

УДК 621.391

**ІНФОРМАЦІЙНА БЕЗПЕКА В НАДШИРОКОСМУГОВИХ
МОБІЛЬНИХ МЕРЕЖАХ: ЗАБЕЗПЕЧЕННЯ ЯКОСТІ
ОБСЛУГОВУВАННЯ ТА ЕКОНОМІЧНО ЕФЕКТИВНЕ
ВПРОВАДЖЕННЯ**

**INFORMATION SECURITY IN ULTRA-WIDEBAND MOBILE
NETWORKS: ENSURING QUALITY OF SERVICE AND COST-
EFFECTIVE IMPLEMENTATION**

*К.А. Трубчанінова, докт. техн. наук, професор
Л.В. Голейчук, аспірант*

Український державний університет залізничного транспорту (м. Харків)

*K.A. Trubchainova, D. Sc. (Techn.), Professor
L.V. Goleichuk, postgraduate student*

Ukrainian State University of Railway Transport (Kharkiv)

У роботі розглянуто питання забезпечення інформаційної безпеки в системах надширокосмугового мобільного зв'язку (UWB) з урахуванням вимог до якості обслуговування (QoS) і фінансової ефективності впровадження відповідних рішень. Проаналізовано сучасні методи захисту на різних рівнях моделі OSI, особливості їх реалізації у мережах UWB, та визначено напрямки оптимізації систем з метою забезпечення надійного захисту інформації при мінімізації негативного впливу на продуктивність і вартість обслуговування.

У сучасних телекомунікаційних системах зростає роль технологій надширокосмугового зв'язку (Ultra-Wideband, UWB), що використовуються у таких сферах, як Інтернет речей (IoT), розумні будинки, медичні сенсорні системи, позиціонування в реальному часі та ін. Завдяки широкому спектру частот і низькій енергоспоживаності UWB забезпечує високу швидкість передачі на малих відстанях із стійкістю до перешкод. Однак безпека таких систем часто залишається вразливою через обмежені обчислювальні ресурси пристроїв та складність забезпечення криптографічного захисту без шкоди для QoS.

В цьому контексті, розглянуто дві основні категорії методів захисту. Методи безпеки на фізичному рівні, зокрема хаотичне модуляційне кодування, застосування псевдовипадкових послідовностей імпульсів, скремблерів та технологій маскування сигналів. Ці підходи не потребують значних обчислювальних потужностей, але забезпечують базовий рівень захисту. Криптографічні засоби, орієнтовані на реалізацію на пристроях із низькою продуктивністю. Наприклад, алгоритми SIMON, SPECK, PRESENT

забезпечують шифрування із малими затримками та енерговитратами, що особливо актуально для автономних UWB-пристроїв. В роботі також розглянуто протоколи автентифікації з мінімальним числом обмінів та використанням одноразових ключів, що знижує ймовірність атаки типу «людина посередині».

Як показано у (), інтеграція засобів безпеки може впливати на ключові параметри QoS: затримку, пропускну здатність, ймовірність втрат пакетів. У випадку з UWB-системами особливо важливим є дотримання низької латентності, зважаючи на специфіку застосування. Для збереження QoS у роботі пропонується підхід до адаптивного регулювання рівня безпеки залежно від поточного рівня загроз або типу трафіку. Наприклад, контрольні пакети можуть мати нижчий рівень захисту, тоді як персональні дані шифруються з максимальними налаштуваннями.

Крім того, запропоновано критерії економічної доцільності впровадження тих чи інших засобів безпеки в UWB-системах:

зменшення енергоспоживання пристроїв → збільшення строку автономної роботи → зниження витрат на технічне обслуговування;

зменшення затримок при обробці → підвищення ефективності системи → менші витрати на інфраструктуру;

відсутність потреби в дорогому апаратному забезпеченні (за рахунок використання легковагових алгоритмів).

Таким чином, адаптивні та ресурсоефективні стратегії безпеки в поєднанні з підтримкою QoS забезпечують оптимальне співвідношення «якість/вартість», що є особливо важливим у масштабних розгортаннях UWB-систем (наприклад, у виробництві, охороні здоров'я, транспорті).

Проведений аналіз показав, що реалізація інформаційної безпеки в UWB-системах повинна враховувати обмеження пристроїв, вимоги до QoS і економічну ефективність. Оптимальним є підхід, що базується на: використанні легковагових криптографічних алгоритмів; впровадженні засобів безпеки на фізичному рівні; застосуванні адаптивного управління рівнем захисту; оцінці економічного ефекту від зменшення витрат на обслуговування та енергію. Подальші дослідження доцільно спрямувати на математичне моделювання балансу між QoS, рівнем захисту та економічними параметрами в різних сценаріях використання UWB.

[1] Serkov, A., Kasilov, O., Lazurenko, B., Pevnev, V., Trubchaninova, K. Strategy of building a wireless mobile communication system in the conditions of electronic counteraction Radioelectronic and Computer Systems, 2023, 2023(2), pp. 160–170.

[2] Mohammed T., Albeshri A., Katib I., Mehmood R. UbiPriSEQ - Deep Reinforcement Learning to Manage Privacy, Security, Energy, and QoS in 5G IoT HetNets, 2020, 10 (20), 7120.

[3] Jon Metzler. Security Implications of 5G Networks. UC Berkeley Center for Long-Term Cybersecurity, 2020, 38 p.

[4] Dzheniuk, N., Yevseiev, S., Lazurenko, B., Serkov, O., & Kasilov, O. A method of protecting information in cyber-physical space .Advanced Information Systems, 2023,7(4), pp. 80–85.

[5] Beshley, Mykola & Kryvinska, Natalia, Beshley, Halyna. Quality of Service Management Method in a Heterogeneous Wireless Network Using Big Data Technology and Mobile QoE Application. Simulation Modelling Practice and Theory. 2023.102771.