

Sławomir J. Ambroziak, Ryszard J. Katulski,

Jarosław Sadowski, Jacek Stefański

Politechnika Gdańska

Wydział Elektroniki, Telekomunikacji i Informatyki

Katedra Systemów i Sieci Radiokomunikacyjnych

80-233 Gdańsk Wrzeszcz, ul. Gabriela Narutowicza 11/12

e-mail: sj_ambroziak@eti.pg.gda.pl, rjkat@eti.pg.gda.pl, Jaroslaw.Sadowski@eti.pg.gda.pl,

jstef@eti.pg.gda.pl

AEGIS — DEMONSTRATOR TECHNOLOGII C-IED

STRESZCZENIE

W artykule przedstawiono budowę i działanie opracowanego na Politechnice Gdańskiej demonstratora technologicznego systemu AEGIS, przeznaczonego do przeciwdziałania atakom z wykorzystaniem prowizorycznych urządzeń wybuchowych detonowanych drogą radiową (RCIED — *Radio Controlled Improvised Explosive Devices*). Przedstawiono zaimplementowaną oryginalną metodę generowania sygnału zagłuszającego o dowolnie ukształtowanym widmie częstotliwościowym, będącą przedmiotem zgłoszenia patentowego o numerze P.398050.

Słowa kluczowe:

prowizoryczne ładunki wybuchowe, IED, C-IED, RCIED, demonstrator technologiczny.

WSTĘP

W XXI wieku konflikty asymetryczne zyskały znaczącą przewagę nad ich klasycznymi odpowiednikami, a siły zbrojne wielu państw konfrontowane są z przeciwnikiem, którego cele, organizacja i środki nie mieszczą się w konwencjonalnym pojęciu wojny. Kluczowymi elementami takiego konfliktu są działania skryte, zmienne i nastawione na zaskoczenie, których celem jest maksymalizacja efektów przy minimalizacji kosztów [3]. W takim stanie rzeczy szczególnego znaczenia nabiera konieczność metodycznego podejścia do kwestii przeciwdziałania prowizorycznym

urządzeniom wybuchowym — IED (Improvised Explosive Device), stanowiącym najczęstsze i najgroźniejsze narzędzie walki słabszej strony konfliktu asymetrycznego.

Na wstępie niniejszego artykułu przedstawiono charakterystykę prowizorycznych urządzeń wybuchowych, zawierającą definicję tego rodzaju broni oraz jej klasyfikację. Następnie przedstawiono budowę demonstratora technologii wytwarzania kurtyny elektromagnetycznej do ochrony przed urządzeniami IED oraz opisano metodę generowania sygnału zagłuszającego pracę systemów, które mogą być wykorzystywane przez stronę konfliktu stosującą urządzenia RCIED (*Radio Controlled IED*), detonowane drogą radiową.

CHARAKTERYSTYKA PROWIZORYCZNYCH URZĄDZEŃ WYBUCHOWYCH

W związku z rozbieżnością polskojęzycznej terminologii używanej do zdefiniowania IED w normie obronnej NO-02-A043 i słownikach NATO (AAP-6 i AAP-19) posłużymy się propozycją uniwersalnej definicji tego rodzaju broni, sformułowanej w [5]: „Prowizoryczne urządzenie wybuchowe (IED) — jest to urządzenie wybuchowe sporządzone w sposób prowizoryczny, przeznaczone do rażenia ludzi i (lub) środków (przedmiotów) materialnych. Zawiera przedmiot wybuchowy i inne elementy (przedmioty) pochodzenia wojskowego i (lub) niewojskowego”.



Fot. 1. Urządzenia IED wykonane na bazie uzbrojenia wojskowego (pociski artyleryjskie, pociski moździerzowe, miny)

Źródło: R. Ambroziak, S. J. Ambroziak, R. J. Katulski, *Metody walki z prowizorycznymi urządzeniami wybuchowymi w świetle doktryny AJP-3.15*, „Zeszyty Naukowe WSOWL”, 2011, nr 4, s. 28–37.

Jest to zatem urządzenie stosunkowo tanie i proste w produkcji, pozwalające jego operatorom na uniknięcie kontaktu zbrojnego z silniejszym przeciwnikiem. Ponadto IED jest bronią efektywną, zbudowaną z elementów zarówno pochodzenia wojskowego (fot. 1.), jak również cywilnego (fot. 2.), ograniczającą możliwości manewrowe wojsk na poziomie taktycznym.



Fot. 2. Urządzenia IED wykonane na bazie materiałów ogólnodostępnych

Źródło: R. Ambroziak, S. J. Ambroziak, R. J. Katulski, wyd. cyt.

Ładunki te, z uwagi na zwykle spektakularny charakter ataku i związane z nim straty przeciwnika, umożliwiają stosującej je stronie konfliktu wpływanie na globalną opinię publiczną i pośrednio na decyzje rządów krajów zaangażowanych w konflikt. W tym stanie rzeczy IED w połączeniu z kampanią informacyjną może mieć nieproporcjonalne oddziaływanie na prowadzone operacje na poziomie operacyjnym, a nawet strategicznym. Przykładem wpływu IED na strategiczne decyzje może być zamach bombowy w Libanie w 2005 roku na byłego premiera tego kraju Rafica Al-Hariri. Ten pojedynczy akt terroru doprowadził do wycofania wojsk syryjskich z terytorium Libanu.

Ze względu na sposób detonacji wyróżnia się następujące rodzaje prowizorycznych urządzeń wybuchowych: naciskowego działania, inicjowane przez podniesienie, kierowane drogą radiową, kierowane przewodowo, umieszczone na samobójcy, umieszczane w pojeździe z kierowcą samobójcą [6]. Urządzenia te mogą różnić się między sobą, jednakże we wszystkich można wyróżnić charakterystyczne elementy, a mianowicie: przełącznik powodujący inicjację działania zapalnika, zapalnik, główny ładunek wybuchowy, źródło zasilania i pojemnik.

Urządzenia IED zazwyczaj są maskowane w celu utrudnienia ich identyfikacji. Przykładowe sposoby ukrywania pułapek wykorzystujących ten rodzaj broni

przedstawiono na fotografii 3. Mogą do tego celu być wykorzystywane kamienie, płaszcze, folia, butelki, opony, a nawet spotkać można IED zalane betonem.



Fot. 3. Przykłady maskowania urządzeń IED

Źródło: R. Ambroziak, S. J. Ambroziak, R. J. Katulski, wyd. cyt.

Z powodu zwiększenia możliwości osiągnięcia celów operacyjnych i strategicznych stosująca IED strona konfliktu stara się rozmieszczać je w dużych skupiskach ludzkich, takich jak targi, często uczęszczane trasy, punkty powodujące skanalizowanie ruchu (mosty, przepusty, wiadukty), punkty powodujące spowolnienie ruchu (wąskie ulice, spowalniacze ruchu) oraz punkty charakterystyczne, np. skrzyżowania ulic, zjazdy z tras głównych i tym podobne.

Zagrożenia związane z prowizorycznymi ładunkami wybuchowymi i konsekwencje ataków przeprowadzanych przy ich zastosowaniu określone zostały w doktrynie AJP-3.15. W celu minimalizacji ryzyka skutecznego ataku oraz ograniczenia jego skutków w razie powodzenia, w dokumencie zawarte zostały priorytety i procedury zwalczania systemu IED zarówno jako całości, jak i poszczególnych jego części [4].

Jak już to zostało napisane, ze względu na sposób detonacji można wyróżnić różne rodzaje prowizorycznych urządzeń wybuchowych. Podczas ataków na siły sojusznicze najczęściej stosowane są urządzenia IED detonowane drogą radiową (RCIED — *Radio Controlled IED*). Dowodem na to jest fakt, iż w Iraku tego typu ataki stanowiły od 50 do 60% wszystkich ataków na siły sojusznicze, jakie przeprowadzono z zastosowaniem IED [6]. W związku z powyższym niezwykle aktualną jest potrzeba neutralizacji urządzeń RCIED poprzez oddziaływanie elektromagnetyczne.

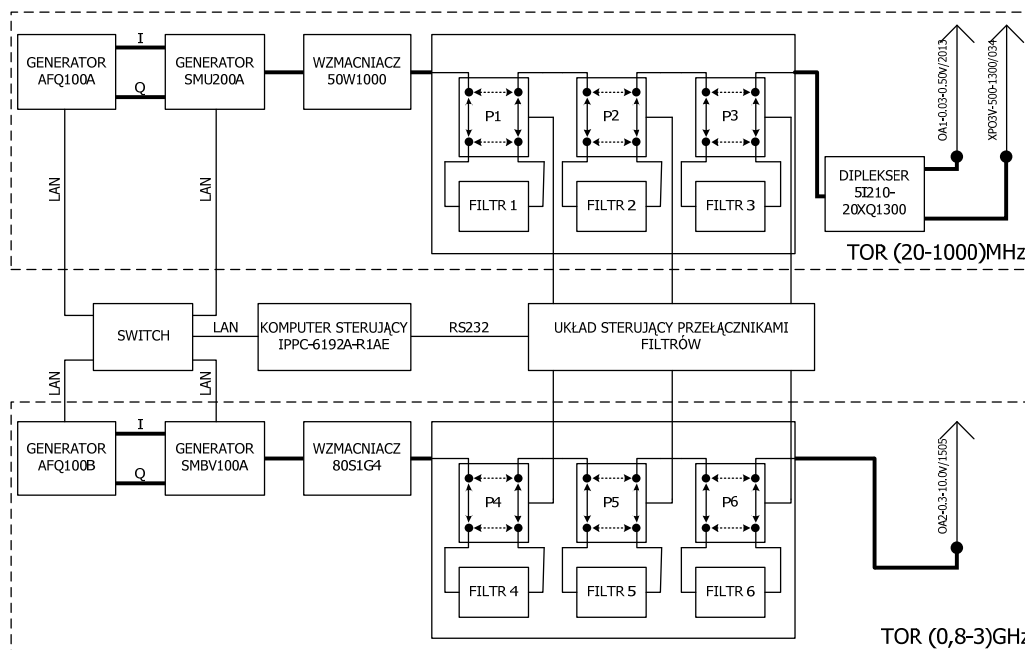
Taki stan rzeczy był powodem podjęcia na Politechnice Gdańskiej w Katedrze Systemów i Sieci Radiokomunikacyjnych prac nad systemem AEGIS, którego zadaniem jest ochrona obiektów mobilnych przed zagrożeniami związanymi z prowizorycznymi urządzeniami wybuchowymi detonowanymi drogą radiową.

NADAJNIK ZAGŁUSZAJĄCY SYSTEMU AEGIS

Nadajnik systemu AEGIS podzielony jest na dwa niezależne tory zagłuszające (rys. 1.) sterowane za pomocą komputera z panelem dotykowym. Pierwszy tor, obejmujący częstotliwości z zakresu od 20 MHz do 1 GHz, zbudowany jest z generatora AFQ100A sygnałów w paśmie podstawowym oraz z generatora SMU200A, przenoszącego widmo sygnału w pasmo wysokich częstotliwości. Tak przygotowany sygnał jest wzmacniany we wzmacniaczu 50W1000, a następnie podawany na zespół przełączanych filtrów pasmowo-zaporowych. W zależności od częstotliwości, które powinny być chronione (tzw. pasma chronione nie powinny być zagłuszane), np. częstotliwości działania wojskowych urządzeń radiokomunikacyjnych, można podłączać dowolne filtry, których przełączanie jest realizowane za pomocą przełączników transferowych (P1, P2, P3) wysokiej mocy. Następnie sygnał jest rozdzielany w dupleksersze 5I210-20XQ1300 na dwa podpasma: od 20MHz do 500MHz oraz od 500MHz do 1GHz, które podawane są na dwie niezależne anteny nadawcze, odpowiednio AO1-0.03-0.50V/2013 oraz XPO3V-500-1300/034.

Z kolei drugi tor zagłuszający, obejmujący częstotliwości z zakresu od 0,8 GHz do 3 GHz, zbudowany jest z generatora AFQ100B sygnałów w paśmie podstawowym. Funkcje generatora częstotliwości nośnej i modulatora realizowane są przez generator SMBV100A. Zagłuszający sygnał w.cz. po wzmocnieniu we wzmacniaczu 80S1G4 podawany jest na zespół filtrów pasmowo-zaporowych, przełączanych w identyczny sposób jak ma to miejsce w pierwszym torze zagłuszającym. Po procesie filtracji sygnał podawany jest na antenę nadawczą OA2-0.3-10.0V/1505.

Należy podkreślić, że wykorzystywane generatory AFQ100A oraz AFQ100B pozwalają na generowanie w danej chwili zagłuszających sygnałów w.cz. w pasmach o szerokościach odpowiednio 240MHz i 528MHz. W zależności od potrzeb zastosowanie tych generatorów w poszczególnych torach zagłuszających może być dowolne.



Rys. 1. Schemat blokowy urządzenia zagłuszającego systemu AEGIS

Źródło: opracowanie własne.

Komputer sterujący IPPC-6192A-R1AE ma za zadanie realizację algorytmu generowania cyfrowej postaci sygnału zagłuszającego na podstawie wprowadzonych przez użytkownika parametrów. Następnie generowany jest sygnał zagłuszający w paśmie podstawowym i dalej w paśmie wysokich częstotliwości. Ponadto komputer sterujący odpowiedzialny jest za sterowanie pracą generatorów AFQ100A, AFQ100B, SMBV100A i SMU200A (za pośrednictwem interfejsów Ethernet) oraz pracą przełączników filtrów (za pośrednictwem interfejsów RS232). Wytypowany komputer ma dotykowy wyświetlacz, co znacząco upraszcza obsługę urządzenia. Dodatkowo całość urządzenia zamontowana jest w dwóch szafach 19" posadowionych na specjalnym wózku, co ułatwia przemieszczanie urządzenia podczas testów. Wygląd demonstratora technologicznego nadajnika AEGIS przedstawiony został na fotografii 4. Parametry techniczne i eksploatacyjne zrealizowanego w powyższy sposób demonstratora zestawione zostały w tabeli 1.



Fot. 4. Wygląd demonstratora technologicznego nadajnika AEGIS

Źródło: opracowanie własne.

Tabela 1. Parametry nadajnika zagłuszającego systemu AEGIS

Zagłuszane pasmo częstotliwości		(20–3000) MHz
EIRP	dla (20–1000) MHz	≤ 80 W
	dla (0,8–3) GHz	≤ 128 W
Szerokość pasma zagłuszanego jednocześnie	dla (20–1000) MHz	≤ 240 MHz
	dla (0,8–3) GHz	≤ 528 MHz
Metoda zagłuszania		Bariera szerokopasmowa
Pobór mocy z sieci elektroenergetycznej		< 1,6 kW (ok. 2,2 kW przy uruchamianiu)
Sterowanie		– przewodowe — LAN – panel dotykowy
Rodzaj elementów promieniujących		– 3 anteny dookólne – kable promieniujące
Zastosowanie		– ochrona obiektów mobilnych przed RCIED na terenie otwartym – zagłuszanie sieci komórkowych w pomieszczeniach – zagłuszanie dowolnych sieci radiokomunikacyjnych – możliwość dostosowania parametrów do wymagań obiorcy

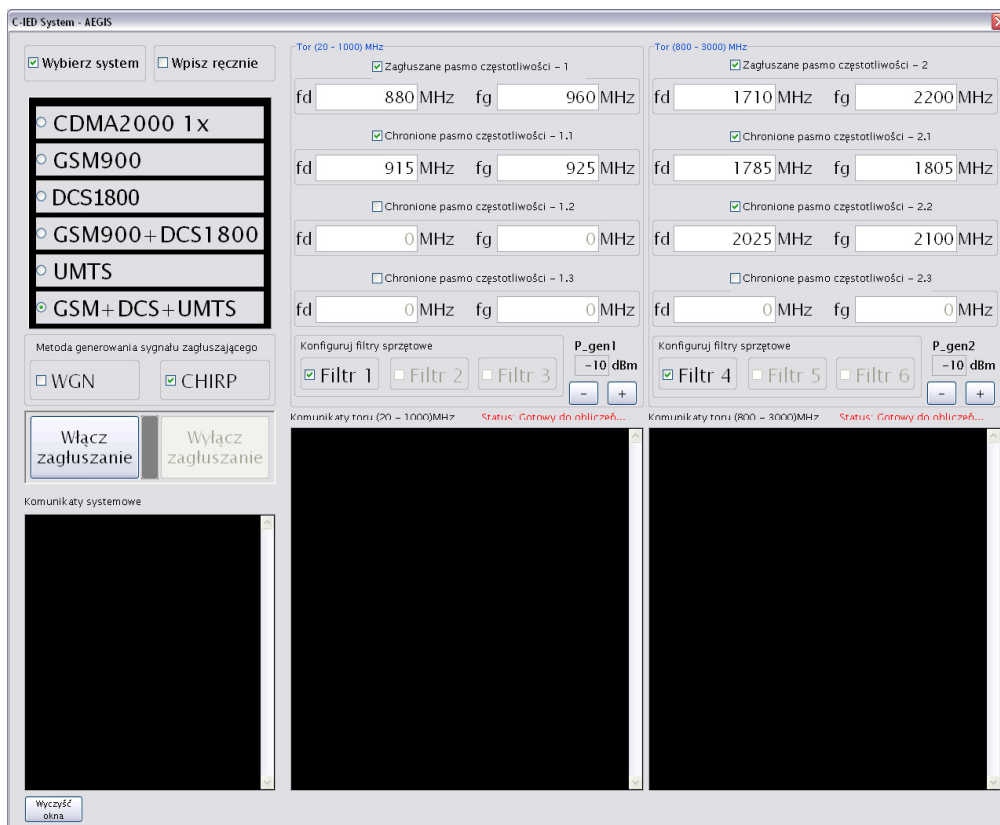
Źródło: opracowanie własne.

INTERFEJS UŻYTKOWNIKA

Na rysunkach 2. i 3. przedstawiony został interfejs użytkownika, który widoczny jest na panelu dotykowym nadajnika AEGIS. Poprzez interfejs użytkownik może wybierać standardowy system do zagłuszania lub wprowadzać parametry sygnału zagłuszającego, wraz z chronionymi pasmami częstotliwości, za pośrednictwem klawiatury numerycznej.

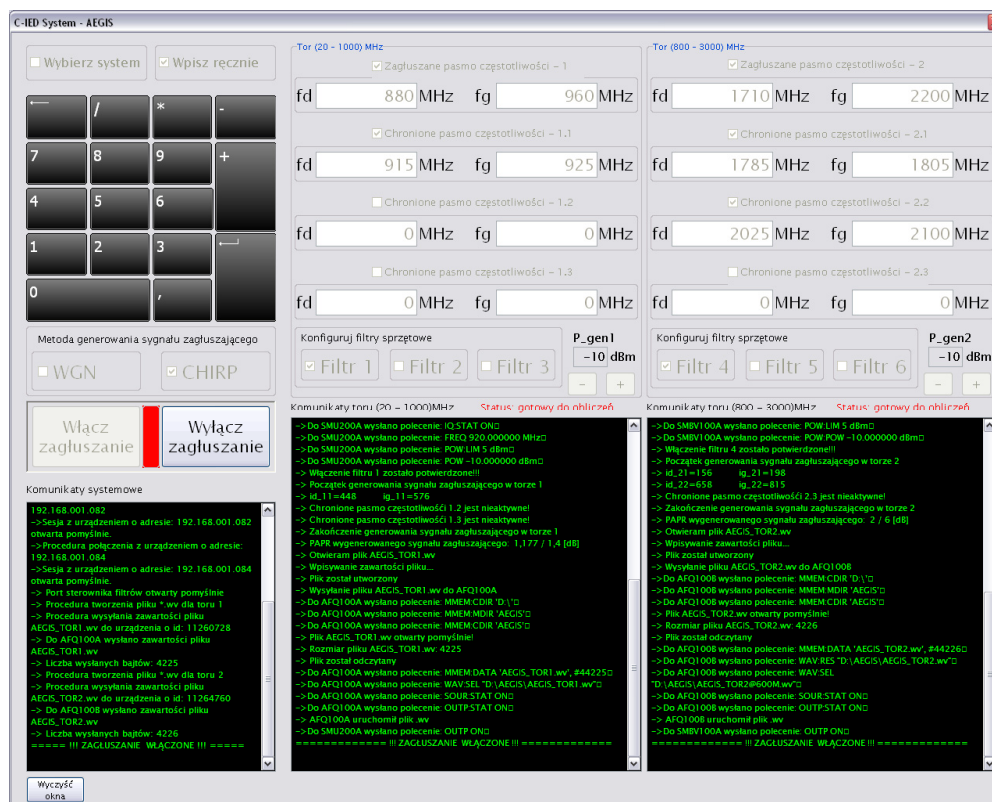
Ponadto możliwy jest wybór metody generowania sygnału zagłuszającego: WGN — na bazie białego szumu gaussowskiego lub CHIRP — na bazie sygnałów z przemiataniem częstotliwości. Użytkownik może także włączać poszczególne

filtry sprzętowe w tor sygnału zagłuszającego oraz sterować mocą poszczególnych generatorów. Pozostałe operacje wykonywane są przez komputer sterujący automatycznie, na podstawie wprowadzonych parametrów oraz zapisanego w pamięci algorytmu pracy.



Rys. 2. Wygląd interfejsu użytkownika — wybór systemu, zagłuszanie wyłączone

Źródło: opracowanie własne.



Rys. 3. Wygląd interfejsu użytkownika — ręczna konfiguracja, zagłuszanie włączone

Źródło: opracowanie własne.

PODSUMOWANIE

W artykule przedstawiono nadajnik systemu AEGIS, emitujący barierę elektromagnetyczną w paśmie od 20 MHz do 3 GHz. Pasma to obejmuje główny zakres środków, jakie można wykorzystać do bezprzewodowej detonacji IED [7]. Dodatkowo przewidziano możliwość określania przez operatora tzw. pasm chronionych, dzięki czemu możliwe jest przeciwdziałanie detonacji urządzeń RCIED, przy jednoczesnym zapewnieniu ciągłości własnej komunikacji. Nadajnik systemu AEGIS jest łatwy w obsłudze dzięki intuicyjnemu interfejsowi użytkownika, natomiast wybór zakłócanych pasm jest ułatwiony dzięki zastosowaniu ekranu dotykowego. Takie rozwiązania pozwalają na dopuszczenie do obsługi urządzenia osoby po krótkim przeszkoleniu.

Zaangażowanie polskiego wojska w ramach międzynarodowych sił wsparcia bezpieczeństwa w Afganistanie ISAF (*International Security Assistance Force*) wymagało i nadal wymaga zapewnienia polskim żołnierzom maksimum bezpieczeństwa. W tym celu wyposażono ich na przykład w systemy obezwładniania elektromagnetycznego. Obecnie przez Siły Zbrojne RP stosowane są między innymi system EJOB-MB izraelskiej firmy Elisra czy wypożyczone od Amerykanów urządzenia zagłuszające DUKE — AN/VLQ-12(V)2 [4].

Należy zwrócić uwagę na fakt, że żaden z oferowanych na rynku systemów nie jest w pełni polskim produktem. Co najwyżej może być dystrybuowany przez polskich pośredników. Taki stan rzeczy był głównym powodem rozpoczęcia prac nad systemem AEGIS, do którego głównych zalet należą: szerokie pasmo generowanych sygnałów zagłuszających, możliwość wyboru wąskich pasm chronionych, a także nieskomplikowana obsługa. Warto też podkreślić, że rozwiązania zastosowane w nadajniku zagłuszającym AEGIS stanowią przedmiot zgłoszenia patentowego P.398050 [2].

Podziękowania

Praca naukowa była finansowana ze środków na naukę w latach 2010–2012 w postaci projektu rozwojowego nr O R00 0007 12. Autorzy pracy pragną podziękować za przydzielone na ten cel środki finansowe.

BIBLIOGRAFIA

- [1] Ambroziak R., Ambroziak S. J., Katulski R. J., *Metody walki z prowizorycznymi urządzeniami wybuchowymi w świetle doktryny AJP-3.15*, „Zeszyty Naukowe WSOWL”, 2011, nr 4, s. 28–37.
- [2] Ambroziak S. J., Katulski R. J., Sadowski J., Stefański J., *Układ do kształtowania widma sygnału radiowego*, zgłoszenie patentowe P.398050, 2012.
- [3] Ciszewski T., *Zarządzanie sytuacją kryzysową w środowisku zagrożonym IED*, „Zeszyty Naukowe WSOWL”, 2010, nr 3, s. 205–224.
- [4] Hołdanowicz G., *Czeskie narzędzie przeciw R2CID*, „RAPORT — Wojsko, Technika, Obronność”, 2010, nr 4, s. 26–29.
- [5] Kowalkowski S., *Improwizowane urządzenia wybuchowe — definicje*, „Przegląd Wojsk Lądowych”, 2010, nr 6, s. 22–27.

- [6] Kowalkowski S., *Zagrożenia i przeciwdziałanie IED*, „Przegląd Wojsk Lądowych”, 2009, nr 5, s. 26–37.
- [7] Witczak A., Fiszer R., Saslekov E., *Mobilne systemy obezwładniania elektronicznego — możliwości realizacji*, VIII Konferencja Naukowo-Techniczna KNTWE '10 „Systemy rozpoznania i walki elektronicznej”, Pisz, 23–25 listopada 2010.

AEGIS — THE C-IED TECHNOLOGY DEMONSTRATOR

ABSTRACT

The article presents a technology demonstrator of AEGIS system, destined for Countering Improvised Explosives Devices. An implemented original method of generation of the jamming signal with freely shaped frequency spectrum is also presented. This method is a subject of patent application No. P.398050.

Keywords:

improvised explosive devices, IED, C-IED, RCIED, technology demonstrator.