObj.value(i, kj);

for(int i = 0; i < this->row; i++) {
    double tmp = tempObj.value(i, i); for(int j = i; j <
        2*this->col; j++) tempObj.value(i, j) /= tmp;
}

for(int i = this->row-1; i >= 0; i~) for(int j = i-
    1; j>=0; j--){
    double tmp = tempObj.value(j, i); for(int k =
        i; k < 2*this->col; k++)
        tempObj.value(j, k) -= tempObj.value(i,
            k)*tmp;
}

for(int i = 0; i < this->row; i++)
    for(int j = 0; j < 2*this->col; j++) if(j >=

```

```

        this->col) Obj.value(i, j-this->col) =
        tempObj.value(i, j);

    return Obj; }

Matrix *Matrix::Minor(int exi, int exj)

{
    Matrix *Obj = new Matrix(this->row-1, this->col-1);
    for (int i = 0; i < this->row; i++)
        for (int j = 0; j < this->col; j++)

            if((i!=exi)&&(i!=exj))
                Obj->value(i - (i > exi ? 1 : 0), j - (j >
exj ? 1 : 0)) = this->value(i,j);
    return Obj;
}

double Matrix::Determinant()
{
    if (this->col != this->row) return-pow( 10, 10);
    if (this->col = 1 && this->row == 1) return this-
>value(0, 0);
    else {

float res = 0;
        for (int i = 0; i < this->row; i++)

res += (i%2 == 0 ? 1 : -1)*this->value(i, 0)*Minor(i, 0)-
>Determinant(); return res;
    } }

Matrix Matrix::Gauss(Matrix Obj) {
    if(this->row !=this->col || Obj.row !=this->row ||
    Obj.col != 1) { cout<<"Gauss: col != row" <<endl;
    return Matrix(0, 0);
    }

/*
    if(this->Determinant() = 0) {
        cout << "Determinant() = 0" << endl; return
        Matrix(0, 0);
    }*/
}

```

```

Matrix Rezult = Matrix(this->row, this->col+1), X =
    Matrix(this->row, 1);

/*Initialition Rezult*/
for(int i = 0; i < this->row; i++)
    for(int j = 0; j < this->col; j++)
        Rezult.value(i, j) = this->value(i, j);
for(int i = 0; i < this->row; i++)
    Rezult.value(i, col) = Obj.value(i, 0);
cout <<"Gauss: inisialization complete" << endl;

//Rezult.Print matrix ();
for(int i = 0; i < this->row; i++) {
    int ki = i;

    while((Rezult.value(ki, i) = 0) && (ki != this->row)) {
        for(int kj = i; kj < this->col+1; kj++) {
            double tmp = Rezult.value(ki, kj);
            Rezult.value(ki, kj) = Rezult.value(i, kj);
            Rezult.value(i, kj) = tmp;
        }
        ki++;
    }
    //Rezult.Print_matrix();

    for(ki = i+1; ki < this->row; ki++) {
        double kof = Rezult.value(ki, i)/Rezult.value(i, i);
        for(kj = i; kj < this->col+1; kj++)
            Rezult.value(ki, kj) -= kof*Rezult.value(i, kj);
    }
    cout<<"Gauss: step 1 complete:" << i << endl;
}
cout<< "Gauss: step 2 complete" << endl;

//Rezult.Print_matrix ();
for(int i = 0; i < this->row; i++) {
    double tmp = Rezult.value(i, i);
    for(int j = i; j < this->col+1; j++) Rezult.value(i, j)
        /= tmp;
}

```



```

}

cout <<"Gauss: step 3 complete" << endl;

//Rezult.Print matrix(); for(int i = this->row-1; i >= 0;
i~) for(int j = i-1; j>=0; j--){
    double tmp = Rezult.value(j, i); for(int k = i; k <
this->col+1; k++)
        Rezult.value(j, k) -= Rezult.value(i, k)*tmp;
}

cout <<"Gauss: step 4 complete"<< endl;

//Rezult.Print_matrix(); for(int j = 0; j < this->row; j++)
    X.value(j, 0) = Rezult.value(j, this->col);

    return X; }

Matrix Matrix::Trans() {
    Matrix Rezult = Matrix(this->col, this->row);

    for(int i = 0; i < this->row; i++)

    for(int j = 0; j < this->col; j++) Rezult.value(j, i) =
this-> value(i, j); return Rezult;
}

```

Програмний модуль Project.cpp

```

#include <vcl.h>

#pragma hdrstop

//-----
USEFORM("Unit1.cpp", Form1);

//-----

// Функція входу у програму моделювання

```

```

WINAPI WinMain(HINSTANCE, HINSTANCE, LPSTR, int) {

    try
    {
        Application->Initialize();
        Application->CreateForm( classid(TForm 1), &Form 1);
        Application->Run();
    }
    catch (Exception &exception)
    {
        Application->ShowException(&exception);
    }
    catch (...) {

        try
        {
            throw Exception("");
        }
        catch (Exception &exception)
        {
            Application->ShowException(&exception);
        }

    }

    return 0;
}

//-----

```

ДОДАТОК Б. Програмний код для реалізації моделі SaaS на основі функціональної парадигми системного програмування.

Послідовна компонента початкового коду (її мінімізована реалізація займає близько **40%** загального обсягу коду програмного модуля мовою програмування Erlang) – моделює мережний TCP шлюз (TCP gateway):

```
start(Port) ->
    register(server, spawn_link(fun() ->
        {ok, Listen} = gen_tcp:listen(Port, [binary,
            {reuseaddr, true}, {active, true}, {packet, 4}]),
        spawn(fun() -> acceptor(Listen, 1) end),
        timer:sleep(infinity)
    end)).

stop() ->
    exit("Stopped by user").
```

Розпаралелена компонента початкового коду (її мінімізована реалізація займає близько **60%** загального обсягу коду програмного модуля мовою програмування Erlang) – моделює балансувальник сервера послуг (application server and RR balancer) за алгоритмом Round Robin:

```
acceptor(ListenSocket, N) ->
    {ok, Socket} = gen_tcp:accept(ListenSocket),
    Nodes = nodes(),
    Length = length(Nodes),
    if
        N >= Length -> spawn(fun() ->
            acceptor(ListenSocket, 1) end);
        N < Length -> spawn(fun() ->
            acceptor(ListenSocket, N+1) end)
    end,
```

```

Node = lists:nth(N, Nodes),
handle(Socket, Node).

handle(Socket, Node) ->
    receive
        {tcp, Socket, Msg} ->
            spawn(Node, 'slave', 'calc', [self(),
binary_to_term(Msg)]),
            receive
                {ack, Result} ->
                    io:format("Result: ~p~n",
[Result]),
                    gen_tcp:send(Socket,
term_to_binary(Result)),
                    gen_tcp:close(Socket)
            end
        end
    end.

```

Просте сервісне застосування, що може реплікуватись у довільній доступній обчислювальній потужності розподіленої сервісної мережної платформи під управлінням вищенаведеного сервера послуг:

```

-module(slave).
-export([calc/2, init/0]).

init() ->
    net_kernel:connect_node('master@DESKTOP-VK9PUOV').

calc(From, Msg) ->
    Result = {fib(Msg), node()},
    From ! {ack, Result}.

```

```
fib(1) ->  
1;  
fib(2) ->  
1;  
fib(N) ->  
fib(N-1) + fib(N-2).
```

ДОДАТОК В. Акти впровадження результатів дисертаційної роботи

“ЗАТВЕРДЖУЮ”

Директор Львівської філії
(керуючої філії Західного
макрорегіону)

ПАТ «Укртелеком» у м. Львові,
кандидат технічних наук



Андрухів Т.В.

03 2017 р.

79007, м. Львів, вул. Дорошенка, 43

АКТ

про впровадження результатів дисертаційної роботи **Демидова Івана Васильовича** на тему «Синтез телекомунікаційних сервісних платформ національного масштабу» на здобуття наукового ступеня доктора технічних наук за спеціальністю 05.12.02 – телекомунікаційні системи та мережі

Даний акт складений про те, що в результаті спільних наукових досліджень в галузі синтезу масштабованих телекомунікаційних сервісних платформ у Львівській філії ПАТ «Укртелеком» були використані запропоновані Демидовим І.В. методи для підвищення ефективності обслуговування навантаження користувачів при масштабуванні сервісних мережних систем, відповідних ЦОД та телекомунікаційних платформ, а також при упровадженні методів підтримки їх функціональної стійкості.

Підприємство підтверджує працездатність розроблених методів диференційованого обслуговування користувачів, адаптивного резервування мережних ресурсів телекомунікаційних платформ у рамках розробленої методології синтезу телекомунікаційних сервісних платформ національного масштабу. За рахунок використання модифікованого методу обслуговування черг та, відповідно, удосконалення процесів обслуговування пріоритезованого трафіку вдалося покращити часові параметри якості обслуговування у 2-7 разів, у залежності від рівня завантаження вузлів мультисервісної мережної платформи компанії.

Результатом застосування запропонованої методології на мережах ПАТ «Укртелеком» є поетапна трансформація магістрального комунікаційного обладнання компанії на рівнях IaaS та PaaS реалізацій із урахуванням поступової переорієнтації на проектування IMS (IP Multimedia Subsystem) інфраструктури у регіональних філіях. При трансформуванні мереж згідно переходу до CBN концепції згідно запропонованої методології оптимізовано

показники щодо функціонування телекомунікаційних сервісних платформ ПАТ «Укртелеком» на рівнях IaaS та PaaS, які наведено у табл. 1 та табл. 2. Похибка моделювання, розрахована за участю інженерів ПАТ «Укртелеком» по відношенню до фактичних даних складає не більше 5-8%.

Таблиця 1. Порівняння прогнозованого та фактичного середньорічних показників продуктивності телекомунікаційних платформ ПАТ «Укртелеком».

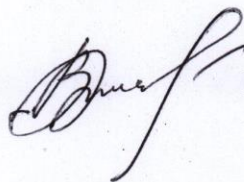
Період, рік	Продуктивність мережі (рівень IaaS) розрахункова, Гбіт/с	Продуктивність мережі (рівень IaaS) фактична, Гбіт/с	Продуктивність мережі (рівень PaaS) розрахункова, Гбіт/с	Продуктивність мережі (рівень PaaS) фактична, Гбіт/с
2011	212	199	205	182
2012	256	281	210	244
2013	240	227	205	188
2014	215	198	214	210
2015	305	294	280	278
2016	312	314	290	299

Таблиця 2. Порівняння прогнозованого та фактичного середньорічних показників сервісної доступності у телекомунікаційних платформах ПАТ «Укртелеком».

Період, рік	Сервісна доступність (рівень IaaS) розрахункова	Сервісна доступність (рівень IaaS) фактична, Гбіт/с	Сервісна доступність (рівень PaaS) розрахункова, Гбіт/с	Сервісна доступність (рівень PaaS) фактична, Гбіт/с
2011	0,998	0,999	0,9989	0,9989
2012	0,999	0,998	0,9990	0,9990
2013	0,999	0,997	0,9991	0,9991
2014	0,986	0,992	0,9990	0,99909
2015	0,995	0,998	0,9995	0,99999
2016	0,999	0,999	0,9998	0,99999

Акт складений для пред'явлення до спеціалізованої вченої ради із захисту дисертацій і не є підставою для фінансових розрахунків.

Начальник відділу планування мереж



Качан В.М.



«ЗАТВЕРДЖУЮ»

Директор

СП «Мікро-код» Лтд

Ю. Д. Добуш

«15» травня 2017 року

АКТ

про впровадження результатів дисертаційної роботи
докторанта кафедри телекомунікацій Національного університету «Львівська
політехніка»
к.т.н., доцента Демидова Івана Васильовича

Даний акт складений про те, що в Українсько-канадському спільному підприємстві у формі Товариства з обмеженою відповідальністю «Мікро-код» ЛТД (м. Львів) використані результати дисертаційної роботи Демидова Івана Васильовича «Синтез телекомунікаційних сервісних платформ національного масштабу». А саме:

1. Пропозиції та рекомендації щодо створення магістральних телекомунікаційних сервісних платформ з відкритою архітектурою, а також розроблення систем фіксації метаданих комунікаційної активності користувачів мережних систем, у тому числі – із використанням DPI-технологій;
2. Концепція мігруючого мережного екрану для виявлення та захисту від небажаної мережної активності сегментів телекомунікаційних платформ;
3. Результати чисельних та експериментальних досліджень на обладнанні підприємства, що дали змогу оцінити ефективність впровадження відкритої сервісної архітектури у телекомунікаційній мережній платформі на рівнях SaaS та PaaS модельних реалізацій.

Підприємство засвідчує, що у рамках виконаних здобувачем наукових досліджень імовірно-часових характеристик телекомунікаційних платформ з відкритою сервісною архітектурою досягнуто відповідність між результатами моделювання та одержаними ним експериментальними даними з відхиленням не більше 5%.

Керівник проектного відділу

Керик Т. Р.



«ЗАТВЕРДЖУЮ»
Проректор з науково-педагогічної роботи
Національного університету
«Львівська політехніка»
доц. Давидчак О.Р.
_____ 2017 р.

АКТ

про використання результатів докторської дисертаційної роботи
к.т.н., доцента Демидова Івана Васильовича
«Синтез телекомунікаційних сервісних платформ національного масштабу»
у навчальному процесі кафедри телекомунікацій

Даний акт складений комісією у складі:

- д.т.н., доц. Стрихалюка Б.М., декана повної вищої освіти, голови Науково-методичної ради Інституту телекомунікацій, радіоелектроніки та електронної техніки;
- к.т.н., доц. Озірковського Л.Д., декана базової вищої освіти Інституту телекомунікацій, радіоелектроніки та електронної техніки;
- д.т.н., проф. Климаша М.М., завідувача кафедри телекомунікацій про те, що в навчальному процесі кафедри телекомунікацій використано результати докторської дисертаційної роботи доц. Демидова І.В. «Синтез телекомунікаційних сервісних платформ національного масштабу», а саме:
 - модернізовано курси лекцій для студентів спеціальності 172 «Телекомунікації та радіотехніка» з дисциплін: «Розподілені сервісні системи та cloud-технології», «Інтернет речей та повсюдний комп'ютинг» у яких, відповідно, використано запропоновані у роботі методи та моделі підвищення ефективності оброблення користувачького навантаження у масштабованих телекомунікаційних сервісних платформах і методологію синтезу розподіленої сервісної системи за критеріями продуктивності та сервісної доступності;
 - створено курс лекцій та лабораторний практикум для студентів спеціальності 172 «Телекомунікації та радіотехніка» з дисципліни «Системне програмування інфокомунікацій», у якому використано методи оптимізації, зокрема розпаралелення програмного коду обробників навантаження для створення ефективних SaaS реалізацій в рамках побудови масштабованих телекомунікаційних сервісних платформ.

Члени комісії:

_____ /Б. М. Стрихалюк/
_____ /Л.Д. Озірковський/
_____ /М.М. Климаш/

ДОДАТОК Г. Список публікацій здобувача за темою дисертації та відомості про апробацію результатів дисертації

Наукові праці, в яких опубліковані основні наукові результати дисертації:

1. Demydov I. The Research of the Availability at Cloud Service Systems / I. Demydov, M. Klymash, Z. Kharkhalis, B. Strykhaliuk, P. Komada // Proceedings of SPIE: Photonics Applications in Astronomy, Communications, Industry, and High-Energy Physics Experiments, USA. – 2017. – Vol. 10445. – doi: 10.1117/12.2280885. (Scopus)

2. Demydov I. The Structural-Functional Synthesis of IoT Service Delivery Systems by Performance and Availability Criteria / Ivan Demydov, Yulia Klymash, Mykola Brych, Mykhailo Klymash // Internet of Things (IoT) and Engineering Applications (Canada). – May, 2017. – Vol. 2. – Issue 1. – P. 1-13. (МНБ)

3. Demydov I. Features of the cloud services implementation in the national network segment of Ukraine / I. Demydov, M. Klymash, M. Beshley, O. Shpur // Information and telecommunication science. K.: NTUU «KPI», 2016. - No.1. - P. 31-38. (МНБ)

4. Бешлей М. І. Розвиток методів передавання даних реального часу шляхом вдосконалення процесів пріоритезації потоків у маршрутизаторах / М. І. Бешлей, В. В. Червенець, І. В. Демидов, В. І. Романчук, О. М. Панченко // Системи обробки інформації. — 2016. — № 5. — С. 114-123. (МНБ)

5. Климаш М.М. Дослідження доступності у хмарних сервісних системах / М.М. Климаш, І.В. Демидов, Мохамед Мехді Ель Хатрі, Ю.Л. Дещинський // Радіоелектроніка та телекомунікації. Вісник Національного університету «Львівська політехніка». – Львів, 2016. – №849. – С. 218-229. (МНБ)

6. Демидов І.В. Моделювання процесів диференційованого обслуговування користувачів хмаринкових сервісних мережних систем / І. В. Демидов, Мухамед Мехді Ель Хатрі, Укаблі Юсеф // Наукові записки Українського науково-дослідного інституту зв'язку. – 2016. – №1(41). – с. 26-34. (Google Scholar)

7. Демидов І. В. Аналіз методів підвищення продуктивності телекомунікаційних мереж хмарних сервісних систем / І. В. Демидов, Мухамед Мехді Ель Хатрі, Укаблі Юсеф // Телекомунікаційні та інформаційні технології. – 2016. – №1. – С. 41-47. (Google Scholar)

8. Демидов І. В. Дослідження імовірнісних характеристик трафіку опорно-транспортної підсистеми мережі мобільного зв'язку / І. В. Демидов, М.М. Климаш, П. О. Гуськов, Мухамед Мехді Ель Хатрі // Наукові записки Українського науково-дослідного інституту зв'язку. – 2015. – №6(40). – С. 11-18. (Google Scholar)

9. Demydov I. V. The structural-functional synthesis of cloud service delivery platform after service availability and performance criteria / I. V. Demydov, B.M. Strykhalyuk, O. M. Shpur, Mohamed Mehdi El Hatri, Y. V. Klymash // Системи обробки інформації. — 2015. — № 1. — С. 144-159. (МНБ)

10. Демидов І. В. Моделювання процесів обслуговування потоків запитів у розподілених сервісних мережних архітектурах / І. В. Демидов, П. О. Гуськов, Мухамед Мехді Ель Хатрі // Наукові записки Українського науково-дослідного інституту зв'язку. – 2015. – №5(39). – С. 44-51. (Google Scholar)

11. Стрихалюк Б.М. Дослідження статистичних параметрів та характеристик інформаційних потоків в гетерогенних мережах / Б.М.Стрихалюк, І.В. Демидов, В.І. Романчук, М.І. Бешлей // Наукові записки УНДІЗ. – 2014. – №6(34). – С. 82-92. (Google Scholar)

12. Стрихалюк Б.М. Структурно-функціональна оптимізація процесів міграції віртуальних машин в розподілених дата-центрах / Б.М. Стрихалюк, З.В. Хархаліс, І.В. Демидов // Комп'ютерні технології друкарства: збірник наукових праць. - 2014. - №32. - С. 69-81. (Google Scholar)

13. Стрихалюк Б. Моделювання хмаринкової мережної системи у гіперболічних віртуальних координатах / Б. Стрихалюк, М. Климаш, І. Демидов // Комп'ютерні технології друкарства. - 2014. - № 32. - С. 3-19. (Google Scholar)

14. Красько О. В. Аналіз параметрів оптичного сигналу в повністю оптичній мережі з комутацією за довжинами хвиль / О. В. Красько,

І.В. Демидов, М.В. Брич // Вісн. Нац. ун-ту «Львів. політехніка». - 2014. - № 796. - С. 140-146. - Бібліогр.: 23 назв. - укр. (МНБ)

15. Klymash M. A Novel Approach of Optimum Multi-Criteria Vertical Handoff Algorithm for Heterogeneous Wireless Networks / M. Klymash, B. Stryhaliuk, I. Demydov, M. Beshley, M. Seliuchenko // International Journal of Engineering and Innovative Technology (IJEIT). – November 2014. – Volume 4, Issue 4(5). – P. 42-52. (МНБ)

16. Климаш М.М. Забезпечення якості обслуговування та оптимізація бізнес-процесів у розподілених системах на основі сервісно-орієнтованої архітектури / М.М. Климаш, І.В. Демидов, М.О. Селюченко, І.Д. Орлевич // Радіоелектроніка та телекомунікації. Вісник Національного університету «Львівська політехніка». – Львів, 2013. – №766. – С. 150-155. (МНБ)

17. Demydov I. Analysis of service workflows distribution and service delivery platform parameters / Ivan Demydov, Orest Lavriv, Bohdan Buhyl, Yuriy Dobush, Mykhailo Klymash // Int. J. Services, Economics and Management. -2013. - Vol. 5. - No. 4. - P. 280-290. (МНБ)

18. Demydov I. Enterprise Distributed Service Platform – Network Architecture and Topology Optimization / I. Demydov, M. Klymash, N. Kryvinska, C. Strauss // Int. J. Space-Based and Situated Computing. -2012. – Vol. 2. - № 1. - pp. 23-30. (МНБ)

19. Бугиль Б.А. Підвищення ефективності розподілу ресурсів телекомунікаційної мережі шляхом зміни маршрутів передавання даних [Електронний ресурс] / Б.А. Бугиль, М.М. Климаш, О.А. Лаврів, І.В. Демидов // Проблеми телекомунікацій. – 2012. – № 4 (9). – С. 32 - 44. – Режим доступу до журн.: http://pt.journal.kh.ua/2012/4/1/124_bugil_resource.pdf. (Google Scholar)

20. Klymash M.M. Analysis of service workflows distribution and SDP parameters / M.M. Klymash, I.V. Demydov, O.A. Lavriv, Yu.D. Dobush// Системи обробки інформації. – Харків, 2012. – Вип. 6 (104). – С. 103-107. (МНБ)

21. Добуш Ю.Д. Аналіз загроз передавання даних у системі «електронного урядування» та оцінка її ефективності / Ю.Д. Добуш, І.В.Демидов,

М.М. Климаш // Вісник Державного університету інформаційно-комунікаційних технологій. – К., 2012. - Т.10, №3. – С.29-36. (Google Scholar)

22. Добуш Ю.Д. Дослідження відкритих сервісних інтерфейсів Parlay в концепції «електронного урядування»/ Ю.Д. Добуш, І.В.Демидов, М.М. Климаш // Комп'ютерні технології друкарства: Зб. наук. пр. – Львів: Українська Академія Друкарства, 2012. – №28. – С. 170-186. (Google Scholar)

23. Самер Аввад. Дослідження обслуговування трафіку на транзитній мережі оператора мобільного зв'язку / Самер Аввад, М. М. Климаш, І.В. Демидов, Б.В. Коваль // Наукові записки Українського науково-дослідного інституту зв'язку. – 2011. – №1 (17). – С. 51-55. (Google Scholar)

24. Klymash M. Traffic routing in telecommunication nets and its diakoptics representation / M. Klymash, B. Strykhalyuk, M. Kaidan, I. Demydov // Computation Problems of Electrical Engineering. –Lviv, 2011. - №1(1). – P.15-19. (МНБ)

Наукові праці, які засвідчують апробацію матеріалів дисертації (форма участі):

25. Demydov I. The Synthesis Methodology of Scalable Telecommunication Service Platforms / Ivan Demydov, Zenoviy Kharkhalis // 2nd IEEE International Conference on Advanced Information and Communication Technologies-2017 (AICT-2017): Conference Proceedings. – Lviv, 2017. – P. 199-203. (МНБ, Scopus) (очна участь із доповіддю 05.07.2017 р.)

26. Demydov I. The Method of Improving the Availability at Cloud Service Systems / Ivan Demydov, Olga Shpur, Rakhman Lutfor, Yurii Deshchynskyi // Матеріали Міжнародної конференції з інформаційно-телекомунікаційних технологій та радіоелектроніки (УкрМіКо'2016/UkrMiCo'2016): Збірник тез. – К.: НТУУ «КПІ», 2016. – С. 446 - 448. (МНБ, Scopus) (очна участь із доповіддю 13.09.2016 р.)

27. Демидов І.В. Впровадження хмарних сервісних систем в національному мережному сегменті України / І.В. Демидов, О.М. Шпур // X Міжнародна науково-технічна конференція «Проблеми телекомунікацій» ПТ-

2016: Збірник матеріалів конференції (19-22 квітня 2016р. м. Київ) - К.: НТУУ «КПІ», 2016. – С. 342-344. (очна участь із доповіддю)

28. Demydov I. Concept of the Migrating Firewall to Scalable Cloud Networks / Ivan Demydov, Orest Lavriv, Zenoviy Kharkhalis, Mohamed Mehdi El Hatri // Сучасні проблеми радіоелектроніки, телекомунікацій, комп'ютерної інженерії TCSET'2016 : матеріали XIII Міжнародної конференції, 23-26 лютого 2016, Львів, Славське, Україна / Міністерство освіти і науки України, Національний університет «Львівська політехніка». - Львів : Видавництво Львівської політехніки, 2016. – С. 643-645. (МНБ, Scopus) (очна участь із доповіддю)

29. Demydov I. Dynamic Correction of Routing Metrics by Pervasive Structural Routing in the Scalable Distributed Service Networks / Ivan Demydov, Mohamed Mehdi El Hatri, Olga Shpur // Problems of Infocommunications Science and Technology (PIC S&T), 2015 Second International Scientific-Practical Conference, 13-15 Oct. 2015, Kharkiv, Ukraine. – P. 164-166. (МНБ, Scopus) (заочна участь, доповідь співавтора)

30. Demydov I.V. The features of cloud service delivery platform structural-functional synthesis / I.V. Demydov, M.M. Klymash, O.M. Shpur, Z.V.Kharkhalis // Міжнародна науково-технічна конференція «Сучасні інформаційно-телекомунікаційні технології»: матеріали науково-технічної конференції (17-20 листопада 2015 р. м.Київ), Т.3 – К: ДУТ. – 2015. – С. 19-21. (очна участь із доповіддю)

31. Demydov I. Mobility Management and Vertical Handover Decision in an Always Best Connected Heterogeneous Network / Ivan Demydov, Marian Seliuchenko, Mykola Beshley, Mykola Brych // Proceedings of XIIIth international conference «The experience of designing and application of CAD Systems in microelectronics» CADSM'2015, 24-27 February, Lviv-Poljana, Ukraine. – 2015. - P. 103-105. (МНБ, Scopus) (очна участь із доповіддю)

32. Strykhalyuk B. Synthesis of distributed service-oriented structures cloud networks is based on algorithm for determining hyperbolic virtual coordinates / Bogdan Strykhalyuk, Olga Shpur, Ivan Demydov, Yulia Klymash // Proceedings of

XIIIth international conference «The experience of designing and application of CAD Systems in microelectronics» CADSM'2015, 24-27 February, Lviv-Poljana, Ukraine. – 2015. - P. 231-235. (МНБ, Scopus) (очна участь із доповіддю)

33. Демидов І.В. Доступність композитних застосувань у сервісно-орієнтованих системах / І.В. Демидов, О.А. Лаврів, О.М. Шпур, М.О. Селюченко // Вимірювальна та обчислювальна техніка в технологічних процесах: матеріали XIII Міжнародної науково-технічної конференції (6-12 червня 2014 р. м. Одеса). – 2014. - с.119-121. (очна участь із доповіддю)

34. Demydov I. The Holographic Network Analysis / Ivan Demydov, Bohdan Strykhalyuk, Mykhailo Klymash // The 2014 IEEE International Black Sea Conference on Communications and Networking (IEEE BlackSeaCom 2014), Odessa, Ukraine – Chisinau, Moldova, May 27-30, 2014. – Chisinau:TUM, 2014. - pp. 66-68. - ACM ISBN: 978-1-4799-4067-7/14 (electronic). (МНБ, Scopus) (очна участь із доповіддю за кордоном)

35. Демидов І.В. Методи фіксації метаданих з'єднань глобальних мобільних телекомунікаційних мереж / І.В. Демидов, Ю.Д. Добуш // Всеукраїнська Науково-практична конференція «Сучасні проблеми телекомунікацій і підготовка фахівців в галузі телекомунікацій – 2013». Матеріали конференції 30 жовтня - 2 листопада 2013 р. – Львів, 2013. – С.167-170. (очна участь із доповіддю)

36. Добуш Ю.Д. Загрози поширенню даних в інфокомунікаційних системах «електронного урядування» / Ю.Д. Добуш, М.М. Климаш, І.В. Демидов // Материалы Международной научно-технической конференции «Информационные проблемы теории акустических, радиоэлектронных и телекоммуникационных систем» (IPST-2012): Тезисы докладов 25-29 сентября 2012 г. – АР Крым, Алушта, 2012. – С.165-166. (очна участь із доповіддю)

37. Dobush Yu. Approach to Secure Distributed Data Storing by Quasi-Random FAT Network Mapping / [Yuri Dobush, Ivan Demydov] // Матеріали Міжнародної науково-технічної конференції «Сучасні проблеми радіоелектроніки,

телекомунікацій, комп'ютерної інженерії» (21-24 лютого 2012 р.). – Львів – Славське, Україна, 2012. – Р. 335. (очна участь із доповіддю)

38. Demydov I. Methods of traffic load balancing in telecommunication networks / Ivan Demydov, Yasser Muayyad Al-Hayali // Науково-методична конференція „Сучасні проблеми телекомунікацій і підготовка фахівців в галузі телекомунікацій – 2012”. Матеріали конференції 1-4 листопада 2012 р. – Львів, 2012. – С.28-30. (очна участь із доповіддю)

39. Samer Awwad. Traffic Design in 4G Broadband Backbone Nets / Samer Awwad, Mykhailo Klymash, Ivan Demydov // Матеріали 11-ї Міжнародної науково-технічної конференції «Досвід розробки та застосування приладотехнологічних САПР в мікроелектроніці» (23-25 лютого 2011 року). – Львів – Поляна, Україна, 2011. – Р. 145 – 146. (МНБ, Scopus) (очна участь із доповіддю)

40. Добуш Ю.Д. Застосування широкосмугових бездротових мереж UMTS/3G для організації мереж моніторингу параметрів розподілених об'єктів / [Ю.Д. Добуш, І.В. Демидов] // Матеріали VII Міжнародної науково-технічної конференції «Сучасні інформаційно-комунікаційні технології» (COMINFO'2011-Livadia): Збірник тез. – К.: ДУІКТ, 2011. – С.154 -155. (заочна участь, доповідь співавтора)