

---

## РЕАЛІЗАЦІЯ ЕФЕКТИВНОЇ БЕЗПЕКИ ТА КОНФІДЕНЦІЙНОСТІ В МЕРЕЖАХ ІОТ

Уманець М. С, Ляшенко О. С.

Харківський національний університет радіоелектроніки, Харків, Україна

Безпека ІоТ відноситься до методів захисту, що використовуються для забезпечення безпеки підключених до Інтернету або мережевих пристроїв. Це сукупність методів, стратегій та інструментів, що використовуються для захисту цих пристроїв від компрометації.

**Метою доповіді** є дослідження методів, що забезпечують реалізацію безпеки в мережах ІоТ. У роботі наводяться результати дослідження найважливіших аспектів захисту у мережі Інтернету речей. У результаті дослідження було визначено такі фактори забезпечення безпеки як:

- вибір операційної системи. Zephyr OS [1] – це операційна система реального часу з відкритим вихідним кодом, спеціально розроблена для систем з обмеженими ресурсами. Вона підтримує роздільне виконання потоків та роздільне зберігання пам'яті, визначає два рівні повноважень, а саме рівень користувача та рівень супервізора.

- Ethernet Time-Sensitive Networking (TSN) - це сучасна технологія у промисловому ІоТ. TSN можна використовувати як протокол каналного рівня в будь-якій системі

- для досягнення апаратної безпеки в мережах ІоТ нам необхідно подбати про чотири аспекти, а саме: ідентифікація пристрою, захист завантаження, захист сховища, захист часу виконання[3].

- Device Identity Composition Engine (DICE) [2] – це ініціатива щодо забезпечення безпеки ІоТ, що вирішує питання безпечного завантаження та атестації без необхідності використання спеціального співпроцесора.

Необхідно зазначити, що використовуючи вищенаведені методи забезпечення мережної безпеки, безпеки операційної системи, та захисту самого пристрою IoT, можна створити надійну, безпечну та конфіденційну мережу IoT.

#### Список літератури

1. Demystifying internet of things security: successful iot device/edge and platform security deployment/ S.Chervu et al. Berkeley, CA: Springer Nature, 2020. 488 p.
  2. Dice.*Trusted Computing Group* URL: <https://trustedcomputinggroup.org/workgroups/dice-architectures/>(date of access: 01.04.2022).
-