системі. Затверджено наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України 8 листопада 2005 р. № 125.

5. ***НД ТЗІ 1.4–001–2000.*** *Типове положення про службу захисту інформації в автоматизованій системі. Затверджено наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 04 грудня 2000 р. № 53.*

6. ***НД ТЗІ 1.1-002-99.*** *Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу. Затверджено наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 28 квітня 1999 р. № 22.*

7. ***Положення*** *про державну експертизу у сфері технічного захисту інформації. Затверджено наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 29 грудня 1999 р. № 62.*

В. А. Козачок

КОНЦЕПТУАЛЬНЫЕ ОСНОВЫ СОЗДАНИЯ КОМПЛЕКСНЫХ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ В ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМАХ

Рассмотрены основные положения концепции по созданию комплексных систем защиты информации в современных информационно-телекоммуникационных системах. Обоснована необходимость создания комплексных систем защиты информации в информационно-телекоммуникационных системах, обеспечивающих обработку информации с ограниченным доступом, а также раскрыты основные положения политики безопасности информации в информационно-телекоммуникационных системах.

Ключевые слова: комплексная система защиты информации; информационно-телекоммуникационная система; техническая защита информации; политика безопасности информации; государственная экспертиза комплексной системы защиты информации.

V. A. Kozachok

CONCEPTUAL BASES OF CREATION COMPLEX INFORMATION SECURITY SYSTEMS IN THE INFORMATION AND TELECOMMUNICATIONS SYSTEMS

The main provisions of the concept to create a comprehensive information security systems in modern information and telecommunication systems. The necessity of creation of complex information security systems in information and telecommunication redundant system in which information is processed with limited access. Substantiated the main provisions of the security policy information in the information and telecommunication redundant system..

Keywords: complex system of information protection; information and telecommunications system; technical information security; information security policy; state expertise of complex information protection system.

УДК 621.396.967.2

А. О. ЛУНТОВСЬКИЙ, д-р техн. наук, професор, БЕРУФС Академія, Дрезден;
А. І. СЕМЕНКО, д-р техн. наук, професор, Державний університет телекомунікацій, Київ

ЗАСТОСУВАННЯ ТЕХНОЛОГІЙ SDN ДЛЯ ПРОГРАМНОЇ РЕАЛІЗАЦІЇ ПРОВАЙДЕРСЬКОГО ЯДРА СИСТЕМ МОБІЛЬНОГО ЗВ'ЯЗКУ 5G МАЙБУТНЬОГО ПОКОЛІННЯ

Розглянуто особливості програмно-конфігурованих мереж SDN, в яких функції передавання трафіку відокремлено від функцій управління мережею. Обґрунтовано доцільність та ефективність використання технологій SDN при створенні систем мобільного зв'язку майбутнього покоління 5G за стандартом IMT 2020.

Ключові слова: програмно-конфігуровані мережі; системи мобільного зв'язку 5-го покоління; функції передавання трафіку; функції управління.

Віртуалізація ресурсів та програмно-конфігуровані мережі

Програмно-конфігурована мережа (***Software-Defined Networking — SDN***) — це віртуалізована мережа для передавання даних, в якій шар менеджменту (контролю або управління) мережею (*Management Plane*) відокремлений від пристроїв передавання даних і реалізується програмним шляхом. SDN являє собою одну з відомих форм віртуалізації обчислювальних ресурсів, зокрема мережних сервісів і додатків (рис. 1). Принципи створення зазначених мереж сформулювали в 2006 році фахівці всесвітньо відомих університетів Берклі та Стенфорда.

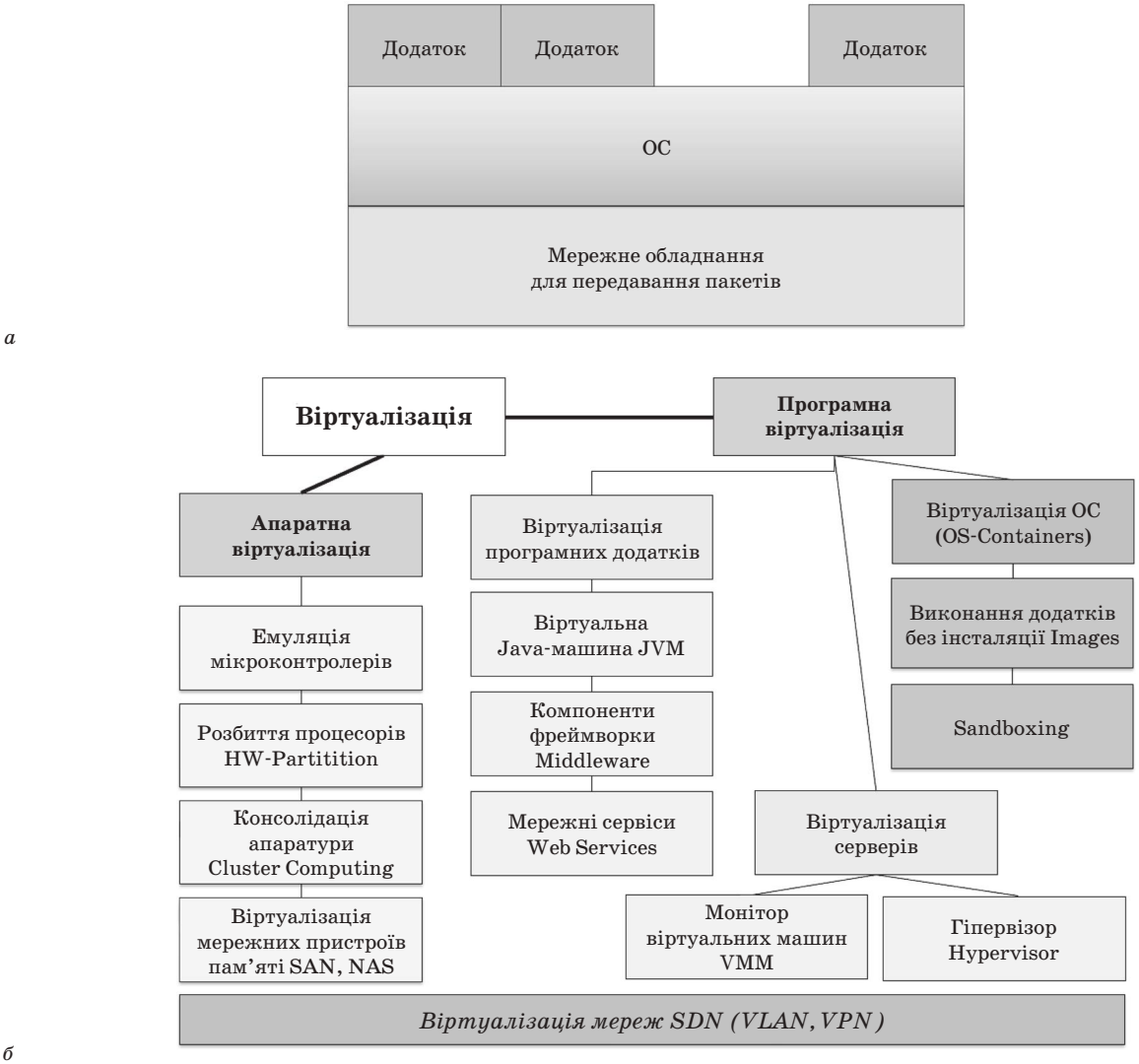


Рис. 1. Віртуалізація ресурсів: *а* — віртуалізація відсутня; *б* — види віртуалізації

Мотивація щодо застосування SDN така.

1. Традиційні мережі занадто статичні, а отже, не відповідають динаміці, притаманній сучасному бізнесу, мережним (віртуальним) серверам, додаткам і сервісам.

2. Завдяки технологіям віртуалізації додатки розподілено сьогодні між безліччю віртуальних машин, які інтенсивно обмінюються даними. Для оптимізації завантаження серверів віртуальні машини часто мігрують, що, у свою чергу, призводить до змін точок «прив'язки» трафіку.

3. Традиційні схеми адресації, логічного поділу мереж, як і способи призначення правил обробки трафіку в сучасних динамічних середовищах втрачають ефективність.

Наприклад, запуск нової віртуальної машини або реконфігурування списків контролю доступу (***Access Control Lists*** — ***ACL***) у великій мережі на всіх мережних пристроях може тривати кілька днів, передусім через орієнтацію наявних інструментів мережного менеджменту (SNMP, MIB) на роботу з окремими фізичними пристроями. У найкращому разі автоматизація призначення параметрів за допомогою протоколу SNMP поширюється на групу пристроїв, що складається з представників одного модельного ряду конкретного виробника, наприклад Cisco MIB.

У мережах типу SDN вся логіка управління покладається на контролери, здатні відстежувати роботу всієї мережі.

Мережі SDN призначено для автоматизованого виконання низки завдань, серед яких:

- емуляція MAC-кадрів і пакетів (MPLS, IP, LAN, мобільний радіозв'язок поколінь 3G, 4G) на рівнях L2 і L3;
- розгортання зон, демаркація користувачів;
- «хмарні послуги» в договорах оренди *Cloud Services*;
- підтримка різноманітних SDN-архітектур і провайдерів (рис. 2).

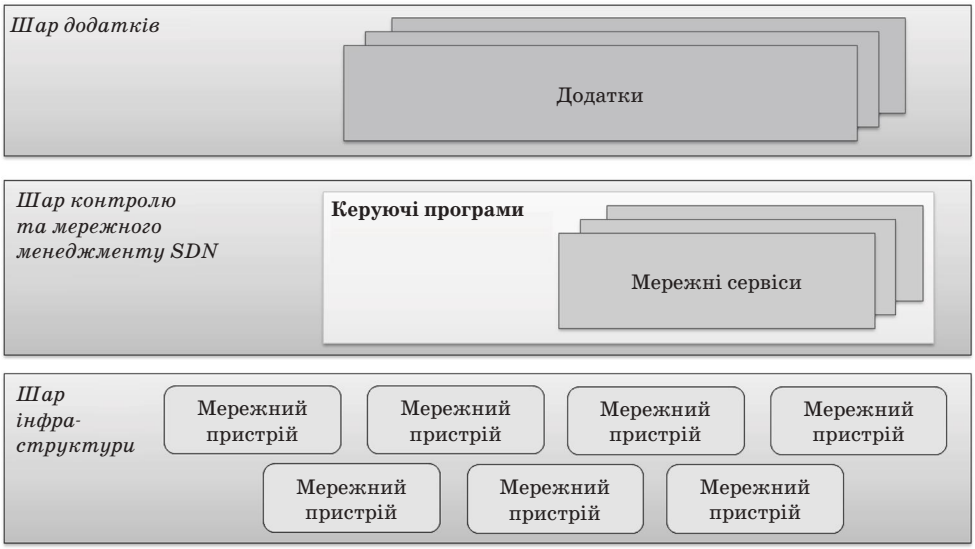


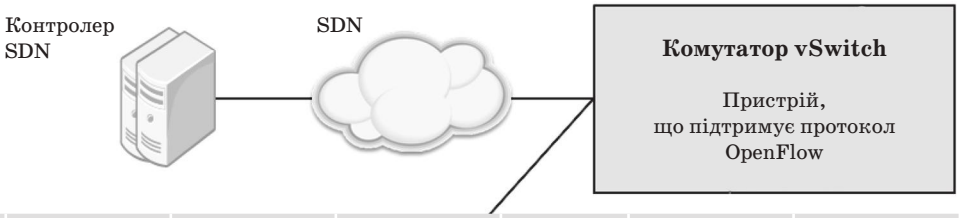
Рис. 2. Архітектура SDN

Підтримкою SDN-архітектур опікуються VMware, Cisco, Juniper, Brocade, HP. Наприклад, відома система VMWare надає для SDN сервіси та (віртуальні) пристрої:

- ♦ програмне забезпечення, яке визначає доступ до мережі SDN;
- ♦ засоби використання фізичної фабрики (PHY NW);
- ♦ засоби використання кількох віртуальних машин;
- ♦ засоби використання кількох віртуальних локальних мереж VLAN на рівні L2;
- ♦ віртуальні комутатори *Virtual Distributed Switch* (vDS);
- ♦ віртуальні мережні карти (vNIC);
- ♦ мережні пристрої, що підтримують відомі протоколи OpenFlow або VXLAN (*Virtual Extensible LAN*).

Рушійною силою поширення та популяризації різних реалізацій концепції програмно-конфігурованої мережі є протокол OpenFlow, який уможливлює незалежний від виробника інтерфейс між логічним контролером мережі та мережним транспортом.

Типову ***таблицю потоків*** (Flow Table) у мережному пристрої, що підтримує універсальний протокол OpenFlow, наведено на рис. 3. Завдяки OpenFlow забезпечується гнучка й ефективна фізична (MAC-) і логічна (IP-) адресація, відбувається реконфігурування потоків для певних сервісів, дотатків та їхніх портів.



Таблиця потоків (Flow Table)

MAC Src	MAC dst	IPsrc	IPdst	TCPdport	...	Action	Count
...	10:20:aa:bb:cc:07	...	...	...	...	Port1	250
...	...	135.66.7.8	...	...	...	Port2	300
...	...	...	...	...	...	Drop	892
...	...	192.168	...	...	...	Local	120
...	...		...	...	...	Controller	11

Рис. 3. Таблиця потоків OpenFlow

Протокол OpenFlow при ідентифікації трафіку оперує поняттям ***потоку***. Ключовим елементом комутатора, що підтримує цей протокол, є згадувана вже таблиця потоків. Група стовпців у лівій частині таблиці формує поля відповідності, де наведено характеристики потоків. Це можуть бути різні параметри, включаючи MAC- і IP-адреси відправника та одержувача, ідентифікатор VLAN, номери протокольних портів TCP і UDP, а також інша інформація. Зазначені дані за допомогою протоколу OpenFlow контролер записує в таблицю комутатора.

Реалізацію принципів SDN із використанням віртуальних комутаторів vSwitch унаочнює рис. 4. Зазначені вирішення на віртуальних комутаторах типу vSwitch рівня L2 застосовують фірми VMWare, Juniper, Cisco, HP, IBM тощо для доступу рівня L3 через шлюз GW (Gateway) до віртуальних машин з певними додатками, до мережних сервісів та сервісів, розміщених у «хмарах» Clouds. Надається захист даних від Malware та багатьох можливих типів загроз рівнів L2, L3, L4, L5-7 на основі використання брандмауерів та антивірусних програм.

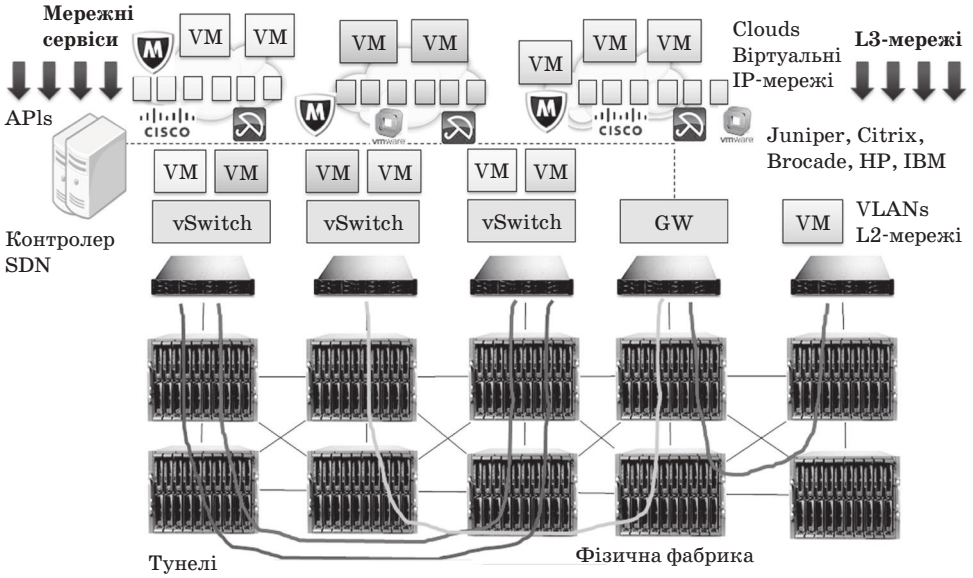


Рис. 4. Використання віртуальних комутаторів vSwitch

Приклад, що ілюструє надання захисту даних та розмежування доступу наведено на рис. 5.

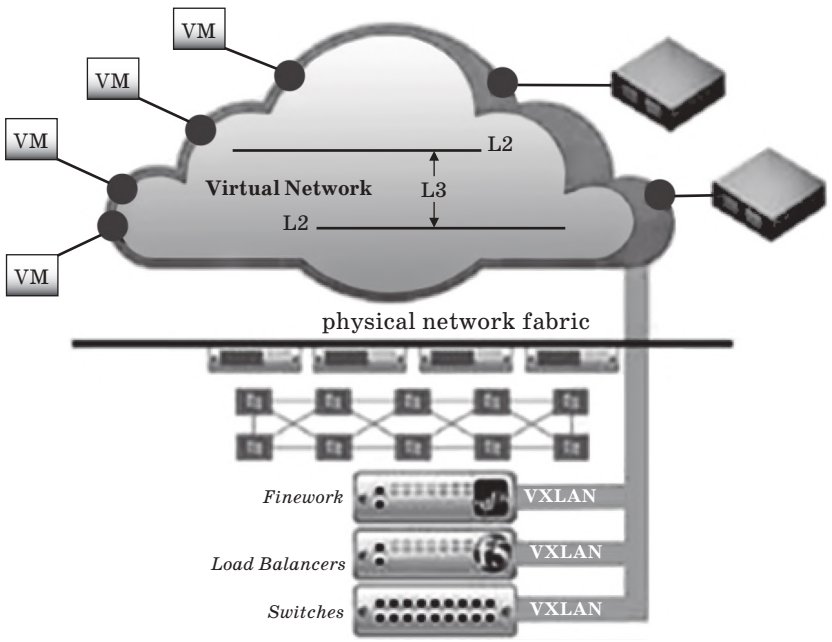


Рис. 5. Розмежування доступу в SDN

Мережні карти серверів vNICs з'єднано з VDS, завдяки чому уможливлюється поділ віртуальних машин на групи портів VDS для підімкнення до мережі. Віртуальний комутатор VDS не прив'язаний до конкретного сервера, але налаштований на кілька серверів і містить такі компоненти:

♦ VShield зони — віртуальний центр обробки даних, що дозволяє захист VM від мережних загроз (фільтрація через FW);

♦ систему vNCS (VMware vCloud Network and Security);

♦ VXLAN протокол (*Virtual Extensible LAN*);

♦ віртуальні міжмережні екрани VPN (*Virtual Private Networks*) та засоби балансування навантаження (*Load Balancers*).

Технології SDN у перспективному поколінні мобільного зв'язку 5G

Провідні фахівці від Deutsche Telekom, NTT DoCoMo, Amtel, Samsung, Telefonica, Vodafone тощо терміново формують своє бачення та технічні вимоги до майбутнього покоління мобільного зв'язку 5G за стандартом IMT 2020.

Дослідження з технології 5G почалися в 2012 році у Франції з досягненням швидкості передавання даних понад 4 Гбіт/с. У 2013 році в Японії було зроблено новий крок у напрямку 5G: апаратура компанії NTT DoCoMo показала можливість передавання даних від користувача зі швидкістю до 10 Гбіт/с (Uplink) на частоті 11 ГГц при смузі пропускання 400 МГц. Передавання даних здійснювалось з автомобіля за швидкості 9 км/год. У жовтні 2014 фірма Samsung Electronics досягла рекордної швидкості передавання даних, що становила 1,2 Гбіт/с при швидкості руху автомобіля 100 км/год та 7,5 Гбіт/с у стаціонарних умовах на частоті 28 ГГц. Але використання таких високих частот доволі проблематичне через велике загасання сигналу в міських умовах.

У Дрезденському технічному університеті відкрито сучасну лабораторію 5G на кафедрі Vodafone з мобільних систем зв'язку. Дослідники зможуть випробувати й оцінити широкий спектр технологій 5G (Enabling Technologies). До них відносять LTE, IEEE 802.20, 802.16e, 802.16a/d/e/m, Multi-gigabit Standard WiGig 60GHz, IEEE 802.11ad, IEEE 1905, Bluetooth v4.2, 6LoWPAN.

Лабораторія 5G містить мережне обладнання та програмне забезпечення, комп'ютерні чіпи, спектрометри та сервіси для «хмарних обчислень».

Сьогодні мобільний зв'язок опікується загалом наданням IP-послуг та переміщенням контенту з одного місця в інше. Проте завтра вже нове покоління матиме змогу контролювати широкий спектр об'єктів у режимі реального часу з невеликим втручанням людини (IoT). Для цього доведеться оптимізувати наявні системи мобільного зв'язку та безпроводові мережі, передусім щодо швидкості, затримок, інтерференції та надійності (рис. 6).

Згідно зі стандартом IMT 2020 5-го покоління 5G передбачається широке використання техніки *Multiple Input Multiple Output* (MIMO 16×16).

Співвідношення швидкостей передавання даних до мобільних користувачів у системах мобільного зв'язку 3G, 4G та 5G унаочнює рис. 7.

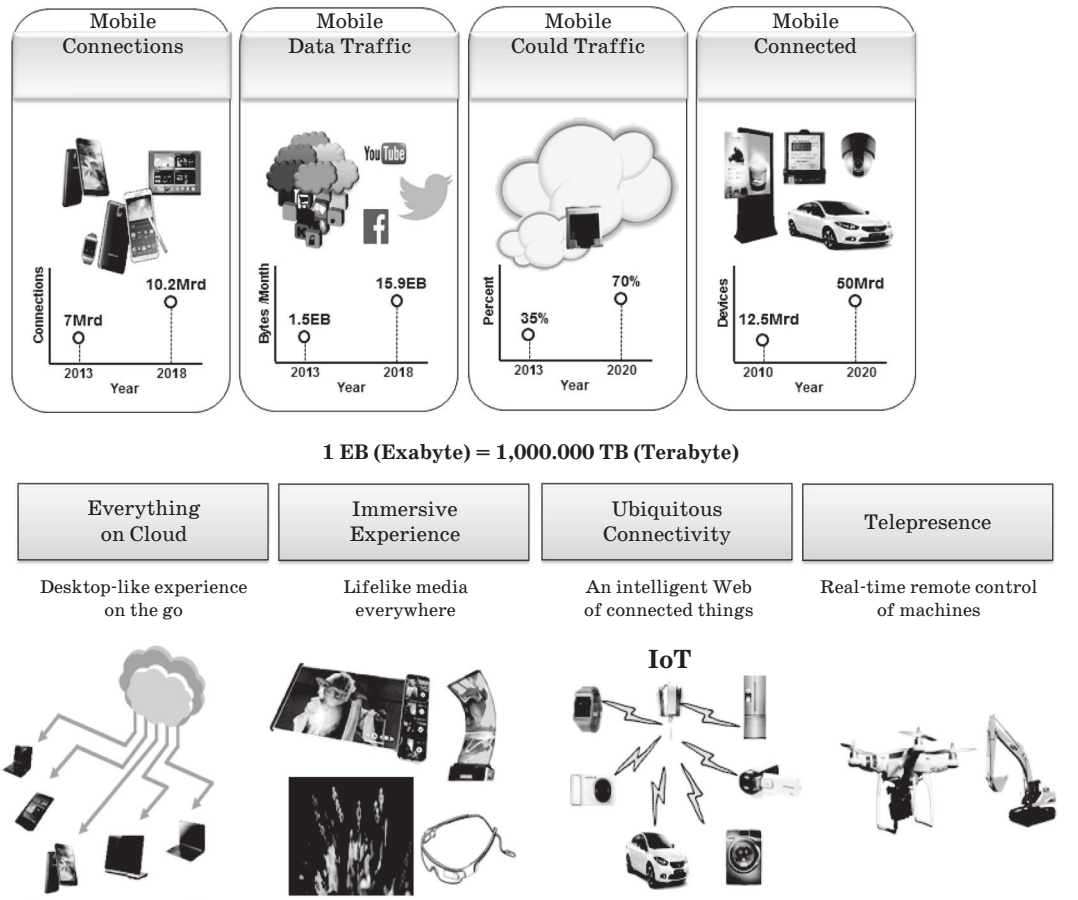


Рис. 6. Нові можливості систем 5G (за поданням Samsung Electronics)

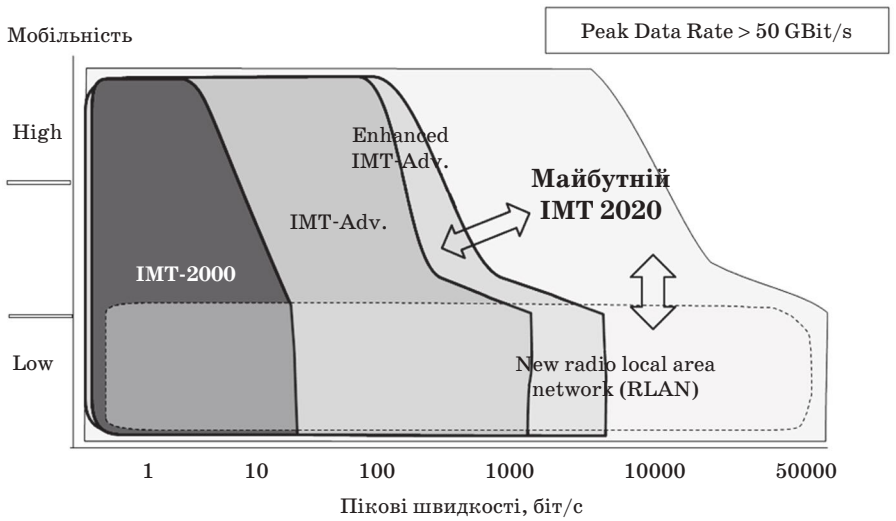


Рис. 7. Від 3G до 5G: співвідношення швидкість-мобільність (за поданням Samsung Electronics)

Як бачимо, застосування технології SDN у рамках систем мобільного зв'язку покоління 5G/IMT 2020 — позиція визначена. Поряд із поліпшенням систем радіодоступу RAN і RLAN завдяки використанню нової бази даних частот DIDO, а також оптимізацією інфраструктури наявних систем 4G/SAE, 3G/UTRAN, 2G/GERAN важливу роль відіграє віртуалізація сервісів ядра, здійснювана за допомогою мереж типу SDN.

Програмна реалізація прототипа провайдерського ядра 5G може здійснюватися на основі мереж SDN із використанням протоколів OpenFlow, VXLAN та віртуальних ОС типу VMWare/ vSwitch, Citrix Xen тощо.

Зауважимо, що мережі SDN ефективні для побудови інфраструктурних «хмарних сервісів». Передусім ідеться про умови, коли за запитом споживачів послуг доводиться автоматично і в найкоротші терміни створювати віртуальні вузли, а також виділяти віртуальні мережні ресурси для них.

У рамках систем мобільного зв'язку покоління 5G/IMT 2020 мережі SDN доцільні для великих центрів обробки даних, оскільки дозволяють скоротити витрати на супровід мережі за рахунок централізації управління на програмному контролері, підвищуючи частку використовуваних ресурсів мережі завдяки динамічному управлінню.

Загальну архітектуру систем мобільного зв'язку покоління 5G ілюструє рис. 8.

Рис. 8. Архітектура систем мобільного зв'язку покоління 5G

Інше перспективне застосування мереж передбачено концепцією IoT. Розглядається «інтернет речей», що ґрунтується на обчислювальних мережах фізичних об'єктів, оснащених убудованими технологіями для взаємодії один з одним або із зовнішнім середовищем.

Інтерес до SDN із боку великих постачальників інтернет-сервісів, хмарних послуг і власників мегаЦОД зрозумілий: нові технології дозволять їм розв'язувати свої завдання ефективніше і, головне, за менші гроші. Перший комерційний проект із побудови програмно-конфігурованої мережі реалізувала в 2007 році компанія Nicira. Незабаром її клієнтами стали NTT docomo, AT&T, EBay, Rackspace. Обсяг ринку зазначених мереж у 2012 році становив близько $200 млн. Прогнозується його зростання до $2,1 млрд не пізніше як 2017 року.

Висновки

Втілення в життя концепції SDN для програмної реалізації провайдерського ядра на практиці, зокрема в мережах 5G, дасть змогу підприємствам і операторам зв'язку отримати незалежні від постачальника функції менеджменту та контролю над мережними компонентами й сервісами будь-якого типу з єдиного центру, що значно спростить їх експлуатацію.

Рутинні функції реконфігурації мережі також спростяться. Адже адміністраторам не доведеться вводити сотні рядків коду конфігурації окремо для різних комутаторів або маршрутизаторів. Характеристики мережі можна буде оперативно змінювати в режимі реального часу.

Відповідно, терміни впровадження нових додатків і сервісів значно скоротяться (Intelligent Web of connected things, Real-time remote control, Mobile Cloud Traffic, Immersive Experience, Lifelike media, Ubiquitous Connectivity, Telepresence тощо).

Література

*1. **Лунтовський, А. О.** Мультисервісні мобільні платформи / А. О. Лунтовський, М. В. Захарченко, А. І. Семенко.— К.: ДУТ, 2014.— 216 с.*

*2. **Лунтовський, А. О.** Інформаційна безпека розподілених систем / А. О. Лунтовський, М. М. Климаш.— Львів: Львів. політехніка, 2014.— 464 с.*

*3. **Лунтовський, А. О.** Розподілені сервіси телекомунікаційних мереж та повсюдний комп'ютинг і Cloud-технології / А. О. Лунтовський, М. М. Климаш, А. І. Семенко.— Львів: Львів. політехніка, 2012.— 368 с.*

*4. **5G Nanocore** (Online, in German).— Режим доступу:*
http://de.scribd.com/doc/87616878/5G-the-Nano-Core

*5. **5G-Laboratory**@TUDresden (Online).— Режим доступу:*
http://www.telecompaper.com/news/dresden-university-to-inaugurate-5g-laboratory--1039172

*6. **From the Internet** of Things to the Web of Things: Resource Oriented Architecture and Best Practices: in «Architecting the Internet of Things» / [Friedemann Mattern a. o.].— Springer, New York – Dordrecht – Heidelberg – London, 2011.— P. 97–129.*

*7. **Benn, H.** 5G Mobile Communications for 2020 and Beyond: Vision and Key Enabling Technologies / Howard Benn // Samsung Electronics.— Oct. 2014.*

*8. **NanoZEIT**@TUD (Online, in German).— Режим доступу:*
http://www.et.tu-dresden.de/etit/index.php?id=556

*9. **Securty Compendium** (Online, in German).— Режим доступу:*
http://www.security-insider.de

*10. **Distributed-Input-Distributed-Output (DIDO)** Wireless Technology A New Approach to Multiuser Wireless / [Steve Perlman a. o.] // DIDO White Paper, Rearden.com, 2014.— 19 p.*

*11. **FQAM**: A modulation scheme for beyond 4G cellular wireless communication / [Sungnam Hong a. o.] // Samsung Electronics, in Globecom Workshops, 2013 IEEE.*

*12. **Limoncelli, T. A.** OpenFlow: A Radical New Idea in Networking / Thomas A. Limoncelli // Communications of the ACM.— N. Y., 2012.— Т. 55, № 8.— P. 42–47.*

*13. **Vodafone Chair** @ TUD (Online).— Режим доступу:*
http://mns.ifn.et.tu-dresden.de/

А. О. Лунтовский, А. И. Семенко

ПРИМЕНЕНИЕ ТЕХНОЛОГИЙ SDN ДЛЯ ПРОГРАММНОЙ РЕАЛИЗАЦИИ ПРОВАЙДЕРСКОГО ЯДРА СИСТЕМ МОБИЛЬНОЙ СВЯЗИ 5G БУДУЩЕГО ПОКОЛЕНИЯ

Рассмотрены особенности программно-конфигурированных сетей SDN, в которых функции передачи трафика отделены от функций управления сетью. Обоснована целесообразность и показана эффективность использования технологий SDN при создании систем мобильной связи будущего поколения 5G по стандарту IMT 2020.

Ключевые слова: программно-конфигурируемые сети; системы мобильной связи 5-го поколения; функции передачи трафика; функции управления.

A. O. Luntovsky, A. I. Semenko

THE SDN TECHNOLOGY FOR 5G IMT PROVIDER CORE SOFTWARE REALIZATION

The features of the software-configured networks (SDN) are shown, in which the traffic transmission functions are separated from the network management. The SDN technology usage expediency and efficiency in future generation 5G IMT 2020 standard mobile communication systems creation is shown.

Keywords: Software-Definded Networks; 5G IMT; transmission functions; network management.