С. М. Табенський[1]
А. О. Бабарика[1]

ВИКОРИСТАННЯ ПЕРСОНАЛЬНИХ GPS-НАВІГАТОРІВ В ЗОНІ ПРОВЕДЕННЯ АНТИТЕРОРИСТИЧНОЇ ОПЕРАЦІЇ: ПЕРЕВАГИ ТА ЗАГРОЗИ

[1]Національна академія Державної прикордонної служби України імені Богдана Хмельницького

Анотація

У доповіді розкрито основні напрямки застосування персональних GPS технологій в умовах проведення антитерористичної операції на Сході України. Розкрито передумови та переваги використання даних технічних засобів. А також основні загрози, які виникають в ході їх експлуатації

Ключові слова: антитерористична операція (АТО)**,** навігація, GPS-навігатор, GPS-спуфінг, подавлювач сигналу GPS

Abstract

The report reveals the main directions of personal GPS technology in terms of anti-terrorist operation in eastern Ukraine. Reveals the conditions and benefits of using these technical means. As well as the main threats that arise in the course of their operation

Keywords: anti-terrorist operation (ATO), navigation, GPS-navigators, GPS-spoofing, interference GPS signal

На сьогоднішній день у умовах ведення бою все частіше і активніше впроваджуються різноманітні засоби автоматизації, що дозволяє зберегти життя та здоров'я військовослужбовців.

Зокрема широкого розповсюдження набуло використання GPS технологій у найрізноманітніших цілях, починаючи від простих GPS-приймачів індивідуального застосування і закінчуючи складними комплексними системами позиціонування та управління.

На початку січня 2015 року, під час захисту ДАП, українські бійці потрапили в полон до терористів, оскільки, рухаючись в тумані, в умовах поганої видимості, відхилилися на 900 метрів від потрібного шляху і потрапили прямо в лігво бандитів.

GPS-навігатори дозволяють точно зорієнтуватися на місцевості в умовах будь-якої видимості. До речі, GPS-навігатор - радіопасивний пристрій, до складу якого входить тільки приймач радіосигналу, тому запеленгувати того, хто ним користується, неможливо. Це дозволяє використовувати GPS-системи для будь-якого водія і рядового бійця.

Волонтери закуповують в зону АТО GPS-навігатори різних видів: автомобільні та туристичні (пішохідні).

Проте використання такого роду GPS-навігаторів має ряд загроз, оскільки в ньому не передбачено автентифікація навігаційної інформації, що дає можливість зловмисникам фальсифікувати данні GPS. Цей процес носить назву спуфінг, і в загальному випадку означає ситуацію, в якій одна людина або програма успішно маскується під іншу шляхом фальсифікації даних[1].

GPS-спуфінг – спуфінг-атака, яка намагається обдурити GPS-приймач, широкомовно передаючи трохи більш потужний сигнал, ніж отриманий від супутників GPS, такий, щоб бути схожим на ряд нормальних сигналів GPS. Ці імітовані сигнали, змінені таким шляхом, щоб змусити одержувача невірно визначати своє місце розташування, вважаючи його таким, яке відправить атакуючий.

Атака GPS-спуфінга починається широкомовним передаванням трохи більш потужного сигналу, який вказує коректну позицію, і потім повільно відхиляється не далеко до позиції, заданої атакуючим, тому що занадто швидке переміщення спричинить за собою втрату сигнального блокування, і в цій точці spoofer стане працювати тільки як передавач перешкод.

Таким чином зловмисник може отримати управління над об’єктом, та направити його в потрібно для нього місце.

На сьогоднішній день існують приклади вдалого використання GPS-спуфінгу, наприклад одна з версій захоплення американського безпілотника Lockheed RQ 170 в північно-східному Ірані в грудні 2011.

Ще однією великою загрозою використання GPS в якості навігаційної системи в умовах ведення бою є повне придушення сигналу, який надходить від супутника до GPS- приймача[2].

Принцип роботи даних пристроїв є дуже простий: генерація шуму (радіоперешкод) на частоті передачі корисного сигналу. Чим потужніша амплітуда шуму (потужність генератора шуму), тим менше ймовірність здійснити зв'язок на частоті генерації шуму і тим більше радіус впливу радіоперешкод.

Ці сигнали не несуть абсолютно ніякої інформації або даних і їх можна назвати просто «білим шумом». Їх користь полягає в тому, що в цьому «білому шумі» просто втрачається корисний, що несе дані сигнал. Таким чином, будь-яка глушилка частот створює навколо себе поле перешкод певної частоти і з певним радіусом.

Існують різні види таких пристроїв, але найбільш поширеним є використання універсальних пристроїв перешкод, що працює на всі діапазони, як стільникових операторів, так і супутникових сигналів та має кілька антен для генерації перешкод на вибраних діапазонах. Часто передбачається можливість селективної роботи, тобто здатність генерувати шум тільки на обраних частотах.

На сьогоднішній день на озброєні Російської Федерації знаходяться цілі комплекси метою яких є створення завад та придушення сигналу, які активно застосовуються російсько-терористичними військами в ході ведення бойових дій.

Прикладом використання таких комплексів (Р-330Ж «Житель») є повна відсутність будь якого виду радіозв'язку, сигналу мобільної мережі та сигналу навігаційної системи GPS під час боїв за місто Дебальцеве.

Виходячи з вище сказаного можна зробити висновок, що в ході проведення антитерористичної операції під час ведення бою не можна повністю покладатись на використання GPS-навігаторів, а використовувати лише в критичних випадках та на відносній відстані від лінії розмежування.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Straight Talk on Anti-Spoofing Securing the Future of PNT. Режим доступу: http://gpsworld.com/. Дата звернення: 23.03.2017.

2. Global positioning systems directorate systems engineering & integration interface specification IS-GPS-200. Режим доступу: http://www.gps.gov/technical/icwg/. Дата звернення: 23.03.2017.

Табенський Сергій Миколайович, викладач кафедри зв'язку, автоматизації та захисту інформації, Національної академії Державної прикордонної служби України імені Богдана Хмельницького, м. Хмельницький, e-mail: nach899@gmail.com

Бабарика Анатолій Олександрович, викладач кафедри зв'язку, автоматизації та захисту інформації, Національної академії Державної прикордонної служби України імені Богдана Хмельницького, м. Хмельницький, e-mail: aob.work@gmail.com

Sergiy Tabenskiy, lecturer in communications, automation and data protection, the National Academy of State Border Service of Ukraine Bohdan Khmelnitsky, Khmelnitsky, e-mail: nach899@gmail.com

Anatoliy Babarika, lecturer in communications, automation and data protection, the National Academy of State Border Service of Ukraine Bohdan Khmelnytsky city. Khmelnitsky, e-mail: aob.work@gmail.com