

*Трубчанінова К. А., к.т.н., доцент,
Ковтун І. В., к.т.н., доцент,
Куриць М. С., к.т.н.
(Український державний університет
залізничного транспорту)*

МОДЕЛЮВАННЯ ПЛОСКОЇ ДВОДІАПАЗОННОЇ АНТЕННОЇ РЕШІТКИ ДЛЯ ПРИЙМАННЯ ХВИЛЬ КРУГОВОЇ ПОЛЯРИЗАЦІЇ

При створенні сучасних антенних систем, наприклад, для вирішення задач радіопеленгації (радіолокації), космічного зв'язку тощо, розробникам часто потребується реалізувати або можливість електронного сканування навколишнього простору в деякій секторі тілесних кутів, або формування багатопроменевої діаграми направленості в цьому секторі. Для вирішення подібних задач використовуються антенні решітки.

Задача сканування суттєво ускладнюється при необхідності забезпечення роботи в широкому діапазоні частот або в декількох діапазонах, саме така задача розглядається в даній роботі. Для цього використовуються малогабаритні антени, які здатні ефективно працювати в широкій смузі частот. Такими антенами є ширококутові, у яких діаграма направленості, вхідний опір мало змінюються при зміні частоти. Зазвичай до ширококутових відносять антени, які зберігають характеристики в смузі частот в декілька десятків процентів. Надширококутові антени створюють групу діапазонних антен, які мають відношення максимальної робочої частоти до мінімальної, яке зветься коефіцієнтом перекриття, 5:1 і більше.

Для таких антен властиво незначна зміна характеристик в достатньо широкому діапазоні частот. Слаба залежність форми діаграми направленості, коефіцієнта направленої дії, вхідного опору та інших характеристик надширококутових антен від частоти пояснюється тим, що поле випромінювання в них формується розподіленими на кінцевій ділянці поверхні антени токами. Зі зміною частоти ця «активна область» переміщується, а її відносні розміри в долях довжин хвиль, залишаються незмінними.

Довгохвильова межа робочого діапазону визначається частотою, для якої активна область змістилася до краю надширококутової антени. Однак, на практиці визначення межі залежить від багатьох факторів, наприклад, від поперечних розмірів фідера, допустимих вносимих втрат. Межа низькочастотного діапазону визначається зовнішніми розмірами антени, а високочастотного - конструктивним виконанням вузла збудження.

Найбільш поширеними є частотно-незалежні антени, виконані у вигляді плоских спіральних,

логоперіодичних, серповидних вібраторних антен. В даний час все частіше застосовуються щілинні антени (так звані антени Вівальді) і решітки з таких випромінювачів. Вони мають ряд переваг: простота виготовлення, малі габарити і вартість. Темою даної роботи є моделювання плоскої дводіапазонної антенної решітки для приймання хвиль кругової поляризації.

Для цього був обраний відповідний тип випромінювача, його розміри, форма, проведено чисельне моделювання даного випромінювача. Були проведені розрахунки, що дозволяють оцінити можливість побудови двовимірної антеною решітки на основі схрещених лінійних елементів, що складаються з антен Вівальді.

Список використаних джерел

1. Serkov A. Noise-like signals in wireless information transmission systems / A. Serkov, V. Breslavets, M. Tolkachov, G. Churyumov, Issam Saad // *Advanced Information Systems*. – 2017. – Vol. 1, №2 – P. 33 - 39. doi: 10.20998/2522-9052.2017.2.06.
2. Серков А. Перспективы развития систем беспроводной связи / А.А. Серков, Б.А. Лазуренко // *Проблемы информатизации. Тез. доп. VI МНТК*, (14 - 16 листопада 2018р., Черкаси-Баку-Бельсько-Бяла-Харків). – Х.: НТУ «ХП», 2018. – С. 22.

*Меркулов В. С., Бізюк І. Г., Чаленко О. В.
(УкрДУЗТ, м. Харків)*

ОРГАНІЗАЦІЙНІ МЕТОДИ ЗАХИСТУ ІНФОРМАЦІЙНИХ РЕСУРСІВ АВТОМАТИЗОВАНОЇ СИСТЕМИ ПЛАНУВАННЯ ВАНТАЖЕННЯ- ВИВАНТАЖЕННЯ

Побудова надійного та ефективного захисту інформаційної системи неможлива без попереднього аналізу можливих загроз її безпеці. Цей аналіз повинен складатися з таких етапів:

- виявлення характеру інформації, яка зберігається в системі;
- оцінювання цінності цієї інформації;
- визначення та класифікація загроз інформації в системі (несанкціоноване зчитування, несанкціонована модифікація і т.д.).

Загрози інформаційним ресурсам можна класифікувати за наступними критеріями:

- інформаційна безпека (загрози конфіденційності даних і програм, загрози цілісності даних, програм, апаратури, загрози доступності даних, загрози відмови від виконання операцій);
- компоненти інформаційних систем, на які загрози націлені (інформаційні ресурси та послуги,