

УДК 004.7:338

ПОРІВНЯЛЬНИЙ АНАЛІЗ ТЕХНОЛОГІЙ ДЛЯ ОРГАНІЗАЦІЇ МЕРЕЖІ ДОСТУПУ ПІДПРИЄМСТВА КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Кузьмін А.А., Колтун Ю.М.

email: artem.kuzmin@nure.ua; yurii.koltun@nure.ua

Харківський національний університет радіоелектроніки, каф. ІМІ
м. Харків, Україна

This work is devoted to the comparative analysis of technologies for organizing access networks in critical infrastructure enterprises. Various approaches, including wired and wireless solutions, were considered. The study examines the advantages and disadvantages of Ethernet, fiber-optic networks, Wi-Fi, LTE, and 5G technologies. A comparative assessment of security, reliability, and deployment costs was conducted. It has been found that hybrid solutions combining wired and wireless networks provide the most balanced approach, ensuring both high performance and flexibility while maintaining the necessary level of security.

Підприємства критичної інфраструктури мають забезпечувати важливі життєві функції суспільства, економіки та національної безпеки держави, тому однією з важливих задач їх функціонування є організація ефективних мереж доступу (МД), що будуть забезпечувати надійну безпеку їх внутрішніх інформаційних ресурсів та безпечний доступ до зовнішніх ресурсів [1]. Мережа доступу у такому підприємстві повинна мати високі продуктивність, відмовостійкість, захищеність від кіберзагроз, а також бути гнучкою та масштабованою. Вона повинна включати резервовані канали зв'язку, багаторівневу автентифікацію, шифрування трафіку та засоби моніторингу мережевої безпеки, щоб забезпечити стабільне функціонування критично важливих систем і мінімізувати ризики несанкціонованого доступу. Первісно, при визначенні підходів щодо організації такого типу МД має проводитися порівняльний аналіз різних технологій, у процесі якого визначаються найбільш прийнятні загальні рішення для забезпечення стабільного та захищеного мережного доступу.

Зокрема у роботі в рамках такого порівняльного аналізу були розглянуті оптичні технології доступу, такі як GPON, що забезпечує високу швидкість передачі даних при мінімальному використанні активного обладнання; EPON, яка використовує стандартні протоколи Ethernet та відзначається гнучкістю масштабування; DWDM, що дозволяє передавати великі обсяги даних на значні відстані завдяки ущільненню каналів за довжиною хвилі; CWDM, як більш економічно вигідний варіант DWDM для середніх і малих мереж.

Крім того, у роботі були досліджені технології бездротового доступу, такі як Wi-Fi, LTE, 5G, що забезпечують високу швидкість передачі даних,

гнучкість розгортання, підтримку мобільних користувачів, масштабованість мережі та зниження витрат на кабельну інфраструктуру.

Проведений аналіз та дослідження були спрямовані перш за все на визначення переваг і недоліків цих технологій та на обґрунтування гібридних рішень на їх основі для організації ефективної мережі доступу підприємства критичної інфраструктури, що в аспекті зазначених вище показників є актуальною задачею. Зокрема такі гібридні рішення технологій кабельних і бездротових мереж, як GPON + Wi-Fi 6, Ethernet + 5G та SD-WAN + LTE, – дозволяють гнучко досягти балансу між безпекою, продуктивністю та мобільністю користувачів.

У процесі зробленого порівняльного аналізу було показано, що з точки зору захищеності інформації внутрішніх ресурсів, для організації фізичних ліній мережі доступу доцільно використовувати технології, що орієнтовані на підтримку оптичного середовища. Зокрема GPON або FTTx. Було показано, що ці технології є найбільш захищеними від зовнішніх факторів, таких як електромагнітні завади, несанкціоновані підключення, радіочастотні перехоплення, а також від атмосферних впливів (грози, вітру), механічних пошкоджень у порівнянні з мідними кабелями, та впливу високочастотного випромінювання, яке може спричиняти завади в традиційних мережах.

Також аналіз показав, що для підвищення масштабованості і гнучкості мережі доступу доцільно використовувати бездротовий доступ, наприклад, технології Wi-Fi 6, LTE, 5G та WiMAX. Однак, для забезпечення належного рівня захищеності необхідно застосовувати такі механізми, як шифрування трафіку (WPA3, IPSec, AES), багаторівнева автентифікація (2FA, цифрові сертифікати), VPN-тунелювання, сегментація мережі (VLAN, SDN), виявлення та запобігання атак (IDS/IPS), а також регулярний моніторинг безпеки та оновлення програмного забезпечення.

Використання вищезазначених технологічних рішень сприяє стабільному функціонуванню інфраструктури підприємства та гарантує надійний доступ до внутрішніх і зовнішніх мережних ресурсів.

Список використаних джерел:

1. Міністерство цифрової трансформації України : вебсайт. URL: <https://thedigital.gov.ua/> (дата звернення: 28.02.2025).
2. Жураковський Є. І., Ковальов О. В. Мережеві технології : навч. посіб. Київ : Видавничий дім «Кондор», 2020. 256 с.
3. Павленко В. М., Олійник Р. П. Аналіз сучасних бездротових технологій зв'язку для критичних інформаційних систем // Вісник НТУУ «КПІ». Серія «Інформатика та обчислювальна техніка». 2021. № 3. С. 45–52.