

УДК 004.7:004.056

ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ КОРПОРАТИВНИХ СИСТЕМ НА ОСНОВІ ТЕХНОЛОГІЇ SD-WAN

Андрій ІВАНУСА, Андрій ПЕТРОВИЧ, Мар'ян ТКАЧ, Юрій ТКАЧ

Львівський державний університет безпеки життєдіяльності

Анотація. У роботі розглянуто впровадження технології SD-WAN для модернізації корпоративної мережі підприємств енергетичного сектору. Проаналізовано переваги програмно-визначальних мереж над традиційними MPLS-каналами, зокрема в аспектах кібербезпеки, автоматизації управління та інтеграції з хмарними сервісами. Описано етапи реалізації проекту на прикладі підприємства енергетики для забезпечення кіберстійкості інфраструктури.

Ключові слова: SD-WAN, інформаційна безпека, корпоративна мережа, автоматизація, хмарні технології.

Abstract. The paper considers the implementation of SD-WAN technology to modernize the corporate network of energy sector enterprises. The advantages of software-defined networks over traditional MPLS channels are analyzed, in particular in the aspects of cybersecurity, management automation, and integration with cloud services. The stages of project implementation are described using the example of an energy enterprise to ensure cyber resilience of the infrastructure.

Keywords: SD-WAN, information security, corporate network, automation, cloud technologies.

Глобальні мережі протягом тривалого часу залишаються критично важливим елементом розвитку технологій, забезпечуючи передачу даних на великі відстані як для військових, так і для корпоративних потреб. Здатність долати географічні обмеження стала рушійною силою вдосконалення систем захисту інформації. Однак традиційні підходи, такі як використання виділених каналів MPLS, перестають відповідати вимогам сучасного хмарного середовища, яке швидко розвивається. Це зумовило появу та активне впровадження програмно-визначальних глобальних мереж (SD-WAN), що дозволяють шифрувати дані в накладених тунелях та забезпечують гнучкість управління трафіком.

Технологія дозволяє об'єднувати різні типи фізичних з'єднань, такі як широкосмуговий інтернет, 4G LTE та MPLS, у єдиний логічний канал зв'язку для підвищення відмовостійкості. Це створює надійну віртуальну надбудову, яка відокремлює програмне забезпечення від фізичного обладнання та забезпечує безперервність сервісів навіть при збоях окремих ліній.

На відміну від традиційної архітектури, модель SD-WAN розроблена для повної підтримки програм, розміщених у локальних центрах обробки даних, а також у публічних і приватних хмарах. Технологія дозволяє

автоматично та динамічно перенаправляти трафік найбільш ефективним шляхом, враховуючи умови мережі, вимоги безпеки та якості обслуговування (QoS). Важливою перевагою є централізоване керування, що підвищує продуктивність додатків та знижує витрати на ІТ-інфраструктуру. Здатність ідентифікувати підозрілі програми та віртуалізувати послуги WAN, включаючи MPLS та 4G/LTE, дозволяє підприємствам безпечно використовувати широкосмуговий зв'язок як основний канал передачі даних.

Завдяки підтримці ініціалізації без участі користувача (Zero Touch Provisioning), конфігурація нових пристроїв завантажується автоматично одразу після підключення до мережі. Такий підхід усуває необхідність фізичної присутності кваліфікованих інженерів на кожній локації, що скорочує час запуску нових філій з кількох днів до лічених годин.

Особливої актуальності впровадження SD-WAN набуває для стратегічно важливих підприємств, таких як Група ДТЕК, що працюють в умовах підвищених ризиків воєнного часу. Складність мережевої інфраструктури та організаційна розгалуженість компанії вимагають підвищення надійності підключення для сотень територіально розподілених філій. Модернізація корпоративної мережі на базі рішення VMware SD-WAN дозволяє уніфікувати підключення, забезпечити гнучку взаємодію з хмарними середовищами та автоматизувати рутинні завдання керування.

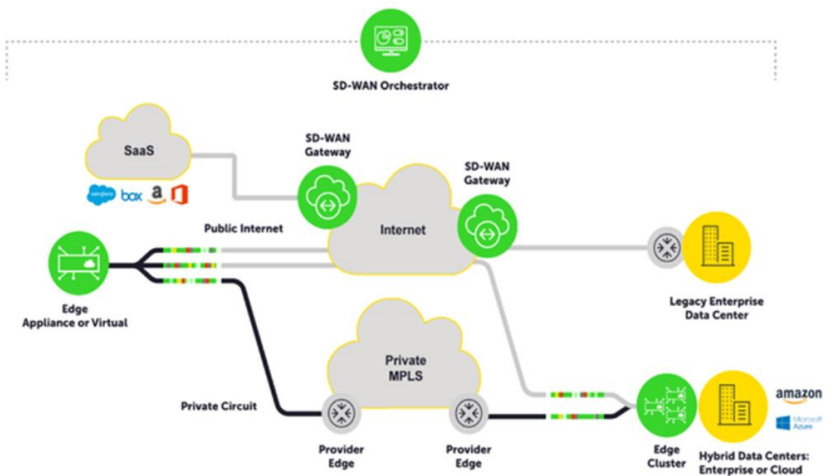


Рисунок 1 – Архітектура рішення SD-WAN

Система здатна автоматично розпізнавати та пріоритизувати чутливий до затримок трафік, зокрема для засобів відеоконференцзв'язку та платформи Microsoft Teams. Це дозволяє забезпечити стабільно високу якість

уніфікованих комунікацій для ефективної взаємодії територіально розподілених команд незалежно від їхнього розташування.

Проект імплементації включає повний життєвий цикл: від аналізу потреб та проектування до впровадження пілотного рішення та інтеграції з існуючими системами безпеки. В результаті впровадження програмно-конфігурованої архітектури компанія отримує гнучку мережу, що легко масштабується, спрощене централізоване керування та можливість швидкого підключення нових філій. Це критично важливо для ефективної роботи розподілених команд та забезпечення безперервності бізнес-процесів в енергетичному секторі, який є критичною інфраструктурою для України.

Ключовим аспектом нової архітектури є підвищення рівня кібербезпеки. Мережа забезпечує повну видимість трафіку, підтримку сучасних методів шифрування та сегментацію для мінімізації збитків у разі порушень периметра. Окрім того, автоматизація процесів дозволяє усунути ризики, пов'язані з людським фактором, та звільнити ресурси IT-фахівців для стратегічних проектів розвитку. Таким чином, перехід на SD-WAN є комплексним рішенням, що забезпечує не лише технічну модернізацію, але й стратегічну стійкість та безпеку корпоративних систем.

Література

1. Goransson P., Black C., Culver T. Software Defined Networks: A Comprehensive Approach. 2nd ed. Morgan Kaufmann, 2016. 436 p.
2. Kerravala Z. The width and breadth of software-defined WAN. Network World. 2018. URL: <https://www.networkworld.com/article/3268802/the-width-and-breadth-of-software-defined-wan.html> (дата звернення: 11.11.2025).
3. Troia S. et al. SD-WAN: An Enabler for Network Function Virtualization and Software Defined Networking. IEEE Communications Magazine. 2020. Vol. 58, no. 5. P. 98–104.
4. Стенлі Д. Віртуалізація мережевих функцій та SD-WAN: революція у корпоративних комунікаціях. Кібербезпека та комп'ютерна інженерія. 2021. № 2(34). С. 45–52.
5. VMware SD-WAN Security Architecture : White Paper. VMware, Inc., 2022. 18 p. URL: <https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/sd-wan/vmware-sd-wan-security-architecture-wp.pdf> (дата звернення: 11.11.2025).