СИСТЕМИ УПРАВЛІННЯ НА ОСНОВІ БЕЗДРОТОВИХ МЕРЕЖ ТА АНАЛІЗ ЇХ ВРАЗЛИВОСТЕЙ

Соболь Д.Ю., Гріненко Т.О.
Харківський національний університет радіоелектроніки, Харків, Україна
Нарєжній О.П.
Харківський національний університет імені В.Н. Каразіна, Харків, Україна

Існує безліч бездротових технологій, найчастіше відомих за назвами, такими як Wi-Fi, Near Field Communication (NFC), Bluetooth, супутниковий зв'язок [1, 2]. Кожна технологія має певні характеристики, які визначаються її сферою застосування. Незважаючи на свій постійний розвиток, дані мережі мають безліч прогалин у системі безпеки, що дозволяє зловмисникам здійснювати перехоплення інформації. **Метою доповіді** є дослідження та аналіз використання бездротових мереж у глобальному суспільстві.

Однією з найпопулярніших бездротових мереж є Wi-Fi. Wi-Fi використовується для передачі даних на короткі відстані та забезпечення доступу до Інтернету. Ще однією поширеною технологією бездротового зв'язку є NFC. NFC використовується для передачі даних на дуже короткі відстані, зазвичай менше 10 см. Супутниковий зв'язок – це технологія передачі даних, яка використовує супутники у космосі для зв'язку із наземною станцією. Супутниковий зв'язок використовується для передачі даних на великі відстані й у місцях, де немає доступу до проводового зв'язку. Кожна з цих бездротових технологій використовується в різних сферах життя та має свої переваги. Також кожна з цих систем має свої вразливості та недоліки, які потрібно враховувати при використанні цих технологій. В доповіді наводяться результати дослідження та аналізу всіх видів вразливостей різних типів бездротових мереж, їх протоколів безпеки. Наводяться та порівняльного аналізу криптостійкості та ефективності захисту інформації від загроз.

Аналіз публікацій за темою дослідження дає розуміння про необхідність захисту бездротових мереж, що є важливим аспектом кібербезпеки, оскільки дані, що надходять через бездротові мережі, можуть бути викрадені або пошкоджені несанкціонованим користувачем [3]. Кожен тип бездротової мережі має свої унікальні методи захисту, такі як шифрування, автентифікація та керування доступом. В результаті дослідження були запропоновані методи захисту систем управління для забезпечення захисту від таких атак як перехват трафіку, модифікація трафіку, злам та крадіжка особистих даних.

Список літератури

1. Pavur, J., Martinovic, I. Building a launchpad for satellite cyber-security research: lessons from 60 years of spaceflight. *Journal of Cybersecurity*. 2022. Vol.8, Issue 1. P. 6-13. DOI: https://doi.org/10.1093/cybsec/tyac008.

2. Zbigniew Piotrowski. Will WPA3 really provide Wi-Fi security at a higher level? *Proceedings SPIE*. 2019. P. 2-11. DOI: https://doi.org/10.1117/12.2525020.

3. Северинов А.В., Черныш, В.И. Анализ угроз и рисков безопасности информации в беспроводных сетях. // Системи управління, навігації та зв'язку.– Вип, 1, 229-232.