Особливості GPS-спуфінгу щодо управління БПЛА

Микийчук Микола
Кафедра метрології, стандартизації та сертифікації
НУ "Львівська політехніка"
Львів, Україна
mykolamm@ukr.net

Марків Володимир
Кафедра метрології, стандартизації та сертифікації
НУ "Львівська політехніка"
Львів, Україна
VMarkiv86@yandex.ua

The article dwells upon the problem of remote-piloted vehicles use in the modern society. The peculiarities of GPS and GPS-spoofing concerning remote piloted vehicles are described. Methods of GPS-spoofing fight are proposed. Also the radio electronic fight and its peculiarities are highlighted.

Ключові слова: безпілотний літальний апарат, GPS, GPS-спуфінг, радіоелектронна боротьба, радіосигнал.

Вступ

В умовах наукового та технологічного прогресу спостерігається інтенсивний розвиток інформаційного суспільства, основним елементом якого є виробництво та використання науково-технічної та інших видів інформації. Тому збільшується потреба в зборі і обробці великих об'ємів даних у різноманітних сферах життя. Для цього застосовують різні методи та засоби. В умовах сьогодення інтенсивно використовують безпілотні літальні апарати (БПЛА) для досліджень та збору інформації, що дозволили людині максимально дистанціюватися від безпосереднього зіткнення із противником [1,8].

Перспективним є застосування БПЛА у різноманітних сферах життя. Багато країн використовують БПЛА для різних цілей, що стосуються аерознімання та досліджень наземних об'єктів. Це ефективний спосіб дослідження. Новітні БПЛА використовують нові технології, камери, радари та ін [2,4].

Однак, незважаючи на те, що безпілотні літальні апарати є популярними в наш час, є ряд проблем, що виникають під час їх використання. Зокрема, поширеним є явище GPS-спуфінгу.

Особливості GPS-спуфінгу

Використання системи глобального позиціонування (*GPS*) є актуальним для управління БПЛА і потребує детального вивчення.

GPS – сукупність радіоелектронних засобів, що дозволяє визначати положення та швидкість руху об'єкта на поверхні Землі або в атмосфері. Положення об'єкту обчислюється завдяки використанню GPS- приймача, який приймає та обробляє сигнали супутників системи глобального позиціонування.

Однак, на сьогодні поширеним є явище GPS-спуфінгу – спуфінг-атаки, яка намагається обманути GPS-приймач, передаючи потужніший сигнал, ніж отриманий від супутників GPS. В результаті, невірно визначається місце розташування.

Оскільки системи GPS працюють вимірюючи час, який потрібний для сигналу, щоб дійти від супутника до одержувача, то імітуючий сигнал має бути спроектований із врахованими затримками часу[5,6,7].

БПЛА може втратити зв'язок з пультом управління в результаті дії невеликого генератора перешкод відповідної потужності. GPS-спуфер перехоплює безпілотник без знищення за допомогою, помилкового сигналу Глобальної системи позиціонування, а саме за допомогою глушіння сигналу позиціонування і подачі хибного сигналу. В результаті користувач спуфера може відправити безпілотник туди, куди побажає.Основним компонентом спуфера є імітатор GPS-сигналів. Цей пристрій використовують для тестування навігаційних

систем. Імітатор сигналів GPS є малопотужний і діє в радіусі десяти метрів. Тому другим компонентом спуфера є підсилювачі, які підвищують потужність помилкового сигналу GPS в десятки разів.

Система спуфінга діє таким чином, що генератор сигналу GPS передає імітацію сигналу декількох супутників через антену на частоті GPS. За умови, що рівень імітуючого сигналу дещо перевищує рівень сигналу реальних супутників GPS-приймач буде сприймати імітований сигнал і обчислювати положення на його основі.

Окремою проблемою є створення поля спуфінга в умовах міської забудови, де відображенню сигналу заважають будівлі, а також радіоатени, конфігурація яких для справжнього сигналу, що надходить із супутників, і сигналу перешкоди – сильно розрізняється.

Для виявлення GPS-спуфінга є різні методи. Наприклад, можливе виділення помилкового сигналу на підставі визначення напрямку щодо джерела. Визначити напрямок можна порівнюючи фази сигналу на декількох антенах. Можна використовувати в якості додаткового джерела інформації доплерівський зсув частот. Це актуально для рухомих об'єктів [5,6,7].

Отже, важливим питанням є забезпечення захисту від несанкціонованих посягань на інформацію про місцезнаходження. Потрібно створювати нові засоби радіоелектронної боротьби на основі фазочастотної теорії вимірювання та перетворення радіосигналів.

Сучасні системи протидії часто енергетично неефективні, з малим радіусом дії сигналів та високовартісні. Саме тому необхідно розробити мобільні систем радіоелектронної боротьби із сучасними видами радіозв'язку за допомогою вимірювання та формування радіосигналів, із радіоканалами керування та зйомкою відеоінформації [3,5].

Висновок

Способи передачі, шифрування та захисту даних, а також вибір радіоканалів є одним із пріоритетних напрямків у сфері метрологічного забезпечення безпілотників.

Будь-яка техніка, що для навігації використовує систему GPS, схильна до спуфінгу. Для захисту від засобів радіоелектронної боротьби потрібно застосовувати шифрування службових сигналів і забезпечення їхньої потужності відповідного рівня. У разі, якщо не можливо підмінити сигнал, то потрібно його вимикати або розробляти методи знищення безпілотних літальних апаратів.

Література

[1] О.Зинченко, "Беспилотные летательные аппараты: применение в целях аэрофотосъемки для картографирования", Ракурс, част.1, 2011, с. 1–12

[2] М.Матійчик, І. Качало, "Тенденції застосування безпілотних повітряних суден в цивільній авіації", Матеріали XI міжнародної наук.-техн. конфер. "ABIA 2013", 2013, С. 97.

[3] В. Мельников, С. Клейменов, А. Петраков, "Информационная безопасность и защита информации: Учебное пособие для вузов по спец. «Информационные системы и технологи»" , Под ред. С.А. Клейменова, 5-е изд., Academia, 2011, 331 с.

[4] J. Barton, "Fundamentals of Small Unmanned Aircraft Flight", Johns Hopkins APL Technical Digest, 2012., V. 31, № 2, pp. 132-149.

[5] L. Bond, "Overview of GPS Interference Issues", GPS Interference Symposium, Volpe National Transportation System Center, Boston, August 27, 1998.

[6] B. Forssel, T. Olsen, " Jamming Susceptibility of Some Civil GPS Receivers" GPS World, № 1.? 2003, p. 54-58.

[7] E. Key, "Technique to Counter GPS Spoofing", International Memorandum, MITRE Corporation, February 17, 1995.

[8] V. Markiv, "Analysis of remote-piloted vehicles use and control system description" , Вісник "Комп'ютерні науки та інформаційні технології", №843, Видавництво Львівської політехніки, 2016, С.347-351