



**НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ПОЛТАВСЬКА ПОЛІТЕХНІКА
ІМЕНІ ЮРІЯ КОНДРАТЮКА**

ЗБІРНИК МАТЕРІАЛІВ

**76-ї НАУКОВОЇ КОНФЕРЕНЦІЇ ПРОФЕСОРІВ,
ВИКЛАДАЧІВ, НАУКОВИХ ПРАЦІВНИКІВ,
АСПІРАНТІВ ТА СТУДЕНТІВ УНІВЕРСИТЕТУ**

ТОМ 1

14 травня – 23 травня 2024 р.

НАУКОВО-ТЕХНІЧНИЙ ПІДХІД ДО КОНФІДЕНЦІЙНОСТІ ПЕРЕДАЧІ ІНФОРМАЦІЇ У БЕЗДРОВОВИХ МЕРЕЖАХ

Широке використання бездротових мереж з різними типами топологій, методів і наборів протоколів вимагають вдосконалення механізмів безпеки.

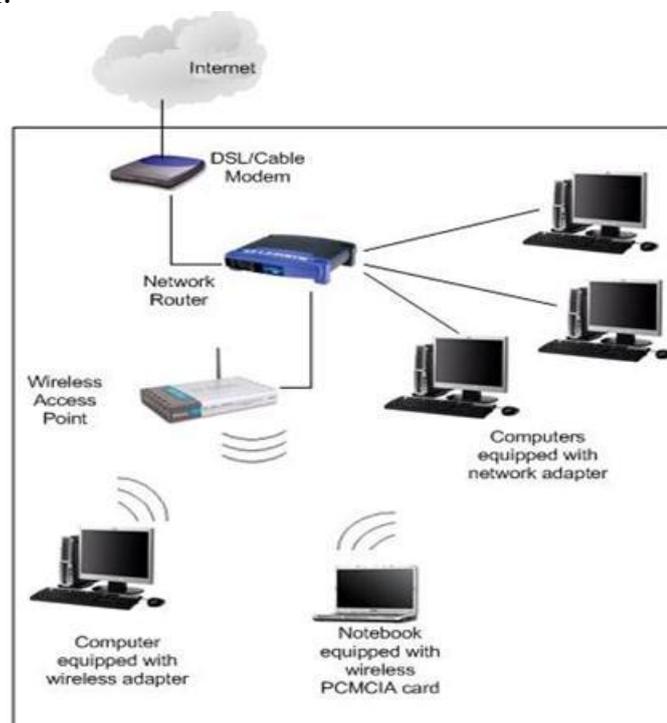


Рисунок 1 – Комбінована мережа передачі інформації

На рис. 1 показано, як здійснюється передача інформації в комбінованій мережі між різними пристроями. Обидві, умовно відокремлені мережі (дротові та бездротові), вимагають суворої автоматичної конфіденційності без порушення цілісності системи. Бездротова мережа дає легкий доступ зловмисникам до транспортного середовища, і цей доступ збільшує загрозу з якою має боротися будь-яка архітектура безпеки.

Відповідно до вищезазначених завдань безпеки, основною метою цього дослідження було визначення основних елементів, пов'язаних із безпекою бездротової мережі, і надання огляду потенційних загроз, вразливостей і контрзаходів (рішень), пов'язаних із безпекою бездротової мережі.

Упровадження бездротової безпеки запобігає несанкціонованому доступу або пошкодженню інформації користувачів, що використовують бездротові мережі. Найпоширенішими типами бездротової безпеки є Wired Equivalent Privacy (WEP) і Wi-Fi Protected Access (WPA) [1].

Захист бездротового зв'язку за стандартом IEEE 802.11 отримав багато критики, оскільки він має певні проблеми безпеки та недосконалий інтерфейс [2].

У роботі використано засоби та заходи по забезпеченню безпеки бездротової мережі, котра підтримує автентичність, цілісність та конфіденційність. Доступність гарантується тим, що бажані мережеві служби доступні в будь-який час, незважаючи на несанкціоновані атаки. Автентичність забезпечується своєчасним виявленням вузла зловмисника, який може маскуватися під надійний вузол мережі. Конфіденційність забезпечує зв'язок лише між споживачами. Цілісність гарантується тим, що повідомлення надіслане з вузла А до вузла В не буде змінено зловмисним вузлом С під час передачі.

В процесі досліджень була запропонована модель взаємозв'язку відкритої системи (OSI), як еталонна модель мережі, для аналізу передачі даних між апаратним і програмним забезпеченням у семирівневій системі. Виконуючи унікальні завдання, кожен рівень поєднує функції для підтримки рівня вище та надання послуг відповідно нижчому рівню.

Загалом, для підтримання сучасного рівня безпеки бездротових мереж, необхідно впроваджувати технологію WPA2 з використанням методології та моделей отриманих в ході даного дослідження, яка включає в себе створення надійного пароля, створення плану забезпечення безпеки і захисту програмного забезпечення, що сприятиме забезпеченню більшої складності для зловмисників і надійну безпеку бездротової мережі.

Література

1. *Безпека в мережі Інтернет [Електронний ресурс]. – Режим доступу: <http://svitppt.com.ua/informatika/osnovni-ponyattya-zahistu-informacii-bezpeka-v-merezhi-internet.html>*
2. *Технології захисту інформації [Електронний ресурс]. – Режим доступу: <https://www.uzhnu.edu.ua/uk/infocentre/get/4186>*
3. *Хмельницький, О.Ю. Цілісність та конфіденційність передачі даних у мережах [Текст] / О.Ю. Хмельницький, Ю.В. Хмельницький // Вимірювальна та обчислювальна техніка в технологічних процесах. – 2013. – № 1. – С. 214-217.*