MOŻLIWOŚCI I OGRANICZENIA SYSTEMU OCHRONY PRZED RCIED

Kamil WILGUCKI, Robert URBAN, Grzegorz BARANOWSKI, Piotr GRĄDZKI, Paweł SKARŻYŃSKI

Zakład Radiokomunikacji i Walki Elektronicznej
Wojskowy Instytut Łączności
05-130 Zegrze, ul. Warszawska 22 A

Streszczenie

W ostatnich latach obserwowane jest zwiększenie liczby ataków na konwoje i pojazdy wojskowe przy wykorzystaniu improwizowanych urządzeń wybuchowych (IED - Improvised Explosive Devices). Urządzenia te są skuteczne, a jednocześnie wykonane stosunkowo niewielkim kosztem, najczęściej z elementów ogólnie dostępnych. IED są stosowane przez różnego rodzaju organizacje zbrojne i terrorystyczne, do niszczenia siły żywej i sprzętu wojskowego przeciwnika. Ładunki wybuchowe mogą być zdetonowane przy wykorzystaniu różnych, najczęściej niestandardowych technik, w tym bezprzewodowych (RCIED - Radio Controlled IED). Zminimalizowanie tych zagrożeń jest zadaniem niezwykle trudnym z uwagi na nieustanne doskonalenie oraz zmiany taktyki stosowania RCIED, co wpływa na konieczność modyfikacji systemów detekcji i przeciwdziałania.

W artykule opisano znane techniki i technologie stosowane do wyzwalania i zakłócania RCIED. Wymieniono obecnie wykorzystywane urządzenia do ochrony przed RCIED oraz wskazano na istotne wymagania i ograniczenia technologiczne, które wpływają na skuteczność ich działania. Następnie przedstawiono własną koncepcję systemu rozpoznania i przeciwdziałania RCIED, zaproponowano algorytmy jego pracy oraz wymieniono poszczególne bloki funkcjonalne. W podsumowaniu przedstawiono krótką analizę efektywności proponowanego systemu, podczas rozpoznania i zakłócania emisji służących do wyzwalania ładunków wybuchowych.

Słowa kluczowe: RCIED, monitoring widma, zakłócanie sygnałów radiowych

WSTĘP

Improwizowane urządzenia wybuchowe są główną przyczyną śmierci żołnierzy międzynarodowych kontyngentów sił stabilizacyjnych w Iraku i Afganistanie [1]. Powstrzymanie tego zagrożenia jest jednym z priorytetów w obszarze zapewnienia bezpieczeństwa żołnierzy uczestniczących w misjach. Badaniami w zakresie zwiększenia odporności na oddziaływanie IED zajmują się środowiska naukowe na całym świecie. Każdego roku organizowane są liczne międzynarodowe konferencje[1] poświęcone zagadnieniom przeciwdziałania IED. Również w naszym kraju problematyka to jest aktualna w związku z nasileniem ataków z wykorzystaniem IED na konwoje i pojazdy uczestniczące w misjach stabilizacyjnych.

Zminimalizowanie zagrożeń związanych z IED jest zadaniem wyjątkowo trudnym z uwagi na nieustanne doskonalenie i modyfikację konstrukcji bomb oraz taktyki ich stosowania, za którymi musi nadążać modyfikacja systemów detekcyjnych i przeciwdziałających. Ładunki wybuchowe mogą być zdetonowane przy wykorzystaniu różnorodnych, najczęściej niestandardowych metod, łącznie z metodami bezprzewodowymi [2]. Metody stosowania IED stale się zmieniają, ponieważ ich skuteczność w dużej mierze zależy od efektu zaskoczenia. Ponadto łatwy dostęp do urządzeń radiowych i ich niewielki koszt utrudnia kontrolę rynku i eliminację projektantów bomb. Szkolenie żołnierzy polegające na rozpoznawaniu ewentualnych zagrożeń związanych z IED oraz ich prawidłowej reakcji

1 Defeating IEDs Conference San Diego, CA, December 6-8.2011 USA; NATO Counter-Improvised Explosive Device (C-IED) Conference 15 - 17 May 2012 Joint Force Training Centre Bydgoszcz Poland, 6th Annual Counter-IEDs Conference London, United Kingdom 30 - 31 May 2012, Counter IED India, 3-5 October 2012, Mumbai India, 7th Annual "Countering IEDs" conference, December 7-9, Washington DC USA.

może przynieść pewne efekty, jednak bez odpowiednich urządzeń pozwalających wykryć, bądź zneutralizować działanie sygnałów inicjujących eksplozję, zapewnienie właściwego bezpieczeństwa żołnierzy jest praktycznie niemożliwe.

W kolejnych punktach artykułu przedstawiono zagadnienia dotyczące możliwości stosowania systemu ochrony przed improwizowanymi urządzeniami wybuchowymi sterowanymi radiowo (RCIED) oraz omówiono ograniczenia, które należy uwzględnić przy projektowaniu takiego systemu. Następnie, na podstawie przyjętych założeń zaproponowano koncepcję sytemu ochrony przed RCIED (SO-RCIED).

1. URZĄDZENIA IED

Improwizowane urządzenia wybuchowe są stosowane przez różnego rodzaju organizacje zbrojne i terrorystyczne, do niszczenia siły żywej i sprzętu wojskowego przeciwnika. Urządzenia IED jako miny pułapki są bardzo skuteczne pomimo stosunkowo niskich nakładów finansowych przeznaczonych na ich wykonanie. W skład takiego urządzenia wchodzą m.in.:

- materiał wybuchowy,
- urządzenie pobudzające (przełącznik),
- środek inicjujący wybuch (zapalnik),
- źródło zasilania,
- kadłub (opakowanie),
- opcjonalnie element zwiększający skuteczność [2].

Urządzenia IED można podzielić na trzy zasadnicze kategorie w zależności od sposobu inicjowania wybuchu. Mogą to być urządzenia pułapki (*Victim Operated*) uruchamiane m.in. przez nacisk, poruszenie ładunku, a także urządzenia czasowe (*Timed*) aktywowane różnego rodzaju przełącznikami czasowymi. Do ostatniej grupy można zakwalifikować urządzenia detonowane na komendę (*Command Operated*), np. poprzez wyciągniecie zawleczki lub wysłanie impulsu elektrycznego. Urządzenia RCIED należą do grupy urządzeń detonowanych na komendę, która przesyłana jest drogą radiową do odbiornika połączonego z układem sterującym, aktywującym zapalnik. Do tego celu mogą służyć m.in. telefony komórkowe, pagery, sterowniki alarmów samochodowych, bezprzewodowe dzwonki do drzwi, zdalnie sterowane zabawki, ale również zmodyfikowane radiostacje doręczne VHF/UHF oraz telefony satelitarne. Wykorzystywane zakresy częstotliwości oraz skrótowy przegląd sygnałów radiokomunikacyjnych stosowanych do sterowania IED przedstawiono w tabeli nr 1 [3]. Oczywiście możliwe jest także wykorzystanie bardziej zaawansowanych technik do inicjacji RCIED jak np. urządzeń pracujących w niestandardowych pasmach częstotliwości, stosujących transmisję z rozproszonym widmem czy jednoczesną transmisję sygnału na wielu częstotliwościach. Takie techniki są trudniejsze do wykrycia i efektywnego zakłócenia, ale również są bardziej kosztowne i wymagają od konstruktora większej wiedzy oraz odpowiedniego zaplecza technicznego.

Najprostszą metodą pozwalającą zapobiec aktywacji urządzeń RCIED jest zakłócenie sygnału radiowego inicjującego wybuch. Wykrycie takiego sygnału jest zadaniem trudnym ze względu na krótki czas emisji oraz szeroki zakres częstotliwości w którym może się on pojawić, obejmujący przede wszystkim pasma komercyjne. Skuteczne zakłócenie całego pasma częstotliwości jest praktycznie niemożliwe i pozbawione sensu z uwagi na zablokowanie własnej łączności radiowej. Dlatego też należy zapewnić selektywne zakłócanie emisji sklasyfikowanych jako stanowiące zagrożenie, uwzględniając informacje uzyskane z monitoringu widma elektromagnetycznego i detekcji sygnałów radiowych.

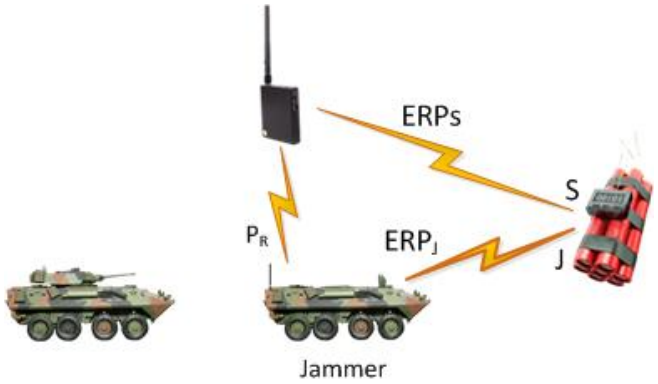
Tabela 1. Przykładowe sygnały radiokomunikacyjne wykorzystywane do sterowania IED [2].

Typ radia	**Zakres częstotliwości**	**Max. moc nadajnika**	**Zasięg (wys. anteny 1m)**
Radio CB (Citizens' Band)	26÷28MHz	12W	40km
Zdalnie sterowane zabawki	27MHz, 35MHz, 40MHz, 49MHz, 72MHz, 75MHz, 2,4GHz, 5GHz	100mW	500m
Bezprzewodowe dzwonki i sterowniki bram	26÷40MHz, 400÷440MHz, 860÷870MHz	10mW	300m
Alarmy samochodowe	300÷315MHz,430÷450MHz, 860÷870MHz	3mW	100m
Transmisje analogowe VHF/UHF	26÷108MHz, 146÷174MHz, 433MHz, 446MHz, 800÷870MHz	25W	50km
Transmisje analogowe i cyfrowe ISM	40,66÷40,70MHz, 433÷435 MHz, 868÷870MHz, 902÷928MHz, 2,4÷2,5MHz	100mW	500m
PMR (Private Mobile Radio)	154MHz, 446MHz	1W	5km
DECT (Digital European Cordless Telephone)	1880÷1900MHz (Europe), 1900÷1920MHz (China), 1910÷1930MHz (L. America), 1920÷1930MHz (USA, Canada)	250mW	200m
GSM (Global System for Mobile Communications)	450÷470MHz, 478÷496MHz, 824÷894MHz, 880÷960MHz, 1710÷1880MHz, 1850÷1990MHz	500mW	10km
UMTS (Universal Mobile Telecommunications System)	1805÷1880MHz, 1920÷2170MHz, 2620÷2690MHz	500mW	1km
Telefony satelitarne	1626.5-1660.5 MHz 1525-1559 MHz	500mW/100W	global
WLAN (Wireless Local Area Network)	2.4÷2.5GHz, 5.1÷5.8GHz*	100mW (4W*)	300m (6km*)
WiMax	2620÷2690MHz, 3,4HGz÷3,8GHz	500mW	1km

2. PROBLEMY SKUTECZNEJ OCHRONY PRZED RCIED

Skuteczna ochrona przed RCIED wymaga zastosowania odpowiedniego zestawu zakłócającego sygnały radiowe inicjujące wybuch. Z danych przedstawionych w tabeli 1 wynika, że zakres częstotliwości jest praktycznie nieograniczony i zależy jedynie od inwencji i możliwości technologicznych projektantów RCIED. Zestaw zakłócający powinien zapewnić strefę ochronną obejmującą otoczenie wozów i patrolów pieszych (rys. 1), a z uwagi na krótki czas trwania emisji wyzwalającej, natychmiastową reakcję na jej wykrycie. Jednocześnie należy przewidzieć możliwość zdefiniowania zabronionych do zakłócania pasm częstotliwości, aby nie zakłócać własnych środków łączności.

Parametrem określającym efektywność zakłócania jest JSR (*jamming (J) to signal (S) ratio*), który przedstawia stosunek mocy sygnału zakłócającego do mocy sygnału zakłócanego [4,5].



Rys. 1. Schemat ochrony przed RCIED

(gdzie: ERP_J – efektywna moc promieniowania zakłóceń, ERP_S – efektywna moc promieniowania sygnału inicjującego RCIED, P_R – odbierana moc promieniowana sygnału inicjującego RCIED)

Minimalna wartość JSR wymagana do skutecznego zakłócenia sygnału wyzwalającego zależy przede wszystkim od jego rodzaju, warunków propagacyjnych i zastosowanej techniki zakłócania. Można wyróżnić kilka technik, które obejmują zakłócanie [5]:

- szumem szeroko i wąskopasmowym (*noise jamming*),
- nośną (*tone jamming*),
- przestrajaną nośną (*swept jamming*),
- impulsami (*pulse jamming*),
- odzewowe (*follower jamming*),
- inteligentne (*smart jamming*).

Wykrywanie i zakłócanie sygnałów sterujących RCIED różni się od typowych działań walki elektronicznej EW (*electronic warfare*) mających na celu przechwycenie, analizowanie i zakłócanie łączności radiowej przeciwnika. W wojskowych urządzeniach radiokomunikacyjnych, w przeciwieństwie do domowej roboty sterowników RCIED, są zaimplementowane mechanizmy ECCM (*electronic counter-countermeasures*) mające na celu utrudnienie, redukcję bądź eliminację wpływu zakłóceń. W tym przypadku czas reakcji systemu zakłócającego może być dłuższy, poprzedzony dokładną analizą, identyfikacją i lokalizacją sygnału. Transmitowana informacja z reguły trwa kilka sekund (z wyjątkiem urządzeń sterowania ogniem) i nie wpływa bezpośrednio na zagrożenie życia żołnierzy.

W przypadku ochrony przed RCIED sygnały inicjujące są bardzo krótkie i pojawiają się zwykle jednorazowo na danym obszarze. Z tego względu nie ma możliwości zastosowania wyrafinowanych metod detekcji oraz identyfikacji sygnałów, a priorytetem jest szybka reakcja na każdy pojawiający się sygnał i jego skuteczne zakłócenie, aby uniemożliwić wywołanie wybuchu. Dzięki temu, że konwój przemieszcza się i mija możliwe miejsca instalacji ładunków, zagrożenie eksplozją jest ograniczone w czasie i dotyczy określonych lokalizacji. Zatem czas trwania zakłóceń w odpowiedzi na pojawiający się sygnał inicjujący RCIED jest zależny od prędkości pojazdów konwoju, które w kilkadziesiąt sekund są w stanie opuścić niebezpieczną strefę. Można wówczas wyłączyć zakłócanie i przejść do trybu monitoringu widma. Działanie SO-RCIED w tym trybie ma zasadnicze znaczenie, ponieważ informacja z monitoringu musi być stale aktualizowana. W przypadku transmisji cyfrowych nie ma konieczności ich ciągłego zakłócania, aby skutecznie zablokować odbiór takiej emisji wystarczy zakłócić ok. jednej trzeciej sygnału w dziedzinie czasu lub częstotliwości [4]. W pozostałym okresie czasu można kontynuować monitoring prowadząc kontrolę zakłócanego kanału i akwizycję celów w innych pasmach częstotliwości.

Inna cechą odróżniającą zakłócanie RCIED od klasycznej EW jest to, że typowe wojskowe stacje zakłóceń mają bardziej skomplikowaną budowę i są przeznaczone do pracy na postoju (z wyjątkiem platform latających). W przeciwieństwie do nich systemy ochrony przed RCIED są stosunkowo niewielkich rozmiarów, projektowane jako urządzenia przewoźne lub przenośne. Wpływa to oczywiście na ich skuteczność ze względu na ograniczone źródło zasilania i rozmiary anten.

Znaczący wpływ na efektywność zakłócania ma typ urządzenia wykorzystywanego do przesłania sygnału inicjującego RCIED. W większości przypadków sygnał inicjujący jest generowany przez ogólnodostępne środki radiowe lub komercyjne systemy telekomunikacyjne (pkt 1). Urządzenia komercyjne jest łatwiej zakłócić, ponieważ znana jest struktura sygnałów i wykorzystywanych przez nie częstotliwości, dzięki czemu możliwe jest przygotowanie optymalnych sygnałów i algorytmów zakłócających dla określonego systemu. Zasadniczą trudnością jest nieprzewidywalność co do typu użytego sygnału i ogromna różnorodność możliwych do wykorzystania rozwiązań. Każdy z wymienionych systemów (tabela 1) ma inną podatność na zakłócanie, którą można określić na podstawie parametrów takich jak maksymalny czas opóźnienia pomiędzy początkiem transmisji sygnału a momentem rozpoczęcia zakłóceń oraz wymagany minimalny czas sygnału zakłócającego aby efektywnie uniemożliwić odbiór sygnału. Wartość tych parametrów można uzyskać z dokumentacji, pomiarów lub przeprowadzonych eksperymentów. Maksymalny czas opóźnienia warunkuje szybkość wykrywania emisji i w najgorszych przypadkach, dla transmisji cyfrowych wynosi poniżej 100ms. Natomiast minimalny czas sygnału zakłócającego w przypadku, gdy jest on zsynchronizowany z sygnałem zakłócanym wynosi od kilku μs do kilkudziesięciu ms, w przeciwnym razie stanowi od 1% do 30% czasu trwania transmitowanego sygnału, w zależności od systemu transmisji.

2.1 Możliwości i ograniczenia SO-RCIED

Analizując możliwości budowy systemu ochrony przed RCIED konieczne jest uwzględnienie kilku aspektów odnoszących się do właściwości odbiornika/detektora, modułu zakłócającego, a także wpływu warunków propagacji i typu terenu.

Właściwości odbiornika/detektora:

- szybkość przestrajania odbiornika (szybkość syntezera i jego stabilność oraz szybkość filtrów preselekcyjnych),
- wysoki zakres dynamiki > 90dB,

- odporność na wysoki poziom sygnału na wejściu odbiornika (poziomy > +30dBm),
- wysoka czułość, zbliżona do wymagań na telefony komórkowe ale przy szerszym paśmie,
- szeroki zakres częstotliwości do poszukiwania emisji,
- wysokiej jakości przetworniki A/C z rozdzielczością 16 bitów,
- wykorzystanie odpowiedniej transformaty czasowo-częstotliwościowej ze zoptymalizowaną rozdzielczością w czasie i częstotliwości,
- złożoność obliczeniowa algorytmu wykrywania i identyfikacji zagrożeń wymagająca zastosowania FPGA i procesora DSP,
- czas na analizę zakresu częstotliwości musi być krótszy niż maksymalny czas opóźnienia pomiędzy początkiem transmisji sygnału a momentem rozpoczęcia zakłóceń.

Właściwości modułu zakłócającego:

- krótki czas strojenia upconvertera, niższy niż 1ms,
- krótki czas reakcji wzbudnika (należy uwzględnić czasu dostępu do pamięci, ładowania i przełączania waveformów),
- wysokiej jakości przetworniki C/A z rozdzielczością 16 bitów,
- wydajny i odporny na wysoką temperaturę pracy wzmacniacz,
- wykorzystanie filtrów RF na wyjściu wzmacniacza do ochrony zakresów częstotliwości wykorzystywanych przez własne systemy radiokomunikacyjne,
- wykorzystanie zakłócania selektywnego, dopasowanego do struktury sygnału, wymagającego synchronizacji czasowej i częstotliwościowej.

Warunki propagacji, typ terenu i zaników:

- wpływ wysokości i położenia anteny zestawu zakłócającego na rozkład charakterystyki promieniowania i zasięg,
- wpływ położenia anteny odbiornika RCIED na skuteczność zakłócania w warunkach zaników [6],
- wpływ typu terenu na zasięg zakłóceń (przenikalności dielektrycznej gruntu), niesprzyjający zwłaszcza w terenie górzystym i suchym,
- bilans energetyczny łącza radiowego (uwzględniający wysokość anten, ich zysk i rzeczywistą moc promieniowaną).

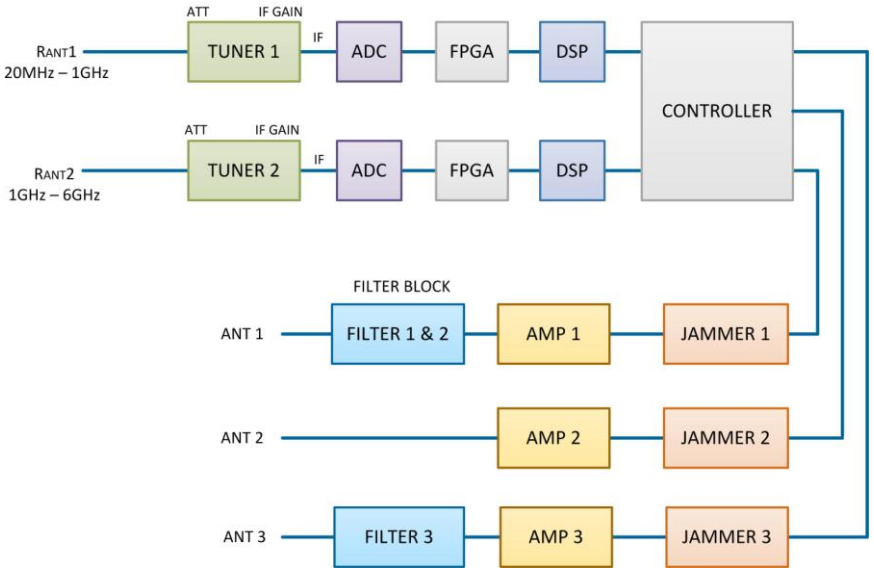
3. KONCEPCJA SYSTEMU

W WIŁ prowadzone są prace mające na celu opracowanie modelu inteligentnego SO-RCIED, pracującego w trybie reaktywnym, który mógłby być instalowany na platformach mobilnych. Tego typu zestawy zakłócające znalazły dotychczas na świecie nieliczne implementacje, np. Crew Duke w armii Stanów Zjednoczonych [6]. Podobne projekty są we wstępnej fazie nawet w zaawansowanych technologicznie państwach europejskich. Technologia potrzebna do realizacji takiego projektu jest dostępna w naszym kraju, dlatego prace będą kontynuowane, a uzyskane rezultaty znajdą zastosowanie przy budowie innych systemów zapewniających ochronę i przetrwanie na polu walki.

Uwzględniając przedstawione w pkt. 2 możliwości i ograniczenia realizacji skutecznej ochrony przed RCIED przyjęto następujące założenia na budowę SO-RCIED:

- możliwe równoczesne, wielozakresowe monitorowanie widma i generacja zakłóceń w trybie odzewowym i zaporowym,
- prowadzenie równolegle wielozakresowej detekcji, klasyfikacji i pomiaru parametrów odbieranych emisji (przetwarzanie sygnałów w układach FPGA i DSP),
- wykorzystanie zestawu filtrów kolokacyjnych w celu eliminacji pozapasmowych zakłóceń, do ochrony własnych środków łączności,
- udostępnienie interfejsów programowych do efektywnego zarządzania i ochrony zasobów częstotliwości oraz planowania zakłóceń,
- zapewnienie możliwości pracy kooperacyjnej większej ilości zestawów SO-RCIED w jednej sieci w celu zwiększenia skuteczności zakłóceń,
- zachowanie kompaktowej budowy przystosowanej do montażu na dowolnej platformie mobilnej (ograniczenie rozmiarów i wagi oraz wykorzystanie tylko 2 szt. anten).

Na rys 2 przedstawiono schemat blokowy proponowanego systemu SO-RCIED.



Rys. 2. Schemat blokowy proponowanego systemu SO-RCIED

Na schemacie można wyróżnić część odbiorczą składającą się z dwóch torów odbiorczych, sterownik pracy systemu oraz część nadawczą z trzema wzbudnikami i wzmacniaczami. Opracowany model będzie posiadał dwie anteny: dwuzakresową antenę

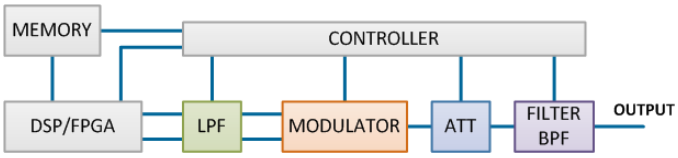
odbiorczą (20MHz÷1GHz, 1GHz÷6GHz) i trójzakresową antenę nadawczą (20÷500MHz, 500÷1000MHz, 1÷6GHz)). Dodatkowo będzie udostępniony interfejs użytkownika, który pozwoli zaprogramować pasma częstotliwości do zakłócania oraz pasma zabronione przeznaczone dla własnych środków łączności.

Algorytm pracy SO-RCIED obejmuje trzy podstawowe funkcje:

- odbiór i analizę sygnałów,
- podjęcie decyzji o zakłócaniu,
- generacja zakłóceń.

Odbiorniki wraz z modułami DSP/FPGA będą przeprowadzać ciągły monitoring, detekcję i ogólną klasyfikację sygnałów pod względem zakresu częstotliwości, pasma sygnału, rodzaju emisji (swój-obcy). Po wykryciu sygnału, który zostanie sklasyfikowany jako niebezpieczny, sterownik pracy systemu uruchomi generację zakłóceń w odpowiednim bloku wzbudników (rys. 3). Następnie sygnał/sygnały zakłócające podane zostaną na bloki wzmacniaczy i po przejściu przez filtry kolokacyjne przesłane do anteny. Poszczególne wzmacniacze będą dopasowane do odpowiedniej sekcji anteny nadawczej. Sygnały zakłócające będą generowane w trzech pasmach: 20÷500MHz, 500÷1000MHz, 1÷6GHz. Przewiduje się wykorzystanie kilku technik zakłócania:

- szumem szeroko i wąskopasmowym,
- przestrajaną nośną,
- odzewowe,
- inteligentne (wykorzystując wcześniej przygotowane sygnały z pamięci sterownika).



Rys. 3. Schemat blokowy wzbudnika

4. PODSUMOWANIE

Zautomatyzowany SO-RCIED będzie zapewniał możliwość prowadzenia jednoczesnego monitoringu widma i zakłócania kilku pasm częstotliwości. Wykorzystanie takiego systemu pozwoli na, szybką reakcję na pojawiające się sygnały radiowe i możliwość zakłócania kilku emisji jednocześnie. Projektowany system może być wykorzystany zarówno w kraju, jak i na misjach, przez służby ustawowo powołane do działań w obliczu zagrożeń terrorystycznych.

Ograniczenia wynikające ze specyfiki użycia RCIED i możliwości technicznych mobilnych zestawów zakłócających mają wpływ na budowę SO-RCIED. Przede wszystkim projektowany system musi mieć ograniczone wymiary (urządzenia, anteny) i powinien być dostosowany do działania przy wykorzystaniu ograniczonych źródeł zasilania dostępnych w miejscach instalacji na platformach mobilnych. W efekcie strefa ochrony jest ograniczona, dlatego ważne jest prowadzenie stałego monitoringu i precyzyjne zakłócanie wykrytych emisji w celu efektywnego wykorzystania mocy wzmacniaczy.

Istotny jest również rodzaj odbiornika, zastosowanych algorytmów detekcji i technik zakłócania sygnałów, które muszą zapewnić szybkie działanie ze względu na różnorodność i krótki czas trwania emisji, które mogą inicjować wybuch IED. Podczas projektowania systemu należy pamiętać, że jego działanie może spowodować zakłócenia łączności wojsk własnych i sojuszniczych. Konieczne jest zatem zarządzanie częstotliwościami w systemie, stosowanie odpowiednio przygotowanych sygnałów zakłócających oraz zapewnienie filtracji niepożądanych produktów na wyjściu wzmacniaczy.

Zwiększenie skuteczności detekcji i zakłócania można osiągnąć wykorzystując kilka systemów SO-RCIED pracujących w kooperacyjnej sieci, w ramach jednego konwoju lub strefy, która wymaga ochrony. Taki system zwiększy możliwość przeciwdziałania RCIED dzięki wymianie informacji uzyskanych z monitoringu widma. Nadajniki pracujące w sieci kooperacyjnej mogą zakłócać te same emisje zwiększając w ten sposób strefę ochrony i zmniejszając wpływ zaników na efektywność zakłócania [7] lub zakłócać jednocześnie kilka emisji w różnych pasmach częstotliwości. Odbiorniki natomiast mogą zapewnić wyższe prawdopodobieństwo detekcji lub krótszy czas skanowania widma. Dodatkowo fizyczna separacja nadajników i odbiorników zainstalowanych w różnych obiektach zapewni lepszą czułość i zwiększy zasięg wykrywania emisji. Komunikacja pomiędzy elementami sieci może być prowadzona przy wykorzystaniu połączeń bezprzewodowych pracujących w wojskowych zakresach częstotliwości np. 4,4GHz, stosując Podsystem Dostępu Bezprzewodowego (PDB) opracowany w WIŁ [8].

LITERATURA

[1] https://www.jieddo.dod.mil/content/docs/JIEDDO_2010_Annual_Report_U.pdf.

[2] P. Saska, F. Klimentowski, P. Kowalczyk, *Charakterystyka Improwizowanych Urządzeń Wybuchowych stosowanych w konflikcie irackim*, Zeszyty Naukowe WSOWL 2008.

[3] K. Wilgucki, R. Urban, G. Baranowski, P. Grądzki, P. Skarżyński, *Automated protection system against RCIED*, MCC2011.

[4] D. L. Adamy, *Tactical Battlefield Communications Electronic Warfare*, Artech House, Inc., 2009 pp. 251-306.

[5] R. A. Poisel, *Modern Communications Jamming Principles and Techniques*, Second Edition, Artech House, Inc., 2011.

[6] http://srcinc.com/uploadedFiles/src/what-we-do/CREW_Duke.pdf.

[7] A. Graham, *Communications, Radar and Electronic Warfare*, John Willey& Sons, Inc., 2011, pp. 137-144, 357-363.

[8] J. Romanik, K. Kosmowski, E. Golan, *Ocena możliwości zastosowania sieci bezprzewodowych WLAN i WiMAX w systemach taktycznych: Wyniki testów wybranych rozwiązań*, Przegląd Telekomunikacyjny - Wiadomości Telekomunikacyjne 2011, Nr 1, s. 23-26 [C-97].