УДК 004.27; 004.32; 004.7

О.О. Скопа,
доктор технічних наук, професор,
Н.Ф. Казакова,
кандидат технічних наук, доцент,
Ж.Ю. Зеленцова

КОНВЕРГЕНЦІЯ ГЛОБАЛЬНОЇ ІНФОРМАЦІЙНОЇ МЕРЕЖІ: ПИТАННЯ УПРАВЛІННЯ ГЕТЕРОГЕННИМИ СЕРЕДОВИЩАМИ З УРАХУВАННЯМ ВИМОГ ТРІАДИ CIA

Розглянуто питання конвергенції глобальної інформаційної мережі. Приділено увагу питанням управління гетерогенними середовищами. Враховано проблеми забезпечення інформаційної безпеки у відкритих системах. Дано поняття про Cloud-структури. Запропоновано архітектурну модель обчислювального середовища, яке програмно конфігурується. Показано її принципову відмінність. Зазначено, що запропонована модель може бути застосована при проектуванні розподілених обчислювальних систем.

Ключові слова: *конвергенція, інформаційна мережа, гетерогенні мережі, конфіденційність, цілісність, доступність, управління, контролінг, програмна зміна конфігурації.*

Рассмотрены вопросы конвергенции глобальной информационной сети. Уделено внимание вопросам управления гетерогенными средами. Учтены проблемы обеспечения информационной безопасности в открытых системах. Дано понятие о Cloud-структуре. Предложена архитектурная модель вычислительной среды, которая программно конфигурируется. Показано ее принципиальное отличие. Отмечено, что предлагаемая модель может быть применена при проектировании распределенных вычислительных систем.

Ключевые слова: *конвергенция, информационная сеть, гетерогенные сети, конфиденциальность, целостность, доступность, управление, контроллинг, программное изменение конфигурации.*

The questions of convergence of the global information network are considered. An attention to the management of heterogeneous environments is paid. Several problems of information security in open systems are stated. An understanding of the Cloud-structure is given. Architectural model of a computing environment that is configured programmatically is proposed. Its fundamental difference is shown. It is observed that the proposed model can be applied to the design of distributed computing systems.

Keywords: *convergence, information network, heterogeneous network, confidentiality, integrity, availability, management, controlling, software configuration change.*

Будь-яка складна інфраструктура вимагає впровадження функцій управління, контролінгу та інформаційної безпеки. Розглянемо процедуру вирішення питання управління гетерогенними середовищами (мережами) з урахуванням вимог 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*) – CIA [1; 2]. У випадку, який розглядається, під *контролінгом* будемо розуміти комплексну систему підтримки управління, спрямовану на координацію взаємодії систем менеджменту та контролю їх ефективності. При експлуатації гетерогенних мереж контролінг забезпечує інформаційно-аналітичну підтримку процесів прийняття рішень і є частиною комплексу визначення певних скеровуючих дій у рамках обраних систем менеджменту. Сучасний контролінг включає в себе управління ризиками, що є невід'ємною частиною систем захисту інформації, велику систему інформаційного супроводу сучасних телекомунікаційних мереж, систему оповіщення шляхом управління системою ключових показників, управління системою реалізації стратегічного, тактичного та оперативного планування, а також систему менеджменту.

Ідея високорівневого управління телекомунікаційними мережами постійно обговорюється вченими та інженерами з кінця 80-х років. У 1988 році Міжнародний консультативний комітет з телеграфії та телефонії (МККТТ) (англ.: (*Consultative Committee for International Telephony and Telegraphy* – CCITT) опублікував рекомендації для мереж, які відомі як документ M.30. Його складова – документ M.3010 "Принципи TMN" (англ.: *Telecommunication Management Network* – TMN) – є основним документом, який містить концепцію управління гетерогенними мережами [3]. Згідно з ним існує декілька підходів реалізації принципів TMN, але вони мають декларативний характер і практично не реалізовані на практиці. Проте згідно з концепцією TMN є низка широко застосовуваних локальних F-, G-, Q- та X-інтерфейсів [4], які реалізують функції управління мережами на низькому рівні. Згідно із зазначеним джерелом кожен інтерфейс призначений для управління певним типом мережевих елементів. Наприклад, інтерфейс F використовується для управління шинами комутаторів та гнучкими мультиплексорами, які активно використовуються для крос-комутації в мережах HetNet.

Наявна концепція TMN припускає, що взаємодія з мережами зв'язку забезпечується за допомогою інтерфейсів (точніше – інтеграційних інтерфейсів). Керуюча мережа TMN – це окремий логічний елемент, який може бути, у свою чергу, дочірнім логічним елементом мережі зв'язку або окремо реалізованим фізичним інтерфейсом. Інтерфейси реалізують процеси:

- FM (англ. *Fault Management* – FM, управління відмовами);
- CM (англ. *Configuration Management* – CM, управління конфігурацією);
- PM (англ. *Performance Management* – PM, управління продуктивністю);
- SM (англ. *Security Management* – SM, управління безпекою).

Звичайно, що з точки зору питання, яке винесене в заголовок, останній із наведених процесів викликає найбільшу зацікавленість. Втім, для цілісності викладу питання розглянемо всі наведені вище процеси та їх взаємозв'язок з точки зору вирішення питання управління гетерогенними мережами.

У найпростішому випадку управління мережами зводиться до завдання усунення колізій та крос-комутації. При цьому сучасні мережеві проблеми висувають більш широкі вимоги до процесу управління. Особливо це положення стосується гетерогенних мереж HetNet (англ. *Heterogeneous Network* – HetNet), для яких властиве нерівномірне навантаження та є актуальними методи його перерозподілу. Зокрема, це стосується методів автоматичної маршрутизації

користувачів та пристроїв між неоднорідними мережами, сервісами й доступними ресурсами. Фактично вже зараз потрібна функція ретрансляції SLA-запитів не тільки між сервісами, але й мережами, тобто мережева інфраструктура повинна бути задіяна на всіх рівнях ієрархії й реалізована "наскрізна" функціональність. Для цього потрібна ідеологія розробки складного апаратно-програмного управління мережею з урахуванням вимог тріади CIA.

Класичним вирішенням проблеми апаратно-програмного управління, що припускає безпечне підключення гетерогенних ресурсів, є застосування методів віртуалізації. Подібні засоби мережного управління на сьогодні реалізуються в *мережах, які програмно конфігуруються* (англ.: *Software Defined Networking* – SDN). При цьому забезпечується достатній захист інформаційних ресурсів, але як недолік, слід зазначити громіздкість програмного забезпечення та складності при його налаштуванні для кожного випадку об'єднання різнорідних мереж.

Безпечна гіпермережева організація SDN запропонована в 2008 році вченими Стенфордського університету. Вона базується на ідеї апаратної віртуалізації, яка вперше була запропонована для IBM System/360 (1964 рік) для організації багатокористувацького доступу до мейнфрейму. Зараз ця ідея широко використовується при побудові локальних та глобальних мереж. Згідно з концепцією безпечної гіпермережевої організації SDN мережа, яка програмно конфігурується, повинна знаходити найефективніший шлях для пересилання пакета, тобто реалізувати *завдання оптимізації крос-з'єднання на програмному рівні*. Такий підхід припускає програмний (на рівні мікропрограм) дозвіл колізій з метою об'єднання канального рівня пристроїв з системами управлінням комутаторами на елементному рівні за допомогою згаданих інтерфейсів TMN. Таким чином, можна зробити висновок про те, що мережі, які програмно конфігуруються, – це програмна реалізація завдання, розв'язуваного на апаратному рівні за допомогою архітектур нового покоління (англ. *Crossbar Switch* – NoC), які реалізовані для високонавантажених рішень. Доцільним є вдосконалення методів забезпечення інформаційної безпеки саме на основі синтезу нових програмних середовищ з використанням сучасних засобів управління ними. Такий програмно-апаратний підхід надасть нові можливості щодо управління мережами в наявних умовах тріади CIA з вирішенням проблем гіпермережевої організації.

Наявність шару віртуалізації та узгодження його з пристроями користувачів дозволяє безпечно поєднувати мережі різних постачальників послуг по "безшовному" принципу. Таким чином, зазначений напрям пропонується розробляти в межах протоколу OpenFlow [6]. Можливості протоколу дозволяють враховувати можливості шару віртуалізації та вирішувати завдання конвергентного управління мережами, погодженого з усіма рівнями "вертикальної ієрархії" від низькорівневого до високорівневого.

Основна перевага зазначеного підходу полягає в тому, що мережні платформи різних постачальників послуг телекомунікацій можуть бути об'єднані по "безшовному" принципу в єдину інфраструктуру з безпечною "наскрізною" функціональністю.

Відкрита версія OpenFlow поки не надає широких можливостей управління гетерогенними середовищами, але низка пропрієтарних мікропрограмних комплексів Cisco, Sap, Oracle вже реалізовані в готових продуктах з урахуванням вимог CIA. Перспективна концепція "безшовних" мереж розробляється в рамках

архітектури Cisco Advanced Borderless Networks Architecture. У цьому сенсі Cisco підкреслює необхідність організації безумовного захищеного підключення "ким завгодно, коли завгодно і на будь-якому пристрої по всьому світі". На сьогодні є різні недостовірні дані про результати тестування перевірених мережевих патернів Cisco Validated Designs для безпечного "безшовного" об'єднання в рамках глобальної мережі.

Розглянемо завдання безпечного управління гетерогенними мережами в рамках проектування окремих hyper-connected-платформ спеціального призначення. Так, згідно з публікацією [6], яка відображає думку фахівців компанії Akamai, питання розгортання інтеграційних hyper-connected-платформ для обслуговування *мультисервісних мереж* спеціального призначення зводяться до високорівневих проблем, які повинні бути враховані у високорівневих контролингових сервісах, а саме:

– *проблеми високої складності*: висока складність структури, яка враховує той факт, що будь-який контент є пов'язаним з несистемною та постійно мінливою структурою пристроїв, користувачів та додатків у сукупності з проблемою розмаїття сервісів та форматів (формати даних, протоколи, кодеки, механізми інформаційної безпеки);

– *проблеми доставки*: проблеми доставки контенту по високонавантажених мережах та узгодження між пов'язаними пристроями користувача пов'язані з тривалими затримками буферизації;

– *проблеми захисту даних та авторських прав*: захист персональної інформації та авторського контенту, що пояснюється поставленою метою впровадження бізнес-моделей із захистом, наприклад, цифрових активів, які доступні за підпискою;

– *проблеми монетизації*: проблема пояснюється мобільністю користувачів та передаванням фрагментованого контенту і, відповідно, складністю застосування рейтингів Нільсена (англ. *Nielsen Ratings*) для виміру обсягів даних (користувачів), які використовуються при монетизації контенту та з іншими цілями (наприклад, передавання реклами).

Як результат проведеного аналізу вирішено, що під *hyper-connected-платформою* будемо розуміти мережеву інфраструктуру, яка утримує в собі взаємопов'язані мережі зв'язку, обчислювальні ресурси та сервіси. Для конвергентного узгодження та представлення платформи у вигляді єдиного мережевого обчислювального середовища є необхідним використання низки інтеграційних рішень. Саму концептуальну модель hyper-connected-платформи представимо так, як це показано на рис. 1.

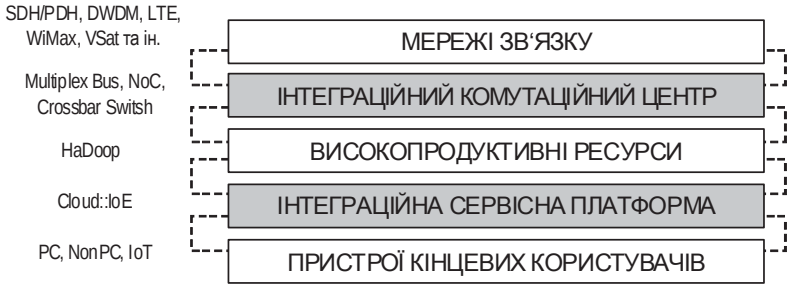

Рис. 1. Модель hyper-connected-платформи

Введемо визначення технологічно використовуваних інфраструктур.

Сервісною підмережею вважатимемо загальне поняття мережевих мультисервісних середовищ, які мають інтеграційні інтерфейси конвергенції, що забезпечують технологічно необхідні процеси, мережеві зв'язки, обчислювальні ресурси та користувацькі сервіси.

Hyper-connected-платформою вважатимемо мультисервісну конвергентну платформу, яка забезпечує користувачам та пристроям підключення і маршрутизацію для виконання таких умов:

– безперешкодне PnP-підключення всіх типів пристроїв;

– безумовне захищене підключення для всіх користувачів з будь-якого пристрою, у будь-якій точці глобальної мережі;

– маршрутизацію між вбудованими сервісами та їх інтеграцію з використанням безпечних протоколів;

– гетерогенне захищене високошвидкісне підключення пристроїв та користувачів до світових гетерогенних мереж зв'язку на умовах "безумовного" доступу, що не вимагає додаткової конфігурації.

У пропонованому рішенні, яке зображено на рис. 1, на низькому рівні hyper-connected-платформа становить взаємопов'язані мережі наземного, рухомого та супутникового зв'язку, де користувачі та пристрої будь-коли отримують безумовний доступ у будь-якій точці глобальної мережі в рамках покриття.

Вторинні мережі зв'язку містять виділені інтеграційні комплекси крос-з'єднання, тобто *інтеграційні комутаційні комплекси*, основною функцією яких є здійснення високошвидкісної захищеної та надійної конвергенції доступних гетерогенних мереж, а також забезпечення процесів управління навантаженням у рамках тріади CIA.

Інтеграційні комутаційні комплекси повинні забезпечувати прямі приєднання до високопродуктивних обчислювальних ресурсів (англ: *Hadoop* – пояснення див. нижче) за допомогою технологій: динамічної комутації, гнучких гібридних мультиплексорів, шин мультиплексорів, високошвидкісних шин AMD Hypertransport та Intel Quickpath, Infiniband, Fibrechanel, а також (у майбутньому) fabric-орієнтованих методів об'єднання комутаторів та мультиплексорів Crossbar Switch та NoC.

Як пояснення зазначимо, що Hadoop є проектом фонду Apache Software Foundation і являє собою вільно поширюваний набір утиліт, бібліотек та окремий програмний каркас для розробки та виконання розподілених програм, що працюють на кластерах, які включають сотні та тисячі вузлів. Згідно з розроблюваною темою Hadoop може використовуватися для реалізації пошукових, контекстних та таких, які мають спеціальні можливості моніторингу, механізмів багатьох високонавантажених Cloud-систем. Стосовно останнього поняття наведемо деякі пояснення.

На цей момент глобальна мережа є складною інфраструктурою, що відрізняється різноманіттям 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,* окремі технологічні складові якої названі Cloud-системами. Згідно з цим технологію Hadoop розроблено (з використанням технології Java) в рамках обчислювальної парадигми MapReduce, відповідно до якої будь-який додаток може бути розділений на велику кількість елементарних завдань, які вирішуються на вузлах кластера та можуть бути приведені до кінцевого результату простими способами.

Крім мереж зв'язку, в IP-сегменті глобальної мережі (наприклад, Інтернет) знаходяться обчислювальні ресурси, які можуть бути розділені на два більші класи: *клас високопродуктивних* та *клас низькопродуктивних ресурсів*. Відобразимо це положення у вигляді моделі (рис. 2).

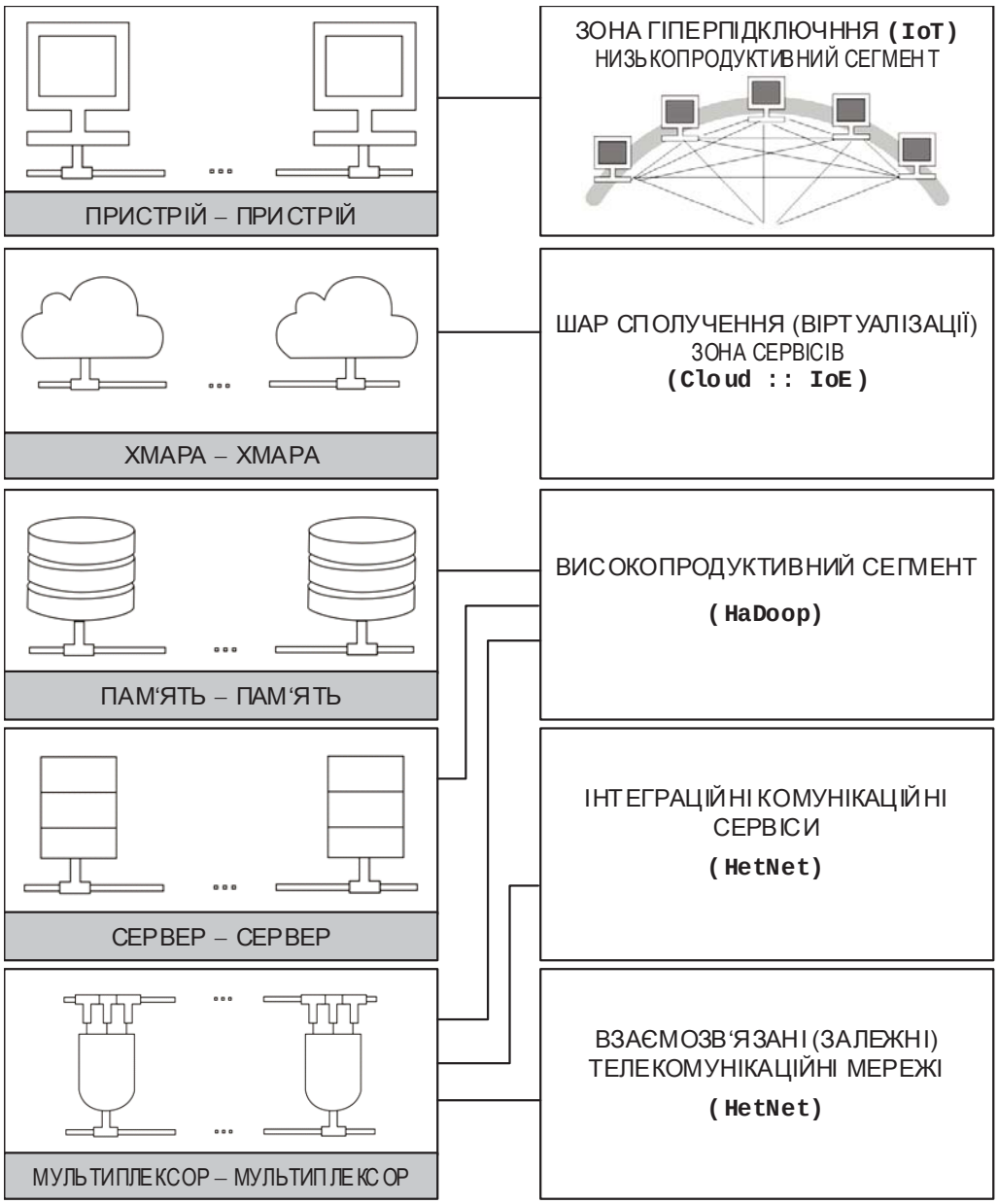

Рис. 2. Модель топологій SDN-мереж в hyper-connected-платформі

Згідно з рис. 2 низькопродуктивні ресурси знаходяться в зоні користувачів та споживачів послуг, які надаються на базі високопродуктивних ресурсів. Об'єднання ресурсів у пропонованій інфраструктурі припускає застосування принципу конвергенції та наявність інтерфейсу віртуалізації. Шар віртуалізації між високопродуктивними та низькопродуктивними ресурсами і, відповідно, користувачами є інтеграційною платформою, яка забезпечує конвергенцію сервісів та безпечний доступ до них споживачів.

Запропонована інфраструктура може бути технологічно реалізована на основі технології мереж з програмною конфігурацією (МПК). Якщо на їхній основі в зоні високопродуктивних та низькопродуктивних ресурсів згідно з рис. 2 може бути застосована технологія віртуалізації обчислювальних ресурсів та реалізоване програмне управління трафіком, то це дозволить вирішити проблему гіперпідключення, у тому числі – на програмному рівні – за допомогою топології SDN-мереж типу:

– "Мультиплексор-Мультиплексор" (англ. *Mux-to-Mux*) на рівні вторинної мережі HetNet;

– "Пам'ять-Пам'ять" (англ. *Storage-to-Storage*) та "Сервер-Сервер" (англ. *Server-to-Server*) – на рівні HaDoop, тобто обчислювальних систем кластерного класу;

– "Хмара-Хмара" (англ. *Cloud-to-Cloud*) – на рівні сервісів логічної віртуалізації, в "хмарному" шарі;

– "Пристрій-Пристрій" (англ. *Machine-to-Machine*) – на рівні користувацьких non-PC та IoT-пристроїв.

Очевидно, що інтеграційна сервісна платформа має на увазі захищене підключення й "нехмарних" сервісів. У цьому випадку вони можуть автоматично інтегруватися в "хмарний" сервіс за допомогою вбудованого "сервісу-оболонки" відповідно до відомої процедури, яка використовується для API-функцій на проміжному рівні (англ. *middleware*) для "обгортки" функцій [5]. Проактивне управління середовищем Middleware-рівня дозволить уникати простоїв у доставці послуг та швидше реагувати та вирішувати виникаючі інциденти (в т.ч. й інциденти у сфері інформаційної безпеки). Middleware-менеджмент є комплексним рішення для моніторингу та управління інтеграційними сервісними платформами, так як врахує всі вимоги тріади CIA, а саме:

– уніфікує та автоматизує управління проміжним рівнем у розподілених середовищах та середовищах Mainframe;

– забезпечить безперебійну роботу системи попередження, проактивні повідомлення та автоматичне усунення проблем при порушенні інформаційної безпеки та систем захисту;

– забезпечить безпечне незалежне адміністрування для проектів Middleware;

– буде відстежувати всі зміни в Cloud-конфігурації та в системах захисту і створювати динамічні звіти в реальному часі;

– виконуватиме моніторинг систем безпеки та готуватиме звітність по всіх транзакціях та по всіх даних додатків, які виконуються в реальному часі.

Управління середовищем Middleware-рівня та транзакціями може:

– поліпшити надійну доставку послуг за допомогою захисту від зниження якості роботи всіх систем та недопущення перерв у їх роботі;

– виявляти та швидше на 92 % вирішувати проблеми інформаційної безпеки [7];

– мінімізувати залежність від централізованої групи Middleware та підвищити продуктивність на 40 % [7];

– уникати втрат доходів та штрафів, пов'язаних зі збоями на рівні захисту важливих транзакцій.

Запропоновані МПК забезпечують "безшовне" сполучення всіх можливих "додатків-розв'язків-сервісів". У свою чергу, запропонована модель інтеграційної платформи реалізує функцію конвергенції на всіх рівнях мережної, обчислювальної та логічної ієрархії. Для об'єднання інфраструктур окремих постачальників "додатків-розв'язків-сервісів", а саме – підмереж може бути використана SDN-мережа з топологією "Fabric-to-Fabric" [7].

Принципова відмінність запропонованої архітектурної моделі полягає в тому, що мається на увазі реалізація наскрізної функціональності у вертикальній та горизонтальній площині розглянутого рішення. Цей тип функціональності характерний для розподілених систем. Для наскрізної функціональності практично неможливо виділити окремі сутності: класи, модулі, функції та ін. На сьогодні для вирішення проблем проектування використовується лише метод АОР (англ.: *Aspect-Oriented Programming* – АОР, аспектно-орієнтоване програмування), запропонований групою Грегора Кічалеса (англ.: *Gregor Kiczales*) [8].

Мультисервісна підмережа є частковим випадком hyper-connected-платформи та становить інтеграційне рішення, яке поєднує окремі види сервісів загально доступних спеціалізованих сегментів мережі Інтернет (англ.: *Internet of Everything*-IoE), відомих як *хмарні поля* (англ.: *Federation Clouds* – FC) з обраним набором функцій. Як приклад можливих підмереж можна навести:

– системи доставки контенту в CDN (англ.: *Content Delivery Network* або *Content Distribution Network* – CDN, мережа доставки або дистрибуції контенту);

– бібліотечні ресурси та пошукові системи;

– мережі державних порталів, які надають послуги, інтегровані в один інтерфейс;

– системи швидкого реагування типу "ЕРА-ГЛОНАСС", що обслуговують спеціальні організації;

– муніципальні, медичні та інші сервіси для населення та ін.

Як вже було визначено, підмережа повинна забезпечувати *конвергенцію мереж, ресурсів, сервісів*.

Запропонована архітектура дозволяє розв'язати проблему безпеки Cloud-платформи завдяки виділенню процедур комутації та маршрутизації в первинних мережах в окрему інтеграційну інфраструктуру. До інтеграційних комутаційних центрів можуть бути підключені окремі модулі фільтрації з функціями автоматичного контролю у WAN (англ.: *Wide Area Network* – WAN, глобальна комп'ютер-на мережа) та LAN (англ.: *Local Area Network* – LAN, локальна комп'ютерна мережа). Зазначимо, що фільтрація трафіка на сучасному етапі функціонування систем доступу до Cloud-платформ базується на методах, які поєднують у собі технологію DPI (англ.: *Deep Packet Inspections* – DPI, глибокий аналіз пакетів) і семантичний аналіз даних, застосовуваних у рамках функціональності сучасних систем DLP (англ.: *Data Loss Prevention* – DLP, захист мереж від витоків) та IDS (англ.: *Intrusion Detection System* – IDS, виявлення вторгнень) [9–18].

Спеціальне питання виділення комутаційного центру для державної підмережі в окрему інфраструктуру, яке є актуальним у зв'язку з перспективами створення державного сегменту мережі Інтернет, не є новою технологічною ідеєю, але класична функціональність припускає розгортання міжнародних вузлів комутації, що обслуговують міжконтинентальні магістральні мережі в рамках стратегічних проектів EPEG (англ.: *Europe-Persia Express Gateway* – EPEG), вузлів зв'язку MPLS, високошвидкісної транзитної магістралі "Європа-Азія". У рамках цього запропонована модель має на увазі магістральні комутаційні мережі, що забезпечують функціональність мереж HetNet у рамках обслуговування комерційної та високоприбуткової сервісної Cloud-платформи, яка опирається на власні глобальні мережі зв'язку [11].

Розглянуті питання конвергенції глобальної інформаційної мережі в сенсі зосередження основної уваги на питаннях управління гетерогенними середовищами з урахуванням наявних проблем забезпечення інформаційної безпеки у відкритих системах, до яких віднесено Cloud-структури. Дано поняття про такі структури. Запропонована архітектурна модель обчислювального середовища, яке програмно конфігурується. Показано принципову відмінність моделі, яка полягає в тому, що основою є реалізація наскрізної функціональності у вертикальній (високопродуктивні рішення) та горизонтальній (низькопродуктивні рішення) площині. Такий тип функціональності свідчить про те, що запропонована модель може бути застосована для розподілених обчислювальних систем.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

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. – 2013. – № 4 (12). – С. 23–40.

2. *Зеленцова Ж.* Інфраструктурні рішення та технології підвищення безпеки обробки даних при хмарних обчисленнях / Ж. Зеленцова, Н. Казакова // Захист інформації і безпека інформаційних систем : матеріали III міжнар. наук.-техн.-конф. (м. Львів, 5–6 червня 2014 р.) Львів : – С. 58–59.

3. *Гринько Д.* Управление гетерогенными сетями связи / Д. Гринько, В. Саякин // Журнал сетевых решений LAN. – 2002. – № 11 [Электронний ресурс]. – Режим доступу : http : // www.osp.ru/lan/ 2002/11/135439/. – Заголовок з екрану, доступ вільний, 22.04.2012.

4. Лекции по управлению телекоммуникационными сетями [Электронний ресурс]. – Режим доступу : http : // siblec.ru/index.php?dn=html&way=bW9kL2h0bWwvY29udGVud C83c2VtL2 NvdXJzZTExNS9pbmRleC5odG0=. – Заголовок з екрану, доступ вільний, 26.06.2014.

5. Управление на промежуточном уровне (Middleware Management) [Электронний ресурс]. – Режим доступу : http : // www.compfort.pl/Upravlenie_na_promezutocnom_urovne_ Middleware_Management_47,0.html?lang=ru. – Заголовок з екрану, доступ вільний, 26.06.2014.

6. The Hyperconnected World : A New Era of Opportunity, White Paper, Akamai [Электронний ресурс]. – Режим доступу : http : // www.akamai. com/dl/akamai/hyperconnected_world.pdf..

7. *Луговой А.В.* Анализ архитектуры глобальных конвергентных решений и синтез агрегированной модели / А.В. Луговой, Ж.Ю. Зеленцова // Вісник Кременчуцького національного університету імені Михайла Остроградського. – 2013. – № 3 (80). – С. 84–91.

8. *Kiczales G.* Aspect-Oriented Programming / G. Kiczales, J. Lamping, A. Mehdhekar, C. Maeda, C. V. Lopes. J. Loingtier, J. Irwin // Proceedings of the European Conference on Object-Oriented Programming (ECOOP). – Springer-Verlag LNCS 1241. – June, 1997.

9. Narus: Cyber 3.0 Analytics for Cyber Security [Электронний ресурс]. – Режим доступу : http : // www.narus.com/. – Заголовок з екрану, доступ вільний, 25.11.2013.

10. *Зеленцова Ж.Ю.* Уязвимости конвергентной инфраструктуры и практические подходы к их устранению / Ж.Ю. Зеленцова, А.В. Луговой // Вісник Східноукраїнського національного університету імені Володимира Даля. – 2013. – № 15(1) (204). – С. 122–129.

11. 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, Є.В. Вавілов, К.Б. Айвазова // ОНЕУ ; кер. О.О. Скопа. – 0112U007713. – Одеса, 2013. – 236 с.

12. *Рыбальский О.В.* Экспериментальное исследование нового метода защиты от ВЧ-навязывания / О.В. Рыбальский, В.А. Хорошко, Л.П. Крючкова // Вісник Східноукраїнського національного університету імені Володимира Даля. – 2009. – № 6 (136). – С. 94–96.

13. *Рыбальский О.В.* Защита информации на промышленном предприятии / О.В. Рыбальский, Л.Н. Скачек, В.А. Хорошко // Сучасна спеціальна техніка. – 2010. – № 3 (22). – С. 24–32.

14. *Щербина Ю.В.* Проблемы объективной оценки параметров защищенных автоматизированных систем / Ю.В. Щербина, Н.Ф. Казакова // Правове, нормативне та метрологічне забезпечення систем захисту інформації в Україні : матеріали IV наук.-техн. конф. (Київ, 1–3 березня 2006 р.) / НТУУ "КПІ". – К. : НТУУ "КПІ", 2006. – С. 60–61.

15. *Kazakova N.* Mobil radio-service management system construction principles // Proceeding of the International Conference TCSET'2002 "Modern Problems of Radio Engineering, Telecommunications and Computer Science" : February 18-23, 2002. – Lviv-Slavsk, Ukraine : Lviv Polytechnic National University – IEEE Networking the World. – 2002. – P. 284.

16. *Скопа О.О.* Аналіз розвитку сучасних напрямів інформаційної безпеки автоматизованих систем / О.О. Скопа, Н.Ф. Казакова // Системи обробки інформації. – 2009. – № 7 (79). – С. 48–54.

17. *Казакова Н.Ф.* Оцінка живучості систем моніторингу інформаційного простору / Н.Ф. Казакова // Восточно-европейский журнал передовых технологий. – 2012. – № 4/2 (58). – С. 12–15.

18. *Казакова Н.Ф.* Аналіз напрямів розвитку інформаційної безпеки у комп'ютерних системах та мережах на основі застосування програмних засобів захисту інформації / Н.Ф. Казакова // Вісник Львівського національного аграрного університету. – 2010. – № 14. – С. 47–57.

Отримано 12.09.2014.