AKADEMIA
OBRONY NARODOWEJ

ZAKŁÓCANIE INFORMACYJNE W OPERACJACH WOJSK LĄDOWYCH

Praca badawcza

WARSZAWA 2001

AKADEMIA OBRONY NARODOWEJ

WYDZIAŁ WOJSK LĄDOWYCH

ZAKŁÓCANIE INFORMACYJNE W OPERACJACH WOJSK LĄDOWYCH

Praca -badawcza wykonana w ramach tematu „INFO-2"

pod kierownictwem i redakcją naukową dr. inż. Józefa JANCZAKA

Kod pracy: 3.15.5.0

WARSZAWA **2001**

Recenzent:

Prof. dr hab. Leopold CIBOROWSKI

Opracował zespół autorski pod kierownictwem i redakcją naukową

dr. inż. Józefa JANCZAKA

Poszczególni członkowie opracowali:

1. dr inż. Józef JANCZAK – wstęp; rozdział: 1, 2 (bez podrozdziału 2.1.); 3; załączniki.
2. dr inż. Bogdan BEZOŃ – rozdział 2 (bez podrozdziału 2.2); 4; zakończenie.

SPIS TREŚCI

WSTĘP

W siłach zbrojnych wielu państw sukcesywnie podnosi się jakość i możliwości bojowe wojsk, wyposażając je w najnowsze osiągnięcia techniczno - elektroniczne końca XX wieku. Szczególną uwagę zwraca się na rozwój środków wykorzystywanych na potrzeby rozpoznania, dowodzenia wojskami i kierowania uzbrojeniem oraz rażenia ogniowego i zakłócania. Coraz większą uwagę zwraca się na problemy dominacji informacyjnej nad przeciwnikiem. Rozwijana jest teoria walki informacyjnej.

Istota walki informacyjnej sprowadzana jest do stwarzania sytuacji utrudniających przeciwnikowi podejmowanie trafnych decyzji, wykonywania sprawnych ruchów wojskami i precyzyjnych uderzeń ogniowych, przy jednoczesnej obronie przed tym samym wojsk własnych. Innymi słowy, walka informacyjna ukierunkowywana jest na dezorientowanie przeciwnika w rzeczywistej sytuacji pola walki, komplikowanie jego warunków działania i w efekcie tego zmuszanie go do podejmowania błędnych decyzji.

Zdaniem autorów pracy badawczej, w uwarunkowaniach Wojska Polskiego „walka informacyjna" traktowana może być jako teoretyczne rozwinięcie problematyki rozpoznania wojskowego, walki elektronicznej i działań psychologicznych[1].

[1] Zaznaczyć jednak trzeba, że prowadzenie walki informacyjnej nie dotyczy tylko i wyłącznie sił i środków podległych pionowi rozpoznania i walki radioelektronicznej. Odpowiedzialnym za prowadzenie walki informacyjnej powinien być dowódca.

Teoria ta pozwala bowiem na integrację posiadanych sił i środków działających w wymiarze informacyjnym.

Rozwijana teoria walki informacyjnej skłania do postawienia pytania: czy nasze wojska lądowe są obecnie przygotowane do prowadzenia tego typu walki, a w tym szczególnie zakłócania informacyjnego oraz w jakim stopniu proces zakłócania przepływu informacji może wpłynąć na prowadzone przez nie działania wojenne?

Próbę zanalizowania powyższych problemów podęli się autorzy w niniejszej pracy badawczej.

Przedmiotem badań uczyniono zakłócanie informacyjne w operacjach wojsk lądowych, postrzegane jako zespół odpowiednio skoordynowanych przedsięwzięć i działań, które dostosowane są do zakłócania procesów rozpoznania, dowodzenia wojskami i kierowania uzbrojeniem przeciwnika.

Treść poznawcza pracy została podporządkowana **osiągnięciu następującego celu**:

Opracować zbiór naukowo uzasadnionych podstaw teorii przygotowania i prowadzenia zakłócania informacyjnego w operacjach naszych wojsk lądowych w aspekcie zapewnienia ich interoperacyjności w ramach Organizacji Traktatu Północnoatlantyckiego.

Osiągnięcie tak zdefiniowanego celu wyłoniło potrzebę rozwiązania następujących **problemów badawczych**:

1. Jaka jest rola i miejsce zakłócania informacyjnego w operacjach wojsk lądowych?

2. Jaki jest zakres i jaka jest treść zadań zakłócania informacyjnego w operacjach wojsk lądowych?

3. Jaki jest udział zakłócania informacyjnego w strukturach procedur pracy sztabowej oraz przebiegu cyklu decyzyjnego pod kątem jej potrzeb w operacjach wojsk lądowych?

4. Na czym powinno polegać prowadzenie zakłócania informacyjnego w operacjach wojsk lądowych?

Przyjmując określoną procedurę badań autorzy uznali, że rozwiązanie poszczególnych problemów badawczych będzie możliwe w wyniku opracowania problemów szczegółowych, które stanowią nazwy podrozdziałów opracowania i zostały wyszczególnione w spisie treści.

Rozwiązywanie wymienionych problemów badawczych, w aspekcie zdefiniowanego wcześniej przedmiotu i celu poznania, oparto o szeroko rozumianą weryfikację następująco brzmiącej **hipotezy roboczej**:

Zakłócanie informacyjne obejmuje przedsięwzięcia i różne formy działalności w zakresie dezorganizacji pracy środków i systemów wykorzystywanych przez przeciwnika na potrzeby rozpoznania, dowodzenia wojskami i kierowania uzbrojeniem.

Przedsięwzięcia zakłócania informacyjnego powinny być wszechstronnie zaplanowane, zorganizowane i prowadzone w operacjach wojsk lądowych, co stanowi warunek konieczny osiągnięcia przewagi na współczesnym i przyszłym polu walki.

Odpowiedzialność za całokształt problematyki związanej z zakłócaniem informacyjnym ponosi dowódca, zaś organizatorem zadań w zakresie jego przygotowania i prowadzenia jest komórka G 2, przy znaczącym współudziale komórki G 3 i specjalistów rodzajów wojsk i służb.

Proces decyzyjny w zakresie zakłócania informacyjnego należy postrzegać jako integralny element procesu dowodzenia w operacjach wojsk lądowych, realizowanego przez jego dowództwo i sztab, zgodnie z obowiązującymi procedurami i technikami w celu oceny sytuacji (tj. określenia tego co się dzieje), zdecydowania co robić (jakie podjąć działania) oraz postawienia zadań i kontroli ich wykonania.

Do weryfikacji przyjętej hipotezy autorzy wykorzystali **empiryczne i teoretyczne metody badawcze**.

W procesie identyfikacji przedmiotu i obszaru badań wykorzystano przede wszystkim: analizę literatury naukowej, analizę dokumentów walki informacyjnej,

obserwację czynną i bierną. Źródłem faktów były prace naukowe, naukowo-badawcze i promocyjne, podręczniki akademickie, materiały studyjne i kompendia opracowane w Akademii Obrony Narodowej.

Analizą literatury objęto także treści z zakresu teoretycznych możliwości prowadzenia zakłócania procesów informacyjnych w walce zbrojnej wybranych państw. Na potrzeby pracy analizowano: książki, podręczniki, czasopisma wojskowe (krajowe i zagraniczne), popularnonaukowe, doniesienia internetowe oraz komunikaty Wojskowych Służb Informacyjnych.

Z literatury ogólnowojskowej i specjalistycznej wykorzystano głównie: regulaminy walki, instrukcje eksploatacyjno-techniczne sprzętu, zbiory norm taktyczno-technicznych i inne dokumenty normatywne. Ponadto wykorzystano dokumenty, materiały i opracowania z ćwiczeń w AON w latach 1996-2001.

Obserwacje bezpośrednie i twórcze objęły analizę procesów decyzyjnych i informacyjnych zachodzących w Dowództwie Wojsk Lądowych oraz w Oddziałach G 2 okręgów wojskowych. Ponadto przeprowadzono analizę pracy planistycznej ww. komórek sztabowych w trakcie ćwiczeń sztabowych i prowadzonych ćwiczeń z wojskami.

Metody, którymi posłużono się w procesie identyfikacji umożliwiły zbadanie:

– struktur organizacyjnych ww. komórek i jednostek wojskowych;

– struktur systemów informacyjnych jednostek elektronicznych oraz określenie wejść i wyjść informacyjnych dla systemu, sposobów, środków i form przetwarzania danych;

– procesu decyzyjnego zachodzącego podczas przygotowania i prowadzenia zakłócania informacyjnego w operacjach wojsk lądowych.

We wszystkich etapach badań stosowano także dostępne teoretyczne metody badawcze, a w szczególności: syntezę, abstrahowanie, porównanie i analogię.

Wielokrotnie porównywano ze sobą różne procesy zachodzące podczas ćwiczeń organów sztabowych rozpoznania G 2 oraz pracy bojowej podległym im jed-

nostek specjalistycznych. Często prowadziło to do wykorzystywania podobnych algorytmów w różnych etapach pracy badawczej.

Abstrahowanie okazało się metodą konieczną, gdyż w grę wchodził system złożony. Nie wszystkie cechy procesów można było zbadać, gdyż zadanie to przekraczało możliwości zespołu badawczego.

W celu uzyskania obiektywnych wyników badań w obszarze tematu zastosowano metodę badania opinii, którą realizowano poprzez wywiady z osobami zajmującymi się problemami walki informacyjnej w SZ RP.

Proces badawczy podzielono na trzy etapy:

1. Wstępny etap badań.
2. Etap badań właściwych.
3. Końcowy etap badań.

Wstępny etap badań obejmował uświadomienie sytuacji problemowej oraz analizę literatury przedmiotu badań. Analiza sytuacji problemowej oraz określenie celu badań pozwoliły na opracowanie scenariusza badań oraz sprecyzowanie problemów badawczych, określenie przedmiotu i obszaru badań, postawienie hipotezy roboczej a także dobór metod i narzędzi badawczych.

Etap badań właściwych ukierunkowano przede wszystkim na weryfikację hipotezy roboczej. Sprecyzowano odpowiedzialność funkcyjną za zakłócanie informacyjne w wojskach lądowych, określono zadania poszczególnych zespołów funkcjonalnych sztabu DWLąd w zakresie jego realizacji. Określono przebieg cyklu decyzyjnego w zakresie zakłócania informacyjnego w operacjach wojsk lądowych oraz formę i treść niezbędnych dokumentów planistycznych i rozkazodawczych.

W końcowym etapie badań dokonano weryfikacji wyników badań w toku dyskusji i konsultacji naukowych ze specjalistami krajowymi i oficerami państw członków NATO przebywającymi w AON, podczas konferencji naukowych i seminariów. Rezultatem badań tego etapu jest opracowanie zwarte wraz z wnioskami. Ponadto autorzy zamierzają wyniki badań opublikować w prasie specjalistycznej, poddać weryfikacji na kolejnych konferencjach naukowych, seminariach nauko-

wych oraz wykorzystać do opracowania materiałów dydaktycznych na potrzeby AON i innych placówek dydaktycznych sił zbrojnych RP.

Praca badawcza zawiera więc wyniki badań istoty, zakresu i treści przedsięwzięć zakłócania informacyjnego w operacjach wojsk lądowych. Sformułowane wnioski i uogólnienia można w większości wypadków odnieść również do innych rodzajów sił zbrojnych. Praca składa się z wstępu, czterech rozdziałów merytorycznych, zakończenia, bibliografii i załączników.

We wstępie uzasadniono potrzebę wyboru i konieczność rozwiązania problemu naukowego. Przedstawiono również podstawy metodologiczne, niezbędne do przeprowadzenia badań. Szczególną uwagę zwrócono na cel i zakres badań, metody badawcze, które doprowadziły do weryfikacji hipotezy roboczej i osiągnięcia celu badań, oraz ocenę dostępnej literatury przedmiotu badań.

W rozdziale pierwszym przedstawiono istotę zakłócania informacyjnego w operacjach wojsk lądowych. Analizując dostępną literaturę, określono jego rolę i miejsce w przyszłych operacjach wojsk lądowych oraz sprecyzowano przedmiot, cel, rodzaje zakłócania i stawiane wymagania.

W rozdziale drugim zamieszczono wyniki badań obejmujące zakres i treść zadań zakłócania informacyjnego w operacjach wojsk lądowych. Przedstawiono możliwości zakłócania sił i środków przeciwnika wykorzystywanych na potrzeby rozpoznania (bezpośredniego i pośredniego) oraz na potrzeby dowodzenia wojskami i kierowania uzbrojeniem

W rozdziale trzecim opracowano przebieg procesu decyzyjnego pod kątem potrzeb zakłócania informacyjnego w operacjach wojsk lądowych. Sprecyzowano odpowiedzialność funkcyjną za zakłócanie informacyjne w wojskach lądowych, określono zadania poszczególnych zespołów funkcjonalnych sztabu DWLąd w zakresie jego realizacji. Szczególną uwagę zwrócono na przebieg cyklu decyzyjnego w zakresie zakłócania informacyjnego oraz formę i treść niezbędnych dokumentów planistycznych i rozkazodawczych. Przykłady dokumentów zilustrowano graficznie oraz zamieszczono w załącznikach.

W zakończeniu określono zasadność wyboru i sformułowania celu badań, problemów badawczych, przyjętych założeń oraz hipotezy roboczej. Dokonano oceny stopnia realizacji zadań badawczych, a także przedstawiono propozycje dotyczące zastosowania uzyskanych rezultatów oraz kierunki dalszego pogłębiania i rozszerzania badań.

Wyniki badań zamieszczone w pracy badawczej są adresowane głównie do pracowników naukowych instytucji wojskowych i cywilnych zajmujących się tą problematyką, pracowników dydaktycznych i studentów uczelni wojskowych oraz kadry dowódczo-sztabowej wojsk lądowych oraz do osób funkcyjnych Sztabu Generalnego WP, Dowództwa Wojsk Lądowych, sztabów okręgów wojskowych i korpusów.

1. ROLA I MIEJSCE ZAKŁÓCANIA INFORMACYJNEGO W OPERACJACH WOJSK LĄDOWYCH

1.1. Istota zakłócania informacyjnego

Współcześni teoretycy wojskowi[1] zakładają, że obecny model walki zbrojnej obejmuje trzy zasadnicze czynniki: rażenie (ogień), manewr (ruch) i informację. Informację postrzega się jako czynnik kluczowy na współczesnym polu walki. Uważa się, że określenie właściwych zależności między czynnikami operacyjnymi[2] zdeterminowane jest posiadaniem informacji dotyczących przeciwnika i sił własnych, obszaru i czasu ich działania. Należy mieć na uwadze, że o wartości informacji decydują: jej treść, wiarygodność i aktualność. Nie chodzi jednak o to, aby wiedzieć wszystko, lecz by wiedzieć wystarczająco dużo, a przede wszystkim więcej niż przeciwnik. Informacja lub jej brak jest czynnikiem decydującym o sukcesie lub porażce. Jest zasadniczym warunkiem umożliwiającym prowadzenie działań, a w określonych sytuacjach staje się czynnikiem samodzielnie decydującym o ich powodzeniu. Starcie dwóch stron jest obecnie walką o informację. Aby zatem zwyciężyć, należy wygrać walkę w wymiarze informacyjnym (walkę informacyjną).

---

[1] S. Koziej, „Teoria sztuki wojennej", wyd. AON, Warszawa 1993.

[2] Do czynników operacyjnych, od których zależy rozmach i przebieg działań operacyjnych, zalicza się: siły, obszar, czas i informację. Por. „Regulamin działań wojsk lądowych", wyd. DWLąd, Warszawa 1999, s. 57.

Walka informacyjna[3] – kooperacja negatywna wzajemna, przynajmniej dwupodmiotowa, realizowana w sferach: rozpoznania (zdobywania informacji), zakłócania informacyjnego i obrony informacyjnej, gdzie każdemu działaniu jednej strony przyporządkowane jest działanie antagonistyczne strony drugiej.

Z powyższego wynika, że zakłócanie informacyjne[4] jest obok zdobywania[5] (rozpoznania) informacji i obrony informacyjnej[6] podstawowym komponentem walki informacyjnej[7].

Zakłócanie informacyjne prowadzi się w celu obniżenia efektywności funkcjonowania systemów dowodzenia i kierowania uzbrojeniem przeciwnika oraz ich zasobów i procesów informacyjno-sterujących. Polega ono na dezorganizacji przedsięwzięć rozpoznawczych przeciwnika, jego dowodzenia i kierowania uzbrojeniem. Zakłócanie informacyjne powinno być skoncentrowane na działalności umożliwiającej racjonalne modelowanie procesu przygotowywania wojsk do realizacji zadań w okresie zaistnienia konfliktu zbrojnego oraz podczas prowadzenia operacji wojsk lądowych[8].

---

[3] L. Ciborowski, „Przestrzenie walki informacyjnej", wyd. AON, Warszawa 1997.

[4] Zakłócanie informacyjne (procesów informacyjnych) przeciwnika to zespół skoordynowanych przedsięwzięć i działań, które dostosowane są do zakłócania procesów dowodzenia wojskami i kierowania środkami walki przeciwnika. Zakłócanie informacyjne przeciwdziała również rozpoznaniu. W zależności od szczebla dowodzenia zakłócanie informacyjne realizują siły i środki walki elektronicznej, działań psychologicznych, działań specjalnych oraz wojska uczestniczące w walce. Zob. „Regulamin działań wojsk lądowych", wyd. DWLąd, Warszawa 1999 r., s.62.

[5] Zdobywanie informacji o przeciwniku odbywa się w warunkach ciągłego prowadzenia walki informacyjnej polegającej na tym, że wszelkim wysiłkom rozpoznawczym jednej strony przeciwstawiane jest zakłócanie informacyjne i obrona informacyjna strony drugiej. Tamże, s.62.

[6] Obrona informacyjna stanowi zespół skoordynowanych przedsięwzięć dostosowanych do uniemożliwienia przeciwnikowi dostępu do zbiorów informacji, które odzwierciedlają lub mogą odzwierciedlać stan faktyczny, usytuowanie i zamiary działania wojsk własnych oraz ochronę własnych procedur dowodzenia wojskami i kierowania środkami walki przed zakłócaniem informacyjnym stosowanym przez przeciwnika. Przedsięwzięcia z zakresu obrony informacyjnej realizują bezpośredni użytkownicy systemów informacyjnych w ramach ich zabezpieczenia bojowego. Tamże, s. 62.

[7] Należy nadmienić, że pojęcie walka informacyjna nie jest dotychczas oficjalnie wyróżniane w dokumentach normatywnych Sztabu Generalnego WP.

[8] Operacje wojsk (sił) lądowych - na szczeblu operacyjnym działania lądowe obejmują harmonizację możliwości wsparcia ze strony całości sił. Wsparcie powietrzne, lądowe, desantu morskiego oraz marynarki wojennej nie są przedstawiane jako odrębne operacje, ale jako jedna wspólna kompleksowa operacja zaplanowana w celu osiągnięcia zamiarów kampanii. Na obszarze lądowym operacji, dowódca lądowy jest jednocześnie wyznaczony jako dowódca wsparcia i jest on odpowiedzialny za synchronizację manewrów, wsparcia ogniowego i ich wstrzymanie. Na szczeblu operacyjnym podstawowymi działaniami lądowymi są działania zaczepne i obronne. Zob.: R. Bojarski „Operacja obronna", wyd. AON, Warszawa 1999.

Wiadomym jest, że szczególna rola w tym zakresie przypada szeroko rozumianemu rozpoznaniu[9]. Znajomość planów przeciwnika stanowi inherentny element procesu przygotowania i prowadzenia zakłócania informacyjnego. Podmiot działań, wykorzystując wszelkie elementy rozpoznawcze zintegrowanego systemu rozpoznania sił zbrojnych (a także elementy rozpoznania agenturalnego), zdobywając niezbędne i w pełni wiarygodne dane dotyczące planowanych działań zbrojnych i niezbrojnych przeciwnika oraz przedsięwzięć realizowanych przez jego struktury rozpoznawcze, może dostarczyć przeciwnikowi tak spreparowanych danych, które wprowadzą go w błąd, spowodują podjęcie niekorzystnych dla niego decyzji oraz będą dla niego stanowić przyczynek podjęcia wymuszonych działań.

Zakłócanie informacyjne powinno być ukierunkowane na zwiększanie entropii informacyjnej komunikatów przeciwnika i dążenie do destrukcji wszelkich ich nośników.

Zakłócanie informacyjne to wszelkie oddziaływanie na otoczenie (obszar zdobywania informacji – rejestratory danych, sygnały będące ich nośnikami, zbiory danych, programy, biblioteki itp.), które doprowadza do zaniku informacji pożądanej, jej deformacji lub wytwarzania danych nieprawdziwych i przez to wpływa negatywnie na inne procesy pola walki.

Istotą zakłócania informacyjnego jest maksymalne ograniczenie napływu danych prawdziwych i powodowanie przez to zniekształcenia obrazu obszaru działań operacyjnych wojsk lądowych. Ten fałszywy obraz obszaru pola walki ma bezpośrednie przełożenie na podejmowanie decyzji oraz działanie środków ogniowych, wykonanie manewru, zaopatrzenie materiałowo - techniczne itp.

Zakłócanie informacyjne w operacjach wojsk lądowych spełnia jak gdyby dwie funkcje. Jedną z nich jest szeroko rozumiana pozoracja, wprowadzanie w błąd przeciwnika. Jej celem jest udostępnienie przeciwnikowi takich postaci danych, które po przetworzeniu będą przedstawiać sytuację nierealną, nie mającą nic wspólnego z rzeczywistością. Drugą funkcją jest dążenie do fizycznej destrukcji nośników danych.

---

[9] Określenia użyto w rozumieniu, iż w rozpoznaniu mieści się również wywiad.

Stosując różne techniki można niszczyć lub uniemożliwić pracę źródłom zdobywania danych, przetwornikom danych i sygnałów oraz układom odbierającym. Można też zmieniać strukturę nośników danych i sygnałów. Innymi słowy, obydwa te sposoby zwiększają stan nieuporządkowania wiedzy o położeniu wojsk, a tym samym zwiększają entropię informacyjną. Jest to proces zróżnicowany zarówno w zakresie obszarów oddziaływania, jak i metod postępowania.

Proces zakłócania informacyjnego w operacjach wojsk lądowych powinien obejmować okres ich przygotowania oraz prowadzenia. Okres przygotowania operacji wojsk lądowych jest stosunkowo długi i charakteryzuje się niewielką dynamiką procesów informacyjnych. Natomiast okres prowadzenia operacji charakteryzuje się dynamiką znacznie większą, a zatem zakłócanie informacyjne musi zachowywać odpowiednie proporcje.

Zakłócanie informacyjne musi uwzględniać sam proces informacyjny, który jest w stosunku do zakłócania pierwotnym. Procesy informacyjne są bardzo skomplikowane, a ich zakłócanie może być spowodowane nie tylko przez działalność celowo zorganizowaną, ale może również wynikać z niedoskonałości poszczególnych elementów. Zakłócanie celowe może być dokonywane w każdym ogniwie procesu informacyjnego, stosownie do potrzeb i możliwości technicznych zakłócania oraz obszaru jego oddziaływania. Najpierw jednak należy zdobyć, odpowiednio wcześnie, dane o potencjalnym przeciwniku, terenie i panujących tam warunkach. W obszarze operacji wojsk lądowych i w jego otoczeniu obiekty podlegające rozpoznaniu mogą zostać zamaskowane i wtedy dla jego organów nie będzie obiektów, które są przez nie wyszukiwane. Ponadto mogą zostać ustawione obiekty fałszywe, które wysyłają identyczne sygnały bodźcowe jak prawdziwe. To może spowodować, że do elementów rozpoznania, a w ślad za nim do dowódców i sztabów napłyną dane niepełne i podejmowane na ich podstawie decyzje mogą być błędne.

W warunkach prowadzenia operacji wojsk lądowych, potok danych jest przetwarzany przez zwiadowców wspomaganych coraz doskonalszymi technicznymi środkami rozpoznania oraz przez sztaby i specjalne zespoły analityczne. Przy wykorzystywaniu urządzeń technicznych, istotny wpływ na ich funkcjonowanie

mają programy, które sterują ich pracą. W wypadku czynnika ludzkiego, dużą rolę odgrywa z kolei sprawność psychofizyczna.

Zakłócanie informacyjne może być prowadzone przy stosowaniu odpowiedniej techniki i metod postępowania. Najbardziej skutecznymi są środki niszczenia, jednak mając na uwadze realia obszaru pola walki nie wszystko można niszczyć. Nie bez znaczenia są także koszty, które powinny być minimalizowane stosownie do osiąganych rezultatów. Warunki te dyktują potrzebę posiadania środków maskowania, pozorowania, zakłócania elektronicznego (aktywnego i pasywnego), środków umożliwiających ingerencję w systemy komputerowe i banki danych, jak również ludzi przygotowanych do realizacji tych zadań. Ilość oraz proporcje tych środków należy dostosować do realiów obszaru pola walki. Metody przygotowania działań w zakresie zakłócania informacyjnego oraz metody użycia sił i środków należy weryfikować stosownie do zmian zachodzących w sytuacji oraz procesach informacyjno-sterujących towarzyszących walce zbrojnej. Dlatego też należy kształtować właściwe proporcje działań w tym zakresie. Wojska lądowe powinny dysponować określonym potencjałem bojowym[10], charakteryzującym się jednoznacznymi wskaźnikami ilościowymi i jakościowymi. Z tego wynikają konkretne potrzeby w zakresie zakłócania, które konieczne należy uwzględnić w planowaniu działań, kierowaniu ruchem wojsk i kierowaniu uzbrojeniem. Pomiędzy stanem posiadanego potencjału bojowego i potrzebami zakłócania zachodzi związek zależności polegający na tym, że mniej doskonały potencjał bojowy wymaga bardziej doskonałego systemu zakłócania informacyjnego, który swoim działaniem zdoła zrekompensować problemy złożonej procedury przemieszczania środków walki na kolejne pozycje bojowe i związane z wykonywaniem przez nie skutecznego rażenia.

Potencjał zakłócania informacyjnego oraz zasady jego prowadzenia muszą być kompatybilne do obezwładnianych zakłóceniami środków przeciwnika oraz uwzględniać jego zasady wykorzystania wojsk w działaniach operacyjnych. W tej problematyce najbardziej istotna jest technika i zasady prowadzenia zakłócania informacyjnego. Dlatego też za punkt odniesienie trzeba przyjmować stan posiadania

[10] Określenie potencjał bojowy użyte jest w rozumieniu, że są to siły i środki przeznaczone do prowadzenia walki zbrojnej, której istotą jest rażenie przeciwnika.

w otaczającej przestrzeni pola walki, niezależnie od tego czy panujące tam warunki są korzystne czy też nie. Z drugiej zaś strony, należy uwzględniać wymagania wynikające z założeń doktrynalnych. Potrzeba dostosowania procedur i technik zakłócania informacyjnego obecnie nie jest właściwie pojmowana. Najczęściej problematyka ta identyfikowana jest tylko z aktywnym zakłócaniem technicznych torów transmisji informacji i z dość prostymi formami generowania fałszywych danych. Natomiast zakłócanie informacyjne można prowadzić w znacznie szerszym zakresie, bowiem wszystko to co związane jest ze zwiększaniem entropii informacyjnej[11], jest zakłócaniem informacyjnym. Przy takim rozumieniu istoty zjawiska, do zakłócania informacyjnego należy również zaliczyć wszelkie formy maskowania i pozorowania. Wiele też można uczynić, w zakresie zakłócania informacyjnego drogą destrukcyjnego oddziaływania na środki przetwarzania danych i czynnik ludzki. Bardzo skutecznymi mogłyby się tu okazać rozwiązania urządzeń zakłócających, wykorzystujące technikę impulsową, natomiast w sferze zakłócania osobowego technika infradźwiękowa i psychotronika.

Skuteczność zakłócania jest uwarunkowana wieloma czynnikami, do których, między innymi, należy zaliczyć:

– posiadanie danych o stanie i funkcjonowaniu procesów informacyjnych u przeciwnika, wykorzystywanej przez niego technice, metodach zdobywania i gromadzenia informacji, czy dowodzeniu, co jest niezbędne do przygotowania od strony technicznej, metodologicznej i organizacyjnej procesu zakłócania;

– dysponowanie środkami rozpoznania, które będą zdobywały dane o funkcjonowaniu systemów informacyjnych przeciwnika, stanie oraz przebiegu procesów informacyjnych, w czasie niezbędnym na uruchomienie procesu zakłócania. Bez danych o pracy tych elementow, nie można podejmować przemyślanych i skutecz-

[11] Entropia informacyjna - miara nieokreśloności zdarzeń stanowiących źródła informacji przy określonym stanie niewiedzy o tych zjawiskach. Jest ona ściśle związana z ilością informacji prawdziwej zawartej w odebranym komunikacie, gdyż za miarę uzyskanej tą drogą przez odbiorcę ilości danych przyjmuje się stopień zmniejszenia nieokreśloności. Dlatego entropia informacyjna, którą odbiorca przypisuje określonemu zjawisku, jest zawsze co najmniej równa entropii fizycznej tego zjawiska lub większej od niej. Tylko w przypadku, gdy odbiorca jest całkowicie poinformowany o statystycznej naturze zjawiska, wartość entropii fizycznej i informacyjnej pokrywają się (entropia fizyczna jest funkcją aktualnego stanu fizycznego określonego obiektu materialnego przy założeniu, że stan ten jest traktowany jako zmienna losowa).

nych przedsięwzięć i zadań zakłócających. Pewne działania w tym zakresie można podejmować na podstawie wiedzy zgromadzonej w bankach danych;

– wyznaczenie i przygotowanie określonych organów, odpowiedzialnych za planowanie i prowadzenie procesu zakłócania. Związana jest z tym cała procedura przygotowania sztabów i wojsk do prowadzenia walki informacyjnej;

– dysponowanie siłami i środkami technicznymi oraz materiałowymi, stosownie do zadań stawianych zakłócaniu. Możliwości techniczne własnych środków powinny umożliwić wykonanie tych zadań, a zatem nie powinny odbiegać jakością od obezwładnianych zakłóceniami środków przeciwnika.

– system informacyjny przeciwnika, który podlega zakłócaniu i zmienia się w wyniku wyeliminowania poszczególnych jego ogniw oraz poprzez dokonanie wewnętrznych zmian uodparniających go na oddziaływanie środków zakłócających. Wraz z nim zmieniają się warunki działania wszystkich środków pola walki. Jest to proces dynamiczny przebiegający z różnym natężeniem w poszczególnych etapach walki. Procesowi temu powinny odpowiadać działania zakłócające poszukujące optymalnych i skutecznych środków i metod oddziaływania. W takim procesie należy unikać szablonów, wykorzystywać teren oraz istniejące warunki taktyczne i operacyjne.

Dążyć należy do uzyskania zaskoczenia w każdym obszarze i skali działania, gdyż procesy informacyjne są nieodzowne w prowadzeniu walki zbrojnej, a zatem zakłócanie ich u przeciwnika prowadzi do obniżenia efektywności jego działań.

Zakłócanie informacyjne pomimo, że może być realizowane w wielu punktach, powinno być postrzegane jako jeden obszar działania, jednolicie planowany pod kątem sposobu rozegrania operacji przez dowódcę, a wykonawcami zadań jest wielu jej uczestników.

Procesy informacyjne, we współczesnych operacjach wojsk lądowych, w zdecydowanej większości są realizowane za pomocą środków elektronicznych, zatem spektrum elektromagnetyczne należy uznać za najważnieisze w procesie ich zakłócania.

W procesie zakłócania informacyjnego niezwykle istotnym czynnikiem jest czas. Zakłócanie, aby spełniało określone zadania powinno w aspekcie czasu reakcji ciągle nadążać a niekiedy wyprzedzać funkcjonowanie procesów informacyjnych. Sprowadza się to do tego, że maskowanie i pozoracja w obszarze zbierania danych powinny zostać wykonane przed penetracją tego obszaru przez odpowiednie elementy rozpoznawcze. Zakłócanie rozpoznania należy więc realizować od chwili rozpoczęcia przez nie pracy. Sygnały w środkach transmisji danych należy zakłócać podczas ich odbioru przez adresatów. Niszczenie powinno być realizowane zaraz po wykryciu obiektu pracującego w systemie informacyjno - sterujacym. Takie warunki czasowe zakłócania są trudne do zrealizowania, dlatego należy dążyć do posiadania sprzętu umożliwiającego takie działanie. Natomiast proces zakłócania należy rozłożyć w czasie w taki sposób, aby u przeciwnika występowały różne stany, m.in.: zanik informacji, opóźnienie lub brak zakłóceń, co w konsekwencji prowadzi do dezorganizacji procesów informacyjnych przy mniejszych wymaganiach ilościowych sprzętu i w zakresie jego czasu reakcji.

1.2. Podstawowe rodzaje zakłócania informacyjnego

Zakłócanie informacyjne, jak wykazano wcześniej, jest realizowane w stosunku do systemów rozpoznania, dowodzenia i kierowania uzbrojeniem, których działanie jest oparte przede wszystkim o środki elektroniczne oraz informatyczne. Zasadniczymi obiektami zakłócania informacyjnego są wiec:

– w systemach łączności – urządzenia odbiorcze różnego rodzaju relacji łączności bezprzewodowej;

– w systemach radionawigacyjnych – różnego typu pokładowe i naziemne urządzenia odbiorczo-wskaźnikowe i odbioru danych nawigacyjnych;

– w systemach radiolokacyjnych – urządzenia odbiorcze różnego typu naziemnych stacji radiolokacyjnych rozpoznania celów, stacji naprowadzania rakiet i kierowania ogniem oraz pokładowych stacji radiolokacyjnych lotnictwa i sił morskich;

– w systemach samonaprowadzania – urządzenia odbiorcze pokładowych stacji radiolokacyjnych oraz urządzenia elektroniczne głowic samonaprowadzających się bomb, pocisków, rakiet, itp.;

– w systemach radiotelesterowania – różnego typu urządzenia odbiorcze środków zapewniających zdalne sterowanie uzbrojeniem, samolotami bezpilotowymi oraz pociskami rakietowymi (przeciwpancernymi, przeciwlotniczymi itp.);

– w systemach optoelektronicznych – różnego typu odbiorcze optoelektroniczne urządzenia prowadzące rozpoznanie w zakresie promieniowania widzialnego oraz bliskiej, średniej i dalekiej podczerwieni;

– w systemach informatycznych – sieci informatycznych rozległe i lokalne oraz zautomatyzowane miejsca pracy na stanowiskach dowodzenia.

Zakłócanie informacyjne może być prowadzone selektywnie na wybrane obiekty i środki elektroniczne, informatyczne lub w sposób zmasowany na środki w wybranych obszarach lub rejonach. W drugim przypadku wszystkie środki elektroniczne i informatyczne przeciwnika w obszarze walki podlegają obezwładnieniu zakłóceniami.

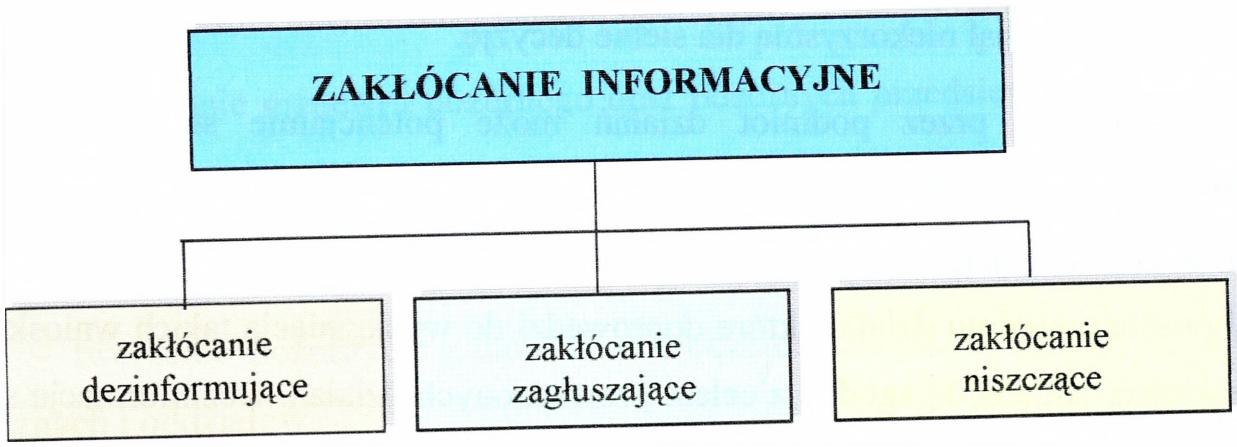
Największą efektywność zakłócania informacyjnego osiąga się przez kompleksowe obezwładnienie zakłoceniami najważniejszych środków (obiektów) elektronicznych i informatycznych przeciwnika w sposób zmasowany, niespodziewanie, w rejonach kluczowych i w decydujących etapach operacji. Mając na uwadze potrzeby operacji, gros sił i środków do zakłócania należy wykorzystać w kluczowych rejonach i okresach działania wojsk. Jest to niezbędne do wyeliminowania ważnych środków elektronicznych przeciwnika, a tym samym stworzenia dogodnych warunków do działania głównych zgrupowań wojsk lądowych, lotnictwa i sił morskich.

Do podstawowych rodzajów zakłócania informacyjnego w operacjach wojsk lądowych zdaniem zespołu autorskiego należy zaliczyć (rysunek 1.):

– zakłócanie dezinformujące;

– zakłócanie zagłuszające;

– zakłócanie niszczące (niszczenie kinetyczne, elektromagnetyczne).



Rys. 1.1. Podstawowe rodzaje zakłócania informacyjnego

1.2.1. Zakłócanie dezinformujące

Zakłócanie dezinformujące to wprowadzanie w błąd przeciwnika przez podanie mylących informacji[12]. W ujęciu wojskowym, to rozpowszechnianie nieprawdziwych wiadomości i dokumentów do zamiaru, organizacji i prowadzenia operacji, a także charakteru ich działania.

Zakłócanie dezinformujące rozpoznania, dowodzenia wojskami i kierowania uzbrojeniem, jako element procesu zakłócania informacyjnego może odbywać się drogą nadawania informacji odzwierciedlających fałszywy obraz pola walki, w formie logicznej i wiarygodnej, która będzie bezpośrednio zrozumiała dla człowieka – np. w postaci meldunków, rozkazów, sygnałów dowodzenia itp.- będzie to dezinformacja osobowa. Może również odbywać się w formie odpowiednio dobranych sygnałów odbieranych przez urządzenia elektroniczne wykorzystywane na

[12]Słownik języka polskiego, t II, wyd. PWN, Warszawa 1981, s. 390.

potrzeby rozpoznania, dowodzenia wojskami i kierowania uzbrojeniem - w tym przypadku będzie to dezinformacja techniczna.

Dezinformacja osobowa. Dezinformacja osobowa to zespół przedsięwzięć polegających na rozpowszechnianiu u przeciwnika odpowiednio spreparowanych wiadomości w celu oddziaływania na jego morale (postawy, zachowania) i intencje, aby podjął niekorzystną dla siebie decyzję.

Uprawiana przez podmiot działań może potencjalnie stanowić jeden z głównych elementów wprowadzania w błąd żołnierzy i ludności cywilnej kraju przeciwnika oraz jego mniejszości narodowych. Dezinformacją będzie takie oddziaływanie podmiotu działań, które doprowadzi do wyciągnięcia takich wniosków i przekonań, jakie będą zgodne z celem prowadzonych działań. Dezinformacja stawia sobie za cel realizację konsekwentnego programu działania zmierzającego do zastąpienia w świadomości wojsk przeciwnika przekonań i poglądów uznanych za niekorzystne dla podmiotu oddziaływania na takie, które są korzystne dla własnych sił prowadzących działania bojowe.

W aspekcie stosowania dezinformacji niezbędne jest wyodrębnienie takich oto dwóch ograniczeń:

– dezinformacja może być stosowana tylko wtedy, gdy istnieje pewna grupa – „masa krytyczna żołnierzy" lub ludności cywilnej przeciwnika już zdezorientowana lub podatna na wpływ;

– dezinformacji nie wolno stosować „pod prąd", to znaczy niecelowe jest przekazywanie informacji, które nie tylko, nie wywołają dezorientacji, ale nawet mogą wzbudzić sprzeciw.

Dezinformacja może potencjalnie pobudzać aberracyjne trendy w celu zaognienia sytuacji w szeregach wojsk przeciwnika i jego społeczeństwie, jednak skuteczna będzie wtedy, gdy umiejętnie wykorzysta już istniejące ogniska zapalne.

Powyższe ograniczenia wypływają bezpośrednio ze specyfiki oddziaływań dezinformacyjnych, które to w swej istocie polegają na modyfikowaniu postaw oraz zachowań stanów osobowych.

Do form dezinformacji osobowej można zaliczyć pozorowanie i manipulację.

Pozorowanie[13] polega na sztucznym tworzeniu „obrazu" (obiektu, czynności itp.) zbliżonego do rzeczywistego. Osiąga się je poprzez:

– tworzenie obiektów pozornych własnych wojsk (wojsk lądowych);

– pozorowanie innych form działań operacyjnych niż faktycznie prowadzone;

– stosowanie manewru pozornego oraz pozornych przedsięwzięć organizacyjnych;

– deformowanie obiektów rzeczywistych;

– tworzenie pozornych stanowisk dowodzenia związków operacyjnych, taktycznych i oddziałów.

Celem działań pozornych jest zmylenie przeciwnika, czyli wprowadzenie go w błąd. Działania pozorne należy definiować jako kompleks organizacyjnych, materiałowych i praktycznych przedsięwzięć, zgodnych z celem i zadaniem operacji, miejscem, czasem oraz sposobem działania wojsk, mających na celu zmylenie przeciwnika co do przyjętego rzeczywistego zamiaru działania walczących sił, ich składu, stanów osobowych, prawdziwych zadań i przewidywanych przedsięwzięć, w toku przygotowywania i prowadzenia operacji. Działania pozorne należą do tych czynności wojsk własnych, które w sposób pośredni wywierają wpływ na przeciwnika, bowiem oddziałują na wyniki jego rozpoznania, jako głównego źródła danych. Jeżeli pozorowanie zostanie uznane za prawdziwe to sprawi, że decyzje będą błędne, a wykorzystanie systemów uzbrojenia – niecelowe. Chęć mylenia przeciwnika była, jest i pozostanie ważnym elementem przygotowania oraz prowadzenia operacji. Będzie dowodem mistrzostwa dowódcy i jego zdolności narzucenia przeciwnikowi swej woli, przejęcia inicjatywy, zaskoczenia go, stworzenia jak najlepszych warunków własnym wojskom do osiągnięcia celu operacji. Dzięki prowadzeniu działań pozornych można osiągać wielkie sukcesy przy małych stratach ludzi, ni-

[13] Pozorowanie jest formą maskowania, a przedsięwzięcia wykonywane w jego zakresie powinny być koordynowane - zdaniem autorów - w ramach obrony informacyjnej, w realizacji zadań której uczestniczą również siły i środki zakłócania informacyjnego.

skim zużyciu materiałów i czasu. W tym sensie działania pozorne są ściśle związane z zasadami sztuki operacyjnej.

Drugą formą dezinformacji osobowej jest **manipulacja**. Termin ten nie jest jednoznaczny i trudny do zdefiniowania. Próby zdefiniowania podejmowane przez autorów na gruncie psychologii społecznej, socjologii i socjotechniki, nie dały jednoznacznych rezultatów. Pojęcie manipulacja dosyć trafnie określa sekwencja „często człowiek otwiera usta tylko po, by kimś manipulować”[14]. To właśnie instrumentalne podejście wydaje się być właściwe dla tego typu działań, ze względu na zadania, jakie realizuje podmiot tych oddziaływań i relacje, jakie zachodzą między podmiotem i przedmiotem tych działań. By zrozumieć istotę manipulacji, jej gnoseologiczne podstawy, celowe wydaje się rozpatrzenie tego pojęcia w kontekście wpływu społecznego i perswazyjnego oddziaływania na postawy i zachowania człowieka. Każdy żołnierz, członek społeczności bezpośrednio lub pośrednio zaangażowanej w walkę zbrojną, podlega pewnemu wpływowi społecznemu.

Można wyróżnić różnego rodzaju percypowanie wpływu manipulacji na stany osobowe, a mianowicie:

– w zachowaniu osoby (lub grupy) zawarte są wyraźne wskazówki świadczące o tym, że osoba ta wywiera wpływ na inną osobę lub grupę w celu zmiany lub modyfikacji postawy i zachowania;

– wskazówki świadczące o wywieranym wpływie są zazwyczaj ukrywane, lecz dostępne poznaniu osoby (grupy) będącej przedmiotem wpływu po dokonaniu przez nią odpowiedniej analizy zachowania lub intencji osoby wywierającej wpływ;

– osoba (grupa) będąca przedmiotem wpływu, nie powinna świadomie zdawać sobie sprawy z wywieranego wpływu;

---

[14]Maliszewski W.: *„Oddziaływanie psychologiczne w operacji obronnej”*. Rozprawa doktorska, AON, Warszawa 1998. Ponadto: M. Montana Czarnawska: *„Jak się bronić przed indoktrynacją”*, Warszawa 1997; K. Czuba: *„Media i władza”*, Warszawa 1995; G.H. Green, C.Cotter: *„Nie pozwól sobą manipulować”*, Warszawa 1997; P. Honey: *„Jak radzić sobie lepiej z ludźmi”*, Warszawa 1997; J. Kirschner: *„Manipulować – ale jak?”*, Warszawa 1994; R. Nawrat: *„Manipulacja społeczna - przegląd technik i wybranych wyników badań”*. W: *„Przegląd Psychologiczny”* 1/1989, s. 125 - 154; J. Reykowski: *„Osobowość a społeczne zachowanie się ludzi”*, Warszawa 1976.

– percepcja danych, jawnych bądź ukrytych, świadczy o tym, czy mamy do czynienia z całkowicie lub częściowo jawnymi metodami wpływu społecznego (wpływaniem na konformizm perswazją), czy też manipulacją;

– manipulacja odnosi się do trzeciego rodzaju percypowania wpływu - może być wykorzystywana jako technika wpływania na behawioralny komponent zachowań i postaw[15];

– epistemologiczną istotą oddziaływania manipulacyjnego jest proces sterowania, który prowadzi do realizacji celów podmiotu działań - zgodnych z celem i obiektywnym interesem własnych sił prowadzących działania operacyjne. Innymi słowy manipulację można znaleźć tam, gdzie odpowiedni przekaz informacyjny (sterowanie), będzie modyfikował postawy i zachowania żołnierzy oraz ludności przeciwnika, tak że sterowana grupa społeczna (pododdział), nie urzeczywistni planów, zaniecha lub zaniedba działań ważnych dla własnej pomyślności, własnych interesów bądź celów tego, kto formalnie nią kieruje i dowodzi[16]. Manipulacją będą więc takie działania, które zmuszają przedmiot do przyjmowania takich postaw, generowania zachowań i czynienia czegoś, czego przedmiot nie chce albo sobie nie życzy. Powinno to być na tyle wyrafinowane sterowanie świadomością przedmiotu działań aby wywoływało u niego wrażenia jakoby to, co czyni, wynikało z jego własnych planów i wypracowanych decyzji.

Manipulacja operuje też uczuciami i wywołuje emocje. Wyznaczone siły, przekazując spreparowane dane, biorą pod uwagę to, iż działania prowadzone są w gęstym otoczeniu społecznym, a przedmiot cierpi na tzw. głód informacyjny. Są w stanie wywołać u przedmiotu szeregu pożądanych emocji i uczuć w celu sprowokowania określonych zachowań czynnościowych i werbalnych. Podmiot będzie w tym wypadku permanentnie dążył do uaktywnienia własnych mechanizmów w celu ograniczenia bądź całkowitego zablokowania kontroli świadomości przedmiotu i w konsekwencji umożliwi narzucenie wzorców postaw i zachowań pochodzących od podmiotu.

---

[15]Por. R. Nawrat, tamże, s.125 - 127.
[16]Por. P. Kołtunowski, tamże, s. 180 -181.

Podejmując więc oddziaływanie na emocje i oczekując efektu w postaci określonych postaw oraz zachowań jako pewnego procesu kompensacji deficytu informacyjnego, można pokusić się o przedstawienie ich jako iloczynu motywu podjęcia określonego zachowania i różnicy danych niezbędnych do normalnego procesu decyzyjnego oraz posiadanych danych.

Najczęściej spotykanymi sposobami manipulowania w celu kształtowania pożądanych postaw i zachowań człowieka, są:

- przekazywanie danych nieprawdziwych;
- preparowanie i przesyłanie do przedmiotu danych nieważnych lub mało ważnych z pominięciem najważniejszych;
- przekazywanie danych o dużym znaczeniu jako marginalnych;
- udostępnianie danych preparowanych w celu wywołania określonych interwencji;
- przesyłanie danych wieloznacznych, utrudniających zrozumienie;
- generowanie nadmiaru danych, by spowodować tzw. „chaos informacyjny".

Pierwszy sposób polega na podaniu przedmiotowi oddziaływania danych z gruntu nieprawdziwych, jednak takich, które powinny utkwić w podświadomości jako możliwe do wystąpienia.

Drugi sposób odnosi się do przekazania danych skierowanych do wojsk przeciwnika i jego ludności na zasadzie przedstawienia rzeczywistego obrazu w „krzywym zwierciadle".

Kolejna technika opiera się na założeniu, że każda postać danej, nawet bardzo istotna, przekazana w dalszej kolejności komunikatu informacyjnego, staje się mniej ważną, nieznaczącą wiadomością, na którą przedmiot nie zwróci uwagi.

Czwarta technika może być sprowadzona do wywoływania tzw. tematów dyżurnych. Permanentne przekazywanie danych (np. o rzezi ludności cywilnej) może stanowić swoisty impuls do podjęcia działań interwencyjnych, dociekania prawdy, ucieczki z pola walki i innych tego typu zachowań.

Przekazywanie danych wieloznacznych, stereotypowych może doprowadzić u ich odbiorcy (przedmiotu oddziaływań) do wytworzenia mylnego obrazu tego, co ważne z punktu widzenia celu prowadzonych działań. Np. informacja o „pełnej izolacji strony przeciwnika w trakcie rozmów na forum ONZ" niesie ze sobą treść, która z pewnością trafi do świadomości przedmiotu, że jego rząd, kraj i naród jest izolowany. Dane o tym, że rozmowy na forum ONZ toczą się nadal, jest „rozmydlona" i nie dostrzegana przez przedmiot oddziaływania.

Ostatni sposób to przekazywanie danych w nadmiarze, które prowadzi do „chaosu informacyjnego". Podmiot może zasypać przedmiot oddziaływania tak dużą ilością danych o faktach i zjawiskach pola walki, że spowoduje u niego brak wrażliwości na istotne i ważne wiadomości.

Dezinformacja techniczna. Dezinformacja techniczna to zespół przedsięwzięć organizacyjnych, wzajemnie powiązanych pod względem celu, czasu i miejsca, umożliwiających skuteczny sposób dezorganizacji pracy i działania różnorodnych środków i systemów, głównie elektronicznych wykorzystywanych przez przeciwnika na potrzeby rozpoznania, dowodzenia wojskami i kierowania uzbrojeniem. Są to urządzenia dostosowane konstrukcyjnie do rejestrowania określonych stanów i efektów, charakterystycznych dla danego środowiska (elektromagnetycznego, akustycznego, magnetycznego, elektrycznego, sejsmicznego i chemicznego). Realizowane przedsięwzięcia w tym zakresie mogą w znacznym stopniu ograniczyć zakres i możliwości wykorzystania tych urządzeń, a ponadto - mimo że nie powodują bezpośrednich materialnych zniszczeń - w wielu sytuacjach są przyczyną znacznych i często bezpowrotnych strat w ludziach i sprzęcie bojowym przeciwnika. Do form dezinformacji technicznej zalicza się pozorowanie oraz mylenie elektroniczne.

Pozorowanie elektroniczne polega na dostarczeniu energii elektromagnetycznej wraz z informacją w taki sposób, aby odbierający nie zorientował się, że pochodzi ona od przeciwnika, zaś przekazaną treść przyjął jako prawdziwą[17]. Pozo-

[17] Pozorowanie elektroniczne jest formą maskowania elektronicznego, a przedsięwzięcia wykonywane w jego zakresie powinny być koordynowane - zdaniem autorów - w ramach obrony informacyjnej, w realizacji zadań której uczestniczą również siły i środki zakłócania informacyjnego.

racja elektroniczna wnosi w system rozpoznania przeciwnika dane nieprawdziwe, które mogą być przez niego przyjmowane i wykorzystywane podczas podejmowania różnorodnych decyzji. Realizuje się ją za pomocą środków elektronicznych (radiowych, radiolokacyjnych, radionawigacyjnych i in.) przez specjalnie przygotowane do tego celu zespoły obsługujące.

Praktyczne stosowanie pozoracji elektronicznej wymaga doskonałej znajomości zasad organizacji systemów elektronicznych przez przeciwnika, sposobów przekazywania danych, stosowanych zabezpieczeń, posiadania odpowiedniego sprzętu oraz ciągłego śledzenia pracy jego środków i systemów.

We współczesnych operacjach wojsk lądowych znaczenie pozoracji elektronicznej będzie permanentnie wzrastać, głównie ze względu na rozmach prowadzonych działań, w których rozpoznanie, dowodzenie wojskami i kierowanie uzbrojeniem będzie odbywało się na dużych przestrzeniach, często na oddzielnych kierunkach, przede wszystkim za pomocą różnorodnych środków elektronicznych (radiostacje, stacje radioliniowe, troposferyczne i inne). Wysoka dynamika i manewrowość działań często stwarzać będą trudne sytuacje, w których dowództwa i sztaby nie będą miały ciągłej łączności z walczącymi wojskami lub jej utrzymanie będzie utrudnione. Ponadto możliwość rażenia i niszczenia środków i obiektów elektronicznych przez lotnictwo, wojska rakietowe i artylerię, desanty i grupy rozpoznawcze może być przyczyną częstego „wypadania" korespondentów z poszczególnych relacji łączności bez wiedzy dowództw i sztabów, co stworzy bardzo korzystne warunki do prowadzenia, np.: dywersji radiowej poprzez podszywanie się pod istniejące, a czasowo nieczynne środki łączności przeciwnika.

Wyposażenie wojsk w coraz doskonalsze systemy rozpoznania ma zasadniczy wpływ na rozwój środków pozoracji pola walki. Umiejętne wykorzystanie urządzeń i obiektów pozornych, pozwala znacznie zmniejszyć straty własne. Wymóg jaki powinien spełniać sprzęt pozorujący pole walki, to maksymalne utrudnienie przeciwnikowi możliwości rozpoznania elementów ugrupowania operacyjnego, systemów dowodzenia i ważnych obiektów infrastruktury obronnej oraz skierowanie jego wysiłku rozpoznawczego i uderzeniowego na rejony pozorne. Budowa wia-

rygodnych rejonów i obiektów pozornych pozwala wprowadzić w błąd przeciwnika co do rzeczywistego stanu rozbudowy inżynieryjnej obszaru obrony, rozmieszczenia elementów ugrupowania operacyjnego i jego ważnych obiektów. Działania te powinny zmuszać przeciwnika do rozproszenia wysiłku rozpoznawczego i uderzeniowego, co z kolei powinno zmniejszyć prawdopodobieństwo zniszczenia prawdziwych elementów obrony. Sprzęt do pozoracji pola walki spełni swoje zadanie, jeśli jego najważniejsze parametry będą w dostatecznym stopniu zbliżone do rzeczywistych. Powinny to być środki umożliwiające budowę obiektów pozornych o bardzo zbliżonym do rzeczywistych charakterystykach wizualnych, termalnych i elektromagnetycznych. Takie obiekty te są szczególnie efektywne przy ataku z powietrza, ponieważ pilot ma zaledwie kilka sekund na ich identyfikację i podjęcie decyzji dotyczącej ataku. Prawdopodobieństwo przeprowadzenia ataku na cel pozorny przy zastosowaniu właściwej techniki pozoracji jest bardzo wysokie. Rozproszenie wysiłku rozpoznawczego przeciwnika zwiększa szansę na przetrwanie elementów rzeczywistych obrony. Środki te będą ulegały ciągłemu rozwojowi, ponieważ pozwalają przy niskich nakładach finansowych znacząco zmniejszyć straty własne.

Mylenie elektroniczne to zamierzone promieniowanie, odpromieniowanie, zmiana, wchłonięcie lub odbicie energii elektromagnetycznej w sposób zamierzony w celu zmylenia, odwrócenia uwagi lub oszukania przeciwnika i jego systemów rozpoznania elektronicznego. Do sposobów mylenia zalicza się:

– wyprzedzająca lub opóźniająca bramka odległości zmieniająca zasięg blokowania radarów impulsowych,

– wyprzedzająca lub opóźniona bramka prędkości, która zmienia prędkość blokowania radarów z falą ciągłą,

– powtarzanie/przekazywanie impulsów - fałszywe echa w odległości lub kącie (listki boczne), , które powodują zamieszanie i przeciążenie układów odbiorczych.

Mylenie może być rozpatrywane w trzech aspektach jako:

– manipulowanie,

– symulowanie,

– imitowanie.

Manipulowanie polega na zmianie profili elektromagnetycznych rozmieszczenia własnego sprzętu elektronicznego w celu uniemożliwienia przeciwnikowi jego rozpoznania. Może być dokonane poprzez zmianę charakterystyk technicznych i profili sprzętu, aby ukryć przed przeciwnikiem dokładny obraz rozmieszczenia własnych sił i środków. Powinno być ostrożnie planowane i realizowane tylko wtedy, kiedy przeciwnik będzie tradycyjnie działał przeciwko wojskom lądowym i będzie dążył do uzyskania obrazu elektronicznego ich ugrupowania operacyjnego. Może obejmować zamierzone (dokonane celowo) transmisje fałszywych informacji. Manipulowanie wymaga pewnej informacji o własnych emisjach elektronicznych (radiowych i nie-radiowych) w dłuższym okresie czasu i podczas wszystkich faz operacji. Przeciwnik bardzo dokładnie będzie studiował emisje elektromagnetyczne w czasie pokoju. Wykorzysta do tego celu każdą okazję, na przykład ćwiczenia specjalistyczne. Jego analitycy będą poszukiwali zmian w sposobach ich wykorzystania i starali wykorzystać te informacje jako wskazówki do określenia zmian w systemach elektronicznych wojsk lądowych.

Manipulowanie jest realizowana przez:

– fałszywe poziomy źródeł promieniowania energii elektromagnetycznej;

– tworzenie fałszywych lub kontrolowanych tras teletransmisyjnych;

– ukrywanie faktycznego natężenia ruchu teletransmisyjnego;

– zmiana parametrów obiektów elektronicznych;

– kontrolowanie naruszenia zasad wymiany radiowej;

– celowy wyciek spreparowanych informacji związanych z fazami operacji.

Symulowanie polega na elektronicznej reprezentacji własnych sił w innym miejscu niż rzeczywista ich lokalizacja. Zmian rejonów należy dokonywać w trakcie trwania ciszy radiowej. Jego celem jest przeciwdziałanie rozpoznaniu przeciw-

nika i utrudnienie określania ugrupowania operacyjnego wojsk, ich rozmieszczenia, potencjalnych możliwości i zamiarów.

Zarówno radiowy jak i nie-radiowy sprzęt powinien być użyty do wytwarzania fałszywych obrazów w ramach symulacji, jednak tylko wtedy gdy przeciwnik ma wystarczające środki do ich wykrycia. Symulacja może być użyta do reprezentowania fałszywych lokalizacji obiektów lub zmian w treści rozkazów operacyjnych. Najczęściej stosowane formy symulowania są więc następujące:

- fałszywe lokalizowanie obiektów,
- zmiana rozkazu operacyjnego.

Imitowanie jest najczęściej postrzegane jako specyficzne (dywersyjne) zakłócanie, ponieważ efekt mylenia jest osiągane wewnątrz systemów elektronicznych przeciwnika. Główna idea imitowania polega na tym, że fałszywe dane wprowadza się bezpośrednio do systemów elektronicznych (radiowych, radionawigacyjnych) przeciwnika przy pomocy własnych urządzeń nadawczych, często utożsamianych z urządzeniami dywersyjnymi. Wejście do sieci przeciwnika wymaga informacji proceduralnej bez której istnieje duże ryzyko zidentyfikowania źródła.

Imitowanie jest realizowana przez:

- uciążliwe transmisje w celu zdenerwowania lub odwrócenia uwagi operatora od jego rzeczywistych zadań;
- planowane bezprawne włączenie się do sieci przeciwnika w celu podania mu fałszywych wiadomości lub rozkazów, aby opóźnić lub skierować jego aktywność na inne, nieistotne obiekty;
- nieautoryzowany dostęp do systemów szyfrowania (najkorzystniejsze było by złamanie kodów i szyfrów) przeciwnika;
- zakłócanie mylące (stosowane w stosunku do systemów nie-radiowych).

Z powyższego wynika, że w celu zaplanowania imitowania, jako zasadniczej formy oddziaływania na systemy elektroniczne przeciwnika należy upewnić się:

– czy posiadane środki dywersyjne są kompatybilne ze środkami przeciwnika podlegającymi tego rodzaju oddziaływaniu?

– jak długo może trwać mylenie?

– co jest szansą na sukces?

– czy będzie ono potwierdzone?

– czy wspiera ono plan główny?

Jak wykazują doświadczenia z minionych konfliktów zbrojnych, szczególnie wojny w Zatoce Perskiej, zakłócanie dezinformujące wydaje się być niezmiernie humanitarnym sposobem walki, umożliwiającym osiąganie celów politycznych i militarnych przy niewielkich kosztach materialnych i ludzkich. Oddziaływanie to można porównać do wysoce efektywnych systemów precyzyjnego rażenia.

1.2.2. Zakłócanie zagłuszające

Zakłócanie zagłuszające jest jednym z ważniejszych elementów składowych zakłócania informacyjnego. Jest ukierunkowane na dezorganizację procesów informacyjnych przeciwnika zachodzących w przestrzeni elektromagnetycznej. W połączeniu z dezinformowaniem powoduje naruszenie u przeciwnika poprawności funkcjonowania procesów rozpoznania, dowodzenia wojskami i kierowania uzbrojeniem. Jego istotą jest wnoszenie do relacji połączeń przeciwnika takich wartości energetycznych, które powodują tłumienie sygnałów użytecznych na wejściu jego urządzeń odbiorczych. Stopień destrukcyjnego oddziaływania zakłócania zagłuszającego na proces informacyjny przeciwnika unaocznia jedno z podstawowych równań teorii informacji stworzonej przez Shannona[18], z którego wynika zależność

[18] Shannon Claude Elood, ur. 1916 r., matematyk amerykański, profesor MIT, członek National Academy of Science, twórca teorii informacji.

określająca ilość informacji jaką można przesłań w kanale łączności o określonych parametrach:

$$I = kT\Delta f \log_2\left(1 + \frac{s}{z}\right)$$

gdzie:

I – ilość informacji,

k – stała charakteryzująca system przesyłania,

T – czas przesyłania informacji,

Δf – szerokość pasma kanału przesyłowego,

s – poziom sygnału,

z – poziom szumu (poziom zagłuszeń).

Możliwości efektywnego zakłócania zagłuszającego środków i systemów elektronicznych przeciwnika wynikają z wad, jakimi odznaczają się te środki i systemy. Zaliczyć można do nich:

– możliwość wykrycia i śledzenia pracy, określenia parametrów taktyczno-technicznych oraz miejsc i rejonów rozmieszczenia wszystkich środków elektronicznych promieniujących energię elektromagnetyczną;

– rejestracja przez elektroniczne urządzenia odbiorcze wszystkich sygnałów, zarówno użytecznych jak i zakłócających, które promieniowane są w przestrzeń elektromagnetyczną.

Zakłócanie zagłuszające prowadzi się we wszystkich rodzajach wojsk, w każdych warunkach terenowych i meteorologicznych, różnorodnymi technikami i sposobami. Realizacja procesu zakłócania zagłuszającego nie jest zatem przedsięwzięciem jednorodnym. Wymaga stosowania odpowiednio dobranych sygnałów zakłócających. W teorii zakłócania [20;22;35;58] wyróżnia się sygnały zakłócające: przypadkowe oraz celowe.

Zakłócenia przypadkowe powstają w wyniku oddziaływania na urządzenia elektroniczne zjawisk przyrodniczych (wyładowań atmosferycznych, oddziaływania zorzy polarnej, wybuchów słonecznych, opadów atmosferycznych) oraz oddziaływania innych urządzeń technicznych (pracy urządzeń przemysłowych, w tym: spawarek, urządzeń wyładowczych, źle zabezpieczonych silników elektrycznych). Powstają również w rezultacie oddziaływania na środki elektroniczne urządzeń elektrycznych (zespoły prądotwórcze, silniki spalinowe z zapłonem iskrowym itp.) lub w wyniku nieumiejętnego rozmieszczenia środków elektronicznych na stanowiskach dowodzenia. Zakłócenia przypadkowe mogą być również pochodzenia kosmicznego oraz jako naturalne wewnętrzne szumy, powstające podczas pracy odbiorczych urządzeń elektronicznych. Zakłócenia przypadkowe mogą powstawać także wewnątrz aparatury.

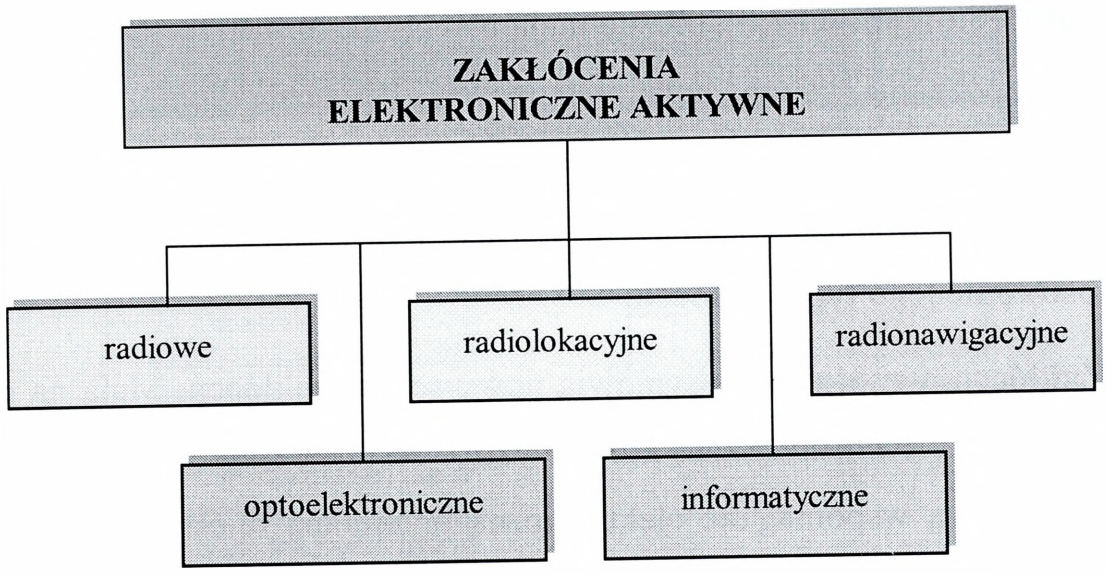
Zakłócenia celowe są wytwarzane przez specjalne stacje (nadajniki) zakłócające lub pasywne retranslatory energii elektromagnetycznej. Z uwagi na charakter powstawania wyróżnia się zakłócenia celowe: aktywne, pasywne[19] oraz kombinowane (w przypadku jednoczesnego stosowania zakłóceń aktywnych i pasywnych).

Zakłócenia elektroniczne aktywne. Zakłócenia elektroniczne aktywne polegają na promieniowaniu przez urządzenie nadawcze zakłócającej energii elektromagnetycznej na częstotliwościach lub w paśmie pracy zakłócanych urządzeń odbiorczych. Mogą być emitowane przez stacje zakłócające stacjonarne i mobilne (polowe).

Zakłócenia elektroniczne aktywne charakteryzują się różnymi parametrami taktyczno-technicznymi dostosowanymi do konkretnych środków i systemów elektronicznych, przeciw którym mają działać. Zakłóceniami aktywnymi oddziaływuje się przede wszystkim na urządzenia odbiorcze poszczególnych środków elektronicznych. Wytwarzane są one na częstotliwościach roboczych, na których dokonywana jest transmisja danych i do których dokładnie dostrajane są nadajniki zakłó-

[19] Zakłócenia pasywne szeroko wykorzystywane są w dezinformacji technicznej.

cające. Wyróżnia się zakłócenia (rysunek 1.2.): radiowe, radiolokacyjne, radionawigacyjne, optoelektroniczne i informatyczne.



Rys. 1.2. Podział aktywnych zakłóceń elektronicznych

Zakłócenia radiowe polegają na celowym promieniowaniu zakłócającej energii elektromagnetycznej powodującej utrudnienie pracy środków radiowych przeciwnika. Zakłócenia radiowe mogą uniemożliwić odbiór sygnałów, pogorszyć słyszalność, spowodować nieprawidłowe działanie urządzeń końcowych, wprowadzić w błąd operatorów lub zwiększyć błędy urządzeń automatycznych. Przy pomocy zakłóceń radiowych można utrudnić lub uniemożliwić pracę jednego urządzenia, kilku lub kilkunastu, a nawet całego systemu łączności określonego szczebla dowodzenia. Zakłócenia radiowe mogą być również wykorzystane do inicjowania pracy zapalników radiowych powodujących detonację bomb, rakiet i pocisków. Mogą one spowodować przedwczesny wybuch lub niewybuch przez całkowite zablokowanie radiozapalnika.

Zakłócenia radiolokacyjne to niepożądane sygnały zniekształcające lub zakłócające sygnały użytkowe, stanowiące nośniki danych w systemach radiolokacyjnych. Mogą być prowadzone przeciwko wszystkim rodzajom radiolokacyjnych urządzeń rozpoznawczych oraz przeciwko radiolokacyjnym środkom sterowania.

Zakłócenia radionawigacyjne polegają na celowym promieniowaniu zakłócającej energii EM powodującej utrudnienie pracy środków i systemów radionawigacyjnych (w tym bliskiej radionawigacji oraz systemów globalnych).

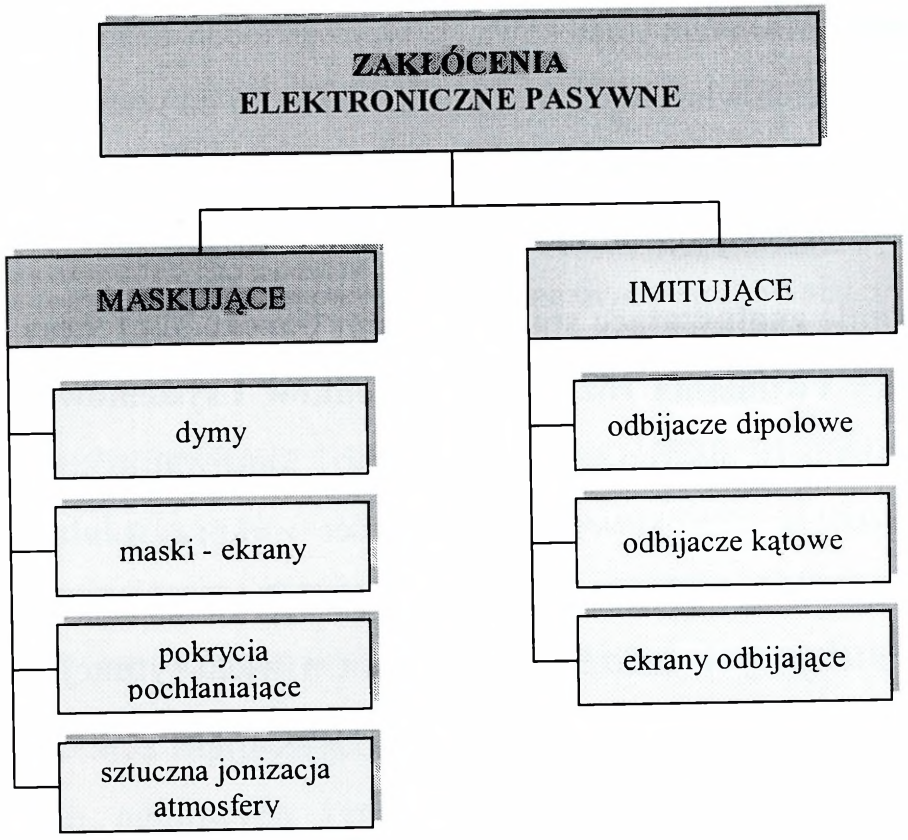
Zakłócenia optoelektroniczne mają na celu dezorganizację funkcjonowania środków rozpoznania i sterowania pracujących w podczerwieni, termolokatorów, urządzeń telewizyjnych oraz urządzeń laserowych. Z uwagi na coraz szersze wykorzystywanie tych środków w działaniach wojsk lądowych należy przewidzieć szerokie stosowanie tego typu zakłóceń.

Zakłócenia czujnikowe stanowią nowy rodzaj zakłóceń. Mają na celu dezorganizację pracy tych urządzeń, które wykorzystują fale sprężyste (infradźwięki, ultradźwięki) i są wspomagane elektroniczną przemianą rejestrowanych efektów. Należy przewidzieć stosowanie tego typu zakłóceń w przyszłych działaniach wojsk lądowych.

Zakłócenia informatyczne stanowią perspektywiczny rodzaj oddziaływania elektronicznego. Mają na celu dezorganizację pracy zautomatyzowanych systemów dowodzenia i kierowania uzbrojeniem.

Zakłócenia elektroniczne pasywne. Pasywne zakłócenia elektroniczne polegają na wtórnym promieniowaniu, odpromieniowywaniu, odbijaniu i rozpraszaniu lub też zmianie lub wchłanianiu energii elektromagnetycznej przez środki nie dysponujące generatorem energii EM w sposób zamierzony w celu zmylenia, odwrócenia uwagi lub oszukania przeciwnika i jego systemów elektronicznych. Zakłócenia pasywne dotyczą najczęściej środków radiolokacyjnych, środków pracujących w podczerwieni oraz urządzeń laserowych. Ze względu na sposób oddziaływania na zakłócane urządzenia rozróżnia się zakłócenia **maskujące i imitujące** (rysunek 1.3).

Zakłócenia maskujące utrudniają lub uniemożliwiają przeciwnikowi wykrycie i obróbkę sygnału użytecznego. Urządzenia rozpoznania elektronicznego przeciwnika rejestrują niepełny i niezgodny z rzeczywistością obraz pracy środków elektronicznych.



Rys. 1.3. Rodzaje pasywnych zakłóceń elektronicznych

Dla uzyskania efektu zakłóceń maskujących wykorzystuje się dymy metalizowane, ekrany maskujące, pokrycia przeciwradiolokacyjne, a także sztuczną jonizację atmosfery.

Zastosowanie środków wywołujących lokalną jonizację atmosfery powoduje zmianę właściwości elektromagnetycznych ośrodka, podobnie jak różnego rodzaju przeciwradiolokacyjne pokrycia maskujące. W przypadku ich użycia wyklucza się możliwość wykorzystania fal elektromagnetycznych do rozpoznania, przekazywania danych i pomiarów. Pasywne zakłócenia mogą być też wywołane przez naturalne czynniki, takie jak deszcz, śnieg, gęsta mgła itp.

Zakłócenia imitujące wprowadzają do zakłócanego systemu fałszywe dane. Za ich pomocą można wytworzyć na ekranie wskaźnika stacji radiolokacyjnej zobrazowanie celu w takim azymucie i odległości, gdzie nie ma celów rzeczywistych. Zakłócenia imitujące - stosowane przede wszystkim w radiolokacji, powodują na wskaźnikach powstawanie fałszywych zobrazowań znaków celów, analogicznych

do znaków celów realnych. Zastosowanie tych zakłóceń dezorientuje przeciwnika oraz utrudnia podjęcie właściwych decyzji. Jako środki do wytwarzania imitujących zakłóceń pasywnych stosowane są odbijacze kątowe[20], odbijacze dipolowe[21], wszelkiego rodzaju pułapki i fałszywe cele radiolokacyjne.

Zakłócanie zagłuszające stanowi zatem bardzo skuteczny sposób dezorganizacji pracy i działania różnorakich środków i systemów elektronicznych wykorzystywanych w dowodzeniu wojskami i kierowaniu uzbrojeniem przeciwnika. Ogranicza ono zakres i możliwości wykorzystania ww. systemów przez poszczególne dowództwa i sztaby a ponadto, mimo że nie powoduje bezpośrednich materialnych zniszczeń, to jednak w wielu sytuacjach jest przyczyną powstających u przeciwnika znacznych strat w sile żywej i sprzęcie bojowym.

W rezultacie zakłócania zagłuszającego środków i systemów elektronicznych przeciwnika następują zmiany w ilości danych przesyłanych do poszczególnych dowództw i sztabów oraz do wojsk wykonujących określone zadania bojowe. Często, mimo sprawności technicznej środków elektronicznych w wielu ogniwach dowodzenia wystąpić może całkowita lub częściowa utrata danych albo opóźnienie w przekazywaniu wiadomości bojowych. Poza tym przekazywane dane mogą być w znacznym stopniu zniekształcone, zamazywane i deformowane. Występować może zmniejszenie ilości danych, poprzez ich tłumienie i deformowanie lub też zwiększenie w wyniku imitowania. Skutkiem tego, do dowództw i sztabów oraz do wojsk i środków walki docierać będą dane niepełne, odznaczające się niskim stopniem wiarygodności, a nawet dopływ danych może być na pewien okres czasu cał-

---

[20] Odbijacze kątowe dzięki zwiększonemu odbijaniu energii elektromagnetycznej są używane do pozorowania obiektów rzeczywistych w otaczającym je tle. Wielkość odbijanej energii zależy od kształtu i rozmiarów odbijaczy. Specjalna konstrukcja odbijaczy kątowych powoduje znaczne odbicia energii przy stosunkowo niewielkich wymiarach.

[21] Odbijacze dipolowe, to najczęściej metalizowane włókna szklane, węglowe i poliamidowe lub metalizowana, odpowiednio cięta folia. Długość tych elementów z reguły odpowiada długości 1/2 λ. Środki dipolowe są przeznaczone do użycia w atmosferze i służą do zakłócania stacji radiolokacyjnych, pozorowania obiektów i maskowania rzeczywistych obiektów. Dipole można wyrzucać w określonych odstępach czasowych, na dużych przestrzeniach. Wyrzucona paczka rozlatuje się tworząc chmurę dipoli. Sygnał odbity od chmury można obserwować na ekranie wskaźnika jako plamę o dużej jaskrawości, plama ta sugeruje istnienie określonego obiektu. Jeśli zostanie wyrzucona duża liczba środków dipolowych w określonym obszarze na ekranie wskaźnika powstaje zobrazowanie w postaci jasnego pasma o znacznej długości (często także szerokości), to z kolei powoduje zakłócenia w pracy stacji oraz zamaskowanie obiektów będących w tym sektorze.

kowicie przerwany. Brak danych lub niski stopień ich wiarygodności uniemożliwia lub utrudnia realizację terminowego, skoordynowanego i operatywnego dowodzenia wojskami i kierowania uzbrojeniem. Obniża to sprawność bojową wojsk, ich siłę uderzeniową i skuteczność działań, uniemożliwia terminowe wykonanie zadań bojowych oraz bardzo często prowadzi do znacznych strat w sile żywej i sprzęcie bojowym.

Zakłócanie zagłuszające może przyjmować formę **rażenia** lub **uderzenia elektronicznego**. Charakteryzuje się wówczas zmasowanym i kompleksowym użyciem, w określonym czasie i miejscu aktywnych środków zakłóceń, w ścisłym powiązaniu z ogniowym rażeniem wybranych obiektów elektronicznych przeciwnika.

Czas zakłócania zagłuszającego powinien być podporządkowany potrzebom wykonania zadań ogniowych i manewrowych. Szczególnie jest to widoczne w walce z systemami obrony powietrznej i systemami dowodzenia wojsk lądowych.

Zakłócanie zagłuszające może być prowadzone selektywnie na wybranych obiektach i środkach elektronicznych lub w sposób zmasowany na środkach elektronicznych w wybranych rejonach. Wówczas wszystkie środki elektroniczne przeciwnika w obszarze walki podlegają zakłóceniu. Największą efektywność zakłócania zagłuszającego osiąga się w wyniku kompleksowego wykonywania różnego rodzaju oddziaływań elektronicznych w stosunku do najważniejszych środków i obiektów elektronicznych przeciwnika w sposób zmasowany, niespodziewanie, na głównych kierunkach i w decydujących etapach działań.

1.2.3. Zakłócanie niszczące

Z badań wynika, że niszczenie w procedurze zakłócania informacyjnego, powinno być ukierunkowane na eliminowanie u przeciwnika wybranych elementów systemu rozpoznania, dowodzenia wojskami i kierowania uzbrojeniem. Może być realizowane drogą stosowania energii kinetycznej i energii elektromagnetycznej.

Niszczenie energią kinetyczną należy stosować w odniesieniu do technicznych elementów rozpoznania, dowodzenia wojskami i kierowania uzbrojeniem. Odbywa się przy użyciu klasycznych środków ogniowych i jest przedmiotem rozważań i szczegółowych badań specjalistów w tej dziedzinie.

Niszczenie energią elektromagnetyczną, nazywane również neutralizacją, może być stosowane w odniesieniu do technicznych urządzeń elektronicznych oraz do zbiorów informatycznych.

Neutralizacja elektroniczna polega na celowym użyciu energii elektromagnetycznej o dużej gęstości mocy zarówno do chwilowego zakłócania pracy jak i uszkodzenia lub zniszczenia tych urządzeń elektronicznych przeciwnika[22], których działanie opiera się na wykorzystaniu mikroelektroniki.

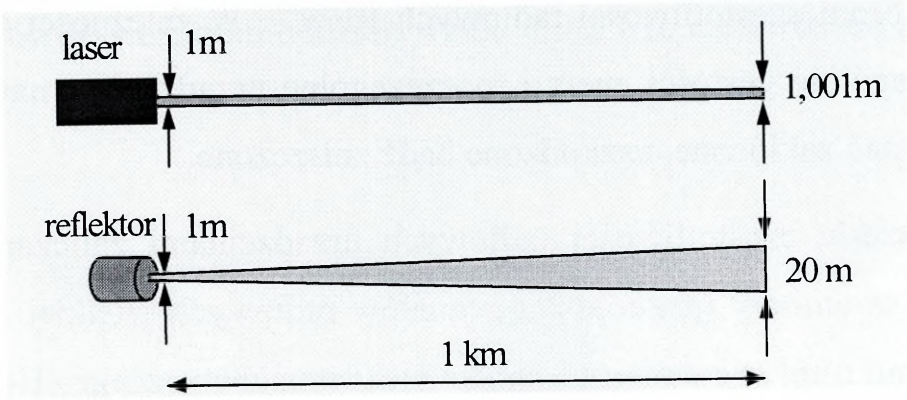
Do niszczenia energią elektromagnetyczną służy całkiem nowy rodzaj broni. Jest to tzw. broń energetyczna EW[23] oraz specyficzna jej odmiana – wiązkowa broń energetyczna DEW[24]. Specyfika broni wiązkowej polega na tym, że wygenerowany i odpowiednio uformowany strumień energii o dużej gęstości bezpośrednio oddziałuje na cel. Powoduje to jego zniszczenie, uszkodzenie bądź wyeliminowanie z walki. Skutek ataku bronią energetyczną jest niemal natychmiastowy, a przygotowania do jej użycia bardzo trudno jest wykryć. Broń wiązkowa pozwala również na wytworzenie w sposób kontrolowany innych efektów towarzyszących np. wybuchom jądrowym oraz efektów nie uwzględnianych dotychczas jako środki walki.

Wiązkowa broń energetyczna jest w stanie zniszczyć lub uszkodzić elementy uzbrojenia przeciwnika, bądź obezwładnić jego siłę żywą. Energia emitowana przez broń wiązkową rozprzestrzenia się z prędkością światła (~300 000 km/s), przy czym może być precyzyjnie dozowana i kierowana na atakowany obiekt. Inne rodzaje broni nie są w stanie razić tak szybko i z taką precyzją. O precyzji niech świadczy rozbieżność strumienia lasera, która na odległości 1 kilometra wynosi zaledwie 0,1%, gdzie na tej samej odległości rozbieżność

---

[22] Ta forma oddziaływania była dotychczas rozpatrywana w sytuacji użycia broni jądrowej, gdzie przy wybuchach część energii zamieniała się w impuls elektromagnetyczny.
[23] ang. Energy Weapon.
[24] ang. Directed Energy Weapon.

strumienia światła reflektora lotniczego o dużej zbieżności wiązki wynosi aż 2000% (20-to krotnie) – co ilustruje rysunek 1.4.



Rys. 1.4. Porównanie rozbieżności wiązki lasera i konwencjonalnego reflektora przeciwlotniczego o dużej zbieżności

Zaletą wiązkowych broni energetycznych jest również to, że na polu walki ich nośniki nie wyróżniają się niczym szczególnym aż do momentu ataku.

W wielu państwach m.in. w Stanach Zjednoczonych, Rosji, Francji, Niemczech, Wielkiej Brytanii, Chinach, Japonii, Szwecji i Izraelu, prace nad wiązkową bronią energetyczną prawdopodobnie wyszły poza sferę prób i doświadczeń laboratoryjnych. Świadczyć o tym mogą zmiany w obowiązujących przepisach. Między innymi w regulaminach SZ USA przewiduje się, że „coraz bardziej liczącym się sposobem prowadzenia walki są akcje militarne związane z użyciem skoncentrowanej energii broni elektromagnetycznej oraz bezpośrednie oddziaływanie na wyznaczone cele (zarówno obiekty, jak i otaczające je środowisko)". Na początku lat 90-tych wprowadzono do tych regulaminów poprawki dotyczące broni energetycznych innych niż elektromagnetyczne oraz broni o nieukierunkowanej emisji energii.

Wiązkową broń energetyczną obecnie można podzielić na trzy podstawowe rodzaje:

– broń częstotliwości radiowych;

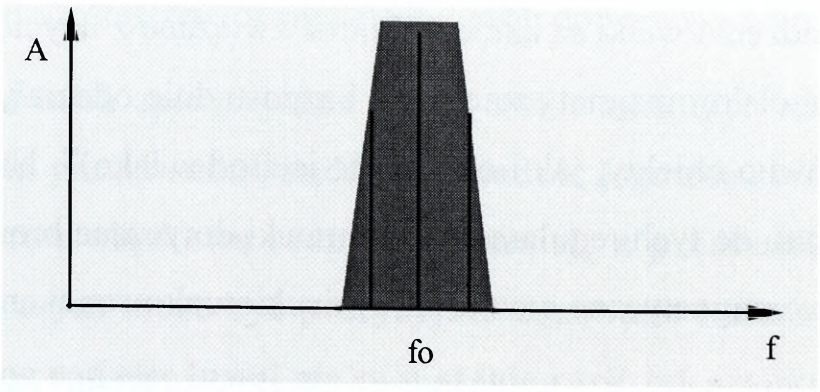
– broń laserową;

– broń cząstek elementarnych.

Broń częstotliwości radiowych. Nasycenie elektroniką nowoczesnych odmian broni, systemów rozpoznawczo-uderzeniowych, dowodzenia i kierowania a szczególnie systemów informatycznych sprawia, że są one szczególnie wrażliwe na działanie broni częstotliwości radiowych RFW[25]. W zależności od parametrów broni, a szczególnie gęstości energii, poszczególne urządzenia a nawet całe systemy, mogą zostać zakłócone, uszkodzone bądź zniszczone.

W zakresie częstotliwości radiowych urządzeniami zaliczanymi do broni wiązkowych są emitery (generatory) sygnałów radiowych wielkiej mocy HERF[26], a zwłaszcza mikrofalowe emitery impulsu elektromagnetycznego (HPM[27]). Emitery HPM wytwarzają w wąskim paśmie częstotliwości, krótkie (mikro lub nanosekundowe) impulsy energii elektromagnetycznej o mocy rzędu gigawatów. Ich odmianą są emitery LERF[28] i UWB, generujące impulsy w znacznie szerszym paśmie częstotliwości, o mocy rzędu dziesiątek megawatów. W emiterach tych udział dominującego czynnika oddziaływania na cel jest jednak nieco odmienny.

Mikrofalowe emitery HPM, najbardziej zaawansowane technicznie z tej grupy urządzeń, działają najskuteczniej, gdy ich częstotliwość emisji pokrywa się z częstotliwością pracy (f_o) obiektu ataku, bądź jego układów wewnętrznych (rysunek 1.5.).

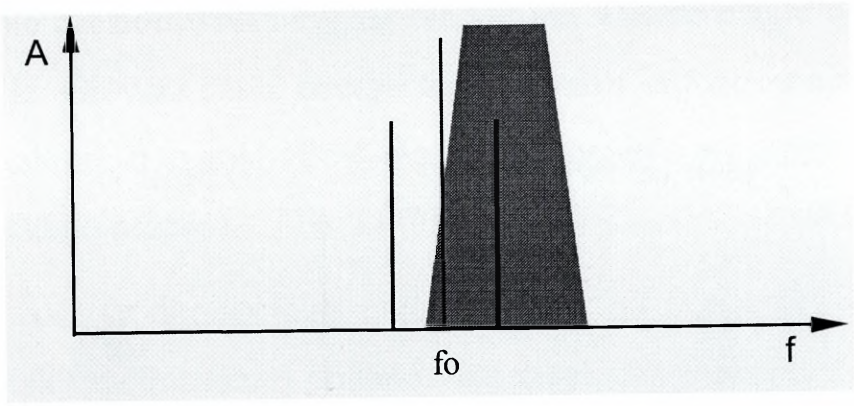


Rys. 1.5. Optymalna charakterystyka widmowa sygnału HPM

[25] ang. Radio Frequency Weapons – broń DEW zakresu częstotliwości radiowych.
[26] ang. High Energy Radio Frequency – sygnły radiowe dużej mocy .
[27] ang. High Power Microwave – emitery mikrofakowe dużej mocy.

W takim przypadku efektem oddziaływania jest najczęściej zniszczenie całego obiektu, bądź uszkodzenie któregoś z jego podzespołów.

Gdy między częstotliwością emitera i obiektu (celu) występują różnice (rysunek 1.6.), wówczas efektem oddziaływania może być uszkodzenie lub zakłócenie pracy obiektu.



Rys. 1.6. Przypadek różnicy częstotliwości pracy emitera HPM i zakłócanego obiektu

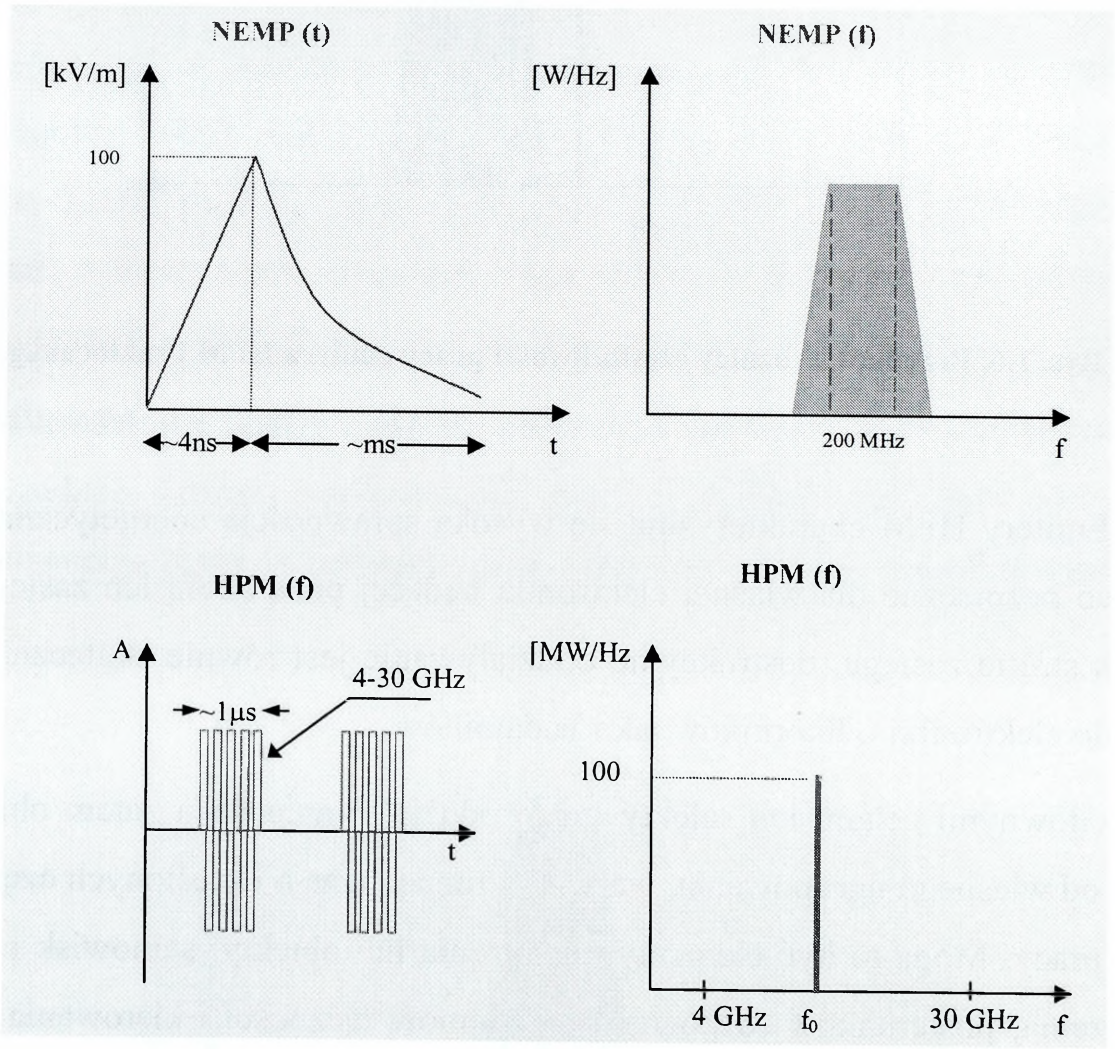
Emitery HPM charakteryzują się wysoką sprawnością energetyczną, są stosunkowo bezpieczne dla własnej elektroniki będącej poza strefą ich zasięgu, natomiast w strefie zasięgu, destrukcyjne oddziaływanie jest równie skutecznie w stosunku do elektroniki odbiorników jak i nadajników.

Głównymi celami ich selektywnego oddziaływania będą zatem obiekty oddalone od własnego ugrupowania, wcześniej rozpoznane o określonych częstotliwościach pracy. Mogą to być elementy, urządzenia lub obiekty: stanowisk i punktów dowodzenia, posterunków rozpoznania, systemów łączności i kierowania uzbrojeniem, okrętów, samolotów, śmigłowców, pocisków rakietowych oraz sztucznych satelitów ziemi z ich naziemną infrastrukturą. Sposób promieniowania to zazwyczaj ukierunkowana wiązka energii mikrofalowej, impulsu elektromagnetycznego, rzadziej promieniowania jonizującego czy strumienia plazmy. Emitery HPM mogą być instalowane w pociskach rakietowych, bombach lotniczych, środkach bezpiloto-

[28] ang. Large Energy Radio Frequency – sygnał radiowy dużej mocy.

wych, sztucznych satelitach Ziemi oraz jako mobilne i stacjonarne emitery naziemne.

Mechanizm wnikania sygnału HPM do obiektów jest podobny jak dla sygnału impulsu elektromagnetycznego wybuchu jądrowego NEMP[29]. Jednak parametry czasowe i widmowe impulsu HPM zasadniczo różnią się od analogicznych parametrów impulsu elektromagnetycznego wybuchu jądrowego NEMP co zostało przedstawione na rysunek 1.7.



Rys. 1.7. Parametry widmowe i czasowe impulsów NEMP i HPM

Impuls NEMP charakteryzuje się czasem narastania rzędu 3-10 ns i czasem opadania rzędu milisekund.

[29] ang. Nuclear Electromagnetic Pulse.

W szczycie impulsu składowa elektryczna pola może osiągnąć wartość ok. 50 kV/m. Natomiast sygnał HPM ma postać impulsu (ciągu impulsów) o czasie trwania rzędu mikrosekundy, wypełnionego sygnałem sinusoidalnym o częstotliwości 4–30 GHz.

Moc w impulsie może osiągnąć 100 MW, ale można spotkać informacje o badaniach nad impulsem o mocy rzędu giga i nawet terawatów.

W zakresie częstotliwości sygnał NEMP ma widmo ciągłe o szerokości listków około 1 GHz. Główna część energii tego impulsu jest zgromadzona w zakresie do 200 MHz. Natomiast sygnał HPM ma postać sygnału wąskopasmowego (praktycznie pojedynczego prążka).

Częstotliwość środkowa tego sygnału zależy od przyjętych rozwiązań technologicznych i jak już wcześniej podano, jest zwykle wybierana z zakresu częstotliwości 4-30 GHz.

Różnice dotyczą przede wszystkim skuteczności stosowanych zabezpieczeń i skutków oddziaływania, co wynika z różnicy parametrów elektrycznych tych sygnałów. Podstawowe drogi wnikania i sposób oddziaływania sygnału HPM na różne obiekty przedstawia tabela 1.1.

Przy obecnym stanie rozwoju urządzeń HPM wykorzystuje się dwa mechanizmy generacji impulsu:

- generacja eksplozyjna (wybuchowa);
- elektroniczny układ generacji.

W zależności od mocy i częstotliwości powtarzania impulsu, urządzenia HPM mogą być montowane na pojazdach, samolotach, w rakietach i pociskach. Mogą być także wykonane w wersji przenośnej w postaci walizki. Szczegóły techniczne rozwiązań takich urządzeń nie są publikowane. Wiadomo jedynie, że w ostatnich latach są prowadzone intensywne badania nad doskonaleniem technologii generacji impulsu.

Tabela 1.1.

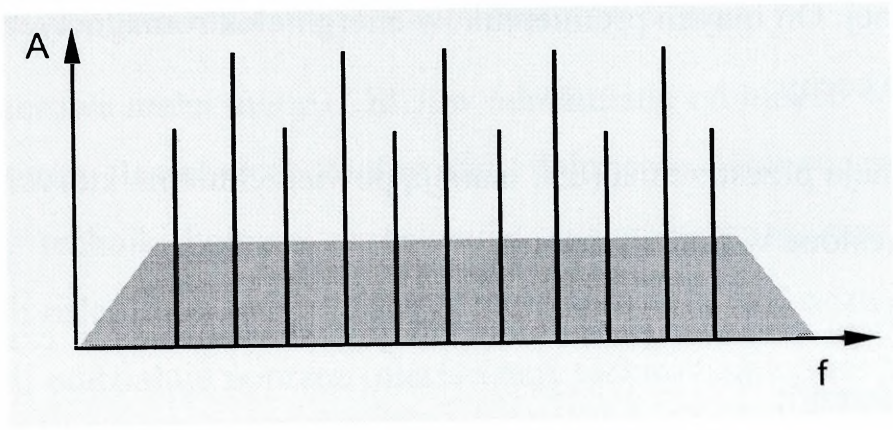
Drogi wnikania
i sposób oddziaływania sygnału HPM

Obiekt rażenia	Drogi wnikania	Skutki oddziaływania
Obiekty łączności i informatyki	- anteny; - kable i przewody metalowe; - otwory i nieciągłości w ekranach elektromagnetycznych.	- spalenie układów elektronicznych; - kasowanie pamięci; - zapłon materiałów (izolacji, obudowy itp.).
Paliwa i materiały wybuchowe	- otwory w konstrukcjach metalowych; - przewody metalowe.	- zapłon i detonacje.
Organizmy żywe	- wnikanie i propagacja wzdłuż wewnętrznych organów ciała; - wzbudzanie prądów wirowych w małych przedmiotach metalowych stanowiących elementy ubioru lub wyposażenia.	- spalenie elementów wyposażenia (przy rażeniu ciągiem impulsów); - degradacja biologiczna trwała (przy gęstości energii 20-100 J/cm^2) lub przejściowa (do 100 mJ/cm^2); - uszkodzenia spowodowane silnym nagrzewaniem elementów metalowych w protezach (np. amalgamatowe plomby).

Emitery typu UWB[30] stanowią drugą grupę urządzeń, które promieniują energię w postaci sygnałów, jednak rozproszonych w wielokrotnie szerszym paśmie częstotliwości i znacznie mniejszej gęstości mocy (rysunek 1.8.).

Energia rozproszona w szerokim paśmie nie niszczy więc elektroniki, a jedynie zakłóca jej pracę lub powoduje uszkodzenie urządzeń. Szerokopasmowość ma jednak tę zaletę, że umożliwia skuteczne oddziaływanie na źródła o nierozpoznanych parametrach w całym zakresie emitowanego pasma. Głównym ich zadaniem będzie zatem prewencyjne zakłócanie nierozpoznanych wcześniej celów.

[30] UWB - ang. Ultra Wide Band – emitery szerokopasmowe.



Rys. 1.8. Charakterystyka amplitudowo-częstotliwościowa emitera typu UWB

Energetyczne oddziaływanie emiterów UWB polega na wywołaniu zjawiska interferencji elektromagnetycznej sygnałów zakłócających z sygnałami użytecznymi (najlepiej w układach rezonansowych), bądź na wytworzeniu efektu lokalnego szerokopasmowego impulsu elektromagnetycznego EMP[31].

Celami ataku emiterów UWB mogą być nierozpoznane stanowiska i punkty dowodzenia, posterunki rozpoznania, systemy łączności i kierowania uzbrojeniem, w tym artylerii i wozów bojowych, a także pokładowe układy elektroniczne okrętów, samolotów, śmigłowców, pocisków rakietowych, torped i innych rodzajów amunicji wyposażonej w sztuczną inteligencję. Można je również wykorzystać do zdalnego detonowania sterowanych radiowo pól minowych. Emitery UWB mogą być instalowane w pociskach rakietowych i artylerii lufowej, bombach lotniczych, a nawet jako amunicja granatników ręcznych[32].

Z powyższego wynika, że przyszłe bomby impulsowe charakteryzować się będą dużymi mocami promieniowania, ponad tysiąc razy większymi niż generują klasyczne środki walki elektronicznej. W literaturze fachowej otrzymały już miano superśrodka zakłócającego. Informacje napływające o badaniach tego zjawiska wykazują, że środkami tymi może być porażona aparatura elektroniczna na znacznym obszarze oraz urządzenia wykonane w technologii „stealth".

---

[31] EMP – ang. Electro-Magnetic Pulse – impuls elektromagnetyczny.

[32] W 1994 roku Rosjanie ujawnili, że dysponują technologią do produkcji całej rodziny kompaktowej amunicji elektromagnetycznej RFM, w której wykorzystuje się eksplozję ładunków konwencjonalnych do gene-

Broń laserowa. Lasery[33] tworzą oddzielną grupę środków wiązkowej broni energetycznej. Od innych promienników energii elektromagnetycznej wyróżniają je następujące cechy:

– koherencja przestrzenna (tzn. istnieją powierzchnie na których amplitudy fali są w pełni określone w funkcji czasu);

– koherencja czasowa (amplituda fali jest skorelowana z czasem w danym punkcie przestrzeni);

– polaryzacja fali;

– wielka widmowa gęstość mocy.

Z koherencji przestrzennej wynika znikoma rozbieżność, która teoretycznie pozwala na skupienie wiązki promieniowania laserowego do średnicy rzędu długości fali.

Dzięki koherencji czasowej promieniowanie może być poddane procesowi modulacji (amplitudy, częstotliwości, fazy i impulsowej). Nieliniowe zjawiska optyczne pozwalają na otrzymywanie wyższych harmonicznych tego promieniowania.

Gęstość mocy promieniowania, nawet bez skupienia, jest niezwykle duża. Może osiągać wartości nawet setek megawatów na centymetr kwadratowy. Ponadto promieniowanie laserowe ma wszystkie klasyczne cechy fal elektromagnetycznych, od których różni się jedynie długością fali.

Współczesne technologie pozwalają na budowę laserów promieniujących w zakresie podczerwieni, światła widzialnego, promieniowania ultrafioletowego, na zakresie promieniowania rentgenowskiego kończąc. Należy jednak pamiętać, że laserowa wiązka energii jest wrażliwa na tłumienie atmosfery, dymy i inne czynniki zmniejszające energię wiązki, co ogranicza zasięg i skuteczność rażenia. Z tej grupy

---

rowania energii elektromagnetycznej. Jako „tradycyjne" źródła zasilania emiterów wykorzystywane są generatory (akceleratory) homopolarne, BWO, MHD, MILO, RKO i inne.

[33] LASER – skrót od angielskich słów: Light Amplification by Stimulated Emission of Radiation – wzmacniacz światła z wymuszoną emisją promieniowania.

środków wyróżnić można broń laserową małej mocy (LEL), dużej mocy (HEL) oraz grupę laserów promieniowania rentgenowskiego XRL.

Broń laserowa małej mocy (LEL), w odróżnieniu od innych wojskowych zastosowań emiterów laserowych (celowniki, dalmierze, oświetlacze), umożliwia obezwładnienie techniki bojowej przeciwnika, systemów rozpoznania czy łączności, poprzez ich oślepienie, bądź czasowe, rzadziej trwałe uszkodzenie. Wiązka laserowa tej broni oddziałuje poprzez interferencję elektromagnetyczną lub wywołuje efekt termiczny wrażliwych elementów elektronicznych, urządzeń optoelektronicznych oraz czujników i sensorów środków rozpoznawczych przeciwnika. Wykorzystuje się zjawisko ablacji[34], zachodzące w wypadku uderzenia promienia laserowego w atakowaną powierzchnię oraz tworzenie fali uderzeniowej i powstawanie odłamków z materiału pancerza. Plazma może zatem uszkodzić czujniki, układy kontrolno – pomiarowe, obserwacyjne itp.

Broń tego typu może być wykorzystana do obezwładniania lekko opancerzonych oraz lekkich wozów bojowych. Może być także stosowana do oślepiania ludzi, chociaż takie jej użycie jest zakazane konwencją.

Broń laserowa dużej mocy (HEL), umożliwia zwalczanie celów wiązką energii znacznie bardziej skoncentrowaną niż wiązki mikrofalowe emiterów HPM. Przy gęstościach energii rzędu 10 MJ/cm^2 efektem jej oddziaływania może być np. termiczne uszkodzenie lub zniszczenie celu. Czynnikiem rażącym jest więc przegrzanie celu lub przepalenie gorącą plazmą wytworzoną na powierzchni rażonego celu.

Broń cząstek elementarnych PBW[35]. Prowadzone są prace nad bronią wiązkową, która działa na zasadzie akceleracji cząstek elementarnych Badania dotyczą dwóch rodzajów emiterów: CBP[36] – emitujących strumień cząstek posiadających ładunek elektryczny (np. strumień elektronów lub protonów) i NPB[37] – emitujących cząstki elementarne bez ładunku (atomy wodoru, strumień neutronów).

---

[34] Ablacja – stopniowe niszczenie, kruszenie, zachodzące w wypadku uderzenia promienia laserowego w atakowaną powierzchnię oraz tworzenie fali uderzeniowej i powstawanie odłamków z materiału pancerza.

[35] PBW - ang. Particle Beam Weapon – broń cząstek elementarnych.

[36] CPB – ang. Charged Particle Beam – strumień cząstek elementarnych z ładunkiem elektrycznym.

Energia strumienia neutronów z emitera NBP jest znacznie większa od strumienia (np. elektronów) z emitera CBP i może przyjąć formę plazmy bądź kilkumilimetrowych zaledwie pierścieni, jednak niosących energię porównywalną z pociskami artyleryjskimi największych kalibrów.

Broń cząstek elementarnych PBW występuje w postaci promienników równokierunkowych, izotropowych oraz promienników kierunkowych.

Promienniki równokierunkowe lub izotropowe występują w formie amunicji artyleryjskiej lub lotniczej, wytwarzającej promieniowanie elektromagnetyczne o własnościach zbliżonych do laserowego. Ich działanie polega na krótkotrwałej emisji promieniowania elektromagnetycznego w zakresie od podczerwieni do nadfioletu oraz na porażeniu czujników i oczu żołnierzy przeciwnika. Źródłem promieniowania jest plazma powstała z gazu szlachetnego.

Promienniki kierunkowe, w odróżnieniu od równokierunkowych, są dodatkowo wyposażone w urządzenia ukierunkowujące strumień promieniowania. Pod względem konstrukcyjnym różnią się też umiejscowieniem ładunku wybuchowego. Charakteryzują się one większą sprawnością i mniejszym prawdopodobieństwem przypadkowego porażenia celów własnych.

Dotychczasowe doświadczenia[38] nad wykorzystaniem broni cząstek elementarnych wykazały, że może ona okazać się o wiele skuteczniejsza od broni laserowej. Cząstki elementarne przenikają bowiem przez obudowę urządzeń, powodując uszkodzenie układów elektronicznych, eksplozję ładunku wybuchowego głowicy lub zapłon paliwa napędowego, przy czym nie wymaga to długiego utrzymywania wiązki na celu, tak jak ma to miejsce w przypadku lasera.

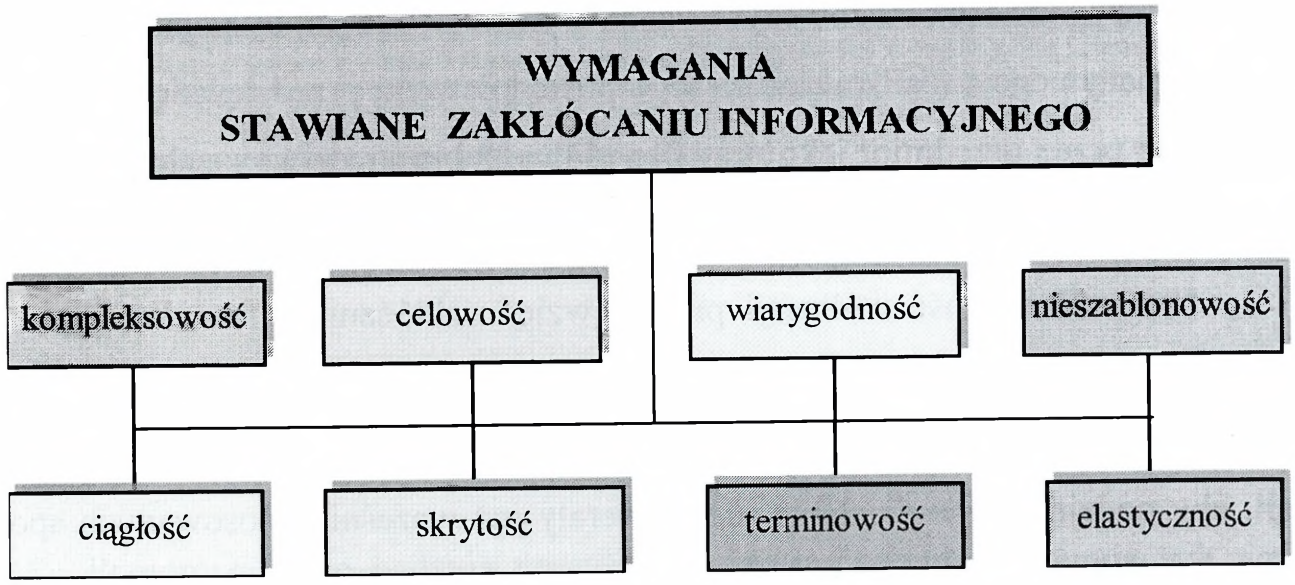
---

[37] NPB – ang. Neutral Particle Beam – strumień neutralnych cząstek elementarnych.
[38] Prowadzone są badania nad tą bronią, m.in.: w Stanach Zjednoczonych, Rosji i Chinach.

1.3. Wymagania stawiane zakłócaniu informacyjnemu

Zakłócanie informacyjne powinno być: kompleksowe, celowe, wiarygodne, nieszablonowe, ciągłe, skryte, terminowe i elastyczne (rysunek 1.8.).

Kompleksowość przedsięwzięć zakłócania informacyjnego odnosi się do stosowania jak najszerszego spektrum środków zakłócania (charakterystycznych dla określonego środowiska elektromagnetycznego, akustycznego, magnetycznego, elektrycznego, chemicznego) z uwzględnieniem wszystkich rodzajów wojsk oraz sił pozamilitarnych biorących udział w operacjach wojsk lądowych.



Rys. 1.8. Wymagania stawiane zakłócaniu informacyjnemu

Warunek kompleksowości dyktowany jest związkami funkcjonalnymi, istniejącymi pomiędzy poszczególnymi elementami walki informacyjnej. Wszelkie działania z nią związane zawsze w finale sprowadzają się do jednego wspólnego celu - stwarzania sytuacji utrudniających przeciwnikowi: podejmowanie trafnych decyzji, wykonywanie sprawnych ruchów wojskami i wykonywanie precyzyjnych uderzeń ogniowych. Innymi słowy, ukierunkowane są na dezorientowanie przeciwnika w sytuacji pola walki, komplikowanie jego warunków działania do tego stop-

nia, by w efekcie tego, spowodować prowadzenie ognia do celów fałszywych, lub miejsc gdzie nie ma żadnych obiektów do rażenia. Dlatego też przedsięwzięcia z tym związane muszą być realizowane kompleksowo i według jednolitej koncepcji, ściśle zsynchronizowanej z rzeczywistym i pozorowanym działaniem wojsk własnych oraz z ich maskowaniem. Wydaje się zatem, że najlepszym rozwiązaniem byłoby, aby cały profesjonalny potencjał zakłócania informacyjnego podporządkowany był tylko jednemu kierownictwu.

Celowość polega na ścisłej zgodności przedsięwzięć zakłócania informacyjnego z zadaniami poszczególnych etapów prowadzonej operacji wojsk lądowych, według zasady logicznego ciągu zdarzeń. Innymi słowy, zakłócanie informacyjne winno mieć cel tożsamy z celem prowadzonych działań operacyjnych, zarówno przy użyciu środków militarnych jak i pozamilitarnych.

Wiarygodność realizowanych zadań wyraża się w tym, by podmiot zakłócania informacyjnego i realizowane za jego pośrednictwem przedsięwzięcia były odczytywane przez przedmiot jako prawdopodobne lub prawdziwe na tle ogólnej sytuacji polityczno - militarnej.

Nieszablonowość realizacji przedsięwzięć zakłócania informacyjnego wydaje się konieczna i celowa. Polegać ona może na unikaniu już raz zastosowanych form zakłócania informacyjnego. Innymi słowy, podmiot powinien dążyć do sytuacji, aby podejmowane działania nie zawierały już wcześniej stosowanych sposobów i miały charakter nowatorskich rozwiązań podporządkowanych jednakże dążeniu do efektu synergicznego w całokształcie zadań realizowanych w operacjach wojsk lądowych.

Ciągłość polega na nieprzerwanym śledzeniu sytuacji operacyjnej i zakłócaniu obiektów z intensywnością dostosowaną do potrzeb operacyjnych i bojowych. Zapewnia się ją przez właściwe zaplanowanie i ciągłe utrzymywanie sił i środków zakłócania w pełnej gotowości bojowej oraz stałym współdziałaniu z innymi rodzajami wojsk i służb.

Skrytość realizacji przedsięwzięć to warunek niezbędny dla uzyskania prowadzenia przy prowadzeniu jakichkolwiek działań w walce zbrojnej. Wydaje się

celowe, by przedsięwzięcia zakłócania informacyjnego były planowane, organizowane i realizowane przez wyznaczone siły w ścisłej tajemnicy zarówno przed przeciwnikiem, jaki i przed wojskami własnymi, z wyjątkiem osób z kręgu planującego całokształt działań bojowych.

Terminowość niesie za sobą wymóg dostarczenia przeciwnikowi spreparowanych danych w takim czasie, by mógł on zareagować właściwie i w odpowiednim czasie, z punktu widzenia osiągnięcia założonego celu w prowadzonych operacjach wojsk lądowych. Terminowa realizacja przedsięwzięć zakłócania informacyjnego i wsparcie ich rzeczywistymi działaniami innych sił i środków może doprowadzić do uzyskania w wojskach przeciwnika pożądanych postaw i zachowań.

Elastyczność opiera się na zasadzie stosowania takich sposobów zakłócania informacyjnego, które są w danej chwili najbardziej skuteczne ze względu na zaistniałą sytuację militarną i polityczną. W tym celu konieczne wydaje się permanentne śledzenie i analizowanie przez wydzielone siły aktualnej sytuacji i skuteczności oddziaływania na wojska przeciwnika i jego ludność.

1.4. Wnioski

Przeprowadzone badania umożliwiają sformułowanie następujących wniosków:

1. Współczesne operacje wojsk lądowych są starciem zbrojnym prowadzonym w wielu wymiarach. Jednym z nich jest wymiar informacyjny, w którym ważną rolę odgrywa zakłócanie informacyjne.

2. Zakłócanie informacyjne prowadzi się w celu obniżenia efektywności funkcjonowania systemów dowodzenia i kierowania uzbrojeniem przeciwnika oraz ich zasobów i procesów informacyjno-sterujących. Polega ono na dezorganizowaniu procesów rozpoznawczych przeciwnika, jego procesów dowodzenia i kierowania uzbrojeniem.

3. Do podstawowych rodzajów zakłócania informacyjnego w operacjach wojsk lądowych należą:

- zakłócanie dezinformujące;
- zakłócanie zagłuszające;
- zakłócanie niszczące (niszczenie kinetyczne, elektromagnetyczne).

4. Zakłócanie informacyjne w operacjach wojsk lądowych powinno być: kompleksowe, celowe, wiarygodne, nieszablonowe, ciągłe, skryte, terminowe i elastyczne.

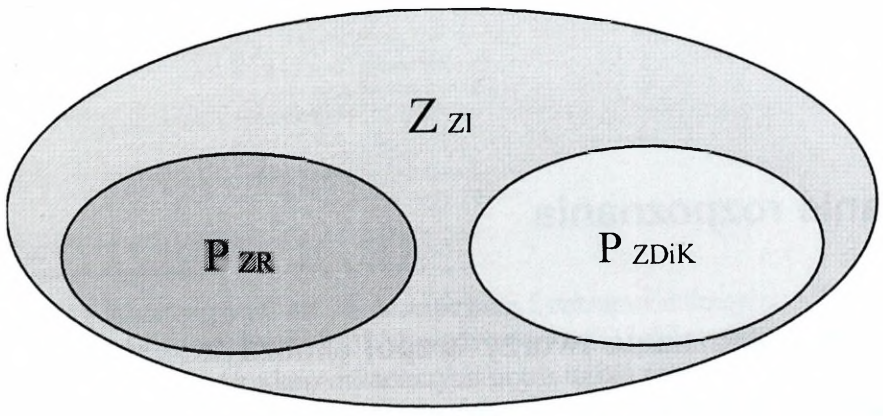
2. ZAKRES I TREŚĆ ZADAŃ ZAKŁÓCANIA INFORMACYJNEGO W OPEACJACH WOJSK LĄDOWYCH

Jak przedstawiono w rozdziale pierwszym, zakłócanie informacyjne w operacjach wojsk lądowych, ze względu na swój zakres odzwierciedla zespół skoordynowanych elementów ukierunkowanych na dezorganizację procesów rozpoznawczych przeciwnika oraz zakłócanie jego procesów dowodzenia wojskami i kierowania uzbrojeniem. Cechy wyróżnialności powinny więc dzielić ogólny zbiór skoordynowanych elementów zakłócania informacyjnego (Z_{ZI}), na dwa podzbiory dostosowane do wyżej wymienionych zadań. Będą to:

– podzbiór skoordynowanych elementów dostosowany do zakłócania procesów rozpoznawczych przeciwnika (P_{ZR});

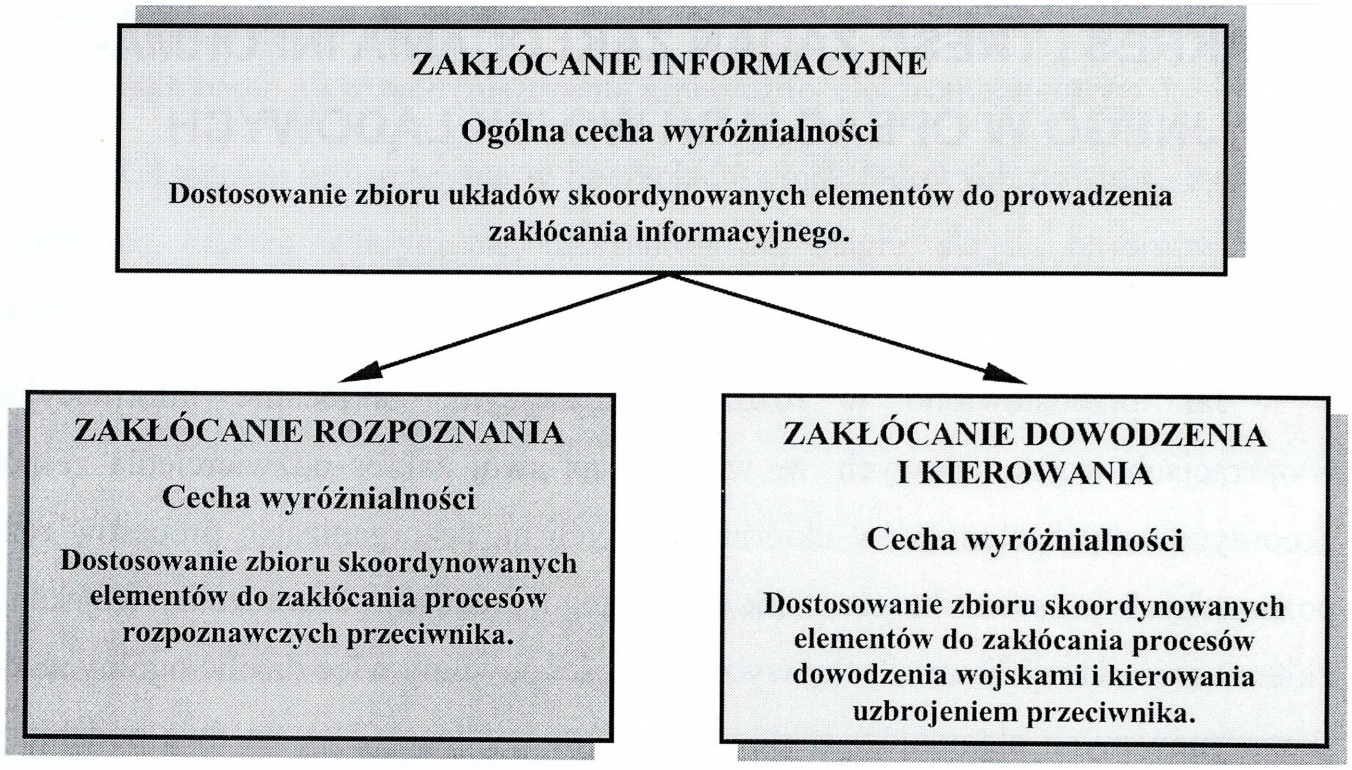
– podzbiór skoordynowanych elementów dostosowany do zakłócania procesów dowodzenia wojskami i kierowania uzbrojeniem (P_{ZDiK}).

Graficzny obraz tego podziału zilustrowano na rysunku 2.1.



Rys. 2.1. Podstawowy podział zakłócania informacyjnego

W świetle powyższego, podstawową strukturę zakłócania informacyjnego oraz cechy wyróżnialności poszczególnych jej elementów można przedstawić jak na rysunku 2.2.



Rys. 2.2. Podstawowy podział zakłócania informacyjnego

Wynika z tego, że elementy zakłócania informacyjnego zostały wyróżnione w aspekcie osiągnięcia konkretnych zamiarów tzn. paraliżowania systemów rozpoznawczych przeciwnika oraz jego szeroko rozumianych procesów dowodzenia i kierowania.

Przedstawione na rysunku 2.2. składowe zakłócania informacyjnego uczyniono przedmiotem szczegółowych badań w dalszej części tego rozdziału.

2.1. Zakłócanie rozpoznania

Zakłócanie rozpoznania tworzy zespół skoordynowanych elementów dostosowany do wnoszenia entropii do zbiorów wszelkich postaci informacji, które mogą być dostępne dla źródeł rozpoznania przeciwnika. Przedsięwzięcia z tym związane

muszą być realizowane kompleksowo, według jednolitej koncepcji ściśle zsynchronizowanej z rzeczywistym planem operacji oraz pozornym działaniem wojsk i ich maskowaniem. Paleta podejmowanych w tym zakresie wysiłków, musi być spójna i precyzyjnie dobierana. Generalnym celem jest stworzenie przeciwnikowi fałszywego obrazu rzeczywistości po drugiej stronie toczących się zmagań. Ów cel odzwierciedlają słowa *„...jest to niezmiernie złożony proces kierowania działaniami przeciwnika przez podmiot mu przeciwny i w nieznany mu sposób"*[1]. Zatem, zakłócanie rozpoznania jest elementem walki informacyjnej prowadzonej z myślą o pośrednim kierowaniu działaniami przeciwnika w taki sposób, aby był tego nieświadomy.

W operacjach wojsk lądowych, zakłócanie rozpoznania powinno odbywać się na wszystkich płaszczyznach i we wszystkich jego elementach, z których przeciwnik czerpie dane. Jego istotą jest wnoszenie entropii informacyjnej do zbiorów danych rozpoznawczych przeciwnika. Dlatego też, w zbiorze skoordynowanych elementów zakłócania rozpoznania (Z_{ZR}) należy wyróżnić:

– podzbiór skoordynowanych elementów dostosowany do zakłócania procesów rozpoznania bezpośredniego[2] (P_{ZRB});

– podzbiór skoordynowanych elementów dostosowany do zakłócania procesów rozpoznania pośredniego[3] (P_{ZRP}).

Graficzne odzwierciedlenie tego podziału zilustrowano na rysunku 2.3.

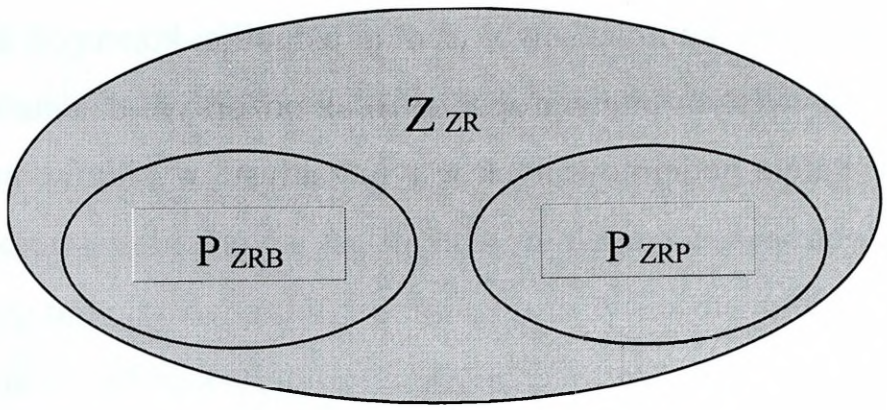
Możliwości rozpoznawcze jednej ze stron zawsze wywierały określony wpływ na formy organizowania i prowadzenia odpowiednich działań kontrrozpoznawczych drugiej strony.

---

[1] L. Ciborowski „Walka informacyjna" str.78, Europejskie Centrum Edukacyjne - Toruń 1999 r.

[2] **Rozpoznanie bezpośrednie** tworzy zespół skoordynowanych źródeł rozpoznania dostosowanych do zdobywania danych w postaci bezpośrednio odbieranych przez układ recepcyjny człowieka. Określone dane docierają bezpośrednio do prowadzącego rozpoznanie w formie zrozumiałej bez udziału przetworników.

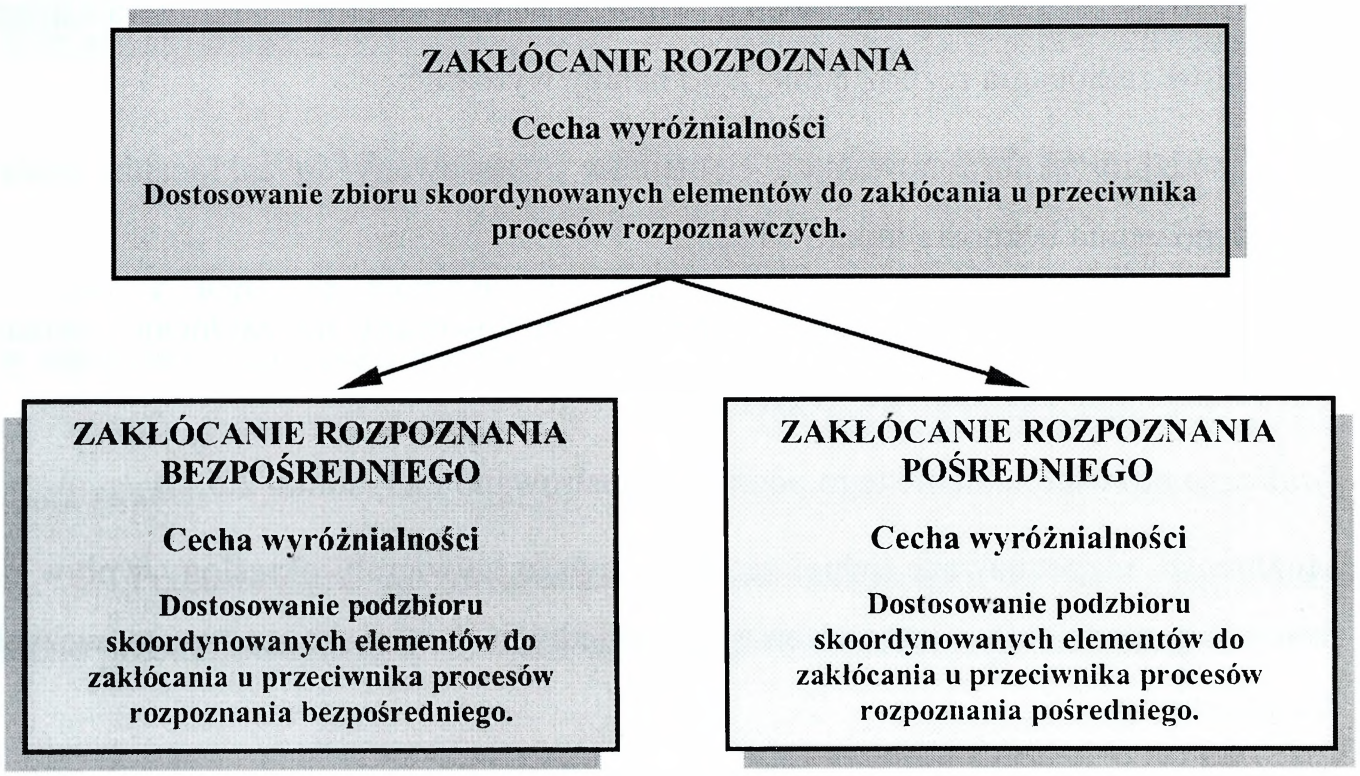
[3] **Rozpoznanie pośrednie** tworzy zespół skoordynowanych źródeł rozpoznania dostosowanych do zdobywania danych przetwarzanych przez specjalne urządzenia w postać zrozumiałą dla prowadzącego rozpoznanie. Pomiędzy zbiorem możliwych danych o rzeczy lub zjawisku a prowadzącym rozpoznanie występują przetworniki.



Rys. 2.3. Podział zakłócania rozpoznania

Przykłady i doświadczenia minionych wojen i konfliktów lokalnych dowodzą, że odpowiednio zorganizowane i prowadzone zakłócanie rozpoznania jest jednym z ważniejszych elementów oddziaływania na przeciwnika.

W aspekcie tego, podstawową strukturę zakłócania rozpoznania i cechy wyróżnialności można przedstawić jak na rysunku 2.4.



Rys. 2.4. Podstawowa struktura zakłócania rozpoznania

Z powyższego wynika, że w trakcie zakłócania rozpoznania można bezpośrednio oddziaływać na układ recepcyjny prowadzącego rozpoznanie lub jego techniczne urządzenia rozpoznawcze. W związku z tym, że układ recepcyjny człowieka,

odzwierciedla w jego świadomości obraz rzeczy materialnej lub abstrakcyjnej (przedmiotu, procesu, zjawiska, pojęcia itp.), który kojarzy się z odbieranym bodźcem. Ową problematykę określa się jako rozpoznanie bezpośrednie.

Rozpoznanie bezpośrednie powszechnie uważane jest za jednym z najstarszych rodzajów rozpoznania, w którym najważniejszą rolę spełnia człowiek utożsamiany najczęściej ze zwiadowcą i jego zmysłami. Owe zmysły, często wspomagane przez odpowiednie urządzenia, odbierają sygnały w formie bezpośrednio dla niego zrozumiałej. Mogą to być sygnały wzrokowe zawarte w paśmie promieniowania widzialnego[4], słuchowe zawarte w paśmie drgań akustycznych[5], jak również bodźce dotykowe[6], smakowe[7] i zapachowe rejestrowane przez zmysł powonienia[8]. Dopuszczalne jest stosowanie urządzeń wspomagających zasięg rozpoznania i czułość zmysłów, jednak bez przetwarzania wymienionych bodźców. Dlatego też, proces zakłócania bezpośredniego powinien być narzędziem, które uniemożliwia bądź utrudnia przeciwnikowi dostęp do wszelkich postaci informacji, które są lub mogą być dostępne dla poznania zmysłowego przeciwnika prowadzącego rozpoznanie.

Z kolei **zakłócanie rozpoznania pośredniego**, realizowane jest za pomocą urządzeń przystosowanych do oddziaływania na systemy zdobywania danych w postaci bezpośrednio nieodbieranych przez układ recepcyjny człowieka. W tym przypadku pomiędzy zbiorem możliwych postaci danych a prowadzącym rozpoznanie, występują urządzenia przekształcające pierwotne sygnały w postać odbieraną przez jego układ recepcyjny. Będą to przede wszystkim urządzenia rozpoznania elektronicznego i zbiory danych do prowadzenia rozpoznania studyjnego.

---

[4] Promieniowanie widzialne (świetlne) – część promieniowania elektromagnetycznego, która jest odbierana przez oko ludzkie. Dla człowieka przyjmuje się zakres długości fal promieniowania widzialnego 0,38 – 0,77 μm. Ilustrowana encyklopedia dla wszystkich. Fizyka, wyd. WNT, Warszawa 1991, s.274.

[5] Drgania akustyczne – zaburzenie rozchodzące się w środowisku sprężystym. Zaburzenie wywołuje chwilowe zmiany gęstości ośrodka, wskutek czego powstają chwilowe różnice ciśnień odbierane przez narząd słuchu. Ucho ludzkie reaguje na drgania akustyczne w zakresie częstotliwości 20 – 18 000 Hz. Tamże, s.77.

[6] Dotyk (zmysł, narząd dotyku) – zdolność odczuwania ucisków wywieranych na skórę i powierzchnię błon śluzowych. Słownik języka polskiego, wyd. PWN, Warszawa 1992, tom I, s.441.

[7] Smak – zmysł zdolny do odróżniania pewnych właściwości chemicznych, którego narządy znajdują się głównie na języku i w ustach. Tamże tom III, s.263.

[8] Powonienie – zmysł węchu, umożliwia odczuwanie zapachu, woni, odoru, itp. Tamże, tom II, s. 873.

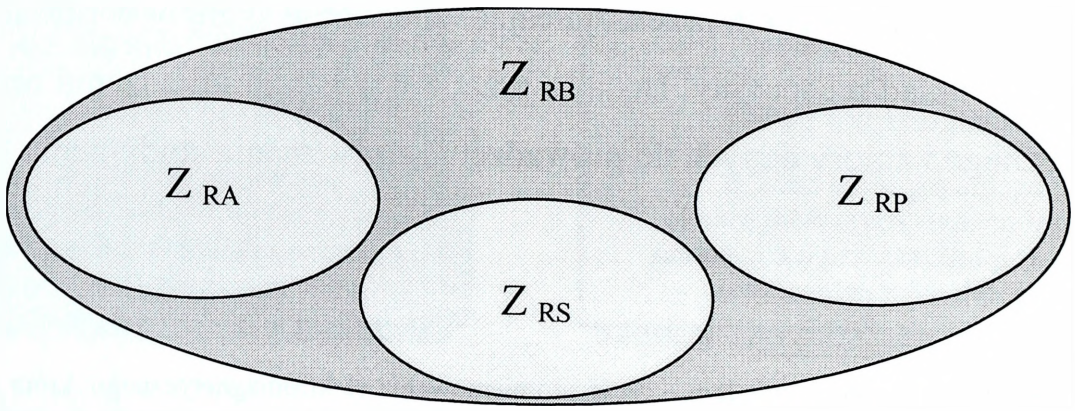
Zakłócanie jednych i drugich, czyli całej struktury rozpoznania, przynosi pożądane efekty i jest jednym z ważniejszych elementów, który należy uwzględniać w operacji wojsk lądowych. Jednak do prowadzenia dalszych rozważań na temat zakłócania owej struktury, niezbędny jest dalszy jej podział.

2.1.1. Zakłócania rozpoznania bezpośredniego

Badania struktury zakłócania rozpoznania bezpośredniego (Z_{RB}) wykazały, że w przypadku operacji wojsk lądowych należy uwzględnić:

- układ skoordynowanych elementów dostosowany do zakłócania rozpoznania agenturalnego (Z_{RA});
- układ skoordynowanych elementów dostosowany do zakłócania rozpoznania specjalnego (Z_{RS});
- układ skoordynowanych elementów dostosowany do zakłócania rozpoznania patrolowego (Z_{RP}).

Graficzny obraz tego podziału zilustrowano na rysunku 2.5.



Rys. 2.5. Podział zakłócania bezpośredniego

Owe trzy komponenty rozpoznania bezpośredniego zwanego też osobowym, powinny być uwzględniane w dalszych rozważaniach tej problematyki. Strukturę

i cechy wyróżnialności zakłócania rozpoznania bezpośredniego zilustrowano na rysunku 2.6.

Rys. 2.6. Podstawowa struktura podzbioru zakłócania rozpoznania bezpośredniego

Jak już wcześniej wspomniano, zakłócanie rozpoznania bezpośredniego oddziałuje bezpośrednio na podmiot, którym jest obserwator niezależnie od tego, jak będzie on nazywany w konkretnym systemie informacyjno-sterującym. Może być określany mianem agenta, zwiadowcy pododdziału specjalnego czy patrolu, jednak zawsze będzie spełniał rolę obserwatora. Dlatego też wszystkie przedsięwzięcia zakłócania rozpoznania bezpośredniego, są skierowane przeciwko niemu.

2.1.1.1. Zakłócanie rozpoznania agenturalnego

Zakłócanie rozpoznania agenturalnego[9] ma na celu uniemożliwienie, bądź utrudnienie przeciwnikowi zdobywania informacji z wywiadu agenturalnego. Polega na prowadzeniu odpowiednio zaplanowanych, skoordynowanych i prowadzonych akcji przeciwagenturalnych.

Rola i znaczenie rozpoznania agenturalnego była doceniana od zamierzchłych czasów. Już Sun Tsu dostrzegał celowość takich działań. Uważał, że informacje pochodzące z wywiadu należy traktować priorytetowo, a tajnych agentów zalecał szczególnie chronić, ponieważ w przypadku, gdy armia zostanie ich pozbawiona, wszelkie działania zbrojne nie mają sensu. Sun Tsu wyróżnia *„pięć rodzajów tajnych agentów (narodowi, wewnętrzni, podwójni, straceni oraz powracający). Jeśli tych pięć typów zatrudnionych agentów pracuje w koordynacji, to są nazwani doskonałą siatką i znajdują się pod szczególną opieką władcy. Tylko oświecony władca oraz zacny generał są w stanie użyć najinteligentniejszych ludzi jako agentów, a z nimi mogą dokonać wielkich rzeczy. Tajne plany i operacje są zasadnicze dla działań wojennych, bez nich armia nie może zrobić żadnego sensownego ruchu. Armia pozbawiona agentów jest doprawdy jak człowiek ślepy i głuchy"*[10].

Przytoczone w cytacie uniwersalne prawdy i aspekty problemu są powszechnie znane, jeśli nawet nie przeciętnym ludziom to na pewno specjalistom, którzy profesjonalnie zajmują się rozpoznaniem agenturalnym.

Planowanie i prowadzenie zakłócania agenturalnego w operacji wojsk lądowych, należy powierzyć ekspertom ze służb kontrwywiadowczych, bowiem ze względu na złożoność i niejawny charakter tej problematyki, nie będzie ona szerzej rozpatrywana w niniejszej pracy badawczej.

---

[9] Rozpoznanie agenturalne – to ogół przedsięwzięć organizacyjnych (tajnych), które mają na celu zdobywanie materiałów i informacji stanowiących tajemnicę państwową i wojskową potencjalnego przeciwnika. Ze względu na dziedzinę zainteresowań w rozpoznaniu agenturalnym można wyróżnić wywiad wojskowy, polityczny, gospodarczy i psychologiczny.

[10] Sun Tsu „Sztuka wojny" wyd. Przedświt, Warszawa 1994, s. 40 i 46.

2.1.1.2. Zakłócanie rozpoznania patrolowego

Zakłócanie rozpoznania patrolowego[11], polega na uniemożliwieniu bądź utrudnieniu realizacji zadań takich jak: wykrycie i obserwacja przeciwnika, rozpoznanie jego sił i charakteru działań, bezpośredniego rozpoznania rejonu, obiektów terenowych, przeszkód, zapór inżynieryjnych, rejonów zniszczeń czy umocnień. Patrol rozpoznawczy może brać udział w realizacji innych przedsięwzięć między innymi takich jak: chwytanie jeńców, zdobywanie dokumentów, wzorów nowego uzbrojenia i sprzętu przeciwnika itp.

Analiza metod pozyskiwania informacji przez zwiadowców pododdziałów specjalnych i patroli, sugeruje wyróżnienie kilku przedsięwzięć związanych z zakłócaniem osobowym.

Zasadnicze przedsięwzięcia zakłócania rozpoznania patrolowego należy ukierunkować na uniemożliwienie bądź utrudnienie zwiadowcom: obserwacji obiektów, penetracji dokumentów oraz ochronę personalną.

Zakłócanie obserwacji powinno polegać na szeroko rozumianym maskowaniu, ochronie i obronie ważnych obiektów takich jak:

- operacyjne i taktyczno-operacyjne dywizjony rakiet, ich systemy kierowania, składy i punkty amunicji;
- stanowiska dowodzenia i węzły łączności;
- środki rozpoznania elektronicznego, powiadamiania i naprowadzania;
- urządzenia i obiekty obrony powietrznej i przeciwlotniczej;
- rejony ześrodkowania wojsk oraz kierunki ich przegrupowania;
- lotniska, lądowiska, porty i bazy morskie, obiekty obrony wybrzeża;

---

[11] Patrol rozpoznawczy jest elementem najczęściej organizowanym i wysyłanym przez oddział rozpoznawczy, w celu wykonania określonych, krótkotrwałych przedsięwzięć lub zadań rozpoznawczych oraz zabezpieczenia własnych wojsk, przed niespodziewanym spotkaniem z przeciwnikiem.

– ważne obiekty komunalne oraz systemy logistycznego zabezpieczenia wojsk;

– systemy zapór inżynieryjnych, szerokich przeszkód wodnych i urządzeń hydrotechnicznych.

Zakłócanie penetracji dokumentów powinno uniemożliwiać zwiadowcom przeciwnika dostęp do prawdziwych planów operacji, mobilizacji, ważnych instrukcji, projektów itp. W ramach zakłócania tej formy rozpoznania, można im udostępnić umiejętnie spreparowane „dokumenty".

Ochrona personalna powinna obejmować wyższych dowódców i ważne osobistości. Powinna uniemożliwiać przeciwnikowi dostęp zarówno do nich samych, jak i faktów z ich życia służbowego i prywatnego. Zainteresowania personalne mogą koncentrować się wokół wykształcenia tych osób, uzyskiwanych przez nich postępów w pracy zawodowej, zajmowanej pozycji, ich wyglądu, autorytetu, upodobań i skłonności, stanu posiadania itp.

Inne formy zakłócania osobowego, które mogą być wykorzystane przeciwko zwiadowcom rozpoznania specjalnego i patrolowego przeciwnika to między innymi: podstęp, wprowadzanie w błąd, tak zwana „biała" i „czarna" propaganda oraz wpływanie i dezinformowanie.

Podstęp jest posunięciem, krokiem lub wybiegiem mającym na celu zmylenie, podejście lub oszukanie kogoś[12]. Jednym z najstarszych i najbardziej znanych przykładów użycia podstępu, jest słynna opowieść o koniu trojańskim, który umożliwił Grekom zdobycie Troi, po dziesięcioletnim bezskutecznym jej oblężeniu[13].

Wprowadzenie w błąd jest jedną z częściej stosowanych metod stosowaną między innymi w działaniach operacyjnych. O jego skuteczności przy zakłócaniu rozpoznania agenturalnego i specjalnego decyduje wiele czynników. Między innymi dostrzec tu można:

– elastyczność reagowania na zmieniającą się sytuację;

– powtarzalność w kreowaniu fałszywych obrazów;

---

[12] Słownik języka polskiego, wyd. PWN, Warszawa 1992, tom II, s.750.
[13] Zburzenie Ilionu Leschesa z Pyrry, wyd. Wiedza Powszechna, Warszawa, 1985, s.82.

- terminowość i ciągłość w realizacji przedsięwzięć;
- trafność doboru narzędzi i form wprowadzania w błąd;
- oryginalność i realistyczną spójność w kreowaniu fałszywych sytuacji;
- kompleksowość podejmowanych działań.

Przestrzeganie tych reguł uwiarygodni kreowane przez nas fałszywe obrazy i w połączeniu z innymi formami zakłócania rozpoznania, może przynieść pożądane rezultaty.

Taki zabieg, udał się między innymi Aliantom w czasie II Wojny Światowej. Po podjęciu decyzji o lądowaniu na Sycylii - chcąc wprowadzić w błąd Niemców - podrzucono w jednym z hiszpańskich portów zwłoki brytyjskiego oficera wraz ze spreparowanymi dokumentami o rzekomych przygotowaniach do inwazji w Grecji. W wyniku tego, niemiecka 11 flotylla torpedowców i prawie całe siły przeznaczone do obrony Sycylii opuściły ją, co sprawiło, że Alianci wylądowali nie napotykając prawie na żaden opór.

Przedsięwzięcia związane z propagandą, w operacjach wojsk lądowych powinno powierzyć się ekspertom od propagandy.

Biała propaganda[14] stanowi element aktywnego zakłócania, oceniany jednak jako mało skuteczny, ponieważ informacje pochodzące z oficjalnych źródeł przeciwnika, siłą rzeczy mają ograniczoną wiarygodność.

Czarna propaganda nie ujawniając swojego źródła, a często podszywając się pod oficjalne źródło przeciwnika, czyni podawane fakty wiarygodnymi.

Przykładem znakomicie zorganizowanej i prowadzonej „czarnej propagandy" w czasie II Wojny Światowej, była brytyjska rozgłośnia *„Gustav Siegfried Eins"* - rzekomo proniemiecka, której twórcą i główną postacią był Stefon Delmer. Finezyjne i wyrafinowane akcje propagandowe - jak to oceniono po wojnie w Niemczech Zachodnich - były wynikiem nie tylko inteligencji i uzdolnień Delme-

[14] Propaganda - rozpowszechnianie jakichś poglądów, idei, haseł, mające na celu kształtowanie określonych, korzystnych dla siebie postaw wśród dużych grup ludzi, manipulowanie zbiorową świadomością, agitacja. Słownik współczesnego języka polskiego, wyd. Wilga, Warszawa 1996, s. 858.

ra, lecz także „jego psychicznego refleksu nabytego w czasie wieloletniej konfrontacji z Niemcami”[15].

Wpływanie[16] jest jedną z technik czarnej propagandy, jednak znacznie bardziej wyrafinowaną. Ten rodzaj zakłócania nie ma na celu zmiany biegu wydarzeń, lecz destabilizację przeciwnika. Nie jest istotne, czy ta forma działania przyniesie korzyści organizatorowi, lecz istotne jest, aby spowodowała szkody u przeciwnika. Działania muszą być na tyle subtelne, aby nie zdradzić swoich sympatii do strony, na której rzecz się działa. Na przykład Sun Tzu radzi, żeby w kraju będącym celem takich działań buntować młodych przeciw starym, aby wykopać przepaść między pokoleniami.

Dezinformowanie jako jedno z przedsięwzięć aktywnego zakłócania, jest zbieżne z wprowadzanim w błąd. O ile jednak wprowadzanie w błąd jest czynnością jednorazową, związaną z konkretnym zadaniem np. taktycznym, to dezinformowanie jest oddziaływaniem długotrwałym. Powinno być prowadzone za pośrednictwem mediów według precyzyjnego planu w taki sposób, aby w konsekwencji doprowadzić do wytworzenia w świadomości, bądź podświadomości nie tylko zwiadowców, ale również żołnierzy i ludności cywilnej, pożądanych poglądów czy zachowań.

W działaniach wojsk lądowych dezinformowanie powinny prowadzić służby specjalne, bowiem stanowi ono syntezę wywiadu oraz zakłócania wszystkich form i metod rozpoznania. Wszelka inicjatywa w tym zakresie, ze strony podwładnych, jest niepożądana i najczęściej szkodliwa. Niższy szczebel, nie znając rzeczywistych zamiarów i planów operacji, może je zdemaskować i zniweczyć podejmując działania dezinformujące z własnej inicjatywy. Z analizy faktów historycznych wynika, że nigdy w nie zdarzyło się, aby dezinformowanie podjęte z inicjatywy niższych szczebli było skuteczne. Zawsze było demaskowane, a jeśli nawet nie, to i tak przynosiło rezultaty odwrotne do zamierzonych. Potwierdzeniem tej tezy może być następujący przykład.

---

[15] W. Kozaczuk Wojna w eterze, wyd. Radia i telewizji Warszawa, 1977, s.111.

[16] Wpływanie – nacisk, oddziaływanie na kogoś lub na coś. Słownik współczesnego języka polskiego, wyd. Wilga, Warszawa 1996, s. 1245.

W czasie pierwszej wojny światowej, ówczesny szef brytyjskiego wywiadu wojskowego Reginald Hall, pod koniec 1914 roku z własnej inicjatywy rozpowszechnił informacje o koncentracji sił brytyjskiej floty do osłony desantu, który rzekomo miał być wysadzony w północnej Holandii pomiędzy rzekami Ems i Wezerą. Wydawać by się mogło, że odniósł sukces, bowiem niemieckie dowództwo uległo dezinformacji i przerzuciło w ten rejon dodatkowe siły. Jednak Brytyjczycy, po wykryciu niemieckiego manewru, a nie znając jego rzeczywistych przyczyn, również zaczęli koncentrować w tym rejonie dodatkowe siły, osłabiając tym samym inne odcinki frontu. Jest to klasyczny przykład, jak podjęta autonomicznie inicjatywa ukierunkowana na dezinformowanie przeciwnika, zadziałała negatywnie również i na własną stronę.

Sposoby i narzędzia wykorzystywane w prowadzeniu tego pokroju działań są bardzo złożone. Ich rodzajowa i ilościowa rozpiętość musi być tak dobierana, aby generowała do systemu rozpoznania przeciwnika takie dane, które stwarzać będą symptomy rzeczywistych działań, sytuacji i zamiarów. Dlatego też działania dezinformujące muszą być zsynchronizowane z innymi przedsięwzięciami, w tym szczególnie z obroną informacyjną i zdemaskowaną już przez przeciwnika częścią działań i rzeczywistych planów. Oderwane od siebie poszczególne ich elementy, nie tylko nie wprowadzają przeciwnika w błąd, ale wręcz zdemaskują fakt ich prowadzenia, co zamiast entropii, zwiększy u niego stan uporządkowania wiedzy o otoczeniu.

Fakt ten wynika z ilościowej miary informacji nazywanej entropią[17]. Miara ta jest nierozerwalnie związana z prawdopodobieństwem zdarzenia i definiowana jest równaniem:

$$I = f(p)$$

[17] Pojęcie entropia po raz pierwszy użyte zostało przez Clausiusa w 1876 r. Później tym samym pojęciem nazwano funkcję opisującą stan układu termodynamicznego i jego zmiany. Związek entropii stosowanej w termodynamice z ilością informacji obszernie zinterpretował C.I. Shannon w 1948 r.
Tu zostało użyte jako miara nieokreśloności i stopnia nieuporządkowania danych o sytuacji, elementach lub stanach znajdujących się w pewnym zbiorze przeliczalnym, które przy określaniu ich możliwej wartości, traktowane są jako zmienne losowe.

gdzie:

I – ilość informacji;

p – wartość prawdopodobieństwa.

Pomiędzy ilością informacji i wartością prawdopodobieństwa zachodzą trzy zależności:

① $$p_1 \leq p_2 \Rightarrow f(p_1) \geq f(p_2)$$

Co oznacza, że im większe jest prawdopodobieństwo zdarzenia, tym mniej informacji przynosi wiadomość, że dane zdarzenie zaszło.

② $$p = 1 \Rightarrow f(p) = 0$$

Z czego wynika, że ilość informacji o zdarzeniu pewnym równa jest 0, a zatem wiadomość o tym zdarzeniu nie niesie w sobie żadnej informacji, bowiem o zdarzeniu pewnym wiemy już wcześniej, że takie zajdzie.

③ $$p = p_1 p_2 \Rightarrow f(p_1 p_2) = f(p_1) + f(p_2)$$

Co oznacza, że informacja o iloczynie zdarzeń, równa jest sumie informacji o poszczególnych zdarzeniach.

Z powyższych zależności wynika, że wszystkie trzy warunki występujące pomiędzy wartością prawdopodobieństwa i ilością informacji spełnia funkcja:

$$I = f(p) = -\log_a p$$

gdzie:

a – ilościowa jednostka miary informacji.

Jeśli natomiast za ilościową jednostkę miary informacji przyjęty zostanie wybór dwustanowy (tak, nie), wówczas ilość informacji mierzona będzie w bitach i wyniesie:

① przy braku wyboru (dla p=1):

$$I = -\log_2 1 = 0 \; bitów;$$

② przy wyborze zdarzenia z 2 możliwości (dla p=0,5):

$$I = -\log_2 0{,}5 = -\log_2 1/2 = -(\log_2 1 - \log_2 2) = 1 \; bit;$$

③ przy wyborze zdarzenia z 8 możliwości (dla p=0,125):

$$I = -\log_2 0{,}125 = -\log_2 1/8 = -(\log_2 1 - \log_2 8) = 3 \; bity;$$

④ przy wyborze zdarzenia z 2^n możliwości (dla $p=1/2^n$):

$$I = -\log_2 \frac{1}{2^n} = -(\log_2 1 - \log_2 2^n) = -(\log_2 1 - n\log_2 2) = n \; bitów.$$

Przytoczone wyżej zasady ustalania ilości informacji są właściwe, ale tylko w sytuacji, kiedy każde zdarzenie zachodzi z takim samym prawdopodobieństwem. To znaczy, kiedy rozkład dyskretnej zmiennej losowej X_d charakteryzuje się ciągiem rozkładów:

$$p_i = P(X_d = x_i)$$

dla:

$$p_1(x_1) = p_2(x_2) = \ldots = p_n(x_n)$$

W praktyce oznacza to, że wcześniej nic nie było wiadomo o zdarzeniach, które mają nastąpić, wiadomo było jedynie, że *n* takich zdarzeń nastąpi. Najczęściej jednak jest tak, że pewnych zdarzeń oczekuje się z mniejszym, a innych z większym prawdopodobieństwem, co oznacza, że coś już wcześniej o nich wiedziano. Wówczas rozkład dyskretnej zmiennej losowej X_d charakteryzować się będzie ciągiem rozkładów:

$$p_i = P(X_d = x_i)$$

dla:

$i=1;2;...;n.$

W takiej sytuacji mówi się o średniej ilości informacji, a wartość tę oblicza się z zależności:

$$\bar{I} = -\sum_{i=1}^{n} p_i \log_a p_i$$

gdzie:

$\bar{I}$ – *średnia ilość informacji.*

Jeśli na przykład dyskretna zmienna losowa X_d charakteryzować się będzie ciągiem rozkładów:

$$p_i = P(X_d = x_i)$$

dla:

$i=1;\ 2;\ 3;\ 4;$

gdzie:

$p_1(x_1) = 0{,}25;$
$p_2(x_2) = 0{,}5;$
$p_3(x_3) = 0{,}125;$
$p_4(x_4) = 0{,}125.$

Wówczas średnia ilość informacji, przypadająca na każdą wiadomość o dowolnym zdarzeniu należącym do zbioru dyskretnej zmiennej losowej X_d, wynosić będzie 1,75 bitów, ponieważ:

$$\bar{I} = \sum_{i=1}^{4} p_i \log_2 p_i =$$

$$= -(0{,}25\log_2 0{,}25 + 0{,}5\log_2 0{,}5 + 0{,}125\log_2 0{,}125 + 0{,}125\log_2 0{,}125) =$$

$$= -\left(\frac{1}{4}\log_2\frac{1}{4} + \frac{1}{2}\log_2\frac{1}{2} + \frac{1}{8}\log_2\frac{1}{8} + \frac{1}{8}\log_2\frac{1}{8}\right) =$$

$$= -\left[\begin{array}{l}\frac{1}{4}(\log_2 1 - \log_2 4) + \frac{1}{2}(\log_2 1 - \log_2 2) + \\ + \frac{1}{8}(\log_2 1 - \log_2 8) + \frac{1}{8}(\log_2 1 - \log_2 8)\end{array}\right] =$$

$$= -\left[\frac{1}{4}(0-2) + \frac{1}{2}(0-1) + \frac{1}{8}(0-3) + \frac{1}{8}(0-3)\right] =$$

$$= -\left(-\frac{2}{4} - \frac{1}{2} - \frac{3}{8} - \frac{3}{8}\right) = \frac{7}{4} = 1{,}75\ \textit{bitów}$$

Gdyby się jednak zdarzyło, że wcześniej nic nie byłoby wiadomo o mających nastąpić zdarzeniach, wtedy dyskretna zmienna losowa X_d charakteryzować się będzie ciągiem rozkładów:

$$p_i = (X_d = x_i)$$

dla:

$i=1, 2,3,...n,$

gdzie:

$$p_1(x_1) = p_2(x_2) = ... = p_n(x_n)$$

co w odniesieniu do analizowanego przykładu przyjmie wartości:

$$p_1(x_1) = 0{,}25;$$
$$p_2(x_2) = 0{,}25;$$
$$p_3(x_3) = 0{,}25;$$
$$p_4(x_4) = 0{,}25.$$

To w takim przypadku średnia ilość informacji $\bar{I}$ wyniesie 2 bity, ponieważ:

$$\bar{I} = -\sum_{i=1}^{4} p_i \log_2 p_i =$$

$$= -(0{,}25\log_2 0{,}25 + 0{,}25\log_2 0{,}25 + 0{,}25\log_2 0{,}25 + 0{,}25\log_2 0{,}25) = 2\ \textit{bity}$$

Z porównania powyższych przykładów wynika, że średnia ilość informacji zależna jest zawsze od wartości prawdopodobieństw, które zostały przypisane zdarzeniom elementarnym występującym podczas realizacji zmiennej losowej X_d. Wynika też to, że średnia ilość informacji osiąga zawsze największą wartość przy realizacji zdarzeń równoprawdopodobnych, czyli w sytuacji, kiedy dane zjawisko (proces), na które składa się n realizacji zmiennej losowej X_d, nie zostało wcześniej rozpoznane.

W teorii ogólnej, średnia ilość informacji określana mianem entropii, oznaczana jest symbolem H i zapisywana równaniem:

1. dla rozkładu dyskretnego:

$$H(X_d) = -\sum_{i=1}^{n} p_i \log_a p_i$$

gdzie:

X_d – *dyskretna zmienna losowa;*

p_i – *prawdopodobieństwo i-tej realizacji dyskretnej zmiennej losowej* X_d;

a – *jednostkowa miara ilości informacji.*

2. dla rozkładu ciągłego:

$$H(X_c) = -\int_{-\infty}^{\infty} f(x) \log_a f(x) dx + C$$

gdzie:

X_c – *ciągła zmienna losowa;*

$f(x)$ – *gęstość prawdopodobieństwa realizacji ciągłej zmiennej losowej* X_c;

a – *jednostkowa miara ilości informacji;*

C – *stała określająca początek liczenia entropii ciągłej zmiennej losowej* X_c.

Tak w pierwszym, jak i w drugim wypadku entropia rozkładu zmiennej losowej (tak ciągłej X_c, jak i dyskretnej X_d), zawsze stanowi miarę nieokreśloności

i stopnia nieuporządkowania sytuacji, elementów względnie stanów, które znajdują się w pewnym zbiorze przeliczalnym i przy określaniu ich możliwej wartości, traktowane są jako realizacje zmiennej losowej, tak ciągłej X_c, jak i dyskretnej X_d.

Z powyższych rozważań wynikają następujące wnioski:

– entropię zmiennej losowej można obliczać tylko wówczas, kiedy są znane charakterystyki probabilistyczne tej zmiennej;

– entropia zmiennej losowej jest tym większa, przy ustalonym zakresie zmienności, im bardziej rozkład prawdopodobieństwa zmiennej losowej jest zbliżony do rozkładu równomiernego;

– dla zbioru niezależnych zmiennych losowych entropia jest sumą entropii jego podzbiorów;

– entropia jest równa zeru tylko dla zmiennej losowej, której zbiór wartości jest równy jedności.

Przytoczona argumentacja jednoznacznie dowodzi i wskazuje, że nadmiar informacji jest niepożądany w działaniu celowym, ponieważ zwiększa entropię informacyjną o przestrzeni i materii pola operacyjnego, na którym to działanie ma być lub jest podejmowane. Dlatego też wszystkie przedsięwzięcia realizowane w tym zakresie, muszą być odpowiednio scentralizowane, kompleksowe, spójne, wiarygodne, nieszablonowe, skryte, terminowe, ciągłe i elastyczne.

2.1.1.3. Zakłócanie rozpoznania specjalnego

Działania specjalne są specyficznym rodzajem rozpoznania. Owa specyfika polega głównie na prowadzeniu samodzielnych działań przez kilkuosobowe zespoły (grupy specjalne) w osamotnieniu i całkowitej izolacji od własnych wojsk, bezpośrednio w ugrupowaniu i na tyłach przeciwnika, w warunkach jego ilościowej przewagi i ciągłego zagrożenia.

Doświadczenia ostatnich konfliktów zbrojnych potwierdzają, że we współczesnych warunkach, działania specjalne nabierają szczególnego znaczenia. Grupy specjalne, działające w ugrupowaniu przeciwnika oraz na jego głębokich tyłach, mogą zdobywać bądź potwierdzać informacje bez względu na pogodę, porę roku, doby itp. Są w stanie określić stan i gotowość bojową przeciwnika, rodzaj i charakter działań, a nade wszystko ustalić dokładne współrzędne wykrywanych obiektów. Dlatego, obiekty ważne z punktu widzenia działań operacyjnych, powinny podlegać szczególnej ochronie i obronie.

Obok zadań rozpoznawczych, jednostki działań specjalnych mogą wykonywać w określonej sytuacji zadania dywersyjne i psychologiczno-propagandowe, a także zadania o szczególnym charakterze np. nawiązywanie kontaktów z przedstawicielami ruchu oporu.

Zakłócanie rozpoznania specjalnego powinno rozpocząć się od ich zwalczania w trakcie przerzutu, następnie uniemożliwiać bądź utrudniać prowadzenie rozpoznania oraz paraliżować wszelkie przejawy ich działalności dywersyjnej, sabotażowej, terrorystycznej i propagandowej. Do realizacji tych przedsięwzięć wyznaczyć można zarówno określone siły wojsk operacyjnych jak i układu pozamilitarnego. Formy zakłócania rozpoznania specjalnego są zbieżne z formami zakłócania patrolowego.

2.1.2. Zakłócanie rozpoznania pośredniego

Zakłócanie rozpoznania pośredniego w operacjach wojsk lądowych, obejmuje wszelkie środki rozpoznania przeciwnika, przystosowane do zdobywania danych w postaci bezpośrednio nieodbieranej przez układ recepcyjny człowieka. W rozpoznaniu pośrednim, pomiędzy zbiorem tych danych a prowadzącym rozpoznanie, występują przetworniki przekształcające dane, w postać odbieraną przez zmysły człowieka. Istotą działania tych przetworników jest odbiór i przekształcenie

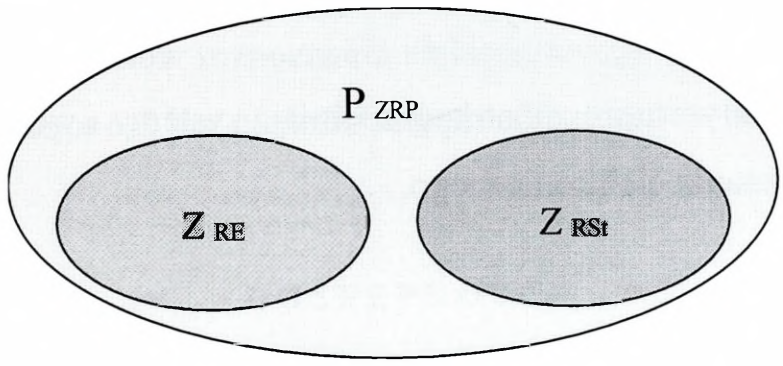
sygnałów - których nośnikami zazwyczaj są fale elektromagnetyczne - najczęściej w postać obrazu rejestrowanego przez zmysł wzroku lub dźwięku rejestrowanego przez zmysł słuchu. Przetworniki wchodzą w skład technicznej struktury rozpoznania, więc w ramach zakłócania pośredniego, oddziałujemy na ową techniczną strukturę systemów i środków przeciwnika.

Stosując te same kryteria, co w poprzednim podrozdziale, w podzbiorze zakłócania rozpoznania pośredniego (P_{ZRP}), należy uwzględnić:

– układ skoordynowanych elementów dostosowany do zakłócania rozpoznania elektronicznego (Z_{RE});

– układ skoordynowanych elementów dostosowany do zakłócania rozpoznania studyjnego (Z_{RSt}).

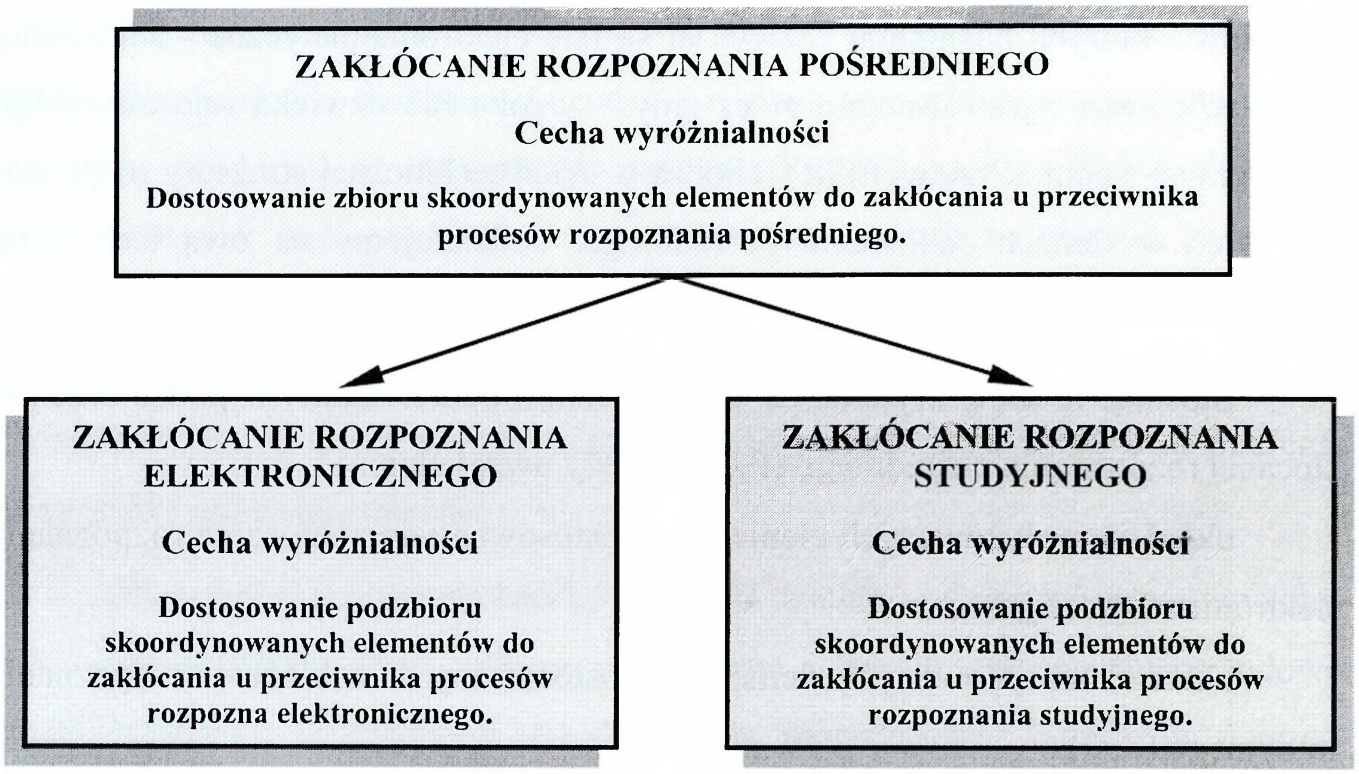
Graficzny obraz tego podziału ilustruje rysunek 2.7.



Rys. 2.7. Podział zakłócania rozpoznania pośredniego

W aspekcie powyższego, podstawową strukturę zakłócania rozpoznania pośredniego i jego cechy wyróżnialności można przedstawić jak na rysunku 2.8.

Badania struktury zakłócania pośredniego toru zdobywania danych przeciwnika wykazały, że może być ono prowadzone różnymi sposobami i przy wykorzystywaniu różnych narzędzi. Ich działanie determinowane jest dążeniem do osiągnięcia stanu, który pozwoli na dostarczeniu wojskom wiernego i aktualnego obrazu pola walki oraz prawdopodobnych przyszłych zachowań strony przeciwnej, oczywiście bez jego wiedzy o inwigilacji.



Rys. 2.8. Podstawowa struktura i cechy wyróżnialności zakłócania pośredniego

To ostatnie kryterium najbardziej spełniają systemy i wchodzące w ich skład urządzenia rozpoznania elektronicznego.

2.1.2.1. Zakłócanie rozpoznania elektronicznego

Rozpoznanie elektroniczne jest jednym z elementów składowych rozpoznania, które ma na celu zdobywanie i przetwarzanie tych danych o przeciwniku, których nośnikami są fale elektromagnetyczne oraz inne efekty uboczne towarzyszące działaniom bojowym. Prowadzi się je w każdych warunkach atmosferycznych bez względu na porę roku i doby. Jest to najszybszy, najtańszy, najbardziej manewrowy i skryty rodzaj rozpoznania.

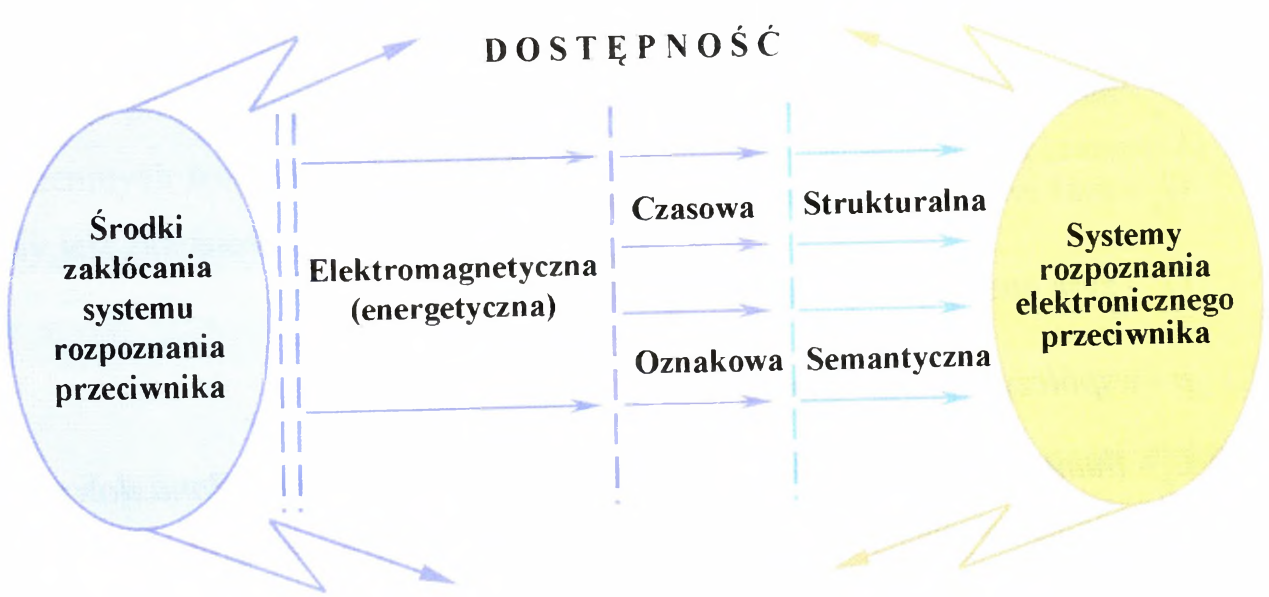
Planując i organizując jego zakłócanie, należy przede wszystkim uwzględnić i wykorzystać mankamenty rozpoznania elektronicznego, do których zalicza się podatność na zakłócenie, dezinformowanie i niszczenie.

Na szczeblu operacyjnym, ogólnie rozumiane zakłócanie rozpoznania elektronicznego powinno obejmować:

- zakłócanie rozpoznania radioelektronicznego;
- zakłócanie rozpoznania radiolokacyjnego;
- zakłócanie rozpoznania optoelektronicznego;
- zakłócanie rozpoznania czujnikowego;
- zakłócanie rozpoznania informatycznego.

Chcąc objąć zakłócaniem wymienione rodzaje zakłócania elektronicznego, muszą być spełnione wszystkie warunki dostępności, które wymagają oddzielnego omówienia.

Jak podkreślono w poprzednim akapicie, proces zakłócania uzależniony jest od **dostępności** do systemów rozpoznania elektronicznego przeciwnika. Owe czynniki, od których dostępność jest uzależniona, przedstawione są na rysunku 2.9.



Rys. 2.9. Dostępność systemów rozpoznania elektronicznego przeciwnika

Dostępność elektromagnetyczna (energetyczna), przy klasycznych modulacjach wąskopasmowych uzależniona jest od stosunku sygnału zakłócającego do poziomu sygnału użytecznego na wejściu urządzenia rozpoznawczego, tzn. poziom

sygnału zakłócającego zawsze powinien być wyższy od poziomu sygnału użytecznego.

Z badań wynika, że głębokość strefy dostępności elektromagnetycznej zależy od parametrów równania przepływu mocy w umownym łączu radiowym utworzonym przez nadajnik wojsk własnych i odbiornik rozpoznawczy przeciwnika. Równanie to, uwzględniając najczęściej wykorzystywane rodzaje propagacji fal elektromagnetycznych w operacjach wojsk lądowych można przedstawić w dwóch postaciach:

1. Przy propagacji fali przyziemnej typu ogólnego wykorzystywanej przy zakłócaniu urządzeń rozpoznania elektronicznego, poziom sygnału zakłócającego można obliczyć wzorem:

$$P_o = \frac{P_n G_n G_o}{p\ L_b}$$

gdzie:

P_o - *moc sygnału zakłócającego na wejściu odbiornika urządzenia rozpoznawczego;*

P_n - *moc nadajnika zakłócającego przekazywana do anteny;*

G_n - *zysk energetyczny anteny nadawczej;*

G_o - *zysk energetyczny anteny odbiorczej;*

p - *współczynnik ochronny emisji;*

L_b - *tłumienność trasy propagacji fali między antenami określona ilorazem:*

$$L_b = \frac{R^4}{h_1^2\ h_2^2}$$

gdzie:

R [km] — odległość między antenami nadajnika i odbiornika;

h_1 *[m] — wzniesienie anteny nadawczej wyrażone zależnością:*

$$h_1 = \sqrt{h_n^2 + h_m^2}$$

h_2 [m] — wzniesienie anteny odbiorczej wyrażone zależnością:

$$h_2 = \sqrt{h_o^2 + h_m^2}$$

gdzie:

h_n, h_o [m] — wysokość wyniesienia anteny nadawczej (odbiorczej) nad ziemią,

h_m (ε, ∂, λ) [m] — wyniesienie pozorne anteny przy danej polaryzacji:

$$h_m = \frac{\lambda}{2\pi}\left[(\varepsilon \pm 1)^2 + (60\lambda\partial)^2\right]^{\pm 1/4}[m]$$

gdzie:

„+" — dla polaryzacji poziomej;

„-" — dla polaryzacji pionowej;

ε, ∂ — przenikliwość elektryczna i konduktywność gruntu na trasie radiowej.

2. Przy propagacji przestrzennej wykorzystywanej do zakłócania powietrznych i naziemnych środków rozpoznania elektronicznego, w równaniu parametr L_b określany jest zależnością:

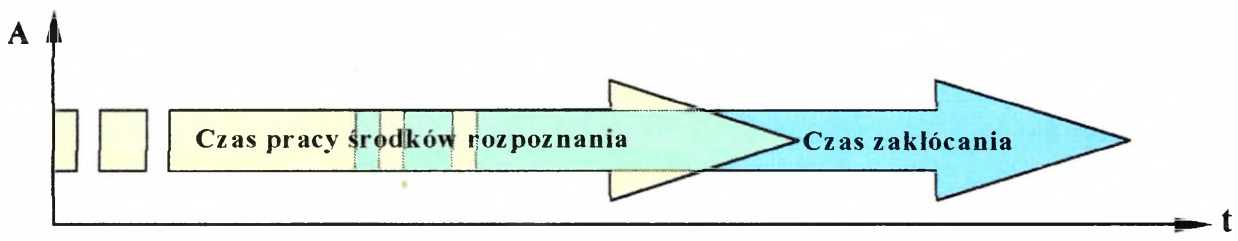
$$L_b = \frac{R^4}{h_n^2 h_o^2}$$

Z powyższych równań wynika, że głębokość strefy dostępności elektromagnetycznej zależy zarówno od mocy nadajnika zakłócającego, wartości zakłócanego sygnału użytecznego, wysokości wyniesienia własnej anteny nadawczej i anteny urządzenia rozpoznawczego przeciwnika, jak również od częstotliwości pracy, polaryzacji fali, rodzaju modulacji, warunków propagacji oraz właściwości dielektrycznych gruntu pomiędzy nadajnikiem i odbiornikiem. Owe parametry, (z wyjątkiem tych, które dotyczą urządzeń rozpoznawczych przeciwnika), powinny być

uwzględniane w trakcie planowania i realizacji przedsięwzięć zakłócania systemów elektronicznych przeciwnika.

Dostępność czasowa jest drugim elementem wyróżnionym na schemacie dostępności (rysunek 2.9.). Jest ona uzależniona od czasu i intensywności pracy urządzeń rozpoznawczych przeciwnika oraz czasu ich zakłócania. Warunkiem koniecznym i niezbędnym efektywnego zakłócania jest zazębianie się owych czasów. Zatem dostępność czasowa jest wprost proporcjonalna do długości okresu zazębiania tych dwóch czasów.

Na rysunku 2.10. wspólny obszar (kolor zielony) wyznacza okresy dostępności czasowej środków rozpoznania elektronicznego przeciwnika dla zakłócania.



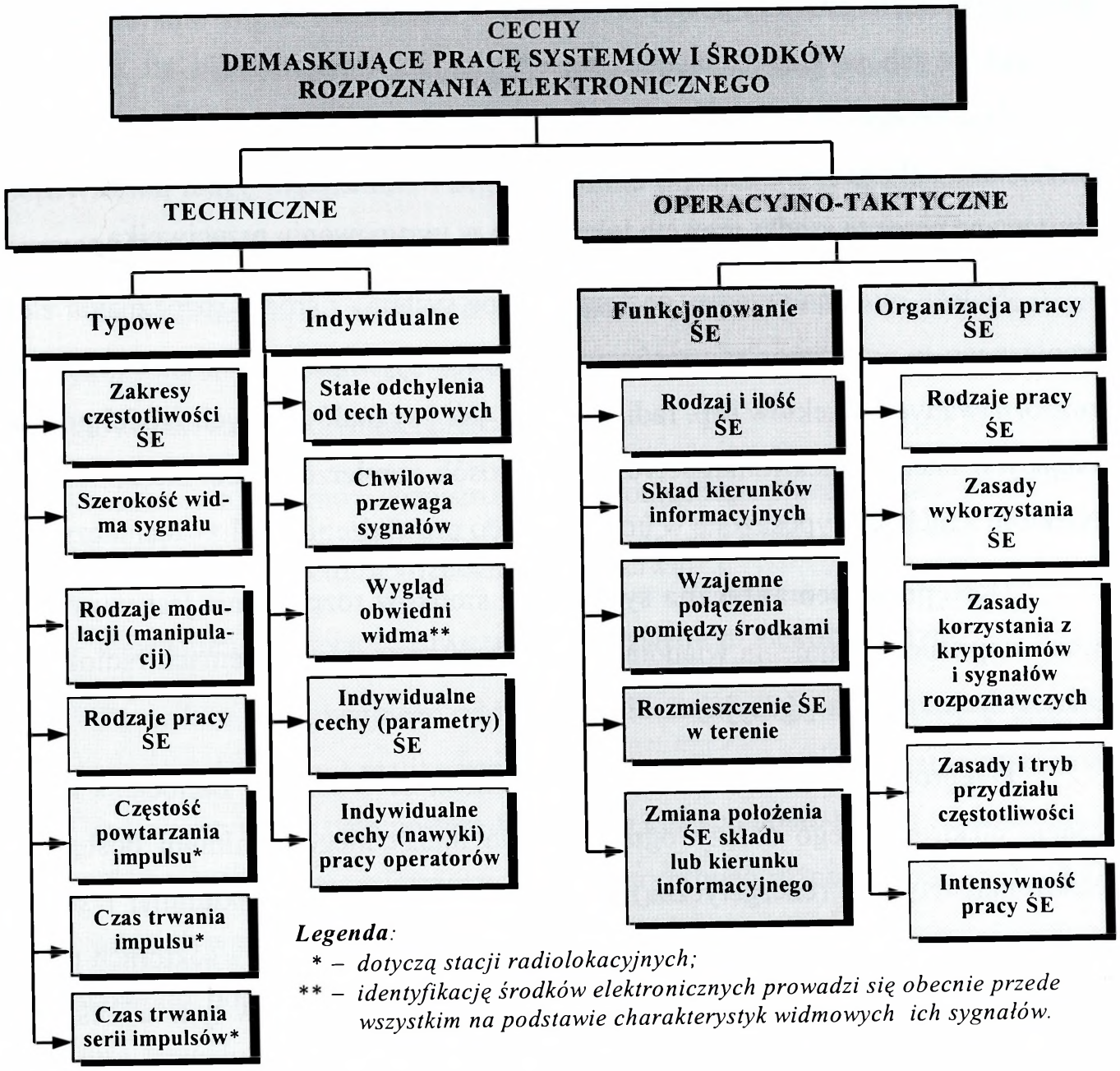
Rys. 2.10. Dostępność czasowa środków rozpoznania elektronicznego dla zakłócania

Dostępność oznakowa i strukturalna uwarunkowana jest istnieniem cech (oznak, właściwości) demaskujących pracę środków rozpoznania elektronicznego przeciwnika (ŚE). Podział tych cech przedstawiono na rysunku 2.11.

Techniczne (informacyjne) cechy rozpoznawcze dotyczą urządzeń elektronicznych, które promieniują energię elektromagnetyczną. Wynikają one ze sposobów i rodzajów pracy tych urządzeń, które pozwalają na ich rozróżnianie. Owe cechy można podzielić na typowe i indywidualne.

Typowe techniczne cechy to wielkości, które umożliwiają określenie charakterystyk elektronicznego środka rozpoznawczego i przyporządkowują go do określonej klasy lub grupy urządzeń.

Indywidualne techniczne cechy to wielkości, według których można określić przynależność elektronicznego środka do rodzaju sił zbrojnych, związku operacyjnego lub taktycznego oraz wyróżnić go spośród innych tego typu urządzeń.



Rys. 2.11 Podział cech demaskujących pracę środków rozpoznania elektronicznego

Operacyjno-taktyczne cechy rozpoznawcze to takie charakterystyki, według których określa się zasady organizacji i wykorzystania środków elektronicznych w systemach rozpoznania bądź kierowania uzbrojeniem. Powyższe cechy pozwalają określić skład bojowy i ugrupowanie systemu oraz określić jego funkcje, sposoby użycia i zagrożenie z jego strony. Można je podzielić na dwie grupy:

1. Cechy określające sposób organizacji i funkcjonowania systemów;
2. Cechy określające sposoby ich pracy.

Zaprezentowany podział cech, demaskujących pracę elektronicznych środków rozpoznania pozwala postawić tezę, że wynikają one z określonego sposobu i warunków ich wykorzystania, przynależności do kraju, rodzaju sił zbrojnych, szczebla dowodzenia i sposobów pracy w systemach rozpoznania, dowodzenia lub kierowania uzbrojeniem. Pierwotnym źródłem tych wszystkich danych, są sygnały emitowane przez te środki oraz ich lokalizacja w ugrupowaniu przeciwnika.

Należy mieć na uwadze, że współczesne systemy i środki rozpoznania elektronicznego są przystosowane zarówno do odbioru własnych sygnałów odbitych od rozpoznawanych obiektów (np. radiolokacja), jak i sygnałów innych źródeł promieniujących energię elektromagnetyczną w sposób zamierzony lub niezamierzony. Niektóre z nich są wyposażone w urządzenia do prowadzenia analizy technicznej.

Dostępność semantyczna systemów i środków rozpoznania jest uwarunkowana stopieniem utajnienia wiadomości przekazywanych w systemach radiokomunikacyjnych, radionawigacyjnych i innych.

Przeprowadzone badania dowodzą również, że w ramach zakłócania rozpoznania elektronicznego należy ograniczyć do niezbędnego minimum dostępność elektromagnetyczną (energetyczną), czasową, oznakowaną, strukturalną i semantyczną własnych środków i urządzeń elektronicznych w strefach i sektorach niepożądanych, tzn. poza przedni skraj obrony wojsk. Istota działań w tym zakresie powinna polegać na szeroko rozumianym ukrywaniu i maskowaniu urządzeń promieniujących energię elektromagnetyczną, a także na ochronie treści danych zawartych w tej energii (emitowanych sygnałach). Realizacja owych przedsięwzięć, powinna być działaniem pierwszoplanowym organizatorów systemów elektronicznych oraz bezpośrednich użytkowników urządzeń.

Zakres i sposób realizacji tych przedsięwzięć w wojskach lądowych należy warunkować okresami: pokoju, kryzysu, wojny.

W okresie pokoju i kryzysu zakłócanie rozpoznania elektronicznego w wojskach lądowych powinno polegać na przestrzeganiu zasad wykorzystania urządzeń elektronicznych określonych instrukcjami eksploatacyjnymi oraz przepi-

sami o ochronie informacji niejawnych[18]. Szczególna uwaga powinna być zwrócona na maskowanie wojsk i obiektów elektronicznych, eliminowanie ich cech demaskujących, wykorzystanie maskujących właściwości terenu, warunków atmosferycznych, etatowych i podręcznych środków maskowania itp. Należy również nadać odpowiednią rangę planowaniu i organizowaniu przedsięwzięć zakłócania elektronicznego oraz szkoleniu sztabów i wojsk w tym zakresie.

W okresie wojny zakłócanie rozpoznania elektronicznego powinno polegać na wykonywaniu przedsięwzięć zawartych w uprzednio opracowanych planach. Do jego głównych zadań powinno należeć:

- niszczenie systemów rozpoznania elektronicznego przeciwnika;
- zagłuszanie systemów rozpoznania przeciwnika;
- zapewnienie bezpieczeństwa własnym systemom elektronicznym.

Procedura destrukcyjnego oddziaływania na tor zdobywania danych (system rozpoznania pośredniego) realizowana jest z zamysłem uniemożliwiania przeciwnikowi wykorzystywania tych postaci danych, do których udało się mu zdobyć dostęp mimo stosowania obrony informacyjnej. Wykorzystując różne techniki energetycznego oddziaływania można niszczyć i czasowo uniemożliwiać pracę systemów i środków do odbioru sygnałów i przetwarzania danych. Można także zmieniać strukturę sygnałów bądź ich nośników, niszcząc tym samym lub zniekształcając zawarty w nich potencjał informacyjny. Innymi słowy, tak jeden, jak i drugi sposób działania zwiększa w torze pośredniego zdobywania danych stan nieuporządkowania wiedzy o przeciwniku, to znaczy zwiększa tym samym entropię informacyjną.

W zakłócaniu elektronicznym, najbardziej zróżnicowane pod względem technicznym, jest zakłócanie rozpoznania radioelektronicznego.

---

[18] „Ustawa o ochronie informacji niejawnych" z dnia 22.01.2000. Dz.U. nr 11, poz. 95, 2000.

2.1.2.1.1. Zakłócanie rozpoznania radioelektronicznego

Zakłócanie rozpoznania radioelektronicznego ma uniemożliwiać bądź utrudniać zdobywanie i przetwarzanie danych o środkach własnych wojsk, promieniujących energię elektromagnetyczną w postaci sygnałów oraz informacje zawarte w tych sygnałach, w całym widmie elektromagnetycznym, od dolnej granicy zakresu radiowego, do górnej granicy zakresu mikrofalowego. Wykorzystując różne techniki energetycznego oddziaływania, można niszczyć lub czasowo uniemożliwiać pracę środkom rozpoznania elektronicznego, przetwornikom danych i sygnałów oraz układom odbierającym. Można także zmieniać strukturę nośników danych i nośników sygnałów, niszcząc tym samym lub zniekształcając zawarty w nich potencjał informacyjny. Zakłócanie rozpoznania radioelektronicznego, może stanowić jeden z ważniejszych elementów zakłócania informacyjnego przeciwnika, bowiem zwiększa w torze zdobywania danych stan nieuporządkowania jego wiedzy o stronie przeciwnej, to znaczy, zwiększa u niego entropię informacyjną. W operacjach wojsk lądowych, zakłócanie elektroniczne należałoby prowadzić za pomocą urządzeń, zainstalowanych na pojazdach i aparatach latających.

Wspomniane zróżnicowanie procesu zakłócenia radioelektronicznego wynika z tego, że należy nim objąć wszystkie środki przeciwnika, które są wykorzystywane do prowadzenia:

- rozpoznania radiowego, radioliniowego i satelitarnego;
- rozpoznania środków radiolokacyjnych;
- rozpoznania radionawigacyjnego.

Zakłócanie rozpoznania radiowego jest procesem, który uniemożliwi bądź utrudni przeciwnikowi zdobywanie danych o stanie ilościowym i jakościowym środków łączności radiowej, radioliniowej i satelitarnej wojsk operacyjnych, miejscu ich rozmieszczenia i sposobach wykorzystania.

Przyjmując za kryterium zakres częstotliwości, możemy wyróżnić zakłócanie rozpoznania krótkofalowego (KF) i ultrakrótkofalowego (UKF), jednak ze względu

na wprowadzanie do wojsk szerokopasmowych urządzeń radioodbiorczych, taki podział rozpoznania radiowego zanika.

W rozpoznaniu radiowym można wyróżnić takie metody zdobywania danych jak:

- poszukiwanie;
- namierzanie;
- przechwytywanie;
- śledzenie aktywności źródeł;
- analiza techniczno – operacyjna sygnałów i ich źródeł.

Zakłócanie poszukiwania zdaniem zespołu badawczego, jest podstawowym procesem, który ma na celu utrudnienie wykrycia i identyfikacji sygnałów wypromieniowanych przez środki radiowe i wyselekcjonowanie tych, którymi prowadzący rozpoznanie jest zainteresowany. Dlatego też, zakłócanie tego procesu jest niezwykle istotne.

Prowadząc zakłócanie poszukiwania, muszą być spełnione następujące warunki:

1. czasowo-przestrzenny – tzn. w tym samym czasie powinno nastąpić spotkanie charakterystyk antenowych nadajnika zakłóceń i odbiornika urządzenia rozpoznawczego;

2. energetyczny – tzn. moc sygnału zakłócającego Pz_{we} na wejściu urządzenia rozpoznawczego musi być nie mniejsza od mocy sygnału użytecznego Ps_{we}:

$$Pz_{we} \geq Ps_{we}$$

3. częstotliwościowy – tzn. nadajnik zakłócający musi być dostrojony do częstotliwości pracy odbiornika urządzenia rozpoznawczego z odpowiednią dokładnością:

$$fo - \frac{\Delta f}{2} \leq fz \leq fo + \frac{\Delta f}{2}$$

gdzie:

fo – częstotliwość pracy odbiornika urządzenia rozpoznawczego;

Δf – szerokość pasma przepuszczania odbiornika;

fz – częstotliwość nadajnika zakłócającego.

Zakłócanie urządzeń rozpoznania radiowego można prowadzić w częstotliwości, kierunku lub równocześnie w częstotliwości i kierunku.

Zakłócanie w częstotliwości polega na przestrajaniu nadajnika zakłócającego w całym jego zakresie lub określonym podzakresie i ustaleniu tych częstotliwości, na których występują sygnały, które zamierzamy zakłócać. Jedną z form zakłócania w częstotliwości jest jednoczesne nadawanie sygnałów zakłócających na kilku częstotliwościach, przy użyciu nadajników wielokanałowych. Te ostatnie są szczególnie przydatne przy zakłócaniu emisji rozproszonych np. typu FH. Nowoczesne urządzenia zakłócające, prawdopodobnie są w stanie generować sygnały w paśmie 12 MHz, pokrywając cały podzakres hoppingu przy modulacji typu FH (±6 MHz). Te nowoczesne urządzenia zakłócające, są prawdopodobnie wyposażone w anteny o charakterystyce kierunkowej lub sektorowej, by nie zakłócać własnych środków pracujących w zakłócanym paśmie częstotliwości.

Zakłócanie w kierunku (sektorze, azymucie) polega na generowaniu sygnałów zakłócających tylko w jednym, określonym kierunku (azymucie). Zmiany azymutu dokonuje się położeniem całego urządzenia zakłócającego lub samej anteny. Jednym ze sposobów jest zakłócanie w jednym lub kilku sektorach, które polega na jednoczesnym generowaniu zakłóceń przez kilka anten kierunkowych.

Namierzanie źródła sygnału, jest kolejnym istotnym elementem procesu rozpoznania radioelektronicznego.

Zakłócanie namierzania jest procesem, który uniemożliwi bądź utrudni przeciwnikowi lokalizację źródeł promieniowania elektromagnetycznego. Prowadzi się je w podobny sposób, jak zakłócanie innych urządzeń rozpoznawczych wyposażonych w system kierowania. Zasadnicza różnica polega na konieczności zakłócania

kilku, (co najmniej dwóch) urządzeń najczęściej rozmieszczonych w znacznej od siebie odległości.

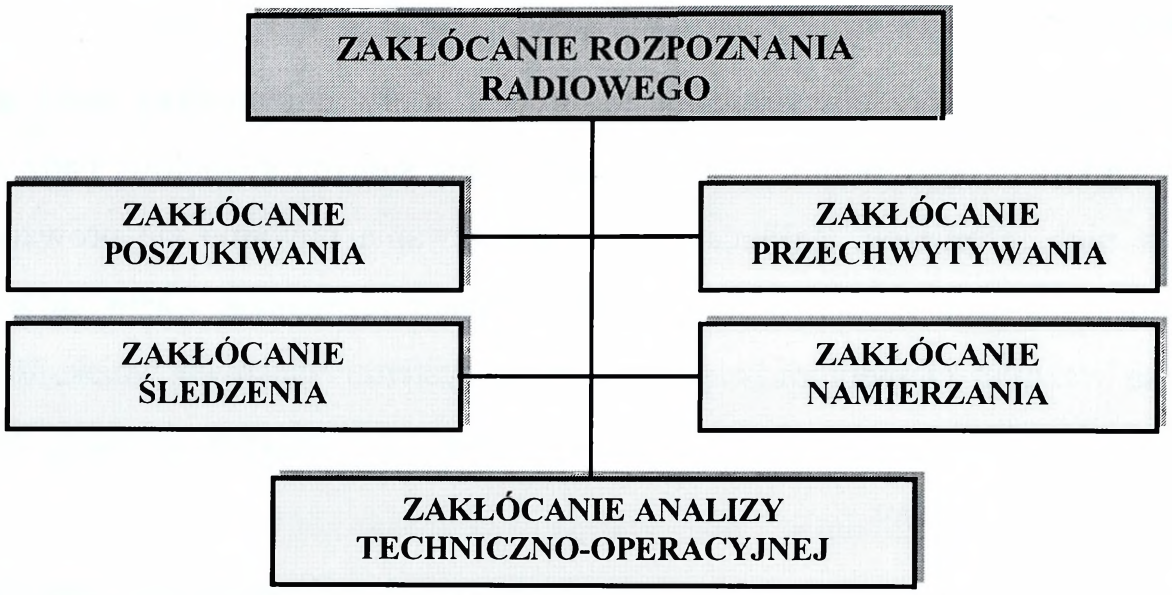
Zakłócanie przechwytywania to proces, który uniemożliwi bądź utrudni przeciwnikowi ciągły odbiór i rejestrowanie bądź samych sygnałów, bądź zawartych w nich informacji. Zakłócanie przechwytywania powinno się prowadzić na częstotliwości tych źródeł, które w danej sytuacji przekazują ważne informacje, bądź są ważnym elementem rozpoznawanego systemu własnych wojsk. Również w tym przypadku, charakterystyki anten urządzeń zakłócających powinny być kierunkowe lub sektorowe.

Zakłócanie śledzenia polega na okresowym dostrajaniu się do częstotliwości pracy rozpoznawanych źródeł i generowaniu na tej częstotliwości energii zakłócającej w kierunku lub sektorze rozmieszczenia urządzeń rozpoznawczych przeciwnika. W związku z tym, że śledzeniu podlegają źródła, których sygnały mają małą wartość informacyjną, przy dostatecznej ilości środków zakłócających można je prowadzić jako element mylenia.

Zakłócanie analizy techniczno-operacyjnej jest procesem zmierzającym do uniemożliwienia bądź utrudnienia przeciwnikowi określenia charakterystycznych cech sygnałów i ich źródeł, które wyróżniają je spośród innych. Dotyczy to sygnałów i obiektów prawdopodobnie znanych przeciwnikowi jak i nowo wprowadzanych. Proces ten, przy kolejnych przypadkach ich wykrycia, uniemożliwi bądź utrudni przeciwnikowi ich identyfikację.

W procesie zakłócania analizy techniczno-operacyjnej, również powinno się dążyć do utrudnienia przeciwnikowi logicznego uporządkowania informacji o rozpoznawanych obiektach, wprowadzając do jego zbiorów fałszywe dane. Owe dane, po przetworzeniu i opracowaniu tworzyć będą obrazy, sytuacje i zarysy rozwiązań koncepcyjnych, które z rzeczywistością nie mają nic wspólnego, względnie bardzo mało. Fałszywe dane mogą dotyczyć składu, rozmieszczenia, stanu ilościowo-jakościowego obiektów oraz sposobów działania czy zamiarów ich użytkowników.

Zaprezentowane elementy składowe procesu zakłócania rozpoznania radiowego ilustruje rysunek 2.12.



Rys. 2.12. Procesy w rozpoznaniu radiowym podlegające zakłócaniu

Przyjmując jako kryterium klasyfikacji rodzaje rozpoznawanych środków radiowych, możemy z niego wydzielić rozpoznanie linii radiowych (radiolinii) i łączności satelitarnej.

Zakłócanie rozpoznania łączności radioliniowej[19], powinno przeciwdziałać bądź utrudniać przeciwnikowi zdobywanie danych dotyczących zarówno tych systemów i środków łączności, jak i logicznych treści przesyłanych w kanałach linii radiowych. Polega na wykrywaniu niepożądanych kierunków emisji sygnałów własnych radiolinii (tzw. listków bocznych) i ich eliminowaniu, bądź generowaniu na tych kierunkach sygnałów zakłócających. Ponieważ w kanałach radioliniowych można tworzyć łącza telefoniczne, telegraficzne, telewizyjne i transmisji danych, zakłócenia o podobnych strukturach sygnałów, mogą stanowić źródła fałszywych danych.

Środki zakłóceń rozpoznania łączności radioliniowej powinny być instalowane w specjalnych aparatowniach poruszających się po drogach rokadowych poszukując sygnałów, bądź na statkach powietrznych (pilotowych i bezpilotowych)

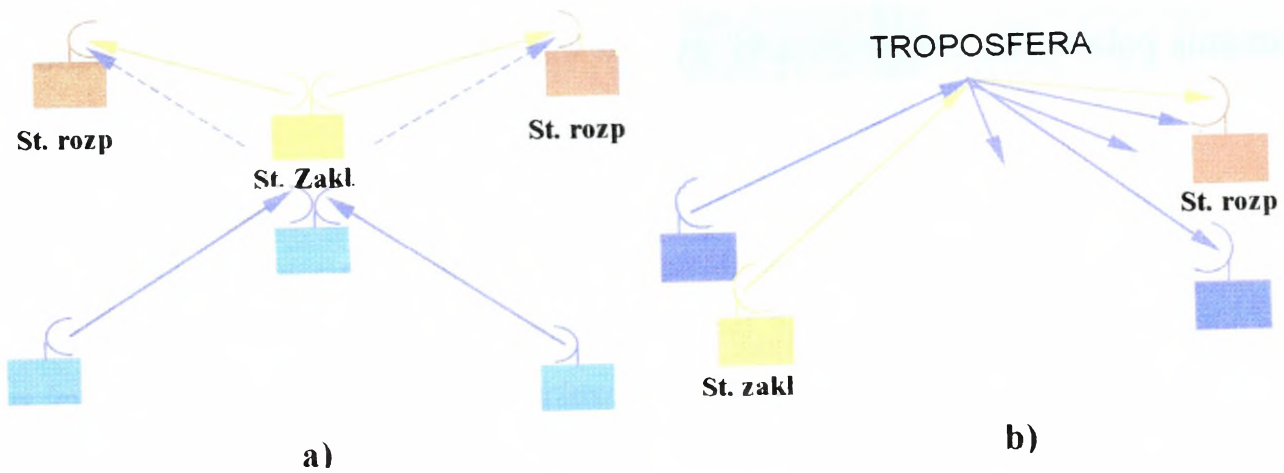
[19] Łączność radioliniowa, jeden z podstawowych elementów eksploatowanych obecnie systemów łączności, umożliwia tworzenie wielokanałowych magistrali wymiany danych, może więc stanowić ważne pod względem informacyjnym źródło rozpoznania.

latających w strefach dyżurowania nad własnym ugrupowaniem. W zakłócaniu rozpoznania radioliniowego należy uwzględnić zarówno środki **horyzontowe jak i pozahoryzontowe**.

Przy zakłócaniu rozpoznania łączności horyzontowej, anteny urządzenia rozpoznawczego i stacji zakłóceń muszą mieć zasięg optyczny (muszą się „widzieć").

W przypadku stacji zakłóceń rozpoznania łączności pozahoryzontowej, przy której wykorzystuje się rozproszenie wiązki na niejednorodnościach troposfery (stąd potoczna nazywa radiolinie troposferyczne), nie jest wymagany warunek widoczności, bowiem anteny urządzenia rozpoznawczego i stacji zakłóceń, mogą się znajdować w znacznej odległości od siebie (poza zasięgiem optycznym).

Ideę zakłócania urządzeń rozpoznania radioliniowego łączności horyzontowej i pozahoryzontowej ilustruje rysunek 2.13.



Rys. 2.13. Zakłócanie urządzeń rozpoznania łączności radioliniowej: a) horyzontowej, b) pozahoryzontowej

Zasięgi łączności w skali globalnej, mogą uzyskiwać abonenci systemów satelitarnych.

Zakłócanie rozpoznanie łączności satelitarnej w naszych wojskach lądowych jest przedsięwzięciem perspektywicznym. Wraz z rozwojem systemów łączności satelitarnej kształtował się nowy rodzaj rozpoznania radioelektronicznego – rozpoznanie łączności satelitarnej. Rozpoznanie łączności satelitarnej obejmuje

przedsięwzięcia prowadzące do zdobywania danych dotyczących środków i systemów łączności wykorzystujących sztuczne satelity Ziemi. Polega na wykrywaniu sygnałów przekazywanych z satelity, ich przechwytywaniu i analizowaniu.

W operacjach wojsk lądowych zarówno obecnie, jak i w najbliższej przyszłości, prawdopodobnie nie będzie wykorzystywana łączność satelitarna, problematyka zakłócania urządzeń przeznaczonych do jej rozpoznania, nie będzie rozpatrywana w tej pracy badawczej.

Zakłócanie rozpoznania systemów radiolokacyjnych[20] powinno uniemożliwiać bądź utrudniać przeciwnikowi zdobywanie danych dotyczących systemów i środków radiolokacyjnych rozpoznania pola walki, artylerii, obrony powietrznej i przeciwlotniczej własnych wojsk. Oprócz ukrywania technicznych cech urządzeń radiolokacyjnych, zakłóceniami można również osłaniać radiolokacyjnie obiekty ugrupowania operacyjnego takie jak: zgrupowania operacyjne wojsk, stanowiska dowodzenia i kierowania, stanowiska startowe i ogniowe artylerii, posterunki rozpoznania pola walki, czy posterunki wykrywania i zwalczania środków napadu powietrznego.

W procesie zakłócania środków rozpoznania radiolokacyjnego niezwykle trudne jest ich poszukiwanie i wykrywanie, bowiem są one urządzeniami pasywnymi, które nie emitują energii elektromagnetycznej. W tych systemach, aktywne są jedynie ich urządzenia sterujące i wymiany danych, których należy poszukiwać. Aby więc wykryć pracujący system rozpoznania radiolokacyjnego, muszą być spełnione podobne warunki jak w przypadku poszukiwania środków radiowych, tzn. energetyczny, częstotliwościowy, przestrzenny oraz czasowy, które zostały omówione w podrozdziale dotyczącym zakłócania rozpoznania radiowego. Zakłóceniami możemy więc objąć te stacje rozpoznania radiolokacyjnego, których aktywne systemy sterowania i wymiany danych zostały wykryte. Oznaczając przez:

- *N – zbiór poszukiwanych stacji rozpoznania radiolokacyjnego;*
- *Na – zdarzenie polegające na wykryciu stacji „w kierunku”;*

---

[20] Rozpoznanie systemów radiolokacyjnych jest drugą częścią składową rozpoznania radioelektronicznego, w którym przedmiotem rozpoznania są pracujące systemy i środki radiolokacyjne. System radiolokacyjny – to zespół sił i środków przeznaczony do prowadzenia rozpoznania radiolokacyjnego i radiolokacyjnego zabezpieczenia działań bojowych.

- *Nb – zdarzenie polegające na wykryciu stacji „w częstotliwości”;*
- *Nab – zdarzenie polegające na wykryciu stacji „w kierunku” i „w częstotliwości”,*

zależności zachodzące pomiędzy zbiorami: N, N_a, N_b, N_{ab} wyrażają się następująco:

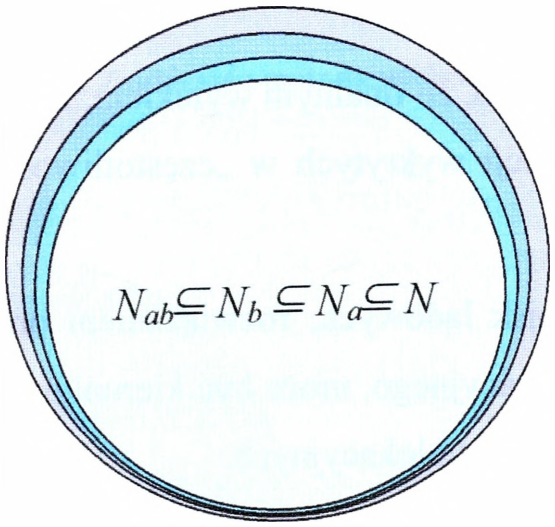
a) przy poszukiwaniu i wykrywaniu pewnym:

$$N = N_a = N_b = N_{ab}$$

ponieważ:

$$N_{ab} \subseteq N_b \subseteq N_a \subseteq N$$

Co geometrycznie interpretuje się jak na rysunku 2.14.



Rys. 2.14. Interpretacja geometryczna zbiorów „pewnego” wykrycia stacji rozpoznania radiolokacyjnego

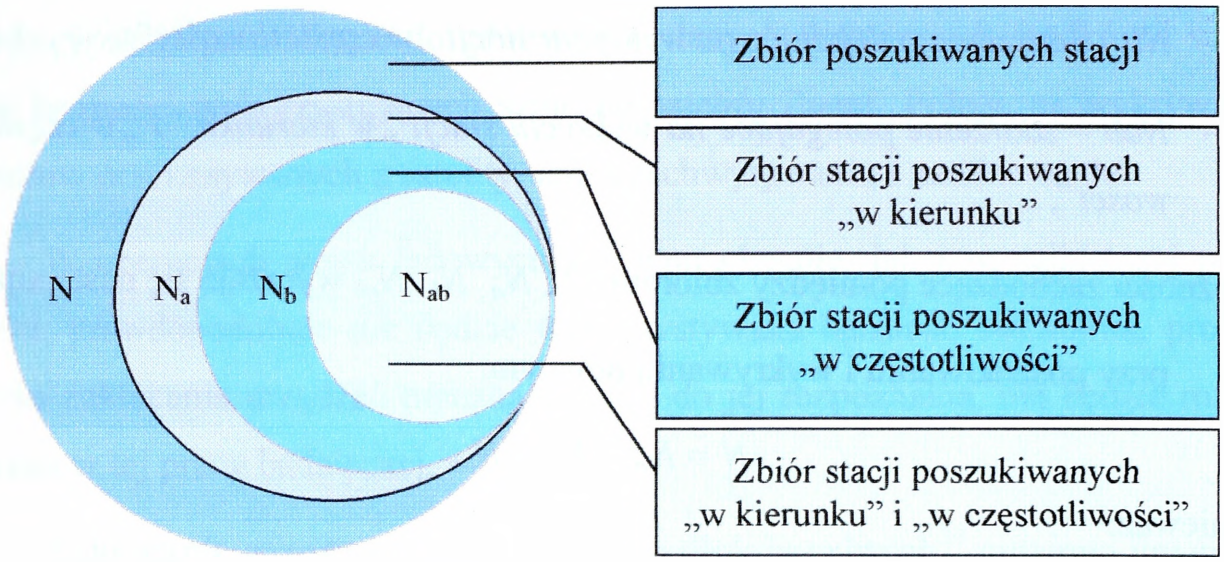
b) przy poszukiwaniu i wykrywaniu prawdopodobnym:

$$N \geq N_a \geq N_b \geq N_{ab}$$

ponieważ:

$$N_{ab} \subset N_b \subset N_a \subset N$$

Co geometrycznie interpretuje rysunek 2.15.



Rys. 2.15. Interpretacja geometryczna zbiorów prawdopodobnego wykrycia stacji rozpoznania radiolokacyjnego

Z powyższego wynika, że finalnym wynikiem, tak w pierwszym jak i drugim przypadku, jest zbiór stacji wykrytych w „częstotliwości" i w „kierunku", czyli zbiór „N_{ab}".

W operacjach wojsk lądowych, rozwiązaniem problemu zakłócania systemów rozpoznania radiolokacyjnego, może być kierunkowe (sektorowe) lub dookólne zakłócanie całych pasm radiolokacyjnych.

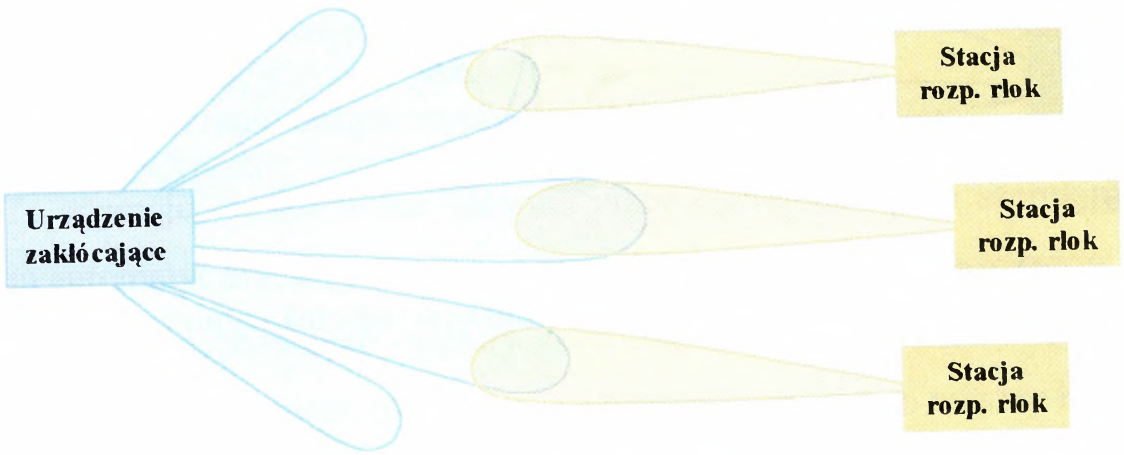
Kierunkowe zakłócanie stacji rozpoznania radiolokacyjnego może być prowadzone metodą z uprzednim poszukiwaniem zakłócanych stacji, lub metodą bez ich poszukiwania, tzw. zakłócanie natychmiastowe.

Zakłócanie bez poszukiwania stacji może być również prowadzone metodą dookólną z wykorzystaniem anteny o charakterystyce kołowej, wiąże się to jednak z ryzykiem zakłócania własnych systemów radiolokacyjnych.

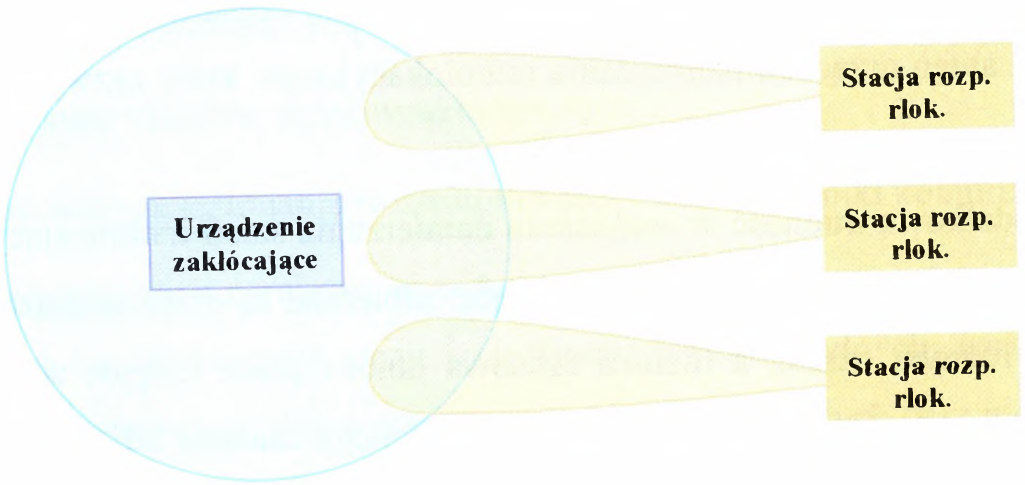
Pierwszą metodę zakłócania w kilku sektorach ilustruje rysunek 2.16, zaś drugą rysunek 2.17.

Do zakłócania wielosektorowego wykorzystuje się kilka anten kierunkowych lub jedną antenę z tzw. szykiem fazowym. W antenach tego typu, są wykorzystywane dyskryminatory fazy, które pozwalają na szybkie i precyzyjne zmiany cha-

rakterystyki anteny. Ta technika umożliwia emisję dowolnego kształtu wiązki sygnału zakłócającego, w dowolnym kierunku lub sektorze.

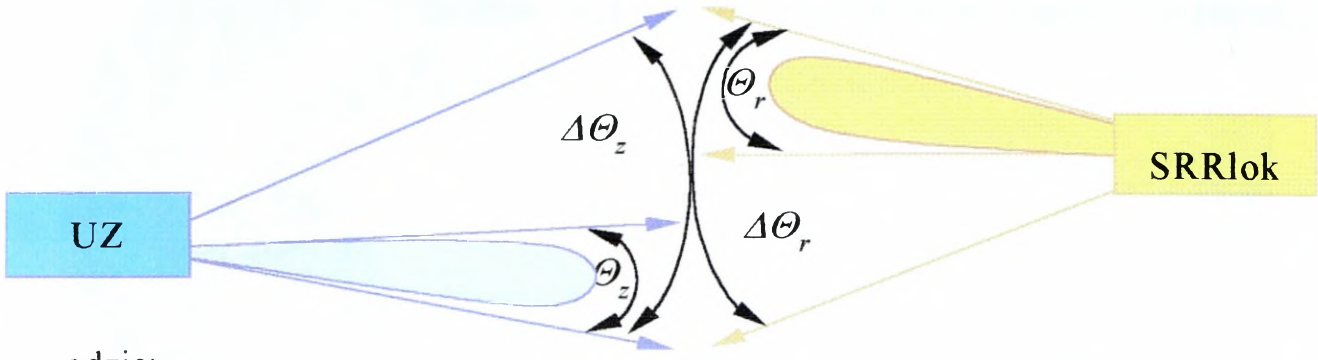


Rys. 2.16. Zakłócanie metodą wielosektorową



Rys. 2.17. Zakłócanie metodą dookólną

W przypadku zakłócania sektorowego należy pamiętać, że anteny urządzeń rozpoznawczych, rzadko obracają się ze stałą prędkością w płaszczyźnie poziomej. Znacznie częściej poruszają się w pewnym określonym zakresie. Z tego faktu wynika dodatkowy warunek zakłócenia polegający na tym, że sektor obserwacji urządzenia rozpoznawanego musi się przynajmniej w części pokrywać (zazębiać) z sektorem urządzenia zakłócającego jak na rysunek 2.18.



gdzie:

- $\Delta\Theta_z$ - sektor zakłócania;
- $\Delta\Theta_r$ - sektor obserwacji stacji rozpoznania radiolokacyjnego

Rys.2.18. Ilustracja warunku „zazębiania się" sektorów urządzenia zakłócającego i stacji rozpoznania radiolokacyjnego

Zakłócanie namierzania w rozpoznaniu systemów radiolokacyjnych realizuje się w podobny sposób jak w przypadku zakłócania rozpoznania radiowego. Pewna specyfika wiąże się jedynie z odmiennymi zakresami częstotliwości oraz charakterystykami anten urządzeń namierzania radiolokacyjnego, które zazwyczaj są sektorowe.

Dodatkową trudność w zakłócaniu namierzania stacji z obracającymi się antenami stanowi fakt, że sygnały zakłócające odbierane są przez urządzenia namierzania w różnym czasie, a różnica czasowa obioru przez kolejne stacje systemu uzależniona jest od szybkości obrotów anteny i sięga czasami kilku sekund. Powoduje to dodatkowe trudności w jednoczesnym zakłóceniu wszystkich namierników systemu.

Zakłócanie analizy techniczno–operacyjnej powinno uniemożliwiać bądź utrudniać przeciwnikowi identyfikację sygnałów, typu, rodzaju i egzemplarza rozpoznawanego urządzenia radiolokacyjnego. Proces zakłócania powinien obejmować zarówno etap zbierania danych o sygnałach i źródłach rozpoznania, jak i zbiory danych zgromadzonych w „bankach danych".

Rozpoznanie rodzaju urządzenia i określenie jego charakterystycznych cech, jest zazwyczaj prowadzone na podstawie analizy sygnałów, które zostały wypro-

mieniowane przez te urządzenia. Owa analiza obejmuje szereg kolejnych operacji, z których najważniejsze to:

- rejestracja sygnału;
- pomiar parametrów sygnału;
- przetworzenie otrzymanych danych.

Te operacje, wykonywane głównie przez operatorów przy szerokim wykorzystaniu automatycznych i półautomatycznych analizatorów i rejestratorów widma, można zakłócać pozbawiając sygnały cech indywidualnych. Parametry stacji radiolokacyjnych, które można określić na podstawie sygnałów to między innymi:

- typ i przeznaczenie stacji;
- stosowane rodzaje pracy i ich tory nadawcze;
- sposoby przeszukiwania przestrzeni;
- liczbę i szerokości wiązek promieniujących w azymucie i elewacji;
- rodzaje układów przeciwzakłóceniowych;
- sposoby przestrajania w częstotliwości i współczynniki kompresji.

Należy przy tym pamiętać, że jednym z podstawowych zadań prowadzonego w czasie pokoju rozpoznania stacji i systemów radiolokacyjnych, jest tworzenie aktualnych baz danych, w tym wzorców sygnałów rzeczywistych oraz metryk stacji radiolokacyjnych.

Tworzone bazy danych zawierają zarówno miejsce instalacji urządzeń, ich rodzaj i przeznaczenie, jak również lokalizację i przeznaczenie systemu, w którego składzie stacja pracuje. Na ich podstawie, w czasie zagrożenia i wojny można wyciągnąć wnioski o składzie, ugrupowaniu i zamiarach działania strony przeciwnej.

Zakłócanie rozpoznania systemów radionawigacyjnych polega na utrudnieniu bądź pozbawieniu przeciwnika możliwości wykrywania systemów i środków radionawigacyjnych wykorzystywanych przez stronę przeciwną.

Dokonując klasyfikacji systemów rozpoznania radionawigacyjnego[21] i ich zakłócania, wyróżnić można kilka kryteriów podziału. Owe kryteria to między innymi ich zasięg, dokładność i miejsce lokalizacji, zakresy wykorzystywanego widma częstotliwości czy cechy sygnałów.

Ze względu na zasięg naziemne systemy rozpoznania radionawigacyjnego dzielą się na systemy rozpoznania bliskiej i dalekiej nawigacji.

Zakłócanie systemów rozpoznania bliskiej nawigacji powinny obejmować środki rozpoznania radiotechnicznego, rozmieszczone na lądzie (aparatach latających, okrętach), których zasięg ograniczony do kilkuset kilometrów. Wykorzystywane podzakresy częstotliwości to fale krótkie i ultrakrótkie, które zapewniają stosunkowo precyzyjną lokalizację.

Zakłócanie systemów rozpoznania dalekiej nawigacji, powinno obejmować środki rozpoznania systemów radionawigacyjnych rozmieszczonych na lądzie (aparatach latających, okrętach), których zasięg jest rzędu od kilku do kilkunastu tysięcy kilometrów.

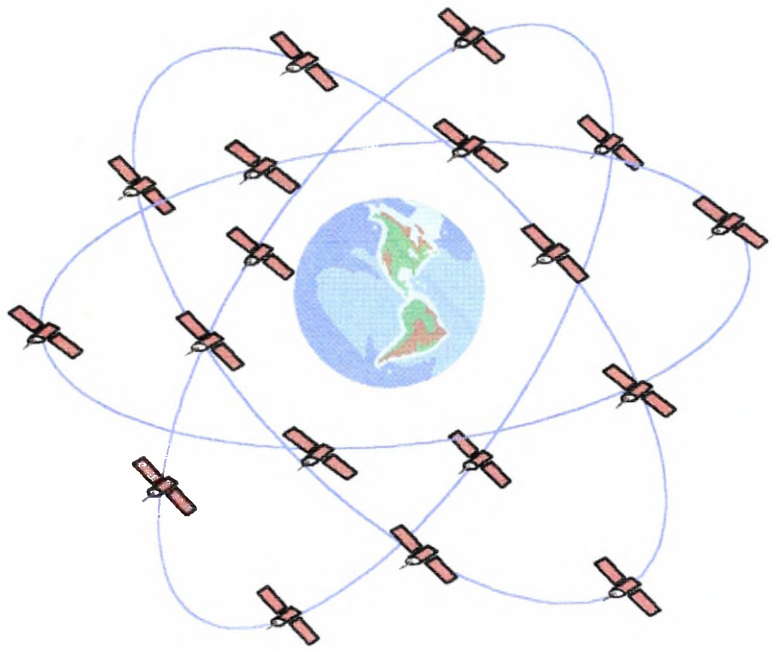
W naziemnych systemach dalekiej nawigacji, wykorzystywane są podzakresy fal średnich, długich i bardzo długich, które nie zapewniają tak dużej precyzji lokalizacji jak poprzednie.

Systemy zakłócania rozpoznania nawigacji, mogą także obejmować środki do prowadzenia rozpoznania systemu radionawigacyjnego zainstalowanego na sztucznych satelitach Ziemi (rysunek 2.19), która mimo znacznej odległości od satelitów (ok. 17.703 km) zapewnia precyzję lokalizacji rzędu od kilku do kilkunastu metrów.

Zatem możliwości prowadzenia zakłócania systemów rozpoznania radionawigacji bliższej i dalszej, są zdeterminowane rozmieszczeniem urządzeń rozpoznania tych systemów oraz zakresami częstotliwości, w których one pracują.

---

[21] System radionawigacyjny tworzy zespół specjalnych urządzeń współpracujących ze sobą lub autonomicznych, rozmieszczonych na ziemi i na obiektach ruchomych (samoloty, okręty, sztuczne satelity Ziemi), przeznaczonych do prowadzenia ruchomych obiektów po wyznaczonych trasach, ich naprowadzania na określone cele lub punkty terenowe oraz kontroli własnego położenia, dowiązywania stanowisk i obiektów itp.



Rys. 2.19. Wykorzystanie w radionawigacji sztucznych satelitów Ziemi

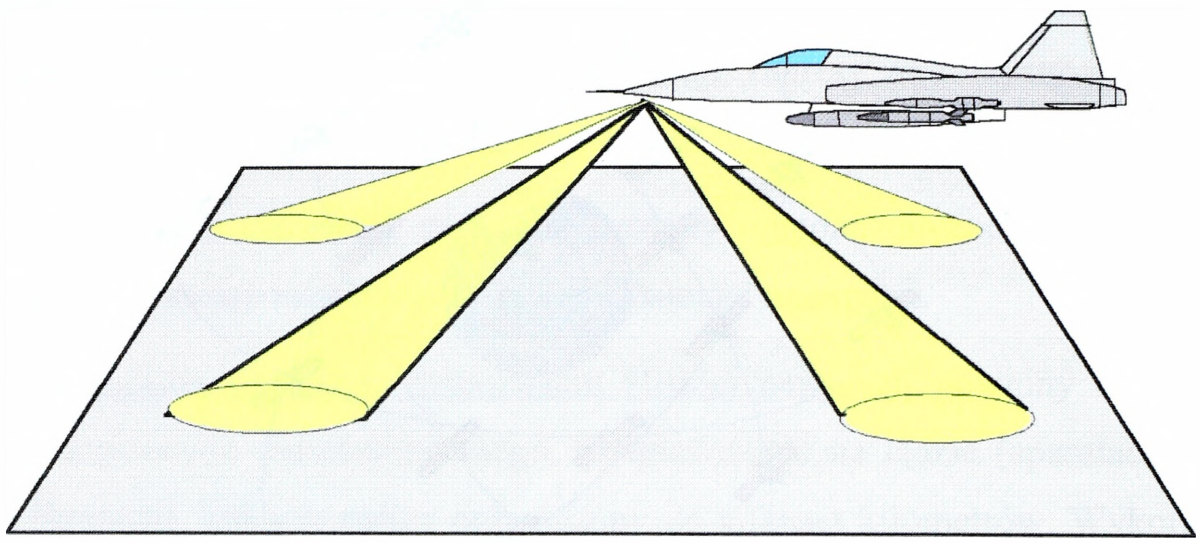
Przyjmując za kryterium podziału sposób pracy systemu radionawigacyjnego, możemy wyróżnić:

– systemy nieautonomiczne - wykorzystujące urządzenia odbiorcze lub odbiorczo – zapytujące, współpracujące z naziemnymi, nawodnymi lub satelitarnymi źródłami sygnałów nawigacyjnych;

– systemy autonomiczne - charakteryzujące się tym, że środki radionawigacyjne są zamontowane tylko na obiektach, umożliwiając określenie ich położenia oraz parametry ruchu, niezależnie od urządzeń zewnętrznych.

Do tych ostatnich zaliczamy m.in. pokładowe impulsowe i dopplerowskie stacje radiolokacyjne wykorzystywane do autonawigacji oraz radiowysokościomierze.

W przypadku systemów autonomicznych, opartych o pokładowe stacje radiolokacyjne, możliwości i sposoby ich zakłócania są identyczne jak w przypadku systemów rozpoznania radiolokacyjnego. Utrudnienie stanowi niewielki zasięg tych środków oraz charakterystyka anten, bowiem w urządzeniach pokładowych np. samolotów, są one zwykle skierowane pod dużym kątem w dół (rysunek.2.20).



Rys. 2.20. Przykładowy rozkład wiązki antenowej radiolokatora dopplerowskiego

Zakres i możliwości zakłócania rozpoznania radionawigacyjnego w przypadku systemów nieautonomicznych, są zróżnicowane w zależności od systemu uzyskiwania danych nawigacyjnych i zakresów wykorzystywanych częstotliwości warunkujących ich zasięg.

Zakłócanie systemów rozpoznania bezkierunkowych radiolatarni hiperbolicznych typu Loran, Decca, Omega, ze względu na ich zakresy pracy (fale średnie, długie i bardzo długie), może być realizowane przy pomocy stacji zakłóceń radiowych pracujących w odpowiednich zakresach częstotliwości, podobnie jak radiolatarnie ultrakrótkofalowego systemu VOR.

W przypadku zakłócania urządzeń rozpoznania odległościowych i kierunkowo – odległościowych systemów takich jak radiodalmierz DME czy systemy TACAN i RSBN, oprócz zakłóceń na częstotliwościach rozpoznawanych radiolatarni, istnieje również możliwość zakłócania na częstotliwościach pokładowych urządzeń zapytujących. Pracują one w paśmie ok. 1000 MHz, więc mogą być zakłócane, na przykład za pomocą stacji typu R-388, pokrywającej ten zakres częstotliwości.

2.1.2.1.2. Zakłócanie rozpoznania radiolokacyjnego

Drugim elementem, który został wyodrębniony z rozpoznania elektronicznego jest rozpoznanie radiolokacyjne. Termin radiolokacja pochodzi od łacińskich słów: RADIUS – promień oraz LOKUS - miejsce. Jego odpowiednikiem jest angielskie określenie RADAR od słów Radio Aids for Defence And Reconnaissance (radiowe pomoce do obrony i rozpoznania). Amerykanie etymologię słowa RADAR wywodzą od słów - RAdio Detection And Ranging (radiowe wykrywanie i namierzanie).

Zatem, **zakłócanie rozpoznania radiolokacyjnego** jest procesem, który ma na celu zapobiegać bądź utrudniać przeciwnikowi wykrywanie obiektów nieruchomych i ruchomych na lądzie, morzu i w powietrzu za pomocą stacji radiolokacyjnych.

Obiekty, takie jak infrastruktura naziemna, okręty, samoloty, rakiety, chmury itp, nazywane są celami radiolokacyjnymi[22], zaś sygnały odbite od tych obiektów - echem radarowym lub echem radiolokacyjnym.

Badania aktualnego stanu oraz tendencji rozwojowych radiolokacji pozwalają stwierdzić, że do wykrywania obiektów pola walki wykorzystywane jest głównie pasmo 3 cm (8-12 GHz), natomiast środki napadu powietrznego wykorzystują pasma 2 i 3 cm (8-20 GHz). Dzięki temu, że energia elektromagnetyczna w zakresie mikrofalowym rozprzestrzeniania się prostoliniowo i ze stałą prędkością w środowisku jednorodnym, możliwe jest określanie współrzędnych rozpoznawanych obiektów, pomiar ich parametrów ruchu lub wielkości bryłowej.

Rozpoznanie radiolokacyjne jest prowadzone przez służby wojskowe i cywilne, które kontrolują przede wszystkim przestrzeń powietrzną, ale także obszary lądowy i morski, zarówno w czasie pokoju jak i wojny. Z tego względu, zakłócanie

---

[22] W wojskach radiotechnicznych WLiOP przedmioty wykryte przez stacje radiolokacyjne nazywane są obiektami. Obiekty niezidentyfikowane lub obce (nieprzyjacielskie) nazywa się celami.

rozpoznania radiolokacyjnego powinno obejmować wszystkie rodzaje wojsk i służb, w których wykorzystywane są systemy i środki radiolokacyjne.

W operacjach wojsk lądowych, rozpoznanie radiolokacyjne powinno być jednym z zasadniczych elementów składowych zakłócania rozpoznania przeciwnika i obejmować:

- systemy rozpoznania obszaru powietrznego;
- systemy nadzorowania pola walki;
- systemy kierowania ogniem;
- systemy obrony przeciwlotniczej;
- systemy rozpoznania powierzchni ziemi SLAR i inne.

Zakłócaniem powinny być objęte systemy wykorzystujące naziemne, brzegowe, czy okrętowe stacje radiolokacyjne, jak również samoloty rozpoznawcze wyposażone zarówno w „klasyczne" stacje radiolokacyjne, jak i stacje obserwacji bocznej.

Zakłócanie naziemnego rozpoznania radiolokacyjnego szczebla operacyjnego powinno być prowadzone na małą głębokość (do 50 km) i skupiać się na systemach rozpoznania pola walki, kierowania ogniem artylerii oraz obserwacji przestrzeni powietrznej.

Uzyskanie wymaganej głębokości, zależy przede wszystkim od technicznych możliwości stacji zakłóceń oraz ich właściwego rozmieszczenia w terenie, stosownie do położenia zakłócanych obiektów oraz odległości, stanowiącej kompromis pomiędzy ich zasięgiem i bezpieczeństwem. Niezależnie od charakteru prowadzonych działań, stacje zakłóceń powinny być rozmieszczane poza zasięgiem głównej masy ognia środków strzelających na wprost.

W operacjach wojsk lądowych, oprócz naziemnych systemów i środków rozpoznania radiolokacyjnego, zakłócaniem na dużą odległość (do 500 km) powinny być objęte środki napadu powietrznego wykorzystywane przez przeciwnika.

Ich pokładowe stacje radiolokacyjne, są przeznaczone nie tylko do wykrywania i lokalizacji obiektów naziemnych, nawodnych i powietrznych, ale również do kierowania i naprowadzania bomb i pocisków rakietowych. Zakłócenia powinny również obejmować lotnicze stacje radiolokacyjne wykorzystywane do nawigacji, określania wysokości lotu lub identyfikacji „swój – obcy".

Zakłócanie powietrznego rozpoznania radiolokacyjnego powinno obejmować swoim zasięgiem środki napady powietrznego na małych, średnich i dużych wysokościach (od 50 do 12 tysięcy metrów). Nowoczesne stacje zakłóceń radiolokacyjnych, powinny uwzględniać wszystkie wymienione typy i rodzaje radiolokatorów pokładowych i obejmować swym zasięgiem obiekty na dowolnej wysokości.

Zakłócanie morskiego rozpoznania radiolokacyjnego, powinno być prowadzone przez wojska lądowe w przypadku, gdy obszar operacji obejmuje pas przybrzeżny. Ich zadania, powinny być przede wszystkim związane z radiolokacyjną osłoną obiektów wzdłuż wybrzeża morskiego i zakłócaniem rozpoznania warunków hydrometeorologicznych w obszarze działań. Zakłócanie morskiego rozpoznania radiolokacyjnego powinno być prowadzone przeciwko autonomicznym urządzeniom radiolokacyjnym okrętów oraz stacjom obserwacji brzegowej przeciwnika.

Przyjmując za kryterium podziału sposoby prowadzenia rozpoznania radiolokacyjnego możemy wyróżnić zakłócanie radiolokacji pasywnej i aktywnej.

Zakłócanie radiolokacji pasywnej polega na zmianach środowiska propagacji fal radiowych i radiolokacyjnym maskowaniu obiektów.

Zmian środowiska można dokonywać m.in. przez sztuczną jonizację odpowiednich warstw atmosfery, stosowanie metalizowanych dymów, barier z dipoli itp.

Zakłócanie radiolokacyjne w ramach maskowania obiektów tzw. osłona radiolokacyjna, powinna być realizowana w szerokim zakresie widma elektromagnetycznego i obejmować (rysunek 2.21.):

– promieniowanie termiczne obiektów o temperaturze wyższej od zera bezwzględnego /absolutnego/ (0K = –273,15°C);

– promieniowanie niezamierzone w zakresie radiowym, powstające przy pracy urządzeń elektronicznych, elektrycznych, silników rakietowych itp.;

– promieniowanie zamierzone różnych urządzeń radiowych znajdujących się na pokładach zakłócanych celów.

Rys. 2.21. Idea zakłócania radiolokacji pasywnej

Przy zakłócaniu radiolokacji pasywnej, podstawowym utrudnieniem są problemy z wykrywalnością tych urządzeń. Ponieważ nie mają one żadnych urządzeń nadawczych, są w zasadzie niewykrywalne i dlatego ważne obiekty powinny być radiolokacyjnie osłaniane - a priori.

Zakłócanie radiolokacji aktywnej polega na wyeliminowaniu radiolokatorów przeciwnika, emitujących w sposób zamierzony własne sygnały. W zakłócaniu radiolokacji aktywnej, wykorzystuje się sygnały impulsowe a od kilkunastu lat używa się do tego celu również sygnałów z falą ciągłą.

Do zalet zakłócania metodą impulsową należy zaliczyć możliwość generacji sygnału bardzo dużej mocy (rzędu megawatów) w postaci impulsu o czasie trwania rzędu milisekund, przy stosunkowo małej mocy średniej nadajnika zakłócającego. Poza tym praca impulsowa daje możliwość jednoczesnego wykrywania i zakłócania dużej liczby obiektów przeciwnika.

Stacja zakłócająca radiolokatory aktywne, powinna posiadać odbiornik umożliwiający poszukiwanie sygnałów radiolokacyjnych, urządzenie zobrazowania i analizy struktury tych sygnałów oraz nadajnik wytwarzający sygnały zakłócające o strukturze sygnałów użytecznych.

Zakłóceniami radiolokacji aktywnej, należałoby objąć następujące rodzaje urządzeń przeciwnika:

– radiolokatory z pasywną odpowiedzią;

– radiolokatory z aktywną odpowiedzią;

– radiolokatory półaktywne.

Zakłócenia radiolokacji z pasywna odpowiedzią obejmują stacje, których praca oparta jest na zdolności celu do odbijania fal radiowych, a więc zdolności do pasywnej odpowiedzi. Odbite sygnały (echa) radiolokacyjnego mogą zawierać dane o położeniu celu (współrzędne dwu- lub trój-wymiarowe), jego kształcie i wymiarach a także parametrach ruchu (prędkości).

Do określania odległości zakłócanej stacji wykorzystuje się zjawisko stałej prędkości rozprzestrzeniania się fal radiowych w środowisku jednorodnym. Odległość tę wyznacza się ze wzoru:

$$R = c \cdot t$$

gdzie:

R – odległość stacji radiolokacyjnej od nadajnika zakłócającego w km;

c – szybkość rozprzestrzeniania się fal radiowych c≈ 300 tys. km/s;

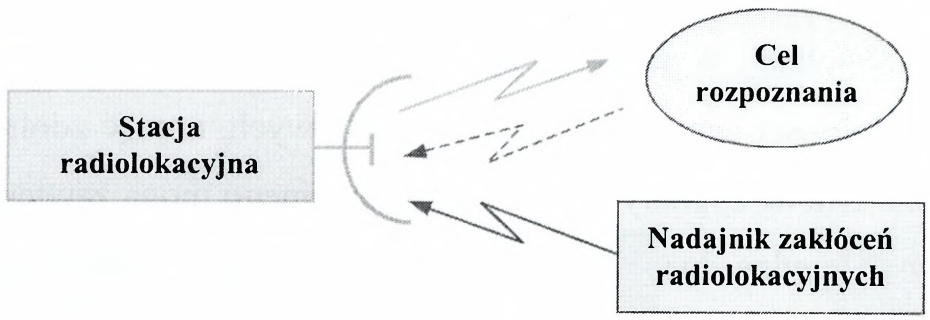
t – czas na pokonanie odległości przez sygnał w sekundach.

Dane o współrzędnych kątowych zakłócanej stacji można uzyskać dzięki kierunkowej charakterystyce anten radiolokacyjnych oraz prostoliniowemu rozprzestrzenianiu się energii elektromagnetycznej w zakresie mikrofalowym.

Pomiar ruchu i szybkości zakłócanej stacji umożliwia zjawisko Dopplera, polegające na zmianie częstotliwości sygnału ruchomego celu. Uzyskanie pozostałych danych umożliwia analiza przechwyconych sygnałów radiolokacyjnych. Ideę zakłócania radiolokacji aktywnej z pasywną odpowiedzią ilustruje rysunek 2.22.

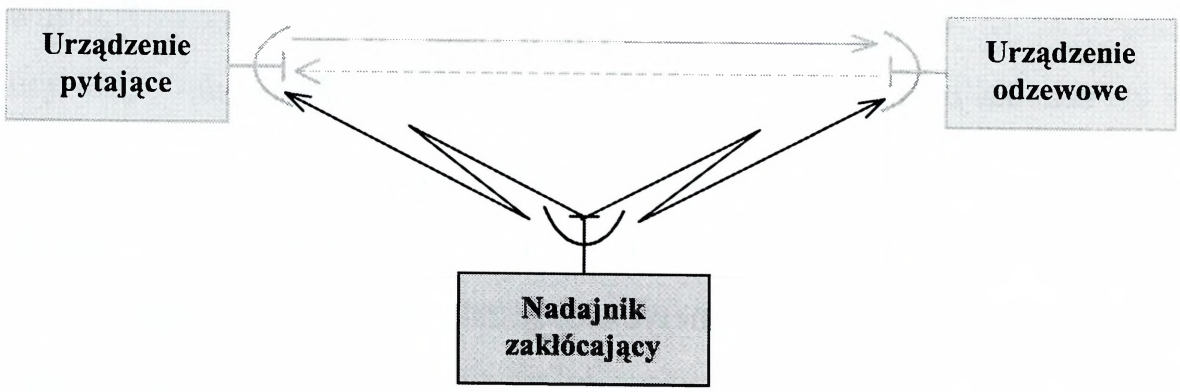
Zakłóceniami objąć można nie tylko stacje będące w bezpośrednim zasięgu fal radiowych, ale także stacje poza horyzontem radiowym. Dla uzyskania bardzo dużych zasięgów zakłócania, wykorzystuje się zjawiska zachodzące w jonosferze. Sygnały nadawane przez stację zakłóceń ulegają w jonosferze ugięciu, po czym tra-

fiają do anteny zakłócanej stacji, analogicznie jak ma to miejsce przy zakłócaniu rozpoznania łączności na falach krótkich.



Rys. 2.22. Zakłócanie pracy radiolokatora aktywnego z pasywną odpowiedzią

Zakłócanie radiolokacji z aktywną odpowiedzią polega na odpromieniowaniu sygnału (zapytującego) stacji radiolokacyjnej lub specjalnego urządzenia odzewowego (odpowiadającego). Ideę zakłócania radiolokacji z aktywną odpowiedzią ilustruje rysunek 2.23.



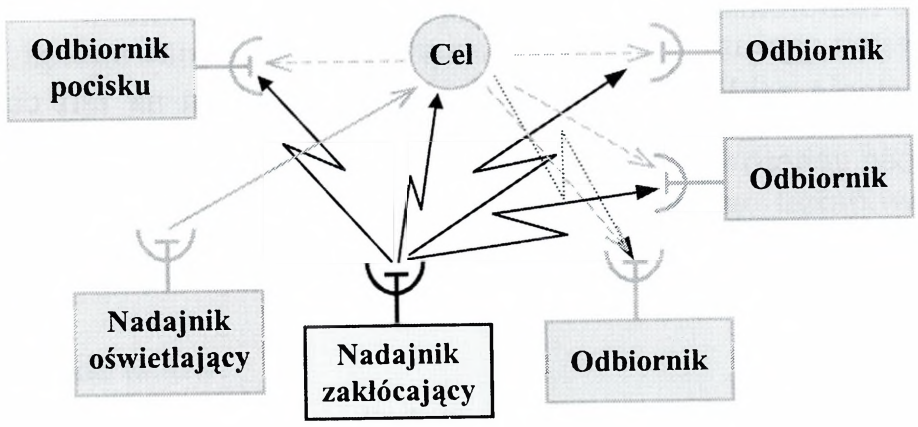
Rys. 2.23. Zakłócanie radiolokacji z aktywną odpowiedzią

Urządzenia tego typu wykorzystuje się do określenia przynależności państwowej w samolotach tzw. określenie „swój – obcy" lub też w systemach radionawigacyjnych z wykorzystaniem radiolatarni. W przypadku gdy nosiciel urządzenia zapytującego wyśle sygnał zapytania to urządzenie odzewowe (radiolatarnia) odpowie na zapytanie wysyłając sygnał zwrotny. Na podstawie opóźnień sygnałów układy przeliczające określą miejsce położenia obiektu.

Ze względu na złożoną strukturę sygnałów i częste zmiany klucza, zakłócanie urządzeń identyfikacji „swój – obcy" jest stosunkowo trudne.

Zakłócanie radiolokacji półaktywnej polega na objęciu zakłóceniami dwu lub więcej stacji radiolokacyjnych, z których jedna przeznaczona jest do „oświetlania" celu a pozostałe do odbioru odbitych sygnałów (radiolokacja bistatyczna lub multistatyczna[23]). Tego rodzaju urządzenia wykorzystywane są do specjalnych zastosowań jak np. dla ułatwienia naprowadzania pocisków kierowanych na cel lub wykrywania obiektów w technologii stealth.

Tę zasadę zakłócania ilustruje rysunek. 2.24.



Rys. 2.24. Zakłócanie radiolokacji półaktywnej

Zakłócanie radiolokacji półaktywnej jest trudne, bowiem pasywny charakter części odbiorczej znacznie utrudnia lokalizację jego elementów.

Przy zakłócaniu urządzeń pracujących na fali ciągłej, należy pamiętać, że następuje jednoczesne wysyłanie i odbiór odbitych sygnałów przez tą samą antenę. Sygnał zakłócający powinien być dokładnie zsynchronizowany z częstotliwością i fazą sygnału użytecznego, bowiem może zostać odfiltrowany przez antenowe układy separacji.

---

[23] Radiolokacja bistatyczna – to zespół dwóch urządzeń z czego jednym jest nadajnik a drugim odbiornik wraz z urządzeniem wskaźnikowym. Radiolokacja multistatyczna to zespół co najmniej trzech urządzeń z czego jednym musi być nadajnik a dwa pozostałe to odbiorniki z urządzeniami wskaźnikowymi. W obydwu przypadkach nadajnik i odbiornik muszą być zsynchronizowane w czasie i w przestrzeni.

Zakłócając urządzenia pracujące na fali ciągłej należy uwzględnić:

1. Urządzenia z falą ciągłą niemodulowaną, a wśród nich:
   - stacje radiolokacyjne dopplerowskie;
   - stacje radiolokacyjne z falą ciągłą z przesunięciem fazowym;
   - stacje radiolokacyjne z falą ciągłą z kodowaniem fazowym.
2. Urządzenia z falą ciągłą modulowaną, a wśród nich:
   - stacje z falą ciągłą modulowaną częstotliwościowo;
   - stacje z modulacją amplitudy i z modulacją fazy;
   - stacje radiolokacyjne z falą ciągłą modulowaną szumem.

Nowoczesne stacje zakłóceń radiolokatorów pracujących na fali ciągłej, powinny mieć możliwość generowania wszystkich wymienionych wyżej rodzajów sygnałów.

2.1.2.1.3. Zakłócanie rozpoznania czujnikowego

Zakłócanie rozpoznania czujnikowego ma na celu utrudnienie bądź uniemożliwienie przeciwnikowi zdobywania oraz przetwarzania tych danych, których nośnikami są fale sprężyste[24] (infradźwięki[25], ultradźwięki[26]) oraz wszelkiego rodzaju uboczne efekty towarzyszące działaniom bojowym, na przykład: termiczne, sejsmiczne, naciskowe, magnetyczne, chemiczne, zapachowe.

Przeprowadzone badania wykazały, że do postrzegania pola walki, przez pryzmat fal sprężystych oraz pozostałych efektów towarzyszących działaniom bo-

[24]Fale sprężyste - zaburzenia rozchodzące się w ośrodku sprężystym. Polegają na drganiu cząsteczek wokół punktu równowagi. Ilustrowana encyklopedia dla wszystkich. Fizyka, wyd. WNT, Warszawa 1991, s. 77.

[25] Infradźwięki - fale sprężyste o częstotliwościach mniejszych niż 16 Hz, czyli poniżej progu słyszalności człowieka. Fale te są słabo tłumione i dlatego rozprzestrzeniają się na stosunkowo duże odległości od źródeł. Mogą być wykorzystane do rejestracji efektów sejsmicznych oraz eksplozji na polu walki. Tamże, s. 112.

jowym, potencjalny przeciwnik może wykorzystać całą rodzinę urządzeń czujnikowych z zastosowaniem elektronicznej przemiany rejestrowanych sygnałów.

W wyniku prowadzonego rozpoznania czujnikowego potencjalny przeciwnik ma możliwość pozyskiwania danych z najbardziej niedostępnych obszarów[27] działań bojowych, w czasie zbliżonym do rzeczywistego. Na szczeblach operacyjnych, za ich pomocą może również śledzić i nadzorować:

– aktywność naszych wojsk lądowych w rejonach oraz wzdłuż wybranych tras, w których zostały rozmieszczone odpowiednie czujniki;

– aktywność naszych wojsk w rejonach rozmieszczenia zapór i pól minowych, przepraw rzecznych, mostów i brodów;

– rejony zaplanowane jako strefy lądowania lub zrzutu jego wojsk desantowo - szturmowych;

– zmiany w funkcjonowaniu wybranych elementów ugrupowania naszych wojsk, ich stanowisk dowodzenia, punktów zaopatrywania, itp.;

– wskazywanie celów.

Zakłócanie rozpoznania czujnikowego w operacjach wojsk lądowych jest przedsięwzięciem perspektywicznym, którego rozwiązania powinny zmierzać do utrudniania wykrywania, pozorowania czujnikowego i niszczenia.

Przedsięwzięcia wykonywane w ramach zakłócania rozpoznania czujnikowego powinny być podzielone na organizacyjne i techniczne. Należy jednak dążyć do tego, aby były one ze sobą ściśle powiązane i wzajemnie się uzupełniały. Należy je ukierunkować na dezorganizację rozpoznania w wyniku ograniczenia pracy i eliminowania tych źródeł, które emitują energię odpowiadającą parametrami sygnałom bodźcowym sensorów: akustycznych, magnetycznych, elektrycznych i chemicznych.

---

[26]Ultradźwięki - fale sprężyste o częstotliwościach większych niż 20 kHz, a więc leżące powyżej zakresu słyszalności człowieka. Mogą być wykorzystane do rozpoznania ultradźwiękowego i rejestracji efektów akustycznych pola walki. Tamże, s. 293.

[27]W przyszłości w rejonie operacji, mogą być rozmieszczane na lądzie, w wodzie lub w powietrzu tysiące miniaturowych czujników wielospektralnych. Miniaturowe biosensory (czujniki zapachu), reagujące na pot ludzki lub wydychane powietrze, mogą nawet wykrywać i śledzić żołnierzy przeciwnika.

Charakterystyczne dla środowiska akustycznego na polu walki są: odgłosy wybuchów, wstrząsy, szum pojazdów mechanicznych i agregatów prądotwórczych. Eliminowanie źródeł hałasu powinno sprowadzać się do wykorzystania maskujących właściwości terenu oraz stosowania okryć tłumiących. Ponadto należy dążyć do unifikacji środków transportu techniki bojowej, co zapobiega ich identyfikowaniu przez systemy czujnikowe.

Przeprowadzone badania wykazały, że generatory infradźwięków mogą być również wykorzystane na polu walki do obezwładniania siły żywej. Obrona przed nimi powinna opierać się na budowaniu tzw. miękkich zasłon, które absorbują energię fali infradźwiękowej, oraz tworzeniu tzw. pól aktywnego hałasu. Istota działania tych pól, polega na wytworzeniu fali dźwiękowej o tych samych parametrach, lecz w fazie odwróconej o 180^0.

2.1.2.1.4. Zakłócanie rozpoznania optoelektronicznego

Zakłócanie rozpoznania optoelektronicznego ma na celu utrudnić bądź uniemożliwić przeciwnikowi zdobywanie oraz przetwarzanie tych danych, których nośnikami są fale elektromagnetyczne pasma optycznego

Do pracy w tym paśmie[28]. skonstruowano całą rodzinę urządzeń optoelektronicznych[29] pozwalających na prowadzenie rozpoznania w zakresie promieniowania widzialnego oraz w całym zakresie podczerwieni, dlatego zakłóceniami należałoby objąć wszelkiego rodzaju urządzenia: telewizyjne, termowizyjne, noktowizyjne oraz laserowe.

---

[28]Pasmo optyczne widma elektromagnetycznego stanowią zakresy: podczerwieni (długość fali 1000 – 0,76μm), światła widzialnego (długość fali 0,76 – 0,38μm), i ultrafioletu (długość fali: 0,38 –0,01μm).

[29] Optoelektronika [gr.],dziedzina nauki i techniki zajmująca się przetwarzaniem sygnałów elektrycznych na optyczne (np. za pomocą diod luminescencyjnych, kineskopów, monitorów ekranowych) oraz optycznych na elektryczne (np. za pomocą fotoogniw, fotopowielaczy, matryc CCD) oraz przesyłaniem danych w postaci sygnałów optycznych (np. światłowodami) i ich magazynowaniem.

Zakłócanie rozpoznania telewizyjnego, powinno być tylko uwzględniane w ramach planowanych przedsięwzięć, natomiast skupić się na dziale telekomunikacji, który zajmuje się przekazywaniem na odległość obrazów ruchomych wraz z towarzyszącym dźwiękiem. Powinno obejmować wszystkie łącza radiowe, radioliniowe i satelitarne wykorzystywane do przekazu telewizyjnego, których zakłócanie zostało wcześniej omówione.

Zakłócanie rozpoznania termowizyjnego w ramach maskowania, powinno obejmować dwa podzakresy widma promieniowania podczerwonego 3 – 5 μm oraz 10 – 13 μm, które są powszechnie wykorzystywane w większości współczesnych kamer termowizyjnych. Główny wysiłek zakłócania, tak jak w poprzednim przypadku, powinien się skupiać na środkach przekazu danych.

Termowizja, w istocie wykorzystywanego zjawiska, podobna jest do noktowizji pasywnej. Różnica polega tylko na tym, że kamery termowizyjne posiadają dodatkowo urządzenie skanujące, które zamienia obraz widziany w wymienionych pasmach podczerwieni na ciąg impulsów elektrycznych.

Zakłócanie noktowizji powinno obejmować urządzenia, które umożliwiają widzenie w całym zakresie promieniowania podczerwonego od 1000 μm do 0,76 μm. Zakres jest podzielony na podczerwień bliską 0,76 – 1,5 μm, średnią 1,5 – 5,6 μm i daleką 5,6 – 1000 μm. W dolnym paśmie podczerwieni dalekiej wyróżniany jest podzakres zwany podczerwienią skrajną.

Obserwacja różnych obiektów w podczerwieni, może być realizowana za pomocą noktowizorów aktywnych lub pasywnych, które wykorzystują naturalne promieniowanie własne obiektu (wszystkie ciała, których temperatura jest wyższa od zera bezwzględnego, emitują własne, niekoherentne promieniowanie podczerwone).

Noktowizory aktywne (starszego typu), są wycofywane z wojsk, bowiem muszą być wyposażone w specjalne reflektory podczerwieni, które demaskują ich pracę.

W działaniach operacyjnych wojsk lądowych, problematyka zakłócania rozpoznania optoelektronicznego powinna być ściśle powiązana z zakłócanie rozpoznania radiolokacyjnego i realizowana przy pomocy ukrywania, dezinformowania i pozorowania optoelektronicznego. W zależności od sposobu, udział poszczególnych przedsięwzięć powinien być różny, np. w zakłócaniu rozpoznania bezpośredniego podstawę powinno stanowić ukrywanie optoelektroniczne.

Przedsięwzięcia wykonywane w ramach zakłócania rozpoznania optoelektronicznego powinny być podzielone na organizacyjne i techniczne.

Przedsięwzięcia organizacyjne mają na celu ukrywanie różnych obiektów wojsk lądowych. Polegają na odpowiednim wykorzystaniu ukryć naturalnych i wynikają z właściwości terenu i przedmiotów terenowych, pory doby (nocy) pogody (mgły), zastosowania zasłon dymnych oraz innych warunków meteorologicznych mających wpływ na obniżenie efektywności środków rozpoznania optoelektronicznego. Przedsięwzięcia te powinny być ściśle skoordynowane i prowadzone według zasad obowiązujących w zakłócaniu rozpoznania radiolokacyjnego.

Do krótkotrwałego zakłócania rozpoznania optoelektronicznego, mogą być użyte specjalne generatory dymotwórcze, wytwarzające tradycyjne zasłony dymne oraz dymy o znacznie podwyższonej lub obniżonej temperaturze. Badania wykazały, że mają one znaczny wpływ na obniżenie efektywności środków rozpoznania optoelektronicznego. Uniemożliwiają lub znacznie utrudniają przeciwnikowi prowadzenie nie tylko obserwacji optycznej, lecz również termowizyjnej i laserowej.

Realizacja przedsięwzięć technicznych zakłócania rozpoznania optoelektronicznego, jest z kolei związana ze stosowaniem różnego rodzaju etatowych oraz podręcznych środków i materiałów używanych do tego celu. Należy podkreślić fakt, że stosowanie środków etatowych, w odróżnieniu od podręcznych, pozwala na znaczne skrócenie czasu przygotowań oraz zapewnia lepsze rezultaty. Tej problematyce należałoby poświęcić więcej uwagi, bowiem mimo wprowadzania na wyposażenie wojsk coraz większej ilości środków optoelektronicznych, w wojskach lądowych obserwuje się tendencję do stopniowego zmniejszania udziału przedsięwzięć związanych z zakłócaniem tego rodzaju rozpoznania.

Natomiast będące aktualne w wyposażeniu wojsk lądowych maski, są najczęściej poliamidowe i charakteryzują się zaledwie dostatecznymi zdolnościami zakłócania rozpoznania optycznego (maskowanie), w zakresie widma widzialnego oraz w bliskiej podczerwieni. Powinny być jak najszybciej zastąpione odpowiednimi pokryciami izolującymi optycznie, termicznie oraz radiolokacyjnie.

Ważnym i jak wykazuje - praktyka ostatnich wojen i konfliktów lokalnych - skutecznym środkiem zakłócania w omawianym widmie, jest malowanie maskujące[30], którego podstawowymi rodzajami powinno być:

– malowanie ochronne (ukrywające);

– malowanie pozorujące;

– malowanie deformujące.

W malowaniu ochronnym należy wykorzystać specjalne farby, które powodują zlewanie się widma obserwowanego celu z widmem tła. Farby takie, nazywane metamorficznymi, powodują zmianę koloru pod wpływem warunków zewnętrznych m.in. temperatury i natężenia oświetlenia.

Malowaniem pozorującym należy pokrywać obiekty pozorne, których kształt, kolorystyka i charakterystyki spektralne, nie powinny odbiegać od obiektów rzeczywistych. Takie cechy obiektów rzeczywistych mają m.in. obiekty pozorne wytwarzane za pomocą zestawu DECEPTION - szwedzkiej firmy Barracuda. Są to obiekty w większości wykonane w skali 1:1, pozorujące sprzęt bojowy taki jak: czołgi, transportery, zestawy artyleryjskie, systemy rakietowe, a nawet mosty, bazy lotnicze itp. Ich koszty produkcji nie przekraczają 0,5 % wartości pozorowanego obiektu. Rozproszenie wysiłku rozpoznawczego przeciwnika na obiektach pozornych, zwiększa szansę na przetrwanie elementów rzeczywistych ugrupowania operacyjnego, bowiem przy zastosowaniu właściwej techniki pozoracji, prawdopodobieństwo przeprowadzenia ataku na cel pozorny jest bardzo wysokie.

---

[30] W naszych wojskach lądowych nie ma etatowych zestawów do malowania maskującego, a przygotowanie stanów osobowych do jego wykonania nie jest wystarczające.

Na szczególną uwagę zasługuje również malowanie deformujące, nazywane kamuflażowym. Do malowania wykorzystuje się różnego rodzaju farby nitrocelulozowe, olejne, kazeinowe oraz farby nowej generacji oparte na dyspersji koloidowej, poliuretanowe i wodne. Przykładowe wzorce malowania kamuflażu sprzętu technicznego należy opracować na różne pory roku, uwzględniając przy doborze farb kolorystykę i charakterystyki spektralne uśrednionego tła terenu, w którym sprzęt będzie używany.

Zakłócanie urządzeń laserowych[31] ma na celu utrudnić bądź uniemożliwić przeciwnikowi korzystanie z tych urządzeń. Powinno obejmować między innymi laserowe urządzenia lotnicze stosowane w:

– nawigacji lotniczej – do pomiaru wysokości i prędkości lotu, oświetlania identyfikowanego terenu, określania współrzędnych kątowych, określania warunków atmosferycznych.

– rozpoznaniu lotniczym – do oświetlania terenu przy wykonywaniu zdjęć lotniczych w nocy i trudnych warunkach atmosferycznych, ukośnego fotografowania dużych obszarów, prowadzenia rozpoznania o wysokiej jakości zobrazowania przy lotach na niskim pułapie, uzyskiwania trójwymiarowych zobrazowań (trzeci wymiar uzyskiwany za pomocą dalmierza laserowego).

W działaniach bojowych lotnictwa – do wybierania i oświetlania wiązką lasera celów punktowych, przewidzianych do ataku bombami i pociskami rakietowymi samonaprowadzającymi się na laserowo oświetlone cele, w zbliżeniowych zapalnikach laserowych oraz kierowania ogniem lufowej broni pokładowej samolotów i śmigłowców.

W wojskach lądowych, zakłócenia powinny obejmować wykorzystywane przez przeciwnika laserowe urządzenia celownicze. Eliminując subiektywne przyczyny niecelności, urządzenia te pozwalają na prowadzenie znacznie bardziej pre-

[31] Nazwa „laser" została utworzona z początkowych liter słów: **L***ight* **A***mplification by* **S***timulated* **E***mission of* **R***adiation* (wzmocnienie światła z wymuszoną emisją promieniowania). Laser – to optyczny generator kwantowy, zwany też generatorem światła spójnego, lub źródłem monochromatycznych fal elektromagnetycznych w zakresie optycznym.

cyzyjnego ognia, zarówno przy strzelaniu z broni lufowej, jak i przeciwpancernych pociskach rakietowych naprowadzanych na cel wiązką lasera.

Lasery mogą być również szeroko wykorzystywane do monitorowania pola walki, oświetlania obiektów ugrupowania operacyjnego i naziemnej infrastruktury, określania warunków atmosferycznych, lądowej nawigacji, a nawet oślepiania siły żywej, chociaż zabraniają tego konwencje genewskie.

2.1.2.1.5. Zakłócanie rozpoznania informatycznego

W przyszłych systemach rozpoznania informatycznego[32] wojsk lądowych, należy liczyć się z systematycznym wzrostem penetracji rozległych i lokalnym sieci informatycznych, które obsługiwać będą zautomatyzowane systemy dowodzenia, zautomatyzowane systemy rozpoznania oraz zautomatyzowane systemy kierowania uzbrojeniem. Już w chwili obecnej, wykorzystywane sieci informatyczne są bogatymi źródłami danych o wojskach walczących stron. Bogate i niezmiernie wartościowe informacje, czerpać też można z promieniowania samych komputerów.

Przeprowadzone badania wykazały, że sieci informatyczne bez odpowiednich zabezpieczeń i mechanizmów ochronnych, narażone są na penetrację i dostęp do ich baz danych, a zgromadzone w nich zasoby i strumienie danych, są narażone na penetrację, rozpoznanie, modyfikację lub zniszczenie. Włączanie się do nich nieupoważnionych użytkowników jest stosunkowo łatwe i dalece prawdopodobne[33]. Mogą oni śledzić, podsłuchiwać i przechwytywać dane, a także prowadzić dezinformację bądź destrukcję.

---

[32]W Regulaminie działań wojsk lądowych, wyd. DWLąd. Warszawa 1999, s.42 w dalszym ciągu używa się pojęcia „system łączności" rozumianego jako ogranizacyjno-techniczny zespół sił i środków łączności i informatyki odpowiadający potrzebom dowodzenia i sterowania środkami rażenia, charakterowi prowadzonych działań i wykonywanym zadaniom.

[33] Należy zdawać sobie sprawę z faktu, że pozyskiwanie tych danych jest stosunkowo łatwe. Poza tym nie wymaga ani skomplikowanych urządzeń ani też specjalistycznego przygotowania załóg. Jako przykład mogą być podani międzynarodowi piraci komputerowi (ang. *hackers*), którzy bez większych przeszkód włamują się nawet do dobrze zabezpieczonych systemów komputerowych m in. Pentagonu. Zatem, nie trzeba być ani „wielkim ani bogatym", aby skutecznie prowadzić rozpoznanie informatyczne.

Stąd też problem zakłócania rozpoznania informatycznego nabiera szczególnego znaczenia. Powinno ono zapewniać ochronę własnych sieci i baz danych, przed dostępem nieuprawnionych użytkowników, piractwem komputerowym oraz celowym modyfikowaniem lub przypadkowym zniszczeniem. Dotyczy to wszystkich poziomów *„działań na informacjach"*, pozyskiwania, przetwarzania, przesyłania i przechowywania. Zakłócanie powinno obejmować penetrację bierną, stanowiący zagrożenie dla zachowania tajemnicy oraz penetrację aktywną, zagrażającą autentyczności danych.

Zakłócanie penetracji biernej – dotyczy dostępu przeciwnika do danych, a w sieciach komputerowych do monitorowania ich przepływu lub ustalenia struktury sieci. Penetracja bierna może być prowadzona w formie: przeglądania, przenikania i wnioskowania.

Przeglądanie – polega na przeszukiwaniu sieci komputerowej w celu pozyskania danych. Jest to proces podobny do śledzenia w kanałach łączności, przy czym istnieją tu dwie istotne różnice. Po pierwsze w sieciach komputerowych dane są przechowywane znacznie dłużej i dlatego są zdecydowanie bardziej narażone na przeglądanie niż kanały łączności na śledzenie. Po drugie, kanały łączności są narażone na śledzenie wtedy, kiedy przeciwnik ma dostęp energetyczny do sygnałów. Natomiast przeglądanie jest możliwe wówczas, gdy przeciwnik „złamie" zabezpieczenia i kody dostępu do sieci lub wybranych obszarów pamięci systemów komputerowych.

Przenikanie – zwane też przeciekaniem informatycznym, dotyczy przepływu danych do nieuprawnionych użytkowników podczas procesów realizowanych przez legalnych użytkowników systemu.

Wnioskowanie – dotyczy procesów ustalenia danych niejawnych, na podstawie ogólnie dostępnych lub jawnych informacji. Na przykład: przechwycenie przez przeciwnika danych ze służby zapatrzenia żywnościowego dotyczącej ilości zamawianej żywności umożliwia określenie ilości żołnierzy danej jednostki.

Zakłócanie penetracji aktywnej – dotyczy ochrony własnych zbiorów lub strumieni danych, przed rozmyślnym ich modyfikowaniem przez przeciwnika.

Celem takiego działania może być pozyskiwanie danych połączone z ich zastępowaniem innymi zbiorami. W jej ramach, przeciwnik może przykładowo wprowadzić do sieci błędne komunikaty i polecenia dotyczące wykonywanych zadań czy obiektów ataku. Jeżeli dane będą zmieniane w umiejętny sposób lub w minimalnym zakresie, to takie zniekształcanie będzie bardzo trudne do wykrycia.

Przy zakłócaniu penetracji aktywnej należy uwzględnić: zniekształcanie, podszywanie i niszczenie danych.

Zniekształcanie (modyfikacja) danych w sieciach komputerowych jest odpowiednikiem aktywnego zakłócania w kanałach łączności. Zniekształcanie może być użyte do wykonywania określonych zmian w bazach danych, zamazywanie dotychczasowych danych przez zapisywanie bezużytecznych informacji lub usuwanie całych plików.

Podszywanie się jest odpowiednikiem dywersyjnych działań dezinformacyjnych w kanałach łączności. Dotyczy sytuacji, w której przeciwnik podszywa się pod uprawnionego użytkownika sieci i w ten sposób uzyskuje dostęp do plików i zbiorów. Odmianą takiego działania jest przypadek, gdy przeciwnikowi uda się wprowadzić program stymulujący funkcje systemu, dzięki czemu uzyskuje dostęp do najbardziej zastrzeżonych informacji.

Niszczenie danych – dotyczy zamierzonego zamazania lub usunięcia części lub całych plików lub programów. Niszczenie danych może być również niezamierzone, spowodowane wadliwym oprogramowaniem lub usterką sprzętu, a także pomyłką użytkownika.

Zakłócanie rozpoznania informatycznego ma na celu uniemożliwić bądź utrudnić przeciwnikowi zdobywanie oraz przetwarzanie tych danych o wojskach lądowych, które są wykorzystywane w sieciach informatycznych rozległych i lokalnych, obsługujących zautomatyzowane systemy dowodzenia, zautomatyzowane systemy rozpoznania oraz zautomatyzowane systemy kierowania (sterowania) uzbrojeniem.

W działaniach wojsk lądowych zakłócanie rozpoznania informatycznego, jest również perspektywicznym rodzajem zakłócania elektronicznego i powinno obejmować: ukrywanie, dezinformowanie i pozorowanie informatyczne. Przedsięwzięcia wykonywane w ramach zakłócania rozpoznania informacyjnego celowo jest podzielić na organizacyjne i techniczne.

Przedsięwzięcia organizacyjne nazywane również administracyjnymi, powinny zawierać określone reguły postępowania obowiązujące w czasie „działania na informacjach", a w szczególności:

- regulacje prawne w zakresie ochrony kryptograficznej;
- przepisy dotyczące organizacji i funkcjonowania służb ochrony systemów;
- normy w zakresie bezpieczeństwa systemów teleinformatycznych;
- zasady dostępu osób korzystających z zasobów sieci komputerowych;
- zbiory procedur i algorytmów postępowania w celu odtworzenia systemów po awariach i dekonspiracji.

Działanie na informacjach niejawnych powinno się odbywać tylko w miejscach do tego przystosowanych, zabezpieczonych przed fizycznym dostępem osób nieuprawnionych. Praktycznie w każdej jednostce i sztabie, gdzie wykonuje się *działania na informacjach niejawnych*, powinny być zorganizowane odpowiednio wyposażone stanowiska pracy. Takie stanowisko powinno być wyposażone w sprzęt komputerowy spełniający wymogi norm krajowych[34], lub sprzęt wykonany w technologii zgodnej z amerykańskimi wymogami – TEMPEST[35]. Dla takiego stanowiska w wojskach lądowych należy m.in. zorganizować:

- strefy ochronne oraz nadzór pomieszczeń i sprzętu (karty magnetyczne, telewizja przemysłowa, rejestracja ruchu osób w sztabie);

[34] Norma Polska PN-92 T-20001/02 pt. „Współdziałanie systemów otwartych (OSI). Podstawowy model odniesienia. Architektura zabezpieczeń".

[35] W latach osiemdziesiątych w USA opracowano certyfikat bezpieczeństwa systemów komputerowych o nazwie TEMPEST. Jego zadaniem była ocena podatności systemów komputerowych na monitorowanie za pośrednictwem fal radiowych. Opracowane normy są chronione na tyle skutecznie, że ich treść nie jest dokładnie znana poza granicami USA [13].

– ochronę przed dostępem do informacji (selektywny dostęp do informacji dla poszczególnych użytkowników przez wprowadzenie zakresu uprawnień i haseł dostępu).

Ważną rolę powinno też odgrywać zabezpieczenie personalne obejmujące: odpowiedni dobór wysoko kwalifikowanych kadr, wysoki poziom szkolenia, okresowe sprawdzanie umiejętności fachowych.

W ramach **przedsięwzięć technicznych** ważną rolę powinna odgrywać programowa ochrona danych[36]. Systemy zabezpieczeń powinny być budowane w oparciu o komputerowe programy ochronne, będące z zasady integralnym elementem systemu operacyjnego. Chronią one przed nieuprawnionym dostępem do całych sieci lub ich fragmentów.

Popularną i zarazem bardzo skuteczną metodą ochrony danych przed odczytem jest ich szyfrowanie. Polega ono na przekształceniu tekstu źródłowego do postaci, która ukrywa zawarte w nim dane. Szyfry należy wykorzystywać zarówno do ochrony danych przechowywanych w pamięciach zewnętrznych komputerów jak i podczas ich transmisji. Zatem, konieczne jest odpowiednie zaprojektowane i wdrożenie w wojskach lądowych odpowiedniego systemu kryptograficznego (z uwzględnieniem zagadnień sterowania szyfrowaniem), który zdecydowanie ograniczy możliwości działania, nawet wyrafinowanego przeciwnika. Taki system powinien zapewnić:

– szyfrowanie danych niejawnych przesyłanych w sieciach teleinformatycznych w sposób zapewniający ich niedostępność;

– wiarygodną identyfikację komputerowych stacji roboczych i użytkowników ze sprawdzaniem ich uprawnień;

– ochronę ruchu w sieciach teleinformatycznych, uniemożliwiających identyfikację stanowisk dowodzenia i ważnych obiektów;

---

[36] Programowa ochrona danych związana jest z klasą stosowanych urządzeń, a jako standard przyjęto klasyfikację opracowaną przez National Computer Security Center (NCSC) w 1985 r. i opublikowaną w tzw. Pomarańczowej Księdze (The Orange Book) na zamówienie Ministerstwo Obrony USA. Kryteria bezpieczeństwa systemów komputerowych podzielono na 4 kategorie, od D – najniższej; C (C1, C2); B (B1, B2, B3); do A (A1) – najwyższej [18].

– ochronę informacji w bazach danych.

Zminiaturyzowane urządzenia elektroniczne, realizujące odpowiednie algorytmy szyfrowania, stanowią integralną część nowoczesnych abonenckich urządzeń łączności, a proces szyfrowania i deszyfrowania odbywa się w czasie rzeczywistym. Jednak problematyka związana z szyfrowaniem, nie będzie szerzej omawiana z uwagi na jej obszerność i złożoność, która wykracza poza ramy niniejszego opracowania.

Ochrona programowa danych, dotyczy również stosowania metod i środków zapewniających ich bezpieczeństwo podczas przechowywania i przetwarzania w systemach komputerowych, a także podczas ich przesyłania w sieciach teleinformatycznych. Obejmuje ona cztery rodzaje sterowania:

– sterowanie szyfrowaniem;

– sterowanie dostępem;

– sterowanie przepływu danych;

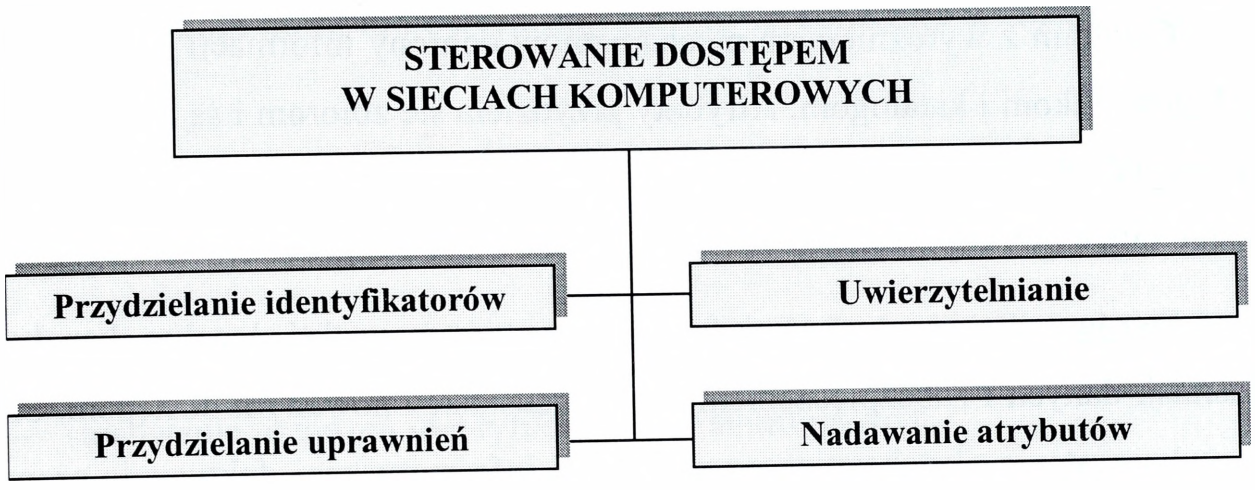
– sterowanie wnioskowaniem.

Sterowanie szyfrowaniem polega na wykorzystaniu odpowiednich programów zabezpieczających własne pliki danych, sterujące procesem szyfrowania jak i przydzielania kluczy, w zależności od przewidywanego poziomu zabezpieczeń i stopnia rozpowszechniania plików (np. tylko użytkownik, grupa użytkowników i inne).

Sterowanie dostępem polega na opracowaniu odpowiednich procedur, zapewniających legalny dostęp uprawnionych użytkowników do obiektów i danych systemu teleinformatycznego. Istota działań w tym zakresie powinna polegać na programowym identyfikowaniu i uwierzytelnianiu tożsamości użytkowników, nadanych im przez zarządzającego siecią. Sterowanie dostępem w sieciach komputerowych obejmuje czynności przedstawione na rysunku 2.25.

Użytkownikowi należy przydzielić identyfikator - czyli nazwę, dzięki której sieć potrafi stwierdzić jego tożsamość. Identyfikator powinien być podawany przy

każdej próbie rejestracji w sieci, która na jego podstawie identyfikuje użytkownika i jednocześnie określa zakres przysługujących mu uprawnień.



Rys. 2.25. Sterowanie dostępem w sieciach komputerowych

Uwierzytelnianie jest czynnością pozwalającą sprawdzić tożsamość osoby posługującej się identyfikatorem. Jest ono realizowane za pomocą *hasła,* które jest ustawowym warunkiem rejestracji w sieci.

Wpisywane hasło nie powinno być widoczne na ekranie terminala, co uniemożliwia jego odczytanie przez osoby nieupoważnione.

Po sprawdzeniu podanego hasła, program zarządzający powinien przechodzić do wykonywania poleceń związanych z realizacją początku sesji. Warto podkreślić, że procedura sprawdzania poprawności hasła powinna odbywać się bezpośrednio w terminalu, co eliminuje transmisję hasła pomiędzy serwerem i terminalem. Zatem, nie ma ani programowej, ani sprzętowej możliwości jego odczytu, na podstawie analizy danych wymienianych z serwerem. Jedynymi miejscami, w których hasło „istnieje" są: terminal i pamięć użytkownika.

Kolejnym elementem ochrony informacji powinno być przydzielenie uprawnień użytkownikom przez zarządzającego siecią. Prawa określają, jakiego rodzaju operacje mogą być wykonywane na zbiorach (np.: prawo do czytania, zapisywania, zakładania katalogów, modyfikacji lub ich przeszukiwania). Uprawnienia dzielą się na dwie kategorie:

– użytkownika - które przyznaje zarządca sieci;

– katalogowe - w których określa się maksymalny zakres dopuszczalnych operacji użytkowników katalogu.

Ostatnim z wyróżnionych mechanizmów ochrony informacji jest nadawanie atrybutów plikom i katalogom. Atrybuty przydziela się zbiorom i są one jednakowe dla wszystkich użytkowników (przykładowo - plik tylko do odczytu lub systemowy, nie może być kopiowany).

Sterowanie przepływem informacji powinno ustalać legalne kanały dla transmisji danych i zabezpieczeniem przed nieusankcjonowanym dostępem. Szerokie wykorzystanie niezabezpieczonej techniki informatycznej, faktycznie prowadzi do niezamierzonej *emisji ujawniającej*. Niecelowym wówczas jest stosowanie metod przedstawionych powyżej, gdyż informacje przesyłane mogą być ujawnione przez tzw. niebezpieczne środki informatyczne.

Emisja ujawniająca jest podstawowym zagrożeniem, jakie niesie za sobą zastosowanie informatyki w procesach przetwarzania i przesyłania informacji niejawnej. W urządzeniu takim jak komputer, promieniują prawie wszystkie elementy, z których się składa (procesor, dysk twardy, stacja dyskietek, klawiatura, monitor). Złe obudowy, odkryte łącza krawędziowe komputerów i urządzeń peryferyjnych (np. drukarek), mogą być antenami emitującymi w czasie przetwarzania danych promieniowanie elektromagnetyczne. Promieniowanie to ma zróżnicowany zasięg i w zależności od zastosowanych elementów zawiera się w granicach 50 - 1500 m. Istnieją udokumentowane przypadki przechwytywania przez specjalne urządzenia oddalone nawet o kilkaset metrów, informacji wyświetlanych na monitorze lub przekazywanych łączami telefonicznymi[37].

---

[37] W trakcie międzynarodowego zjazdu hackerów w Almere (Holandia), w którym uczestniczyło ponad 2000 osób, prof. E. Moeller z politechniki w Auchen pokazał, jak za pomocą zwykłego telewizora, prostej anteny oraz nieco zmodyfikowanego odbiornika, można bez trudu, z odległości kilkuset metrów, odczytywać dane wyświetlane na monitorze komputera. Odczyt z monitora nie nastręczał żadnych trudności nawet wtedy, kiedy obok siebie pracowało kilka komputerów. Do pokazu wykorzystywano zwykły analogowy, czarno - biały telewizor bez żadnych przeróbek. Przystawka do odbioru wykonana była z powszechnie dostępnych części, a koszt jej wykonania nie przekroczył 2000 DEM [13].

W celu zmniejszenia zasięgu emisji ujawniającej koniecznym jest zastosowanie odpowiednich przedsięwzięć takich jak:

– stosowanie tylko sprzętu atestowanego, o obniżonym poziomie emisji, spełniającego wymogi norm krajowych, lub sprzętu wykonanego w technologii TEMPEST;

– stosowanie odpowiednich osłon i kabin ekranujących (w warunkach polowych stosować można metalowe siatki lub namioty z tkaniny ekranującej);

– stosowanie utajnionych linii transmisji danych (łączy światłowodowych);

– stosowanie urządzeń identyfikujących i alarmujących.

Sterowanie wnioskowaniem dotyczy przypadków, kiedy dane o klauzuli „poufne", mogą mieć zmienioną klauzulę na „jawne" i będą udostępnione do szerokiej dystrybucji. Celem sterowania wnioskowaniem powinno być uruchomienie dodatkowych mechanizmów kontroli przepływu tych danych, aby nie doprowadziło do ujawnienia poufnych danych.

Jim Settle, konsultant ds. bezpieczeństwa FBI jest przekonany, że przyszła wojna będzie polegać na blokowaniu dostępu do informacji i wprowadzaniu w błąd strony przeciwnej, przez celowe jej zakłócanie lub ułatwienia w dostępie do fałszywych informacji. Uzyskana w tym zakresie przewaga spełniać może nie tylko funkcje wspomagające walkę zbrojną, ale może również spełniać funkcje odstraszania. Już dziś, postrachem wszystkich użytkowników sieci i systemów komputerowych są bardzo skuteczne narzędzia, które umożliwiają zdalne wprowadzanie wirusów komputerowych, dostosowanych programowo do samopowielania się i szybkiego rozprzestrzeniania w sieciach informatycznych.

Ogromne znaczenie w zakłócaniu informatycznym mogą mieć również tak zwane bomby logiczne, które jako odpowiednio opracowane aplikacje programowe, będą dostosowane do uaktywniania się na określone wcześniej sygnały lub według zaprogramowanych reżimów czasowych[38].

[38] Eksplozja bomby logicznej to aktywacja nowych funkcji elementu logicznego lub komputera, które prowadzą do zniszczenia lub zdeformowania sprzętu i oprogramowania. Jedną z odmian współczesnej bomby logicznej jest tak zwany *koń trojański*, który umożliwia potajemne wnikanie do baz danych i wydobywa-

Wprowadzenie ich do sieci przeciwnika, może paraliżować jego systemy łączności, zaopatrzenie i transport, a nawet dopływ energii elektrycznej i w następstwie tego - działanie w obszarze operacji lub w danym regionie.

Współczesne narzędzia walki informatycznej, stwarzają możliwości podejmowania skutecznej działalności ukierunkowanej na sterowanie procesami decyzyjnymi przeciwnika, nie tylko w skali taktycznej czy operacyjnej, ale nawet w skali strategicznej. Skoro systemy obrony większości państw oparte są na systemach komputerowych, wprowadzenie do nich złożonych zbiorów precyzyjnie dobranych prawdziwych i sfałszowanych danych, może tworzyć z góry zaplanowane nastroje społeczne i klimat polityczny, które w efekcie spowodują podejmowanie decyzji zgodnych z oczekiwaniami sprawcy tych manipulacji. Natomiast w skali operacyjnej, przeciwnik może nie być zdolny do podjęcia jakichkolwiek działań.

Inną metodą zakłócania jest wprowadzenie tzw. „konia trojańskiego". Wykorzystali to Amerykanie podczas wojny z Irakiem. Mimo embarga, kilka miesięcy wcześniej sprzedali do Iraku drukarki komputerowe, których odbiorcą było wojsko. Wewnątrz drukarek były zainstalowane specjalne nadajniki, które codziennie podawały swoją pozycję do przelatującego satelity. Zlokalizowane w ten sposób cele wojskowe bez przeszkód bombardowano.

2.1.2.2. Zakłócanie rozpoznania studyjnego

Panuje powszechnie przekonanie, że prowadzenie rozpoznania związane jest tylko z działalnością określonych elementów rozpoznawczych. Takie podejście jest wielkim uproszczeniem, bowiem na każdym szczeblu dowodzenia, występują zarówno elementy rozpoznawcze jak i sztabowe komórki rozpoznania, zajmujące się przetwarzaniem i opracowywaniem danych rozpoznawczych. Praca, jaka odbywa się w komórkach sztabowych, polega na scalaniu w jedną całość fragmentarycznych

---

nie z nich informacji. Wirusy komputerowe, bomby logiczne i „skażone" komputerowe elementy elektroniczne, po zainstalowaniu w broni lub innym sprzęcie, mogą w wybranym przez eksperta momencie, spowodować uszkodzenia i tym samym wyeliminować je z użycia.

danych dostarczanych przez systemy, podsystemy i elementy rozpoznawcze. Działalność ta ma charakter studyjny, stąd też często proces ten określany jest mianem rozpoznania studyjnego[39]. W okresie pokoju rozpoznanie studyjne odgrywa najważniejszą rolę w działalności sztabowych komórek rozpoznawczych. Płynne przejście do działań zbrojnych, zależy od jakości prowadzonego rozpoznania studyjnego właśnie w okresie pokoju.

Z powyższego wynika, że **zakłócanie rozpoznania studyjnego** jest procesem, który ma na celu uniemożliwianie bądź utrudnianie przeciwnikowi przetwarzania danych rozpoznawczych, dostarczanych przez systemy, podsystemy i elementy rozpoznawcze.

Specyfiką zakłócania rozpoznania studyjnego jest to, że nie oddziałuje ono w sposób bezpośredni na system zdobywania danych, lecz uniemożliwia lub utrudnia korzystanie z danych zdobytych przez elementy i systemy rozpoznawcze wojsk przeciwnika, ich sąsiadów i przełożonych. Typowym efektem zakłócania rozpoznania studyjnego jest błędna prognoza zagrożenia (przewidywane warianty działań przeciwnika) przedstawiana dowódcy, sztabowi w procesie planowania operacji. Zakłócanie rozpoznania studyjnego powinno mieć negatywny wpływ na przetwarzanie danych u przeciwnika oraz wytwarzanie informacji przydatnych w procesie przygotowania i prowadzenia działań zbrojnych. Zatem, zakłócanie rozpoznania studyjnego ma dwoisty charakter. Owa dwoistość polega na tym, że powinno obejmować proces zasilania sztabu w dane rozpoznawcze oraz funkcjonowanie ogniwa rozpoznania danego szczebla organizacyjnego (personel, osoby funkcyjne).

Ważną rolę w procesie rozpoznania studyjnego przeciwnika, odgrywają jego banki danych. Od ilości i jakości zgromadzonych danych oraz umiejętnego ich wykorzystania, zależą w znacznej mierze rezultaty pracy sztabowych komórek oraz jednostek (pododdziałów) wydzielających elementy i podsystemy rozpoznawcze.

---

[39] Rozpoznanie studyjne to rodzaj rozpoznania wojskowego, przygotowany pod względem fachowym i technicznym do gromadzenia, analizowania i przetwarzania wszelkich danych rozpoznawczych (najczęściej fragmentarycznych) i na tej podstawie opracowywanie informacji o znacznie większej wartości użytecznej. Niezależnie od uwarunkowań sytuacyjno-czasowych ma ono charakter ciągły. [21;33]

Dlatego w operacji wojsk lądowych, zakłócanie ich funkcjonowania powinno być priorytetowym przedsięwzięciem.

Z przedstawionych uwarunkowań funkcjonowania rozpoznania studyjnego przeciwnika wynika, że jego zakłócanie jest niezmiernie ważnym, ale zarazem bardzo trudnym do realizacji przedsięwzięciem. Jego celem powinno być utrudnianie gromadzenia, wszelkich danych (najczęściej fragmentarycznych), zdobywanych przez system rozpoznania oraz przeciwdziałanie analizie i przetwarzaniu ich w nowe informacje, o znacznie większej wiarygodności i wartości użytecznej. Powinno być prowadzone ciągle, niezależnie od uwarunkowań sytuacyjno-czasowych, zarówno w okresie pokoju, kryzysu jak i czasie wojny.

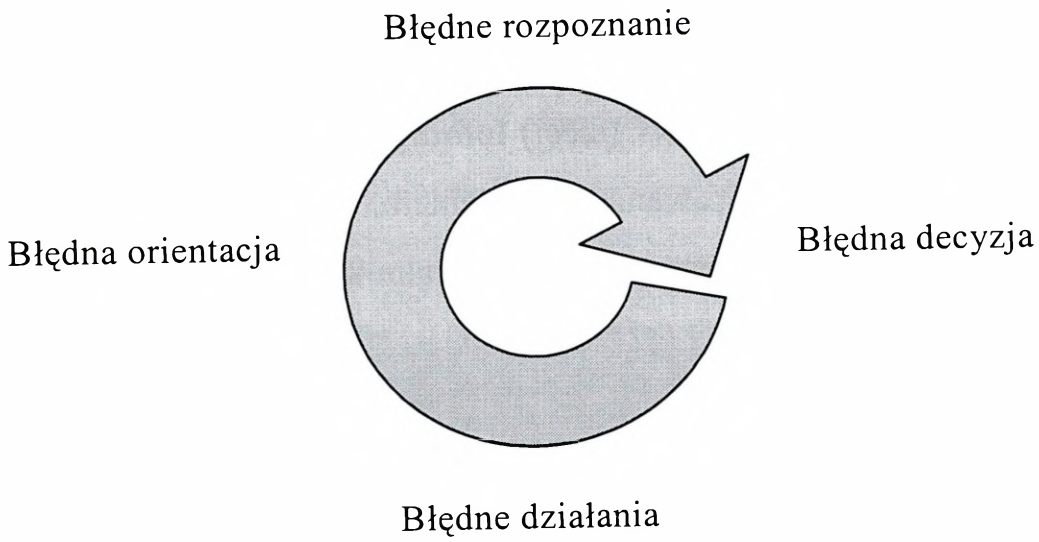
Skuteczność zakłócania rozpoznania studyjnego przeciwnika, uwarunkowana jest między innymi skutecznością działań przeciwrozpoznawczych podejmowanych w ramach maskowania. W tym celu, powinny być wykorzystywane wszystkie dostępne na szczeblu operacyjnym jego formy, to znaczy pozorowanie, dezinformowanie i ukrywanie. Szczególna uwaga powinna być zwrócona na proces gromadzenia informacji o naszych wojskach, który jak wiadomo obejmuje: zbieranie, rejestrację, selekcję i przechowywanie informacji. Do jego zakłócania należy wykorzystać cały arsenał środków zaprezentowany w poprzednich podrozdziałach, lecz ukierunkowany na wprowadzenie w błąd organów sztabowych przeciwnika, zmylenia ich, co do zdolności bojowej, morale i inwencji własnych sił, a w szczególności:

- prowokowanie przeciwnika do podejmowania działań, które w istocie będą dla niego niekorzystne;
- przeciążanie grup analizy danych przeciwnika nadmiarem bezwartościowych danych;
- sugerowanie przeciwnikowi określonych wzorców zdarzeń, które powodować będą małą skuteczność jego działań;
- obniżanie zdolności bojowej przeciwnika na skutek występowania opóźnień lub podejmowania niewłaściwych działań.

Aby zakłócanie odniosło pożądany skutek należy dążyć do stanu, w którym przeciwnik:

- nie będzie w stanie odróżnić danych prawdziwych od fałszywych;
- po analizie sytuacji, oceni działania mylące jako prawdziwe;
- podejmie działania przeciwko pozorowanym celom i sytuacjom.

Efekty tego rodzaju działania można zobrazować w postaci tzw. „błędnego koła" (rysunek 2.26),



Rys. 2.26. Model „błędnego koła"

w którym:

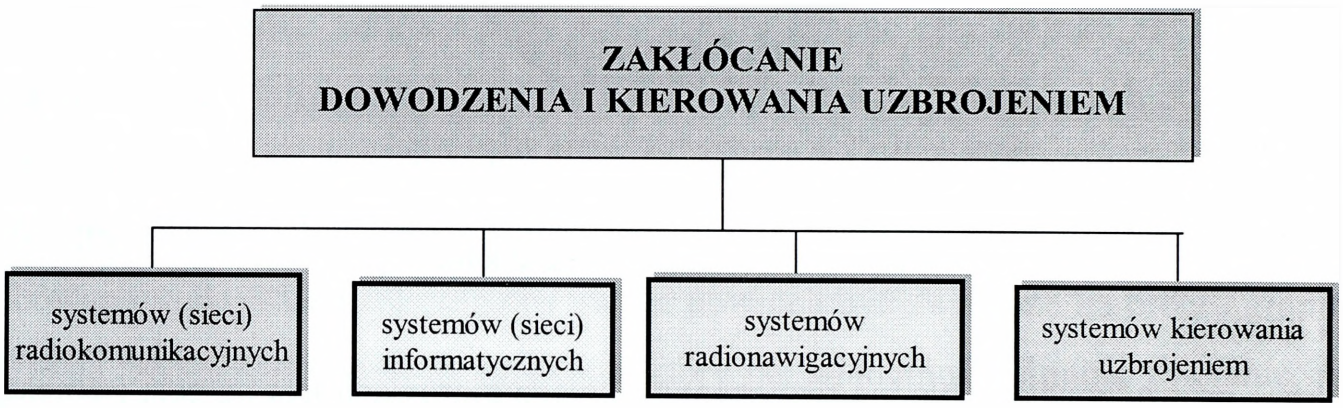
- prowadzone jest błędne rozpoznanie (uwaga kierowana jest na cele i obiekty pozorne);
- istnieje błędna (zła) orientacja w sytuacji na polu walki;
- podejmowane są błędne (niewłaściwe) decyzje;
- prowadzone błędne działania są niekorzystne dla przeciwnika.

W okresie pokoju, ważną rolę odgrywają organizowane ćwiczenia z udziałem obserwatorów zagranicznych, gdzie powinny być wykorzystane aplikacyjne warianty działania naszych wojsk. Wnioski z takich ćwiczeń powinny budzić wątpliwości i podważać prawdziwość dotychczasowych opracowań, komunikatów, meldunków czy zestawień organów rozpoznawczych przeciwnika[40] lub utwierdzać w przekonaniu o ich poprawności, jeśli stwierdzimy, że określone zbiory opracowanych informacji rozpoznawczych są błędne.

[40] W okresie pokoju opracowywane są odpowiednie wzorce doktrynalne, natomiast w okresie działań wojennych możliwa jest ich weryfikacja (na podstawie systematycznie powtarzających się informacji o stosowanych środkach walki lub rozwiązaniach taktyczno-operacyjnych).

2.2. Zakłócanie dowodzenia i kierowania uzbrojeniem

Zakłócanie dowodzenia i kierowania uzbrojeniem stanowi – zdaniem zespołu autorskiego - zespół skoordynowanych elementów dostosowany do wnoszenia entropii informacyjnej[41] do procesów dowodzenia wojskami przeciwnika i procesów kierowania jego uzbrojeniem, które realizowane są przy pomocy: systemów (sieci) radiokomunikacyjnych, systemów (sieci) informatycznych, systemów radionawigacyjnych oraz systemów kierowania uzbrojeniem. Podział zakłócania dowodzenia i kierowania uzbrojeniem zilustrowano na rysunku 2.27.



Rys. 2.27. Podział zakłócania dowodzenia i kierowania uzbrojeniem

2.2.1. Zakłócanie systemów (sieci) radiokomunikacyjnych

Zakłócanie systemów (sieci) radiokomunikacyjnych polega na celowym promieniowaniu zakłócającej energii elektromagnetycznej powodującej utrudnienie pracy elektronicznych środków łączności radiowej KF i UKF, łączności radiolinio-wej (horyzontowej i pozahoryzontowej) oraz radiosatelitarnej przeciwnika.

W wyniku zakłócania można utrudnić lub uniemożliwić pracę jednego urządzenia, kilku lub kilkunastu, a nawet całego systemu łączności określonego szczebla

dowodzenia. Ten rodzaj zakłócania jest najbardziej ekonomicznym a zarazem skutecznym sposobem dezorganizacji pracy systemów radiokomunikacyjnych przeciwnika. Może uniemożliwić odbiór sygnałów, pogorszyć słyszalność, spowodować nieprawidłowe działanie urządzeń końcowych, wprowadzić w błąd operatorów lub zwiększyć błędy urządzeń automatycznych.

Zakłócanie systemów radiokomunikacyjnych odbywa się przy pomocy specjalnych nadajników stacjonarnych lub mobilnych stacji: przewoźnych, powietrznych (samolotowych ,śmigłowcowych) i okrętowych. Wyróżnia się również nadajniki zakłócające jednorazowego użytku[42], które mogą być przenoszone jako specjalna amunicja artyleryjska lub urządzenia zrzucane z samolotu lub śmigłowca bądź rozmieszczae przez grupy dywersyjno-rozpoznawcze. Bardzo ważną rolę w **procesie zakłócania systemów radiokomunikacyjnych odgrywa dobór parametrów sygnału zakłócającego do sygnału zakłócanego**. Powinien on być dokonywany według kryteriów zilustrowanych na rysunku 2.28.

Ze względu na szerokość zakłócanego pasma:

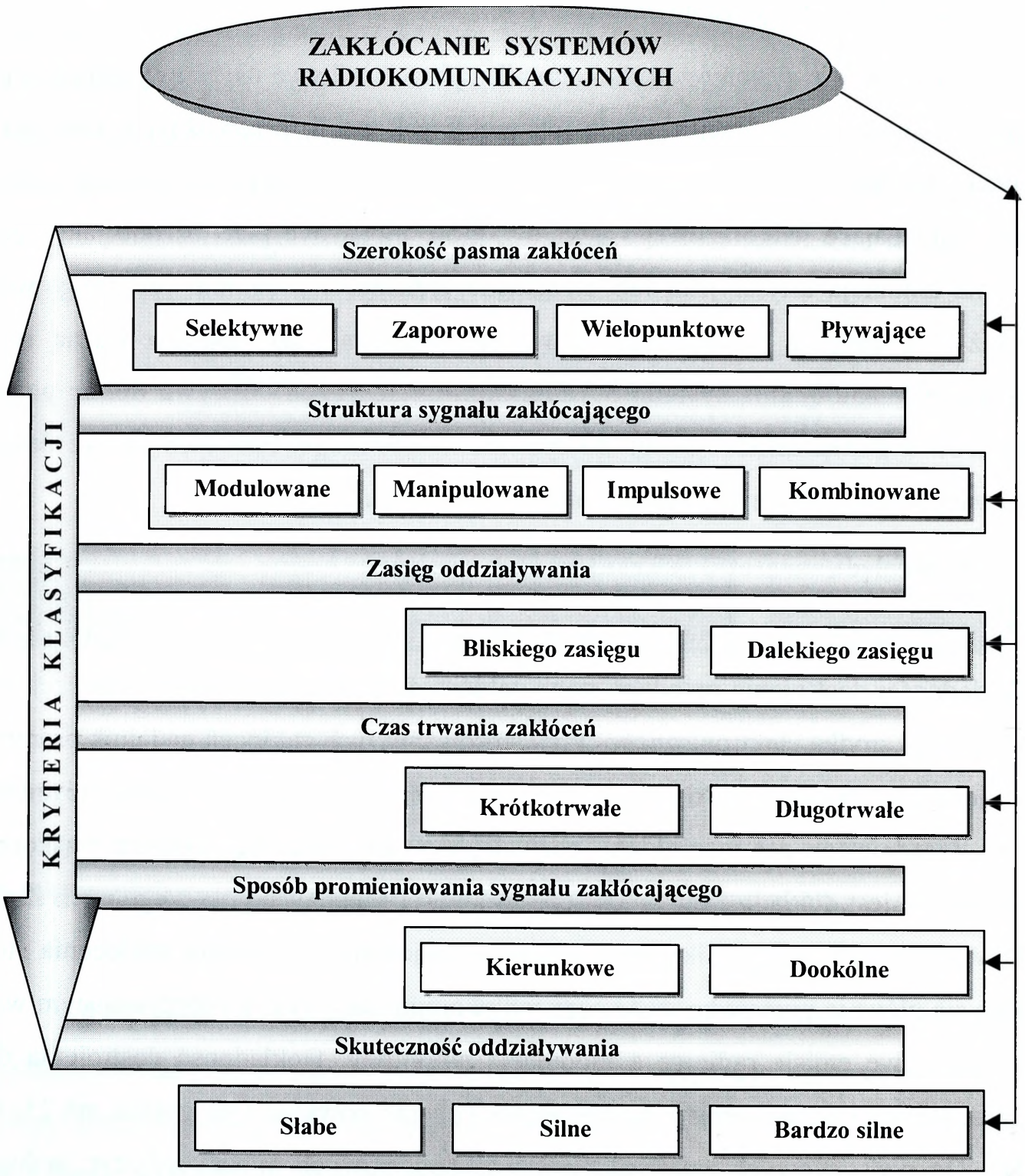
– Zakłócenia selektywne (waskopasmowe, punktowe), które wymagają dużej dokładności dostrojenia urządzeń stacji zakłócającej do częstotliwości roboczej zakłócanego środka elektronicznego. Przy stosowaniu tych zakłóceń nadajnik promieniuje sygnał zakłócający o szerokości pasma optymalnej do zakłócanego urządzenia. Zasadniczym zaś warunkiem, pozwalającym na realizację zakłóceń wąskopasmowych, jest dokładna znajomość częstotliwości roboczych poszczególnych środków radiowych przeciwnika. W działalności bojowej tego rodzaju zakłócenia stosuje się głównie przeciwko systemom radiokomunikacyjnym wykorzystującym wąskopasmowe emisje radiowe z modulacją amplitudy. Dokładność dostrojenia do częstotliwości nośnej emisji wąskopasmowych nie powinna być gorsza niż 15-30 Hz. Do podstawowych zalet zakłóceń wąskopasmowych można zaliczyć maksymalny zasięg zakłóceń (cała moc zakłóceń przypada na częstotliwość zakłócaną)

---

[41] Stany nieuporządkowania i chaosu wprowadza się w wyniku prowadzenia: dezinformacji, zagłuszania i niszczenia – patrz rozdział 1.

[42] Szczegółowy opis nadajników zakłócających znajduje się w literaturze przedmiotu.

oraz minimalny wpływ na pracę własnych stacji. Spośród wad wyróżnia się: konieczność rozpoznania zakłócanych emisji; łatwość uniknięcia zakłóceń selektywnych; wymagana znajomość zakłócanej częstotliwości; mało efektywne wykorzystanie środków zakłócających.



Rys. 2.28. Kryteria doboru zakłóceń radiokomunikacyjnych

– Zakłócenia zaporowe (szerokopasmowe), które stosowane są do jednoznacznej dezorganizacji pracy kilku a nawet kilkudziesięciu środków radiowych. Za po-

mocą specjalnych nadajników szerokopasmowych lub nadajników zakłócających jednorazowego użycia można prowadzić zagłuszanie całych podzakresów częstotliwości wykorzystywanych przez przeciwnika.

Zakłócenia zaporowe stosuje się m.in. w wypadku słabego rozpoznania spektrum elektromagnetycznego wykorzystywanego przez przeciwnika. Są one stosowane do zagłuszania całych systemów radiokomunikacyjnych, a ich celem jest uniemożliwienie przeciwnikowi korzystania z częstotliwości roboczych położonych w określonym paśmie (podzakresie). Podstawowymi zaletami zakłóceń zaporowych są: efektywne oddziaływanie przeciwko zmiennym częstotliwościowo źródłom emisji; wymagają minimalnego sterowania; mogą być wykorzystane do zakłócania wielu sygnałów; zmuszają do rekonfigurowania rozbudowanych sieci łączności. Spośród wad można wyróżnić: duża nieefektywność wykorzystania mocy nadajników, która rozkłada się proporcjonalnie na wszystkie częstotliwości zakłócanego pasma; duże prawdopodobieństwo zakłócenia pracy własnych stacji.

– Zakłócenia wielopunktowe są wykorzystywane do zakłócania pojedynczych częstotliwości. Ich główną zaletą jest zwiększona efektywność zakłócania w porównaniu z zakłócaniem selektywnym (punktowym).

– Zakłócenia pływajace polegają na punktowo-zaporowym przemieszczaniu (przemiataniu) energią zakłócającą po zakłócanych częstotliwościach. Podstawowymi zaletami zakłóceń pływających są: efektywne użycie zakłóceń przeciwko sieciom wieloczęstotliwościowym; cała moc sygnału zakłócającego jest skupiona w danej chwili na jednej częstotliwości; maksymalny zasięg zakłóceń; możliwość sterowania własnymi stacjami w celu uniknięcia zakłóceń interferencyjnych. Spośród wad można wyróżnić skomplikowaną konstrukcję urządzenia.

Ze względu na strukturę sygnału zakłócającego:

– Zakłócenia modulowane (szumowe) są to drgania wielkiej częstotliwości modulowane amplitudowo, częstotliwościowo lub fazowo. Jednym z bardziej rozpowszechnionych rodzajów zakłóceń modulowanych są zakłócenia szumowe, charakteryzujące się przypadkowymi zmianami napięcia modulującego. Zakłócenia te

są otrzymywane przez modulację drgań wielkiej częstotliwości sygnałem szumowym. Zakłócenia szumowe mogą być stosowane w celu dezorganizacji pracy różnych rodzajów pracy radiostacji, a przede wszystkim pracy fonicznej.

– Zakłócenia manipulowane są drganiami wielkiej częstotliwości manipulowane ręcznie lub automatycznie amplitudowo, częstotliwościowo lub fazowo. Stosowane są najczęściej do zakłócania wąskopasmowych emisji telegraficznych z manipulacją amplitudy lub częstotliwości.

– Zakłócenia impulsowe są postępującymi po sobie krótkotrwałymi sygnałami zakłócającymi, modulowanymi czasem trwania impulsu, amplitudą, częstotliwością, fazą lub kilkoma parametrami jednocześnie. Zakłócenia te charakteryzują się bardzo krótkim czasem promieniowania energii (rzędu mikrosekund). Są to emisje modulowane ciągami impulsów, wytworzonymi przez nadajnik zakłócający i wypromieniowane na częstotliwościach zakłócanych środków elektronicznych. Jeśli częstotliwość i faza zakłóceń pokrywa się z częstotliwością i fazą zakłócanej stacji, mamy do czynienia z zakłóceniami synchronicznymi. Jeżeli natomiast te parametry się nie pokrywają, ma się do czynienia z zakłóceniami impulsowymi asynchronicznymi. Zakłócenia te mogą być odzewowe (jednokrotne lub wielokrotne) albo niezależne (nie odzewowe). Zakłócenia impulsowe są wykorzystywane do zakłócania środków pracujących impulsowo, np. radiostacji nowej generacji, stacji radiolokacyjnych, cyfrowych stacji radioliniowych, urządzeń radiotelesterowania rakietami itp.

– Zakłócenia kombinowane są to drgania wielkiej częstotliwości modulowane i manipulowane równocześnie kilkoma sposobami, na przykład impulsowe zakłócenia radiowe w połączeniu z szumową modulacją amplitudy. Tego rodzaju zakłócenia stosowane są głównie do naruszania pracy środków radioliniowych oraz radiotelegrafii z przesuwem częstotliwości.

Ze względu na zasięg działania:

– Zakłócenia bliskiego zasięgu zapewniają skuteczną dezorganizację pracy środków elektronicznych przeciwnika na odległość do 10 km od miejsca pracy nadajnika lub stacji zakłócającej. Występują m.in. podczas użycia nadajników zakłó-

cających jednorazowego użytku, autonomicznych środków zakłócających statków powietrznych oraz niektórych środków wykorzystywanych na szczeblu taktycznym.

– Zakłócenia dalekiego zasięgu zapewniają skuteczne zagłuszanie i dezorganizację pracy środków elektronicznych przeciwnika na odległość powyżej 10 km (nawet do kilkuset kilometrów). Takie zasięgi zakłóceń uzyskuje się wykorzystując naziemne i powietrzne stacje dużej mocy.

Ze względu na czas trwania:

– Zakłócenia krótkotrwałe prowadzone są w czasie równym, a nawet krótszym od czasu nadawania jednego lub kilku sygnałów przeciwnika.

– Zakłócenia długotrwałe polegają na zakłócaniu pracy elektronicznych środków elektronicznych w czasie od kilkunastu minut do kilku godzin. Występują m.in. przy wykorzystaniu nadajników zakłócających jednorazowego użytku.

Ze względu na sposób promieniowania:

– Zakłócenia dookólne występują wówczas, gdy promieniowanie anteny odbywa się we wszystkich kierunkach z jednakową mocą. Stosuje się je wówczas, gdy nie są znane miejsca rozmieszczenia zakłócanych środków. Anteny dookólne są stosowane w nadajnikach zakłócających jednorazowego użytku i często w stacjach pracujących w ruchu. Ujemną cechą zakłóceń dookólnych jest stosunkowo niski poziom gęstości energii wynikający ze znacznego jej rozproszenia.

– Zakłócenia kierunkowe występują wtedy, gdy energia elektromagnetyczna jest promieniowana przez antenę stacji zakłócającej o specjalnie dobranej charakterystyce, w kierunku zakłócanego środka elektronicznego przeciwnika. Dzięki kierunkowości anten gęstość energii zakłócającej w punkcie odbioru jest znacznie większa niż przy antenach dookólnych. Chcąc stosując tego typu zakłócenia należy znać miejsca rozmieszczenia zakłócanych środków przeciwnika. Zakłócenia kierunkowe zwiększają efektywność wykorzystania mocy nadajnika. Stosowanie takich zakłóceń jest konieczne w przypadku zagłuszania znacznie oddalonych urządzeń oraz wykorzystujących złożone struktury sygnału.

Ze względu na skuteczność[43] działania:

– Zakłócenia słabe są to takie zakłócenia, przy których natężenie pola elektrycznego sygnału zakłócającego (E_z) w punkcie odbioru u przeciwnika, jest większe od natężenia sygnału użytecznego (E_s) i przewyższa je średnio o 3-5 %. Przy tego rodzaju zakłóceniach poziom zakłóceń w punkcie odbioru sygnału użytecznego powoduje utratę lub obniżenie wiarygodności przesyłanych danych w granicach 5-15%. Oznacza to, że w wypadku stosowania słabych zakłóceń występują tylko pewne zniekształcenia przekazywanych danych. W relacjach łączności utrudniony jest odbiór telegramów lub prowadzenie bezpośrednich rozmów. W większości wypadków odbiór jest możliwy przez doświadczonego operatora (oficera sztabu) przygotowanego do pracy w warunkach zakłóceń. Istnieje potrzeba powtarzania transmisji w granicach 10-15%.

– Zakłócenia silne są to takie zakłócenia, przy których natężenie pola elektrycznego sygnału zakłócającego w punkcie odbioru po stronie przeciwnika jest większe o 5-15 % od natężenia pola elektrycznego sygnału użytecznego środka elektronicznego przeciwnika. Tego typu zakłócenia powodują utratę lub obniżenie wiarygodności danych od 15 do 50 %. Oznacza to, że w relacjach łączności będzie poważnie utrudniony odbiór, a nawet utrata znacznej części danych. W najnowszych systemach może dojść do zerwania synchronizacji sieci a w konsekwencji dezorganizacja ich pracy.

Zakłócenia bardzo silne zakłócenia (tłumiace) są to takie zakłócenia, przy których natężenie pola elektrycznego sygnału zakłócającego w punkcie odbioru po stronie przeciwnika jest ponad 50% wyższe od natężenia pola elektrycznego sygnału użytecznego. Tak wysoki poziom zakłóceń powoduje zerwanie łączności i całkowitą utratę danych.

---

[43] Skuteczność zakłóceń to zdolność do pozbawienia przeciwnika możliwości odbioru danych przesyłanych przez jego środki łączności. Polega na dostarczeniu do zakłócanego urządzenia odbiorczego takiej porcji energii zakłócającej, która przy jego parametrach technicznych, rodzaju pracy oraz warunkach taktycznych, uniemożliwi poprawne odebranie sygnału użytecznego. W zależności od rodzaju zakłócanego systemu (środka) radiokomunikacyjnego, przy jej ocenie należy uwzględniać różne czynniki.

Realizując proces zakłócania systemów radiokomunikacyjnych przeciwnika należy zawsze dążyć do tego, aby zapewnić takie warunki techniczne i organizacyjne, które umożliwią właściwą skuteczność i efektywność tego procesu oraz stworzą warunki do osiągnięcia celów i zadań w aktywnej i ofensywnej walce z systemami elektronicznymi przeciwnika.

Problematyka oceny skuteczności zakłócania systemów (sieci) radiokomunikacyjnych na częstotliwościach ustalonych szczegółowo przedstawiona została przez autorów w licznych opracowaniach [20;22;35;58]dotyczących walki radioelektronicznej[44].

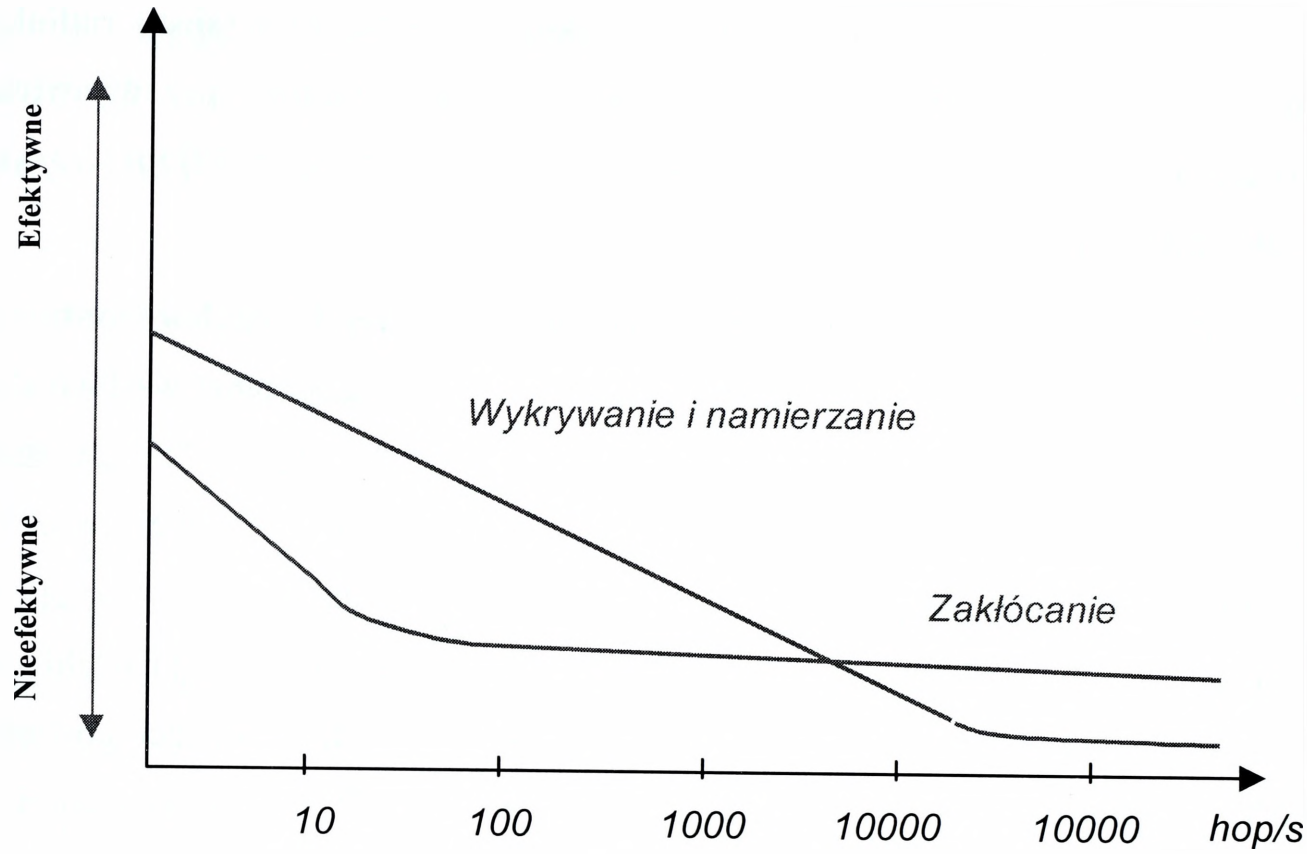
Zakłócanie łączności radioliniowej (horyzontowej i pozahoryzontowej) oraz radiosatelitarnej związane jest z koniecznością uwzględniania wąskich charakterystyk kierunkowych anten stacji odbiorczych. Jeżeli antena odbiorcza stacji skierowana jest w stronę przeciwną do stacji zakłócającej, to skuteczne naruszenie jej pracy może być zapewnione tylko przy pomocy nadajników zakłócających o dużej mocy. Najwyższą skuteczność zakłóceń łączności radioliniowej i satelitarnej osiąga się przy pomocy stacji zakłócających zainstalowanych na statkach powietrznych (śmigłowcach, samolotach). Stacje takie o mocy 50-200 W, w zależności od lotu samolotu (śmigłowca), są w stanie skutecznie zdezorganizować pracę środków radioliniowych na głębokość do 200 km.

Z kolei o **odporności na zakłócanie radiokomunikacyjnych urządzeń wykorzystujących emisje rozproszone** (a także wykrywanie i namierzanie) decydują ich charakterystyczne parametry. Zalicza się do nich m.in.: wykorzystywane pasmo (zakres) rozproszenia, liczbę i zestaw częstotliwości skaczących, częstość zmian, system synchronizacji, pseudolosowe kodowanie zmian częstotliwości itp. Podatność na zakłócenia determinowana jest w zasadzie przez wykorzystywane pasmo częstotliwości oraz liczbę i zestaw częstotliwości skaczących. Szerokość stosowanego pasma rozproszenia stwarza problem polegający na zabezpieczeniu odpowied-

---

[44] W siłach lądowych USA ocena skuteczności zakłóceń łączności radiowej UKF i KF na fali przyziemnej dokonywana jest przy pomocy zbliżonego aparatu matematycznego zamieszczonego w Communications Jamming Handbook FM 34-40-7. Dużą pomoc świadczą także: podręczny kalkulator GTA 30-6-5 oraz zestaw szablonów ang. The Jampot Fan będące w wyposażeniu komórek WE.

niej gęstości mocy sygnału zakłócającego w całym zakresie częstotliwości. Liczba i zestaw częstotliwości może mieć natomiast wpływ na efektywność zastosowania zakłóceń wielopunktowych i pływających (śledzących). Szybkość zmian częstotliwości w paśmie stanowi większy problem dla rozpoznania i namierzania radiowego niż dla zakłóceń co ilustruje rysunek 2.29.



Rys. 2.29. Wpływ częstotliwości skoków na efektywność zakłócania (rozpoznania i namierzania)

Jak wynika z rysunku, skuteczność zakłóceń śledzących maleje dopiero powyżej 10000 zmian częstotliwości na sekundę a jej efektywność jest większa dla małej szybkości zmian częstotliwości i zmniejsza się wraz z jej wzrostem.

W celu zakłócania sygnału szerokopasmowego można stosować wszystkie metody zakłóceń: zakłócenia selektywne, wielopunktowe, zaporowe i pływające.

Przy zastosowaniu **zakłóceń wąskopasmowych i wielopunktowych** wyróżnia się dwie metody postępowania:

1. Eliminowanie kanałów wykorzystywanych do realizacji skoków;
2. Uniemożliwienie synchronizacji początkowej w sieci.

Pierwszą metodę realizuje się wykorzystując system nadajników zakłócających emitujących zakłócenia wąskopasmowe lub wielopunktowe. W tym przypadku konieczne jest wcześniejsze ustalenie pasma[45], w którym zakłócana radiostacja pracuje oraz na jakich częstotliwościach odbywają się skoki. Następnie należy wykorzystać taką liczbę nadajników zakłócających, żeby wyeliminować przynajmniej 50% zajmowanych częstotliwości. Metoda ta jest mało efektywna i organizacyjnie trudna do zrealizowania.

Bardziej celowym jest wykorzystanie zakłóceń selektywnych do uniemożliwienia synchronizacji w sieci. Sygnał synchronizacji wstępnej emitowany jest na stałej częstotliwości i trwa z reguły kilka sekund. Pozwala to, przy zastosowaniu odpowiednio szybkiej stacji zakłóceń wykryć tę emisję i zakłócić (zerwać) synchronizację sieci. Istotną wadą tej metody jest fakt, że synchronizacja początkowa w sieci FH jest realizowana tylko w momencie jej uruchamiania, stąd występuje bardzo rzadko. Współczesne radiostacje FH, po dokonaniu synchronizacji, mogą utrzymywać ten stan przez kilka dób. Poza tym radiostacje posiadają możliwość zaprogramowania kilku systemów podziału częstotliwości sieci. Mogą więc stosunkowo szybko przejść do pracy na innym zestawie częstotliwości, bez konieczności ponownej synchronizacji.

Zakłócenia szerokopasmowe są – obecnie - najodpowiedniejszym sposobem zakłócania emisji FH. Wynika to z możliwości wytworzenia przez stację sygnału zakłócającego o stosunkowo szerokim paśmie częstotliwości (12 MHz). Poważną wadą jest natomiast duże rozproszenie mocy i możliwość zakłócania własnych radiostacji pracujących w tym paśmie. Pewnym rozwiązaniem problemu jest podzielenie pasma na kilka podzakresów, które można zakłócać przez odpowiedni zestaw nadajników zakłócających jednorazowego użytku. Zakresy podziału można dobrać w taki sposób, aby osiągnąć zakładany poziom skuteczności zakłóceń, tzn. odpowiedni poziom gęstości mocy w całym zakłócanym paśmie częstotliwości. W stosunku do emisji rozproszonych najlepsze efekty zakłóceń dają sygnały o strukturze

---

[45] W radiostacjach ze skokową zmianą częstotliwości jak standard przyjmuje się pasmo 12 MHz (± 6 MHz od częstotliwości środkowej).

szumu. Odpowiednio wysoki poziom szumu w kanale szerokopasmowym, utrudni układowi decyzyjnemu odbiornika sygnałów FH podjęcie prawidłowej decyzji o odebranym sygnale. Praktyka dowiodła, że zakłócanie szumem emisji rozproszonych umożliwia uzyskanie wymaganej skuteczności zakłóceń.

Wytworzenie zakłóceń pływających (śledzących) tj. przemieszczających się w określonym paśmie umożliwia zakłócanie relacji FH poprzez wyeliminowanie pewnej liczby aktywnych kanałów częstotliwości. Metoda ta zapewnia osiągnięcie w zakłócanej emisji określonej wartości prawdopodobieństwa błędu przy dostatecznej liczbie zakłócanych kanałów. Umożliwiłoby to wykorzystanie stacji zakłócających, które umieszczałyby swoje emisje zakłócające w przydzielonym im paśmie, jednocześnie przemiatając je emisją zakłócającą w sposób płynny lub skokowy. Podobnie jak przy zakłóceniach szerokopasmowych, korzystnym byłoby podzielenie całego zakłócanego pasma na kilka podpasm, i przydzielenie ich kilku nadajnikom zakłócającym. Nadajniki takie po wykryciu emisji FH powinny przystąpić do zakłóceń, przemiatając przydzielone podpasmo częstotliwości z szybkością zbliżoną do zmian częstości skoków w emisji FH lub większą. Ta metoda zakłóceń wydaje się być równie efektywna jak zakłócenia szerokopasmowe.

Technicznie możliwe jest skonstruowanie typowej śledzącej stacji zakłócającej, która podążałaby za zmianami częstotliwości sygnału FH z taką szybkością, że zakłócenia byłyby skuteczne. Jednak, w przypadku wykorzystania przez przeciwnika, używającym większej ilości stacji pracujących w systemie FH, zakłócenia te mogą okazać się mało skuteczne. Wewnątrz zakłócanego pasma, oprócz sygnału zakłócanej sieci będą znajdowały się podobne sygnały pochodzące od radiostacji pracujących w innych sieciach. Może to spowodować, że algorytm poszukiwania i śledzenia transmisji okaże się nieefektywny i urządzenie zakłócające nie będzie w stanie skutecznie jej zakłócić. Skuteczność zakłóceń wzrośnie, gdy zakłócany sygnał będzie wyróżniał się spośród pozostałych sygnałów np. większą mocą.

Uogólniając, należy stwierdzić że zakłócanie urządzeń wykorzystujących emisje rozproszone w szerokim paśmie jest stosunkowo trudne. Niemniej jednak, przy wykorzystaniu odpowiednich środków, szczególnie szerokopasmowych stacji za-

kłóceń o dużej mocy sygnału, NZJU oraz stacji z pływającym (śledzącym) sygnałem, możliwe jest uzyskanie zadowalających efektów zakłócania.

2.2.2. Zakłócanie systemów (sieci) informatycznych

Z badań wynika, że zakłócanie stosowane w odniesieniu do systemów (sieci) informatycznych przeciwnika przyjmuje najczęściej formę złośliwego oprogramowania, które powoduje blokowanie dostępu do zbiorów danych, wymazanie w krótkim czasie ich dużej liczby, spowalnianie pracy programów użytkowych itp. Wielu specjalistów uważa, że przyszła wojna będzie polegała na blokowaniu dostępu do prawdziwych danych i wprowadzaniu w błąd strony przeciwnej przez celowe ułatwienia w dostępie do danych fałszywych. Twierdzi się, że w odróżnieniu od broni jądrowej, narzędzia zakłócania informacyjnego są w zasięgu materialnych możliwości prawie każdego państwa. Ich użycie umożliwia dezorganizację pracy systemów informatycznych przeciwnika do tego stopnia, że nie będzie on zdolny do podejmowania racjonalnych działań. Biorąc pod uwagę fakt, że systemy obrony większości państw oparte są na systemach informatycznych, aby przeprowadzić skuteczny atak, wystarczy zakłócić ich pracę przy pomocy odpowiedniego, złośliwego oprogramowania.

Złośliwym programem nazywa się specjalne kody wyrządzające szkody w urządzeniach i sieciach informatycznych. Niektórzy specjaliści posługują się określeniem *„malware”* (zlepek z ang. *malicious software* – oprogramowanie złośliwe)[46]. Do programów tych należy zliczyć: „wirusy”, „konie trojańskie”, „bomby logiczne”, „robaki komputerowe”, „bakterie” nazywane również „królikami” oraz wiele im podobnych.

Niektóre „wirusy” podejmują działania natychmiast po wprowadzeniu do systemu, a niektóre wprowadzone są w postaci odpowiednio zaszyfrowanej lub uśpio-

---

[46] Garfinkel S., Spafford G.: *„Bezpieczeństwo w Unixie i Internecie”*, Warszawa 1997, s. 31.

nej. Charakteryzują się tym, że po wprowadzeniu do systemu komputerowego podejmują jedynie działania mające na celu samoreplikację i dotarcie do najistotniejszych elementów systemu. Sygnałem do podjęcia działań destrukcyjnych jest ich aktywacja po określonym czasie lub zaistnieniu określonych warunków w systemie. Celami dla tego rodzaju wirusów są urządzenia komputerowe pracujące w sprzęcie bojowym i zabezpieczeniu logistycznym, ich uruchamianie może nastąpić np. za pomocą sygnału radiowego.

Koncepcja zastosowania **„wirusów komputerowych"** wprowadzonych do systemów informatycznych przeciwnika (ang. CVW - Computer Virus Weapon) w celu zakłócenia pracy systemów dowodzenia i kierowania po raz pierwszy została sprawdzona w czasie wojny w rejonie Zatoki Perskiej.

„Konie trojańskie" otrzymały swoją nazwę ze względu na analogię ze znanym mitem greckim. Są one podprogramami, które (wmontowane w oryginalne programy użytkowe, np. gry, arkusze kalkulacyjne czy edytory) mogą na określony sygnał lub komendę wymazywać bazy danych, formatować dyski itp. Użytkownik może na przykład myśleć, że program jest grą. W czasie gdy program wyświetla komunikat o tym, że aktualizuje bazy danych, bądź zada pytanie w stylu „jaki wybierasz poziom zaawansowania?", program może w tym czasie faktycznie usuwać pliki, formatować dysk czy w inny sposób modyfikować dane. Inną metodę wprowadzenia „konia trojańskiego" wykorzystali Amerykanie podczas wojny z Irakiem. Przed nałożeniem embarga, sprzedali do Iraku drukarki komputerowe, których odbiorcą było wojsko. Wewnątrz drukarek były zainstalowane specjalne nadajniki, które codziennie podawały swoją pozycję do przelatującego satelity. Zlokalizowane w ten sposób cele wojskowe precyzyjnie i bez przeszkód bombardowano.

„Bomby logiczne" są najczęściej „podkładane" w programach przez informatyków, którzy mają legalny dostęp do systemu. Impulsem wyzwalającym „wybuch bomby" może być obecność odpowiednich plików, określona data, wybrany dzień tygodnia czy jakiś użytkownik uruchamiający aplikację. Odpalona bomba logiczna może zniszczyć lub zniekształcić dane, spowodować zatrzymanie pracy komputera lub w inny sposób zniszczyć system. Bomby logiczne mają podobne działanie jak

powszechnie wykorzystywane zabezpieczenia, które mogą np. uniemożliwiać korzystanie z oprogramowania z chwilą utraty ważności licencji użytkownika.

„Robaki komputerowe" to programy, które mogą działać samodzielnie, a których zadaniem jest rozprzestrzenianie się za pośrednictwem połączeń sieciowych. Możliwa jest taka sytuacja, w której poszczególne części jednego robaka będą działać w różnych komputerach sieci. Same robaki nie zmieniają innych programów, ale mogą przenosić złośliwe kody, które dokonują zmian. Podstawowym zadaniem robaków komputerowych jest wypełnianie pamięci komputerów taką ilością zupełnie przypadkowo generowanych danych, że prowadzi to do istotnego spowolnienia pracy sieci lub wręcz do całkowitego jej zablokowania.

„Bakterie", zwane również „królikami", to programy, które nie uszkadzają plików wprost. Ich jedynym zadaniem jest rozmnażanie. Typowy program – bakteria lub program – królik może nie robić nic innego niż dzielić się na dwie kopie i uruchamiać je w środowisku zasobów. Może też tworzyć dwa nowe pliki, z których każdy jest kopią programu wyjściowego. Oba nowe programy będą się następnie dalej mnożyły, tworząc kolejne „potomstwo". Bakterie reprodukują się wykładniczo i zajmują ogromną ilość czasu procesora, pamięci, przestrzeni dyskowej i innych zasobów, przez co użytkownik nie może z nich dalej korzystać.

2.2.3. Zakłócanie systemów radionawigacyjnych

Z badań wynika, że zakłócanie systemów radionawigacyjnych jest zespołem takich celowych i skoordynowanych działań organizacyjnych i technicznych, które uniemożliwią lub utrudnią obiektom ruchomym przeciwnika określenie swojego miejsca położenia w przestrzeni.

Ogólnie systemy radionawigacyjne[47] podzielić możemy na:

– autonomiczne – charakteryzujące się tym, że ich środki radioelektroniczne są tylko wewnątrz poruszających się obiektów i umożliwiają określenie położenia niezależnie od urządzeń zewnętrznych (naziemnych lub kosmicznych). Do urządzeń takich zaliczamy np. radiowysokościomierze i Dopplerowskie stacje radiolokacyjne;

– nieautonomiczne – wykorzystujące odbiorcze lub odbiorczo – zapytujące urządzenia współpracujące z naziemnymi lub satelitarnymi źródłami sygnałów nawigacyjnych.

W przypadku systemów autonomicznych opartych o pokładowe stacje radiolokacyjne możliwości i sposoby zakłócania są identyczne jak w zakłócaniu systemów radiolokacyjnych. Zakłócanie jest zwykle utrudnione ze względu na trudności z wykryciem ich pracy powodowane niewielkim zasięgiem tych stacji radiolokacyjnych i kierunkiem emisji promieniowania elektromagnetycznego, które zwykle skierowane jest pod dużym kątem w dół.

Możliwości i zakres rozpoznania i zakłócania w przypadku systemów nieautonomicznych są zróżnicowane w zależności od zakresu wykorzystywanych częstotliwości i systemu uzyskiwania danych nawigacyjnych. Siły zbrojne wszystkich państw wykorzystują różne nieautonomiczne operacyjno-taktyczne i taktyczne systemy radionawigacyjne.

Ogólnie podzielić je można na systemy bliskiej i dalekiej nawigacji. Każdy z tych rodzajów systemów wymaga odrębnego oddziaływania, inne też są czynniki, które determinują możliwości oraz skuteczność jego zakłócania. Technika zakłócania systemów radionawigacyjnych polega na wprowadzeniu w kanały odbiorcze

---

[47] System radionawigacyjny: 1) zespół współpracujących ze sobą urządzeń radionawigacyjnych rozmieszczonych na ziemi i w obiektach ruchomych (samoloty, okręty), przeznaczony do zabezpieczenia prawidłowego prowadzenia tych obiektów po wyznaczonej trasie, naprowadzania w określone punkty lądowania samolotów bez widoczności, kontroli i regulacji itp.; 2) sposób określania pozycji ruchomego obiektu za pomocą pokładowych urządzeń radionawigacyjnych współpracujących z naziemnymi pomocniczymi urządzeniami radionawigacyjnymi. System radionawigacyjny służy więc ogólnie do określania miejsca położenia obiektów ruchomych (zarówno cywilnych jak i wojskowych) w przestrzeni trójwymiarowej za pomocą urządzeń umieszczonych na tych obiektach i wykorzystaniu urządzeń bazowych o ustalonym w danym momencie czasowym położeniu.

systemów, sygnałów uniemożliwiających określenie współrzędnych. W takich rodzajach systemów jak promieniowy i hiperboliczny, urządzenia odbiorcze znajdują się tylko u użytkownika. W systemach kołowych i kołowo-promieniowych (bliższej radionawigacji), pracujących metodą odzewowych radioodległościomierzy impulsowych, odbiorniki znajdują się zarówno w urządzeniach pokładowych, jak i bazowych.

Radiotechniczny system bliskiej nawigacji to system obejmujący środki radiotechniczne rozmieszczone na lądzie (aparatach latających, okrętach), mające promień działania ograniczony do kilkuset kilometrów. System ten zwykle pracuje na krótkich i ultrakrótkich zakresach fal radiowych, odznacza się stosunkowo duża dokładnością. W przypadku systemów kołowych i kołowo-promieniowych takich jak **radiodalmierz DME** czy systemy **TACAN** i **RSBN**, oprócz zakłócania odbiorników pokładowych urządzeń zapytujących istnieje również możliwość zakłócania odbiorników radiolatarni. Urządzenia te pracują w paśmie 1000 MHz i mogą być rozpoznawane i zakłócane przy wykorzystaniu urządzeń do zakłócania systemów rozpoznania radiolokacyjnego, które będą przedmiotem dalszych rozważań.

Radiotechniczny system dalekiej nawigacji to system obejmujący środki radiotechniczne rozmieszczone na lądzie (aparatach latających, okrętach), które mają promień działania – rzędu kilku tysięcy kilometrów. Środki tego systemu pracują zazwyczaj w zakresach średnich, długich i bardzo długich fal radiowych.

Urządzenia pokładowe systemów **Loran**, **Decca**, **Omega,** podobnie jak urządzenia odbiorcze ultrakrótkofalowego systemu **VOR,** mogą być zakłócane przy pomocy radiowych urządzeń zakłócających pracujących w odpowiednich zakresach częstotliwości. W przypadku urządzeń radionawigacyjnych, pasywny charakter pracy urządzeń pokładowych powoduje istotne problemy z ich zakłócaniem.

Zakłócanie systemów promieniowych, należy więc prowadzić wykorzystując naziemne stacje zakłóceń, skutkiem czego, pokładowe urządzenia odbiorcze nie będą wskazywały kierunku na bazową stację naziemną systemu, lecz kierunek maksymalnego sumarycznego pola elektromagnetycznego w danym punkcie. Możliwe odległości i wymaganą moc zakłóceń stacji, oblicza się według podobnych zasad,

jak w przypadku obezwładnienia zakłóceniami łączności radiowej, odpowiednio zwiększając współczynnik zakłóceń K_z.

Zakłócanie środków i systemów radionawigacyjnych dalekiego i globalnego zasięgu, które są w większości systemami różnicowo - odległościowymi z impulsowym lub ciągłym promieniowaniem energii elektromagnetycznej, ułatwione jest z tego względu, że stacje bazowe wykorzystują jedną, zwykle znaną częstotliwość roboczą.

Zakłócanie takich systemów powinno polegać na zagłuszaniu lub myleniu pokładowych urządzeń odbiorczo-wskaźnikowych. Czynniki warunkujące skuteczność zakłóceń są następujące:

- dostosowanie częstotliwości sygnału zakłócającego do sygnału użytecznego;
- generowanie sygnału o właściwej strukturze i niezbędnej mocy;
- dyslokacja środków zakłócających pomiędzy urządzeniami nadawczymi a odbiorczymi.

Czynniki te mają szczególnie istotne znaczenie w procesie zakłócania satelitarnych globalnych systemów radionawigacyjnych, bowiem systemy dalekiego zasięgu powinny również obejmować środki radiotechniczne, zainstalowane na sztucznych satelitach ziemi.

Analiza funkcjonowania globalnego systemu radionawigacji satelitarnej wskazuje, iż spośród jego trzech segmentów (kosmicznego[48], kontrolnego[49] i użytkowego[50]) najbardziej podatny na zakłócenia jest segment użytkowy. Zakłócenia te

---

[48] Np. Segment kosmiczny systemu GPS NAVSTAR obejmuje 24 satelity (w tym 6 zapasowych) poruszających się po 6 różnych orbitach nachylonych do płaszczyzny równika pod kątem 55^0 i okrążających Ziemię w ciągu 12 godzin w odległości 20200 km od jej powierzchni [3;19;21].

[49] Segment kontrolny systemu GPS NAVSTAR tego systemu składa się z 10 naziemnych stacji śledzących satelity, które obliczają i wysyłają odpowiednie poprawki do stacji głównej MCS, gdzie z kolei obliczane są efemerydy i wysyłane do satelitów [3;19;21].

[50] Segment użytkowy systemu GPS NAVSTAR składa się z różnorodnych wojskowych i cywilnych odbiorników GPS zaprojektowanych w taki sposób, aby była możliwość odbierania, dekodowania i przetwarzania sygnałów GPS. Są to odbiorniki samodzielnie funkcjonujące lub wbudowane w inne urządzenia. Zastosowania obejmują nawigację (powietrzną, morską, lądową), wyznaczanie pozycji, transfer czasu, pomiary geodezyjne i wiele innych [3;19;21].

mogą powstawać w sposób niezamierzony[51] (przypadkowy) w wyniku niekompatybilności różnych urządzeń radioelektronicznych lub też mogą być zamierzone (celowe) sygnały zakłócające emitowane przez komórki walki informacyjnej [19;20].

Zakłócenia niezamierzone to przede wszystkim częstotliwości harmoniczne, listki boczne, efekty intermodulacji oraz te, których nie udaje się ustalić przy pomocy tradycyjnych metod kontroli częstotliwości. Są one groźne dla globalnego systemu radionawigacji satelitarnej z tego względu, że nawet nadajniki małych mocy mogą zakłócić odbiorniki tego systemu w promieniu do 10 km. Podatność odbiorników systemu na zakłócenia emitowane przypadkowo przez powszechnie używane nadajniki jest sprawą ewidentną, co wpływa niekorzystnie na działania operacyjne prowadzone w oddalonych obszarach (rejonach). Pracę takich odbiorników mogą na przykład zakłócać telefony komórkowe. Wykorzystują one sygnały radiowe do synchronizacji w pracy multipleksowej, powodując zakłócenia w torze odbiorczym systemu nawigacji.

Do emitowania **zakłóceń zamierzonych (celowych)** globalnego systemu radionawigacyjnego w określonych obszarach (rejonach) można masowo użyć przenośnych nadajników zakłócających jednorazowego użytku. Są to urządzenia o bardzo małych rozmiarach, których koszt jednostkowy, według amerykańskich szacunków, nie powinien przekroczać 100 dolarów.

Należy mieć na uwadze, że współczesne środki bojowe mogą wykorzystywać (alternatywnie lub równocześnie) różne urządzenia radionawigacyjne co powoduje konieczność wielospektralnego skoordynowanego zakłócania w celu zapewnienia zakładanej skuteczności. Godnym podkreślenia jest również fakt, że przy współczesnej unifikacji urządzeń radionawigacyjnych zakłócanie obszarowe (tak jak w przypadku systemów radionawigacyjnych dalekiego zasięgu) spowoduje zakłócenie również własnych środków. Ewentualne użycie zakłóceń radionawigacyjnych wy-

---

[51] Zakłócenia niezamierzone (przypadkowe) powstają w wyniku oddziaływania zjawisk przyrodniczych (naturalnych) oraz urządzeń technicznych na środki elektroniczne. Występują najczęściej podczas wyładowań atmosferycznych, oddziaływania zorzy polarnej lub wybuchów słonecznych, grawitacyjnego oddziaływania księżyca i innych ciał niebieskich, pływów skorupy ziemskiej i pływów oceanicznych, refrakcji jonosferycznej i troposferycznej, opadów atmosferycznych, pracy urządzeń przemysłowych, w tym: spawarek, urządzeń wyładowczych, źle zabezpieczonych silników elektrycznych i in. [3;19;21].

magać więc będzie uprzedniego dokładnego rozważenia strat i korzyści wynikających z jego zastosowania.

2.2.4. Zakłócanie systemów kierowania uzbrojeniem

Analiza rozwiązań światowych przeprowadzona na podstawie dostępnych materiałów źródłowych umożliwia wyróżnienie czterech zasadniczych grup kierowania uzbrojeniem: zdalne[52], programowe[53], samonaprowadzające[54], kombinowane[55]. W każdej z tych grup wyróżnić można różnorodne urządzenia techniczne wykorzystujące fale elektromagnetyczne, zjawiska świetlne, dźwiękowe, magnetyczne, cieplne, bezwładnościowe, żyroskopowe i inne. W większości systemów kierowania uzbrojeniem wykorzystuje się urządzenia radiolokacyjne, telewizyjne, termowizyjne, laserowe oraz radiowe.

W **kierowaniu radiolokacyjnym** wykorzystuje się przede wszystkim samonaprowadzanie aktywne, półaktywne i pasywne. W każdej z wybranych metod cel musi być odpowiednio „oświetlony" wiązką radiolokacyjną, a pocisk przemieszcza się w wiązce lub też sam wypracowuje sygnały korygujące. Następnie, wykorzystując pasmo promieniowania własnego celu (np. w paśmie 1 – 2 mm), pocisk

---

[52] Kierowanie zdalne realizowane jest z wykorzystaniem specjalnych urządzeń dokonujących automatycznie pomiaru wzajemnego położenia celu i środka rażenia, przetwarzania tych danych na sygnały kierowania (wiązki prowadzącej) oraz ich przesyłania do środka rażenia kanałem radiowym lub zakodowane w sygnale urządzenia pomiarowego (np. stacji radiolokacyjnej). Układy sterowania automatycznego są wrażliwe na wszelkiego rodzaju zakłócenia. W starszych systemach stosowane są układy sterowania ręcznego lub półautomatycznego. Podstawą wypracowania komend jest śledzenie obiektu kierowanego przez operatora i ciągłe porównywanie rzeczywistych parametrów jego przemieszczania się (lotu) z parametrami pożądanymi [1;20;21].

[53] Kierowanie programowe (autonomiczne lub nieautonomiczne) stosowane jest głównie w wypadku, kiedy wyrzutnia i cel są nieruchome, np. w pociskach „ziemia – ziemia". W takich warunkach tor lotu środka rażenia, czyli tzw. program lotu, zostaje uprzednio ustalony, przy czym uwzględnia się warunki atmosferyczne wpływające na zniekształcenie tego toru. Wyróżnia się kierowanie: programowe automatyczne, astronawigacyjne, radionawigacyjne, bezwładnościowe [1;20;21].

[54] „Samonaprowadzanie" polega na samoczynnym kierowaniu się środka rażenia na cel. Umieszczony w nim układ wykrywania odróżnia cel od otoczenia, określa jego położenie i kieruje lotem pocisku tak, aby nastąpiło spotkanie się jego środka z celem albo powoduje jego samolikwidację. Może być stosowane, gdy istnieje możliwość wyróżnienia celu z otaczającego go tła. Z uwagi na miejsce znajdowania się pierwotnego źródła energii wykorzystywanego do pracy układu kierowania wyróżnia się samonaprowadzanie: pasywne, półaktywne i aktywne [1;20;21].

z odległości 1 – 1,5 km może pasywnie naprowadzić się na cel. Zaletą środków bojowych wykorzystujących radiolokacyjne systemy kierowania jest możliwość ich stosowania w nocy oraz prawie w każdych warunkach pogodowych.

Wadą natomiast jest niska odporność zarówno na zakłócenia aktywne emitowane przez nadajniki zakłóceń szumowych i odzewowych, jak i na zakłócenia pasywne wytwarzane przez dipole, pułapki radiolokacyjne oraz odbijacze kątowe.

Pociski (bomby) **naprowadzane telewizyjnie** mają wbudowaną w głowicę kamerę, z której obraz przesyłany jest do monitora operatora (pilota) naprowadzającego pocisk na cel. Obraz ten znacznie ułatwia rozpoznanie i zniszczenie celu. Naprowadzenie pocisku (bomby) na cel odbywa się półautomatycznie lub ręcznie. Wadą telewizyjnego systemu kierowania jest jego niska efektywność w warunkach złej lub ograniczonej widoczności. Można go również zakłócić stosując zasłony dymne.

Systemy kierowania w podczerwieni (termowizyjne) uzupełniają układy telewizyjne. Umożliwiają bowiem zwalczanie celów w nocy oraz w warunkach ograniczonej widoczności. Zasada działania termowizyjnych systemów kierowania jest zbliżona do wykorzystywanej w kierowaniu telewizyjnym, z tym że w systemach termowizyjnych kamera umieszczona w głowicy pocisku widzi obraz termiczny atakowanego obiektu formowany na podstawie różnicy temperatur celu i otaczającego go środowiska. Dodatkową zaletą tego układu jest dwukrotnie większy (niż przy laserowym lub telewizyjnym układzie) zasięg wykrywania celu oraz możliwość wykrywania celów ukrytych i zamaskowanych[56]. Wadą tego systemu jest jego podatność na działanie pułapek termicznych.

W **laserowych systemach kierowania (samonaprowadzania),** cel podświetlany jest światłem lasera bądź z nosiciela amunicji (wyrzutni naziemnej, samolotu) lub ze źródła zewnętrznego. Pocisk lecący w kierunku celu naprowadza się samoczynnie na odbitą od celu wiązkę promieni laserowych, kierując się na oświe-

---

[55] Kierowanie kombinowane jest połączeniem kilku różnych systemów, przy czym każdy system kieruje lotem na określonym odcinku toru, lub pracuje jednocześnie z innymi systemami [1;20;21].

[56] Praktycznie układy te znalazły zastosowanie w wojnie w rejonie Zatoki Perskiej w 1991 r. [1;21;33].

tlone miejsce (punkt) odbicia. Laserowe systemy kierowania zapewniają wysoką celność sterowanej amunicji. Nie są jednak odporne na działanie zakłóceń pasywnych.

Ponieważ każdy z systemów kierowania ma swoje zalety, ale również i wady, to zazwyczaj do kierowania środkami rażenia (zwłaszcza o większej sile rażenia lub przeznaczonych do uderzeń precyzyjnych) używa się kilku systemów jednocześnie lub włączanych kolejno w miarę ruchu pocisku po trajektorii lotu. O ich doborze i możliwych kombinacjach decydują takie czynniki, jak: wymagany zasięg oddziaływania, dopuszczalna masa urządzeń sterujących, wpływ warunków meteorologicznych i ich wrażliwość na zakłócenia. Systemy kierowania są z reguły urządzeniami wielokanałowymi, umożliwiającymi jednoczesne sterowanie kilkoma obiektami wykonawczymi. Realizację tego zapewniają wyspecjalizowane komputery pokładowe i urządzenia zapewniające wysoką niezawodność oraz skuteczność sterowania.

Ocena wykorzystywanych systemów kierowania uzbrojeniem [1;21] wykazuje, że obecnie możliwe jest zakłócanie nieautonomicznych i kombinowanych (częściowo automatycznych) systemów kierowania rakietami, ponieważ w zestaw sterowania tych rakiet wchodzą urządzenia elektroniczne, które współpracują z naziemnymi środkami elektronicznymi rozwiniętymi w określonych punktach kierowania szczebla operacyjnego i taktycznego. Konieczność elektronicznej współpracy w relacjach: „ziemia – powietrze" i „powietrze – ziemia" czyni wszystkie te urządzenia wrażliwymi na rozpoznanie i zakłócanie elektroniczne.

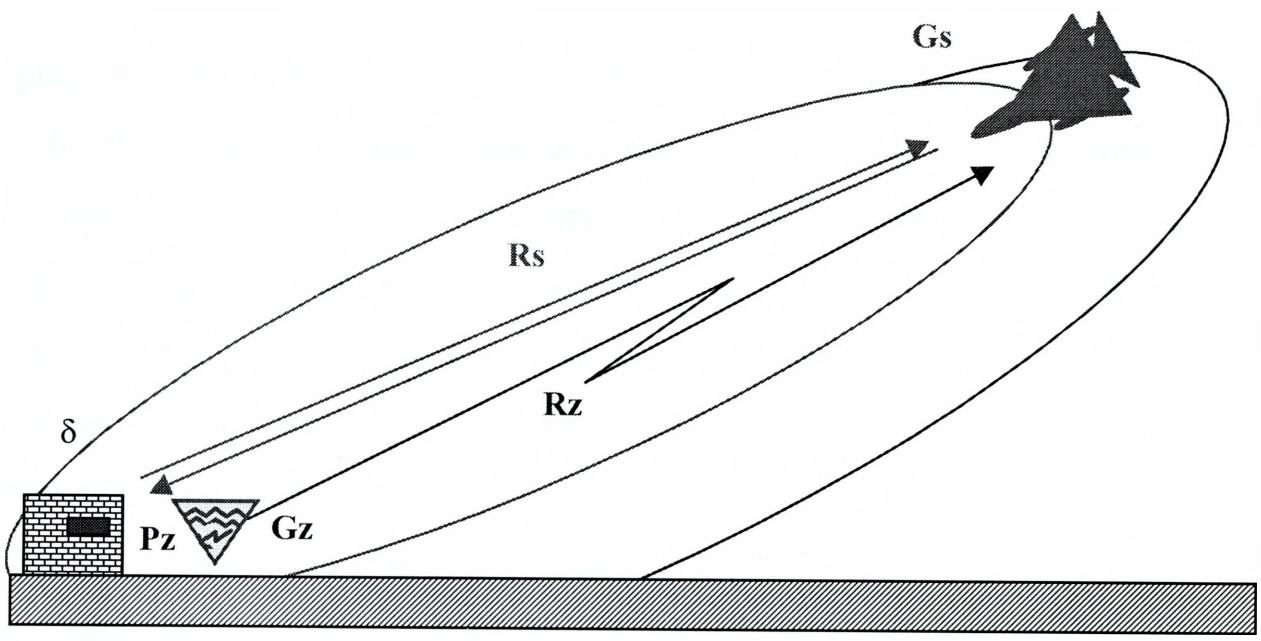
Z przeprowadzonych analiz [60] wynika, że obecnie **niemożliwe jest zakłócanie elektroniczne autonomicznych, najczęściej z góry zaprogramowanych systemów kierowania rakiet.** W systemach tych program lotu rakiet ustala się przed ich wystrzeleniem i steruje za pomocą urządzeń znajdujących się na ich pokładach, niezależnie od ośrodków naziemnych. Dzięki temu, są one niewrażliwe na zakłócania elektroniczne wytwarzane z zewnątrz (przez fałszywy cel lub pułapki radiolokacyjne z ziemi albo z pokładu samolotu). Istnieje jednak możliwość zakłócenia zbliżeniowych zapalników radiowych tych rakiet. Oddziaływanie zakłóceniа-

mi na zapalniki może spowodować ich wcześniejsze zadziałanie na znacznej wysokości lub w takiej odległości, która jest większa od promienia rażenia głowicy bojowej. W rezultacie stosowanych zakłóceń zapalników zbliżeniowych rakieta nie doleci do zaprogramowanego celu. W wypadku zakłócania zbliżeniowych zapalników radiowych rakiet, stacje zakłócające należy rozmieszczać w rejoniach osłanianych obiektów.

Doświadczenia i przeprowadzone badania wykazują, że **najkorzystniej jest obezwładniać zakłóceniami urządzenia śledzenia radiolokacyjnego, a także relacji radiowych dowodzenia i automatycznego kierowania (sterowania).** Zakłócenia urządzeń systemów śledzenia rakiet klasy „powietrze – ziemia" mogą się odbywać w strefie radiolokacyjnej widzialności i poza nią. Można założyć, że jeśli rakieta jest śledzona radiolokacyjnie i sterowana na całej trasie lotu, to zakłócenie urządzenia śledzącego, np. samolotu nosiciela rakiety przeciwnika jest możliwe na całej trasie jego lotu, tj. od rubieży startu rakiety (pocisku kierowanego) do rubieży jej naprowadzania na obiekt naziemny. Do zakłócania urządzeń radiolokacyjnego śledzenia można wykorzystywać naziemne lub samolotowe stacje zakłóceń radiolokacyjnych, wytwarzające zakłócenia szumowe i impulsowo – odzewowe.

Zakłócanie pracy stacji radiolokacyjnych za pomocą celowych sygnałów zakłócających jest możliwe, ponieważ urządzenia odbiorcze tych stacji rejestrują nie tylko sygnały użyteczne dla stacji (odbite od celu) ale i inne sygnały promieniowane przez urządzenia zakłócające, na tej samej częstotliwości. Sygnał użyteczny wypromieniowany przez stację radiolokacyjną, zanim dotrze do układów wejściowych urządzenia odbiorczego, musi przebyć drogę od stacji do celu i z powrotem. W wyniku tego moc sygnału użytecznego znacznie się zmniejsza i jest odwrotnie proporcjonalna do odległości od celu podanej w czwartej potędze. Nadajniki zakłócające mają przewagę nad stacjami radiolokacyjnymi, ponieważ sygnał zakłócający przebywa drogę tylko między stacją zakłócającą, a zakłócaną stacją radiolokacyjną. Tłumienie sygnału zakłócanego jest znacznie mniejsze. Moc sygnału zakłócającego w punkcie odbioru zakłócanej stacji radiolokacyjnej jest więc odwrotnie proporcjonalna do kwadratu odległości od stacji radiolokacyjnej podanej w drugiej potędze.

W praktyce oznacza to, że istnieje możliwość uzyskania gęstości mocy wystarczającej do efektywnego zakłócania pracy stacji radiolokacyjnej nawet dużej mocy za pomocą stacji zakłócającej o mniejszej mocy, co zilustrowano na rysunku 2.30.



Rys. 2.30. Graficzna interpretacja zakłóceń radiolokacyjnych

Wymienione uwarunkowania można wyrazić następującymi równaniami:

– moc sygnału użytecznego stacji radiolokacyjnej odbitego od celu i odbieranego przez urządzenia odbiorcze stacji[57]:

$$P_{sr} = \frac{P_s G_s^2 \delta \lambda^2}{(4\pi)^3 R_s^4}$$

gdzie:

P_{sr} *[W] - moc sygnału użytecznego stacji radiolokacyjnej odbitego od celu;*

P_s *[W] - moc nadajnika stacji radiolokacyjnej (moc stacji);*

G_s *- zysk kierunkowy anteny stacji radiolokacyjnej;*

δ *- efektywna powierzchnia odbijająca obserwowanego celu;*

λ *[m]- długość fali radiowej;*

R_s *[km] - odległość stacji radiolokacyjnej od celu.*

– moc sygnału zakłócającego odbieranego przez urządzenia odbiorcze zakłócanej stacji radiolokacyjnej[58]:

$$P_{sz}=\frac{P_z G_z G_s \lambda^2}{(4\pi R_z)^2}$$

gdzie:

P_{sz} [w]- moc sygnału zakłócającego w punkcie odbioru zakłócanej stacji radiolokacyjnej;

P_z [W] - moc stacji zakłócającej;

G_z - zysk kierunkowy anteny stacji zakłócającej;

G_s - zysk kierunkowy anteny zakłócanej stacji radiolokacyjnej;

λ [m]- długość fali radiowej;

R_z - odległość między stacją zakłócającą a odbiornikiem zakłócanej stacji radiolokacyjnej.

Przy jednakowej mocy stacji radiolokacyjnej i stacji zakłócającej i przy równych odległościach stacji radiolokacyjnej do celu i do stacji zakłócającej, moc sygnału zakłócającego będzie znacznie przewyższała moc sygnału użytecznego odbitego od celu.

Przedstawione równania, zarówno dla sygnału stacji radiolokacyjnej, jak i sygnału zakłócającego, pozwalają określić wielkość mocy stacji zakłócającej, jaka jest wymagana do skutecznego zakłócenia pracy stacji radiolokacyjnej przeciwnika. Należy więc podzielić drugie równanie przez pierwsze i wprowadzić odpowiedni stosunek sygnału zakłócającego do sygnału użytecznego stacji radiolokacyjnej przeciwnika, odbitego od celu.

Z równań tych wynika, że wielkość potrzebnej mocy stacji zakłócającej jest odwrotnie proporcjonalna do kwadratu odległości. Oznacza to, że im większa jest odległość celu od stacji radiolokacyjnej przeciwnika, tym mniejsza moc jest potrzebna do skutecznego obezwładniania zakłóceniami pracy tej stacji. Skuteczne zakłócenie elektroniczne stacji radiolokacyjnych przeciwnika znajdujących się na

---

[57] Por.: K. Kokot, „Podstawy radiolokacji", wyd. WAT, Warszawa 1968, s. 148.

małych odległościach względem stacji zakłócających jest znacznie trudniejsze niż na większych odległościach. Dla zakłóceń radiolokacyjnych korzystny jest przypadek, kiedy odległość stacji radiolokacyjnej od obiektu (R_s) jest znacznie większa lub równa odległości do stacji zakłóceń (R_z).

Należy mieć na uwadze, że środki śledzenia radiolokacyjnego rakiet klasy „ziemia – ziemia" można skutecznie obezwładniać zakłóceniami za pomocą samolotowych stacji zakłócających, odznaczających się znacznym zasięgiem i dużą skutecznością zakłóceń. Zakłócanie może być przeprowadzone na trasach lotu rakiet w całej strefie śledzenia stacji radiolokacyjnej.

Do zakłócania elementów elektronicznych zarówno systemów dowodzenia, jak i kierowania uzbrojeniem (systemów termowizyjnych, czujnikowych, laserowych, i in.) można będzie w przyszłości wykorzystać generatory impulsu elektromagnetycznego bądź urządzenia mikrofalowe generujące energię o dużej gęstości mocy (np. lasery).

2.3. Wnioski

W wyniku przeprowadzonych badań wykazano, że:

1. Zakłócanie rozpoznania u przeciwnika, jest ważnym elementem procesu zakłócania informacyjnego w operacjach wojsk lądowych. Stanowi zespół skoordynowanych przedsięwzięć i działań zmierzających do ukrywania zbiorów wszelkich postaci danych o rzeczywistym stanie, usytuowaniu i zamiarach działania wojsk lądowych, które są lub mogą być dostępne dla źródeł rozpoznania przeciwnika.

Ogólnie rozumiane zakłócanie rozpoznania można podzielić na dwa rodzaje: zakłócanie rozpoznania bezpośredniego i zakłócanie rozpoznania pośredniego.

---

[58] Tamże

Zakłócanie rozpoznania bezpośredniego powinno obejmować stany osobowe rozpoznania agenturalnego, specjalnego i patrolowego oraz wykorzystywane przez nich metody takie jak obserwacja, penetracja dokumentów i danych personalnych.

Do zakłócania rozpoznania bezpośredniego powinny być również wykorzystane takie formy jak: podstęp, wprowadzanie w błąd, tak zwana „biała" i „czarna" propaganda oraz wpływanie i dezinformowanie.

Strukturę zakłócania rozpoznania pośredniego tworzą elementy zakłócania rozpoznania elektronicznego i zakłócania rozpoznania studyjnego.

Zakłócanie rozpoznania elektronicznego u przeciwnika, powinno obejmować systemy i środki rozpoznania radioelektronicznego, radiolokacyjnego, optoelektronicznego, czujnikowego i informatycznego.

Zakłócaniu podlegać powinny głównie układy odbiorcze aktywnych środków rozpoznania elektronicznego, zakłócanie pasywnych środków jest znacznie utrudnione, bowiem ich praca „na odbiór" znacznie utrudnia ich wykrycie, które jest niezbędnym warunkiem efektywnego zakłócania. Pośrednio można oddziaływać na te środki ograniczając do niezbędnego minimum dostępność własnych, nadawczych środków i urządzeń elektronicznych w niepożądanych strefach i sektorach, bądź zakłócając systemy kierowania i prawdopodobne sektory i rubieże ich rozwinięcia.

Zakłócanie aktywnych systemów i urządzeń rozpoznania elektronicznego, polega na wnoszeniu do układów odbiorczych urządzeń przeciwnika dodatkowych wartości energetycznych, powodując przesterowanie ich układów wejściowych, podwyższenie poziomu szumów, zaniki i niejednoznaczności w odczycie danych, a nawet ich uszkodzenie lub zniszczenie.

Zakłócanie rozpoznania studyjnego polega na niszczeniu bądź modyfikowaniu zbiorów baz danych przeciwnika oraz ukrywanie (pozbawianie) indywidualnych cech rozpoznawczych własnych środków elektronicznych.

2. Zakłócanie dowodzenia i kierowania uzbrojeniem stanowi zespół skoordynowanych elementów dostosowany do wnoszenia entropii informacyjnej do procesów dowodzenia wojskami przeciwnika i procesów kierowania jego uzbrojeniem,

które realizowane są przy pomocy: systemów (sieci) radiokomunikacyjnych, systemów (sieci) informatycznych, systemów radionawigacyjnych oraz systemów kierowania uzbrojeniem.

Zakłócanie systemów (sieci) radiokomunikacyjnych polega na celowym promieniowaniu zakłócającej energii elektromagnetycznej powodującej utrudnienie pracy elektronicznych środków łączności radiowej KF i UKF, łączności radiolinio-wej (horyzontowej i pozahoryzontowej) oraz radiosatelitarnej przeciwnika.

Zakłócanie stosowane w odniesieniu do systemów (sieci) informatycznych przeciwnika przyjmuje najczęściej formę oprogramowania złośliwego, które powoduje blokowanie dostępu do informacji, wymazanie w krótkim czasie dużej liczby zbiorów danych, spowalnianie pracy programów użytkowych.

Zakłócanie systemów radionawigacyjnych jest zespołem takich celowych i skoordynowanych działań organizacyjnych i technicznych, które uniemożliwią lub utrudnią obiektom ruchomym przeciwnika określenie swojego miejsca położenia.

W większości systemów kierowania uzbrojeniem wykorzystuje się urządzenia radiolokacyjne, telewizyjne, termowizyjne, laserowe oraz radiowe. Zakłócanie systemów kierowania uzbrojeniem polega więc na dezorganizacji pracy tych urządzeń.

3. METODYKA I TREŚĆ PRACY W CYKLU DECYZYJNYM ZAKŁÓCANIA INFORMACYJNEGO W OPERACJACH WOJSK LĄDOWYCH

3.1. Przebieg cyklu decyzyjnego w zakresie zakłócania informacyjnego

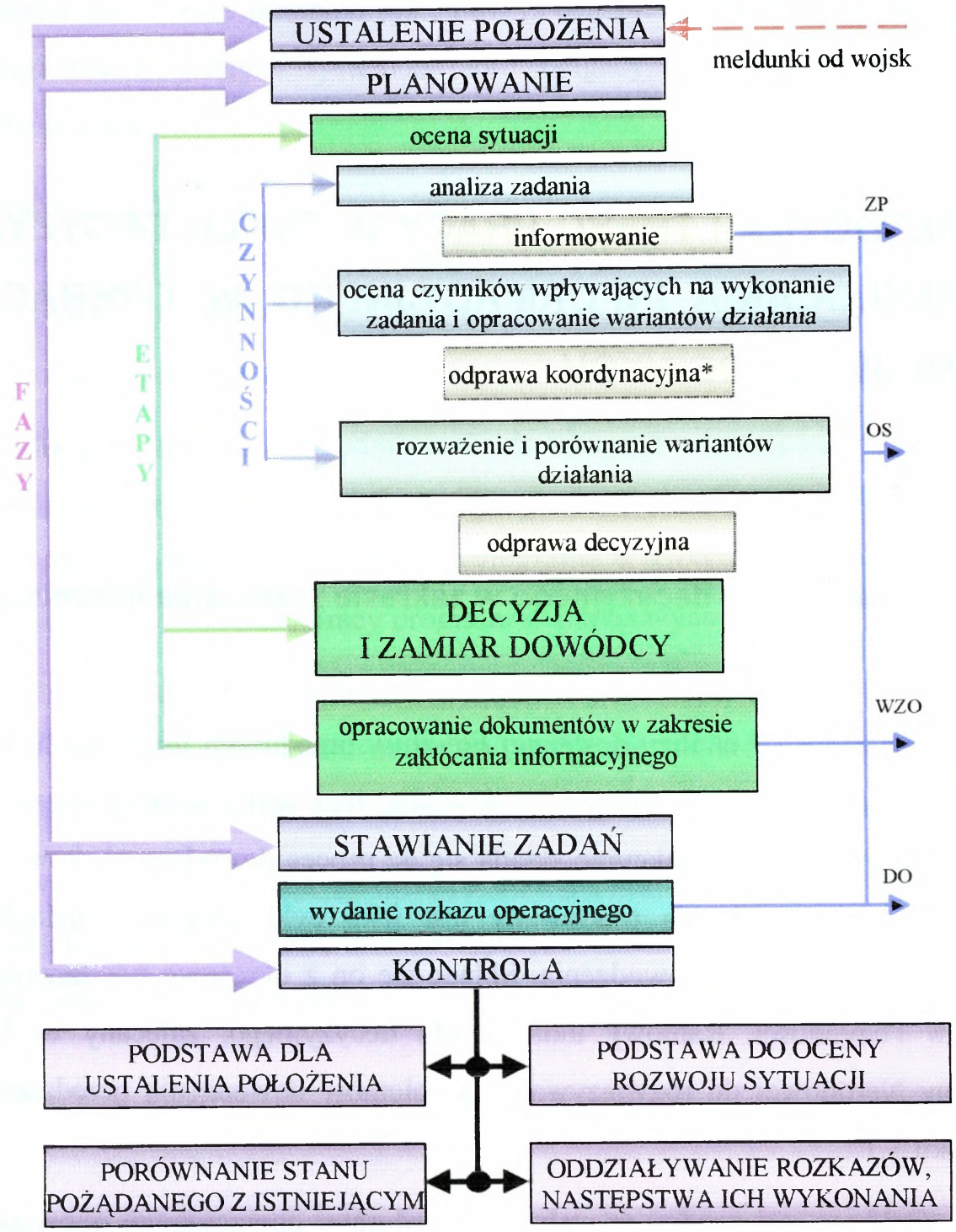
Jak wynika z analizy dostępnej literatury przedmiotu badań [8;29;21], całokształt przedsięwzięć związanych z dowodzeniem realizowanym przez komórki organizacyjne i osoby funkcyjne składa się na proces dowodzenia[1], który z operacyjnego punktu widzenia traktowany jest jako cykl decyzyjny jednakowy na wszystkich szczeblach dowodzenia. Składa się on z okresowo powtarzających się etapów i czynności. Ramowy układ cyklu decyzyjnego, zalecany w Akademii Obrony Narodowej do rozwiązywania problemów dowodzenia przedstawiono na rysunku 3.1[2].

Cykl ten jest zgodny ze stałymi procedurami operacyjnymi obowiązującymi w siłach zbrojnych głównych państw NATO oraz uwzględnia dorobek polskiej myśli wojskowej.

Z powyższego wynika, że cykl decyzyjny w zakresie zakłócania informacyjnego jest nierozerwalnie związany z procesem dowodzenia, realizowanym przez komórki organizacyjne i osoby funkcyjne na stanowiskach dowodzenia.

---

[1] Proces ten symbolicznie można przedstawić w postaci koła, które utrzymywane jest w ruchu przez ciągłe zdobywanie, przetwarzanie i wykorzystywanie danych, stanowiących podstawę do powzięcia decyzji i opracowania planu działania oraz opracowania zadań (dyrektyw, rozkazów, zarządzeń) i przekazania ich wykonawcom.



LEGENDA:

ZP – zarządzenie przygotowawcze;
OS – orientowanie w sytuacji;
WZO – wstępne zarządzenie operacyjne;
RO/RL – rozkaz operacyjny / logistyczny;
* – liczba, miejsce i cele odpraw koordynacyjnych określa dowódca lub szef sztabu.

Rys. 3.1. Ramowy układ cyklu decyzyjnego

---

[2] Opracowano na podstawie: J. Michniak i inni, „Metody i treść pracy zespołów funkcjonalnych na stanowisku dowodzenia wojsk lądowych", wyd. AON, Warszawa 2000, s. 29.

W procesie tym najważniejsze zadania powinien realizować zespół rozpoznania centrum dowodzenia SD, którego w aspekcie zadań wykonywanych w ramach walki informacyjnej należy – zdaniem autorów pracy badawczej – postrzegać jako **zespół działań informacyjnych**. W kontekście powyższego zespół ten powinien składać się z następujących grup: planowania, badań i informowania, rozpoznania, zakłócania informacyjnego, obrony informacyjnej oraz topograficznej oceny terenu. Udział powinny brać także zespoły planowania i dowodzenia w centrum dowodzenia oraz zespół łączności i informatyki centrum wsparcia dowodzenia i łączności. Uczestniczyć w nim powinny również zespoły funkcjonalne centrum wsparcia działań w ramach nałożonych na nich obowiązków w zakresie planowania i zabezpieczenia działań bojowych.

Cykl decyzyjny w zakresie zakłócania informacyjnego przebiega w czterech łączących się i przenikających się nawzajem fazach: ustalenia położenia, planowania, stawiania zadań i kontroli. Jego celem powinno być określenie kolejności, sposobów i terminów wykonania zadań z zakresu zakłócania informacyjnego w operacjach wojsk lądowych.

3.2. W fazie ustalania położenia w zakresie zakłócania informacyjnego

Ustalenie położenia jest punktem wyjściowym całego cyklu dowodzenia. Faza ta rozpoczyna się z chwilą otrzymania zadania, niekiedy meldunku w formie prośby lub wiadomości w ramach prowadzonej stałej obserwacji i napływu danych o sytuacji, ale także w wyniku zaistniałej sytuacji i nie dającego się przewidzieć jej rozwoju.

W związku z poszukiwaniem odpowiednio ukierunkowanej decyzji – przedmiotem działań na tym etapie jest – przede wszystkim zebranie wszystkich istotnych faktów oraz określenie czynników wywierających wpływ na daną sytuację, ich ocenę i uporządkowanie.

Występują tutaj różne formy pracy sztabowej, z wykorzystaniem technicznych środków przetwarzania danych. Z powodów czasowych i dużej ilości danych w wielu wypadkach regułą będzie to, że etap ten będzie musiał zostać zrealizowany wcześniej.

Ważne jest to, aby podczas oceny otoczenia, właściwie zdecydować kiedy zajdzie potrzeba zdobycia nowych danych, a kiedy posiadana baza danych wystarczy w dalszym postępowaniu. Tylko w nielicznych wypadkach taki podział i segregowanie danych osiągać będzie wystarczający stopień pewności.

Ustalenie położenia jest najczęściej zapoczątkowywane przez **„Informowanie o położeniu"**. Ma ono na celu poinformowanie dowódcy i sztabu o zaistniałej sytuacji i określenie dalszego algorytmu postępowania.

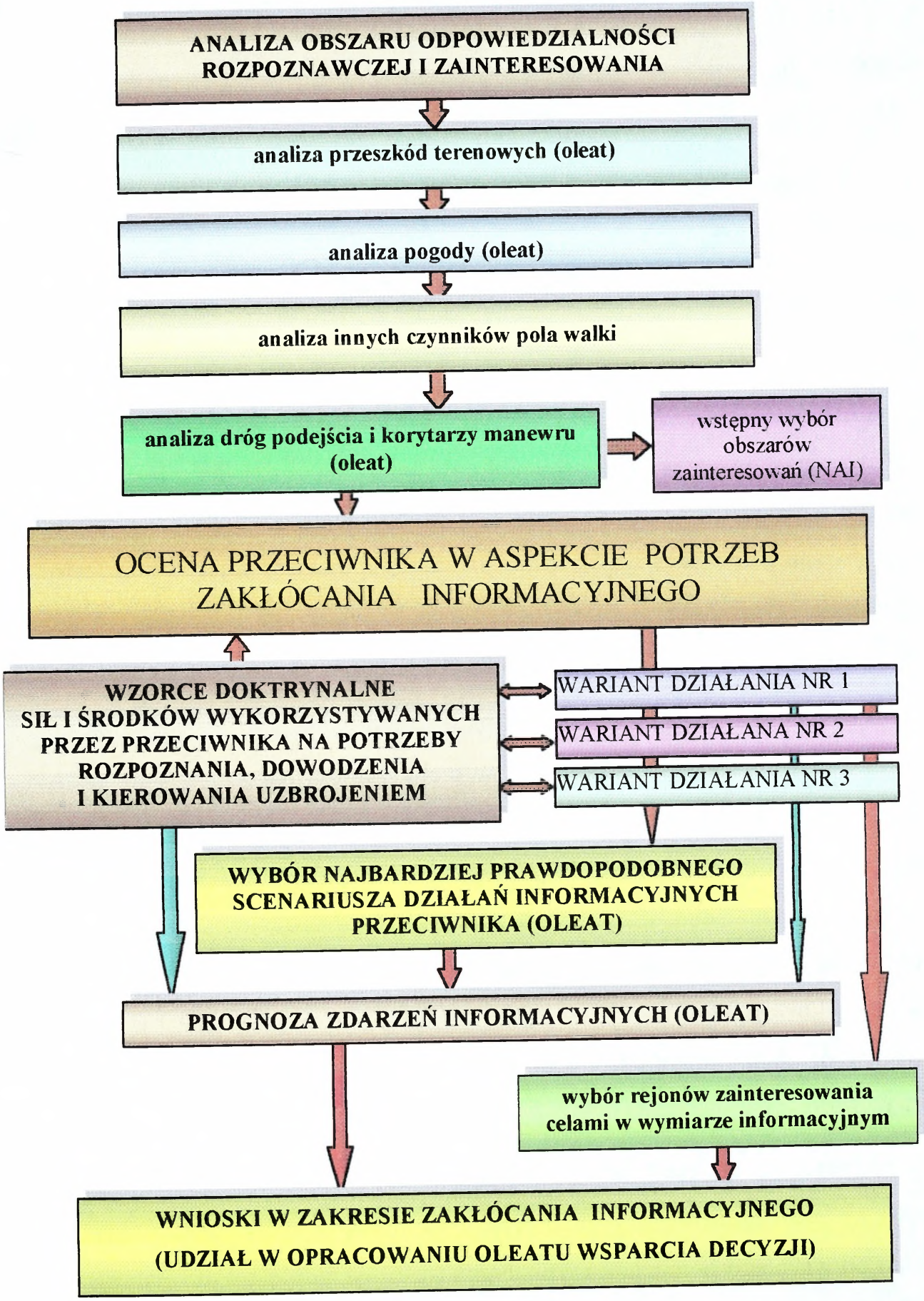
Faza ustalenia położenia dla **zespołu działań informacyjnych centrum dowodzenia SD DWLąd** jest początkiem procesu informacyjnego przygotowania pola walki[3]. W procesie tym należy rozpatrywać również problemy zakłócania informacyjnego (rysunek 3.2.).

Do głównych zadań, jakie w tej fazie powinien realizować zespół działań informacyjnych w zakresie zakłócania informacyjnego – zdaniem autorów opracowania – należą:

– zebranie, uporządkowanie, a następnie zobrazowanie danych o położeniu i ukompletowaniu sił i środków wykorzystywanych przez przeciwnika na potrzeby rozpoznania, dowodzenia i kierowania uzbrojeniem w dotychczasowych działaniach;

– zebranie i uporządkowanie danych o otoczeniu pola walki (o obszarze działań, terenie, pogodzie, warunkach demograficznych itp.), mającym wpływ na wymiar informacyjny działań;

[3] Problematyka informacyjnego (rozpoznawczego) przygotowania pola walki (ang. Intelligence Preparation of the Battlefield), której ważnym komponentem jest elektroniczne przygotowanie pola walki (ang. Electronic Preparation of the Battlefield) jest przedmiotem opracowań studyjnych w AON, w których autor również uczestniczył [8;21]. Stanowi ona ważną procedurę planowania działań wojsk sojuszniczych NATO.



Rys. 3.2. Informacyjne przygotowanie pola walki w zakresie zakłócania informacyjnego

– określenie braków i luk w wiedzy o przeciwniku i terenie w wymiarze informacyjnym;

– zebranie i uporządkowanie danych o położeniu i realizowanych zadaniach przez potencjał walki informacyjnej (rozpoznania, zakłócania i obrony informacyjnej) wojsk lądowych;

– ukierunkowanie cyklu realizowanych przedsięwzięć zgodnie z zadaniami postawionymi przez dowódcę;

– wykonywanie bieżących przedsięwzięć wynikających z zadań.

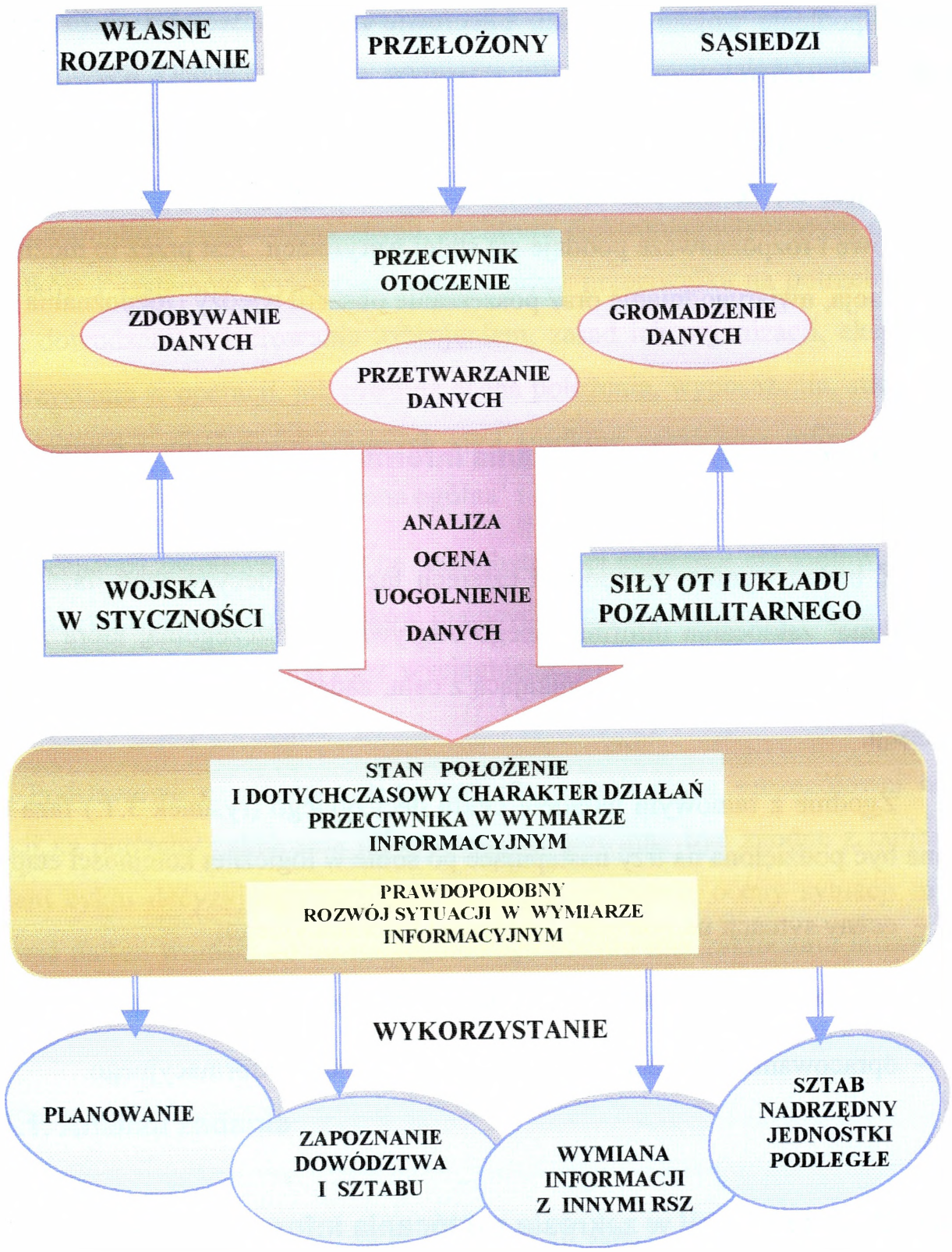
Podczas pracy w fazie ustalenia położenia zespół działań informacyjnych na centrum dowodzenia SD DWLąd. powinien sporządzić wstępną ocenę sytuacji, dającą sztabom podległych wojsk niezbędne dane do dalszej pracy. Wnioski w tej fazie należy zobrazować w takich dokumentach, jak: mapa informacyjna lub sytuacyjna (oleat[4] sytuacji bojowej), zarządzenie przygotowawcze, dyrektywa operacyjna i inne.

Celem ustalenia położenia na potrzeby zakłócania informacyjnego jest zebranie, uporządkowanie, a następnie zobrazowanie danych o położeniu i potencjale walki informacyjnej przeciwnika, a głównie o dotychczasowych działaniach jego systemów rozpoznania, dowodzenia i kierowania uzbrojeniem oraz o środowisku pola walki (o terenie, pogodzie, warunkach demograficznych, warunkach propagacji fal elektromagnetycznych itp.). Należy ocenić również położenie oraz dotychczasowe działania wojsk własnych w zakresie zakłócania informacyjnego (rysunek 3.3.).

Podstawę do ustalenia położenia przeciwnika powinny stanowić meldunki wojsk w styczności, rozkazy operacyjne i komunikaty szczebla nadrzędnego, meldunki od własnego potencjału rozpoznania (jeśli był lub jest w działaniu), informacje uzyskane od sąsiadów, sił obrony terytorialnej oraz układu pozamilitarnego.

---

[4] Oleat – (łac. *Oleatus* = zwilżony oliwą) przezroczysty, natłuszczony papier z wykresem części jakiegoś rysunku, zawierający pewne szczegóły, odczytywany po przyłożeniu go do zasadniczego rysunku, mapy itp. „Słownik wyrazów obcych", wyd. PWN, Warszawa 1979.



Rys. 3.3. Przebieg fazy ustalania położenia

Położenie sił i środków zakłócania informacyjnego wojsk własnych należy ustalać z kolei na podstawie meldunków od podwładnych. Zebrane dane powinny być porządkowane i ewidencjonowane oraz poddawane wstępnej analizie, ocenie i uogólnieniu. Opracowane w ten sposób dane stają się materiałem wyjściowym do procesu planowania zakłócania informacyjnego. Mogą być zasilane nimi

również podległe wojska, sąsiedzi, oficerowie rodzajów wojsk i służb oraz inni uprawnieni zainteresowani.

Cechą szczególną fazy ustalania położenia z punku widzenia zakłócania informacyjnego jest to, że ma ono charakter działania ciągłego, podczas którego dane szczątkowe i rozpoznawcze poddaje się stałej weryfikacji. Jest przez to możliwa ich aktualizacja, uwiarygodnianie oraz poszerzanie obszaru wiedzy (rozpoznania).

3.3. W fazie planowania zakłócania informacyjnego

Z badań wynika, że spośród czterech faz cyklu decyzyjnego, faza druga – planowanie[5] zakłócania informacyjnego odgrywa rolę szczególną, która związana jest z jej określoną specyfiką wynikającą z celu, zadań i nietypowych sposobów ich realizacji.

Zgodnie z ramowym układem cyklu decyzyjnego (rysunek 3.1.) faza ta powinna być podzielona na trzy następujące po sobie w logicznej kolejności etapy:

- oceny sytuacji na potrzeby zakłócania informacyjnego;
- wypracowanie koncepcji prowadzenia zakłócania informacyjnego;
- opracowania dokumentów w zakresie zakłócania informacyjnego.

3.3.1. Ocena sytuacji w zakresie zakłócania informacyjnego

Z praktyki działania sztabów wynika, że etap ocena sytuacji[6] zajmuje w fazie planowania działań wojennych specjalne miejsce. Stwierdzenie to odnosi się rów-

---

[5] Planowanie jest skoordynowanym i złożonym procesem sztabowym, ukierunkowanym na wypracowanie najlepszej metody wykonania postawionych zadań lub zadań możliwych do wykonania w przyszłości.

[6] Celem tego etapu jest dogłębne zrozumienie zadania otrzymanego od przełożonego, jego zamiaru (w tym myśli przewodniej), szczegółowa ocena zagrożeń oraz czynników wpływających na wykonanie zadania, opracowanie, rozważenie i porównanie wariantów działania wojsk korpusu, a w konsekwencji stworzenie dowódcy warunków do podjęcia decyzji [8;20;21].

nież w całej rozciągłości do planowania zakłócania informacyjnego w operacjach wojsk lądowych. Ocenę sytuacji w wymiarze informacyjnym należy postrzegać jako ważny element ogólnej oceny sytuacji operacyjnej i położenia wojsk. W jej ramach określany jest obszar działań, dokonywana jest ocena środowiska pola walki (terenu, warunków meteorologicznych, spektrum elektromagnetycznego) oraz ocena środków i systemów wykorzystywanych przez przeciwnika na potrzeby rozpoznania, dowodzenia i kierowania uzbrojeniem, zasad ich organizacji, eksploatacji i wykorzystania w operacji, jak również ocena położenia, wyposażenia, stanu gotowości bojowej i możliwości własnych sił i środków zakłócania informacyjnego. Pod względem zakresu może być ona ogólna[7] i szczegółowa.

Ocena szczegółowa polega na wszechstronnej analizie i prawidłowej ocenie wszystkich podstawowych czynników mających wpływ na pracę środków i działanie systemów informacyjnych oraz wyciągnięcie właściwych wniosków co do zakresu ich użycia na polu walki.

Podstawowe czynności realizowane w ramach etapu szczegółowej oceny sytuacji na potrzeby zakłócania informacyjnego powinny być zgodne z ramowym układem cyklu decyzyjnego (rysunek 3.1.). Na podstawie oceny sytuacji można wysuwać dalsze wnioski co do szczegółowego planowania zakłócania informacyjnego w konkretnych prowadzonych operacjach wojsk lądowych.

3.3.1.1. Analiza zadania

Ogólnie można określić, że w toku analizy zadania jako czynności w procesie oceny sytuacji precyzuje się, co i w jakim celu należy wykonać, aby zrealizować otrzymane zadanie.

---

[7] Ocena ogólna dokonywana jest w czasie pokoju, kryzysu i w okresie wojny. W ramach oceny ogólnej należy rozpatrzyć wszystkie posiadane dane o systemach walki informacyjnej przeciwnika oraz wojsk własnych, jak również o właściwościach ich pracy i eksploatacji. Dane o ogólnej sytuacji w wymiarze informacyjnym należy wykorzystać podczas planowania i organizowania całego kompleksu przedsięwzięć walki informacyjnej. Podczas rozwiązywania problemów zakłócania informacyjnego stają się one niezbędne również do określenia warunków, zasad i rodzajów pracy systemów rozpoznania, dowodzenia wojskami i kierowania uzbrojeniem przeciwnika.

Podczas analizy zadania[8] dokonywanej w zespole działań informacyjnych prowadzona jest wstępna ocena posiadanych wiadomości o przeciwniku oraz środowisku pola walki i wskazanie luk w rozpoznaniu (wiedzy o przeciwniku). Analiza zadania to proces intelektualny zespołu, mający na celu rozpatrzenie również zadań walki informacyjnej, której ważnym komponentem jest zakłócanie informacyjne. **Powinna umożliwiać określenie zadań zakłócania informacyjnego oraz sposobów ich wykonania na tle sytuacji operacyjnej, otrzymanych zadań ogólnowojskowych i ograniczeń swobody działania (czasu, obszaru[9] oraz sił).**

Do głównych zadań zespołu działań informacyjnych w tej fazie należy:

– wstępna analiza i ocena posiadanych wiadomości o środowisku działań oraz o siłach i środkach wykorzystywanych przez przeciwnika na potrzeby rozpoznania, dowodzenia wojskami i kierowania uzbrojeniem;

– wypracowanie wstępnej oceny przeciwnika w tym zakresie;

– wypracowanie wniosków do dalszej pracy w procesie informacyjnego przygotowania pola walki;

– wypracowanie wniosków do dalszej pracy w zakresie planowania rozpoznania, zakłócania i obrony informacyjnej;

– wykonywanie bieżących zadań.

---

[8] Należy udzielić odpowiedzi na następujące pytania:
– jaki jest zamiar przełożonego oraz jaka jest rola wojsk lądowych w realizacji jego planu zakłócania informacyjnego?
– czego wymaga przełożony i jakie zadania należy wykonać dla zrealizowania jego zamiaru?
– jakie istnieją ograniczenia swobody działania (obszar, czas, siły)?
– jakie znaczące zmiany sytuacji nastąpiły od czasu podpisania dyrektywy operacyjnej przez przełożonego?

[9] Obszar pola walki dla walczących wojsk dzieli się na strefę działania, strefę oddziaływania i strefę zainteresowania. W poszczególnych strefach należy uwzględnić różne wymiary pola walki: szerokość, głębokość, wysokość lub przestrzeń powietrzną, czas, spektrum elektromagnetyczne. Przy czym spektrum elektromagnetyczne nie jest ograniczone żadną strefą, lecz warunkami propagacji fal, a jego rozpatrywanie odnosi się zarówno do wymiaru lądowego, jak i powietrznego, w którym będzie działać przeciwnik [6;8].

3.3.1.2. Informowanie operacyjne

W toku informowania operacyjnego prowadzonego pod koniec analizy zadania lub po jej zakończeniu szef zespołu działań informacyjnych przedstawia ogólną sytuację przeciwnika wraz z wstępną jego oceną i pierwszymi możliwymi wariantami jego działania, przeciwstawiającymi się wykonaniu zadania własnego.

W wyniku informowania operacyjnego szef zespołu działań informacyjnych zapoznawany jest z kolei z wieloma zagadnieniami, które mają znaczny wpływ na dalszy przebieg cyklu decyzyjnego, a mianowicie:

- sprecyzowane zadanie własne;
- myśl przewodnia dowódcy;
- kryteria do porównania wariantów działania;
- wytyczne do pracy sztabu wynikłe z wstępnej kalkulacji czasu.

W sprecyzowanym zadaniu i w myśli przewodniej dowódcy powinny znaleźć odzwierciedlenie również problemy związane z osiąganiem zakładanych celów w ramach zakłócania informacyjnego.

Etap ten kończy się postawieniem zadań przez szefa zespołu działań informacyjnych (na podstawie wytycznych dowódcy) co do dalszego przebiegu procesu informacyjnego przygotowania pola walki. Treścią tych zadań może być na przykład: liczba wariantów działania oraz aspektów oceny przeciwnika (również w wymiarze informacyjnym); terminy i forma wypracowania ocen; zakres i metody poszukiwania brakujących wiadomości; źródła danych itp.

Po tym etapie powinny być również wysłane zarządzenia przygotowawcze do wojsk; należy w nich ująć także problemy zakłócania informacyjnego.

Problematyka zakłócania informacyjnego powinna znaleźć odzwierciedlenie także w zadaniach i wytycznych specjalistów rodzajów wojsk i służb w ramach ich obowiązków w zakresie planowania i zabezpieczenia działań bojowych.

3.3.1.3. Ocena czynników wpływających na wykonanie zadania i opracowanie koncepcji zakłócania informacyjnego dla poszczególnych wariantów operacji wojsk lądowych

Celem tej czynności, realizowanej w ramach etapu oceny sytuacji jest zidentyfikowanie i szczegółowa ocena czynników, które w różny sposób będą wpływać na realizację otrzymanego zadania oraz ustalenie kilku realnych sposobów jego wykonania, czyli wariantów działania.

Z analizy dostępnej literatury źródłowej [6;8;21] wynika, że ocena czynników wpływających na wykonanie zadania w wymiarze informacyjnym obejmuje:

– środowisko pola walki (warunki terenowe, atmosferyczne, propagacyjne, stanu bezpieczeństwa informacyjnego w obszarze przyszłych działań i in.);

– działania przeciwnika w wymiarze informacyjnym;

– potencjał zakłócania informacyjnego wojsk własnych;

– inne, które należy uwzględnić np. czas, możliwości zabezpieczenia logistycznego.

3.3.1.3.1. Ocena środowiska pola walki

Do oceny środowiska pola walki w wymiarze informacyjnym zespół działań informacyjnych centrum dowodzenia SD DWLąd powinien wykorzystać przytaczaną wcześniej procedurę informacyjnego przygotowania pola walki, w której należy uwzględnić również problemy rozwiązywane w ramach zakłócania informacyjnego (rysunek 3.1.), a mianowicie:

– wpływ konkretnych warunków terenowych na realizację przedsięwzięć zakłócania informacyjnego, zwłaszcza ze względu na możliwości techniczne syste-

mów i środków rozpoznania oraz systemów dowodzenia i kierowania uzbrojeniem przeciwnika. W tym celu należy wykorzystać oleat oceny terenu[10] (przeszkód terenowych), na którym zaznaczone są obszary trudno przejezdne, nieprzejezdne i ograniczające swobodę manewru. Dodatkowo należy określić obszary zakryte dla rozprzestrzeniania się energii elektromagnetycznej, w tym zakryte dla prowadzenia rozpoznania elektronicznego, rejony niesprzyjające rozmieszczeniu środków elektronicznych i zakłócania informacyjnego [6;8;20].

– wpływ konkretnych warunków atmosferycznych[11] na realizację przedsięwzięć zakłócania informacyjnego. W tym celu należy wykorzystać oleat oceny warunków atmosferycznych [6;8;20] sporządzony w zespole działań informacyjnych. Specjaliści z grupy zakłócania informacyjnego, wchodzącej w skład tego zespołu, powinni rozważyć wpływ pogody na teren i prowadzone działania oraz na rozmieszczenie i funkcjonowanie elementów rozpoznania przeciwnika oraz komponentów jego systemu dowodzenia i kierowania uzbrojeniem.

– określenie dróg podejścia i korytarzy manewru. W tym celu należy wykorzystać oleat dróg podejścia i korytarzy manewru, który wykonuje się dla całego zespołu działań informacyjnych centrum dowodzenia SD. Specjaliści z grupy zakłócania informacyjnego, analizując oleaty dróg podejścia powinni dodatkowo określić przeszkody terenowe, które utrudnią lub uniemożliwią manewr siłami i środkami rozpoznania oraz dowodzenia i kierowania uzbrojeniem przeciwnika [6;8;20]. Obok lądowych dróg podejścia analizie należy poddać korytarze i drogi podejścia w przestrzeni powietrznej [6;8;20]. Specjaliści z grupy zakłócania informacyjnego powinni wykorzystać w tym celu ilustracje korytarzy powietrznych i dróg podejścia samolotów i śmigłowców przygotowane przez oficerów z zespołu lotnictwa wojsk

---

[10] Wykonywany jest dla całego sztabu przez zespół oficerów z grupy topograficznej oceny terenu. Specjaliści z grupy zakłócania informacyjnego mogą korzystać z oleatów i opisów przeszkód terenowych wykonanych przez tę grupę, a specjalistyczną ocenę terenu mogą prowadzić samodzielnie lub z udziałem specjalistów grupy topograficznej oceny terenu [6;8;20].

[11] Analizę tę wykonują oficerowie grupy prognozy pogody. Specjaliści z grupy zakłócania informacyjnego korzystają z opracowanej już prognozy i wyciągają wnioski dotyczące wpływu warunków atmosferycznych na pracę przede wszystkim technicznych środków dowodzenia i kierowania uzbrojeniem oraz wchodzących w ich skład urządzeń elektronicznych [6;8;20].

lądowych [6;8;20]. Wnioski z analizy dróg podejścia i korytarzy manewru pozwalają na wstępne określenie obszarów zainteresowania.

Ocena czynników środowiska pola walki prowadzi do sformułowania następujących pytań dotyczących realizacji zadań zakłócania informacyjnego:

– w jaki sposób przeciwnik może zamaskować rzeczywiste rejony rozmieszczenia wojsk, a przede wszystkim elementy rozpoznania, komponenty systemu dowodzenia i kierowania uzbrojeniem oraz gdzie zorganizuje ich rejony pozorne?

– gdzie i w jakim stopniu może być pozorowane przegrupowanie wojsk, a przede wszystkim elementy systemów rozpoznania, dowodzenia i kierowania uzbrojeniem?

– jakie są możliwości wykorzystania warunków terenowych oraz miejscowych zasobów do realizacji przedsięwzięć zakłócania informacyjnego?

3.3.1.3.2. Ocena przeciwnika w aspekcie potrzeb zakłócania informacyjnego

Z przeprowadzonych analiz wynika, że ocena przeciwnika w wymiarze informacyjnym stanowi część składową prognozy zagrożenia ogólnego, a w procesie wypracowywania koncepcji zakłócania informacyjnego jest jednym z filarów służących poprawnemu jej opracowaniu. Do zasadniczych wymagań stawianych zespołowi działań informacyjnych centrum dowodzenia SD DWLąd prowadzącemu ocenę przeciwnika w sferze informacyjnej należą:

– szczegółowa i wnikliwa znajomość sił i środków wykorzystywanych przez przeciwnika na potrzeby rozpoznania, dowodzenia i kierowania uzbrojeniem;

– znajomość i świadomość celu działania;

– ciągłość i systematyczność pracy;

– bazowanie na wiarygodnych danych;

– uwzględnienie wszystkich zależności i czynników, mogących mieć wpływ na przyszłe działania przeciwnika w wymiarze informacyjnym;

– w wynikach prognozy zachowanie proporcji między szczegółowością i ogólnością;

– przestrzeganie terminowości podczas dokonywania prognozy;

– formułowanie wniosków z przeprowadzonej prognozy.

Prognoza działań przeciwnika w wymiarze informacyjnym powinna polegać na określeniu podstawowych danych dotyczących możliwości bojowych sił i środków wykorzystywanych przez przeciwnika na potrzeby dowodzenia i kierowania uzbrojeniem. Dane dotyczące stanu etatowego i wyposażenia stanowisk dowodzenia poszczególnych szczebli, środków kierowania uzbrojeniem, ugrupowania środków rozpoznania i zakłócania, a także środków elektronicznych, jakie mogą wystąpić na każdym szczeblu dowodzenia i w każdej jednostce organizacyjnej przeciwnika, powinny być gromadzone na bieżąco w komputerowych bazach danych. Z punktu widzenia zakłócania informacyjnego dokumenty prognozy działań przeciwnika w wymiarze informacyjnym należy wykonywać w postaci tabel, schematów, wykresów oraz graficznie na oleatach ugrupowania sił i środków. Prognoza działań przeciwnika w wymiarze informacyjnym powinna znaleźć odzwierciedlenie również w aneksie „zakłócanie informacyjne" do dyrektywy operacyjnej oraz w rozkazach bojowych jednostek zakłóceń.

Wynika stąd, że prognoza działań przeciwnika w wymiarze informacyjnym powinna obejmować (rysunek 3.2.):

– analizę wzorców doktrynalnych sił i środków wykorzystywanych przez przeciwnika na potrzeby dowodzenia i kierowania uzbrojeniem;

– opracowanie oleatu sytuacyjnego w wymiarze informacyjnym;

– wariantowanie działań przeciwnika w wymiarze informacyjnym;

– opracowanie oleatu zdarzeń w wymiarze informacyjnym;

– udział w opracowaniu oleatu wsparcia decyzji.

Doktrynalne wzorce działań sił i środków wykorzystywanych przez przeciwnika na potrzeby dowodzenia i kierowania uzbrojeniem[12].

Powinny zawierać wszystkie dane o sposobach działania i sprzęcie elektronicznym przeciwnika, zawarte w regulaminach i instrukcjach taktyczno-technicznych. Z powyższego wynika, że należy poddać wnikliwej analizie poszczególne komponenty systemów rozpoznania, dowodzenia i kierowania uzbrojeniem przeciwnika (w szczególności systemy łączności i informatyki; systemy radionawigacyjne; systemy i środki kierowania i sterowania uzbrojeniem; systemy walki informacyjnej) we współdziałaniu z zespołem planowania centrum dowodzenia SD DWLąd, z zespołem dowodzenia i łączności centrum wsparcia dowodzenia oraz z zespołami specjalistycznymi centrum wsparcia działań.

W ocenie systemów i środków rozpoznania przeciwnika należy uwzględnić:

– rodzaj środków rozpoznania bezpośredniego (agenturalnego, specjalnego, patrolowego) oraz pośredniego (elektronicznego i studyjnego);

– przewidywany ich zasięg i możliwości rozpoznawcze;

– parametry taktyczno–techniczne poszczególnych rodzajów środków i ich odporność na oddziaływanie ogniowe i elektroniczne;

– ich cechy rozpoznawcze, ochronę i obronę;

– taktykę ich użycia podczas walki, możliwości zastąpienia innymi środkami oraz powiązanie systemów rozpoznania z innymi środkami walki.

Ocenie tej powinny podlegać zarówno środki naziemne, jak i powietrzne, a w obszarze nadmorskim – także środki sił morskich.

---

[12] Głównymi składowymi rozpatrywanymi w czasie przygotowania dowolnego wzorca doktrynalnego są: sposób prowadzenia działań przez przeciwnika w każdym etapie walki (marsz, natarcie, obrona); sposób zabezpieczenia i wsparcia logistycznego działań; struktura organizacyjna; sprzęt i wyposażenie [6;8;20].

W ocenie systemów łączności i informatyki[13]– w uzgodnieniu z zespołem dowodzenia i łączności centrum wsparcia dowodzenia stanowiska dowodzenia DWLąd – należy rozpatrzyć:

– rodzaj i liczbę stanowisk dowodzenia i węzłów łączności, ich przestrzenne rozmieszczenie, strukturę oraz sposób rozwinięcia w terenie, system ochrony i obrony;

– rodzaj i liczbę kanałów transmisji (relacji) między poszczególnymi węzłami łączności i indywidualnymi użytkownikami oraz ich strefy dostępności elektromagnetycznej i podatności na rozpoznawanie[14];

– wykorzystanie poszczególnych pasm widma elektromagnetycznego (poszczególnych częstotliwości), rodzajów środków i zasady ich eksploatacji podczas walki;

– parametry techniczne określonych rodzajów środków łączności rzutujące na możliwości ich rozpoznania i zakłócania;

– sposoby i zakres utajniania wiadomości, możliwości maskowania i pozorowania systemów łączności oraz inne dane rzutujące na pracę środków łączności;

– podatność stacjonarnego systemu łączności sił zbrojnych przeciwnika, jego systemu telekomunikacyjnego, a także rozgłośni radiowych i telewizyjnych na oddziaływanie informacyjne.

Ocenie poddawany powinien być także stan bezpieczeństwa środków informatycznych będących w wyposażeniu zespołów funkcyjnych poszczególnych stanowisk dowodzenia. W tym celu powinny być analizowane dokumenty normatywne z zakresu bezpieczeństwa i przepisy prawne obowiązujące w wojskach własnych.

Wnioski z oceny systemu łączności i informatyki powinny dotyczyć: określenia możliwości zdezorganizowania poszczególnych systemów, sposobów organi-

---

[13] W specjalistycznej literaturze informatycznej systemy łączności i informatyki określane są jako systemy teleinformatyczne [16;21].

[14] Metodykę określania stref dostępności elektromagnetycznej przedstawiono w [21].

zacji obrony przed rozpoznaniem i zakłócaniem przez przeciwnika jego najważniejszych elementów składowych, a także przed niszczeniem węzłów łączności, kablowych linii łączności (przewodowych i światłowodowych) oraz ważnych środków łączności.

W ocenie systemów radionawigacyjnych – w uzgodnieniu z zespołem lotnictwa wojsk lądowych centrum wsparcia działań stanowiska dowodzenia DWLąd – należy rozpatrzyć:

– rodzaj i przeznaczenie systemu, zasięg jego funkcjonowania, powiązanie między systemami oraz urządzeniami autonomicznymi;

– parametry taktyczno–techniczne systemów i ich wpływ na sposoby prowadzenia działań bojowych przez przeciwnika i taktykę użycia środków walki;

– liczbę i dyslokację punktów radionawigacyjnych, jeśli są one rozmieszczone w rozpatrywanym obszarze działań.

Dużą wagę należy przywiązywać do oceny satelitarnych systemów radionawigacyjnych ze względu na ich bardzo duży zasięg i szerokie wykorzystanie przez różne rodzaje sił zbrojnych i wojsk.

Wnioski z oceny powinny dotyczyć określenia stopnia dezorganizacji poszczególnych rodzajów systemów, możliwości organizacji przez przeciwnika ich obrony przed rozpoznaniem, zakłócaniem oraz niszczeniem poszczególnych jego elementów. Mogą także dotyczyć ustalenia wpływu funkcjonowania tych systemów na sposób prowadzenia działań wojennych przez przeciwnika.

W ocenie systemów i środków kierowania uzbrojeniem oraz środków identyfikacji celów – w uzgodnieniu z zespołami specjalistycznymi centrum wsparcia działań stanowiska dowodzenia DWLąd – należy rozpatrzyć:

– rodzaj systemów[15], ich zasięg, warunki, w jakich mogą pracować, techniki stosowane w sterowaniu;

---

[15] Podział systemów i środków kierowania uzbrojeniem przedstawiono w podrozdziale 2.2.4.

– częstotliwości i zakresy pasm, na których pracują;

– możliwości zmiany warunków sterownia;

– punkty kierowania i ich wrażliwość na rozpoznanie, zakłócanie oraz niszczenie ogniowe;

– posiadane zabezpieczenia.

Podczas oceny systemów kierowania uzbrojeniem należy zwrócić uwagę na dużą różnorodność ich elementów nawet w jednym rodzaju środków. Często głowica jest wymienna, każdy zaś rodzaj głowicy może mieć inny system naprowadzania. Należy też zwrócić uwagę na warunki, w jakich poszczególne rodzaje środków mogą być użyte. Niewłaściwe warunki terenowe lub atmosferyczne mogą uniemożliwić użycie określonego rodzaju systemu.

Wnioski z takiej oceny powinny dotyczyć: określenia stopnia dezorganizacji poszczególnych rodzajów środków walki; możliwości organizacji ich obrony przez przeciwnika przed rozpoznaniem, a szczególnie w zakresie maskowania i pozorowania celów; możliwości ich obrony przed zakłócaniem; możliwości wykorzystania warunków terenowych i atmosferycznych do ograniczenia użycia broni precyzyjnego rażenia.

Oprócz danych dotyczących systemów i środków wykorzystywanych przez przeciwnika na potrzeby rozpoznania, dowodzenia i kierowania uzbrojeniem należy gromadzić charakterystyki osobowo-zawodowe dowódców poszczególnych szczebli dowodzenia (jednostek walki informacyjnej i jednostek elektronicznych), co pozwoli na ustalenie, jakich decyzji należy spodziewać się po określonym dowódcy i właściwą prognozę działań strony przeciwnej. Technika ich tworzenia jest różna w czasie pokoju i wojny. W czasie pokoju dane o przeciwniku powinny być dostarczane przez przełożonego, a w czasie wojny nowe informacje, potwierdzające działanie przeciwnika, jako pierwsze uzyskują pododdziały prowadzące rozpoznanie. Jest to więc obieg danych odwrotny w stosunku do pokojowego.

W obydwu sytuacjach **grupa zakłóceń informacyjnych** zespołu działań informacyjnych centrum dowodzenia SD DWLąd powinna być zobowiązana do po-

siadania aktualnej bazy danych o przeciwniku. Wzorce doktrynalne powinny być przechowywane w specjalnych bankach danych. Po rozpoczęciu działań operacyjnych wzorce opisujące siły i środki wykorzystywane przez przeciwnika na potrzeby rozpoznania, dowodzenia i kierowania uzbrojeniem powinny być wykorzystywane do wskazywania ważnych obiektów, które należy rozpoznać lub zakłócić. Służą one także do wskazania celów, które powinny być niszczone środkami ogniowymi.

Informacje zawarte we wzorcach działań informacyjnych powinny być potwierdzane w zespole działań informacyjnych centrum dowodzenia SD DWLąd, do którego napływają dane od jednostek pełniących dyżury bojowe lub od przełożonego. Zweryfikowane dane służą do opracowania modeli doktrynalnych w czasie opracowania prognozy, przed rozpoczęciem działań operacyjnych, a w czasie ich trwania – do ich korekty w zależności od zmian w ugrupowaniu przeciwnika. W zespole działań informacyjnych centrum dowodzenia SD DWLąd tworzy się kilka oddzielnych wzorców działań informacyjnych przeciwnika. Pierwszy zawiera dane o węzłach łączności, drugi dotyczy pozostałych urządzeń emitujących energię elektromagnetyczną (np. stacji radiolokacyjnych), a trzeci określa zasady użycia sił i środków walki informacyjnej, za który bezpośrednią odpowiedzialność powinni ponosić specjaliści z grupy obrony informacyjnej. Przykładowe oleaty przedstawione są m in. przez autorów w literaturze przedmiotu [20].

Do pełnego zobrazowania działań przeciwnika w wymiarze informacyjnym niezbędna jest również analiza działań przeciwnika powietrznego i systemów przeciwlotniczych. Dlatego ze szczególną uwagą powinno się analizować wzorce doktrynalne działań samolotów (śmigłowców) i elementów obrony przeciwlotniczej. W razie potrzeby należy wykonać odpowiednie wzorce porównawcze zasięgów wybranych stacji radiolokacyjnych w odniesieniu do środków napadu powietrznego przeciwnika [20].

Oleat sytuacyjny w wymiarze informacyjnym. W wyniku połączenia: oleatu oceny terenu, oleatu dróg podejścia i korytarzy manewru, wzorca doktrynalnego sposobu działania przeciwnika powinien powstać w grupie zakłócania infor-

macyjnego oleat sytuacyjny (sytuacji operacyjnej) w wymiarze informacyjnym[16]. Oleat ten należy wykonać na podstawie:

– danych o sytuacji bieżącej (z rozpoznania i zakłócania informacyjnego);

– wiadomości od przełożonego;

– danych od jednostek osłonowych i sąsiadów;

– innych źródeł (np. uchodźców, dezerterów, wojsk obrony terytorialnej, układu pozamilitarnego).

Dokument ten powinien odzwierciedlać graficzny obraz sytuacji bojowej w wymiarze informacyjnym połączony z koncepcją doktrynalną, zgodną z obowiązującymi zasadami rozmieszczenia sił i środków oraz prawdopodobnym zamiarem przeciwnika, w odniesieniu do terenu i warunków meteorologicznych. Tak przygotowany oleat powinien stanowić podstawę do dalszych rozważań nad prawdopodobnym działaniem sił i środków wykorzystywanych przez przeciwnika na potrzeby dowodzenia i kierowania uzbrojeniem[17].

Oleat należy sporządzać w takiej skali jak wykorzystywane mapy[18]. Wiadomości z banków danych (wzorce ugrupowania) należy przerysować na oleaty z zachowaniem norm, a następnie je uaktualniać na podstawie bieżących danych. Dla przejrzystego zobrazowania sytuacji wszystkie potwierdzone wiadomości o przeciwniku uzyskane od przełożonego i podwładnych należy traktować jako pewne i nanosić je linią ciągłą, natomiast położenie wynikające z zasad doktrynalnego działania należy przedstawić liniami przerywanymi. W ten sposób powstanie prawdopodobny obraz aktualnego położenia elementów wykorzystywanych przez przeciwnika na potrzeby dowodzenia i kierowania uzbrojeniem [20].

---

[16] Opracowanie tego oleatu rozpoczyna wg poglądów amerykańskich kolejny etap informacyjnego przygotowania pola walki, który nazywany jest integracją zagrożeń. L. Ciborowski, R. Polko, „Planowanie i organizowanie walki zbrojnej według poglądów NATO, cz. II: Informacyjna preparacja pola walki", wyd. AON Warszawa 1996, s. 29.

[17] W zespole G 2 mogą być wykonywane jeszcze dwa oleaty bieżącej sytuacji: na potrzeby rozpoznania i obrony informacyjnej.

[18] L. Ciborowski, R. Polko, „Planowanie i organizowanie walki zbrojnej wg poglądów NATO, cz. II. Informacyjna preparacja pola walki", AON, Warszawa 1996, s. 36.

Podczas oceny sytuacji w wymiarze informacyjnym należy poddać analizie i w miarę możliwości ustalić:

– ogólną liczbę obiektów przeciwnika w strefie odpowiedzialności rozpoznawczej wojsk lądowych;

– liczbę obiektów rozpoznania przeciwnika w strefie odpowiedzialności rozpoznawczej wojsk lądowych z podziałem na poszczególne rodzaje środków;

– liczbę i rodzaj obiektów przeciwnika, które ze względu na promieniowaną energię mogą się znaleźć w zasięgu rozpoznania w trakcie realizacji zadania przez wojska lądowe.

W zakończeniu oceny sytuacji w wymiarze informacyjnym należy sprecyzować wnioski wynikające z potrzeb zakłócania informacyjnego. Niezbędne jest określenie liczby obiektów i źródeł, których zakłócenie jest konieczne (lub pożądane) z uwagi na zadania realizowane przez wojska lądowe. Ponadto z grupą rozpoznania zespołu G 2 należy ustalić priorytety zakłócania poszczególnych obiektów i źródeł.

Kolejny etap pracy specjalistów **grupy zakłócania informacyjnego** powinien obejmować wypracowanie prawdopodobnych wariantów działania przeciwnika w wymiarze informacyjnym. Wypracowane warianty należy udostępnić pozostałym grupom zespołu działań informacyjnych, oficerom zespołu planowania centrum dowodzenia SD DWLąd, a także specjalistom zespołu dowodzenia i łączności z centrum wsparcia dowodzenia oraz zespołom specjalistycznym z centrum wsparcia działań do koordynowania działań jednostek wykonujących zadania bojowe.

Wariantowanie działań przeciwnika w wymiarze informacyjnym. Warianty zdarzeń w wymiarze informacyjnym powinny być opracowywane z uwzględnieniem oceny przygotowanej przez specjalistów z grupy rozpoznania zespołu działań informacyjnych centrum dowodzenia SD DWLąd. Na tej podstawie specjaliści grupy zakłócania informacyjnego powinni określić prawdopodobny wariant działania przeciwnika w wymiarze informacyjnym oraz sprecyzować potrzeby w zakresie uzupełniania brakujących danych. W wypracowanym wariancie powin-

no się uwzględnić wpływ pogody i terenu na działania bojowe przeciwnika oraz w określonym czasie opisowo lub w sposób graficzny prognozować, jak jego siły i środki będą wykonywać manewr (np. wzdłuż jakich dróg podejścia i korytarzy manewru, z wykorzystaniem jakich środków łączności). Ponadto należy brać pod uwagę, w jakim zakresie działanie przeciwnika może odbiegać od wzorców doktrynalnych lub w jaki sposób przeciwnik może zmieniać szerokość i głębokość ugrupowania czy rozmieszczenie elementów ugrupowania bojowego, aby sprostać wymaganiom pogody i terenu.

Rozważając wpływ pogody i terenu na działania przeciwnika odbiegające od wzorców doktrynalnych, należy dokonać analizy jego możliwości w zakresie rozpoznania, zapewnienia łączności, wykrywania celów, czy kierowania ogniem. Opracowywany wariant działań w wymiarze informacyjnym powinien uwzględniać dane z rozpoznania, które pozwolą na ustalenie obiektów przeciwnika oraz potencjalnych rejonów ich rozmieszczenia.

Należy rozważyć także działania przeciwnika mające na celu maskowanie stanowisk dowodzenia (punktów obserwacyjnych) przed rozpoznaniem i zakłóca-

niem. W obrębie danego segmentu korytarza manewru należy analizować przewidywane rozmieszczenie jednostek przeciwnika (węzłów łączności) oraz innych środków emitujących energię elektromagnetyczną. W trakcie wariantowania zdarzeń w wymiarze informacyjnym powinny zostać rozważone normy taktyczne, sposoby i możliwości działania przeciwnika, szczególnie te, które powodują uzyskanie korzystnego stosunku sił, tempa działań oraz zaskoczenia. Analiza danych z rozpoznania i wariantów zdarzeń informacyjnych powinna być skoncentrowana na określeniu linii widzialności optycznej i radiowej w pasach (rejonach) działań pierwszorzutowych związków taktycznych i związków operacyjnych wojsk lądowych. Ponadto należy ustalić obszary nadające się do ukrycia i maskowania bądź ugrupowania wojsk, bowiem zmniejszają one możliwość rozpoznania. Należy określić także obszary, które wojska własne mogą wykorzystać do tych samych celów. Analiza musi uwzględniać rejony, z których przeciwnik może uzyskać jak największy zasięg rozpoznania.

W wariantach zdarzeń w wymiarze informacyjnym należy ujmować również charakterystyki emisji elektromagnetycznych poszczególnych elementów oraz ich umiejscowienie. Pogoda i teren mają wpływ na wykorzystanie systemów rozpoznania i zakłócania przeciwnika, przede wszystkim zaś na pracę urządzeń emitujących energię elektromagnetyczną, wpływając na rozmieszczenie poszczególnych elementów tych systemów. Warianty użycia źródeł energii elektromagnetycznej powinny uwzględniać przyszłe działania i zmieniać się w zależności od czasu i miejsca na polu walki. Specjaliści grupy zakłócania informacyjnego powinni dokonywać analiz systemów elektronicznych i węzłów objętych wzorcami doktrynalnmi, współdziałając z grupami rozpoznania i obrony informacyjnej.

Po rozpoczęciu zbierania danych przez własne systemy rozpoznawcze, do poszczególnych komórek zespołu działań informacyjnych powinny być przekazywane aktualne dane o ugrupowaniu przeciwnika oraz o jego działaniach również w wymiarze informacyjnym. Specjaliści z grupy zakłócania informacyjnego powinni wstępnie opracowywać napływające dane i porównywać je z danymi zawartymi w wariantach sytuacji oraz we wzorcach działań. Pozwala to na:

– przekazywanie aktualnych danych przełożonemu i podległym jednostkom w trakcie wymiany wiadomości o przeciwniku;

– dokonywanie korekty wariantów działań w wymiarze informacyjnym;

– dokonywanie przez grupę wraz ze współpracującymi specjalistami z innych rodzajów służb identyfikacji emiterów energii elektromagnetycznej;

– korygowanie lokalizacji obiektów przeciwnika wykorzystywanych na potrzeby dowodzenia i kierowania uzbrojeniem na podstawie ich cech identyfikacyjnych, ustalenie linii rozgraniczenia wojsk oraz wyselekcjonowanie ważnych pod względem informacyjnym celów i obiektów.

Warianty działania przeciwnika powinny być poddawane weryfikacji za pomocą komputerowych i symulacyjnych modeli oceny zagrożenia w wymiarze informacyjnym[19], w trakcie gier wojennych (taktycznych) itp.

Efektem pracy specjalistów z grupy zakłócania informacyjnego powinno być opracowanie prawdopodobnego wariantu działania przeciwnika w wymiarze informacyjnym, po czym należy dokonać jego ostatecznej weryfikacji podczas spotkań roboczych zespołu działań informacyjnych i zespołu planowania centrum dowodzenia SD DWLąd. Finalnym efektem tych spotkań powinien być wybór wariantu działania w wymiarze informacyjnym[20] (wariant powinien uwzględniać działania przeciwnika przewidywane przez grupę rozpoznania z zespołu działań informacyjnych). Na jego podstawie należy przystąpić do szczegółowego planowania zakłócania. Jeśli wariant działania przeciwnika w wymiarze informacyjnym proponowany przez zespół działań informacyjnych nie zostanie zaakceptowany, należy rozpatrzyć pozostałe warianty, wcześniej odrzucone.

Przy wariantowaniu działań przeciwnika powinien również powstać plan alternatywny (zapasowy), który powinien znacząco odbiegać od wzorców doktrynalnych. Taki wariant działania przeciwnika, zazwyczaj przeczy logice działania i czasami jest sprzeczny z dotychczas znanymi zasadami walki. Planem alternatywnym może być także odrzucony wariant działania w wymiarze przeciwnika z niektórymi elementami działania sprzecznymi z obowiązującymi normami. Przykładowe warianty działań przeciwnika w wymiarze informacyjnym zilustrowane są w literaturze przedmiotu [20].

Oleat zdarzeń w wymiarze informacyjnym. Na podstawie wybranego wariantu działania powinien być sporządzany przez specjalistów grupy zakłócania informacyjnego (w uzgodnieniu z grupą rozpoznania i grupą obrony zespołu działań informacyjnych) oleat zdarzeń w wymiarze informacyjnym. Swoją formą nie powi-

---

[19] Do oceny zagrożenia radioelektronicznego, np. systemu łączności korpusu można wykorzystać modele komputerowe i symulacyjne:
– A. Barczak, J. Janczak, K. Mamcarz, „Komputerowy model oceny zagrożenia radioelektronicznego perspektywicznego systemu łączności związku operacyjnego wojsk lądowych". Praca naukowo-badawcza, Zegrze: WSOWŁ 1996.
– A. Barczak, J. Janczak, K. Mamcarz, „Model symulacyjny zagrożenia radioelektronicznego systemu łączności związku operacyjnego wojsk lądowych". Praca naukowo-badawcza, Zegrze WSOWŁ, 1997.

nien odbiegać od oleatu zdarzeń wykonywanego przez oficerów z grupy rozpoznania[21]. W grupie zakłócania informacyjnego powinno być wyeksponowane położenie sił i środków wykorzystywanych przez przeciwnika na potrzeby dowodzenia i kierowania uzbrojeniem, zaznaczonych zazwyczaj w określonych odstępach czasowych. Oleat zdarzeń powinien być sporządzany na podstawie jednego, najbardziej prawdopodobnego wariantu działania przeciwnika. Położenie wojsk przeciwnika należy oceniać według linii czasowych co 1, 2, a nawet co 4 godziny w zależności od szczebla na jakim się rozpatruje lub według zasięgu środków ogniowych[22]. Linie czasowe (TPL)[23] powinny uwzględniać i ujmować wszystkie drogi podejścia i korytarze manewru. Nowe położenie przeciwnika należy zaznaczać przewidywaną rubieżą w terenie, niekiedy rubież ta powinna otrzymać nazwę własną. Poza tym należy określić rejony (obszary) szczególnego zainteresowania (NAI)[24]. Są to z zasady takie obszary, w których elementy rozpoznania są w stanie określić sposób działania przeciwnika. W ramach obszarów NAI należy wyznaczyć punkty kontrolne, w stosunku do których trzeba rozmieścić elementy rozpoznawcze. Połączenie danych z własnych elementów rozpoznawczych oraz z rozpoznania przełożonego pozwala na określenie ważnych zdarzeń na polu walki oraz wytypowanie elementów walki informacyjnej, które dostarczają danych na temat kierunków działań prowadzonych przez przeciwnika i celów, jakie pragnie osiągnąć. Specjaliści grupy zakłócania informacyjnego dokonujący analizy powinni dostrzec różnicę pomiędzy zdarzeniami, które już nastąpiły i zostały rozpoznane, a tymi, które są tylko przewidywane. Ponadto powinni kontrolować działania przeciwnika zmierzające do wprowadzania w błąd, aby nie dopuścić do skupienia wysiłku własnych jednostek zakłócania na obiektach (obszarach) pozornych.

Po rozpoczęciu działań operacyjnych wiedza o tym, gdzie i kiedy może nastąpić istotne zdarzenie na polu walki, może zostać wzbogacona[25]. Należy mieć na uwadze, że rejony zainteresowania celami w wymiarze informacyjnym nie zawsze będą się znajdować na drogach podejścia. Często występować będą poza nimi ze względu na specyfikę pracy oraz możliwości bojowe sprzętu, głównie elektronicz-

---

[20] Wynikiem analizy są wnioski – odpowiedzi na pytania: co?, kiedy?, gdzie?; jak?, w jakim celu?

[21] W wypadku ograniczonego czasu na planowanie może być wykonywany wspólny oleat zdarzeń dla całego zespołu działań informacyjnych SD korpusu.

[22] W armii amerykańskiej co godzinę, dwie, lub cztery w zależności od szczebla dowodzenia, a w Bundeswehrze ilość linii czasu określana jest wg zasięgu środków ogniowych.

[23] TPL – ang. Time Phase Line.

[24] NAI – ang. Named Areas of Interest.

[25] Przeciwnik będzie dążyć do ograniczenia strumienia danych o swoim działaniu i stan naszej wiedzy może nie zmienić się mimo rozpoczęcia działań.

nego. Rejony te są jednak ważne, gdyż znajdują się w najbardziej prawdopodobnych miejscach decydujących zdarzeń czy też działań na polu walki oraz mogą w nich występować cele wysoko opłacalne[26].

Rejony zainteresowania powinny stanowić podstawę do wariantowania zdarzeń w wymiarze informacyjnym, ponieważ wskazują kierunki działania przeciwnika, ogniskują zbieranie danych oraz są uwzględniane w opracowaniu wymagań wobec informacji pozyskiwanych przez rozpoznanie. Aby trafnie określić zamiary przeciwnika, jego aktywność w obrębie dróg podejścia lub obszaru określonego jako NAI może być porównana ze wskaźnikami aktywności występującymi w obszarze innego NAI, w obrębie innej drogi podejścia. Poziom aktywności może również stanowić dla rozpoznania i zakłócania informacyjnego wskazówkę o istnieniu jakiegoś urządzenia w obrębie obszaru niekontrolowanego. Rejony zainteresowania są bowiem celami dla zakłócania informacyjnego. Numeracja NAI powinna być ustalona podczas spotkań koordynacyjnych wewnątrz zespołu działań informacyjnych. Ustalenia te są niezbędne dla wyeliminowania błędów i dwuznaczności w oznaczeniach lub oznaczeń dublujących, ponieważ niektóre obszary NAI mogą się pokrywać w różnych zespołach. Przykłady oleatu zdarzeń w wymiarze informacyjnym przedstawione są w literaturze przedmiotu [20].

Udział w opracowaniu oleatu wsparcia decyzji. Oleat ten w zasadzie wykonuje zespół planowania centrum dowodzenia SD DWLąd, przy współudziale zespołu działań informacyjnych oraz zespołu artylerii z centrum wsparcia działań[27]. Specjalista zespołu działań informacyjnych powinien wrysować zaakceptowany wariant działania przeciwnika (w którym należy uwzględnić również jego siły i środki wykorzystywane na potrzeby dowodzenia i kierowania uzbrojeniem), dający podstawy do wykonania tego oleatu.

Oleat wsparcia decyzii – jak określono w materiałach źródłowych [23;60; 62;88] jest końcowym i zarazem najważniejszym dokumentem procesu informacyjnego przygotowania pola walki. Wykonywany jest na potrzeby śledzenia prognozowanej sytuacji przeciwnika i powinien być pomocny dowódcy w procesie podejmowania decyzji. Oleat wsparcia decyzji nie ogranicza kompetencji dowódcy, lecz wskazuje wydarzenia oraz możliwe działania przeciwnika, w określonym miejscu i czasie, które wymagać będą podjęcia określonych decyzji. Temu właśnie służą

---

[26] Cele o znaczeniu decydującym dla działania wojsk przeciwnika.
[27] Jego wykonanie jest „podstawową funkcją wyznaczonej w tym celu przez dowódcę triady".

określone na wzorcu wsparcia decyzji tzw. obszary zainteresowania celami (TAI[28]), punkty decyzyjne (DP[29]) i linie czasowe. Przykładowe oleaty wsparcia decyzji z uwzględnieniem wymiaru informacyjnego przedstawione są w literaturze przedmiotu [20].

Wnioski. Z oceny działania przeciwnika w wymiarze informacyjnym wypływają określone wnioski odpowiadające na następujące pytania[30]:

– w jakim rejonie (kierunku) i w jakim czasie – z uwagi na działanie przeciwnika – należy określić punkt ciężkości w zakresie realizacji przedsięwzięć zakłócania informacyjnego?

– przeciwko jakim rodzajom i środkom wykorzystywanym przez przeciwnika na potrzeby rozpoznania, dowodzenia i kierowania uzbrojeniem należy przede wszystkim zaplanować przedsięwzięcia zakłócania informacyjnego?

– w jaki sposób najskuteczniej wprowadzić poszczególne elementy rozpoznania przeciwnika w błąd?

– jakie środki wykorzystywane przez przeciwnika na potrzeby rozpoznania, dowodzenia i kierowania uzbrojeniem należy zniszczyć, a jakie obezwładnić zakłóceniami.

3.3.1.3.3. Ocena wojsk własnych w zakresie zakłócania informacyjnego

Podczas ocena wojsk własnych w zakresie zakłócania informacyjnego należy określić możliwości taktyczno-bojowe środków i systemów zakłócania informacyjnego, a ponadto należy dokonać oceny czynnika czasu oraz warunków i możliwości zabezpieczenia logistycznego (materiałowego i technicznego).

---

[28] TAI – ang. Target Areas of Interest.
[29] DP – ang. Decision Point.
[30] Proces prognozowania działań kończy się z chwilą podjęcia decyzji przez dowódcę i ogłoszenia zamiaru. Zespół G 2, niezależnie od tego jak obszerna i dokładna wydaje się być dokonana analiza i ocena terenu i pogody, zawsze musi liczyć się z innym, odmiennym od przyjętych schematów działaniem przeciwnika oraz zawsze musi być przygotowany do powtórzenia cyklu ocen i przeprowadzenia analiz od początku.

W **ocenie środków i systemów zakłócania**[31] wojsk własnych należy uwzględnić:

- rodzaj i liczbę systemów zakłócania w obszarze odpowiedzialności DWLąd oraz sił powietrznych;
- ich możliwości bojowe i techniczne, warunki, czas i sposoby użycia;
- rejony rozwinięcia własnych sił i środków (strefy dyżurowania samolotów), obszary oraz głębokość oddziaływania;
- możliwości niszczenia obiektów zakłócania przeciwnika za pomocą broni samosterującej naprowadzonej na źródło promieniowania energii elektromagnetycznej;
- możliwości i przewidywany zasięg użycia środków pasywnych oraz warunki atmosferyczne sprzyjające użyciu tego rodzaju środków;
- możliwości użycia broni elektromagnetycznej (powodującej niszczenie układów elektronicznych), obszary jej użycia oraz zasięg zniszczeń.

Przy ocenie środków zakłócania należy uwzględnić też rodzaj tych środków, które mogą być najbardziej zagrożone.

Ocena czynnika czasu ma szczególne znaczenie dla rozwiązywania problemu zsynchronizowania trzech elementów: sił, przestrzeni i czasu, to znaczy zidentyfikowania rozwiązań pozwalających na rozmieszczenie wystarczających sił we właściwym obszarze i w nakazanym czasie. Czas jest czynnikiem ograniczającym swobodę działania. Dotyczy to również realizacji przedsięwzięć zakłócania informacyjnego. Wnioski wynikające z oceny czasu powinny dotyczyć:

- określenia czasu niezbędnego na zaplanowanie zadań zakłócania informacyjnego w operacjach wojsk lądowych;
- czasu rozpoczęcia i okresów organizowania przedsięwzięć pozornych z punktu widzenia faktycznych działań wojsk;

---

[31] Z uwagi na restrukturyzację wojsk lądowych autorzy pracy badawczej nie odnoszą się swoich rozważaniach do konkretnej struktury organizacyjnej sił i środków zakłócania informacyjnego.

– rozpoczęcia i zakończenia realizacji poszczególnych zadań zakłócania informacyjnego;

– czasu prowadzenia kontroli zaplanowanych przedsięwzięć zakłócania informacyjnego.

Podczas **oceny warunków i możliwości zabezpieczenia logistycznego** – w uzgodnieniu z zespołem materiałowym i technicznym centrum zabezpieczenia działań stanowiska dowodzenia DWLąd – należy rozpatrywać:

– ilość środków niezbędnych do prowadzenia zakłócania informacyjnego.

– ilość, rodzaj etatowych środków i materiałów niezbędnych do realizacji poszczególnych zadań zakłócania informacyjnego;

– ilość, rodzaj uzbrojenia, sprzętu zdobycznego i uszkodzonego oraz możliwości wykorzystania go do realizacji przedsięwzięć zakłócania informacyjnego.

Uogólnione wnioski z oceny ww. czynników powinny prowadzić do wypracowania koncepcji prowadzenia zakłócania informacyjnego w odniesieniu do ustalonych w zespole planowania centrum dowodzenia SD DWLąd i przedstawionych w toku **odprawy koordynacyjnej**[32] wariantów działania wojsk lądowych.

Wnioski te powinny dotyczyć m.in.[33]:

– określenia elementów ugrupowania operacyjnego przeciwnika, które przede wszystkim należy zakłócić, oraz miejsca punktu ciężkości zakłócania informacyjnego;

– określenia sił i środków jednostek bojowych, jakie powinny być wykorzystane do realizacji przedsięwzięć zakłócania informacyjnego (w uzgodnieniu ze specjalistami zespołu planowania centrum dowodzenia SD DWLąd.);

– wyspecyfikowania zadań, które należy postawić związkom operacyjnym i taktycznym.

---

[32] W odprawie koordynacyjnej bierze udział szef zespołu działań informacyjnych, w której przedstawia – w razie potrzeby – wnioski z zagrożenia w wymiarze informacyjnym oraz z oceny wojsk własnych w zakresie zakłócania informacyjnego.

[33] Wnioski z oceny wojsk własnych należy ujmować w apendyksie do aneksu „zakłócanie informacyjne".

Koncepcje prowadzenia zakłócenia informacyjnego dla poszczególnych wariantów działania wojsk lądowych. W wyniku rozważenia poszczególnych czynników wpływających na wykonanie zadania oraz po zapoznaniu się z przyjętymi wariantami działań operacyjnych wojsk lądowych grupa zakłócania informacyjnego (specjalista odpowiedzialny na ocenę własnych wojsk) powinien opracować koncepcje zakłócania informacyjnego dla poszczególnych wariantów. Oznacza to, że w ramach tej czynności powinno powstać, niejako równolegle, kilka przyszłych planów prowadzenia zakłócania informacyjnego w operacjach wojsk lądowych.

Badania literatury źródłowej [6;8;20;35] oraz materiały z ćwiczeń prowadzonych w AON[34] wskazują, że koncepcja zakłócania informacyjnego dla każdego wariantu operacji wojsk lądowych powinna zawierać:

– określenie punktu (punktów) ciężkości w zakresie realizacji przedsięwzięć zakłócania informacyjnego;

– przedsięwzięcia niezbędne do realizacji zadań zakłócania informacyjnego w operacji (operacjach) wojsk lądowych;

– wstępny podział sił i środków przeznaczonych do realizacji zadań zakłócania informacyjnego;

– wstępne ugrupowanie sił i środków do zakłócania oraz pozorowania obiektów pozornych.

W miarę posiadanego czasu należy wzbogacić je, np. tabelami podziału zadań na potrzeby zakłócania informacyjnego oraz schematami (oleatami) zawierającymi dane dające się zilustrować. Należy mieć na uwadze, że szczególnie ważne zadania zakłócania informacyjnego nie powinny być ujawniane bez zgody dowódcy, a zatem i bezpośrednio odzwierciedlane w tych dokumentach.

---

[34] W latach 1997 – 2000.

3.3.1.4. Rozważenie i porównanie koncepcji zakłócania informacyjnego w poszczególnych wariantach działania wojsk lądowych

Rozważenie wariantów działania jest kolejną czynnością sztabu w zakresie planowania, której celem jest określenie zalet i wad poszczególnych wariantów wykonania zadania w konfrontacji z prawdopodobnym sposobem działania przeciwnika. Najczęściej stosowaną techniką powinna być symulacja[35] przyszłych działań zgodnie z przyjętymi wariantami, będąca próbą określenia przyszłych zdarzeń zgodnie z zasadą: akcja – reakcja – przeciwreakcja.

Uczestnikami symulacji powinni być członkowie zespołu planowania (po stronie wojsk własnych) oraz zespołu działań informacyjnych (po stronie przeciwnika) centrum dowodzenia SD DWLąd. Uczestniczyć w niej powinni również przedstawiciele zespołów z centrum wsparcia dowodzenia, centrum wsparcia działań i innych komórek (w tym specjalista grupy zakłóceń informacyjnych) stosownie do ustaleń szefa sztabu. W miarę rozważania kolejnych wariantów działania (symulacji) przedstawiciel G 2 (grupy zakłócania informacyjnego) powinien dokonać zestawienia zalet i wad każdego wariantu, z punktu widzenia prowadzenia zakłócania.

W trakcie symulacji – jeżeli dowództwo dysponuje wystarczającą ilością czasu – powinny być identyfikowane również fakty i przewidywania niezbędne do sporządzenia planu synchronizacji działań (wstępnego zarysu graficzno-tabelarycznego), po jednym dla każdego wariantu działania. W planach tych powinny być skoordynowane również przedsięwzięcia zakłócania informacyjnego. W tym celu oficerowie (specjaliści) rodzajów wojsk i służb, przygotowując koncepcje użycia swych wojsk, powinni uwzględniać również problemy zakłócania informacyjnego poszczególnych komponentów systemów dowodzenia i kierowania uzbrojeniem przeciwnika.

---

[35] Etapy postępowania w trakcie przygotowywania i przeprowadzania symulacji oraz podstawowe techniki rozważania wariantów działania (wg etapów, kierunków, obiektów) są wystarczająco przedstawione w literaturze przedmiotu [6;8;20].

Sformułowane w wyniku symulacji wnioski i oceny poszczególnych wariantów działania, a wraz z nimi i koncepcji prowadzenia zakłócania informacyjnego powinny być wykorzystane do ich porównania, a zatem do ich przyjęcia, zmodyfikowania bądź wręcz odrzucenia jako nie spełniające wymaganych kryteriów.

Porównanie koncepcji zakłócania informacyjnego w poszczególnych wariantach działania. Realizowane na tym etapie czynności powinny polegać na rzeczowym porównaniu ze sobą przygotowanych i rozważonych wariantów działania oraz na wyłonieniu tego wariantu, który będzie rekomendowany dowódcy. Proces porównania dokonywany jest w toku **odprawy koordynacyjnej**, a jej przebieg jest ustalany przez szefa sztabu, który jest jej organizatorem. W jej trakcie poszczególne zespoły funkcjonalne SD w formie krótkich meldunków powinny przedstawić wyniki swojej pracy.

W toku swoich wystąpień szef zespołu działań informacyjnych centrum dowodzenia SD DWLąd, oprócz oceny środowiska pola walki oraz wojsk przeciwnika, powinien przedstawić koncepcje prowadzenia rozpoznania, zakłócania i obrony informacyjnej[36] we wszystkich rozpatrywanych wariantach działania[37]. Istotą jego wystąpienia w odniesieniu do zakłócania informacyjnego powinno być precyzyjne wyartykułowanie zalet i wad poszczególnych wariantów wpływających na sposób wykonania zadań zakłócania. Odprawa koordynacyjna powinna zatem doprowadzić do jeszcze większej koordynacji zarysu planu operacji wojsk lądowych z opracowaną koncepcją prowadzenia w jej toku zakłócania informacyjnego.

Końcowym przedsięwzięciem odprawy koordynacyjnej jest porównanie wariantów działania, które w zależności od decyzji szefa sztabu może być realizowane metodą rozważenia wad i zalet, metodą głosowania lub metodą kryteriów (określonych przez dowódcę podczas analizy zadania). Należy mieć na uwadze, że porównanie wariantów działania jest jedną z najważniejszych czynności w procesie pracy

---

[36] Koncepcje prowadzenia zakłócania informacyjnego we wszystkich rozpatrywanych wariantach działania przygotowuje grupa zakłócania informacyjnego zespołu G 2.

[37] W wypadku ograniczonego czasu trwania odprawy koordynacyjnej może zaistnieć sytuacja, kiedy będzie musiał wskazać jedynie wariant najkorzystniejszy z punktu widzenia wykonania zadań obrony informacyjnej.

dowództwa. Ma bowiem na celu wyłonienie wariantu rekomendowanego dowódcy. Kończy ono również etap oceny sytuacji.

3.3.2. Decyzja i zamiar dowódcy w zakresie zakłócania informacyjnego

Zgodnie z ramowym układem cyklu decyzyjnego (rysunek 3.1.) podjęcie przez dowódcę decyzji i ogłoszenie zamiaru do operacji odbywa się podczas **odprawy decyzyjnej**[38]. Za jej przebieg i organizację ponosi odpowiedzialność szef sztabu[39]. Na odprawie decyzyjnej prezentowane są wyniki pracy sztabu, a szef sztabu wskazuje rekomendowany wariant działania.

W trakcie swoich wystąpień szef zespołu działań informacyjnych oprócz oceny środowiska pola walki oraz wojsk przeciwnika powinien przedstawić **propozycję prowadzenia rozpoznania, zakłócania[40] i obrony informacyjnej w operacji wojsk lądowych**, a ponadto powinien być w gotowości do udzielenia odpowiedzi na ewentualne pytania dowódcy[41], w celu wyjaśnienia wszelkich wątpliwości wykonania zadań zakłócania informacyjnego. Propozycja ta stanowi rozwinięcie koncepcji prowadzenia zakłócania informacyjnego dla wariantu rekomendowanego. Powinna zatem zawierać:

– określenie punktu (punktów) ciężkości w zakresie realizacji przedsięwzięć zakłócania informacyjnego;

– przedsięwzięcia niezbędne do realizacji zadań zakłócania informacyjnego w operacji (operacjach) wojsk lądowych;

---

[38] W odprawie tej obok dowódcy i szefa sztabu uczestniczą kierownicy zespołów organizacyjno – funkcjonalnych stanowiska dowodzenia.

[39] Przykład układu odprawy decyzyjnej przedstawiony jest w: [6;39].

[40] Propozycję prowadzenia zakłócania informacyjnego w operacjach wojsk lądowych przygotowuje grupa zakłócania informacyjnego zespołu działań informacyjnych.

[41] Należy zaznaczyć, że odprawa decyzyjna nie stanowi forum dla dyskusji oficerów sztabu.

– podział sił i środków przeznaczonych do realizacji zadań zakłócania informacyjnego;

– sposób ugrupowania i rozwinięcia środków do zakłócania oraz do imitowania obiektów pozornych oraz powiązanie ich z systemami rzeczywistymi;

– priorytety w zakresie realizacji zadań zakłócania informacyjnego.

Końcową czynnością odprawy decyzyjnej jest dokonanie przez dowódcę wyboru jednego z przedstawionych przez sztab wariantów działania i ogłoszenie go jako swojej decyzji. Na bazie tej decyzji dowódca ogłasza swój zamiar działania[42]. Wskazuje w nim między innymi priorytety we wsparciu i zabezpieczeniu działań. Uwzględniony powinien być również wymiar informacyjny.

Bezpośrednio po odprawie decyzyjnej szef zespołu działań informacyjnych powinien zapoznać z zamiarem dowódcy podległy zespół oraz wydać końcowe wytyczne do planowania szczegółowego oraz opracowania dokumentów planistycznych i rozkazodawczych, określając czas jego zakończenia. Dopiero w wyniku sprecyzowania powyższych danych grupa zakłócania informacyjnego ma podstawy do ostatecznego opracowania dokumentów na potrzeby zakłócania w operacji (operacjach) wojsk lądowych.

3.3.3. Opracowanie dokumentów do zakłócania informacyjnego

Opracowanie dokumentów na potrzeby zakłócania informacyjnego stanowi końcowy etap fazy planowania (rysunek 3.1.) sztabu dowództwa wojsk lądowych. Do czasu opracowania niniejszej pracy badawczej nie zostały wypracowane wzory dokumentów na potrzeby zakłócania informacyjnego.

---

[42] Struktura zamiaru ogłaszanego przez dowódcę na koniec odprawy decyzyjnej nie jest sformalizowana. Zamiar działania może zawierać: podział sił; sposób działania; elementy dowodzenia i koordynacji; ugrupowanie; podział odpowiedzialności w obszarze tyłowym; priorytety we wsparciu i zabezpieczeniu działań; łączność. „Regulamin działań wojsk lądowych", wyd. DWLąd., Warszawa 1999, s. 55.

Z badań wynika, że dokumenty te powinny w formie i treści być zbliżone do dokumentów opracowywanych w sztabie dowództwa i obowiązujących w wojskach. Stąd też przez analogię można określić dokumenty jakie powinny być opracowywane na potrzeby zakłócania informacyjnego, tj.:

1. Planistyczne – „Plan zakłócania informacyjnego w operacjach wojsk lądowych" wraz z załącznikami.

2. Rozkazodawcze – Aneks H „Zakłócanie informacyjne" wraz z apendyksami.

3. Inne dokumenty (robocze, sprawozdawcze) – w zależności od potrzeb.

Plan zakłócania informacyjnego w operacjach wojsk lądowych. Na podstawie ogłoszonego przez dowódcę zamiaru działania oraz wcześniejszych ustaleń zawartych w koncepcji i propozycji zakłócania informacyjnego należy opracować plan jego prowadzenia w operacjach wojsk lądowych. Bezpośrednią odpowiedzialność za jego opracowanie powinien ponosić szef grupy zakłócania informacyjnego.

Plan zakłócania informacyjnego[43] w operacjach wojsk lądowych powinien być opracowywany w formie opisowo – tabelarycznej (część 1) i uzupełniony załącznikami (oleatami) w formie graficznej (część 2).

Część tabelaryczna planu powinna być wykonywana przez oficerów grupy zakłócania informacyjnego zespołu działań informacyjnych SD DWLąd we współdziałaniu z oficerami planującymi uderzenia lotnicze i artyleryjskie. W górnej części planu (tabeli) należy wyszczególnić siły i środki zakłócające, a na osi czasu nanieść dla nich zadania z zakresu zakłócania informacyjnego. W dolnej części planu (tabeli) wymienia się zadania stawiane zakłócaniu informacyjnemu oraz obszary zainteresowania (obiekty), na które będzie skierowane oddziaływanie. Wskazuje się także obszary przeciw którym prowadzone będzie zakłócanie informacyjne oraz

---

[43] Plan zakłócania informacyjnego jest jednym z trzech dokumentów planistycznych jakie powinny być wykonywane w G 2 w zakresie walki informacyjnej. Na potrzeby rozpoznania opracowuje się „Plan zbierania informacji", a na potrzeby obrony powinien być opracowywany „Plan obrony informacyjnej". Poza tym podczas opracowywania planu działań wojsk lądowych oficerowie zespołu G 2 SD DWLąd wrysowują „decyzję" (wariant działania) przeciwnika dającą podstawy do wykonania wzorca wsparcia decyzji (w wyniku wypracowanych zagadnień w informacyjnym przygotowaniu pola walki) [6;8].

obiekty, które objęte będą tego rodzaju oddziaływaniem. W wypadku planowania użycia nadajników zakłóceń jednorazowego użycia należy określić w tym planie ilość kompletów oraz sposób wykonania tego zadania. Oleat (przykład) planu zakłócania informacyjnego przedstawiono w załączniku 1.

Cześć graficzna planu zakłócania informacyjnego powinna być wykonywana w ścisłym porozumieniu z grupą rozpoznania i obrony informacyjnej zespołu działań informacyjnych oraz we współdziałaniu z oficerami planującymi uderzenia lotnicze i artyleryjskie.

Dokument ten sporządzany na folii lub kalce technicznej powinien obejmować (załącznik 2):

- punkty odniesienia;
- rubież styczności wojsk;
- przedni skraj bronionego obszaru (FEBA);
- linie rozgraniczenia;
- zasadnicze i zapasowe rubieże rozwinięcia pododdziałów zakłócania informacyjnego (na rubieżach należy zaznaczyć dozwolone rejony rozwinięcia środków zakłócania);
- zadania pododdziałów zakłócania informacyjnego;
- zasięgi zakłócania rozpoznania i kierowania uzbrojeniem;
- planowane rejony użycia NZJU i ich zasięgi;
- stanowiska ogniowe pododdziałów artylerii strzelającej pociskami z NZJU;
- stanowiska dowodzenia sztabów własnego, nadrzędnego i współdziałającego;
- lądowiska śmigłowców walki informacyjnej (zakłócających);
- obszary i rejony zainteresowania.

Problematyka zakłócania informacyjnego powinna mieć również odzwierciedlenie w planach użycia rodzajów wojsk i służb (w częściach graficznych, opisowych) i w odpowiednich apendyksach do aneksów. Należy w nich uwzględnić:

– wnioski z oceny systemów przeciwnika wykorzystywanych na potrzeby dowodzenia i kierowania uzbrojeniem w odpowiednich rodzajach wojsk lub służb;

– wnioski z oceny potencjału wojsk własnych na potrzeby zakłócania informacyjnego;

– zakres realizacji zadań zakłócania informacyjnego przewidzianych dla ich rodzaju wojsk lub służb;

– czynności (przedsięwzięcia) pozorne i zgranie ich z faktycznym działaniem ich rodzaju wojsk, czy służb;

– główne przedsięwzięcia przeciwrozpoznawcze;

– procedury postępowania podczas wystąpienia zakłóceń celowych lub interferencyjnych (wzajemnych);

– inne – wg potrzeb.

Sporządzenie planu zakłócania informacyjnego umożliwia przygotowanie wstępnego zarządzenia operacyjnego sztabu DWLąd, które może być wysłane do wojsk biorących udział w realizacji przedsięwzięć zakłócania. Umożliwia ono wcześniejsze postawienie zadań, zwłaszcza jeżeli czas na przygotowanie działań jest ograniczony. Układ wstępnego zarządzenia operacyjnego jest taki sam jak dyrektywy operacyjnej. Punkty, których nie można na tym etapie opracować, należy pozostawić puste.

Aneks „H – zakłócanie informacyjne" do dyrektywy operacyjnej.

Aneks „H – zakłócanie informacyjne" opracowywany jest równolegle z rozkazem operacyjnym DWLąd[44]. Bezpośrednią odpowiedzialność za jego sporządzenie po-

[44] W sporządzeniu rozkazu operacyjnego biorą udział również oficerowie zespołu działań informacyjnych, opracowując punkt 1 (sytuacja), 3c (zadania dla elementów wspierających), 3d (wytyczne koordynujące i współdziałanie w zakresie realizacji zadań obrony informacyjnej) oraz zasilają w niezbędne informacje inne punkty rozkazu.

winien ponosić szef grupy zakłócania informacyjnego. Układ aneksu, który przedstawiono w załączniku 3 pod względem formy i treści powinien być zgodny z aneksami[45] opracowywanymi w zespole działań informacyjnych i w innych zespołach specjalistycznych SD DWLąd.

Do aneksu powinny być opracowywane niezbędne apendyksy, np.:

– ocena działań przeciwnika w wymiarze informacyjnym;

– wnioski z oceny wojsk własnych na potrzeby zakłócania informacyjnego;

– tabelaryczny plan koordynacji przedsięwzięć w zakresie zakłócania informacyjnego;

– rejony i częstotliwości zastrzeżone;

– dokumenty normatywne z zakresu bezpieczeństwa informacyjnego;

– inne, według potrzeb.

Z analizy wzorów dokumentów rozkazodawczych, wykonywanych podczas ćwiczeń w AON i dokumentów standaryzacyjnych NATO wynika, że apendyksy mogą mieć formę tekstową, graficzną lub tekstowo – graficzną. W gruncie rzeczy zależy ona od wykonawcy danego dokumentu.

3.4. W fazie stawiania zadań

Sposób postawienia zadań może być różny i będzie zależał od wielu czynników (m. in.: od posiadanego czasu, stopnia doświadczenia i wyszkolenia dowództw, stanu posiadania i poziomu technicznych środków łączności i wspomagania procesu dowodzenia).

---

[45] W zespole działań informacyjnych opracowywane są:
– w grupie rozpoznania – aneks *„B – rozpoznanie"* do dyrektywy operacyjnej wraz z niezbędnymi apendyksami;
– w grupie obrony informacyjnej – aneks *„N – obrona informacyjna"* do dyrektywy operacyjnej wraz z niezbędnymi apendyksami.

Formalne przekazanie wykonawcom zadań wynikających z decyzji dowódcy rozpoczyna się po zakończeniu opracowania pełnego rozkazu operacyjnego wraz z niezbędnymi aneksami i apendyksami. Zgodnie jednak z przyjętą procedurą dowodzenia podwładni mogą otrzymać zadania bojowe wcześniej w formie zarządzenia przygotowawczego (ZP), wstępnego zarządzenia operacyjnego (WZO), jeżeli dowódca (osobiście lub na wniosek szefa sztabu) uzna za celowe ich wydanie.

Postawienie zadań może odbyć się na SD DWLąd (przyjmuje wówczas formę odprawy koordynacyjnej poświęconej temu problemowi) lub na SD podwładnych. W drugim wypadku wykorzystuje się do tego celu zastępcę dowódcy, innych oficerów sztabu (w tym i z zespołu działań informacyjnych) lub (oraz) oficerów łącznikowych.

Z powyższego wynika, że szef zespołu działań informacyjnych nie ma kompetencji do bezpośredniego stawiania zadań. Uczestnicząc jednak w tym przedsięwzięciu, może wyjaśniać niezbędne dane ujęte w rozkazie operacyjnym, dotyczące przeciwnika, terenu oraz prowadzenia rozpoznania, zakłócania informacyjnego i obrony informacyjnej. Zwłaszcza, że po postawieniu zadań z reguły odbywa się koordynacja działań pomiędzy podległymi jednostkami. Czynność ta – zdaniem autorów – odgrywa bardzo ważną rolę w koordynowaniu zadań zakłócania informacyjnego wykonywanych przez różne jednostki.

3.5. W fazie kontroli

Kontrola stanowi ostatnią fazę cyklu decyzyjnego procesu dowodzenia (rysunek 3.1.). Jednocześnie zapewnia ona ciągłość tego procesu, gdyż jej rezultaty stanowią postawę do uaktualniania posiadanych danych o sytuacji, a głównie ustalania położenia i realizacji kolejnych faz cyklu.

Z badań wynika, że za realizację procesu kontroli odpowiedzialny jest dowódca każdego szczebla dowodzenia. Kontrola powinna być realizowana przez:

ustanowienie elementów dowodzenia i koordynacji działań; organizację synchronizacji działań, monitorowanie sytuacji, podejmowanie działań mających na celu zmniejszenie różnicy pomiędzy stanem zaplanowanym a rzeczywistym.

Kontrola wykonywania zadań w zakresie zakłócania informacyjnego jest więc istotną częścią działań podejmowanych w tej fazie cyklu, a jej cechą szczególną jest to, że należy postrzegać ją w dwóch aspektach: przeciwnik – wojska własne.

W pierwszym wypadku konieczne jest określenie, w jaki sposób realizowane przedsięwzięcia mogą oddziaływać na funkcjonowanie organów rozpoznania, dowodzenia i kierowania uzbrojeniem przeciwnika, a tym samym uzyskanie odpowiedzi na pytania:

– w jaki sposób przeciwnik reaguje na nasze działania w zakresie zakłócania informacyjnego, a głównie w zakresie zakłócania elementów rozpoznania oraz dowodzenia i kierowania uzbrojeniem?

– do jakich wniosków mogą lub powinny go skłonić dane przedsięwzięcia zakłócania informacyjnego?

W drugim wypadku należy wykryć i usunąć niedociągnięcia powstałe w czasie realizacji zadań zakłócania informacyjnego przez wojska własne i w razie potrzeby poprawić ich skuteczność.

Z powyższego wynika, że bardzo ważną rolę podczas kontroli realizacji zadań zakłócania informacyjnego odgrywa *monitorowanie sytuacji*. W tym celu powinny być wykorzystywane dane:

– z meldunków od wojsk;

– z wizyt dowódcy (oficerów sztabu, a w tym i z zespołu działań informacyjnych) u podległych mu wojsk;

– od wysyłanych grup kontrolnych;

– z elementów kontroli organizowanej po linii funkcjonalnej przez specjali-

stów rodzajów wojsk[46] (działalność grup rozpoznawczych, kontrola radiowa, radiolokacyjna, optoelektroniczna, informatyczna i in.).

Do głównych zadań zespołu działań informacyjnych w tej fazie w zakresie zakłócania informacyjnego powinno należeć:

– bieżące informowanie dowódcy o sytuacji przeciwnika;

– kontrola efektów zaplanowanych działań w zakresie zakłócania informacyjnego i ewentualne ich korygowanie oraz stawianie zadań dodatkowych, wynikających z rozwoju sytuacji (według opracowanego harmonogramu, który może stanowić załącznik do planu zakłócania informacyjnego);

– bieżące prowadzenie dokumentacji na potrzeby zakłócania informacyjnego (mapy sytuacyjnej, dokumentów pomocniczych, uaktualniania baz danych itp.).

3.6. Wnioski

W wyniku przeprowadzonych badań przebiegu procesu decyzyjnego pod kątem potrzeb zakłócania informacyjnego w operacjach wojsk lądowych wykazano, że:

1. Odpowiedzialność za całokształt problematyki związanej z zakłócaniem informacyjnym ponosi dowódca, zaś organizatorem zadań w zakresie jego przygotowania i prowadzenia jest komórka G 2, przy znaczącym współudziale komórki G 3 i oficerów specjalistów rodzajów wojsk i służb.

2. Celowym jest utworzenie w centrum dowodzenia SD DWLąd zespołu działań informacyjnych, w którego składzie przewidziano grupę zakłócania informacyjnego.

---

[46] Bardzo ważnym elementem kontroli zakłócania informacyjnego może być lotnictwo wojsk lądowych wyposażone w urządzenia rozpoznania fotograficznego, radiowego, radiolokacyjnego i optoelektronicznego. Może prowadzić zatem w określonej sytuacji pola walki monitoring zarówno wojsk własnych, jak i przeciwnika.

3. Przebieg cyklu decyzyjnego w zakresie zakłócania informacyjnego jest integralnym elementem procesu dowodzenia, realizowanym przez dowództwo wojsk lądowych, zgodnie z obowiązującymi procedurami i technikami.

4. Metodyka pracy sztabu DWLąd w zakresie zakłócania informacyjnego oparta jest na ramowym układzie cyklu obowiązującego w sztabie dowództwa.

5. Forma i treść dokumentów wykonywanych na potrzeby zakłócania informacyjnego jest zgodna z wzorami obowiązującymi w sztabie dowództwa. Mogą być one wykonywane sposobem tradycyjnym bądź z wykorzystaniem ogólnodostępnych środków informatycznych.

Autorzy pracy badawczej są przekonani, że w niedługim czasie proces planowania operacji wojsk lądowych, w tym i zakłócania informacyjnego, będzie zautomatyzowany[47]. O słuszności powyższej tezy dobitnie świadczą wnioski z wojny w rejonie Zatoki Perskiej, gdzie wykorzystane przez wojska koalicji antyirackiej nowe technologie, głównie w dziedzinie automatyzacji, informatyzacji dowodzenia i kierowania uzbrojeniem doprowadziły do sytuacji, w której Irak przegrał wojnę zanim ona się na dobre rozpoczęła.

[47]Uważa się, że zautomatyzowany system dowodzenia będzie niefunkcjonalny, jeżeli jego budowa oparta jest na nieperspektywicznych rozwiązaniach strukturalno-organizacyjnych. Współczesne wymagania oraz aspekty interoperacyjności stwarzają konieczność dążenia do jego funkcjonalnej standaryzacji i integracji wszystkich elementów przygotowania wojsk oraz kierowania nimi w działaniach bojowych.

4. PROWADZENIE ZAKŁÓCANIA INFORMACYJNEGO W OPERACJACH WOJSK LĄDOWYCH

4.1. Kierowanie zakłócaniem informacyjnym

Kierowanie zakłócaniem informacyjnym jest postrzegane jako podstawowa funkcja dowodzenia, którą spełnia dowódca poprzez szefa G-2. Udział w kierowaniu zakłócaniem informacyjnym bierze również w ograniczonym zakresie G-3 oraz specjaliści rodzajów wojsk. Kierowanie zakłócaniem informacyjnym odbywa się z punktów dowodzenia działaniami informacyjnymi rozwiniętych przy stanowisku dowodzenia wojsk lądowych, związków operacyjnych i związków taktycznych.. Do głównych zadań szefa G-2 lub zespołu ludzi wyznaczonych przez niego w tym zakresie zalicza się: dokonywanie identyfikacji, analiz i podziału wykrytych obiektów do zakłócania; koordynowanie zadań zakłócania w dowództwie (sztabie związku operacyjnego i taktycznego); przekazywanie zadań podległym siłom i środkom; koordynacja działań systemu zakłócania z pododdziałami innych rodzajów wojsk; szczegółowe planowanie zakłócania na kolejne dni operacji.

Kierowanie zakłócaniem informacyjnym wymaga utrzymania niezawodnej łączności z podsystemami (elementami) zakłóceń zarówno w pionie dowodzenia jak i w pionie podległości funkcjonalnej. W pionie podległości funkcjonalnej dodatkowo powinno być zapewnione zdalne sterowanie stacjami zakłóceń.

Dla kierowania zakłócaniem informacyjnym należy wykorzystać sieć łączności DWLąd oraz zorganizować sieć łączności, opartą na pracy węzłów łączności stanowisk dowodzenia jednostek zakłóceń. W tak zorganizowanej sieci łączności

należy zapewnić dowodzenie między organami rozpoznania i zakłócania DWLąd, związków operacyjnych i taktycznych oraz rodzajami sił zbrojnych.

Warunkiem sprawnego kierowania zakłócaniem informacyjnym jest stały dopływ informacji rozpoznawczych (sytuacyjnych) i bojowych, które stanowią również podstawę do wprowadzania korekt do planu zakłócania, wypracowania zadań i postawienia ich wykonawcom.

Kierowanie zakłócaniem informacyjnym zawiera w sobie ponadto takie przedsięwzięcia jak:

- nawiązywanie i utrzymanie współdziałania;
- realizacja zadań zabezpieczenia bojowego i logistycznego;
- odtwarzanie zerwanego systemu dowodzenia i łączności;
- kontrola i udzielanie pomocy w wykonaniu zadań.

Do charakterystycznych właściwości kierowania zakłócaniem informacyjnym należą: celowość, przewidywanie, operatywność, ciągłość, elastyczność, skrytość[1].

Działalność elementów ugrupowania bojowego systemu zakłóceń wynikająca z zadań kierowania zakłócaniem informacyjnym koncentruje się na:

- aktualizacji planu zakłócania oraz zadań stosownie do zmian sytuacji na polu walki;
- odtwarzaniu utraconego współdziałania;
- przemieszczeniu podsystemów (elementów) zakłócania na nowe rubieże, w nowe rejony, kierunki;
- odtworzeniu zniszczonych ogniw systemu zakłócania;
- realizacji przedsięwzięć bojowego i logistycznego zabezpieczenia działań zakłócania informacyjnego.

---

[1] Omówione są w Regulaminie działań wojsk lądowych. DWLąd, Warszawa 1999

Aktualizacja planu zakłócania oraz zadań stosownie do zmian sytuacji na polu walki wynika z konieczności przestrzegania zasady celowości zakłócania i ciągłości jego planowania. Wymuszają ją ciągłe zmiany sytuacji na polu walki, nowe zadania oraz teren, także pozyskiwane dane o przeciwniku, które mogą powodować np. przeniesienie wysiłku zakłócania. Czynność ta może dotyczyć całości systemu lub jego części, ale zawsze powoduje potrzebę wypracowania nowych zadań lub aktualizację dotychczasowych.

Aktualizacja planu zakłócania polega na wniesieniu poprawek do wykonanego planu, informowaniu o nich szefów pozostałych rodzajów wojsk, przełożonego funkcjonalnego (w pionie specjalistycznym) oraz sąsiadów. Zadania zakłócania wynikłe wskutek korekty planu zakłócania powinny być krótkie i konkretne, przystosowane do przekazania przez techniczne środki łączności.

Odtworzenie współdziałania może być wynikiem wcześniejszego zerwania łączności współdziałania, wyeliminowania z walki bądź wyjścia z walki jednego z partnerów dotychczas współdziałających ze sobą. W pierwszej kolejności powinno się odtworzyć współdziałanie z pododdziałami łączności, artylerią, OPL, sąsiadami, siłami OT i układu pozamilitarnego.

Odtworzenie współdziałania szefa zespołu działań informacyjnych centrum dowodzenia SD DWLąd z siłami wymienionymi wyżej polega na uzgodnieniu tych problemów, których realizacja została przerwana. Dokonane uzgodnienia powinny być niezwłocznie przekazane w postaci wytycznych (zadań) zainteresowanym elementom zakłócania. Treścią wytycznych mogą być między innymi nowe sygnały i zadania współdziałania, nowe częstotliwości i kryptonimy łączności, sposoby wzajemnej identyfikacji itp.

Przemieszczenie elementów (podsystemów) zakłócania w nowe rejony (na kolejne rubieże i kierunki) jest jednym z trudniejszych problemów stojących przed przez zespołem działań informacyjnych centrum dowodzenia SD DWLąd oraz dowódcami elementów zakłócających. Chodzi tu o takie momenty jak: trasy przemieszczenia, wybór i czas nowych rejonów (rubieży i kierunków) rozwinięcia. Realizacja tego przedsięwzięcia wymaga uprzednich uzgodnień z zespołem dowodze-

nia centrum dowodzenia SD DWLąd., ciągłego współdziałania z artylerią i wojskami inżynieryjnymi oraz siłami OT, po to, aby elementy zakłóceń nie traciły czasu na rekonesans nowych rejonów, a zostały w nie wprowadzone, oraz po to, aby uniknąć strat od własnych środków ogniowych.

Zmiana położenia elementów (podsystemów) zakłócania łączy się ze zwiększonym zagrożeniem ze strony przeciwnika, dlatego też istotnego znaczenia nabiera zabezpieczenie bojowe i logistyczne oraz o jak najszybsze osiągnięcie gotowości do wykonania zadań.

Odtworzenie zniszczonych ogniw systemu zakłócania może być spowodowane następującymi przyczynami: zniszczenie lub obezwładnienie elementu zakłóceń, zerwanie łączności dowodzenia zakłócaniem, zużyte środki walki, niemożność pokonania terenu itp.

W takiej sytuacji zespół działań informacyjnych centrum dowodzenia SD DWLąd powinien nakazać wydzielenie elementu z odwodu zakłócania (jeżeli taki przewidziano), przygotować zadania zakłócania i postawić je bezpośrednio dowódcy elementu zakłóceń lub spowodować odtworzenie zapasów środków walki.

Realizacja przedsięwzięć bojowego i logistycznego zabezpieczenia działań zakłócania informacyjnego odbywa się zgodnie z postanowieniami obowiązujących regulaminów walki.

4.2. Funkcjonowanie zakłócania w podstawowych rodzajach działań operacyjnych wojsk lądowych

Prowadzenie zakłócania informacyjnego bez względu na rodzaj operacji wojsk lądowych uzależnione jest od efektów planowania w sztabowych komórkach G 2 i G-3. Zakres jego prowadzenia uzależniony jest od: czasu, przestrzeni i charakteru zadań realizowanych przez jednostki wojsk operacyjnych.

Prowadzenie zakłócania informacyjnego polega na określeniu jego celów, postawieniu zadań właściwym ugrupowaniom środków zakłócania, ich pracy bojowej oraz manewrze przy zapewnieniu ciągłego dowodzenia i kierowania tymi środkami.

4.2.1. Prowadzenie zakłócania w działaniach obronnych

Prowadzenie zakłócania informacyjnego w działaniach obronnych zasadniczo nie różni się od „pracy" jego elementów w pozostałych rodzajach działań operacyjnych wojsk lądowych. To działanie przeciwnika wymusza odpowiednie zachowanie elementów, które powinny stosować takie sposoby jego prowadzenia jakie w danych okolicznościach przyniosą najlepsze efekty.

Celem zakłócania informacyjnego w działaniach obronnych wojsk lądowych jest zmniejszenie lub pozbawienie możliwości wykonania zadań przez systemy rozpoznania, dowodzenia i kierowania uzbrojeniem przeciwnika.

Cel zakłócania informacyjnego wynika z zadań jakie otrzymały związki operacyjne i taktyczne wojsk lądowych. Dowódca określając cel swojego działania określa jednocześnie cele dla poszczególnych rodzajów wojsk i służb. Każda z komórek organizacyjnych w zależności od otrzymanego zadania i określonego ogólnego celu działań, określa cele cząstkowe. Jednym z takich celów cząstkowych jest prowadzenie zakłócania informacyjnego.

Ogólny cel zakłócania informacyjnego, który chce osiągnąć dowódca określonego szczebla dowodzenia powinien być precyzyjnie określany w stosunku do poszczególnych rodzajów środków, poszczególnych ogniw dowodzenia, kierunków i pasów działania. Zakłócany cel musi być realny do osiągnięcia i mieć swoje uzasadnienie w posiadanym potencjale (tj. siłach i środkach)[2]. Postawienie nierealnych celów obniża możliwości do osiągnięcia nawet tych zadań, które są w zasięgu moż-

[2] W zależności od szczebla dowodzenia zakłócanie informacyjne realizują siły i środki walki elektronicznej, działań psychologicznych, działań specjalnych oraz wojska uczestniczące w walce.

liwości środków występujących na danym szczeblu dowodzenia. Rzetelnie przeprowadzona analiza i prognoza zagrożeń w ramach oceny sytuacji (IPB[3], EPB[4]), pozwala jasno sprecyzować cel prowadzonych działań w dziedzinie zakłócania informacyjnego. Ogólny cel realizuje się przez cele pośrednie (cząstkowe). Cele pośrednie realizuje się w różnych fazach operacji obronnej wojsk lądowych, do których zalicza się:, np.:

– zerwanie dowodzenia w jednym ogniwie na określony czas prowadzonych działań;

– zerwanie lub dezorganizowanie dowodzenia w jednym ZO, ZT lub oddziale;

– zerwanie lub dezorganizowanie współdziałania w okresie wprowadzania nowych sił do walki;

– zerwanie lub dezorganizowanie współdziałania między środkami ogniowymi a nacierającymi wojskami na określonym szczeblu;

– zakłócanie konkretnego systemu rozpoznania przeciwnika w określonym czasie;

– zakłócanie określonego systemu kierowania środkami ogniowymi;

– utrudnienie przeciwnikowi zakłócania określonego systemu dowodzenia lub kierowania środkami walki;

– utrudnienie dezorganizowania dowodzenia własnymi wojskami.

Cele pośrednie powinny być tak precyzowane, aby ich osiągnięcie dawało wymierne korzyści[5] dla walczących wojsk, a zarazem wyzwalało możliwości realizacji zadań. Zadania te mają różny zakres realizacji w poszczególnych etapach działań obronnych:

---

[3] EPB ang. Electronic Preparation of the Battlefield - elektroniczne przygotowanie pola walki.
[4] IPB ang. Information Preparation of the Battlefield - informacyjne przygotowanie pola walki.
[5] Formułowane cele powinny więc być przemyślane pod kątem działania wojsk w działaniach obronnych i przynosić im korzyści w zakresie zmniejszonej skuteczności ognia przeciwnika, ograniczonego tempa działania, wreszcie zwiększonej swobody manewru własnych wojsk i środków walki.

1. W okresie przygotowania operacji przedsięwzięcia powinny uwzględniać:

– intensywne przeciwdziałanie rozpoznaniu systemów i środków nowo uruchamianych, zmieniających częstotliwość (pasma), charakter pracy, kody i dyslokację, zwiększających intensywność pracy, obejmujących swym zasięgiem nowe rejony wojsk lotniczych, zgrupowań lądowych i morskich, sił szybkiego reagowania, wojsk desantowych, systemów ogniowych dalekiego zasięgu, wojsk specjalnych, w tym szczególnie rozpoznawczo-dywersyjnych, rozpoznania strategiczno-operacyjnego;

– zakaz lub ograniczenie zakresu wykorzystania i maskowanie pracy systemów i środków promieniujących energię elektromagnetyczną wojsk szczebla taktycznego i operacyjnego, z wyjątkiem wykonujących zadania stałe w okresie pokoju[6].

– stosowanie w szerokim zakresie dezinformacji (osobowej i technicznej), realizowanie zadań zakresu pasywnego (biernego) zakłócania elektronicznego w rejonach rozwinięcia wojsk i podstawowych środków ogniowych, elementów systemu rozpoznania i dowodzenia, liczby i kierunków przegrupowania, składu i rodzajów uzbrojenia, terminu osiągnięcia gotowości bojowej, rozpoczęcia działań, itp.;

– zakłócanie (jeśli toczy się podczas wojny), naziemnych, powietrznych i morskich środków dalekiego rozpoznania, sieci radiowych zbierania informacji, środków elektronicznych systemów ogniowych wykonujących uderzenia na wojska lub w strefach odpowiedzialności, systemów operacyjnego dowodzenia, współdziałania i powiadamiania.

Zadania te mogą częściowo wykonywać siły i środki rozwinięte i pracujące w okresie pokoju, środki bojowe wojsk obrony powietrznej, marynarki wojennej, związków taktycznych i operacyjnych, rozwinięte wzdłuż granicy lub będące w styczności z przeciwnikiem.

---

[6] Dotyczy to szczególnie systemów polowych dowodzenia i OPL.

2. Z chwilą rozpoczęcia operacji obronnej:

– prowadzenie intensywnego poszukiwania (w ramach rozpoznania informacyjnego) elementów rozpoznania, dowodzenia i kierowania uzbrojeniem jako obiektów do zakłócania dezinformującego, zagłuszającego oraz niszczącego. Szczególna uwaga musi być zwrócona na rejony głównego zgrupowania wojsk przeciwnika, ważne środki rozpoznania i ogniowe, rejony dyslokacji obiektów dowodzenia oraz nowe systemy elektroniczne;

– zakłócanie systemów radiokomunikacyjnych przeciwnika, a w szczególności systemów łączności radiowej UKFi KF, radioliniowej i radiosatelitarnej zgodnie z przyjętą koncepcją do prowadzenia walki informacyjnej;

– zakłócanie powietrznych i naziemnych stacji radiolokacyjnych w okresach wykonywania zadań, szczególnie poprzedzających zmasowane uderzenia lotnicze, rakietowe itp.;

– zakłócanie systemów radionawigacyjnych w obszarach działania środków ogniowych przeciwnika lub obszarach działania jego wojsk, ze szczególnym zwróceniem uwagi na czas nocny i w warunkach ograniczonej widoczności;

– zakłócanie zautomatyzowanych systemów dowodzenia, posterunków rozpoznania i naprowadzania, obszarów koncentracji wojsk przez zrzucenie nadajników zakłócających jednorazowego użycia;

– prowadzenie dezinformacji (osobowej i technicznej) w podatnych na taką działalność systemach i środkach;

– wykonanie zadań maskowania za pomocą pasywnych środków zakłócania według opracowanego planu walki informacyjnej wynikających z tego zagrożeń środkami naprowadzającymi się przeciwnika;

– w przypadku posiadania broni naprowadzającej się na źródła EM, użycie jej w stosunku do najważniejszych obiektów elektronicznych przeciwnika i głównych zgrupowań jego wojsk;

– kompleksowe oddziaływanie psychologiczne na wojska przeciwnika.

3. W toku działań obronnych:

– punkt ciężkości zakłócania informacyjnego powinien skupiać się na obniżeniu efektywności działania systemów i środków rozpoznania, dowodzenia, naprowadzania lotnictwa, wojsk rakietowych i artylerii głównego zgrupowania uderzeniowego, stosownie do zmieniającej się sytuacji na polu walki. Szczególną uwagę powinno zwraca się na:

– intensywne wykrywanie nowo uruchamianych emisji elektromagnetycznych oraz pojawiających się nowych obiektów elektronicznych;

– śledzenie zachodzących zmian w rozpoznawanych systemach elektronicznych głównego zgrupowania uderzeniowego;

– zakłócanie desantów, oddziałów wydzielonych, grup rajdowych oraz sił specjalnych działających w głębi;

– prowadzenie zakłócania na korzyść sił wykonujących kontrataki i przeciwuderzenia lub zmasowane uderzenia ogniowe;

– zakłócanie wojsk dokonujących okrążeń i wspieranie zgrupowań ogólnowojskowych wychodzących z okrążenia;

– wspieranie sił dokonujących manewru odejścia i wycofania na kolejne pozycje;

– kontynuowanie zakłócania zautomatyzowanych systemów dowodzenia, posterunków rozpoznania i naprowadzania, obszarów koncentracji wojsk przez zrzucenie nadajników zakłócających jednorazowego użycia;

– kontynuowanie prowadzenia dezinformacji (osobowej i technicznej) w podatnych na taką działalność systemach i środkach;

– wszechstronne oddziaływanie psychologiczne na nacierające wojska przeciwnika.

Podczas odpierania ataku przeciwnika przez wojska broniące głównego obszaru obrony, wysiłek zakłócania informacyjnego powinien skupiać się na zagłuszaniu relacji radiowych łączności UKF dowodzenia oddziałów i pododdziałów

głównego zgrupowania uderzeniowego przeciwnika, jak również relacji radiowych dowodzenia i naprowadzania lotnictwa taktycznego.

W czasie wprowadzania przez przeciwnika do walki odwodów, wysiłek zakłócania informacyjnego powinna być skupiona na zagłuszaniu łączności radiowej dowodzenia artylerią i oddziałami wprowadzanymi do walki oraz posterunkach naprowadzania lotnictwa.

W przypadku udziału ZO, ZT WL w działaniach opóźniających, wysiłek zakłócania informacyjnego powinien koncentrować się na zadaniach zmierzających do prowadzenia zagłuszania elektronicznego w sieciach radiowych dowodzenia i współdziałania. Powinny być realizowane także przedsięwzięcia dezinformowania oraz oddziaływania psychologicznego.

4.2.2. Prowadzenie zakłócania w działaniach zaczepnych

Podstawowym zadaniem zakłócania informacyjnego w działaniach zaczepnych (kontruderzeniu) jest dezorganizacja systemów dowodzenia pierwszorzutowych wojsk przeciwnika oraz jego systemu rozpoznania, dowodzenia i kierowania uzbrojeniem na kierunku działań.

Prowadzenie zakłócania informacyjnego w działaniach zaczepnych odbywa się według tych samych zasad co w obronie, charakteryzuje się jednak pewnymi specyficznymi cechami. Wymaga koncentracji wysiłku zakłócania przed rozpoczęciem działań, w związku z czym wymusza szybkie uruchomienie (rozwinięcie) systemu zakłócania. Jego wysoka efektywność jest charakterystyczna dla działań zaczepnych. W działaniach wojsk lądowych szczególną uwagę należy zwrócić na:

– zakłócanie systemów dowodzenia, rozpoznania i kierowania uzbrojeniem sił pierwszorzutowych przeciwnika, broniących się w strefie osłonowej;

– wykrywanie (we współdziałaniu z elementami rozpoznania) sił i obiektów działających w głębi operacyjnej, przeznaczonych do wykonywania przeciwuderzeń i kontrataków oraz obsadzenia kolejnych pozycji obrony, a także zakłócanie systemów i środków obsługujących odwody i ich elementy zabezpieczające;

– rubieże wprowadzenia odwodów, (w tym wykrywanie obiektów na kolejnych rubieżach i zakłócanie systemów dowodzenia i kierowania uzbrojeniem sił na kierunkach ich wprowadzania);

– zakłócanie systemów dowodzenia i kierowania uzbrojeniem wojsk broniących przeszkód wodnych, prowadzących rozpoznanie przepraw i wojsk podchodzących oraz środków ogniowych ostrzeliwujących rejony przepraw;

– osłonę elektroniczną mostów oraz wojsk na przeprawach przed uderzeniami lotnictwa, wykonanie (z odbijaczy kątowych) pozornych przepraw, mostów, dróg dojazdowych itp.;

– dezorganizację dowodzenia wojskami wycofującymi się na kolejne rubieże, ich systemów rozpoznania, współdziałania i zabezpieczenia materiałowo-technicznego;

– inne zadania, wynikające z rozwoju sytuacji operacyjno-taktycznej.

Podczas prowadzenia zakłócania informacyjnego w działaniach zaczepnych sztabowa komórka G 2 funkcjonuje podobnie jak w pozostałych rodzajach działań bojowych. Należy jednak liczyć się z częstą zmianą położenia stanowisk dowodzenia ZT i oddziałów a wraz z nimi elementów zakłócających, co może wpływać na ciągłość ich pracy oraz jakość łączność i obiegu informacji między nimi.

Praca bojowa elementów zakłócających odbywa się według tych samych zasad jak w działaniach obronnych, niemniej jednak w zależności od zachowania przeciwnika, niektóre z nich będą się częściej przemieszczać.

4.2.3. Prowadzenie zakłócania w specyficznych warunkach pola walki

Cechą charakterystyczną działań w specyficznych warunkach pola walki (w lesie, w górach, zimą, w aglomeracji miejskiej, na przeszkodzie wodnej) jest konieczność ich prowadzenia przez tworzone zgrupowania taktyczne wojsk lądowych najczęściej na izolowanych kierunkach, niekiedy znacznie od siebie oddalonych. Ważną rolę odgrywa manewr sił i środków z wykorzystaniem niewielkiej ilości dróg, niskie tempo i ogniskowy charakter działań. W tych okolicznościach pomyślność działań w dużej mierze zależeć będzie od inicjatywy, umiejętności i jakości dowodzenia siłami i środkami zakłócania informacyjnego.

Zakłócanie w terenie lesisto – jeziornym. Teren lesisto – jeziorny to obszar, którego ponad 50% powierzchni pokryte jest lasami i jeziorami. Z wojskowego punktu widzenia, obszar ten charakteryzuje się wieloma istotnymi czynnikami, które należy brać pod uwagę przy określaniu ich wpływu na prowadzenie zakłocania w tym terenie. Należą do nich m.in.:

- wielkość (powierzchnia) masywów leśnych i jezior;
- charakterystyka obszarów leśnych (ich rodzaj i gęstość);
- charakterystyka hydrograficzna jezior;
- ewentualna obecność bagien i rzek;
- właściwości klimatyczne i glebowe terenu;
- stopień zagospodarowania (gospodarka leśna) terenu.

Na europejskim TDW, zwłaszcza w pasie nadmorskim, znaczne obszary zajmuje teren lesisto – jeziorny. Typowym przykładem takiego obszaru w Polsce jest Pojezierze Pomorskie i Mazurskie.

Prowadzenie zakłócania w takim terenie jest bardzo złożone ze względu na:

- kanalizację ruchu wojsk na leśnych drogach i przesmykach między jeziorami;

– ograniczone możliwości wykorzystania sił i środków zakłócania informacyjnego;

– skomplikowane warunki zajmowania rejonów rozwinięcia i wykonywania manewru.

Teren lesisto – jeziorny zasługuje na specyficzną uwagę, ze względu na różnorodność swojej rzeźby oraz pokrycie. Główną przeszkodą, która wpływa na przygotowanie i prowadzenie zakłócania w tym terenie są kompleksy leśne z jeziorami różnej wielkości. Dostępność tego terenu zależy między innymi od stopnia zagospodarowania. Las zagospodarowany charakteryzuje się większą liczbą dróg i przesiek, grunt jest zazwyczaj osuszony i oczyszczony. Taki las sprzyja przede wszystkim prowadzeniu rozpoznania osobowego .

Duże znaczenie na prowadzenie działań w terenie lesisto – jeziornym ma także pora roku i aktualne warunki atmosferyczne. Latem teren ten sprzyja skrytej rozbudowie inżynieryjnej, rozmieszczeniu i maskowaniu dużej liczby wojsk oraz elementów zabezpieczenia logistycznego. Niestety, utrudnia wykonywanie manewrów wojskami oraz prowadzenie zakłócania zarówno powietrznego jak i naziemnego. Ponadto w lecie, zwłaszcza podczas suchych i upalnych dni, wzrasta zagrożenie pożarowe, które utrudnia, nawet czasowo uniemożliwia działania wojsk. Walka z żywiołem wymaga zaangażowania dodatkowych sił i środków do likwidacji jego skutków.

Z diametralnie odmiennymi warunkami mamy do czynienia w terenie lesisto – jeziornym zimą. Las nie zapewnia wtedy dogodnych warunków maskowania, utrudnione jest także pokonywanie terenu. Ruch wojsk możliwy jest tylko po drogach. Z drugiej jednak strony zimą, szczególnie gdy występują niskie temperatury można pokonać obszary, których przekroczenie jesienią czy wiosną jest niemożliwe.

Wiosną i jesienią, ze względu na większą liczbę opadów, czy roztopy zwiększa się wilgotność gleby. Drogi polne są trudno przejezdne, a bagniste obszary stają się przeszkodami nie do pokonania.

W terenie lesisto – jeziornym zimą jest cieplej a latem chłodniej, także mniejsze niż w terenie otwartym dobowe wahania temperatury. Ponadto, wilgotne leśne powietrze sprzyja powstawaniu rosy i szronu, co wymaga specjalnej troski o stan sprzętu technicznego. Mgły, często występujące w terenie lesisto – jeziornym znacznie utrudniają prowadzenie obserwacji; mają też ujemny wpływ na rozprzestrzenianie się fal elektromagnetycznych, szczególnie wykorzystywanych w wyższych zakresach częstotliwości.

Dzięki właściwościom maskującym teren lesisto – jeziorny sprzyja bazowaniu grup specjalnych i stwarza dogodne warunki do prowadzenia działań dywersyjnych, dezinformacyjnych i psychologicznych.

Obszary lesisto – jeziorne przyczyniają się do tworzenia licznych naturalnych rubieży terenowych, które z jednej strony utrudniają prowadzenie zakłócania w działaniach zaczepnych, zaś z drugiej – ułatwiają wykonanie zadań w obronie.

Analizowany teren ma więc wiele dodatnich i ujemnych cech wpływających na organizację i prowadzenie zakłócania informacyjnego. Do dodatnich należy przede wszystkim zaliczyć:

– łatwość określenia kierunków uderzeń (zamiaru) przeciwnika;

– łatwość rozbudowy inżynieryjnej terenu, ze względu na dużą dostępność materiałów, niezbędnych do realizacji tego przedsięwzięcia;

– dogodne warunki maskowania sił i środków oraz fortyfikacji obronnych;

– wolne tempo działania przeciwnika, spowodowane koniecznością pokonywania wielu naturalnych i sztucznych przeszkód.

Do cech ujemnych, które wpływają na organizowanie i prowadzenie zakłócania informacyjnego w terenie lesisto – jeziornym trzeba zaliczyć m.in.:

– słabo rozwiniętą sieć dróg, która znacznie ogranicza przemieszczanie wojsk;

– trudne warunki manewru środków zakłócania, a także pewne ograniczenia manewru energią elektromagnetyczną;

– utrudnione współdziałanie;

– utrudnione organizowanie i utrzymanie łączności;

– możliwość występowania lokalnych i rozległych pożarów;

– zmniejszenie zasięgów pracy środków łączności radiowej UKF, a powoduje pogorszenie warunków współdziałania pomiędzy elementami i podsystemami zakłócania;

– możliwość skrytego podejścia przeciwnika do pododdziałów zakłóceń (w terenie lesisto-jeziornym są dogodne warunki do prowadzenia np. działalności dywersyjno - rozpoznawczej).

Właściwa realizacja zadań w terenie lesisto – jeziornym wymaga szczegółowego i dokładnego przygotowania pododdziałów pod względem znajomości terenu i odpowiedniego wyposażenia. Brak wyraźnie dostrzegalnych przedmiotów terenowych, nie tylko utrudnia orientację, ale także dowodzenie wojskami oraz organizacje, koordynacje i współdziałanie. Ponadto w obszarach leśnych występują często naturalne zakłócenia łączności radiowej.

Podsumowując stwierdzić należy, że teren lesisto – jeziorny tworzy specyficzne warunki prowadzenia zakłócania informacyjnego, które odpowiednio wykorzystane mogą być dodatkowym atutem podczas prowadzenia zakłócania informacyjnego.

Zakłócanie w terenie górzystym. Elementemami, które decydują o możliwości prowadzenia zakłócania informacyjnego w terenie górzystym[7] są zbocza i ich nachylenie (stromość) mierzone w stopniach. Pod względem dostępności zbocza dzielą się na: bardzo łagodne, łagodne, łagodnie spadziste, spadzisto strome, strome, bardzo strome, urwiste. Pierwsze są dostępne dla wszystkich pojazdów, ostatnie zaś - dla specjalnie przygotowanych. Dostępność zboczy zależy nie tylko

[7] Teren górzysty to teren o bardzo urozmaiconej rzeźbie, ze stromymi zboczami, wyraźnymi grzbietami, głęboko wciętymi dolinami i licznymi urwiskami. Różnice wysokości bardzo często przekraczają 200 m, a niekiedy sięgają do 1000 m. na 1 km, kąty nachylenia zboczy dochodzą nawet do 90^0. W zależności od położenia nad poziomem morza góry dzielą się na: niskie, średnie, wysokie. Wyczerpującą charakterystykę terenu górzystego przedstawili H. Stasiewicz, Wł. Łaski w: „Topografa wojskowa", wyd. MON, Warszawa 1983, s. 55.

od ich stromości, także od rodzaju gruntu i jego nawilgocenia, a w zimie od grubości pokrywy śnieżnej.

Rzeźba terenu górzystego wywiera znaczny wpływ na: możliwości ochronne wojsk, możliwości prowadzenia zakłócania informacyjnego, przekraczalność terenu, wykorzystanie technicznych środków łączności (głównie zasięg środków łączności radiowej), a także urządzeń zakłócających.

Rzeźba terenu wywiera też wpływ na możliwość orientowania się w terenie oraz ocenę odległości. Anomalie magnetyczne utrudniają korzystanie z wszelkich przyrządów ułatwiających orientację i określanie kierunku.

Wzgórza i wzniesienia nadają się natomiast doskonale do rozmieszczenia elementów zakłócania informacyjnego, utrudniają niestety ich przemieszczanie się, zwłaszcza wyposażonego w samochody specjalne, czy opancerzone transportery zakłócające. Ograniczają także zasięg i dokładność (wskutek trudności związanych z dowiązaniem topograficznym) urządzeń zakłócania oraz namierzania radiowego UKF i radiolokacyjnego. Blisko 1,5 - krotnie wzrasta czas rozwijania tych urządzeń.

Teren górzysty ogranicza prędkość opancerzonych transporterów zakłócających i samochodów do wartości:

- 8 - 12 km/h przy nachyleniu zbocza 10 - 15°;
- 5 - 8 km/h przy nachyleniu zbocza 15 - 20°.

Powoduje też zwiększenie zużycia MPS nawet o 75% w warunkach zimowych.

Duża liczba pól martwych i zakrytych oraz ograniczone pole widzenia utrudnia prowadzenie zakłócania z naziemnych punktów oraz z powietrza, z drugiej jednak strony doliny i wąwozy mogą być wykorzystane do ukrywania wojsk, wnikania śmigłowców specjalnych w głąb ugrupowania przeciwnika.

Prowadząc zakłócanie informacyjne w terenie górzystym należy wiedzieć jak unikać niebezpieczeństw powodowanych zjawiskami przyrody[8], a także jak je wykorzystać lub wywołać np. w jaki sposób wywołać lawinę śnieżną lub kamienną albo osypisko, aby zatarasować drogę na kierunku działania przeciwnika, zniszczyć technikę bojową i spowodować straty w sile żywej.

Zakłócanie w zimie. Zima w naszej szerokości geograficznej charakteryzuje się częstymi i szybkimi zmianami temperatury, które niejednokrotnie powodują częściowe lub całkowite topnienie śniegu. W takich okresach w jednolitej dotychczas pokrywie śnieżnej tworzą się ciemne plamy, widoczne z dużej odległości. Istnienie ciemnych plam na pokrywie śnieżnej, przyczyniać się może do demaskowania wojsk posiadających zimowe ubiory maskujące. Natomiast dużo śniegu może oznaczać kłopoty zwłaszcza gdy są w marszu. Głęboki śnieg będzie zmieniał okoliczny krajobraz, utrudniając orientowanie się w terenie. Śnieg zakrywa wszelkiego rodzaju przeszkody i niebezpieczne miejsca, tworząc niebezpieczne pułapki. Te i jeszcze wiele innych swoistych problemów wpływa na proces przygotowania i prowadzenia działań zakłócających w okresie zimowym.

Do czynników sprzyjających prowadzeniu działań zakłócania informacyjnego w zimie należą:

– niska temperatura powietrza, częste zawieje i opady śnieżne zmniejszające w znacznym stopniu aktywność i gotowość bojową przeciwnika;

– duża możliwość istnienia luk w ugrupowaniu przeciwnika powstałych na skutek charakterystycznych cech obrony w zimie organizowanej w osiedlach, lasach i zagajnikach sprzyjają przenikaniu grup dywersyjnych na jego tyły tyły;

– zamarzanie przeszkód wodnych i bagien ułatwia ich pokonanie oraz stwarza duże możliwości niespodziewanego pojawienia się w innych rejonach, a tym samym osiągnięcie czynnika zaskoczenia w działaniu;

---

[8] W związku z różną wyniosłością poszczególnych wierzchołków i grzbietów nad poziomem morza, różnorodnością typów skał oraz wskutek działania promieni słonecznych, gwałtownych zmian temperatury, wiatrów a także ciągłych zmian geologicznych, obserwuje się w górach występowanie takich zjawisk jak: kamieniopady, obwały lodowe, lawiny śnieżne, osypiska, gwałtowne zmiany pogody.

Do czynników utrudniających prowadzenie zakłócania informacyjnego w zimie należą:

– gwałtowne zmiany temperatury i pogody (mrozy, odwilże, zawieje śnieżne) utrudniają wykonanie zadań oraz wymagają stosowania niezbędnych środków technicznych w celu zabezpieczenia gotowości bojowej sprzętu technicznego i obsług w każdej sytuacji i w każdych warunkach;

– ograniczona ilość dróg oraz trudności w przemieszczaniu się po bezdrożach wymaga stosowania skomplikowanych manewrów;

– przemieszczanie się w czasie silnych mrozów, szczególnie w ciche noce po lodoszreni i wywołany tym szum słyszany na odległość 300 m i więcej, utrudnia skryte przemieszczanie się pododdziałów zakłócających działających w styczności z przeciwnikiem.

Prowadzenie zakłócania informacyjnego przeciwnika w zimie wymaga od sztabów wszystkich szczebli szczególnie dokładnego planowania i organizowania działań.

Dlatego też przystępując do planowania i organizowania zakłócania informacyjnego w zimie, sztab DWląd., zespół działań informacyjnych centrum dowodzenia SD DWLąd (a w szczególności grupa zakłócania informacyjnego) powinien przede wszystkim wziąć pod uwagę zadanie, które wykonuje lub będzie wykonywał i w zależności do niego określić zadania oraz wydzielić niezbędne siły i środki zapewniające jego wykonanie.

W przygotowaniu zakłócania informacyjnego szczególnie ważne są następujące czynniki:

1. Podczas przygotowania działań należy brać się pod uwagę prawdopodobne warunki atmosferyczne w przewidywanym rejonie działania. Silny chłód, silne wiatry i burze śnieżne mogą powodować poważne ograniczenia widoczności, propagacji fal elektromagnetycznych i manewrowości, a tym samym utrudnić wykonanie zadania. Szybka zmiana z suchego mrozu na wilgotną pogodę może stworzyć szczególne problemy dla stanu osobowego i techniki zakłócającej.

2. W skrajnym chłodzie, praktycznie każde zadanie wymaga więcej czasu na realizację, a określenie dopuszczalnego czasu działania elementu dokonane musi być na etapie planowania. Czas ten w warunkach zimowych zależy od postawionego zadania, sytuacji, warunków atmosferycznych, charakteru terenu, grubości i stanu pokrywy śnieżnej. Prędkość poruszania się pojazdów kołowych przy pokrywie śnieżnej 15-20 cm – zostanie znacznie ograniczona. Indywidualne przygotowanie do działań wymaga zwrócenia uwagi na szczegóły, takie jak umundurowanie i wyposażenie. Stan osobowy działający w tych warunkach wymaga dodatkowego czasu odpoczynku oraz zwiększonych dostaw wysoko kalorycznego pożywienia.

3. Z powodu obfitych opadów śniegu elementy zakłócania informacyjnego mogą być uzależnione we dużej mierze od linii komunikacyjnych, działanie po bezdrożach może być utrudnione bądź wręcz uniemożliwione.

4. Zakrycie i ukrycie jest jednym z ważniejszych obowiązków w stosunku do ludzi i sprzętu w warunkach zimowych. Wykonywanie posterunków obserwacyjnych, ukryć dla sprzętu w zmarzlinie lub lodzie bez specjalistycznego przygotowania, wyposażenia lub materiałów wybuchowych może być utrudnione.

5. Kierowanie zakłócaniem informacyjnym w zimie w zasadzie nie różni się od kierowania nim w innych porach roku. Niemniej jednak warunki zimowe posiadają pewne swoiste właściwości, które należy uwzględniać, szczególnie na etapie planowania.

4.3. Wnioski

W wyniku przeprowadzonych badań w zakresie prowadzenia zakłócania informacyjnego w operacjach wojsk lądowych wykazano, że:

1. Kierowanie zakłócaniem informacyjnym odbywa się z punktów dowodzenia działaniami informacyjnymi rozwiniętych przy stanowisku dowodzenia wojsk lą-

dowych, związków operacyjnych i związków taktycznych. Polega ono na ciągłym podejmowaniu decyzji przez szefa G-2 lub zespół ludzi wyznaczonych przez niego.

Do głównych zadań w tym zakresie zalicza się: dokonywanie identyfikacji, analiz i podziału wykrytych obiektów do zakłócania; koordynowanie zadań zakłócania w dowództwie (sztabie związku operacyjnego i taktycznego); przekazywanie zadań podległym siłom i środkom; koordynacja działań systemu zakłócania z pododdziałami innych rodzajów sił zbrojnych; szczegółowe planowanie zakłócania na kolejne dni operacji.

2. Prowadzenie zakłócania informacyjnego bez względu na rodzaj operacji wojsk lądowych uzależnione jest od efektów planowania w sztabowych komórkach G-2 i G-3. Zakres jego prowadzenia uzależniony jest od: czasu, przestrzeni i charakteru zadań realizowanych przez jednostki wojsk operacyjnych.

Celem zakłócania informacyjnego w działaniach obronnych wojsk lądowych jest zmniejszenie lub pozbawienie możliwości wykonania zadań przez systemy rozpoznania, dowodzenia i kierowania uzbrojeniem przeciwnika.

Prowadzenie zakłócania informacyjnego w działaniach zaczepnych odbywa się według tych samych zasad co w obronie. Wymaga jednak koncentracji wysiłku zakłócania przed rozpoczęciem działań, a w ślad za tym wymusza szybkie uruchomienie (rozwinięcie) systemu zakłócania.

Cechą charakterystyczną działań w specyficznych środowiskach walki (w lesie, w górach, zimą, w aglomeracji miejskiej, na przeszkodzie wodnej) jest konieczność prowadzenia działań przez wojska lądowe zazwyczaj na izolowanych kierunkach, niekiedy znacznie od siebie oddalonych, najczęściej przez tworzone zgrupowania taktyczne. Ważną rolę odgrywa manewr sił i środków z wykorzystaniem niewielkiej ilości dróg, niskie tempo i ogniskowy charakter działań. W tych okolicznościach dużo zależeć będzie od inicjatywy, umiejętności i jakości dowodzenia siłami i środkami zakłócania informacyjnego.

ZAKOŃCZENIE

Zakres badań i zastosowane metody badawcze pozwoliły na osiągnięcie założonego celu badań, realizację zadań badawczych o charakterze poznawczym i końcową weryfikację hipotezy roboczej, a wnioski zawarte w poszczególnych rozdziałach są odpowiedzią na postawione problemy badawcze. Stanowią one podstawę do sformułowania następujących twierdzeń:

– procesy informacyjne są nieodłączne w prowadzeniu walki zbrojnej, a skuteczne zakłócenie ich u przeciwnika prowadzi do obniżenia skuteczności jego działania;

– zakłócanie informacyjne może być realizowane we wszystkich sferach dostępnych zdobywaniu informacji przez przeciwnika oraz w odniesieniu do jego sił i środków wykorzystywanych na potrzeby dowodzenia wojskami i kierowania uzbrojeniem;

– zakłócanie informacyjne jest realizowane przez wszystkie strony biorące udział w konflikcie, za pomocą wszystkich dostępnych środków;

– zakłócanie informacyjne nie jest nowością i było realizowane już od najdawniejszych czasów, a historia jego stosowania jest tak samo długa jak historia wojen;

– we współczesnej walce zbrojnej, zakłócanie informacyjne jest realizowane głównie za pomocą środków zakłóceń elektronicznych oraz specjalistycznych środków niszczenia, a obszar elektromagnetyczny uznawany jest za priorytetowy dla jego prowadzenia.

Zdaniem autorów praca badawcza stanowi próbę rozwiązania problemu zakłócania informacyjnego w operacjach naszych wojsk lądowych. Mimo to badania należy kontynuować. Konieczność ta wynika zarówno z charakteru głównego problemu badawczego, który jest problemem otwartym, jak też z istnienia w jego otoczeniu wielu nie opracowanych naukowo problemów. W pierwszej kolejności dalszymi badaniami należy objąć problem planowania i organizowania zakłócania informacyjnego w operacjach połączonych.

BIBLIOGRAFIA

1. Antczak St.: „Systemy kierowania i uzbrojenia w polskich siłach powietrznych", wyd. AON, Warszawa 1997.
2. Bezoń B.; Janczak J.: „Analiza współczesnych systemów łączności w kontekście integracji SZ RP z NATO", wyd. AON, Warszawa 1999.
3. Bordon W., Bodziński R., Fellner A., Ligęza S.: „System GPS NAVSTAR", Poznań 1997.
4. Campen A. D: „The first Information War", Virginia 1992.
5. Chajtman S.: „Systemy i procesy informacyjne", wyd. PWE, Warszawa 1986.
6. Ciborowski L.: „Informacyjna preparacja pola walki", referat w materiałach III KNTWRE, wyd. WAT, Żegiestów 1997.
7. Ciborowski L.: „Rola i miejsce rozpoznania w systemie obronnym RP", wyd. AON, Warszawa 1993.
8. Ciborowski L, Polko M.: „Planowanie i organizowanie walki zbrojnej wg poglądów NATO", wyd. AON, Warszawa 1996.
9. Ciborowski L.: „Przestrzenie walki informacyjnej", wyd. AON, Warszawa 1997.
10. Ciborowski L.: „Walka informacyjna", wyd. ECE, Toruń 1999.
11. Globan-Klas T.;Sienkiewicz P.: „Społeczeństwo informacyjne: Szanse, zagrożenia, wyzwania", wyd. Fundacji Postępu Telekomunikacji, Kraków 1999.
12. Grabau. R.: „Sechs Dimensionen des Kriegers", w: „Soldat und Technik", nr 6, 1986.
13. Grafinkel S.; Spafford G.: „Practical Unix and Internet Seciurity", wyd. II, O'Reilly & Associates, Inc. Sebastopol USA, Opracowanie wersji polskiej Kresak P.: Bezpieczeństwo w Unixie i Internecie, wyd. RM, Warszawa 1997
14. Idzikiewicz A. Z.: „Ochrona informacji w procesie przetwarzania", wyd. PWE, Warszawa 1979.
15. „Instrukcja o maskowaniu wojsk", cz. II – zasady maskowania operacyjnego", wyd. Szt. Gen. WP, Warszawa 1976
16. Janczak J.: „Obrona radioelektroniczna mobilnych systemów łączności", wyd. AON, Warszawa 1998.
17. Janczak J.: „Walka informacyjna na współczesnym polu walki", referat w materiałach (cz. 1) na VII Konferencji Telekomunikacji i Informatyki, wyd. WIŁ, Zegrze 1998.
18. Janczak J.: „Analiza informacji o siłach i środkach przeciwnika w kontekście budowy komputerowej bazy danych", wyd. AON, Warszawa 1998.
19. Janczak J.; Nowacki G.; Scheffs W.: „Możliwości wykorzystania systemu globalnej nawigacji satelitarnej GPS NAWSTAR w wojskach lądowych RP", wyd. AON, Warszawa 1999.

20. Janczak J.; Bezoń B.; Scheffs W.: „Walka elektroniczna w działaniach taktycznych wojsk lądowych", wyd. AON, Warszawa 1999.
21. Janczak J.: „Obrona informacyjna w działaniach wojsk lądowych", wyd. AON, Warszawa 2000.
22. Janczak J.: „Kierunki rozwoju rozpoznania oraz zakłócania elektronicznego", wyd. AON, Warszawa 2001.
23. Komow S.A.: „O sposobach i formach prowadzenia walki informacyjnej", w: Wojennaja Myśl, Moskwa 1997
24. Kozaczuk W.:"„Wojna w eterze". Warszawa 1977.
25. Koziej St.: Czynniki walki zbrojnej, w: „ZN AON" nr 4, 1993.
26. Koziej S.: „Teoria sztuki wojennej", wyd. AON, Warszawa 1993.
27. Kurnal J.: „Zarys teorii organizacji i zarządzania". Warszawa 1970.
28. Maliszewski W.: „Oddziaływanie psychologiczne w operacji obronnej". Rozprawa doktorska, wyd. AON, Warszawa 1998.
29. Markiewicz L.: „Ultradźwięki i infradźwięki", wyd. PWN, Warszawa 1979.
30. Mazur M.: „Jakościowa teoria informacji", Warszawa 1970.
31. Mitiugow W.: „Fizyczne podstawy teorii informacji", wyd. PWN, Warszawa 1980.
32. Neri F.: „Introduction to Electronic Defense Systems". Artech House, Inc., 1991.
33. Nowacki G.: „Walka informacyjna – próba kategoryzacji". Rozprawa doktorska, wyd. AON, Warszawa 1999.
34. Piekarski H.: „Istota i charakter walki radioelektronicznej w SZ RP", wyd. AON, Warszawa 1993.
35. Piekarski H.: „Walka radioelektroniczna", wyd. MON, Warszawa 1980.
36. Pierce J. R.: „Symbole, sygnały i szumy", wyd. PWN, Warszawa 1967.
37. Popper K. R.: „Logika odkrycia naukowego", wyd. PWN, Warszawa 1977.
38. Pytkowski W.: „Organizacja badań i ocena prac naukowych", wyd. PWN, Warszawa 1985.
39. „Regulamin działań wojsk lądowych", wyd. DWL, Warszawa 1999.
40. Ross J. D.: Wojna o informację. W: „Army", 2/1994.
41. Rotkiewicz W.: „Kompatybilność elektromagnetyczna w radiotechnice", wyd. KiŁ, Warszawa 1978.
42. Rutkowski C.: „Podstawowe pojęcia z dziedziny bezpieczeństwa i obronności państwa", w: „Myśl Wojskowa" nr 2, 1996.
43. Schwartau Winn.: „Information Warfare - Cyberterrorism: Protecting Your Personal Security in the Electronic Age". 1993.
44. Seidlar. J.: „Nauka o informacji". T I, II, wyd. WNT, Warszawa 1983.
45. Shannon. C. E, Warren. W.: „The Mathematical Theory of Communication". The University of Illinois Press, Urbana 1949.
46. Sienkiewicz P.: „Podstawy teorii systemów", wyd. AON, Warszawa 1994.
47. Sokołowski A.: „Ochrona informacji komputerowych", wyd. MON, Warszawa 1987.

48. Stankiewicz W.: „Ekonomika wojenna", wyd. MON. Warszawa 1981.
49. Starry M. D., Arneson C. W.: Działania informacyjne, w: „Military Review"nr 6, 1996.
50. Stalings W.: Ochrona danych w sieci i w intersieci, wyd. WNT, Warszawa 1997.
51. Sun Tzu: „Sztuka wojny", wyd. Wydawnictwo Przedświt, Warszawa 1994.
52. Szulc B.: „Walka zbrojna w kontekście ogólnej teorii walki i teorii konfliktów", wyd. AON, Warszawa 1996.
53. Szydłowski A.: „O psychologicznym podłożu maskowania", w: Myśl Wojskowa nr 4/96.
54. Ścibiorek Z: „Wpływ nowych środków walki na działania bojowe wojsk lądowych", wyd. AON, Warszawa 1993.
55. Świątnicki W. Z.: „Bronie inteligentne", wyd. ISBN, Warszawa 1992.
56. Tarasiuk B.: „Zautomatyzowane systemy dowodzenia wojsk lądowych", wyd. AON, Warszawa 1992.
57. Toffler Alvin i Heidi: „War and Anti-War" Tłumaczenie z języka angielskiego Barbara i Lech Budreccy: Wojna i antywojna", wyd. Warszawskie Wydawnictwo Literackie - Muza S.A. Warszawa1997.

Załącznik 1

Klauzula tajności

PLAN ZAKŁÓCANIA INFORMACYJNEGO W OPERACJACH WOJSK LĄDOWYCH – Część 1

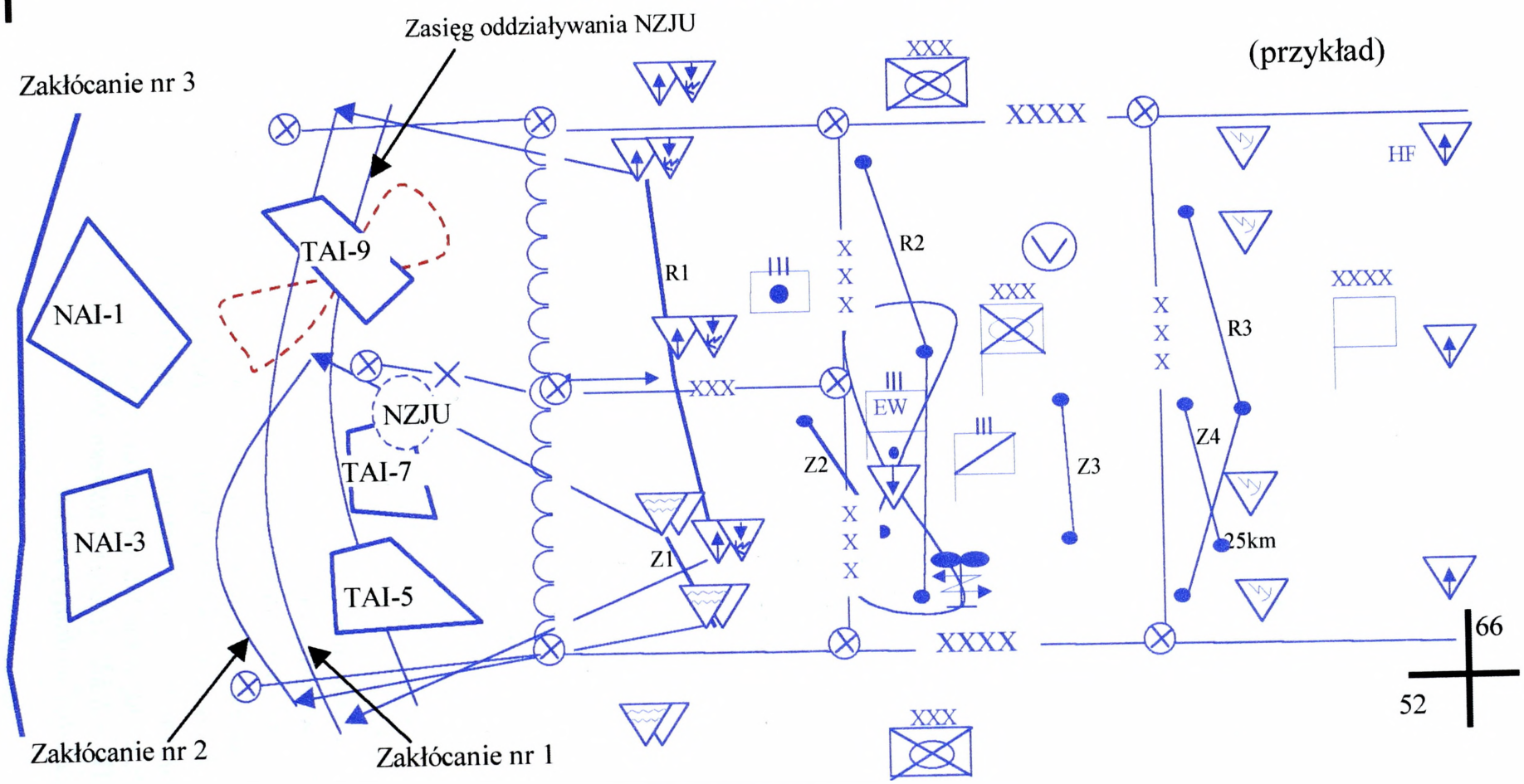
CZAS / WYKONAWCA	2 4 6 8 10 12 14 16 18 20 22	2 4 6 8 10 12 14 16 18 20
pel	1 A — 2 C	
e. śm. WI	3	
BAA	1 — 20 NZJU A - 1500	

ZADANIE	Dezorganizacja systemu dowodzenia .....K 1	Dezorganizacja systemu kierowania uzbr. ...K 2	Dezorganizacja systemu dowodzenia . . .K 3	Dezorganizacja systemu dowodzenia . . .K 4	 5
Obszar zainteresowania	A - TAI – 8 B - TAI – 9	C - TAI - 10 D - TAI - 7	E ..... F		
Zakłócane cele po wykryciu	A-2300 A-3000	A-2300 A-3000	A-.... A-.....	A-..... A-.....	

Klauzula tajności

96
48

Oleat „Plan zakłócania informacyjnego w operacji obronnej wojsk lądowych” – część 2



Załącznik 3

H-1

klauzula tajności

Kopia nr 4 z 50 kopii
DWLĄD. KOBYŁKOWO (.....; .....),
NIEBIESCY
251700 A July 2001
168 A

ANEKS H „ZAKŁÓCANIE INFORMACYJNE" DO DYREKTYWY OPERACYJNEJ DWLĄD. nr 1

Dokumenty odniesienia:
Mapa, 1501 EUROPA; arkusze: 168 A; 168 B; 168 C; 168 D; wydanie 1-OTSG; skala 1 : 500 000.
Strefa czasowa: ALFA – *może być ponownie powtórzona.*

1. SYTUACJA

a. Siły przeciwnika

(1) Siły główne - *odesłanie do: Aneks B (rozpoznanie) do planu działania DWląd.*

(2)Systemy rozpoznania przeciwnika – *uogólniona charakterystyka wykorzystywanych przez przeciwnika środków rozpoznania.*

(3)Systemy dowodzenia i kierowania uzbrojeniem przeciwnika - *krótka charakterystyka wykorzystywanych środków łączności, stacji radiolokacyjnych i innych środków elektronicznych.*

b. Wojska własne

*(1)*Przedsięwzięcia zakłócania informacyjnego realizowane przez przełożonego - *wymienia się jakie przedsięwzięcia z zakresu zakłócania informacyjnego realizował będzie przełożony na kierunku działania wojsk lądowych.*

(2)Wsparcie innych RSZ w zakresie *zakłócania informacyjnego – wymienia się jakie przedsięwzięcia z zakresu zakłócania informacyjnego realizowane będą przez inne rodzaje sił zbrojnych – lotnictwo, siły morskie*

(3)Przedsięwzięcia sąsiadów – *przedsięwzięcia w zakresie zakłócania informacyjnego realizowane przez sąsiadów.*

(4)Przydział wzmocnienie – *wymienia się jakie siły zakłócania informacyjnego zostały przydzielone, jakie podporządkowane czasowo, jakie się wydziela.*

c. Założenia.

(1)Plan działania – *odnośnik do Aneks C.*

*(2)*Przewidywane przedsięwzięcia przeciwnika - *jakie przedsięwzięcia obrony informacyjnej może zastosować przeciwnik w operacjach.*

(3) Spodziewane nowe systemy i środki *rozpoznania, dowodzenia i kierowania uzbrojeniem - krótka charakterystyka użycia nowych systemów zakłócania informacyjnego w toku prowadzonych działań.*

(4)Przewidywana taktyka użycia środków *ww. środków* przez przeciwnika.

2. ZADANIE – *Jakie zadanie z zakresu zakłócania informacyjnego realizować będzie szczebel wydający rozkaz.*

klauzula tajności
H-1

3. WYKONANIE

a. Koncepcja działania (zamiar). *Określenie głównego wysiłku WE. Wyjaśnienie sposobu wykorzystania elementów ugrupowania bojowego. Patrz plan działania Aneks C.*

b. Zadania dla elementów ugrupowania bojowego. *W kolejnych podpunktach stawiane są zadania dla poszczególnych elementów ugrupowania bojowego. Nie powtarza się zadań postawionych w dyrektywie operacyjnej i w apendyksach.*

c. Koordynacja działań. *Wyszczególnienie informacji dotyczących dwóch i więcej elementów ugrupowania bojowego i podanie niezbędnych współrzędnych, linii koordynacyjnych. Czasy rozpoczęcia i zakończenia zakłócania informacyjnego. Ustalenia w zakresie zastrzeżonych i zabronionych częstotliwości. Czasy gotowości do działań – mogą być powtórzone.*

4. ZABEZPIECZENIE LOGISTYCZNE

a. Zaopatrywanie w sprzęt zakłócania informacyjnego – *odwołanie do aneksu „Plan zabezpieczenia logistycznego".*

b. Zabezpieczenie techniczne przydzielonych środków *zakłócania informacyjnego - odwołanie do aneksu „Plan zabezpieczenia logistycznego".*

c. Uzupełnienie.- *odwołanie do aneksu „Plan zabezpieczenia logistycznego".*

5. DOWODZENIE I ŁĄCZNOŚĆ

a. Dowodzenie -*rozmieszczenie wysuniętego i głównego SD, własnego i przełożonego oraz jednostek współdziałających. Ich kolejne miejsca rozwinięcia.*

b. Łączność - *odesłanie do aneksu łączność Aneks L (łączność - elektronika) do planu działania.*

[podpis dowódcy (dowolny)]
(.....nazwisko dowódcy...)
(.....stopień.....

ZA ZGODNOŚĆ
(..poświadczenie G3..)

APENDYKSY:

1. Oleat – działań informacyjnych przeciwnika.
3 Wykaz wykrytych środków przeciwnika wykorzystywanych na potrzeby rozpoznania, dowodzenia i kierowania uzbrojeniem.
4 Wykaz celów do zakłócania informacyjnego.
5 Rejony i częstotliwości zastrzeżone.
6 Plan zakłócania informacyjnego.
7 Inne – wg potrzeb.

Rozdzielnik: B

Jeżeli aneks jest wysyłany oddzielnie od dyrektywy, musi być opisany tak jak dyrektywa (strona tytułowa, podpis, rozdzielnik). Natomiast w sytuacji gdy jest on integralną częścią dyrektywy i jest rozprowadzany według tego samego rozdzielnika, wystarczy sam tytuł dokumentu.- wówczas w aneksie nie umieszcza się tekstu zaznaczonego ramkami.