УДК 004.77
Зуй М.С.[1], Тягунова М.Ю.[2], Киричек Г.Г.[2]
[1] студ. гр. КНТ-514м НУ «Запорізька Політехніка»
[2] канд. техн. наук, доц. НУ «Запорізька Політехніка»

# ЗАСТОСУВАННЯ СУЧАСНИХ ТЕХНОЛОГІЙ ПРИ РОЗРОБЦІ МЕРЕЖЕВИХ ІНФРАСТРУКТУР

У сучасному цифровому світі функціонування будь-якої організації нерозривно пов'язане з наявністю стабільної, масштабованої та захищеної мережевої інфраструктури. Зростання обсягів даних, розвиток хмарних технологій, інтернету речей (IoT), віддаленого доступу та цифрових сервісів вимагає від мереж нових підходів до проєктування та управління. У зв'язку з цим дедалі більшого поширення набувають такі технології, як програмно-налаштовані мережі (SDN), віртуалізація мережевих функцій (NFV), хмарні обчислення, IoT-платформи та системи забезпечення кібербезпеки.

Програмно-налаштовані мережі (SDN) є одним із найважливіших напрямів розвитку сучасної інфраструктури [1]. Вони дозволяють централізовано керувати мережею, відокремлюючи логіку управління від фізичних пристроїв. Це забезпечує більшу гнучкість, спрощує налаштування, розширення мережі та дозволяє швидко впроваджувати нові сервіси. SDN активно використовується у великих дата-центрах, корпоративних мережах, а також при побудові інфраструктур на основі хмарних рішень.

Віртуалізація мережевих функцій (NFV) — це підхід, за якого функції, що раніше реалізовувалися виключно апаратними засобами (наприклад, маршрутизатори, фаєрволи, балансувальники навантаження), замінюються програмними модулями. Це дозволяє уникнути значних капітальних витрат на обладнання, пришвидшити розгортання нових сервісів та забезпечити масштабованість. NFV у поєднанні з SDN відкриває нові горизонти для гнучкої та динамічної мережевої архітектури.

Ще одним потужним інструментом є хмарні обчислення, які зміщують акцент з локальної інфраструктури на розподілену. Інтеграція з провайдерами хмарних сервісів (AWS, Google Cloud, Azure) дозволяє підприємствам зберігати, обробляти й аналізувати великі обсяги даних без потреби в потужному локальному обладнанні. Це критично важливо для компаній, які працюють у гібридному або повністю дистанційному форматі, де наявність доступу до централізованих ресурсів у реальному часі є життєво необхідною умовою [2].

Важливою складовою є також інтернет речей (IoT), який формує новий клас мереж, де взаємодіють датчики, пристрої збору та передавання інформації, модулі керування. Інтернет речей (IoT) – це концепція, за якої фізичні об'єкти оснащуються датчиками, програмним забезпеченням та

іншими технологіями для обміну даними з іншими пристроями та системами через мережу. Наприклад, у сфері "розумного дому" популярними є термостати Nest, системи безпеки як Ring або розумне освітлення Philips Hue, які дозволяють керувати параметрами житла дистанційно. В промисловості IoT реалізовано через системи моніторингу обладнання в реальному часі, такі як платформи від Siemens, що дозволяють виявляти потенційні збої і проводити профілактичне обслуговування. У сільському господарстві застосовують IoT-рішення, наприклад, системи зрошення, які на основі даних про вологість ґрунту автоматично регулюють подачу води.

Такі системи мають багато переваг. Завдяки автоматизації процесів зменшуються витрати часу та ресурсів, наприклад, у промислових системах можна знизити простій обладнання. Розумні пристрої дозволяють здійснювати дистанційний контроль та управління, що забезпечує високий рівень комфорту у побуті і бізнесі. IoT-платформи дозволяють оперативно реагувати на зміни умов, що критично для оперативного прийняття рішень, наприклад, у сільському господарстві чи логістиці.

Проте залишаються і певні недлоліки подібних систем, наприклад, питання безпеки та залежність від стабільності мережі. Збільшення кількості підключених пристроїв створює більше потенційних точок доступу для кібератак. Різноманітність стандартів та протоколів може ускладнювати інтеграцію різних пристроїв в єдину мережу. Наявність великої кількості пристроїв підвищує вимоги до надійності та стабільності мережевого з’єднання.

Таким чином, IoT надає значні можливості для оптимізації процесів і покращення якості життя, проте для повноцінного використання цієї технології необхідно вирішувати питання безпеки та сумісності пристроїв.

Однак розвиток складних мережевих архітектур потребує особливої уваги до питань кібербезпеки. Збільшення кількості підключених пристроїв, обсягів переданих даних і використання віддалених платформ створює численні потенційні вектори атак. У цьому контексті важливим є впровадження сучасних засобів шифрування, механізмів багаторівневої автентифікації, систем виявлення вторгнень (IDS/IPS), безпечного управління доступом (Zero Trust) та постійного моніторингу мережевого трафіку.

Отже, інтеграція сучасних технологій у процес проєктування, розгортання та обслуговування мережевих інфраструктур є ключем до побудови ефективних, безпечних і адаптивних систем. Застосування SDN, NFV, хмарних платформ, IoT-рішень та інструментів автоматизації дозволяє відповідати сучасним викликам цифрової трансформації. Для молодих фахівців знання й уміння працювати з такими технологіями стають не просто конкурентною перевагою, а необхідною умовою успішної професійної діяльності.

## СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Ram A., Analysis of Software-Defined Networking (SDN) / Ram A., Chakraborty Sw. K. // Performance in wired and wireless networks across various topologies, including single, linear, and tree structures. Indian Journal of Information Sources and Services. - 2024. – № 14. P. 39-50.

2. Киричек Г.Г., Реалізація технологій для розгортання програм у контейнері. / Киричек Г.Г., Тягунова М.Ю., Смірнов В.В. // Таврійський науковий вісник. Серія: Технічні науки. – 2023. – №6. – С.26-34. DOI: https://doi.org/10.32782/tnv-tech.2023.6.4