

УДК 621.391.001.12/.18

**Орлов Є. В.**, аспірант (Тел. +380 44 248 75 97. E-mail: evorlov@ukr.net )  
(Державний університет телекомунікацій, м. Київ)

## ПРОГРАМНО-КОНФІГУРОВАНІ МЕРЕЖІ: АРХІТЕКТУРА, МІЖНАРОДНА СТАНДАРТИЗАЦІЯ

**Орлов Є. В. Програмно-конфігуровані мережі: архітектура, міжнародна стандартизація.** Аналізується стан міжнародної стандартизації програмно-конфігурованих мереж (Software-Defined Network, SDN), архітектура яких, на відмінність від традиційної, передбачає відділення площини управління від площини передачі даних, а також використання спеціалізованого протоколу для обміну управляючою інформацією між двома площинами, наприклад протоколу OpenFlow.

**Ключові слова:** програмно-конфігурована мережа, стандартизація, протокол, комутатор, контролер, віртуалізація, SDN

**Орлов Є. В. Програмно-конфигурируемые сети: архитектура, международная стандартизация.** Анализируется состояние международной стандартизации программно-конфигурируемых сетей (Software-Defined Network, SDN), архитектура которых, в отличие от традиционной, предполагает отделение плоскости управления от плоскости передачи данных, а также использование специализированного протокола для обмена управляющей информацией между двумя плоскостями, например протокола OpenFlow.

**Ключевые слова:** програмно-конфигурируемая сеть, стандартизация, протокол, коммутатор, контроллер, виртуализация, SDN

**Orlov Ye. V. Software-Defined Networks (SDN): architecture, international standardization.** The article presents analysis of the state of SDN (Software-Defined Network) international standardization. The most significant difference between SDN and traditional network architecture is that the former decouples the control and data planes, employing a specialized protocol for the control data exchange between the two planes (i.e. OpenFlow protocol).

**Keywords:** software-defined network, standardization, protocol, switch, controller, virtualization, SDN

**Вступ.** Сучасний етап розвитку комп'ютерних систем можна охарактеризувати зростанням ролі розподілених мережевих структур унаслідок об'єктивного зниження темпів зростання продуктивності окремих вузлів та необхідністю організації їх спільної роботи для досягнення потрібних характеристик. До прикладів цього процесу можна віднести розповсюдження багатоядерних процесорів, багатоканальну організацію оперативної пам'яті, ускладнення обчислювальних кластерів, центрів обробки даних та ін.

Організація потоків даних в таких структурах вимагає нових підходів до управління із-за лавиноподібного збільшення комутаційних правил та трудомісткості управління мережевою інфраструктурою [1]. Це пов'язано, з одного боку, з існуванням великої кількості різноманітних комунікаційних технологій, часто закритих та несумісних, з іншого боку – існуючі мережеве обладнання, як правило, спеціалізовані для «типових» локальних мереж і не дозволяють реалізувати багатокритеріальне та «багаторівневе» управління в складних гетерогенних структурах.

Традиційний підхід до вирішення проблеми мережевих взаємодій припускає послідовну обробку одиниць передачі, зокрема пакетів, на кожному рівні еталонної моделі мережевої взаємодії ISO/OSI: комутатори другого рівня покликані виконувати фільтрацію та пересилку кадрів між портами на основі MAC-адресів, влучний VLAN та влучний QoS, класичні маршрутизатори використовуються для об'єднання сегментів мережі на основі IP-адресів, шлюзи забезпечують трансляцію мережевих адресів та контроль інформаційних потоків. На кожному рівні використовуються свої правила обробки (комутаційні матриці, таблиці маршрутизації, списки доступу та ін.) і різні формати даних. Сучасне мережеве устаткування дозволяє організувати управління трафіком на основі інформації декількох рівнів, що дозволяє ефективніше обробляти трафік, але істотно ускладнює апаратуру, оскільки фактично приводить до поєднання декількох пристроїв в одному, при цьому алгоритми та методи комутації третього і четвертого рівнів є в переважній більшості закритими розробками виробників і мають обмежені виробником можливості настройки.

Одним їх напрямів “модернізації” класичного підходу до організації мережевої архітектури є створення програмно-конфігурованих мереж – ПКМ (англ. Software Defined Networks - SDN), що використовують протокол OpenFlow [2].

До основних переваг мереж SDN відносять централізоване управління в мультівендорному середовищі, зменшення складності мережі за рахунок автоматизації, вищу швидкість впровадження інновацій, збільшення надійності та безпеки мережі, забезпечення узгодженості політик управління доступом, інжинірингу трафіку, параметрів якості послуг, безпеки та ін., вузько спрямоване (“точкове”) управління мережею, поліпшення якості сприйняття послуг користувачами. Передбачається, що з урахуванням вказаних переваг SDN стане новим стандартом для майбутніх мереж.

Основна ідея ПКМ полягає в тому, щоб не змінюючи існуючого мережевого устаткування відокремити (перехопити) управління цим устаткуванням (маршрутизаторами та комутаторами) за рахунок створення спеціального програмного забезпечення, яке може працювати на звичайному окремому комп'ютері, і яке знаходиться під контролем адміністратора мережі.

**Архітектура програмно-конфігурованих мереж.** Суть концепції ПКМ зводиться до розділення процесів пересилки даних (forwarding) та управління потоками (control) [3]. Безпосередньо пересилку виконують спеціальні комутатори OpenFlow на основі універсальних таблиць потоків (ТП), які формуються та підтримуються зовнішнім управляючим компонентом – контроллером мережі [4]. Ключова особливість управління ПКМ в тому, що як ТП в комутаторах, так і правила функціонування самих контролерів доступні для управління зовнішніми програмними засобами через спеціалізовані API, як показано на Рис. 1.

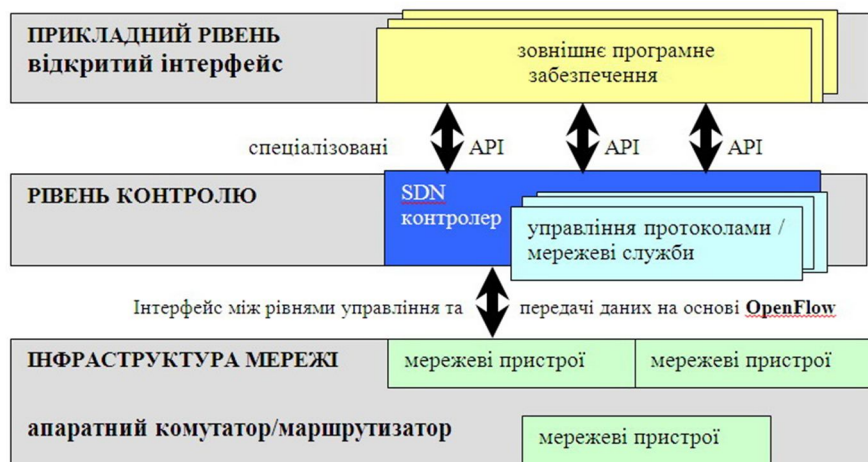


Рис. 1. Архітектура програмно-конфігурованих мереж

В архітектурі SDN можна виділити три рівні (Рис. 1):

- інфраструктурний рівень, що надає набір мережевих пристроїв (комутаторів і каналів передачі даних);
- рівень управління, що включає мережеву операційну систему, яка забезпечує додаткам мережеві сервіси та програмний інтерфейс для управління пристроями та мережею;
- прикладний рівень – для гнучкого та ефективного управління мережею – прикладні вирішення високорівневого управління мережею (засоби забезпечення безпеки, балансування навантаження, програмного міжмережевого екрану, адміністрування, виявлення вторгнень, а також функції інжинірингу трафіку, управління мобільністю, управління доступом, організації енергоефективної роботи мережі та ін.).

Виділення функції управління в окремий рівень та її делегування центральному компоненту (контролеру мережі) націлені на оптимізацію мережевих конфігурацій для вирішення прикладних завдань і, зокрема, дозволяють отримати наступні переваги:

формати даних, правила обробки та технології передачі в комутаторі не обмежені певним рівнем взаємодії, типом устаткування або виробником;

одиниця передачі може бути задана багатовимірним вектором, що включає поля з різних рівнів моделі мережевої взаємодії;

при побудові правил пересилки пакетів можуть застосовуватися методи автоматизованої корекції потоків залежно від навантаження компонентів та інших критеріїв;

контролери мережі можуть об'єднуватися в мережеві домени, які дозволяють оптимізувати та резервувати канали передачі.

Розширена функціональність ПКМ визначається не тільки розподіленим способом управління, але і структурою таблиць потоків, що містять правила пересилки трафіку. Як показано на Рис. 2, кожен запис в ТП містить шаблон пакету (поля заголовків), статистичні лічильники та набір інструкцій (дій).

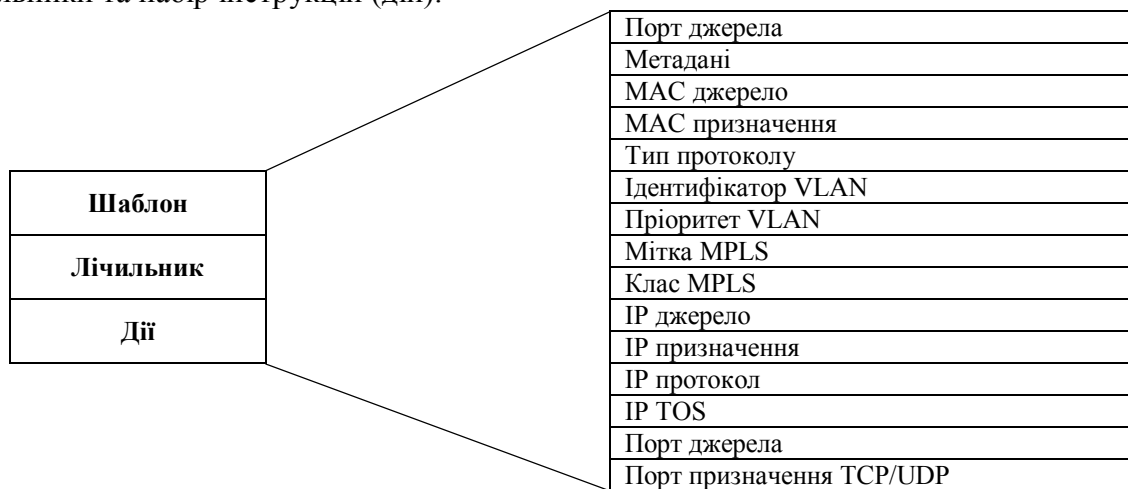


Рис. 2. Структура запису таблиці протоколів

Комутатор OpenFlow послідовно порівнює вміст передаваного кадру із записами ТП і при збігу виконує вказані в записі дії. Якщо збіг не знайдений, то залежно від налаштувань комутатора пакет може бути відкинтий або відправлений OpenFlow-запрос контролеру для ухвалення рішення. Контролер може додавати, модифікувати, видаляти записи з таблиць як на основі аналізу пакетів, що отримуються від мережевого устаткування, так і виходячи з власних алгоритмів роботи.

Специфікація OpenFlow визначає різноманітний набір інструкцій для обробки одиниць передачі, серед яких пересилка до порту(ів) або контролеру (Output), зміна полів (Set-Field, Change-TTL), робота з тегами IEEE 802.1Q та MPLS (Push-Tag/Pop-Tag), групові операції (Group) та ін. Також існує специфікація гібридного комутатора з підтримкою як OpenFlow-операцій, так і класичної комутації [4].

За допомогою протоколу OpenFlow фахівці витрачають менше часу на початкові налаштування мережі та передають її в експлуатацію в практично автоматичному режимі для підтримки заданого QoS. Всі маршрутизатори та комутатори об'єднуються під управлінням Мережевої Операційної Системи (МОС), яка забезпечує додаткам доступ до управління мережею, і яка постійно відстежує конфігурацію засобів мережі. Потік даних flow таблиць OpenFlow (OpenFlow pipeline) містить безліч flow таблиць, які можна об'єднати в деревовидні структури, що дозволяє ефективніше використовувати асоціативну пам'ять TCAM та реалізувати практично будь-які сценарії обробки і просування даних. Процес просування таблиць завжди починається з першої таблиці з номером "0", а закінчується, якщо немає вказівки на наступну flow таблицю з великим номером. Деревовидна структура

(1) будуватися за допомогою вказівки виконання номерів наступних таблиць та виконання функцій цих таблиць:

$$f_{Tn+1} = (f_{Tn-1}, \dots) + f_{Tn}; \quad (1)$$

Протокол OpenFlow вирішує також проблему залежності від мережевого устаткування якого-небудь конкретного постачальника, оскільки ПКМ (SDN) використовує загальні абстракції для пересилки пакетів, які МОС використовує для управління мережевими комутаторами. Можна сказати, що OpenFlow – це протокол нижнього рівня для програмування комутаторів.

Теоретично SDN дає можливість абсолютної гнучкості в управлінні трафіком, теоретично – легке балансування трафіку без залучення окремого приладу (устаткування). На практиці, у SDN є три великі проблеми, які вирішують всі розробники: *транспорт* від контролера до комутаторів; *стиківка* з традиційною мережею; *безпека* мережі.

Основні вимоги до SDN, запропоновані консорціумом ONF [5]:

1. Централізоване управління для мультівендорного устаткування.
2. Зниження складності налаштувань та конфігурації мережі за рахунок автоматизації настройки та конфігурації.
3. Високий рівень змінності в реальному часі для підтримки нових комерційних вимог.
4. Посилення безпеки та стабільності роботи мережі.
5. Детальний контроль мережі для служб підтримки сервісів.
6. Збір, обробка статистики мережі і управління.

За допомогою сучасних маршрутизаторів зазвичай вирішуються два основних завдання: передача даних (*forwarding*) – просування пакету від вхідного порту на певний вихідний порт та управління даними – обробка пакету та ухвалення рішення про тих, куди його передавати далі, на основі потокового стану маршрутизатору. Це відповідає рівню передачі даних, на якому зібрані засоби передачі (лінії зв'язку, канало-утворюючі устаткування, маршрутизатори, комутатори) і рівню управління станами засобів передачі даних (Рис. 3).

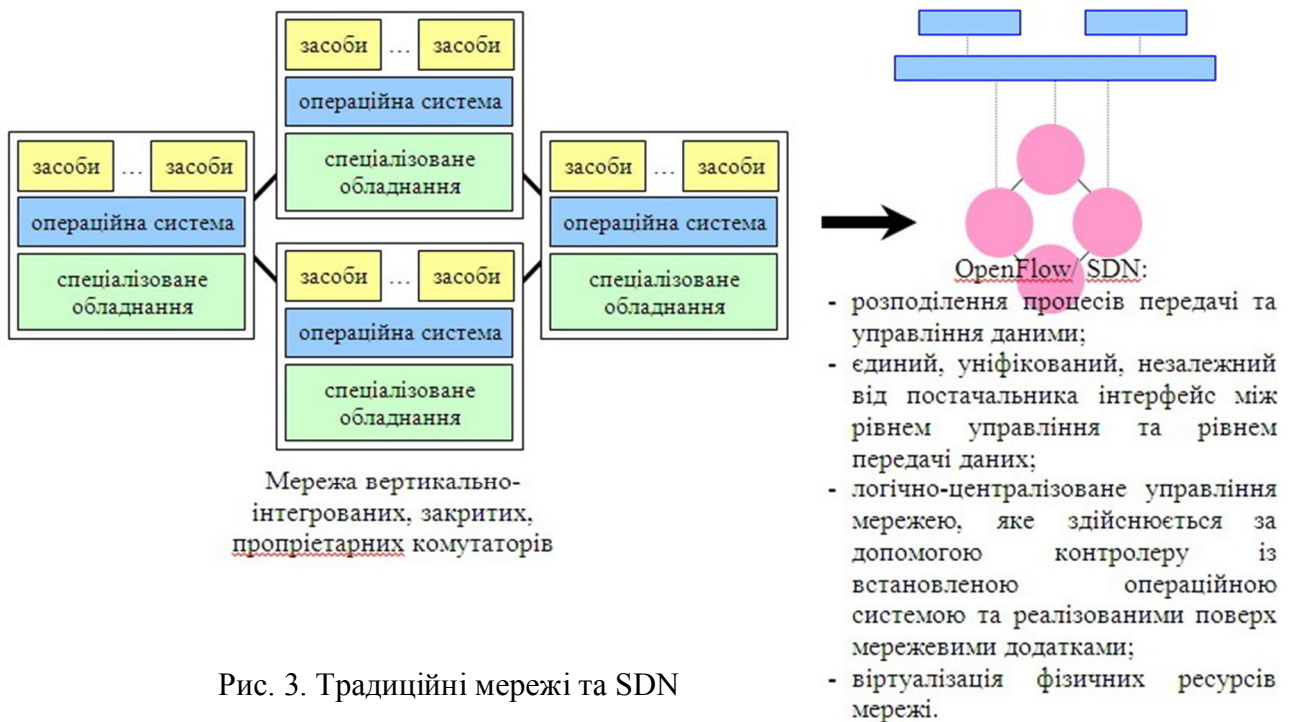


Рис. 3. Традиційні мережі та SDN

Розвиток маршрутизаторів до цих пір йшов по шляху зближення цих рівнів, проте з ухилом на передачу (апаратне прискорення, вдосконалення програмного забезпечення та впровадження нових функціональних можливостей для збільшення швидкості прийняття рішення по маршрутизації шкільного пакету), тоді як рівень управління залишався достатньо

примітивним та спирався на складні розподілені алгоритми маршрутизації та хитромудрі інструкції по конфігурації та налаштуванню мережі.

Логічно-централізоване управління даними в мережі припускає винесення всіх функцій управління мережею на окремий фізичний сервер, контролер, який знаходиться у веденні адміністратора мережі. Контролер може управляти як одним, так і декількома OpenFlow-комутаторами і містить мережеву операційну систему, що надає мережеві сервіси по низькорівневому управлінню мережею, сегментами мережі та станом мережевих елементів, а також додатки, що здійснюють високорівневе управління мережею та потоками даних.

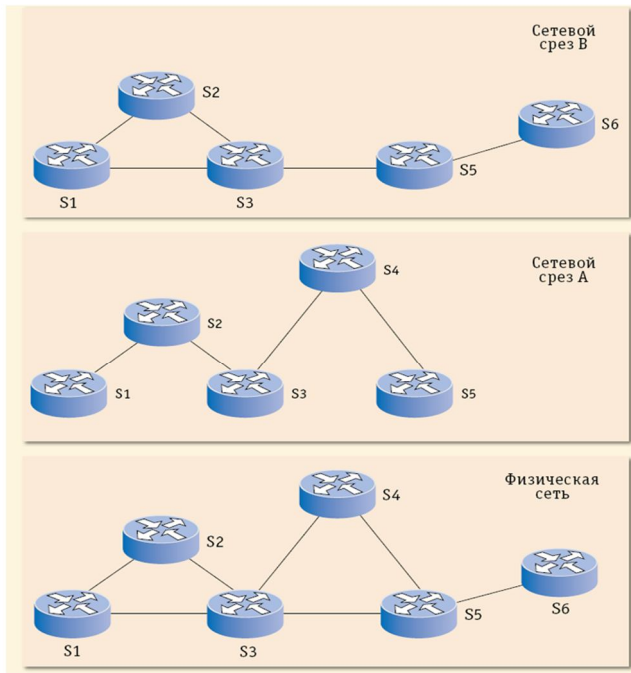


Рис. 4. Віртуалізація в SDN

Одна з ідей, що активно розвивається в рамках SDN, – це віртуалізація мереж з метою ефективнішого використання мережевих ресурсів (Рис. 4). Під віртуалізацією мережі розуміється ізоляція мережевого трафіку – групування (мультиплексування) декількох потоків даних з різними характеристиками в рамках однієї логічної мережі, яка може розділяти єдину фізичну мережу з іншими логічними мережами або мережевими зрізами (network slices). Кожен такий зріз може використовувати свою адресацію, свої алгоритми маршрутизації, управління якістю сервісів та ін.

Віртуалізація мережі дозволяє: підвищити ефективність розподілу мережевих ресурсів і збалансувати навантаження на них; ізолювати потоки різних користувачів і додатків в рамках однієї фізичної мережі; адміністраторам

різних зрізів використовувати свої політики маршрутизації і правила управління потоками даних; проводити експерименти в мережі, використовуючи реальну фізичну мережеву інфраструктуру; використовувати в кожному зрізі тільки ті сервіси, які необхідні конкретним додаткам.

**Стандартизація програмно-конфігурованих мереж.** Розробкою стандартів SDN і дослідженнями в цьому напрямі в даний час займається велике число галузевих об'єднань та міжнародних організацій, в яких беруть участь зацікавлені комерційні компанії – виробники мережевого устаткування, оператори мереж, розробники програмного забезпечення (ПЗ).

Концепція SDN активно просувається, проте її розуміння ще не устоялося, а ключові стандарти знаходяться на різних стадіях розробки та апробації, тому сьогодні загальноприйняте визначення поняття SDN відсутнє. Так, галузеві організації – Фонд відкритих мережевих технологій (Open Networking Foundation, ONF), Робоча група по інженерних завданнях Інтернет (Internet Engineering Task Force, IETF) та МСЕ-Т (Сектор стандартизації Міжнародного союзу електрозв'язку) – пропонують наступні визначення:

ONF: SDN – динамічна, керована та здатна до адаптації мережева архітектура, в якій розділені рівні управління мережею та передачі даних, що забезпечує програмне управління мережею та абстрагування/ізоляцію (рівня) мережевої інфраструктури від (рівня) додатків та мережевих послуг/сервісів [6].

IETF: SDN – підхід до побудови мереж, що забезпечує пряме управління ресурсами та мережами, а також їх розподіл за рахунок додавання власних засобів обробки, адміністрування та програмного управління за допомогою відкритих мережевих інтерфейсів і абстракції (абстрагування, ізоляції) рівня мережі [7].

МСЕ-Т: SDN – технологія побудови мереж, яка дозволяє реалізувати централізований, програмований рівень управління та ізоляцію (абстракцію) рівня даних; при цьому рівні управління та даних розділені, завдяки чому оператори мереж зв'язку можуть безпосередньо управляти своїми віртуальними ресурсами і мережами. Програмований рівень управління – рівень управління, який повинен бути програмованим і керованим централізованим чином; ізоляція (абстракція) рівня даних – моделі рівня даних повинні бути абстрактними і спрощеними, а не спеціалізованим апаратним забезпеченням [8].

Дослідженням загальних питань і стандартизацією SDN займаються ONF, IETF, Дослідницька група інтернет-технологій (Internet Research Task Force, IRTF), Європейський інститут по стандартизації в області телекомунікацій (European Telecommunications Standards Institute, ETSI) та МСЕ-Т. Представники Форуму широкосмугових мереж (Broadband Forum, BBF) вивчають деякі окремі питання побудови та експлуатації мереж SDN. В рамках робочої групи «Інноваційні послуги та ринкові вимоги» (Service Innovation & Market Requirements) виділений проект SD-313 – комерційні вимоги та структура SDN в широкосмугових телекомунікаційних мережах (Business Requirements and Framework for SDN in Telecommunication Broadband Networks). Проект припускає проведення досліджень в області сценаріїв переходу до мереж SDN, включаючи варіанти підтримки SDN частиною устаткування, а також впровадження функціональності SDN при оновленні ПЗ.

Окремі питання стосовно SDN розглядаються і учасниками Форуму оптичної міжмережевої взаємодії (Optical Internetworking Forum, OIF). Ця некомерційна організація, яка розробляє угоди по реалізації (Implementation Agreement, IA) для устаткування оптичних мереж, оцінює концепцію SDN як перспективну і займається розробкою вимог до SDN в частині транспортних мереж з боку операторів (оптичних) мереж і постачальників послуг, структури SDN та її співвідношення з архітектурою оптичних мереж з автоматичною комутацією (Automatically Switched Optical Network, ASON), а також демонстрацією і тестуванням SDN.

Вимоги OIF до SDN з погляду операторів транспортних мереж включають:

- функції рівня управління транспортної мережі SDN;
- функціональні вимоги до оркестратора, що координує функції та служби на різних рівнях транспортної мережі і з кінця в кінець в суміжних доменах SDN;
- співвідношення рівнів SDN в транспортній мережі – рівня передачі даних, управління, адміністрування та оркестровки.

Апробацією стандартів, що розробляються, та розробкою відкритих рішень SDN займаються декілька організацій:

OpenDaylight – об'єднання галузевих виробників, включаючи IBM, Juniper Networks, Cisco, Red Hat, VMware, Citrix, Ericsson, Microsoft, NEC, Big Switch Networks, Brocade Communications Systems. Метою проекту є створення єдиної відкритої платформи SDN, розробка відкритої структури класів (фреймворка) в якості основа для створення готових продуктів та сервісів різними учасниками ринку;

Open vSwitch – проект з розробки програмного комутатора SDN з відкритим початковим кодом для застосування у віртуалізованому мережевому середовищі. У проекті беруть участь компанії Citrix, Red Hat, Canonical, Oracle, FreeBSD Foundation, Nicira;

OpenStack – проект з розробки комплексу безкоштовних відкритих програмних засобів для створення хмарної обчислювальної інфраструктури та сховищ даних, що включає підтримку SDN. У проекті представлені компанії AT&T, AMD, Brocade Communications Systems, Canonical, Cisco, Dell, EMC, Ericsson, Groupe Bull, HP, IBM, Inktank, Intel, NEC, Rackspace Hosting, Red Hat, SUSE Linux, VMware, Yahoo!.

Основних напрямів стандартизації та розробки, стандартизуючі організації, об'єднання галузевих виробників та проекти з розробки відкритого ПЗ представлені в [9].

ONF, як родоначальник SDN, ставить за мету формування нової архітектури мережі та устаткування, що припускає відділення площини управління від площини передачі, і докладає значні зусилля до подолання виникаючих проблем, пов'язаних із складнощами

міграції від традиційних мереж до SDN і з труднощами стандартизації площини передачі із-за перешкод з боку провідних світових виробників устаткування.

IETF слідує в сторону SDN іншим шляхом, додаючи властивості відкритих інтерфейсів в існуючу архітектуру та захищаючи, таким чином, вкладені інвестиції. Недоліками при цьому є обмежена відкритість та значне ускладнення мережі, оскільки устаткування повинне підтримувати старі та нові технічно/технологічні рішення.

ETSI, маючи спеціалізовану групу ISG для стандартизації NFV, зосереджує значні зусилля на доказовій базі спроможності концепції. При цьому відома проблема продуктивності функціонування визначає реалізацію мережевих функцій на промислових серверах, хоча створення спеціалізованого устаткування для NFV також актуально.

Метою OpenStack є створення хмарної операційної системи для оркестровки обчислень, зберігання, реалізації мережевих функцій. У цьому напрямі досягнутий значний прогрес, проте потрібний час для того, щоб перетворити цю систему на готове, зокрема в комерційному плані, рішення.

Таким чином, створення ПКМ дозволить відокремити рівень управління мережевим устаткуванням від рівня управління передачею даних, створити програмно-керований інтерфейс між мережевими додатками та транспортним середовищем та перейти від управління окремим устаткуванням до управління мережею в цілому.

### **Література**

1. Software-Defined Networking: The New Norm for Networks [Electronic resource] / ONF. – 2012. – Mode of access: <https://www.opennetworking.org/images/stories/downloads/white-papers/wp-sdn-newnorm.pdf>. -Date of access: 05.04.2013.
2. Олизарович Е. В. Метод автоматизации построения программно-конфигурируемых сетей / Е. В. Олизарович Е.В., А. И. Бражук // Вестник Гродзенского государственного университета им. Я.Купалы. – 2013. – №3(159). – С. 128-134.
3. Смелянский Р. В. Программно-конфигурируемые сети [Электронный ресурс] / Р. В. Смелянский // Открытые системы. – 2012. – №9. . – Режим доступа: <http://www.osp.ru/os/2012/09/13032491>. - Дата доступа: 05.04.2014.
4. OpenFlow Switch Specification Version 1.2 [Электронный ресурс] / ONF. - 2012. - Режим доступа: –<https://www.opennetworking.org/images/stories/downloads/specification/openflow-spec-v1.2.pdf>. – Дата доступа: 15.08.2014.
5. Software-defined networking: the new norm for Networks [Электронный ресурс] / (ONF White Paper April 13, 2012). – 2012. // – Режим доступа: [https://www.opennetworking.org/publications/whitepaper/13/04/2012/sdn-new\\_norm.pdf](https://www.opennetworking.org/publications/whitepaper/13/04/2012/sdn-new_norm.pdf). – Дата доступа: 22.03.2013.
6. Software-Defined Networking (SDN) Definition [Электронный ресурс] / ONF. // – Режим доступа: <https://www.open-networking.org/sdn-resources/sdn-definition>. – Дата доступа: 07.03.2014.
7. Draft Formal Specification: Framework for Software-De-fined Networks (SDN) / IETF. – 02/2013. [Электронный ресурс] // – Режим доступа: <https://tools.ietf.org/html/draft-shin-sdn-formal-specification-03>. – Дата доступа: 07.03.2014.
8. Framework of Telecom SDN (Software-Defined Networking): ITU-T Draft Recommendation Y.FNsdn, 02/2013.
9. Egawa T. SDN standardization Landscape from ITU-T Study Group 13 // ITU Workshop on SDN Geneva, Switzerland, 4 June 2013.