

УДК 004.735

Самойлик С.С.¹, Шараєвська О.А.²

¹ доц. каф. РТТ НУ «Запорізька політехніка»

² студ. гр. РТ-918СП НУ «Запорізька політехніка»

ПИТАННЯ БЕЗПЕКИ ПЕРЕДАВАННЯ ДАНИХ В МЕРЕЖІ ІОТ LORAWAN

Використання інтернет речей (IoT) у повсякденному житті, надає звичайним користувачам абсолютно новий рівень комфорту. Але якщо елементи такої системи не будуть належним чином захищені від несанкціонованого втручання, то замість користі вони принесуть шкоду, надавши кіберзлочинцям лазівку для підриву інформаційної безпеки. Захист даних в будь-якій мережі IoT, незалежно від конкретного стандарту чи технології, повинен відповідати таким критеріям: End-to-end-конфіденційність даних користувача на рівні додатку; взаємна ідентифікація абонентського пристрою і мережі; перевірка цілісності даних при передаванні на радіоінтерфейсу; конфіденційність сигнальної інформації (керуючих команд); безпечне зберігання ідентифікаторів абонентського пристрою і його повноважень; оперативне усунення знайдених вразливостей в ПО компонентів мережі та абонентських терміналів; можливість використання вітчизняних засобів криптографічного захисту інформації.

Для забезпечення захисту інформації, що передається та перевірки цілісності даних при передаванні їх радіоінтерфейсу в мережі IoT LoRaWAN передбачена багаторівнева система безпеки (рис. 1).

1-й рівень. AES-шифрування на рівні додатку (end-to-end, тобто між абонентським терміналом і сервером додатків) за допомогою 128-бітного змінного сесійного ключа Application session key (AppSKey).

2-й рівень. AES-шифрування і перевірка цілісності повідомлень на мережевому рівні (між абонентським терміналом і сервером) за допомогою 128-64 бітного змінного сесійного ключа Network session key (NwkSKey).

3-й рівень. Стандартні методи аутентифікації і шифрування інтернет протоколу (IPsec, TLS і т. П.) При передаванні даних по транспортній мережі

між вузлами мережі (базова станція, мережевий сервер, join-сервер, сервер додатків).

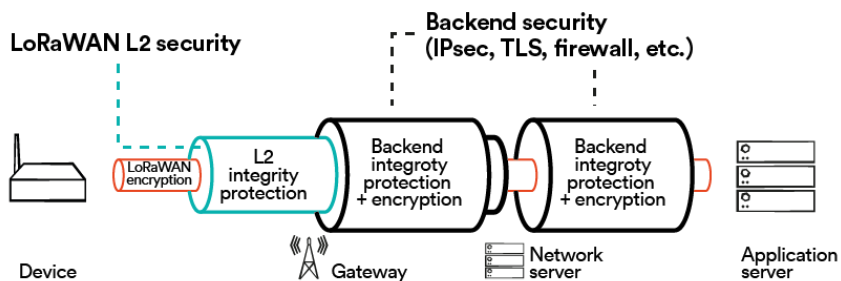


Рисунок 1 – Загальна схема безпеки даних в мережі LoRaWAN.

Таким чином LoRaWAN має всі фундаментальні складові, що необхідні та використовуються будь-якою сучасною технологією бездротового зв'язку. Власна безпека LoRaWAN, як це передбачено в специфікації, має супроводжуватися безпечною реалізацією і безпечним розгортанням цих пристроїв і / або мереж для підтримки вбудованих механізмів безпеки протоколу.