УДК 621.396:004.7

ДОСЛІДЖЕННЯ ТЕХНОЛОГІЙ БЕЗПРОВІДНОГО ЗВ'ЯЗКУ В ІНТЕРНЕТІ РЕЧЕЙ: ПЕРЕВАГИ, ОБМЕЖЕННЯ ТА ПОТЕНЦІЙНІ ЗАГРОЗИ

Стрименешенко О.С.,
Науковий керівник – д. т. н., проф. Агеєв Д. В.
Харківський національний університет радіоелектроніки
(61166, Харків, пр. Науки, 14,
каф. Інфокомунікаційної інженерії ім.Поповського В.В.,
e-mail: oleksandr.strymeneshenko@nure.ua

The Internet of Things (IoT) plays an important role in our modern lives, facilitating automation and convenience in many aspects of our daily and professional lives. One of the key aspects of the IoT is wireless communication, which allows devices to communicate with each other and with central servers without the need for physical connection via cables. In this article, we will explore the benefits, limitations, and potential threats of wireless communication in the IoT.

Однією з найважливіших переваг безпровідного зв'язку в IoT є його зручність та мобільність. За допомогою безпровідних технологій можна підключити пристрої до мережі з будь-якого місця без необхідності проведення кабелів. Це особливо корисно у випадку розгортання IoT у великих просторах, таких як промислові об'єкти чи будівлі.

Другою важливою перевагою є масштабованість безпровідних мереж. Безпровідні технології дозволяють легко розширювати м ережі, додавати нові пристрої та розширювати покриття без значних витрат на інфраструктуру. Це робить безпровідний зв'язок ідеальним варіантом для масштабування IoT у великих містах чи інших густих населених пунктах.

Незважаючи на всі його переваги, безпровідний зв'язок в IoT має свої обмеження. Наприклад, деякі технології можуть мати обмежений діапазон дії та проблеми з проникненням сигналу через стіни або інші перешкоди. Це може обмежувати місце використання певних типів безпровідних пристроїв та технологій, особливо у великих будівлях чи спорудах з товстими стінами.

Додатковим обмеженням є витрата енергії. Деякі безпровідні протоколи можуть вимагати значних витрат енергії для передачі даних, що може стати проблемою для пристроїв з обмеженим живленням, таких як датчики або вбудовані системи.

Попри всі його переваги, безпровідний зв'язок в IoT також відкриває двері для різних потенційних загроз та вразливостей. Наприклад, безпровідні мережі IoT можуть стати об'єктом різних кібератак, серед яких особливо небезпечними є DDoS-атаки та атаки на викидання сервісу (DoS-атаки). Ці атаки відносяться до так званих "відмов у обслуговуванні"

(Denial of Service, DoS) або "розподіленого відмов у обслуговуванні" (Distributed Denial of Service, DDoS) атак.

Вони полягають у перевантаженні мережі чи сервера штучно створеним трафіком, що надходить з багатьох джерел одночасно. Зловмисники можуть використовувати масштабні ботнети (мережі комп'ютерів, що керуються зловмисниками без відома їх власників) для організації DDoS-атак. Це може призвести до перевантаження мережевого обладнання, відмови серверів або інших пристроїв у мережі, що призводить до тимчасової недоступності для легітимних користувачів та серйозних фінансових втрат для організацій. [1]

Ці типи атак можуть бути особливо небезпечними в контексті IoT, оскільки багато пристроїв у безпровідних мережах не мають достатнього рівня захисту, щоб відбити масштабні атаки. Крім того, зловмисники можуть використовувати вразливості в програмному забезпеченні або недоліки в конфігурації мережі для організації атак.

Також передача особистих даних через безпровідні мережі викликає серйозні питання щодо приватності та захисту цих даних. Оскільки безпровідні мережі передають дані через радіосигнали, вони можуть бути вразливі до перехоплення та несанкціонованого доступу. Наприклад, зловмисник, який має технічні знання та відповідне обладнання, може перехопити передані дані із безпровідної мережі, які можуть містити особисті інформаційні дані, такі як імена, адреси, номери телефонів, фінансові дані тощо.

Несанкціонований доступ до особистих даних може мати серйозні наслідки для користувачів та організацій. Це може призвести до крадіжки особистої ідентифікаційної інформації, фінансового шахрайства, витрат на відновлення даних та репутаційних втрат для організацій. Крім того, якщо конфіденційна інформація потрапить в руки зловмисника, це може вплинути на довіру користувачів до системи або послуг, що пропонуються через IoT.

Таким чином, забезпечення безпеки та захисту особистих даних у безпровідних мережах IoT важливо для підтримки приватності користувачів та довіри до систем IoT. Для цього можуть бути використані різноманітні заходи безпеки, такі як шифрування даних, аутентифікація користувачів, використання захищених протоколів зв'язку та систем управління доступом до мережі. Такі заходи допомагатимуть запобігти несанкціонованому доступу до особистих даних та зберегти конфіденційність інформації користувачів у безпровідних мережах IoT.

Список використаних джерел:

1. Горбань, А. В. Кібербезпека в інтернеті речей / А. В. Горбань, І. С. Постернак // Інформаційні технології та комп’ютерна інженерія. – 2018. – № 2 (46). – С. 35–40.