КОНЦЕПЦІЯ ZERO TRUST В АРХІТЕКТУРІ БЕЗПРОВОДОВИХ СИСТЕМ

Куля Ю.Е.

Кафедра інфокомунікаційної інженерії ім. В.В. Поповського,
Харківський національний університет радіоелектроніки,
Україна

E-mail: yuliia.kulia@nure.ua

Abstract

This article examines the principles and practical application of the Zero Trust concept in the architecture of modern wireless communication systems. It emphasizes that traditional perimeter security models are becoming ineffective in the context of distributed networks and the growing number of connected devices. The Zero Trust concept is based on constant authentication, the principle of least privilege, and continuous monitoring of user and device behavior. Particular attention is paid to the integration of the Zero Trust model into 5G and Wi-Fi 6 network architectures, including the use of ZTNA, SDN, NFV, and edge computing technologies. The paper presents the benefits and challenges of implementation, as well as practical recommendations for building a secure next-generation wireless infrastructure. Implementing Zero Trust increases system resilience to cyberattacks, ensures reliable data protection, and creates the foundation for secure sixth-generation (6G) networks.

Сучасні безпроводові мережі від корпоративних Wi-Fi до глобальних інфраструктур 5G стають ключовим елементом цифрової взаємодії, забезпечуючи безперервний доступ до даних і сервісів. Однак відкрита природа радіосередовища робить такі системи вразливими до широкого спектру загроз: від перехоплення трафіку та підробки ідентичності до складних кібератак на інфраструктурний рівень [1].

Традиційні підходи до мережної безпеки, засновані на периметральному захисті (trust but verify), перестали відповідати реаліям розподілених і мобільних архітектур. У цих умовах ключового значення набуває концепція Zero Trust (ZT) – модель «нульової довіри», орієнтована на постійну перевірку кожного суб'єкта та кожної транзакції у мережі.

Zero Trust припускає, що будь-який користувач, пристрій чи сервіс не може вважатися довіреним за умовчанням, незалежно від його розташування – всередині або за межами корпоративного контуру. Цей підхід є особливо актуальним для безпроводових систем, де фізична межа мережі фактично відсутня, а кількість підключень зростає експоненційно.

Основна концепція Zero Trust

Концепція Zero Trust була вперше сформульована Джоном Кіндевегом (John Kindervag, Forrester Research, 2010) і згодом розвинена Національним інститутом стандартів та технологій США (NIST SP 800-207, 2020). Її фундаментальні принципи включають.

1. Постійна перевірка ідентичності (Continuous Authentication), коли кожен пристрій та користувач повинні проходити ідентифікацію під час кожного запиту до ресурсу. Використовуються багатофакторна автентифікація (MFA), біометрія та механізми контекстної оцінки ризику.

2. Мінімізація прав доступу (Least Privilege Access), при яких користувач отримує доступ лише до тих ресурсів, які справді необхідні виконання його завдань. У безпроводових мережах це реалізується через сегментацію та мікросегментацію трафіку (microsegmentation).

3. Моніторинг та аналіз поведінки (Behavioral Analytics), ця система постійно аналізує мережну активність, виявляючи аномалії. Алгоритми машинного навчання дозволяють виявляти нехарактерні дії користувачів та пристроїв у реальному часі.

4. Шифрування та контроль даних, тут вся передача даних у бездротовому середовищі повинна здійснюватись у зашифрованому вигляді (наприклад, через WPA3, TLS 1.3, IPsec). Додатково впроваджуються політики контролю та маркування даних (Data Loss Prevention) [2], (рис.1).

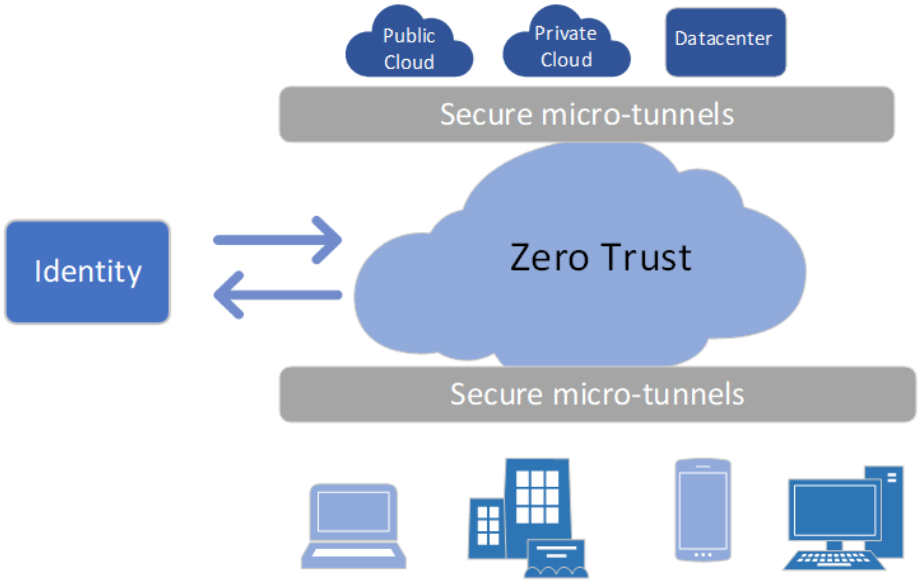

Рис. 1. Основна концепція Zero Trusty

Архітектура Zero Trust у безпроводових системах

Застосування Zero Trust у безпроводових системах передбачає трансформацію їхньої архітектури від статичної, ієрархічної моделі до динамічної, контекстно керованої структури.

Рівень доступу

На рівні доступу реалізуються такі механізми як, 802.1X та EAP-TLS для безпечної автентифікації пристроїв; використання цифрових сертифікатів та центру сертифікації (PKI); динамічне призначення VLAN та політик залежно від профілю пристрою.

Приклад: при підключенні ноутбука співробітника система перевіряє сертифікат, геолокацію, версію ОС, наявність антивіруса і лише після цього дозволяє доступ до корпоративних ресурсів.

Рівень управління та аналітики

Централізований контролер Zero Trust Network Access (ZTNA) забезпечує: збирання телеметрії від усіх точок доступу (Access Points); аналіз поведінки користувачів; динамічне оновлення політик безпеки в режимі реального часу.

ZTNA інтегрується з системами SDN (Software-Defined Networking) та SIEM (Security Information and Event Management), що дозволяє централізовано керувати безпекою бездротової інфраструктури.

Рівень додатків та даних

На прикладному рівні застосовуються технології: Identity-Aware Proxy (IAP) – забезпечує перевірку користувача перед доступом до хмарних програм; Zero Trust Application Gateway – сегментує доступ між сервісами; CASB (Cloud Access Security Broker) – контролює взаємодію із зовнішніми SaaS-платформами.

Впровадження Zero Trust в архітектурі 5G та Wi-Fi 6

Сучасні стандарти безпроводових систем – 5G, Wi-Fi 6/6E – вже передбачають можливість інтеграції з Zero Trust-моделлю.

В архітектурі 5G Core елементи безпеки реалізовані у вигляді сервісних функцій (Network Security Functions), які забезпечують: ідентифікацію та аутентифікацію пристроїв (AUSF, SEPP); шифрування даних користувача (UPF Encryption); ізоляцію зрізів мережі (Network Slicing Security) та контролює взаємодії між сервісами через Service-Based Architecture (SBA) [4].

У мережах Wi-Fi 6 концепція Zero Trust проявляється через: індивідуальну аутентифікацію клієнтів (OFDMA+WPA3-Enterprise); динамічне керування політиками доступу та інтеграцію із корпоративними ZTNA-контролерами.

Таким чином безпроводові технології наступного покоління не просто підтримують Zero Trust, а спочатку проектуються з урахуванням її вимог.

Переваги та недоліки реалізації

До переваг можна віднести:
- суттєве зниження ризику компрометації мережі під час витоку облікових даних;
- можливість централізованого управління політиками та аудиту;
- покращення безпеки IoT-пристроїв з обмеженими ресурсами;
- підтримка гібридних середовищ (on-premises+cloud).

Недоліки:
- підвищена складність впровадження та налаштування політик безпеки;
- необхідність оновлення застарілих пристроїв, які не підтримують ZT;
- можливе збільшення затримок під час багаторівневої автентифікації;
- вимоги до постійної доступності інфраструктури керування ідентичністю.

Практичні рекомендації щодо впровадження

Щодо рекомендацій по впровадженню концепції Zero Trust, то розпочати можна з інвентаризацію пристроїв та сегментації бепроводової мережі. Реалізації централізованої системи ідентифікації (SSO+MFA). Використовувати автоматизований контроль відповідності пристроїв безпеці [5-6]. Спробувати інтегрувати рішення ZTNA, SDN, SIEM та CASB у єдину екосистему та впровадити постійний моніторинг та машинне навчання для виявлення аномалій.

Висновок

Концепція Zero Trust стає невід'ємним елементом архітектури сучасних безпроводових систем, забезпечуючи високий рівень захищеності в умовах складності мережевих взаємодій. Відмова від периметральної моделі та перехід до безперервної перевірки довіри дозволяє організаціям створювати адаптивні, самозахищені мережі, стійкі до зовнішніх та внутрішніх загроз.

В майбутньому у Zero Trust є великі шанси стати ключовою ланкою в проектуванні безпечних безпроводових систем шостого покоління (6G) та корпоративних мереж нового типу.

Література

1. NIST SP 800-207. Zero Trust Architecture [Електронний ресурс] / National Institute of Standards and Technology. – Gaithersburg : NIST, 2020. – 59 с. – URL: https://nvlpubs.nist.gov/nistpubs/Special-Publications/NIST.SP.800-207.pdf (дата звернення: 28.10.2025).
2. Kindervag, J. No More Chewy Centers: Introducing the Zero Trust Model of Information Security [Електронний ресурс] / J. Kindervag // Forrester Research. – 2010. –URL: https://media.paloaltonetworks.com/documents/Forrester-No-More-Chewy-Centers.pdf (дата звернення: 28.10.2025).
3. Cisco Systems. *Zero Trust for Wireless Networks.* White Paper, 2023.
4. IEEE Communications Magazine. *Zero Trust in 5G and Beyond.*, 2024.
5. Microsoft Security. *Zero Trust Deployment Guide.*, 2022.
6. Palo Alto Networks. *Implementing Zero Trust in Wireless and IoT Environments.*, 2023.