УДК 004.27; 004.32; 004.7

Н.Ф. Казакова,
кандидат технічних наук,
Ж.Ю. Зеленцова

КОНВЕРГЕНЦІЯ ГЛОБАЛЬНОЇ ІНФОРМАЦІЙНОЇ МЕРЕЖІ: ПИТАННЯ СИНТЕЗУ ІНФРАСТРУКТУРИ

Показано, що для організації глобальних мережевих обчислювальних рішень є доцільним використання конвергентного підходу та конвергентної обчислювальної інфраструктури. Такий напрям є найбільш прогресивним рішенням у галузі мережевої організації обчислень. Зазначено, що в його основі застосовується принцип конвергенції, який припускає об'єднання принципово різних слабко зв'язаних обчислювальних ресурсів на основі подібності.

Ключові слова: *конвергенція, глобальна інформаційна мережа, хмарні обчислення, інфраструктура, мережеві сервіси.*

Показано, что для организации глобальных сетевых вычислительных решений целесообразно использование конвергентного подхода и конвергентной вычислительной инфраструктуры. Отмечено, что такое направление является наиболее прогрессивным решением в области сетевой организации вычислений. Отмечено, что в его основе применяется принцип конвергенции, который предполагает объединение принципиально разных слабосвязанных вычислительных ресурсов на основе сходства.

Ключевые слова: *конвергенция, глобальная информационная сеть, облачные вычисления, инфраструктура, сетевые сервисы.*

For wide area network computing solutions it should be appropriate to apply a convergent approach and converged computing infrastructure. This direction is the most advanced solution in the field of network algorithms. It is grounded on the principle of convergence, that combines fundamentally different loosely coupled computing resources.

Keywords: *convergence, global information network, cloud computing, infrastructure, network services.*

На цей час глобальна мережа є складною інфраструктурою, що вирізняється розмаїттям зв'язків та обчислювальних ресурсів. Розширення сервісної різноманітності, надання численних послуг у мережі Інтернет, поява окремих інтеграційних платформ, що поєднують мережі, ресурси та 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 – *Cloud-структуру*. Очевидно, що для зазначених цілей необхідна адаптація окремих успадкованих сервісів та розробка нових з наскрізною функціональністю, організованих за "безшовним" принципом.

На сьогодні взаємопов'язані телекомунікаційні мережі представлені трьома великими сегментами – *наземним*, *мобільним* та *супутниковим*. Очевидно, що основна проблема конвергентного об'єднання мереж полягає в їх раніше незалежному розвитку і, відповідно, у часто технологічній непогодженості, що викликає порушення положень тріади CIA, тобто стандартної моделі інформаційної безпеки, яка за визначенням включає такі суттєві властивості, як *конфіденційність* (англ. *confidentiality, privacy*), *цілісність* (англ. *integrity*), *доступність* (англ. *availability*).

Другою проблемою є підвищене навантаження в споживчих сегментах глобальної мережі, що вимагає особливої уваги розробників. Таким чином, одним із завдань цього дослідження є пошук методів та архітектурних рішень, які дозволять забезпечити *гетерогенне високошвидкісне захищене підключення користувачів до світової телекомунікаційної системи за умови "безумовного" доступу до мережі*. У свою чергу, за наявності погодженої гетерогенної інфраструктури з реалізацією автоматичної маршрутизації трафіка навантаження з високонавантажених сегментів мережі може бути перерозподілене на будь-який вільний сегмент за умови забезпечення конфіденційності, цілісності та доступності інформації. Відповідно, метою статті є визначення перспектив зміни глобальної мережевої інфраструктури з метою виконання зазначених умов.

У загальноприйнятому розумінні глобальною мережею є Інтернет. Втім, функціонування Cloud-систем не обмежується зазначеною мережею. Існує достатня кількість мереж спеціального призначення, які інтегровані у Cloud-системи, але з певними односторонніми обмеженнями. Відомості про них та їх застосування у військовій сфері НАТО станом на початок XXI сторіччя наведено, наприклад, у [1] та ін.

У 2010 році компанія Cisco опублікувала звіт "Cisco® Visual Networking Index (VNI) Forecast (2010–2015)" [2]. У звіті визначено основні ознаки IP-мереж майбутнього. Так, передбачається, що для них буде характерною велика кількість підключених до Cloud-мережі обчислювальних пристроїв типу *Internet of Things* (IoT), або "Інтернет-пристроїв", які мають невелику продуктивність та слабку захищеність від несанкціонованих впливів. На момент складання звіту до 2015 року їх очікувалося 15 млрд одиниць. Крім того, у звіті прогнозується експонентне збільшення кількості мережевих користувачів – більше 3 млрд, що складе 40 % від прогнозованої кількості населення планети. Це також не поліпшить ситуації в сенсі підтримання необхідного рівня інформаційної безпеки у Cloud-мережі. Така ситуація призведе до того, що користувачі та пристрої будуть створювати множину унікальних включень до мережі. Відповідно, компанія Cisco передбачає, що дві проблеми будуть об'єднані в одну, котра відома дослідникам та інженерам як проблема гіперпідключеності (англ. *Hyper-Connected*). У [3] зазначено, що кількість очікуваних унікальних підключень в 2020 році досягне 212 млрд, а у [2] передбачається, що на кожного користувача буде припадати два-три мобільні пристрої.

Виходячи з наведеного вище, можна зробити висновок про те, що основне споживче навантаження буде продовжувати концентруватися в мобільному та IP-сегменті телекомунікаційного середовища, а це означає, що конвергентний підхід дозволить не тільки оптимально організувати роботу Cloud-мережі в певних сегментах, але й досягти рівномірного розподілу навантаження за рахунок надійних та захищених резервних каналів.

Сервіс-орієнтована методологія, яка планується застосовуватися для проектування користувацьких сервісів з обслуговуванням уніфікованих SLA-запитів (англ. *Service Level Agreement*), орієнтована на те, що якість послуг повинна відповідати поняттю "розмаїття" та забезпечувати вимоги тріади CIA. Якщо вище обговорювалося питання про об'єднання первинних телекомунікаційних мереж, то тут уже йдеться про високорівневі сервісні мережі з великим розмаїттям функцій, які можуть бути доступні користувачам, тобто постає проблема об'єднання сервісів. Поза сумнівом, поняття про Cloud-систему включає все розмаїття понять про обчислювальні ресурси (технічні та програмні), які входять до неї, засоби зв'язку та засоби забезпечення виконання умов тріади CIA, що, по суті, є їх повною конвергенцією.

Таким чином, виходячи з викладеного вище, з метою знаходження інфраструктурних рішень та технологій підвищення ефективності функціонування обчислювальних мереж на основі Cloud-технологій із забезпеченням розмаїття сервісів, включаючи сервіси з безпеки обробки даних в умовах тріади CIA, доцільно розглядати не тільки конвергенцію первинних мереж (наземного зв'язку, мобільного радіозв'язку та систем супутникового зв'язку), але й, як наслідок, – конвергенцію підключених обчислювальних ресурсів та конвергенцію сервісів так, як це відображено на рис. 1. Як видно з нього, очевидним є той факт, що для конвергенції сервісів у зоні користувачів необхідна розробка спеціального стандартизованого інтеграційного інтерфейсу.

Інтеграційні сервіси застосовуються з початку цього сторіччя. Технічні та технологічні рішення інтеграції необхідні не тільки в зоні користувацьких сервісів, а й на всіх рівнях ієрархії глобальної телекомунікаційної системи. Їх найбільш характерна особливість – гнучкість, яка дозволяє забезпечити безумовне підключення всіх видів сервісів до гетерогенних телекомунікаційних мереж. Такі мережі відомі з наукової та технічної літератури як гетерогенні мережі зв'язку типу HetNet (англ. *heterogeneous network)*. На цей час актуальність питання не втратила своєї вагомості. У взаємопов'язаних мережах потрібною буде також організація безумовного доступу до них користувачів за допомогою функції автоматичної маршрутизації трафіка з метою пошуку доступної мережі.

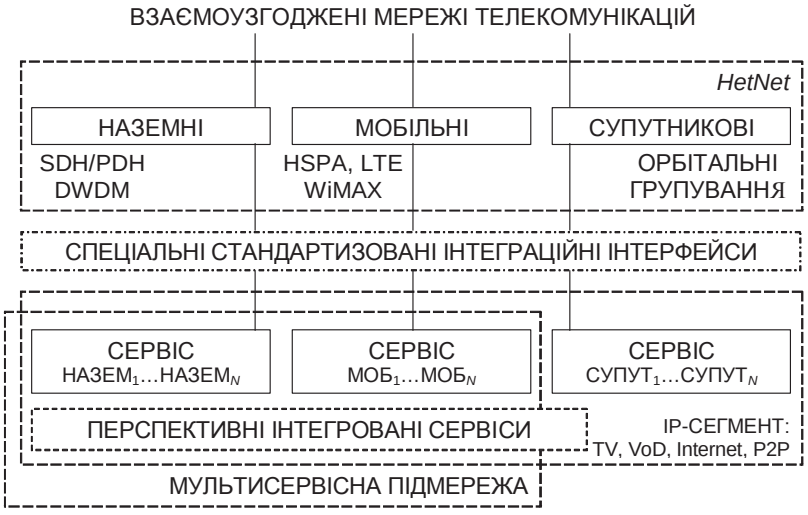

Рис. 1. Принцип конвергенції мереж, ресурсів та сервісів

З боку кінцевих користувачів, безумовно, є зручнішим використання інтеграційних сервісних платформ, які забезпечують одночасний безперервний захищений доступ до всіх сервісів у рамках єдиного інтерфейсу без необхідності повторної авторизації та ідентифікації в кожному сервісі (рис. 1). Такі можливості єдиної аутентифікації [4; 5] забезпечуються за допомогою технології єдиного доступу (англ.: *Single Sign-On* – SSO). Вона має на увазі сполучення процесів ідентифікації (ID) та аутентифікації (Authn) з єдиною точкою відмови. Технологія вже реалізується низкою виробників технічного та програмного оснащення для Cloud-систем (наприклад, *Vmware, Google, Pay Pal* [6]).

Наступною перспективною до впровадження сервісною інтеграційною платформою, що відповідає вимогам тріади CIA, є платформа Windows Azure, яка планується до використання у Cloud-системах. Це, по суті, є шина додатків *AppFabric*, яка становить Fabric-орієнтоване рішення, реалізоване для сервісів, у яких користувач може додатково отримати захищений доступ до користувацької шини пристроїв у зоні клієнтів, сервісної шини, шини додатків та шини даних [7].

Розвиток інтеграційних платформ у зоні користувачів, відповідно, припускає й розвиток складних сервісних функціональних підмереж, що функціонують у складі гетерогенних мереж та забезпечують доступ до наземних, мобільних та супутникових систем (рис. 1). На сьогодні розмаїття мережевих комунікацій з їх одночасною активною інтеграцією в мережу комерційних послуг та засобів державного управління збільшується по експоненті. Відповідно, *актуалізується питання організації захищених державних підмереж*, тобто – *державного Інтернету* [8]. У цьому сенсі низка експертів підкреслюють, що необхідною є чергова сервісна та функціональна сегментація IP-мереж (насамперед тих, які відповідають поняттям про Cloud-технології), що визначається розумінням споживачів різниці між державними, приватними та гібридними "хмарними" впровадженнями [9].

Що стосується характеристик підмереж, то наявні літературні першоджерела свідчать про те, що за версією Cisco глобальна мережа буде мати виражений мультимедійний характер. Так, вже на сьогодні обсяг розміщеної у Cloud-сховищах відеоінформації становить 5 млн людинороків (розмірність – за визначенням у [2]). До 2017 року медіа-трафік складатиме 69 % від усього обсягу споживчого Інтернет-трафіка. Практично 2/3 медіатрафіку до 2017 року буде забезпечуватися за рахунок мереж доставки контенту Content Delivery Network (CDN). Використання цифрового телебачення до 2017 року зросте в 5 разів [2]. У цілому прогнозується щорічне зростання споживчого трафіку, включаючи TV, Video on Demand (VoD), Інтернет та P2P, на 80–90 %, що потребує забезпечення відповідних кроків щодо захисту інформації.

У [2; 10; 11] показано, що з 2012 по 2017 рік очікується збільшення мобільного трафіку в 13 разів, насамперед за рахунок використання можливостей Інтернету. Також зросте швидкість наземного широкосмугового Інтернету до 28 Мбит/с. З цього приводу можна зазначити, що на практиці вже сьогодні модернізуються магістральні мережі і, відповідно, середньотарифна швидкість наближається до позначки 100 Мбіт/с.

Дослідники компанії Akamai звертають увагу, що найближчим часом буде актуальним питання про створення *інтеграційних hyper-connected-платформ*, які будуть здатні підтримувати велику кількість унікальних підключень за умови

надання послуг із забезпеченням вимог тріади CIA [12]. При цьому масове підключення пристроїв та користувачів передбачає вимогу великої кількості сервісів, які повинні забезпечити інтеграційні платформи.

Такі передумови розвитку ринку, як розвиток сервісних підмереж, з одного боку, відкривають перед розроблювачами величезні перспективи – зростає обсяг виробництва та реалізації продукції. Згідно з [13] світовий ринок конвергентної інфраструктури до 2017 року складе $402 млрд, а обсяг ринку Internet of Things – $8.9 трлн до 2020 року [3]. Обговорюючи перспективи розвитку мультисервісних підмереж, для початку варто визначити рамки структурних та технологічних проблем, які пов'язані з розгортанням розглянутих вище гетерогенних обчислювальних комплексів. Назвемо їх *Hyper-Connected Platforms (HCP),* тобто *платформи, що забезпечують підключення великої кількості користувачів, пристроїв та обробку великих обсягів даних* з урахуванням принципу вимог тріади CIA. Щодо HCP, то тут існує ціла низка архітектурних проблем базової інфраструктури [12; 14], вирішення яких є актуальним у сенсі питання, яке винесено в заголовок. Як показав аналіз, насамперед необхідним є приділення однакової уваги як логічним рішенням високого рівня, так і апаратним рішенням низького рівня. Необхідно пригадати, що Інтернет був розроблений як одна із версій пакетної радіомережі (мається на увазі – технологія передавання даних з комутацією пакетів). Звичайно, що на той час він не був розрахований на сучасні завдання та цілі.

Категорія проблем реалізації мережевих сервісів, що забезпечують безпечний та надійний доступ і доставку даних, в цілому зводиться до вирішення колізій при відправленні одного біта інформації та забезпечення зв'язку між двома кінцевими точками в рамках вимог тріади CIA [14]. Таким чином, згідно з тим же джерелом при розширенні функціональності сервісів проблему гіперпідключення необхідно обговорювати, починаючи саме із синтезу інфраструктури, яка повинна бути легкою у використанні для всіх користувачів та такою, для якої є можливою реалізація інтеграції будь-якого програмно-апаратного рішення. Практично йдеться про формат підключення *Plug&Play* (PnP), тобто про технологію швидкого підключення пристроїв, які можуть бути оснащені необхідними програмно-апаратними розширеннями, уже в самій глобальній мережі [14]. Виходячи з цього, проблема гіперпідключення повинна розглядатися на всіх рівнях мережної інфраструктури, а це, у свою чергу, при організації "швидкого" підключення IoT-пристроїв вимагає технологічних змін на рівні мереж зв'язку – наземних, мобільних, супутникових. Ще наприкінці минулого сторіччя комітет, створений за участю Microsoft, Honeywell та Intel (фірми-розробники стандарту Plug&Play), з метою швидкого підключення до глобальних мереж запропонували застосовувати стандартні міжмережеві протоколи, що було позитивно сприйнято світовою спільнотою. Таке рішення, як показав час, виявилося неефективним, а проблеми, які виникли, не розв'язані й до сьогодні. Насамперед основна невирішена проблема пов'язана з організацією "індентифікованої" доставки, що, у свою чергу, пов'язано з обмеженими можливостями DNS-ідентифікації та загальноприйнятою організацією доступу до вузлів зв'язку. На першому етапі розвитку інформаційних мереж зазначена проблема вирішувалася на основі MAC-адрес мережевих карт, потім – за допомогою протоколу IP, а на сьогодні – на основі IPv6. Сучасний підхід також є недосконалим, позаяк гарантує роботу пристроїв в рамках вимог

тріади CIA, поки не буде змінена адреса маршрутизатора та, відповідно, MAC- або IP-адреса [14].

Вирішення проблеми, яке вже знайшло своє відображення на практиці, базується на використанні динамічних IP-адрес, що застосовуються телекомунікаційними компаніями для надання доступу користувачам до мережевих послуг. Втім, у [14] стверджується, що таке вирішення є тимчасовим, яке не в повній мірі відповідає вимогам тріади CIA, а також вимогам щодо швидкості обміну даними у рамках Cloud-системи, а лише є орієнтованим на особливості діючої інфраструктури і, таким чином, для гіперпідключень необхідним є пошук більш ефективного рішення. Слід зазначити, що сьогодні більшість домашніх мереж мають одну публічну IP-адресу, а самі пристрої "ховаються" за NAT (англ. *Network Address Translation – перетворення мережевих адрес*), тобто не досягають DNS-провайдера і фактично можуть бути загублені в мережі, що прямо призводить до порушень вимог тріади CIA [14].

Існує ще низка проблем безпечного доступу та доставки повідомлень, які потребують свого вирішення та повинні бути розв'язані в рамках синтезу глобальної конвергентної інфраструктури. Так, існує невирішена проблема реплікації MAC-адрес пристроїв, які можуть бути оснащені засобами швидкого доступу до Cloud-систем. Її суть полягає в існуванні "сірих" реплікацій зазначених пристроїв. Наступна проблема – проблема "ідентифікованої" доставки, яка виникла внаслідок появи анонімних мереж, що активно розширюються. Виникнення таких мереж викликане бажанням окремих груп користувачів анонімізувати свій трафік в мережі. Таким чином, *проблема гарантованої доставки* повинна вирішуватися із застосуванням гібридних методів, що дозволяють сховати особисті дані користувачів та одночасно організувати надійну доставку достовірних даних на всі їх пристрої.

Доступ через Wi-Fi-мережі. Блокування доступу через навантаження. Активне використання безпровідного трафіка Wi-Fi при організації доступу становить проблему, пов'язану, насамперед, із забезпеченням вимог тріади CIA, що потребує управління обліковими записами на кожному кроці на шляху передавання даних. Будь-яке невиконання вимог тріади CIA призведе до блокування точок доступу. Вирішення цього завдання поки не існує: для мереж властива наявність паразитного (анонімного) трафіку, який передається по телекомунікаційних мережах і не ідентифікується. Проблема зростає з кожним роком і, таким чином, її вирішення, так як і вирішення її окремих складових є актуальним й потребує подальших досліджень.

Проблема ідентифікації та облікових записів повинна розглядатися як завдання більш високого інфраструктурного рівня зі зміною логіки ідентифікації, наприклад, як частина функціональності технології Single Sign-On [15]. У цьому сенсі пропонується просте рішення, яке вже частково використовується в окремих платформах. Так, проблема гіперпідключеності може бути звужена, якщо як підключення розглядати підключення до мережі одного користувача та усього кола пов'язаних з ним мережевих пристроїв. У такому випадку інформація може бути доставлена на будь-який активний пристрій користувача, а після реплікування – на всі зв'язані з ним пристрої.

Подібне вирішення, як зазначалося вище, пропонує до реалізації платформа Apple ICloud, яка дозволяє через інтеграційний інтерфейс синхронізувати всі

Apple-пристрої користувача та забезпечує доставку медіа-інформації (поки що) за допомогою "хмарного" сервісу.

Проблема гіперпідключеності припускає можливе блокування доступу в результаті зростаючого навантаження на Інтернет-з'єднання, тобто завдання управління IoT-пристроями вимагає зміни логіки інфраструктури, а також узгодження політик постачальників по "безшовному" принципу на шляху передавання даних. Особливо це актуально для мереж Wi-Fi, які обслуговують підключені пристрої, виставляючи пріоритет стосовно відстані пристрою до антени. Таким чином, у Wi-Fi-мережах близького радіозв'язку повинна бути реалізована послуга пошуку доступної мережі з найкращими параметрами доступу з автоматичною установкою з'єднання та маршрутизацією на альтернативні мережі.

У цілому, для вирішення завдання потрібна зміна принципів спільної взаємодії відповідної технічної, організаційної, правової та нормативної бази з метою забезпечення безперешкодного підключення, тобто PnP, до інфраструктури будь-якого користувача та будь-якого пристрою, а також підключення будь-якого надійного програмного додатка при проблемі гіперпідключеності. Для цього потрібне комплексне вирішення низки фундаментальних завдань політичного, правового та інженерного характеру.

Первинні мережі. На низькому рівні мережі електрозв'язку представлені первинними мережами. Як правило, у їх складі розглядаються безпосередньо лінії зв'язку, підсилювальне та каналоутворююче устаткування. До вторинних мереж зі всіма комутаційними потужностями належить світова публічна мережа телефонного користування PTSN (англ. *Public Switched Telephone Network*). В Україні вона названа телефонною мережею загального користування (ТМЗК). За допомогою неї надається переважна більшість мережевих послуг, у тому числі Інтернет та мобільний зв'язок.

Проведемо аналіз проблемних питань для наземних мереж. Так, на думку експертів, враховуючи нові вимоги до мережевих послуг, структура ТМЗК є застарілою [14]. Втім, саме ця інфраструктура є найбільшою мережею зв'язку у світі та основним постачальником послуг електрозв'язку.

Засоби електрозв'язку організовано з використанням двох технологій – передачі *даних з комутацією пакетів* і *з комутацією каналів*. Технологія передачі даних з комутацією каналів є перевіреним надійним розв'язком для доставки, насамперед, голосової інформації при високій економічній ефективності та низьких ризиках у сенсі забезпечення вимог тріади CIA, враховуючи наявність великої кількості резервних каналів [16]. Цими каналами може підключатися Gigabyte Ethernet.

Для подальшого розуміння суті питання наведемо значущі характеристики стандартів, які використовуються в сучасних мережах та на основі яких можлива конвергенція мереж, ресурсів та сервісів.

– SDH/PDH, включаючи SDH (англ. *Synchronous Digital Hierarchy)*, – традиційна синхронна цифрова ієрархія, яка має модульну структуру та передає ущільнений сигнал з підвищенням базової швидкості, і PDH (*англ.: Plesiochronous Digital Hierarchy*) – плезиохронна цифрова ієрархія, яка дозволяє мультиплексування потоків у первинних мережах на основі імпульсно-кодової модуляції та значно збільшує пропускну здатність, що є основним вузьким міс-

цем технології комутації каналів, зокрема SDH. Технічне обладнання – гібридні оптико-коаксіальні телевізійні мережі та стандартне телекомунікаційне устаткування.

– DWDM – високошвидкісна транспортна волоконно-оптична мережа (англ. *Dense Wavelength Division Multiplexing*) забезпечує спектральне ущільнення каналів та дозволяє організувати багатоканальну передачу даних за двома напрямами. Цей стандарт передбачає надання всіх видів телекомунікаційних послуг: MPLS, Frame Relay, TDM, SDH, IP, ATM включно. Фактично він є окремим напрямом канальної комутації, який спеціально створений для розгортання мереж із точки зору забезпечення надійності та захищеності від сторонніх впливів, врахо-вуючи вимоги тріади CIA. Всі зазначені технології, які входять до стандарту, за-безпечують практично абсолютний захист підмереж при використанні кільцевої топології. Технічне обладнання – використання будь-яких технічних систем з пропускною здатністю від 320 до 2560 Гбіт/с.

Для технології канальної комутації розроблено низку інтерфейсів цифрової телефонії (наприклад, EX – Європейський Союз, TX – Північна Америка, JX – Японія). Їх основа – стандарт PDH. Зазначена технологія забезпечує як мультиплексування сигналу, так і роздільне шифрування кожного з каналів, даючи можливість розгортання захищених телефонних мереж. Крім того, як вже зазначалося, резервними каналами можливе підключення 10 Gigabit Ethernet: цим вирішується актуальне питання високошвидкісного широкосму-гового захищеного передавання даних за схемою "трафік"–"трафік-інтернет"–"трафік".

Ідея реорганізації засобів електрозв'язку виключно за допомогою технологій із пакетною комутацією та з використанням ідей мереж NGN (*англ. Next Generation Network*), що була на початку поточного сторіччя, на практиці виявилася неможливою. Завадою до широкої перебудови став той факт, що мережі NGN становлять мультисервісні "пакетні" мережі з різними функціональними сегментами, які часто є несумісними між собою, особливо в сенсі забезпечення інформаційної безпеки та захисту даних. Водночас застосування пакетної комутації призвело до розгортання функціональних сервісних підмереж та дозволило реалізувати принципово нові особливо актуальні види сервісів, наприклад, мультимедіа та надання послуг VoIP (*англ. Voice over IP*), Інтернет, VPN, IPTV, Vod та ін., а також розгортання мереж WAN (англ. *Wide Area Network* – глобальна комп'ютерна мережа).

Те, що стосується технологій з пакетною комутацією та ідей NGN, надає достатньо фактів для того, щоб зробити висновок про існування теоретичних та практичних першопричин, які дозволяють вирішити проблему об'єднання неоднорідних мереж у Cloud-систему з врахування вимог тріади CIA.

Технології на базі використання канальної комутації, у свою чергу, забезпечують ощадливі та надійні рішення для магістральних мереж, які не в змозі забезпечити пакетна комутація. Втім їх істотним недоліком є відмова в обслуговуванні, викликана перевантаженням мультиплексорів, що значно знижує їх роль з точки зору застосування у Cloud-системах. Водночас у локальних та зонових мережах, при підключенні до Cloud-систем, активно використовується одночасне існування як NGN, так і ліній з "канальними" інтерфейсами EX/TX. При такій організації передавання даних інформаційна безпека забезпечується методами протоколів MPLS, Frame Relay, TDM, SDH, IP, ATM.

Системи супутникового зв'язку. Супутникові системи зв'язку, як правило, відносять до первинних мереж, окремо виділяючи лише великі магістральні напрямки (стволи), які розраховані на передачу великих обсягів даних. Вони, у сенсі їх використання як виду магістрального зв'язку, на сьогодні поступилися наземним волоконно-оптичним мережам. Втім, як зазначається у [17], вони будуть затребувані вже до 2020 року, зважаючи на зростання обсягів даних у глобальних мережах, що обслуговуватимуть глобальні Cloud-системи.

До існуючих магістральних супутникових мереж СНД, які передбачаються до використання з метою захищеного доступу до Cloud-систем, належать уже прийняті в експлуатацію та включені до складу мереж російські супутникові комплекси "Ямал-300" та "Ямал-402", супутникова система "Ямал-401", що вводиться в експлуатацію наприкінці 2014 року, а також космічні комплекси ВАТ "Газпром космічні системи". Передбачається, що всі зазначені системи зможуть обслуговувати російських та закордонних споживачів при організації захищеного доступу до Cloud-систем [18].

Крім зазначених супутникових комплексів, слід відзначити супутники системи зв'язку "Експрес" нового покоління російської державної компанії "Космічний зв'язок". Два супутники цієї системи вже запущено в 2014 році. Створюване орбітальне угруповання буде забезпечувати повне покриття та захищений доступ до хмарних сервісів всіх країн євроазійського континенту [19].

Для окремих споживачів специфічних хмарних сервісів та для їх моніторингу передбачено та розпочато побудову відомчих мереж, які засновані на базі малих орбітальних комплексів з малою пропускною здатністю – VSAT (*англ. Very Small Aperture Terminal*). Захищений та конфіденційний доступ до мережі організовується на базі використання малопотужних антен та приймально-передавального технічного обладнання, які здатні забезпечити передавання даних зі швидкістю не більше 2048 кбіт/с. Цього достатньо для збору специфічних даних та управління системами захисту та безпеки інформації.

Для надання послуг Інтернет супутниковий зв'язок передбачає виділення лише асинхронних каналів. З урахуванням вимог щодо захищеного передавання даних між споживачем та Cloud-системою вимагається організація двох каналів підключення: для вхідного та вихідного трафіка. Це вимагає відповідних програмно-технічних рішень щодо задоволення вимог тріади CIA. За швидкістю підключення ця технологія, незважаючи на достатню складність настроювання, може забезпечити високошвидкісне підключення за низьких витрат. Супутниковий канал може бути задіяний одночасно декількома сотнями користувачів, що є актуальним у регіонах зі слабкорозвиненою мережевою інфраструктурою наземного та мобільного зв'язку. Це дозволяє включити розглядувану технологію до загальної структури конвергенції різнорідних мереж та застосовувати у віддалених регіонах та на морських територіях. На цей час технологія активно використовується для надання послуг цифрового радіомовлення DVB, що дозволяє організувати приймання супутникового телебачення та забезпечувати доступ до глобальних мереж.

Мобільні мережі. За прогнозами, які є в багатьох аналітичних статтях (наприклад у [2]), кількість мобільних сервісів і користувачів інтенсивно зростає. Як правило, на кожного користувача в середньому припадає 2–3 мобільних пристрої. Цей напрям удосконалення мереж радіозв'язку має більшу перспективу

глобального розвитку за рахунок того, що мобільні простої при підключенні проходять лише перевірку облікових записів користувачів у відповідній мережі. Однак при цьому за умови спрощення процедури реєстрації збільшується вірогідність несанкціонованого доступу до конфіденційної інформації, що потребує відповідних удосконалень як з точки зору розробки програмного забезпечення, так і програмно-технічного устаткування.

Базові мобільні станції попередніх поколінь підключались і сьогодні підключаються переважно до магістралей ТМЗК. Слід враховувати, що основні мобільні мережі розгорнуті на базі технології HSPA (англ. *High Speed Packet Access*). У мережах 4G передбачено, що магістральна передача організовується без організації доступу через ТМЗК. При цьому швидкість доступу становить 100 Мбіт/с для мобільних об'єктів і не менше ніж 1 Гбіт/с для стаціонарних користувачів.

На поточний момент активно впроваджуються високошвидкісні мобільні мережі наступного покоління LTE-advanced або 3GPP Реліз 10 (*англ. Long Term Evolution*). Стандарт LTE, офіційно віднесений до 4G, передбачає багатоантенну передачу даних, підтримує ретрансляцію, передбачає конвергенцію спектра та розширення смуги частот, а також дозволяє розвертати гетерогенні мережі HetNet [20]. До стандарту 4G також належить технологія Mobile Wimax (Release 2) (англ. *Worldwide Interoperability for Microwave Access – WiMAX*). WiMAX заснована на методах обробки широкого спектра частот. Вона використовується для організації високошвидкісних мереж Wi-Fi доступу, а також дозволяє організовувати безумовне передавання даних до точок доступу до Cloud-систем, які не мають певного географічного положення. WiMAX часто застосовується в промислових мережах для організації віддаленого моніторингу об'єктів у системах SCADA (англ. *Supervisory Control and Data Acquisition – SCADA*) та має технологічні можливості для використання як у магістральних каналах, так і в зонових та локальних мережах. Відповідно, технологія WiMAX, з точки зору вирішення завдань, які становлять предмет дослідження, є найбільш доцільною для подальшого аналізу.

Що стосується організації маршрутизації та доступу до базової станції, то при використанні технології WiMAX мобільні станції отримують доступ до Wi-Fi за принципом "змагання": перевага віддається мобільним станціям, які найбільш близько розташовані до базової станції. Для забезпечення рівноправного доступу у WiMAX реалізована конвергенція спектра та низка алгоритмів з організацією взаємодії з канальним рівнем мобільних пристроїв. При підключенні для будь-якої станції у точці доступу створюється виділений слот, який є недоступним для інших користувачів, що відповідає вимогам тріади CIA.

Що ж стосується мереж стандарту 802.16, у них MAC використовує алгоритм планування: будь-якій користувацькій станції потрібно підключитися до точки доступу, де для неї буде створено виділений слот, недоступний іншим користувачам.

Вторинні мережі HetNet: питання комутації та крос-з'єднання при захищеному доступі до Cloud-систем. Поряд з питанням конвергентного об'єднання гетерогенних мереж HetNet постає проблема апаратного узгодження мереж різного типу при підключенні до Cloud-систем. При цьому мається на увазі конвергенція наземних, рухомих та супутникових систем, "канальних" та

“пакетних” методів передавання даних, які функціонують у рамках єдиної мережі наземного електрозв’язку та мають різні системи організації безпечного передавання даних.

При конвергентному об’єднанні узгодження окремих “канальних” та “пакетних” вторинних мереж може проводитися на основі як статичної, так і динамічної комутації. При цьому слід враховувати, що статична комутація використовується для узгодження мереж одного типу, а динамічна – застосовується для узгодження мереж різних типів. Для прикладу зауважимо, що на сьогодні вже поєднуються мережі E1/SIP(NGN), а також мережі з канальною комутацією різних стандартів – EX/TX.

До нових рішень апаратного узгодження мереж належать *гнучкі гібридні мультиплексори*. Будь-які мультиплексори є частковим випадком комутаторів і призначені для побудови вузлів крос-з’єднання з наданням інтегрованих послуг “голос+дані”. Гнучкі гібридні мультиплексори широко застосовуються для розгортання захищених високонадійних мереж спеціального зв’язку – мереж залізничного транспорту, нафто- та газодобувної промисловості, підприємств електроенергетичного комплексу, військового, космічного, урядового зв’язку й управління та ін. Для підвищення їх швидкодії застосовується технологія мультиплексуючих шин Multiplex Bus. Архітектура уніфікованих інтерфейсів мережевих шин, що поєднують мультисервісні мережі, реалізується у двох нових технологіях. В [21, 22] наведено дані про цілу низку “Crossbar Switch”-рішень для створення гнучких мережевих розв’язків щодо високопродуктивних “мереж на чипі” (англ.: “*On a Chip*” – NoC), які вже широко застосовуються в кластерних системах. Мережі на чипі NoC і Crossbar Switch тільки починають впроваджуватися в кластерних системах, перебуваючи на етапі розробки й тестування. На цей час як їх попередники широко використовуються шини, які добре зарекомендували себе, але є технологічно застарілими з точки зору відповідності тріаді CIA: AMD Hypertransport та Intel Quickpath.

Висновок

Показано, що для організації глобальних мережевих обчислювальних рішень є доцільним використання конвергентного підходу та конвергентної обчислювальної інфраструктури. Цей напрям на сьогодні належить до найбільш прогресивних рішень в області мережевої організації обчислень. В його основу покладено принцип конвергенції, що припускає об’єднання принципово різних слабкозв’язаних обчислювальних ресурсів на основі подібності. Конвергентна інфраструктура має необхідну гнучкість для інтеграції нових технологічних рішень без необхідності зміни архітектури та розглядається як архітектурна основа організації складних мультисервісних мереж. При цьому ресурси можуть бути оперативно надані та звільнені з мінімальними експлуатаційними витратами та звертаннями до провайдера. Споживачі хмарних обчислень можуть значно зменшити витрати на інфраструктуру інформаційних технологій (у короткостроковому та середньостроковому планах) і гнучко реагувати на зміни обчислювальних потреб, використовуючи властивості *обчислювальної еластичності* хмарних послуг.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Government Network Management Profile (GNMP) [Текст] / Washington : U.S. Government Printing Office, FIPS PUB 179. U.S. Department of Commerce, National Institute of Standards and Technology, November 1992.

2. Global Internet Traffic Projected to Quadruple by 2015. Press Release. Cisco. 2011 [Електронний ресурс]. – Режим доступу \www/ URL : http : // newsroom.cisco.com/press-release-content?type=webcontent&articleId= 324003. – Заголовок з екрану, доступ вільний, 26.09.2013.

3. Internet of things : $8.9 trillion market in 2020, 212 billion connected things. ZDNet. October 3, 2013 [Електронний ресурс]. – Режим доступу \www/ URL : http : // www.zdnet.com/internet-of-things-8-9-trillion-market-in-2020-212-billion-connected-things-7000021516/. – Заголовок з екрану, доступ вільний, 12.12.2013.

4. *Казакова Н.Ф.* Дослідження та застосування в системах захисту інформації кореляційного критерію подібності графічних структур [Текст] / Н.Ф. Казакова, О.О. Фразе-Фразенко // Системи обробки інформації. – 2014. – № 2(118). – С. 246. – ISSN 1681-7710.

5. *Казакова Н.Ф.* Синтез методу виділення контурів у системах ідентифікації на основі усереднення перепадів яскравості [Текст] / Н. Ф. Казакова, О.О. Фразе-Фразенко // Інформаційна безпека. – 2013. – № 2(10). – С. 48-57. – ISSN 2224-9613.

6. *Wang R.* Signing me onto your accounts through facebook and google : A traffic-guided security study of commercially deployed single-sign-on web services [Текст] / R. Wang, S. Chen, X. F. Wang // Security and Privacy (SP), 2012 IEEE Symposium on. – IEEE, 2012. – С. 365–379.

7. *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.

8. *Куликов В.В* РФ появится защищенный государственный интернет [Електронний ресурс] // Портал : RG.RU – Российская Газета. Режим доступу \www/ URL : http : // www.rg.ru/2013/10/27/internet-site.html. Заголовок з екрану, доступ вільний, 28.10.2013.

9. *Florentine Sh., Olavsrud Th.* Forecast for Cloud Computing, CIO, December 2013 [Електронний ресурс] // Портал : cio.com. Режим доступу \www/ URL : http : // www.cio.com/article/745155/2014_Forecast_for_Cloud_Computing. – Заголовок з екрану, доступ вільний, 18.03.2014.

10. *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. – 2013. – № 4(12). – С. 23–40. – ISSN 2224-9613.

11. *Зеленцова Ж.* Інфраструктурні рішення та технології підвищення безпеки обробки даних при хмарних обчисленнях [Текст] / Ж. Зеленцова, Н. Казакова // Захист інформації і безпека інформаційних систем : ІІІ міжнар. наук.-техн.-конф., 5-6 червня 2014 р. : матер. конф. НУ –Львівська політехніка. м. Львів. – С. 58–59.

12. The Hyperconnected World : A New Era of Opportunity, White Paper, Akamai [Електронний ресурс] // Портал : akamai.com. Режим доступу \www/ URL : http : // www.akamai.com/dl/akamai/hyperconnected_world.pdf. Заголовок з екрану, доступ вільний, 13.12.2013.

13. *Vellante D.* Converged Infrastructure Takes the Market by Storm, Wikibon, Aug 2012 [Електронний ресурс] // Портал : wikibon. org. Режим доступу \www/ URL : http : // wikibon.org/wiki/v/Converged_Infrastructure_Takes_the_ Market_by_Storm. – Заголовок з екрану, доступ вільний, 23.09.2012.

14. *Frankston B.* The Internet : Missing the Light, CircleID Internet Infrastructure, Jul 2013 [Електронний ресурс] // Портал : без назви. Режим доступу \www/ URL : http : // frankston.com/public/?n=CILight. – Заголовок з екрану, доступ вільний, 18.09.2013.

15. Single Sign-On [Електронний ресурс] // Портал : OneLogin. Режим доступу \www/ URL : http : // www.onelogin.com/product/single-sign-on/. – Заголовок з екрану, доступ вільний, 18.09.2013.

16. *Казакова Н.Ф.* Аспекти надійної роботи автоматичних систем з послідовно-паралельним з'єднанням резервуючих елементів [Текст] / Н.Ф. Казакова // Вісник національного університету "Львівська політехніка". – 2012. – № 738. – С. 235–245. – ISSN 0321-0499.

17. *Анпилогов В.Р.* Спутниковые системы связи : современное состояние и тенденции развития в мире и в России [Електронний ресурс] // Портал : vsat-tel. Режим доступу \www/ URL : http : // vsat-tel.ru/library/art_32.htm. – Заголовок з екрану, доступ вільний, 15.07.2014.

18. *Севастьянов Д.Н.* Российский рынок спутниковой связи ждут перемены [Текст] / Д.Н. Севастьянов // Электросвязь. – 2013. – № 12 [Електронний ресурс] // Портал : gazprom.

Режим доступу \www/ URL : http : www.gazprom-spacesystems.ru/ru/news/ publications/ index.php?ELEMENT_ID=2958. – Заголовок з екрану, доступ вільний, 21.01.2014.

19. В помощь клиентам. Зоны покрытия действующих спутников [Електронний ресурс] // Портал : Федеральное государственное унитарное предприятие. – Режим доступу \www/ URL : http : // www.rscc.ru/customer/87/200/. – Заголовок з екрану, доступ вільний, 28.12.2013.

20. 4G : Аналитический обзор Ericsson [Електронний ресурс] // Портал : ericsson. Режим доступу \www/ URL : http : // www.ericsson.com/res/site_RU/ docs/wp-lte-4g.pdf. – Заголовок з екрану, доступ вільний, 22.04.2011.

21. *Lee K.A* distributed crossbar switch scheduler for on-chip networks [Текст] / K. Lee, S.J. Lee, H.J. Yoo // Proceedings of the IEEE 2003 : Custom Integrated Circuits Conference. – IEEE, 2003. – С. 671–674.

22. *Nomura K.* et al. Novel design of three-dimensional crossbar for future network on chip based on post-silicon devices [Текст] // 1st International Conference on "NanoNet'06" : Nano-Networks and Workshops, 2006. – IEEE, 2006. – С. 1–5.

Отримано 14.05.2014