

Інфраструктурні рішення та технології підвищення безпеки обробки даних при хмарних обчисленнях

Жанна Зеленцова¹, Надія Казакова²

1. Network Cloud Cube-2, Україна, м. Кременчук
e-mail: Zh.Andreeva@gmail.com

2. Одеський національний економічний університет,
Україна, м. Одеса, e-mail: kaz2003@ukr.net

Annotation: *Global Internet characterized by a constant increase in complexity and diversity, in this regard are discussed effective methods of network organization, generally involving convergent integration of networks into a single logical infrastructure. First of all, it concerns low-level network organization and deployment of complex multi-service networks and subnets service and global platforms with high-level services available to users. For these purposes, applies several productive approaches to unified computing. The authors propose a model of hyper-connected platform and service subnets.*

Keywords: converged infrastructure, convergence of network, telecommunication network, multi-service network, unified computing, service subnet, hyper-connected platform

Мережні сервіси були запропоновані в 80-х роках. Їхня архітектурна організація успадковується від симетричних багатопроцесорних систем, що обслуговуються на базі операційної системи UNIX. Ця операційна система лягла в основу організації міжмережевої взаємодії між окремими обчислювальними вузлами. Як результат, стало можливим будь-яку мережу розглядати як розподілену суперкомп'ютерну систему в комплексі з класичною багатопроцесорною обчислювальною архітектурою в мережному середовищі. Технологічний розв'язок завдання, що полягало в об'єднанні географічно розподілених вузлів у суперкомп'ютерну систему, було досягнуте, але довгий час вузьким місцем мережної реалізації була *неконтрольована мережна затримка* й можлива *втрата даних* при їхній передачі. Це було неприпустимо відносно розв'язку широкого кола завдань і забезпечення необхідного рівня надійності експлуатації та безпеки передавання даних при хмарних обчисленнях. Поставлені завдання були вирішені на основі таких основних підходів, як [1, 10, 11]:

– *гарантована доставка даних* на базі стека протоколів TCP/IP, який являє собою погоджене об'єднання двох типів мережних інтерфейсів – протоколу передачі даних TCP і протоколу «міжмережевого» взаємодії IP. На сьогодні це сімейство багато в чому замінило й повністю реалізує стек базової моделі OSI (ISO/IEC 7498-1), і пропонується до використання в якості стандарту;

– *проблема затримки* була вирішена за допомогою *уніфікованих обчислень*, які дозволили збільшити продуктивність процесорів, і лягли в основу Risc-процесорів. У результаті стало можливим забезпечення нанометричної затримки при передаванні даних у мережних середовищах.

Крім відзначеного, при розв'язанні поставлених завдань, стали використовуватися *fabric-орієнтовані методи* на основі протоколу P2P.

Надійне, високошвидкісне та безпечне об'єднання [2, 3] обчислювальних майданчиків на сьогоднішній день забезпечується протоколами *Fibre Chanel* і *Infiniband* з високою пропускну здатністю, а у рамках одного центру обробки даних (ЦОД) – *AMD Hypertransport* та *Intel Quickpath*. У результаті затримка при узгодженні географічно розподілених майданчиків ЦОД не перевищує нанометричного розміру. Саме із застосуванням цих технологічних підходів розгорнуті найбільші високопродуктивні глобальні захищені обчислювальні комплекси *Amazon Web Services*, *Windows Azure* і ряд інших сервісів. *Amazon Web Services* поєднує більш 450 тис. серверів, розмішених на всіх континентах. В них мережне розпізнавання забезпечується по IP-патерну 10.x.x.x та *Windows Azure* – 8 глобальних ЦОД [1, 4].

У доповіді показано, що в основі глобальних хмарних обчислювальних рішень використовуються конвергентний підхід та архітектура конвергентної обчислювальної інфраструктури. Цей напрямок відноситься до найбільш прогресивних розв'язків в області захищеної мережної організації. В його основу покладено *принцип конвергенції*, який припускає об'єднання принципово різних слабкозв'язаних обчислювальних ресурсів на основі подібності. Конвергентна інфраструктура має необхідну гнучкість для інтеграції нових технологічних розв'язків без необхідності зміни архітектури й може розглядатися в якості архітектурної основи організації складних мультисервісних мереж з хмарною організацією обчислень [4-7].

Виходячи зі сказаного, *метою завдання*, тема якого винесена в заголовок, є відображення технологічних розв'язків і фундаментальної бази з метою пошуку оптимальних напрямків розробки конвергентних мережних інфраструктур з хмарною організацією обчислень. У доповіді результати представлені у вигляді концептуальних мережних моделей, які дозволяють конкретизувати подальші етапи розробки мережних інфраструктур нового покоління з хмарною організацією обчислень.

Існуюча глобальна мережа є складною інфраструктурою. Вона відрізняється різноманіттям зв'язків та обчислювальних ресурсів. Розширення сервісної різноманітності, надання численних послуг у мережі Інтернет, поява окремих інтеграційних платформ, що поєднують мережі, ресурси й сервіси різних технологічних сегментів – усе це стимулює дослідників розглядати поняття глобальної мережі ширше, а саме – як *єдину мультисервісну інфраструктуру, погоджену на всіх рівнях мережної інтеграції*. Це має на увазі конвергентне об'єднання не тільки обчислювальних ресурсів в IP-мережах, але й первинних мереж електрозв'язку в єдине глобальне обчислювальне середовище. Очевидно, що для цих цілей буде потрібно адаптація окремих успадкованих сервісів та розробка нових сервісів з наскрізною функціональністю, яка

застосовується в розподілених сервісах, організованих по «безшовному» принципу [5-8].

Історичний розвиток наземних мереж електрозв'язку починається з початку ХХ століття. Уже наприкінці ХХ почалося розгортання мереж рухомого зв'язку (у т.ч. радіозв'язку) для організації мереж мобільної телефонії. На початку ХХІ століття до мереж зв'язку підключилися супутникові системи. У сукупності всі вони являють собою взаємопов'язані мережі з організацією вторинних мереж комутації для об'єднання сегментів різних стандартів.

Т.ч., взаємопов'язані телекомунікаційні мережі на сьогоднішній день представлені трьома великими сегментами – наземним, рухомих та супутниковим зв'язком. Очевидно, що основна проблема конвергентного об'єднання мереж, які в даний момент стали частиною єдиної світової мережної інфраструктури, полягає в їх раніше незалежному розвитку, а, відповідно – вони часто є технологічно непогодженими.

Другою значимою проблемою є підвищене навантаження в популярних споживчих сегментах мережі, що вимагає особливої уваги розроблювачів [9].

Виходячи зі сказаного, завданням доповіді є відображення знайдених методів та архітектурних розв'язків, які дозволяють забезпечити *гетерогенне високошвидкісне захищене підключення користувачів до світової телекомунікаційної системи на умові «безумовного» доступу до мережі*. У свою чергу, при наявності погодженої гетерогенної інфраструктури з реалізацією автоматичної маршрутизації трафіка – навантаження з високонавантажених сегментів мережі може бути перерозподілене на будь-який вільний сегмент без втрати цілісності та достовірності інформації. З цією метою в доповіді розглянуті й представлені кількісні та якісні характеристики мережі й перспективи їх розвитку. На основі представлених даних показано, що актуальним питанням, яке вимагає свого розв'язку, є питання не тільки *конвергенції обчислювальних ресурсів, підключених до мережі, але й конвергенції сервісів*.

Висновки

Розглянуті у доповіді інфраструктурні й технологічні рішення дозволяють спроекувати глобальні мережні середовища, які відповідають сучасним вимогам глобальної обчислювальної інфраструктури. У результаті запропонована модель hyper-connected-платформи.

Література

- [1] Зеленцова, Ж. Ю. Конвергенция глобальной сети как новый этап развития: Обзор инфраструктурных решений и технологий с целью нахождения решений для повышения безопасности обработки данных при облачных вычислениях / Ж. Ю. Зеленцова, Н. Ф. Казакова // Інформаційна безпека. – Луганськ : СНУ ім. В.Даля. – 2013. – №4(12). – С. 23-40. – ISSN 2224-9613.
- [2] Казакова, Н. Ф. Автоматизация процесса адаптации информационных систем до инцидентов информационной безопасности / Н. Ф. Казакова, С. В. Вавілов // Інформаційна безпека. – Луганськ : СНУ ім. В.Даля. – 2013. – №4(12). – С. 49-56. – ISSN 2224-9613.
- [3] Удосконалення принципів та методів інформаційного забезпечення, інформаційної та фінансово-економічної безпеки підприємств та організацій сфери економіки, бізнесу та фінансів [Звіт про НДР] : (проміжн.) / О. О. Скопа, Н. Ф. Казакова, О. В. Орлик, Ю. В. Щербина, А. О. Петров, С. Л. Волков, О. І. Мацків, О. Г. Єсіна, А. Ю. Вакула, О. О. Фразе-Фразенко, А. В. Мінін, О. О. Йона, С. В. Вавілов, К. Б. Айвазова // ОНЕУ ; кер. О. О. Скопа. – 0112U007713. – Одеса, 2013. – 236 с.
- [4] Казакова, Н. Ф. Исследование информационных потоков в комплексных системах защиты информации и метод расчета пропускной способности [Текст] / Н. Ф. Казакова, Е. О. Тискина, В. А. Хорошко // Інформаційна безпека. – 2009. – №2(2). – С. 105-115.
- [5] Казакова, Н. Ф. Анализ принципиальной задачи факторизации модели отказа предоставления услуги в сети NGN на уровне управления сетью [Текст] / Н. Ф. Казакова, В. И. Гура // Інформаційна безпека. – 2010. – №1(3). – С. 127-131.
- [6] Казакова, Н. Ф. Визначення показників для вирішення завдань прогностичного контролю мультисервісних телекомунікаційних мереж [Текст] / Н. Ф. Казакова, О. О. Скопа // Сучасний захист інформації. – 2010. – Спецвипуск (4). – С. 55-61.
- [7] Казакова, Н. Ф. Принципиальные задачи классификации и анализа моделей для программно-прогностического контроля мультисервисных телекоммуникационных сетей [Текст] / Н. Ф. Казакова, Н. М. Бильк, Г. А. Гундерич // Вісник національного університету кораблебудування. – 2010. – №2(431). – С. 125-132.
- [8] Казакова, Н. Ф. Застосування програмно реалізованого прогностичного контролю для вирішення практичних завдань забезпечення якості надання послуг у захищених інформаційних мережах [Текст] / Н. Ф. Казакова // Сучасна спеціальна техніка. – 2012. – №2(29). – С. 86-95.
- [9] Сиропятов, О. А. Проблема моделювання трафіку у мержах доступу до недовірених систем [Текст] / О. А. Сиропятов, Н. Ф. Казакова // Інформаційна безпека. – 2013. – № 1(9). – С. 185-189.
- [10] Луговой, А. В. Анализ архитектуры глобальных конвергентных решений и синтез агрегированной модели [Текст] / А. В. Луговой, Ж. Ю. Зеленцова // Вісник Кременчуцького національного університету імені Михайла Остроградського. – 2013. – № 3(80). – С. 84-91.
- [11] Зеленцова, Ж. Ю. Уязвимости конвергентной инфраструктуры и практические подходы к их устраниению [Текст] / Ж. Ю. Зеленцова, А. В. Луговой // Вісник Східноукраїнського національного університету імені Володимира Даля. – 2013. – №15(1)(204). – С. 122-129.