

Józef Janczak

Zakłócanie Informacyjne

Biblioteka Główna
Akademii Sztuki Wojennej

54287



09-054287-000-0

54287



AKADEMIA OBRONY NARODOWEJ

AKADEMIA OBRONY NARODOWEJ

Józef JANCZAK

ZAKŁÓCANIE INFORMACYJNE



WARSZAWA

2001

Recenzent

prof. dr hab. Leopold CIBOROWSKI

Projekt okładki

Genowefa Majchrowska

ISBN 83-88062-87-5

Sygn. AON 5369/2001

78842

Druk i oprawa: Akademia Obrony Narodowej – Wydział Wydawniczy
00-910 Warszawa, al. gen. A. Chruściela 103, tel./faks 681-37-52
Zam. nr 1521/2001

SPIS TREŚCI

WSTĘP	5
1. ROLA I MIEJSCE ZAKŁÓCANIA INFORMACYJNEGO W WALCE ZBROJNEJ	10
1.1. Istota zakłócania informacyjnego	10
1.2. Podstawowe rodzaje zakłócania informacyjnego	24
1.2.1. Zakłócanie dezinformujące	26
1.2.2. Zakłócanie zagłuszające	43
1.2.3. Zakłócanie niszczące	55
1.3. Podział zakłócania informacyjnego	72
2. ZAKRES I TREŚĆ PRZEDSIĘWZIĘĆ ZAKŁÓCANIA ROZPOZNANIA PRZECIWNIKA	74
2.1. Zakłócania rozpoznania bezpośredniego	78
2.1.1. Zakłócanie rozpoznania agenturalnego	80
2.1.2. Zakłócanie rozpoznania patrolowego	81
2.1.3. Zakłócanie rozpoznania specjalnego	89
2.2. Zakłócanie rozpoznania pośredniego.....	91
2.2.1. Zakłócanie rozpoznania elektronicznego.....	92
2.2.1.1. Zakłócenia rozpoznania radio- elektronicznego.....	95

2.2.1.2. Zakłócanie rozpoznania radio- lokacyjnego	113
2.2.1.3. Zakłócanie rozpoznania czujnikowego ...	125
2.2.1.4. Zakłócanie rozpoznania opto- elektronicznego	128
2.2.1.5. Zakłócanie rozpoznania informatycznego	135
2.2.2. Zakłócanie rozpoznania studyjnego	149
3. ZAKRES I TREŚĆ PRZEDSIĘWZIĘĆ ZAKŁÓCANIA DOWODZENIA PRZECIWNIKA	155
3.1. Zakłócanie systemów (sieci) łączności	156
3.2. Zakłócanie systemów (sieci) informatycznych	173
3.3. Zakłócanie systemów radionawigacyjnych	177
4. ZAKRES I TREŚĆ PRZEDSIĘWZIĘĆ ZAKŁÓCANIA KIEROWANIEM UZBROJENIEM PRZECIWNIKA	186
ZAKOŃCZENIE	197
BIBLIOGRAFIA	199

WSTĘP

Bogata historia walki zbrojnej dowodzi, że na przestrzeni dziejów sukcesywnie odbywało się wzmacnianie potencjału bojowego sił zbrojnych. Motorem postępu w tej dziedzinie były osiągnięcia nauki i techniki. W obecnych czasach szczególną uwagę zwraca się na rozwój środków wykorzystywanych na potrzeby rozpoznania, dowodzenia i łączności, walki elektronicznej oraz nowej generacji środków niszczenia. Coraz większą uwagę zwraca się również na problemy dominacji informacyjnej nad przeciwnikiem. Rozwijana jest teoria walki informacyjnej. W dobie powszechnej informatyzacji pola walki pokonanie przeciwnika w sferze informacyjnej może okazać się czynnikiem decydującym o ogólnym sukcesie w walce zbrojnej.

Istota walki informacyjnej sprowadzana jest do stwarzania sytuacji utrudniających przeciwnikowi podejmowanie trafnych decyzji, wykonywania sprawnych przemieszczeń wojsk i precy-

zyjnych 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. Współczesna walka informacyjna traktowana jest jako teoretyczne rozwinięcie problematyki rozpoznania wojskowego, walki elektronicznej¹ i rażenia ogniowego. Teoria ta pozwala bowiem na integrację posiadanych sił i środków działających w sferze informacyjnej, w której wykorzystuje się kompleksowo wojskowe systemy informatyczne do uzyskania przewagi nad przeciwnikiem oraz osiągnięcia zamierzonych celów walki zbrojnej. U podstaw powyższej teorii legło przekonanie, że zastosowanie systemów informatycznych w celu osiągnięcia przewagi informacyjnej nad przeciwnikiem może prowadzić do uniknięcia groźby wybuchu klasycznego konfliktu zbrojnego.

Rozwijana teoria walki informacyjnej skłania do postawienia pytania: czy nasze wojska są obecnie przygotowane do prowadzenia tego typu walki, a w tym szczególnie zakłócania informa-

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.

cyjnego oraz w jakim stopniu proces zakłócania przepływu informacji może wpłynąć na prowadzone przez nie działania wojenne?

Próbę przedstawienia powyższych problemów podjęto w niniejszym opracowaniu, w którym zawarto **istotę, zakres i treść przedsięwzięć zakłócania informacyjnego w walce zbrojnej XXI wieku**².

Powyższą problematykę przedstawiono przede wszystkim w aspekcie operacyjno-taktycznym, uwzględniając charakter i właściwości współczesnych działań zbrojnych. Takie ujęcie wynika z faktu, że zakłócanie informacyjne nie stanowi przedsięwzięcia zbrojnego, którego realizacją zajmuje się tylko wąski krąg specjalistów, lecz jest sferą szerokiej i aktywnej działalności dowódców, sztabów i wojsk ukierunkowanej na dezorganizację rozpoznania, dowodzenia i kierowania uzbrojeniem przeciwnika. Należy prowadzić je na lądzie, w powietrzu i na morzu, a także w przestrzeni elektromagnetycznej z udziałem wszystkich rodzajów sił zbrojnych i wojsk, stosownie do posiadanego uzbrojenia i jego możliwości bojowych.

² Wiek XXI jest postrzegany jako epoka budowy społeczeństwa informacyjnego. Por.: Globan-Klas T., Sienkiewicz P., „Społeczeństwo informacyjne: Szanse, zagrożenia, wyzwania”, wyd. Fundacji Postępu Telekomunikacji, Kraków 1999.

Opracowanie składa się z wstępu, czterech rozdziałów merytorycznych, zakończenia, bibliografii.

W rozdziale pierwszym przedstawiono istotę zakłócania informacyjnego w walce zbrojnej. Określono jego rolę i miejsce w walce zbrojnej oraz sprecyzowano przedmiot, cel, rodzaje i podstawowy podział.

W rozdziale drugim przedstawiono zakres i treść przedsięwzięć zakłócania rozpoznania przeciwnika. Uznano za niezbędne zdeorganizowanie pracy jego elementów rozpoznania bezpośredniego (agenturalnego, patrolowego, specjalnego) oraz pośredniego (elektronicznego i studyjnego).

W rozdziale trzecim przedstawiono zakres i treść przedsięwzięć zakłócania dowodzenia przeciwnika. Zwrócono uwagę na konieczność dezorganizacji pracy jego systemów (sieci) łączności, systemów (sieci) informatycznych oraz systemów radionawigacyjnych.

W rozdziale czwartym przedstawiono zakres i treść przedsięwzięć zakłócania kierowania uzbrojeniem przeciwnika, którymi objęto jego urządzenia radiolokacyjne, telewizyjne, termowizyjne, laserowe oraz radiowe.

Myślą przewodnią niniejszej monografii była chęć przedstawiania złożonych problemów zakłócania informacyjnego

w walce zbrojnej w sposób przystępny, na poziomie popularno-naukowym. Treści poszczególnych rozdziałów adresowane są do szerokiej rzeszy Czytelników interesujących się problematyką walki zbrojnej, w której coraz większą rolę odgrywa zakłócanie, będące ofensywną formą współczesnej konfrontacji zbrojnej w sferze informacyjnej.

Mam nadzieję, że przedstawione w monografii treści przybliżą Czytelnikowi złożoną problematykę zakłócania informacyjnego, która nabiera znaczenia wraz z cyfryzacją i informatyzacją pola walki.

Przyjemnej lektury życzy

Autor

1. ROLA I MIEJSCE ZAKŁÓCANIA INFORMACYJNEGO W WALCE ZBROJNEJ

1.1. Istota zakłócania informacyjnego

Współcześni teoretycy wojskowi³ zakładają, że obecny model walki zbrojnej obejmuje trzy zasadnicze czynniki: rażenie (ogień), manewr (ruch) i informację. Informację postrzegają jako czynnik kluczowy na współczesnym polu walki. Uważają, że określenie właściwych zależności między czynnikami operacyjnymi⁴ 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 wszyst-

³ S. Koziej, „Teoria sztuki wojennej”, wyd. AON, Warszawa 1993.

⁴ Do czynników operacyjnych, od których zależy rozmach i przebieg działań operacyjnych, zalicza się: siły, obszar, czas i informację. Por. „Regulamin działań wojsk lądowych”, wyd. DWŁąd, Warszawa 1999, s. 57.

kim więcej niż przeciwnik. Informacja lub jej brak jest czynnikiem decydującym o sukcesie lub porażce w walce zbrojnej. Jest zasadniczym warunkiem umożliwiającym prowadzenie działań zbrojnych, 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 sferze informacyjnej, którą po wojnie w rejonie Zatoki Perskiej w 1991 roku przyjęto określać mianem walka informacyjna⁵.

Walka informacyjna⁶ – 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 jest obok zdobywania⁷ (rozpoznania) informacji i obrony informacyjnej⁸ podstawowym komponentem walki informacyjnej⁹.

⁵ A., D. Campen, „The first Information War”, ed. AFCA International Press Fairfax, Virginia 1992.

⁶ L. Ciborowski, „Walka informacyjna”, wyd. ECE, Toruń 1999.

⁷ 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.

Zakłócanie informacyjne¹⁰ 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.

Zakłócanie informacyjne prowadzi się więc w celu obniżenia efektywności funkcjonowania systemów dowodzenia i kierowania uzbrojeniem przeciwnika oraz ich zasobów i procesów informacyjno-sterujących¹¹. Polega ono na dezorganizacji pracy

⁸ 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.

⁹ Należy nadmienić, że pojęcie walka informacyjna nie jest dotychczas oficjalnie wyróżniane w dokumentach normatywnych Sztabu Generalnego WP.

¹⁰ Por.: „Regulamin działań wojsk lądowych”, wyd. DWŁąd, Warszawa 1999, s. 62.

¹¹ Systemy informacyjno – sterujące stanowią zespoły powiązanych ze sobą funkcjonalnie i organizacyjnie elementów (sił i środków). Przeznaczone są do zdobywania, przetwarzania, gromadzenia i dystrybucji danych niezbędnych do podjęcia decyzji na wszystkich szczeblach organizacyjnych, a ich strukturę stanowią: źródła informacji, przetworniki informacji, nośniki informacji, układy odbierające oraz relacje systemowe.

elementów rozpoznawczych oraz systemów dowodzenia i kierowania uzbrojeniem przeciwnika. Zakłócanie informacyjne powinno być skoncentrowane na działalności umożliwiającej racjonalne modelowanie procesu przygotowywania wojsk do realizacji zadań w okresie zaistnienia konfliktu zbrojnego oraz podczas prowadzenia działań zbrojnych.

Wiadomym jest, że szczególna rola w tym zakresie przypada szeroko rozumianemu rozpoznaniu¹². 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 przez niego decyzji, które stanowić będą dla niego przyczynę podjęcia wymuszonych działań.

¹² Określenia użyto w rozumieniu, iż w rozpoznaniu mieści się również wywiad.

Zakłócanie informacyjne powinno być ukierunkowane na zwiększanie entropii informacyjnej¹³ komunikatów przeciwnika i dążenie do destrukcji wszelkich nośników danych.

Zakłócanie informacyjne należy postrzegać również jako 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 deformowania lub wytwarzania danych nieprawdziwych i przez to wpływa negatywnie na inne procesy pola walki.

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

¹³ 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 odebranych 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).

Zakłócanie informacyjne w walce zbrojnej spełnia jak gdyby dwie funkcje. Jedna z nich jest szeroko rozumiane pozorowanie, mające na celu wprowadzanie w błąd przeciwnika. Jego celem jest udostępnienie przeciwnikowi takich postaci danych, które po przetworzeniu będą przedstawiać sytuację nierealną, a zarazem maksymalnie stwarzającą pozory działań rzeczywistych. Druga funkcja jest dezorganizacja pracy systemów dowodzenia wojskami i kierowania uzbrojeniem przeciwnika oraz dążenie do fizycznej destrukcji nośników danych.

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 walce zbrojnej powinien obejmować okres przygotowania działań zbrojnych oraz ich prowadzenia. Okres przygotowania działań zbrojnych jest stosunkowo długi i charakteryzuje się niewielką dynamiką procesów informacyjnych. W okresie tym proces zakłócania informacyjnego

powinien być realizowany w ograniczonym wymiarze, głównie w zakresie dezinformowania. Natomiast okres prowadzenia działań zbrojnych powinien charakteryzować się znacznie większą dynamiką i różnorodnością stosowanych przedsięwzięć.

Z powyższego wynika, że w obydwu okresach zakłócania informacyjnego należy zachować odpowiednie proporcje, wynikające z rodzaju działań zbrojnych i sposobów ich przygotowania i prowadzenia.

W zakłócaniu informacyjnym należy 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 wcześniej, dane o potencjalnym przeciwniku, terenie i panujących tam warunkach. W obszarze działań zbrojnych i w jego otoczeniu obiekty podlegające rozpoznaniu są najczęściej zamaskowane. Wówczas organy (elementy) rozpoznawcze mogą napotykać na duże trudności ze zdobywaniem danych rozpoznawczych. Po-

nadto przeciwnik może pozorować 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 nie zawsze trafne, a nawet błędne.

W warunkach prowadzenia działań zbrojnych, 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 należy prowadzić różnymi sposobami, przy pomocy odpowiednich środków i metod postępowania (przedsięwzięć). Najbardziej skutecznymi są środki niszczenia, jednak mając na uwadze realia obszaru pola walki nie wszystkie obiekty w sferze informacyjnej można zniszczyć. Nie bez znaczenia są także koszty, które powinny być minimalizowane stosownie do osiągniętych rezultatów. Warunki te dyktują potrzebę posiadania środków maskowania (ukrywania, dezinformowania, pozorowania), zagłuszania 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 (rejonu) działań zbrojnych.

Ważną rolę odgrywają również sposoby przygotowania działań w zakresie zakłócania informacyjnego oraz metody użycia sił i środków. Należy weryfikować je stosownie do zmian zachodzących w sytuacji oraz procesach informacyjno-sterujących towarzyszących walce zbrojnej. Dlatego też należy kształtować właściwe proporcje pomiędzy podejmowanymi przedsięwzięciami (działaniami) w tym zakresie. Wojska powinny dysponować określonym potencjałem bojowym¹⁴, charakteryzującym się jednoznacznymi wskaźnikami ilościowymi i jakościowymi. Z tego wynikają konkretne potrzeby w zakresie zakłócania, które konieczne należy uwzględnić w planowaniu działań, dowodzeniu wojskami 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

¹⁴ Określenie potencjału bojowy użyte jest w rozumieniu, że są to siły i środki przeznaczone do prowadzenia walki zbrojnej, której istotą jest rażenie przeciwnika.

rubieże (pozycje) bojowe i związane z wykonywaniem przez nie skutecznego rażenia.

Potencjał zakłócania informacyjnego oraz zasady jego użycia powinny być kompatybilne do obezwładnianych zakłóceniami środków przeciwnika. Należy uwzględnić również zasady wykorzystania wojsk własnych w przyszłych działaniach zbrojnych. W tej problematyce najbardziej istotne są posiadane środki (urządzenia) techniczne, określone sposoby i metody ich wykorzystania oraz zasady prowadzenia zakłócania informacyjnego. Dlatego też za punkt odniesienia należy przyjmować stan posiadania w otaczającym obszarze (rejonie) 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 sposobów zakłócania informacyjnego obecnie nie zawsze 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, jest zakłócaniem informacyjnym. Przy takim rozumieniu istoty zjawiska, do zakłócania informacyjnego należy również zaliczyć wszelkie formy masko-

wania i pozorowania. Wiele też można uczynić, w zakresie zakłócania informacyjnego drogą destrukcyjnego oddziaływania na środki przetwarzania danych i czynnik ludzki. W pierwszym wypadku bardzo skutecznym może okazać się zastosowanie urządzeń zakłócających, wykorzystujących energię elektromagnetyczną, natomiast w drugim, tj. w sferze zakłócania osobowego bardziej przydatne mogą okazać się technika infradźwiękowa¹⁵ oraz z dziedziny psychotroniki¹⁶.

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

– posiadanie danych o stanie i funkcjonowaniu procesów informacyjnych u przeciwnika, wykorzystywanej przez niego urządzeń i środkach technicznych, metodach zdobywania i gromadzenia informacji, czy dowodzeniu, co jest niezbędne do przy-

¹⁵ Infradźwięki – fale sprężyste o częstotliwościach mniejszych niż 16 Hz, a więc leżące poniżej zakresu ludzkiej słyszalności. Fale te są słabo tłumione i dlatego rozprzestrzeniają się na duże odległości od źródła. Mogą być wykorzystane do rejestracji efektów sejsmicznych i eksplozji na polu walki. „Ilustrowana encyklopedia dla wszystkich. Fizyka”, wyd. WNT, Warszawa 1991, s. 112.

¹⁶ Psychotronika – nauka interdyscyplinarna z pogranicza biofizyki, biochemii, biocybernetyki, psychofizjologii. Wyodrębniona z parapsychologii, zajmuje się badaniem interakcji między organizmami żywymi oraz procesami energetycznymi zachodzącymi między nimi a ich środowiskiem wewnętrznym i zewnętrznym, a także opisem i wyjaśnieniem oddziaływań świadomości z innymi procesami, jak: fizycznymi, biologicznymi, psychicznymi i innymi. „Internetowa Encyklopedia PWN”.

gotowania 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 elementów, nie można podejmować przemyślanych i skutecznych przedsięwzięć i zadań w zakresie zakłócania informacyjnego. 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 w zakresie zakłócania informacyjnego. Możliwości techniczne własnych środków powinny umożliwić wykonanie tych zadań, a zatem nie powinny odbiegać jakością od obezwładnianych zakłóceniami środków rozpoznania, dowodzenia wojskami i kierowania uzbrojeniem przeciwnika.

– system informacyjny przeciwnika, który podlega zakłócaniu i zmienia się w wyniku wyeliminowania poszczególnych jego ogniw oraz poprzez dokonanie wewnętrznych zmian uodporniających 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 operacji (walki) walki. Procesowi temu powinny odpowiadać odpowiednie działania w zakresie zakłócania, ukierunkowane na poszukiwanie optymalnych i skutecznych metod oddziaływania. W procesie tym należy unikać działań szablonych, maksymalnie wykorzystywać właściwości maskujące terenu oraz istniejące warunki taktyczne i operacyjne.

Dążyć należy do uzyskania zaskoczenia w każdym obszarze 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 wymiarach (sferach), powinno być postrzegane jako jeden obszar działania, jednolicie planowany pod kątem sposobu rozegrania działań zbrojnych przez dowódcę, a wykonawcami zadań w jego zakresie powinien być szeroki krąg uczestników.

Procesy informacyjne, we współczesnych działaniach zbrojnych, w zdecydowanej większości są realizowane za pomocą środków elektronicznych, zatem spektrum elektromagnetyczne¹⁷ należy postrzegać za najważniejsze w procesie zakłócania informacyjnego.

W procesie zakłócania informacyjnego niezwykle istotnym czynnikiem jest również czas. Aby można było wykonać określone zadania w zakresie zakłócania należy ciągle nadążać a niekiedy wyprzedzać funkcjonowanie procesów informacyjnych w aspekcie czasu ich funkcjonowania. Sprowadza się to do tego, że maskowanie i pozorowanie 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.

Z kolei zakłócanie dowodzenia wojskami i kierowania uzbrojeniem należy realizować w rejonach (obszarach) odbioru sygnałów informacyjno-sterujących przez adresatów. Natomiast

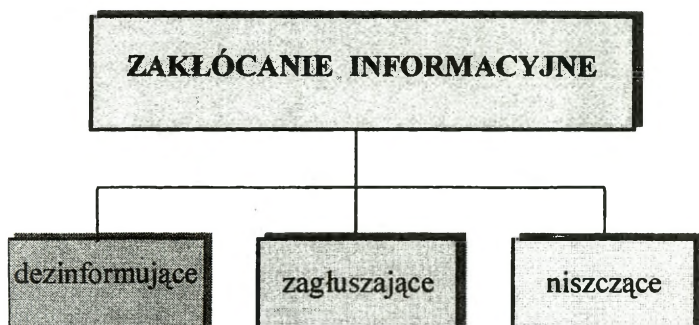
¹⁷ „Spektrum elektromagnetyczne” jest często określane jako „przestrzeń elektromagnetyczna”, „eter”, niekiedy jako „czwarty wymiar”. Wykorzystanie spektrum elektromagnetycznego jest możliwe dzięki zbudowaniu urządzeń promieniujących energię elektromagnetyczną i urządzeń ją odbierających. Współdziałanie między tymi urządzeniami może wystąpić wówczas gdy pracują one na tej samej częstotliwości, a warunki rozprzestrzeniania pozwalają urządzeniom odbiorczym na odbiór energii elektromagnetycznej wysyłanej przez urządzenia nadawcze.

niszczenie powinno być realizowane zaraz po wykryciu obiektu pracującego w systemie informacyjno - sterującym. Takie warunki czasowe zakłócania informacyjnego są często trudne do spełnienia, dlatego należy dążyć do posiadania urządzeń technicznych, umożliwiających 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 odnośnie środków technicznych i w zakresie ich odpowiednio krótkiego czasu reakcji.

1.2. Podstawowe rodzaje zakłócania informacyjnego

Z dotychczasowych rozważań wynika, że do podstawowych rodzajów zakłócania informacyjnego należy zaliczyć (rys. 1.1):

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



Rys. 1.1. Podstawowe rodzaje zakłócania informacyjnego

Realizację zadań na potrzeby poszczególnych rodzajów zakłócania informacyjnego umożliwia dezorganizacja pracy najważniejszych elementów rozpoznawczych oraz systemów dowodzenia i kierowania uzbrojeniem przeciwnika w sposób zmasowany, niespodziewanie, w rejonach kluczowych i w decydujących etapach działań zbrojnych.

1.2.1. Zakłócanie dezinformujące

Zakłócanie dezinformujące polega na wprowadzaniu w błąd przeciwnika przez podanie mylących informacji. W ujęciu wojskowym, to rozpowszechnianie nieprawdziwych wiadomości i dokumentów co do zamiaru, przygotowania operacji (walki), a także charakteru ich prowadzenia.

Zakłócanie dezinformujące jako element składowy walki informacyjnej 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. Problematyka ta utożsamiana jest najczęściej z dezinformacją osobową.

Zakłócanie dezinformujące może również odbywać się w formie odpowiednio dobranych sygnałów odbieranych przez urządzenia elektroniczne wykorzystywane na potrzeby rozpoznania, dowodzenia wojskami i kierowania uzbrojeniem. Działania takie utożsamiane są wówczas z dezinformacją techniczną.

Dezinformacja osobowa. Dezinformacja osobowa to zespół przedsięwzięć polegających na rozpowszechnianiu u przeciwnika odpowiednio spreparowanych wiadomości w celu od-

działania 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. Celem dezinformacji osobowej jest realizacja 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 zbrojne.

W aspekcie stosowania dezinformacji osobowej 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 zdeorientowana 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 wpływają bezpośrednio ze specyfiki oddziaływań dezinformujących, które to w swej istocie polegają na modyfikowaniu postaw oraz zachowań stanów osobowych.

Do form dezinformacji osobowej można zaliczyć pozorowanie i manipulowanie.

Pozorowanie¹⁸ polega na sztucznym tworzeniu „obrazu” (obiektu, czynności itp.) zbliżonego do rzeczywistego. Osiąga się je przez:

- tworzenie obiektów pozornych własnych wojsk;
- pozorowanie innych form działań niż faktycznie prowadzone;
- stosowanie manewru pozornego oraz pozornych przedsięwzięć organizacyjnych;
- deformowanie obiektów rzeczywistych;
- tworzenie pozornych stanowisk dowodzenia związków operacyjnych, taktycznych i oddziałów.

¹⁸ Pozorowanie jest formą maskowania, a przedsięwzięcia wykonywane w jego zakresie powinny być koordynowane w ramach obrony informacyjnej, w realizacji zadań której uczestniczą również siły i środki zakłócania informacyjnego.

Celem działań pozornych jest zmylenie przeciwnika, czyli wprowadzenie go w błąd. Działania pozorne stanowią kompleks organizacyjnych, materiałowych i praktycznych przedsięwzięć, zgodnych z celem i zadaniami operacji (walki), 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 oraz prowadzenia operacji (walki). 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 działań zbrojnych. 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 (walki). Dzięki prowadzeniu działań pozornych można osiągać wielkie sukcesy przy małych stratach ludzi, niskim zużyciu materiałów i czasu. W tym sensie działania pozorne są ściśle związane z zasadami sztuki operacyjnej.

Drugą formą dezinformacji osobowej jest **manipulowanie**. Termin ten nie jest jednoznaczny i trudny do zdefiniowania. Próby zdefiniowania podejmowane przez autorów na gruncie psychologii społecznej, socjologii i socjotechniki, nie dały jednoznacznych rezultatów¹⁹. Pojęcie manipulowanie dosyć trafnie oddaje stwierdzenie „często człowiek otwiera usta tylko po, by kimś manipulować”. 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 manipulowania, 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 manipulowania 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;

¹⁹ W. Maliszewski: „Oddziaływanie psychologiczne w operacji obronnej”, wyd. AON, Warszawa 1998.

– 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;

– 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 postaw²⁰;

– epistemologiczną istotą oddziaływania manipulacyjnego jest proces sterowania, który prowadzi do realizacji celów podmiotu działań – zgodnych z celem i obiektywnym interesem własnych sił prowadzących działania zbrojne. Innymi słowy manipulację można prowadzić tam, gdzie odpowiedni przekaz informacyjny (sterowanie), będzie modyfikował postawy i zachowania żołnierzy oraz ludności cywilnej przeciwnika, tak że sterowana

²⁰ Por.: R. Nawrat: „Manipulacja społeczna – przegląd technik i wybranych wyników badań”. W: „Przegląd Psychologiczny” 1/1989, s. 125–127.

grupa społeczna (np. pododdział), nie wykona zadania, zaniecha lub zaniedba działań ważnych dla własnej pomysłowości, własnych interesów bądź celów tego, kto formalnie nią kieruje i dowodzi. 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.

Podczas manipulowania oddziałuje się też na uczucia oraz 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 szereg 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.

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 pożądanых 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 utkwąć 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”.

Trzeci sposób 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.

Czwarty sposób może być sprowadzony 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, są „rozmydlone” i nie dostrzegane przez przedmiot oddziaływania.

Piaty 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 oraz 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 prawdziwą²¹. Pozorowanie elektroniczne wnosi do systemu 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 pozorowania elektronicznego wymaga doskonałej znajomości zasad organizacji systemów elektronicznych przeciwnika, sposobów przekazywania danych, stosowanych zabezpieczeń, posiadania odpowiedniego sprzętu oraz ciągłego śledzenia pracy jego środków i systemów.

We współczesnej walce zbrojnej znaczenie pozorowania elektronicznego 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,

²¹ Pozorowanie elektroniczne jest formą maskowania elektronicznego, a przedsięwzięcia wykonywane w jego zakresie powinny być koordynowane w ramach obrony informacyjnej, w realizacji zadań której uczestniczą również siły i środki zakłócania informacyjnego.

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, 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, gdyż stanowi to maksymalne utrudnienie przeciwnikowi możliwości rozpoznania elementów ugrupowania operacyjnego (bojowego), systemów dowodzenia i ważnych obiektów infrastruktury obszaru (rejonu) działań zbrojnych oraz skierowanie jego wysiłku rozpoznawczego i uderzeniowego na rejon i obiekty pozorne. Budowa wiarygodnych rejonów i obiektów pozornych pozwala wprowadzić w błąd prze-

ciwnika co do rzeczywistego stanu rozbudowy inżynieryjnej obszaru (rejonu) działań, głównie obronnych, rozmieszczenia elementów ugrupowania operacyjnego (bojowego) i jego ważnych obiektów. Działania te powinny zmuszać przeciwnika do rozproszenia wysiłku rozpoznawczego i uderzeniowego, co z kolei powinno zmniejszyć prawdopodobieństwo zniszczenia obiektów rzeczywistych. 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 są szczególnie przydatne przy ataku przeciwnika z powietrza, ponieważ pilot ma zaledwie kilka sekund na ich identyfikację i podjęcie decyzji dotyczącej ataku. Prawdopodobieństwo przeprowadzenia ataku na cel pozorny przy zastosowaniu właściwego sposobu 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 elek-

tromagnetycznej w sposób zamierzony w celu zmylenia, odwrócenia uwagi lub oszukania przeciwnika i jego systemów rozpoznania elektronicznego. Do sposobów mylenia zalicza się:

- wyprzedzającą lub opóźniającą bramkę odległości zmieniającą zasięg blokowania radarów impulsowych;
- wyprzedzającą lub opóźniającą bramkę 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.

Do podstawowych **form mylenia** zalicza się: manipulowanie, symulowanie, imitowanie.

Manipulowanie elektroniczne polega na zmianie profili elektromagnetycznych własnego sprzętu elektronicznego w celu uniemożliwienia przeciwnikowi jego rozpoznania. Może być dokonane poprzez zmianę charakterystyk technicznych i profili elektromagnetycznych 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 naszym wojskom, a także gdy będzie dążył do uzyskania obrazu elektromagnetycznego ich ugrupowania operacyjnego (bojowego). Może obejmo-

wać 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 (walki). Należy mieć na uwadze, że 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 organizacji, użytych środkach i sposobach ich wykorzystania.

Manipulowanie elektroniczne jest realizowana przez:

- emitowanie fałszywych poziomów źródeł promieniowania energii elektromagnetycznej;
- tworzenie fałszywych lub kontrolowanych tras teletransmisyjnych;
- ukrywanie faktycznego natężenia ruchu telekomunikacyjnego;
- zmianę parametrów elektronicznych obiektów;
- kontrolowanie naruszenia zasad wymiany radiowej;
- celowy wyciek spreparowanych informacji związanych z fazami operacji (walki).

Symulowanie polega na elektronicznej reprezentacji własnych sił w innym miejscu niż rzeczywista ich lokalizacja. Zmian rejonów należy dokonywać w okresach zakazu pracy środków

elektronicznych na nadawanie (w czasie trwania tzw. „ciszy radiowej”). Jego celem jest przeciwdziałanie rozpoznaniu przeciwnika i utrudnienie określania ugrupowania operacyjnego (bojowego) wojsk własnych, ich rozmieszczenia, potencjalnych możliwości, zamiarów itp.

Środki elektroniczne (zarówno radiowe jak i nie-radiowe) powinny być użyte do wytwarzania pozornych (fałszywych) obrazów (obiektów) w ramach symulacji, jednak tylko wtedy gdy przeciwnik ma wystarczające siły i urządzenia do ich wykrycia. Symulacja może być wykorzystana zarówno do tworzenia obiektów pozornych (reprezentowania fałszywych ich lokalizacji) jak i zmian w treści rozkazów operacyjnych. Najczęściej stosowanymi formami symulowania są więc:

- fałszywe lokalizowanie obiektów,
- zmiana rozkazu operacyjnego.

Imitowanie jest najczęściej postrzegane jako specyficzne (dywersyjne) zakłócanie, ponieważ efekt mylenia jest osiągany 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 relacji informacyjnych przeciwnika wymaga znajomości

zasad i procedur ich pracy, bez których istnieje duże ryzyko szybkiego zidentyfikowania źródła dywersyjnego oddziaływania.

Imitowanie jest realizowana przez:

- planowane bezprawne włączenie się do relacji informacyjnych 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);
- uciążliwe transmisje w celu zdenerwowania lub odwrócenia uwagi operatora od jego rzeczywistych zadań.

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 z wojny w rejonie Zatoki Perskiej, zakłócanie dezinformujące wydaje się być niezmiernie humanitarnym sposobem konfrontacji zbrojnej, umożliwiającym osiągnięcie celów 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 przede wszystkim w przestrzeni elektromagnetycznej. W połączeniu z dezinformacją techniczną powoduje naruszenie u przeciwnika poprawności funkcjonowania systemów rozpoznania elektronicznego, a także systemów dowodzenia 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 zagłu-

szającego na proces informacyjny przeciwnika unaocznia jedno z podstawowych równań teorii informacji stworzonej przez Shannona²², z którego wynika zależność określająca ilość informacji jaką można przesłać 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;

²² Shannon Claude Elwood, ur. 1916 r., matematyk amerykański, profesor MIT, członek National Academy of Science, twórca teorii informacji.

– rejestrację 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 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 (np. zespołów prądotwórczych, silników spalinowych z zapłonem iskrowym) lub w wyniku nieumiejętnego rozmieszczenia środków elektronicznych na stanowiskach dowodzenia. Zakłócenia przypadkowe mogą być również pochodzenia kosmicznego oraz jako naturalne

wewnętrzne szумы, 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, pasywne²³ oraz kombinowane (w przypadku jednoczesnego stosowania zakłóceń aktywnych i pasywnych).

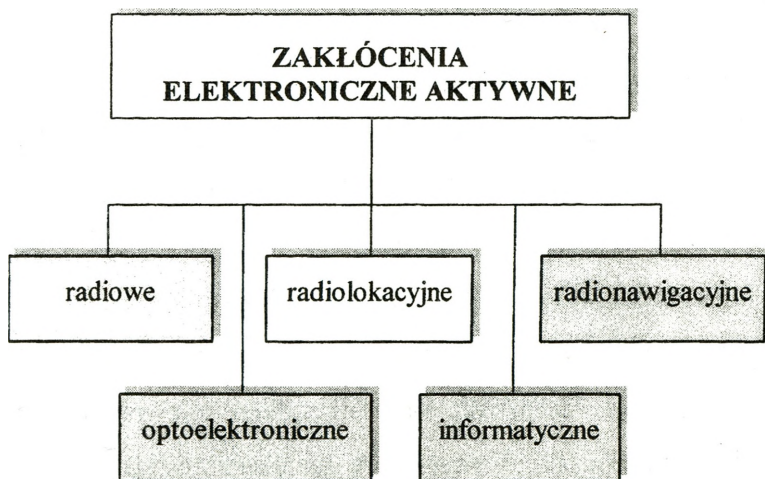
Zakłócenia elektroniczne aktywne. Zakłócenia elektroniczne aktywne polegają na promieniowaniu przez urządzenia nadawcze zakłócającej energii elektromagnetycznej na częstotliwościach lub w paśmie pracy zakłócanych urządzeń odbiorczych. Mogą być emitowane przez stacje zakłócające stacjonarne i mobilne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

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

²³ Zakłócenia pasywne stosowane są również w dezinformacji technicznej.

których dokładnie dostrajane są nadajniki zakłócające. Wyróżnia się zakłócenia (rys. 1.2): radiowe, radiolokacyjne, radionawigacyjne, optoelektroniczne i informatyczne.

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.



Rys. 1.2. Podział aktywnych zakłóceń elektronicznych

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 detonacje 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 elektromagnetycznej powodującej utrudnienie pracy środków i systemów radionawigacyjnych (w tym bliskiej radionawigacji oraz systemów globalnych).

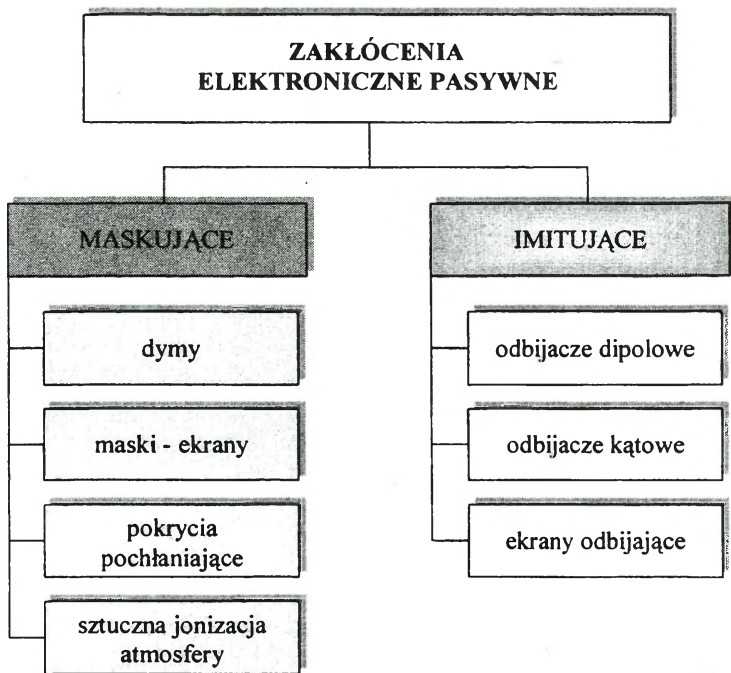
Zakłócenia optoelektroniczne mają na celu dezorganizację funkcjonowania środków rozpoznania i sterowania pracujących w podczerwieni, termolokatorów, urządzeń telewizyjnych oraz urządzeń laserowych. Z uwagi na coraz szersze wykorzystywanie tych środków w działaniach wojsk należy przewidzieć szerokie stosowanie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

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

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

Zakłócenia elektroniczne pasywne. Pasywne zakłócenia elektroniczne polegają na wtórnym promieniowaniu, odpromieniowywaniu, odbijaniu i rozpraszaniu lub też zmianie albo wchłanianiu energii elektromagnetycznej przez środki nie dysponujące generatorami energii elektromagnetycznej 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 urządzenia rozpoznawcze przeciwnika rozróżnia się zakłócenia **maskujące i imitujące** (rys. 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 zobrazenie celu w takim azy-mucie i odległości, gdzie nie ma celów rzeczywistych. Zakłócenia imitujące - stosowane przede wszystkim w radiolokacji, powodują na wskaźnikach powstawanie fałszywych zobrażeń znaków celów, analogicznych do znaków celów realnych. Zastosowanie tych zakłóceń dezorientuje przeciwnika oraz utrudnia podjęcie właściwych decyzji. Jako środki do wytwarzania imitujących za-

kłóceń pasywnych stosowane są odbijacze kątowe²⁴, odbijacze dipolowe²⁵, wszelkiego rodzaju pułapki i fałszywe cele radiolokacyjne.

Zakłócanie zagłuszające stanowi więc bardzo skuteczny sposób dezorganizacji pracy i działania różnorodnych środków oraz systemów elektronicznych wykorzystywanych w rozpoznaniu, dowodzeniu wojskami i kierowaniu uzbrojeniem przeciwnika. Ogranicza ono zakres i możliwości wykorzystania różnorodnych systemów przez poszczególne dowództwa i sztaby a ponadto, mimo że nie powoduje bezpośrednich materialnych zniszczeń, to jednak w wielu sytuacjach jest przyczyną po-

²⁴ 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.

²⁵ Odbijacze dipolowe, to najczęściej metalizowane włókna szklane, węglowe i poliamidowe lub metalizowana, odpowiednio cięta folia. Długość tych elementów z reguły odpowiada długości fali elektromagnetycznej ($1/2 \lambda$). 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 jasności, 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.

wstających u przeciwnika znacznych strat w sile żywej oraz w środkach walki.

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 przesyłaniu wiadomości i dokumentów 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 mogą docierać dane niepełne, odznaczające się niskim stopniem wiarygodności, a nawet dopływ danych może być na pewien okres czasu całkowicie 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 wy-

konanie 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.

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 działań zbrojnych 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

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 przeciwnika²⁶, których działanie opiera się na wykorzystaniu mikroelektroniki.

²⁶ Ta forma oddziaływania była dotychczas rozpatrywana w sytuacji użycia broni jądrowej, gdzie przy wybuchach część energii zamieniała się w impuls elektromagnetyczny.

Do niszczenia energią elektromagnetyczną służy całkiem nowy rodzaj broni. Jest to tzw. broń energetyczna EW²⁷ oraz specyficzna jej odmiana – wiązkowa broń energetyczna DEW²⁸. 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.

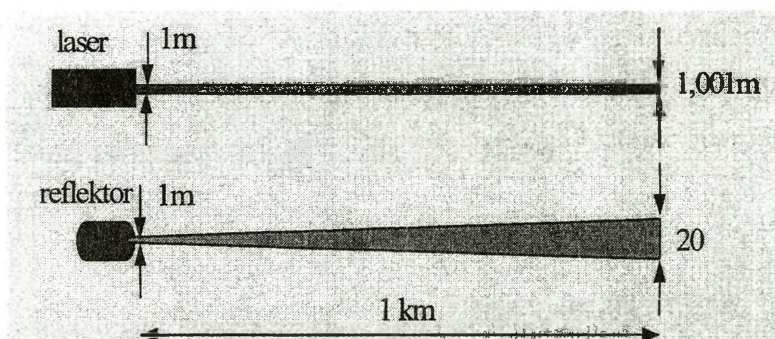
Wiązkowa broń energetyczna jest w stanie zniszczyć lub uszkodzić elementy uzbrojenia przeciwnika, bądź obezwładnić jego siłę żywą. Energia emitowana przez broń wiązkową rozprzestrzenia się z prędkością światła (~300 000 km/s), przy czym może być precyzyjnie dozowana i kierowana na atakowany obiekt. Inne 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 strumienia światła reflektora prze-

²⁷ ang. Energy Weapon.

²⁸ ang. Directed Energy Weapon.

ciwlotniczego o dużej zbieżności wiązki wynosi aż 2000%, czyli jest 20 razy większa. Porównanie rozbieżności ww. wiązek zilustrowano na rys. 1.4.

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



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

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 sił zbrojnych USA przewiduje się, że „co-

raz bardziej liczącym się sposobem prowadzenia działań zbrojnych są akcje militarne związane z użyciem skoncentrowanej energii broni elektromagnetycznej oraz bezpośrednio oddziaływanie na wyznaczone cele (zarówno obiekty, jak i otaczające je środowisko)". Na początku lat 90. wprowadzono do tych regulaminów poprawki dotyczące broni energetycznych innych niż elektromagnetyczne oraz broni o nie ukierunkowanej 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, a szczególnie systemów rozpoznawczo-uderzeniowych, dowodzenia wojskami i kierowania uzbrojeniem oraz systemów informatycznych sprawia, że są one szczególnie wrażliwe na działanie broni częstotliwości radiowych RFW²⁹. W zależności od parametrów broni, a szczególnie gęstości energii, poszczególne urządzenia a nawet całe systemy, mogą zostać zakłócone, uszkodzone bądź zniszczone.

²⁹ ang. Radio Frequency Weapons – broń DEW zakresu częstotliwości radiowych.

W zakresie częstotliwości radiowych urządzeniami zaliczanymi do broni wiązkowych są emiterzy (generatory) sygnałów radiowych wielkiej mocy HERF³⁰, a zwłaszcza mikrofalowe emiterzy impulsu elektromagnetycznego (HPM³¹). Emiterzy HPM wytwarzają w wąskim paśmie częstotliwości, krótkie (mikro lub nanosekundowe) impulsy energii elektromagnetycznej o mocy rzędu gigawatów. Ich odmianą są emiterzy LERF³² 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.

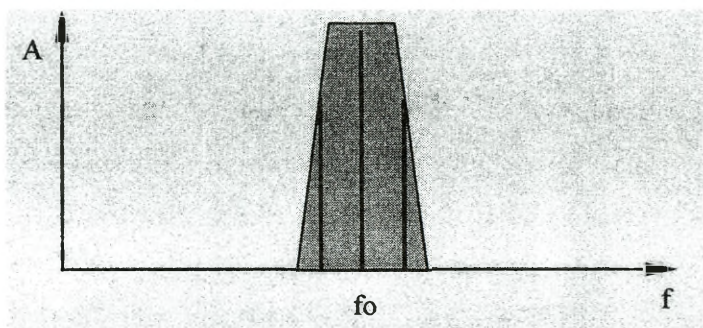
Mikrofalowe emiterzy HPM, najbardziej zaawansowane technicznie z tej grupy urządzeń, działają najskuteczniej, gdy ich częstotliwość emisji pokrywa się z częstotliwością pracy (f_0) obiektu ataku, bądź jego układów wewnętrznych (rys. 1.5).

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

³⁰ ang. High Energy Radio Frequency – sygnały radiowe wysokiej energii.

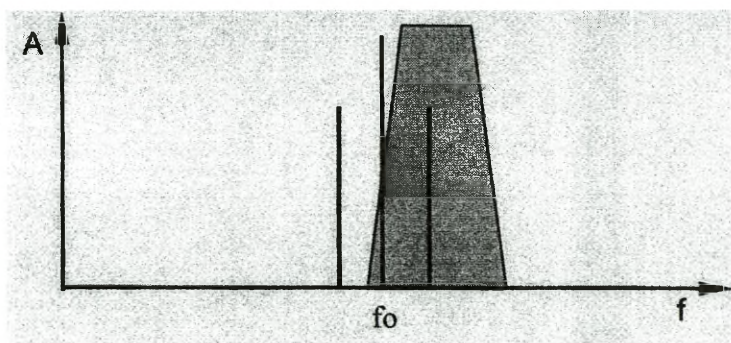
³¹ ang. High Power Microwave – emiterzy mikrofalowe wysokiej mocy.

³² ang. Large Energy Radio Frequency – sygnał radiowy wielkiej energii.



Rys. 1.5. Optymalna charakterystyka widmowa sygnału HPM

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



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

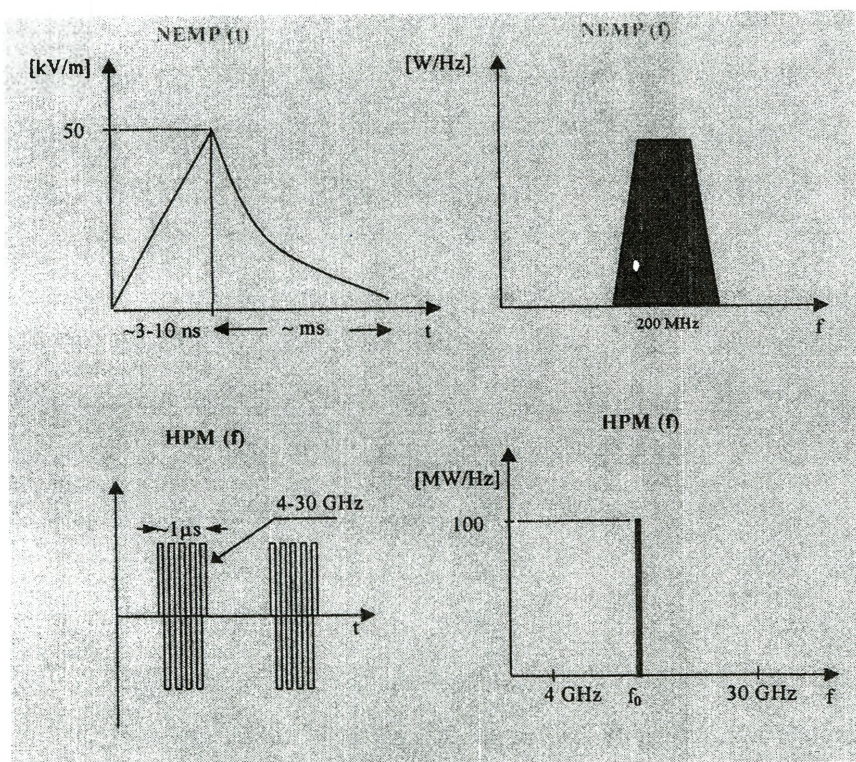
Emitery HPM charakteryzują się wysoką sprawnością energetyczną, są stosunkowo bezpieczne dla własnej elektroniki będącej poza strefą ich zasięgu, natomiast w strefie zasięgu, destrukcyjne oddziaływanie jest równie skutecznie w stosunku do elektroniki odbiorników jak i nadajników.

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 bezpilotowych, 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 NEMP³³. Jednak parametry czasowe i widmowe im-

³³ Ang. Nuclear Electromagnetic Microwave Pulse.

pulsu HPM zasadniczo różnią się od analogicznych parametrów impulsu elektromagnetycznego wybuchu jądowego NEMP co zostało przedstawione na rys. 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. W szczycie impulsu składowa elektryczna pola może osiągnąć wartość ok. 50 kV/m. Sygnał HPM natomiast 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 a nawet terawatów.

W zakresie częstotliwości sygnał NEMP ma widmo ciągle 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.

Tabela 1.1

**DROGI WNIKANIA
I SPOSÓB ODDZIAŁYWANIA SYGNAŁU HPM**

Obiekt rażenia	Drogi wnikania	Skutki oddziaływania
Obiekty łączności i informa- tyki	– 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/cm²) lub przejściowa (do 100 mJ/cm²); – uszkodzenia spowodowane silnym nagrzewaniem elementów metalowych w protezach (np. amalgamato- we plomby).

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

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

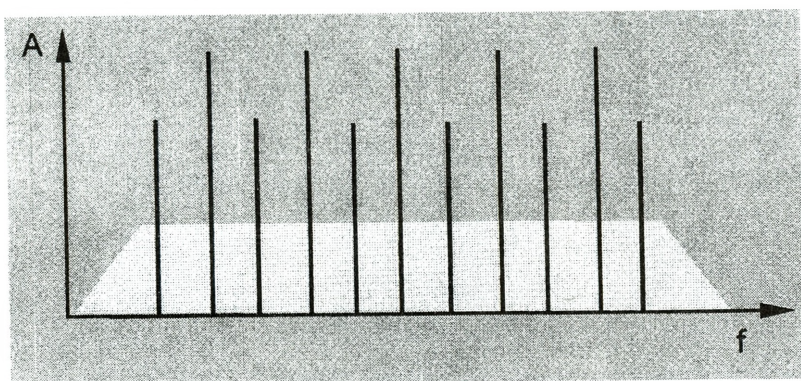
W zależności od mocy i częstotliwości powtarzania impulsu, urządzenia HPM mogą być montowane na pojazdach, samolotach, w rakietach i pociskach. Mogą być także wykonane w wersji przenośnej w postaci walizki.

Szczegóły techniczne rozwiązań takich urządzeń nie są publikowane. Wiadomo jedynie, że w ostatnich latach są prowadzone intensywne badania nad doskonaleniem technologii generacji impulsu.

Emitery typu UWB³⁴ stanowią drugą grupę urządzeń, które promieniują energię w postaci sygnałów, jednak rozproszonych w wielokrotnie szerszym paśmie częstotliwości i znacznie mniejszej gęstości mocy (rys. 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.

³⁴ 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 EMP³⁵.

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 raketowych, torped i innych ro-

³⁵ EMP – ang. Electro-Magnetic Pulse – impuls elektromagnetyczny.

dzajów amunicji wyposażonej w sztuczną inteligencję. Można je również wykorzystać do zdalnego detonowania sterowanych radiowo pól minowych. Emitery UWB mogą być instalowane w pociskach raketowych i artylerii lufowej, bombach lotniczych, a nawet jako amunicja granatników ręcznych³⁶.

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 super-środka zakłócającego. Informacje napływające o badaniach tego zjawiska wykazują, że środkami tymi może być porażona aparatura elektroniczna na znacznym obszarze oraz urządzenia wykonane w technologii trudno wykrywalnej ang. „stealth”.

Broń laserowa. Lasery³⁷ tworzą oddzielną grupę środków wiązkowej broni energetycznej. Od innych promienników energii elektromagnetycznej wyróżniają je następujące cechy:

³⁶ W 1994 roku Rosjanie ujawnili, że dysponują technologią do produkcji całej rodziny kompaktowej amunicji elektromagnetycznej RFM, w której wykorzystuje się eksplozję ładunków konwencjonalnych do generowania energii elektromagnetycznej. Jako „tradycyjne” źródła zasilania emiterów wykorzystywane są generatory (akceleratorzy) homopolarne, BWO, MHD, MILO, RKO i inne.

³⁷ LASER – skrót od angielskich słów: Light Amplification by Stimulated Emission of Radiation – wzmacniacz światła z wymuszoną emisją promieniowania.

- 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). 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 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 ablacji³⁸, zachodzące w wypadku uderzenia promienia laserowego w atakowaną powierzchnię oraz tworzenie fali uderzeniowej i powstawanie odłamków z materiału pancerza. Plasma może zatem uszkodzić czujniki, układy kontrolno – pomiarowe, obserwacyjne itp.

³⁸ Ablacja – stopniowe niszczenie, kruszenie, zachodzące w wypadku uderzenia promienia laserowego w atakowaną powierzchnię oraz tworzenie fali uderzeniowej i powstawanie odłamków z materiału pancerza.

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 PBW³⁹. Prowadzone są prace nad bronią wiązkową, która działa na zasadzie akceleracji cząstek elementarnych. Badania dotyczą dwóch rodzajów emiterów: CBP⁴⁰ – emitujących strumień cząstek posiadających ładunek elektryczny (np. strumień elektronów lub protonów) i NPB⁴¹ – emitujących cząstki elementarne bez ładunku (atomy wodoru, strumień neutronów). Energia strumienia neutronów z emitera NBP jest znacznie większa od strumienia (np. elektronów) z emi-

³⁹ PBW – ang. Particle Beam Weapon – broń cząstek elementarnych.

⁴⁰ CPB – ang. Charged Particle Beam – strumień cząstek elementarnych z ładunkiem elektrycznym.

⁴¹ NPB – ang. Neutral Particle Beam – strumień neutralnych cząstek elementarnych.

tera 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.

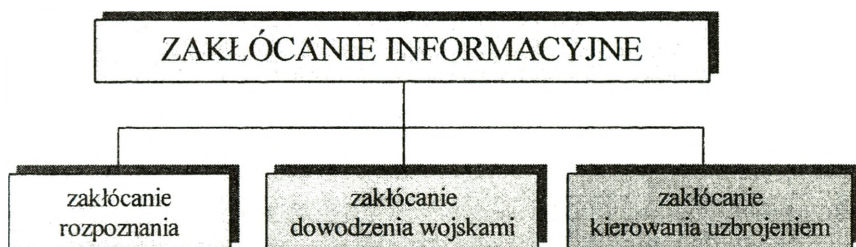
Promienniki kierunkowe, w odróżnieniu od równokierunkowych, są dodatkowo wyposażone w urządzenia ukierunkowujące strumień promieniowania. Pod względem konstrukcyjnym różnią się też umiejscowieniem ładunku wybuchowego. Charakteryzują się one większą sprawnością i mniejszym prawdopodobieństwem przypadkowego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

Dotychczasowe doświadczenia⁴² 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.

1.3. Podział zakłócania informacyjnego

Zakłócanie informacyjne ze względu na swój zakres oddziaływania odzwierciedla zespół skoordynowanych elementów ukierunkowanych na dezorganizację procesów rozpoznawczych przeciwnika oraz zakłócanie jego procesów dowodzenia wojskami i kierowania uzbrojeniem. W świetle powyższego, podstawowy podział zakłócania informacyjnego można przedstawić jak na rys. 1.9.

⁴² Prowadzone są badania nad tą bronią, m.in.: w Stanach Zjednoczonych, Rosji i Chinach.



Rys. 1.9. Podstawowy podział zakłócania informacyjnego

Elementy zakłócania informacyjnego zostały wyróżnione więc w aspekcie osiągnięcia konkretnych celów oddziaływania, tj. paraliżowania elementów rozpoznawczych przeciwnika, dezorganizacji pracy szeroko rozumianych systemów dowodzenia wojskami i kierowania uzbrojeniem. Zostały one uczynione przedmiotem rozważań w kolejnych rozdziałach opracowania.

2. ZAKRES I TREŚĆ PRZEDSIĘWZIĘĆ ZAKŁÓCANIA ROZPOZNANIA PRZECIWNIKA

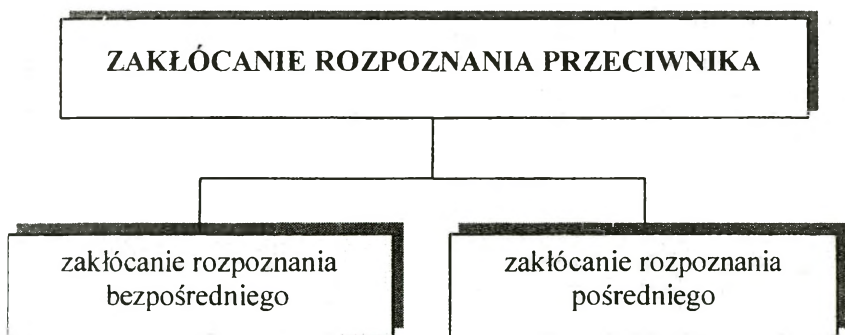
Zakłócanie rozpoznania tworzy zespół skoordynowanych elementów dostosowany do wnoszenia entropii do zbiorów wszelkich postaci informacji, które mogą być dostępne dla źródeł rozpoznania przeciwnika. Przedsięwzięcia z tym związane należy realizować kompleksowo, według jednolitej koncepcji ściśle zsynchronizowanej z rzeczywistym planem operacji (walki) oraz z pozornym działaniem wojsk i ich maskowaniem. Paleta podejmowanych w tym zakresie wysiłków, powinna być spójna i precyzyjnie dobierana. Generalnym celem jest stworzenie przeciwnikowi fałszywego obrazu rzeczywistości po drugiej stronie toczących się zmagających. Ów cel odzwierciedlają słowa⁴³ „...*jest to niezmierznie złożony proces kierowania działaniami przeciwnika przez podmiot mu przeciwny i w nieznanym mu sposób*”. Zatem, zakłócanie rozpoznania jest elementem walki informacyjnej pro-

⁴³ L. Ciborowski, „Walka informacyjna”, wyd. ECE, Toruń 1999, s. 78.

wadzonej z myślą o pośrednim kierowaniu działaniami przeciwnika w taki sposób, aby był tego nieświadomy.

Zakłócanie rozpoznania należy prowadzić wielokierunkowo, we wszystkich wymiarach pola walki, w odniesieniu do wszystkich elementów, przy pomocy których przeciwnik pozyskuje dane rozpoznawcze. Jego istotą powinno być wnoszenie entropii informacyjnej do zbiorów danych rozpoznawczych przeciwnika.

W aspekcie powyższego, podstawową strukturę zakłócania rozpoznania można przedstawić jak na rys. 2.1.



Rys. 2.1. Podstawowa struktura zakłócania rozpoznania

W trakcie zakłócania rozpoznania można więc 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 to ową problematykę określa się jako rozpoznanie bezpośrednie.

Rozpoznanie bezpośrednie⁴⁴ powszechnie uważane jest za jeden z najstarszych rodzajów zdobywania danych o stronie przeciwnej, w którym najważniejszą rolę spełnia człowiek utożsamiany najczęściej ze zwiadowcą i jego zmysłami. Owe zmysły, często wspomagane przez odpowiednie urządzenia techniczne, odbierają sygnały w formie bezpośrednio dla niego zrozumiałej. Mogą to być sygnały wzrokowe zawarte w paśmie promieniowania widzialnego⁴⁵, słuchowe zawarte w paśmie drgań akustycznych⁴⁶,

⁴⁴ 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.

⁴⁵ Promieniowanie widzialne (światłne) – 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.

⁴⁶ 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.

jak również bodźce dotykowe⁴⁷, smakowe⁴⁸ i zapachowe rejestrowane przez zmysł powonienia⁴⁹. Przewiduje się stosowanie urządzeń wspomagających zasięg rozpoznania i czułość zmysłów, jednak bez przetwarzania wymienionych bodźców. Dlatego też, **zakłócanie rozpoznania bezpośredniego powinno uniemożliwiać bądź utrudniać przeciwnikowi dostęp do wszelkich postaci informacji, które są lub mogą być dostępne dla poznania zmysłowego przeciwnika realizującego proces zdobywania danych o naszych wojskach, obszarze ich działania, zamiarach itp.**

Z kolei **zakłócanie rozpoznania pośredniego**⁵⁰, realizowane jest za pomocą urządzeń przystosowanych do oddziaływania na systemy zdobywania danych w postaci bezpośrednio nieodbywalnych przez układ recepcyjny człowieka.

⁴⁷ 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.

⁴⁸ Smak – zmysł zdolny do odróżniania pewnych właściwości chemicznych, którego narządy znajdują się głównie na języku i w ustach. Tamże, tom III, s. 263.

⁴⁹ Powonienie – zmysł węchu, umożliwia odczuwanie zapachu, woni, odoru, itp. Tamże, tom II, s. 873.

⁵⁰ Rozpoznanie pośrednie tworzy zespół skoordynowanych źródeł rozpoznania dostosowanych do zdobywania danych przetwarzanych przez specjalne urządzenia w postaci zrozumiałą dla prowadzącego rozpoznanie. Pomiedzy zbiorem możliwych danych o rzeczy lub zjawisku a prowadzącym rozpoznanie występują przetworniki.

W tym przypadku pomiędzy zbiorem możliwych postaci danych a prowadzącym rozpoznanie, występują urządzenia przekształcające pierwotne sygnały w postać odbieralną przez jego układ recepcyjny. Będą to przede wszystkim urządzenia rozpoznania elektronicznego i zbiory danych do prowadzenia rozpoznania studyjnego.

Zakłócanie jednych i drugich, czyli całej struktury rozpoznania pośredniego przeciwnika, przynosi pożądane efekty i jest jednym z ważniejszych elementów, który należy uwzględniać w walce zbrojnej. Jednak do prowadzenia szczegółowych rozważań na temat zakłócania, niezbędny jest dalszy podział owej struktury.

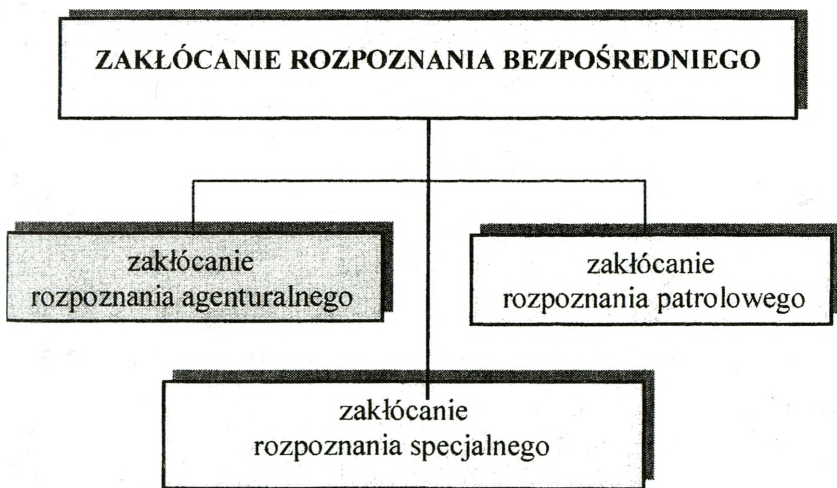
2.1. Zakłócania rozpoznania bezpośredniego

Z wcześniejszych rozważań wynika, że podczas zakłócania rozpoznania bezpośredniego oddziałuje się 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 on rolę obserwatora. Dlatego też wszystkie przedsięwzięcia zakłócania roz-

poznania bezpośredniego, są skierowane przeciwko niemu. W zakłócaniu rozpoznania bezpośredniego można więc wyróżnić:

- układ skoordynowanych elementów dostosowany do zakłócania rozpoznania agenturalnego;
- układ skoordynowanych elementów dostosowany do zakłócania rozpoznania specjalnego;
- układ skoordynowanych elementów dostosowany do zakłócania rozpoznania patrolowego.

Owe komponenty rozpoznania bezpośredniego zwanego też osobowym tworzą jego strukturę, którą ilustruje rys. 2.2.



Rys. 2.2. Podstawowa struktura zakłócania rozpoznania bezpośredniego (osobowego)

2.1.1. Zakłócanie rozpoznania agenturalnego

Zakłócanie rozpoznania agenturalnego⁵¹ 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 w V w.p.n.e chiński filozof, wędrowny doradca dworski 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*

⁵¹ 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.

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”⁵².

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 oraz prowadzenie zakłócania agenturalnego powierza się ekspertom ze służb kontrwywiadowczych. Ze względu na złożoność i niejawny charakter tej problematyki, nie będzie ona szerzej przedstawiona w niniejszym opracowaniu.

2.1.2. Zakłócanie rozpoznania patrolowego

Zakłócanie rozpoznania patrolowego⁵³, polega na uniemożliwieniu bądź utrudnieniu realizacji zadań takich jak: wykrycie i obserwacja przeciwnika, rozpoznanie jego sił i charakteru dzia-

⁵² Sun Tsu, „Sztuka wojny”, wyd. Przedświt, Warszawa 1994, s. 40 i 46.

⁵³ 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.

łań, 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: chwywanie jeńców, zdobywanie dokumentów, wzorów nowego uzbrojenia i sprzętu bojowego przeciwnika itp.

Analiza metod pozyskiwania informacji przez zwiadowców rozpoznania patrolowego i specjalnego, umożliwia wyróżnienie wielu 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 pododdziały 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;

– rejonny ześrodkowania wojsk oraz kierunki ich przegrupowania;

– lotniska, lądowiska, porty i bazy morskie, obiekty obrony wybrzeża;

– 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 (walki), 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. Należy uniemożliwić 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 patrolowego oraz

specjalnego 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 kogoś⁵⁴. Jednym z najstarszych i najbardziej znanych przykładów użycia podstępu, jest słynna opowieść o koniu trojańskim, który umożliwił Grekom zdobycie Troi, po dziesięcioletnim bezskutecznym jej oblężeniu⁵⁵.

Wprowadzenie w błąd jest jedną z częściej stosowanych metod stosowaną między innymi w działaniach zbrojnych. 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;
- 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.

⁵⁴ Słownik języka polskiego, wyd. PWN, Warszawa 1992, tom II, s. 750.

⁵⁵ Zburzenie Ilionu Leschesa z Pyrry, wyd. Wiedza Powszechna, Warszawa, 1985, s. 82.

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 na Sycylii nie napotykając prawie na żaden opór.

Przedsięwzięcia związane z propagandą należy powierzyć ekspertom od propagandy.

Biała propaganda⁵⁶ stanowi element aktywnego zakłócania, oceniany jednak jako mało skuteczny, ponieważ informacje pochodzące z oficjalnych źródeł przeciwnika, siłą rzeczy mają ograniczoną wiarygodność.

⁵⁶ 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.

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 Stefan Delmer. Finezyjne i wyrafinowane akcje propagandowe – jak to oceniono po wojnie w Niemczech Zachodnich – były wynikiem nie tylko inteligencji i uzdolnień Delmera, lecz także „jego psychicznego refleksu nabytego w czasie wieloletniej konfrontacji z Niemcami”⁵⁷.

Wpływanie⁵⁸ jest jedną z form prowadzenia 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

⁵⁷ W. Kozaczuk, „Wojna w eterze”, wyd. RiTV Warszawa, 1977, s.111.

⁵⁸ Wpływanie – nacisk, oddziaływanie na kogoś lub na coś. Słownik współczesnego języka polskiego, wyd. Wilga, Warszawa 1996, s. 1245.

działań buntować młodych przeciw starym, aby wykopać przepaść między pokoleniami.

Dezinformowanie jako jedno z przedsięwzięć aktywnego zakłócania, jest zbieżne z wprowadzaniem 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 przeciwnika, pożądanych poglądów czy zachowań.

W działaniach zbrojnych przedsięwzięcia dezinformowania 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 działań (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 zdema-

skowane, a jeśli nawet nie, to i tak przynosiło rezultaty odwrotne do zamierzonych. Potwierdzeniem tej tezy może być następujący przykład. 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 przedsię-

wzięciami, 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.

Dlatego też przedsięwzięcia realizowane w tym zakresie, powinny być odpowiednio scentralizowane, kompleksowe, spójne, wiarygodne, nieszablonowe, skryte, terminowe, ciągłe i elastyczne.

2.1.3. Zakłócanie rozpoznania specjalnego

Rozpoznanie specjalne jest specyficznym rodzajem rozpoznania⁵⁹. Owa specyfika polega głównie na prowadzeniu samodzielnych działań przez kilkusobowe 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.

⁵⁹ Rozpoznanie specjalne realizowane w ramach działań specjalnych, obejmuje zdobywanie dokładnych, terminowych i wiarygodnych danych (informacji) o przeciwniku i obszarze działań siłami grup specjalnych, rozmieszczonych w głębi ugrupowania i na zapleczu przeciwnika służących „do planowania operacji i sterowania środkami rażenia.

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

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 zbrojnych, powinny podlegać szczególnej ochronie i obronie.

Proces zakłócania rozpoznania specjalnego powinien więc rozpocząć się od zwalczania grup specjalnych w trakcie przerzutu, następnie uniemożliwiać bądź utrudniać prowadzenie rozpoznania oraz paraliżować wszelkie przejawy ich działalności dywersyjnej, sabotażowej, terrorystycznej i propagandowej. Do realizacji tych przedsięwzięć należy wyznaczyć zarówno określone siły wojsk operacyjnych jak i układu pozamilitarnego. Formy zakłócania rozpoznania specjalnego są – jak podkreślono wcześniej – zbieżne z formami zakłócania rozpoznania patrolowego.

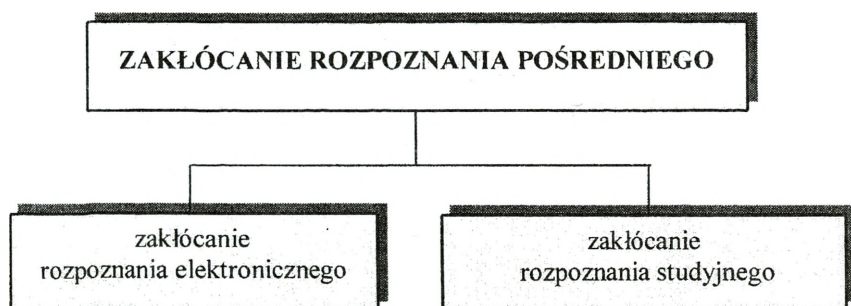
2.2. Zakłócanie rozpoznania pośredniego

Zakłócanie rozpoznania pośredniego obejmuje wszelkie środki rozpoznania przeciwnika, przystosowane do zdobywania danych w postaci bezpośrednio nieodbieralnej 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, oddziałuje się na ową techniczną strukturę systemów i środków przeciwnika.

W aspekcie powyższego, podstawową strukturę zakłócania rozpoznania pośredniego można przedstawić tak jak na rys. 2.3.

Analiza struktury zakłócania rozpoznania pośredniego przeciwnika wykazuje, że może być ono prowadzone różnymi sposobami i przy wykorzystywaniu różnych narzędzi. Działania w tym zakresie determinowane są dążeniem do osiągnięcia stanu, który nie pozwoli na dostarczenie elementom rozpoznawczym przeciwnika wiernego i aktualnego obrazu pola walki oraz prawdopodob-

nych przyszłych zachowań naszych wojsk. Kryterium to najbardziej spełniają systemy oraz wchodzące w ich skład urządzenia rozpoznania elektronicznego.



Rys. 2.3. Podstawowa struktura zakłócania rozpoznania pośredniego

2.2.1. Zakłócanie rozpoznania elektronicznego

Zakłócanie rozpoznania elektronicznego⁶⁰, ze względu na dużą jego różnorodność powinno obejmować:

- zakłócanie rozpoznania radioelektronicznego;
- zakłócanie rozpoznania radiolokacyjnego;

⁶⁰ 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.

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

W ramach zakłócania rozpoznania elektronicznego należy ograniczyć do niezbędnego minimum dostępność własnych środków i urządzeń elektronicznych w strefach i w sektorach niepożądanych, tzn. poza przednim skrajem 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 należy warunkować okresami: pokoju, kryzysu i wojny.

W okresie pokoju i kryzysu zakłócanie rozpoznania elektronicznego powinno polegać na przestrzeganiu zasad wykorzystania urządzeń elektronicznych określonych instrukcjami eksploatacyjnymi oraz przepisami o ochronie informacji niejawnych⁶¹. Szczególna uwaga powinna być zwrócona na maskowanie wojsk

⁶¹ „Ustawa o ochronie informacji niejawnych” z dnia 22.01.2000. DzU, nr 11, poz. 95.

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 elementy rozpoznania pośredniego, tj. na zdobywanie danych realizowana jest z zamiarem uniemożliwiania przeciwnikowi wykorzystywania tych postaci danych, do których udało się mu zdobyć dostęp mimo stosowania obrony informacyjnej. Wykorzystując różne środki zakłócania elektronicznego 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 znacznie 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 rozpoznania elektronicznego, najbardziej różnicowane pod względem technicznym, jest zakłócanie elementów rozpoznania radioelektronicznego.

2.2.1.1. 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 środki zakłócania, można niszczyć lub czasowo uniemożliwiać pracę środkom rozpoznania radioelektronicznego, 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 (naszych wojskach), to znaczy, zwiększa u niego entropię informacyjną. Powyższy proces zakłócania należy prowadzić za pomocą urządzeń, zainstalowanych na pojazdach i aparatach latających.

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

- rozpoznania radiowego, radioliniowego i satelitarnego;
- rozpoznania systemów radiolokacyjnych;
- rozpoznania systemów radionawigacyjnych.

Zakłócanie rozpoznania radiowego jest procesem, który uniemożliwia bądź utrudnia przeciwnikowi zdobywanie danych o stanie ilościowym i jakościowym środków łączności radiowej, radioliniowej i satelitarnej naszych wojsk, miejscu ich rozmieszczenia a także sposobach wykorzystania.

Przyjmując za kryterium zakres częstotliwości, możemy wyróżnić zakłócanie rozpoznania łączności radiowej krótkofalowej⁶² (KF) i ultrakrótkofalowej⁶³ (UKF), jednak ze względu na

⁶² Fale krótkie: $f = 3 \cdot 10^6 - 3 \cdot 10^7$ Hz; $\lambda = 10 - 10^2$ m.

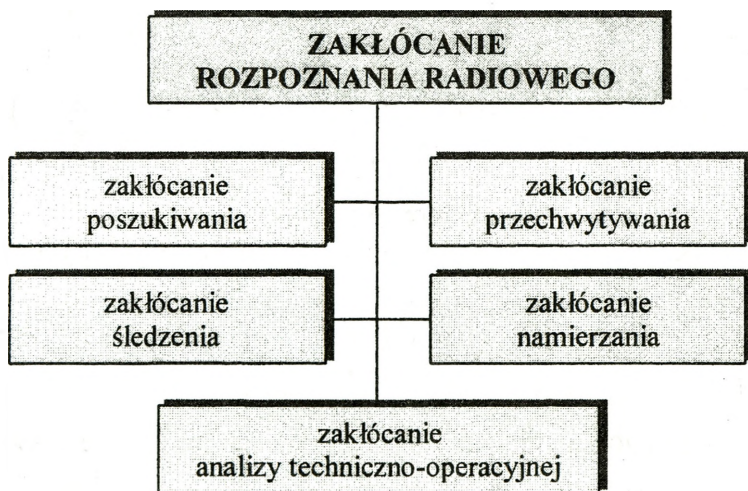
⁶³ Fale ultrakrótkie: $f = 3 \cdot 10^7 - 3 \cdot 10^8$ Hz; $\lambda = 1 - 10$ m.

wprowadzanie do wojsk szerokopasmowych urządzeń radioodbiornych, 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.

Z powyższego wynika, że poszczególne metody zdobywania danych rozpoznawczych powinny być objęte procesem zakłócania, co zilustrowano na rys. 2.4.



Rys. 2.4. Procesy w rozpoznaniu radiowym podlegające zakłócaniu

Zakłócanie poszukiwania jest podstawowym procesem, który ma na celu utrudnienie wykrycia i identyfikacji sygnałów wypromieniowanych przez środki radiowe i wyselekcjonowanie tych, którymi prowadzący rozpoznawanie 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 $P_{z_{we}}$ na wejściu urządzenia rozpoznawczego musi być nie mniejsza od mocy sygnału użytecznego $P_{s_{we}}$:

$$P_{z_{we}} \geq P_{s_{we}}$$

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

$$f_0 - \frac{\Delta f}{2} \leq f_z \leq f_0 + \frac{\Delta f}{2}$$

gdzie:

f_0 – częstotliwość pracy odbiornika urządzenia rozpoznawczego;

Δf – szerokość pasma przepuszczania odbiornika;

f_z – 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 zamierza się 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. ze skokową zmianą częstotliwości typu FH⁶⁴. Nowoczesne urządzenia zakłócające, są w stanie generować sygnały w paśmie 12 MHz, pokrywając cały podzakres tzw. hoppingu przy modulacji typu FH (± 6 MHz). Te nowoczesne urządzenia zakłócające, są najczęściej 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

⁶⁴ ang. Frequency Hopping.

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.

Zakłócanie namierzania⁶⁵ 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.

⁶⁵ Namierzanie źródła sygnału, jest kolejnym istotnym elementem procesu rozpoznania radioelektronicznego.

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 zarówno sygnałów jak i obiektów prawdopodobnie znanych przeciwnikowi oraz 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 doty-

czyć przede wszystkim składu, rozmieszczenia, stanu ilościowo-jakościowego obiektów oraz sposobów działania czy zamiarów ich użytkowników.

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

Zakłócanie rozpoznania łączności radioliniowej⁶⁶, 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 aparatuwniach poruszają-

⁶⁶ 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.

cych się po drogach rokadowych poszukując sygnałów, bądź na statkach powietrznych (pilotowych i bezpilotowych) 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”).

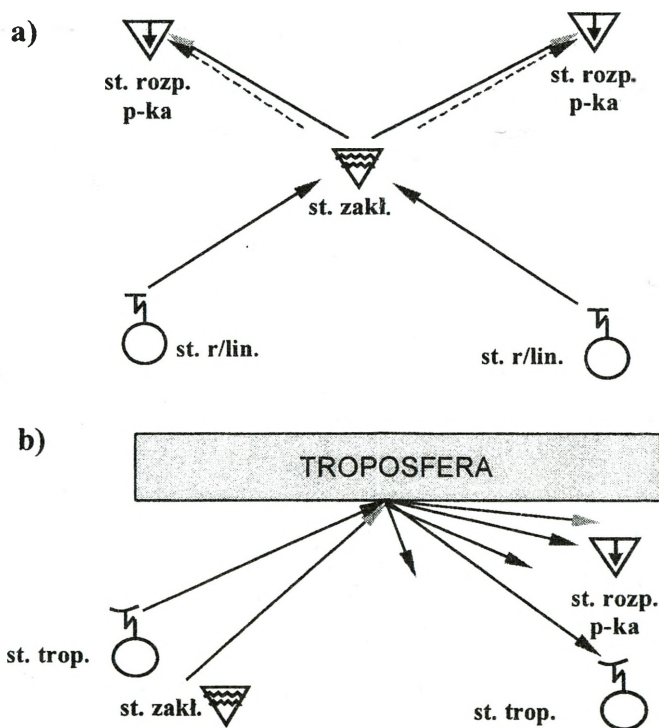
W przypadku stacji zakłóceń rozpoznania łączności pozahoryzontowej, przy której wykorzystuje się rozproszenie wiązki na niejednorodnościach troposfery (stąd potoczna nazywa radiolinie troposferyczne), nie jest wymagany warunek widoczności, bowiem anteny urządzenia rozpoznawczego i stacji zakłóceń, mogą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

Ideę zakłócania urządzeń rozpoznania radioliniowego łączności horyzontowej i pozahoryzontowej ilustruje rys. 2.5.

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

Zakłócanie rozpoznania łączności satelitarnej jest przedsięwzięciem perspektywicznym. Należy mieć na uwadze, że 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.



Rys. 2.5. Zakłócanie urządzeń rozpoznania łączności radioliniowej:
a) horyzontowej, b) pozahoryzontowej

Polega na wykrywaniu sygnałów przekazywanych z satelity, ich przechwytywaniu i analizowaniu. Problematyka zakłócania urządzeń przeznaczonych do rozpoznania łączności satelitarnej powinna polegać na dezorganizacji tych procesów metodami i sposobami przedstawionymi powyżej.

Zakłócanie rozpoznania systemów radiolokacyjnych⁶⁷

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 (bojowego) takie jak: zgrupowania 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

⁶⁷ 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 oraz radiolokacyjnego zabezpieczenia działań wojsk.

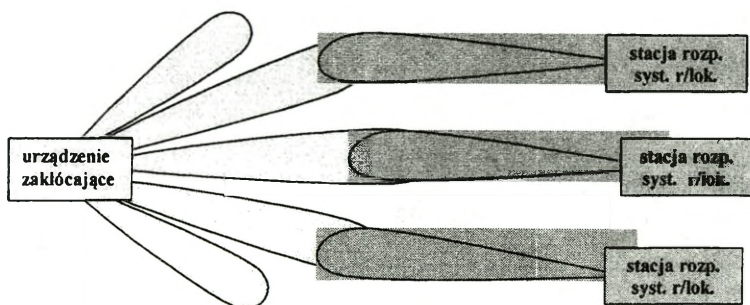
elektromagnetycznej. W tych systemach, aktywne są jedynie ich urządzenia sterujące i wymiany danych, których należy poszukiwać. Aby więc wykryć pracujący system rozpoznania radiolokacyjnego, muszą być spełnione podobne warunki jak w przypadku poszukiwania środków radiowych, tzn. energetyczny, częstotliwościowy, przestrzenny oraz czasowy, które zostały omówione w podrozdziale dotyczącym zakłócania rozpoznania radiowego. Zakłóceniami można więc objąć te stacje rozpoznania radiolokacyjnego, których aktywne systemy sterowania i wymiany danych zostały wykryte.

Rozwiązaniem problemu zakłócania systemów rozpoznania radiolokacyjnego, może być kierunkowe (sektorowe) lub dookólne zakłócanie całych pasm radiolokacyjnych.

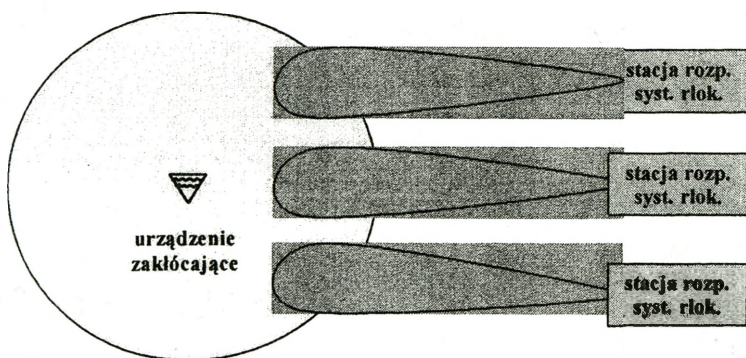
Kierunkowe zakłócanie stacji rozpoznania radiolokacyjnego może być prowadzone metodą z uprzednim poszukiwaniem zakłócanych stacji, lub metodą bez ich poszukiwania, odbywa się wówczas tzw. zakłócanie natychmiastowe.

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 rys. 2.6, metodę drugą rys. 2.7.



Rys. 2.6. Zakłócanie metodą wielosektorową



Rys. 2.7. Zakłócanie metodą dookólną

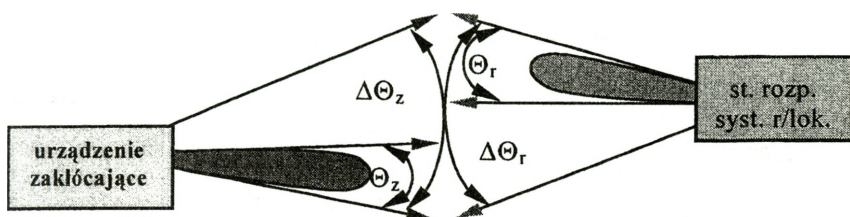
Do zakłócania wielosektorowego wykorzystuje się kilka anten kierunkowych lub jedną antenę z tzw. szykiem fazowym.

W antenach tego typu, są wykorzystywane dyskryminatory fazy, które pozwalają na szybkie i precyzyjne zmiany charakterystyki anteny. Ta technika umożliwia emisję dowolnego kształtu wiązki sygnału zakłócającego, w dowolnym kierunku lub sektorze.

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 rys. 2.8.

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



gdzie:

- $\Delta\Theta_z$ – sektor zakłócania;
- $\Delta\Theta_r$ – sektor obserwacji stacji rozpoznania radiolokacyjnego;
- st. rozp. syst. r/lok. – stacja rozpoznania radiolokacyjnego.

Rys.2.8. Ilustracja warunku „zazębiania się” sektorów urządzenia zakłócającego i stacji rozpoznania radiolokacyjnego

Dodatkową trudność w zakłócaniu namierzania stacji z obrotującymi 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 unie możliwiać 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 wypromieniowane 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 przeciwwzakłóceńowych;
- 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 radionawigacyjnego⁶⁸ 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.

⁶⁸ 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.

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

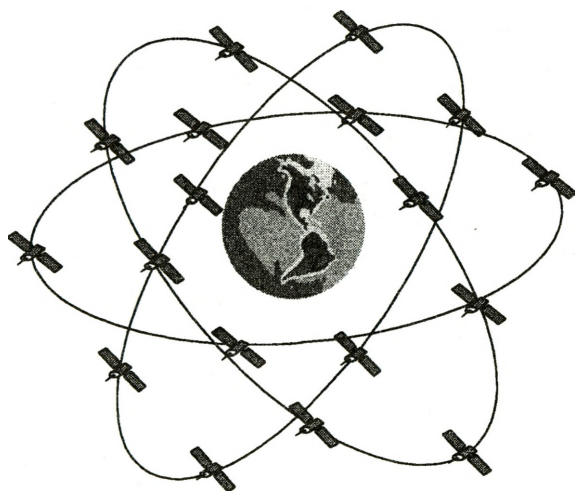
Zakłócanie systemów rozpoznania bliskiej nawigacji powinny obejmować środki rozpoznania radiotechnicznego, rozmieszczone na lądzie (aparatach latających, okrętach), których zasięg ograniczony jest do kilkuset kilometrów. Wykorzystywane podzakresy częstotliwości to fale krótkie i ultrakrótkie, które zapewniają 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 (rys. 2.9.), która mimo znacznej odległości od satelitów (około 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.



Rys. 2.9. Wykorzystanie w radionawigacji sztucznych satelitów Ziemi

2.2.1.2. 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 określe-

nie RADAR od słów *Radio Aids for Defence And Reconnaissance* (radiowe pomoce dla obrony i rozpoznania). Amerykanie etymologię słowa RADAR zaś 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 radiolokacyjnymi⁶⁹, 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 rozprzestrzenia się prostoliniowo i ze stałą prędkością w środowisku jednorodnym, możliwe jest określanie współrzędnych rozpoznawanych obiektów, pomiar ich parametrów ruchu lub wielkości bryłowej.

⁶⁹ W wojskach radiotechnicznych przedmioty wykryte przez stacje radiolokacyjne nazywane są obiektami. Obiekty niezidentyfikowane lub obce (nieprzyjacielskie) nazywa się celami.

Rozpoznanie radiolokacyjne jest prowadzone przez służby wojskowe i cywilne, które kontrolują przede wszystkim przestrzeń powietrzną, ale także obszar lądowy i morski, zarówno w czasie pokoju, konfliktu jak i wojny. Z tego względu, zakłócanie rozpoznania radiolokacyjnego powinno obejmować wszystkie rodzaje wojsk i służb, w których wykorzystywane są systemy i środki radiolokacyjne i obejmować:

- systemy rozpoznania obszaru powietrznego;
- systemy nadzorowania pola walki;
- systemy kierowania ogniem;
- systemy obrony przeciwlotniczej;
- systemy rozpoznania powierzchni ziemi SLAR⁷⁰ 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 szczególnie 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.

⁷⁰ SLAR – ang. Side-Looking Airborne Radar.

Uzyskanie wymaganej głębokości, zależy przede wszystkim od technicznych możliwości stacji zakłóceń oraz ich właściwego rozmieszczenia w terenie, stosownie do położenia zakłócających 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.

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 raketowych. Zakłócenia powinny również obejmować lotnicze stacje radiolokacyjne wykorzystywane do nawigacji, określania wysokości lotu lub identyfikacji „swoj – obcy”.

Zakłócanie powietrznego rozpoznania radiolokacyjnego powinno obejmować swoim zasięgiem środki napadu 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 oraz obejmować swym zasięgiem obiekty na dowolnej wysokości.

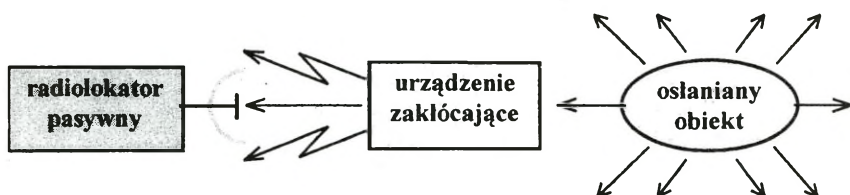
Zakłócanie morskiego rozpoznania radiolokacyjnego, powinno być prowadzone przez wojska w przypadku, gdy obszar operacji (walki) obejmuje pas przybrzeżny. Ich zadania, powinny być przede wszystkim związane z radiolokacyjną osłoną obiektów wzdłuż wybrzeża morskiego i zakłócaniem rozpoznania warunków hydrometeorologicznych 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 można 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 (rys. 2.10):



Rys. 2.10. Idea zakłócania radiolokacji pasywnej

- promieniowanie termiczne obiektów o temperaturze wyższej od zera bezwzględnego /absolutnego/ ($0\text{K} = -273,15^{\circ}\text{C}$);
- 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.

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 pasywną 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 trójwymiarowe), jego kształcie i wymiarach a także parametrach ruchu (prędkości).

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

$$R = c \cdot t$$

gdzie:

R – odległość stacji radiolokacyjnej od nadajnika zakłócającego w km;

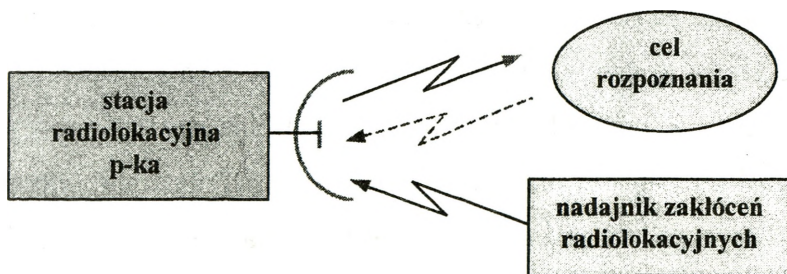
c – szybkość rozprzestrzeniania się fal elektromagnetycznych $c \approx 300$ tys. km/s;

t – czas na pokonanie odległości przez sygnał w sekundach.

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

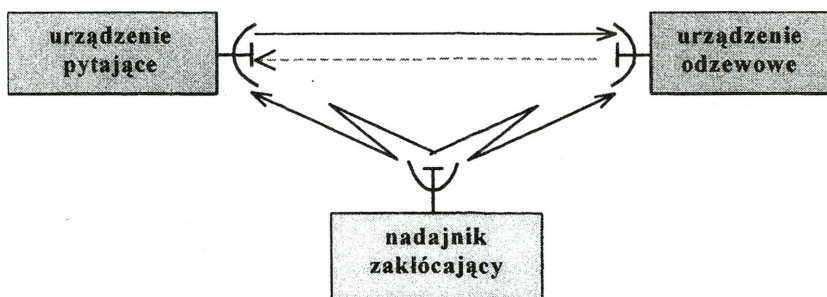
Pomiar ruchu i szybkości zakłócanej stacji umożliwia zjawisko Dopplera, polegające na zmianie częstotliwości sygnału ruchomego celu. Uzyskanie pozostałych danych umożliwia analiza przechwyconych sygnałów radiolokacyjnych. Ideę zakłócania radiolokacji aktywnej z pasywną odpowiedzią ilustruje rys. 2.11.

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



Rys. 2.11. 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 rys. 2.12.

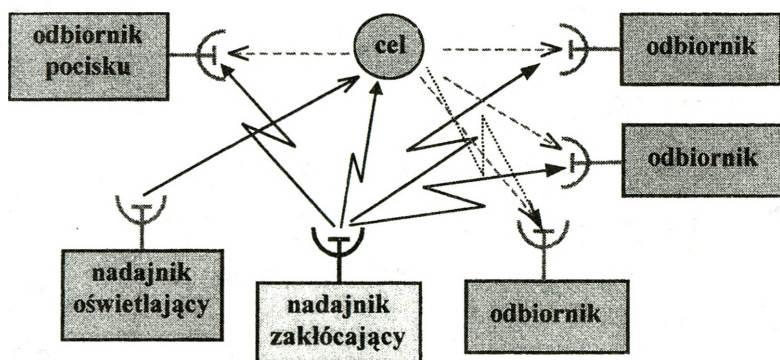


Rys. 2.12. Zakłócanie radiolokacji z aktywną odpowiedzią

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 określają 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 multistatyczna⁷¹). Tego rodzaju urządzenia wykorzystywane są do specjalnych zastosowań jak np. dla ułatwienia naprowadzania pocisków kierowanych na cel lub wykrywania obiektów w technologii trudno wykrywalnej (ang. stealth). Tę zasadę zakłócania ilustruje rys. 2.13.



Rys. 2.13. Zakłócanie radiolokacji półaktywnej

⁷¹ 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.

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 jednocześnie 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.

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.

2.2.1.3. Zakłócanie rozpoznania czujnikowego

Zakłócanie rozpoznania czujnikowego ma na celu utrudnienie bądź uniemożliwienie przeciwnikowi zdobywania oraz przetwarzania tych danych, których nośnikami są fale sprężyste⁷² (infradźwięki⁷³, ultradźwięki⁷⁴) oraz wszelkiego rodzaju uboczne efekty towarzyszące działaniom bojowym, na przykład: termiczne, sejsmiczne, naciskowe, magnetyczne, chemiczne, zapachowe.

Z doświadczeń konfliktów lokalnych ostatnich lat wynika, że do postrzegania pola walki, przez pryzmat fal sprężystych oraz pozostałych efektów towarzyszących działaniom zbrojnym, 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 najbar-

⁷² 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.

⁷³ 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.

⁷⁴ 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.

dziej niedostępnych obszarów⁷⁵ działań zbrojnych, w czasie zbliżonym do rzeczywistego. Przy ich pomocy może również śledzić i nadzorować:

- aktywność wojsk w rejonach oraz wzdłuż wybranych tras, w których zostały rozmieszczone odpowiednie czujniki;
- aktywność wojsk w rejonach rozmieszczenia zapór i pól minowych, przepraw rzecznych, mostów i brodów;
- rejonny 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 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

⁷⁵W przyszłości w obszarze operacji (rejonie walki), 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.

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.

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 bazy transportowej środków walki, co zapobiega ich identyfikowaniu przez systemy czujnikowe.

Analiza współczesnych konfliktów zbrojnych sugeruje, 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 na tworzeniu tzw. pól aktywnego hałasu. Istota działania tych pól, polega na wytworzeniu fali dźwiękowej o tych samych parametrach, lecz w fazie odwróconej o 180° .

2.2.1.4. 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 paśmie⁷⁶ skonstruowano całą rodzinę urządzeń optoelektronicznych⁷⁷ 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.

Zakłócanie rozpoznania telewizyjnego, powinno być uwzględniane w ramach planowanych przedsięwzięć w zakresie dezorganizacji procesu zdobywania danych przez przeciwnika. Szczególna uwaga powinna być skupiona na zakłócaniu przekazywania na odległość obrazów ruchomych wraz z towarzyszącym

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

⁷⁷ 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 fotoogniów, fotopowielaczy, matryc CCD) oraz przesyłaniem danych w postaci sygnałów optycznych (np. światłowodami) i ich magazynowaniem.

im dźwiękiem. Procesem zakłócania należy objąć wszystkie środki radiowe, radioliniowe i radiosatelitarne wykorzystywane do transmisji przekazu telewizyjnego. Sposoby zakłócania ww. środków zostały przedstawione w podrozdziale 2.2.1.1.

Zakłócanie rozpoznania termowizyjnego 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 transmisji 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 ten 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.

Problematyka zakłócania rozpoznania optoelektronicznego powinna być ściśle powiązana z zakłócaniem rozpoznania radiolokacyjnego i realizowana przy pomocy ukrywania, dezinformowania i pozorowania optoelektronicznego. W zależności od sposobu zakłócania, 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 wojskowych. Polegają na odpowiednim wykorzystaniu ukryć naturalnych i wynikają z właściwości terenu i przed-

miotów 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. Praktyka wskazuje, 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 ich przygotowania oraz zapewnia lepsze rezultaty. Tej problematyce należałoby poświęcić więcej uwagi, bowiem mimo wprowadzania na wyposażenie wojsk coraz większej ilości środków optoelektronicznych, obserwuje się ten-

dencję do stopniowego zmniejszania udziału przedsięwzięć związanych z zakłócaniem tego rodzaju rozpoznania.

Natomiast będące aktualne w wyposażeniu wojsk siatki maskujące, są najczęściej poliamidowe i charakteryzują się zaledwie dostatecznymi zdolnościami zakłócania rozpoznania optycznego (maskowania), 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 maskujące⁷⁸, 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.

⁷⁸ W naszych wojskach nie ma etatowych zestawów do malowania maskującego, a przygotowanie stanów osobowych do jego wykonania nie jest wystarczające.

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 (bojowego), bowiem przy zastosowaniu właściwego sposobu pozorowania, prawdopodobieństwo przeprowadzenia ataku na cel pozorny jest bardzo wysokie.

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 laserowych⁷⁹ 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 raketowymi samonaprowadzającymi się na laserowo oświetlone cele, w zbliżeniowych zapalnikach laserowych oraz kierowania ogniem lufowej broni pokładowej samolotów i śmigłowców.

⁷⁹ Nazwa „laser” została utworzona z początkowych liter słów: Light Amplification by Stimulated Emission of Radiation (wzmocnienie światła z wymuszoną emisją promieniowania). Laser – to optyczny generator kwantowy, zwany też generatorem światła spójnego, lub źródłem monochromatycznych fal elektromagnetycznych w zakresie optycznym.

W wojskach lądowych, zakłócenia powinny obejmować wykorzystywane przez przeciwnika laserowe urządzenia celownicze. Eliminując subiektywne przyczyny niecelności, urządzenia te pozwalają na prowadzenie znacznie bardziej precyzyjnego ognia, zarówno przy strzelaniu z broni lufowej, jak i przeciwpancernych pociskach raketowych 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.

2.2.1.5. Zakłócanie rozpoznania informatycznego

W przyszłych systemach rozpoznania informatycznego należy liczyć się z systematycznym wzrostem penetracji rozległych i lokalnych sieci teleinformatycznych, 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 niezmiennie wartościowe informacje, czerpać też można z promieniowania samych komputerów.

Z powyższego wynika, 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, stają się obiektami rozpoznania, modyfikacji lub zniszczenia. Włączanie się do nich nieupoważnionych użytkowników jest stosunkowo łatwe i dalece prawdopodobne⁸⁰. Mogą oni śledzić, podsłuchiwać i przechwytywać dane, a także prowadzić dezinformację bądź niszczenie.

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, stanowiąc zagrożenie dla zachowania tajemnicy oraz penetrację aktywną, zagrażającą autentyczności danych.

⁸⁰ 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 i zakłócanie informatyczne.

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 informa-

cji. Na przykład: przechwycenie przez przeciwnika danych z logistyki dotyczących np. ilości zamawianego pieczywa 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 umiędzony 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.

Niszczzenie 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 własnych, które są wykorzystywane w sieciach informatycznych rozległych i lokalnych, obsługujących zautomatyzowane systemy dowodzenia, zautomatyzowane systemy rozpoznania oraz zautomatyzowane systemy kierowania (sterowania) uzbrojeniem.

W działaniach zbrojnych 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 stanowiska powinny być wyposażone w sprzęt komputerowy spełniający wymogi norm krajowych⁸¹, lub sprzęt wykonany w technologii zgodnej

⁸¹ Norma Polska PN-92 T-20001/02 pt. „Współdziałanie systemów otwartych (OSI). Podstawowy model odniesienia. Architektura zabezpieczeń”.

z amerykańskimi wymogami – TEMPEST⁸². Dla takiego stanowiska należy m.in. zorganizować:

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

- 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 danych⁸³. Systemy zabezpieczeń powinny być budowane w oparciu o komputerowe programy ochronne, będące z zasady integralnym elementem systemu ope-

⁸² 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 elektromagnetycznych. Opracowane normy są chronione na tyle skutecznie, że ich treść nie jest dokładnie znana poza granicami USA.

⁸³ 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.

racyjnego. 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 zaprojektowanie i wdrożenie na potrzeby sił zbrojnych 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;
- 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.

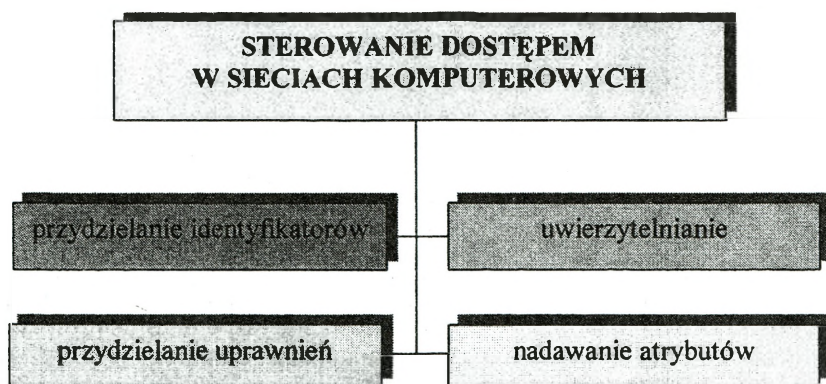
Ochrona programowa danych, dotyczy również stosowania metod i środków zapewniających ich bezpieczeństwo podczas przechowywania i przetwarzania w systemach komputerowych, a także podczas ich przesyłania w sieciach teleinformatycznych. Obejmuje ona cztery rodzaje sterowania:

- 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 rys. 2.14.

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. 2.14. 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 zarządcą 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 niezabezpieczonych komputerów 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 telefonicznymi⁸⁴.

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);

⁸⁴ W trakcie międzynarodowego zjazdu hackerów w Almere (Holandia), w którym uczestniczyło ponad 2000 osób, prof. E. Moeller z politechniki w Aachen 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 nastroczał 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.

– 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.

Należy sądzić, 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 odstraszenia. 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 sfalszowanych 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.

2.2.2. 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 danych dostarczanych przez systemy, podsystemy i elementy rozpoznawcze. Działalność ta ma charakter studyjny, stąd też często proces ten określany jest mianem rozpoznania studyjnego⁸⁵. W okresie pokoju rozpoznanie studyjne odgrywa najważniejszą rolę w działal-

⁸⁵ 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.

ności 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 i sztabowi w procesie planowania operacji (walki). 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 dezorganizować zarówno proces zasilania sztabu w dane rozpoznawcze jak

i 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 umiejętności ich wykorzystania, zależą w znacznej mierze rezultaty pracy sztabowych komórek oraz jednostek (pododdziałów) wydzielających elementy i podsystemy rozpoznawcze. Dlatego 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 przeciwozpoznawczych podejmowanych w ramach maskowania.

W tym celu, powinny być wykorzystywane wszystkie dostępne na danym szczeblu 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;

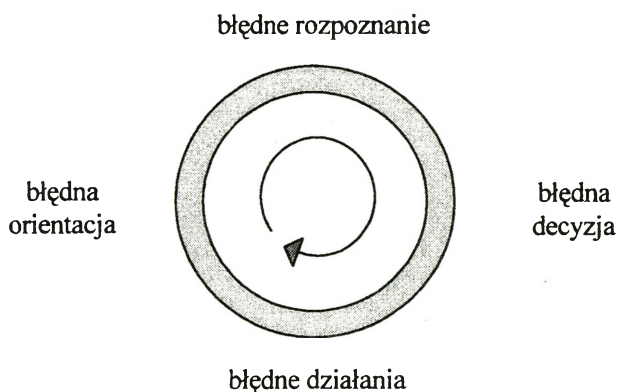
- obniżanie zdolności bojowej przeciwnika na skutek występowania opóźnień lub podejmowania niewłaściwych działań.

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” (rys. 2.15), w którym:



Rys. 2.15. Model „błędnego koła”

- 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.

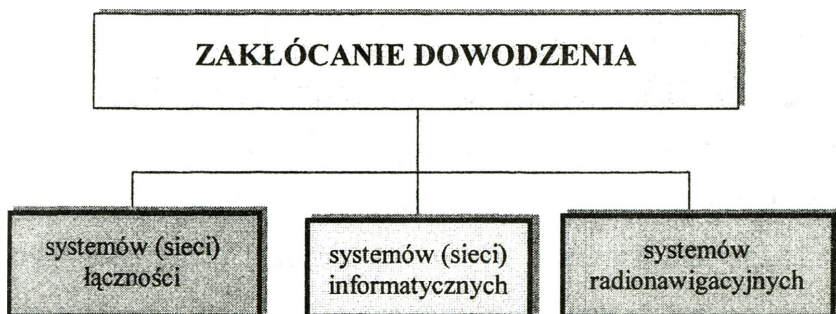
W okresie pokoju, ważną rolę odgrywają organizowane ćwiczenia z udziałem obserwatorów zagranicznych, gdzie powinny być wykorzystane aplikacyjne warianty działania naszych wojsk.

Wnioski z takich ćwiczeń powinny budzić wątpliwości i podważać prawdziwość dotychczasowych opracowań, komunikatów, meldunków czy zestawień organów rozpoznawczych przeciwnika⁸⁶ lub utwierdzać w przekonaniu o ich poprawności, jeśli stwierdzimy, że określone zbiory opracowanych informacji rozpoznawczych są błędne.

⁸⁶ 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).

3. ZAKRES I TREŚĆ PRZEDSIĘWZIĘĆ ZAKŁÓCANIA DOWODZENIA PRZECIWNIKA

Zakłócanie dowodzenia stanowi zespół skoordynowanych elementów dostosowany do wnoszenia entropii informacyjnej⁸⁷ do procesów dowodzenia wojskami przeciwnika, które realizowane są przy pomocy: systemów (sieci) łączności, systemów (sieci) informatycznych, systemów radionawigacyjnych. Podział zakłócania dowodzenia zilustrowano na rys. 3.1.



Rys. 3.1. Podział zakłócania dowodzenia

⁸⁷ Pojęcie „entropia informacyjna” zostało wyjaśnione w rozdziale 1.1.

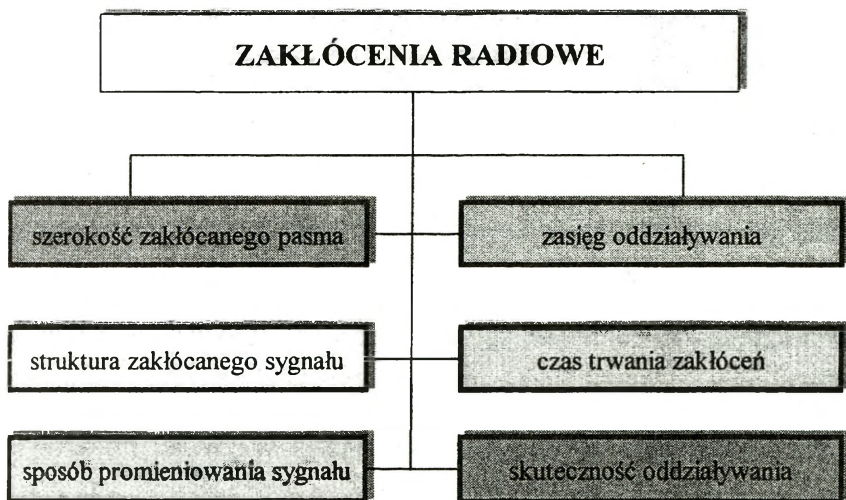
3.1. Zakłócanie systemów (sieci) łączności

Zakłócanie systemów (sieci) łączności polega na celowym promieniowaniu zakłócającej⁸⁸ energii elektromagnetycznej powodującej utrudnienie pracy środków łączności radiowej KF i UKF, łączności radioliniowej (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 szerebla 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 (sieci) łączności odbywa się przy pomocy specjalnych nadajników stacjonarnych lub mobilnych stacji: przewoźnych, powietrznych (samolotowych, śmigłowcowych) i okrętowych. Wyróżnia się również nadajniki zakłócające jedno-

⁸⁸ Podstawowe rodzaje zakłócania: dezinformującego, zagłuszającego i niszczącego przedstawiono w podrozdziale 1.2.

razowego użycia⁸⁹, które mogą być przenoszone jako specjalna amunicja artyleryjska lub urządzenia zrzucane z samolotu lub śmigłowca bądź rozmieszczane przez grupy dywersyjno-rozpoznawcze. Bardzo ważną rolę w **procesie zakłócania systemów (sieci) łączności odgrywa dobór parametrów sygnału zakłócającego do sygnału zakłócanego**. Powinien on być dokonywany według kryteriów zilustrowanych na rys. 3.2.



Rys. 3.2. Kryteria doboru zakłóceń radiowych

⁸⁹ Szczegółowy opis nadajników zakłócających znajduje się w literaturze przedmiotu.

Ze względu na szerokość zakłócanego pasma:

1. Zakłócenia selektywne (wąskopasmowe, punktowe), które wymagają dużej dokładności dostrojenia urządzeń stacji zakłócającej do częstotliwości roboczej zakłócanego środka elektro-nicznego. 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) oraz minimalny wpływ na pracę własnych stacji. Spośród wad wyróżnia się: konieczność rozpoznania zakłócanych emisji; łatwość uniknięcia zakłóceń selektywnych; wymaganą znajomość zakłócanej częstotliwości; mało efektywne wykorzystanie środków zakłócających.

2. Zakłócenia zaporowe (szerokopasmowe), które stosowane są do jednoznacznej dezorganizacji pracy kilku a nawet kilkudziesięciu środków radiowych. Za pomocą 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: dużą nieefektywność wykorzystania mocy nadajników, która rozkłada się proporcjonalnie na wszystkie częstotliwości zakłócanego pasma; duże prawdopodobieństwo zakłócenia pracy własnych stacji.

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

4. Zakłócenia pływające 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:

1. 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.

2. 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.

3. 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 zakłócającej 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 radiolinowych, urządzeń radiotelesterowania rakietami itp.

4. 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:

1. 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 zakłócających jednorazowego użycia, autonomicznych środków zakłócających statków powietrznych oraz niektórych środków wykorzystywanych na szczeblu taktycznym.

2. 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.

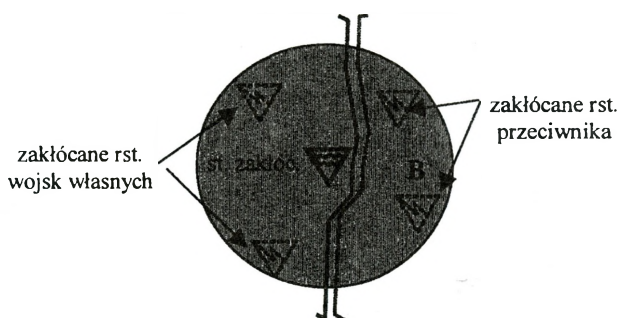
Ze względu na czas trwania:

1. Zakłócenia krótkotrwałe prowadzi się w czasie równym, lub krótszym od czasu nadawania sygnałów przez przeciwnika.

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

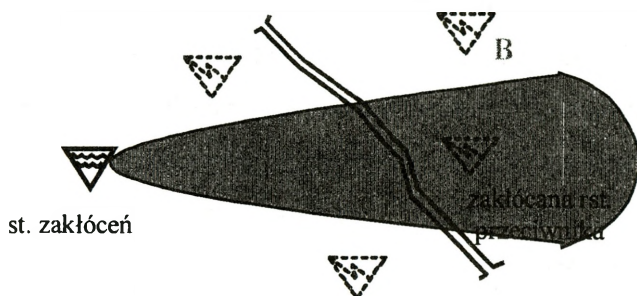
Ze względu na sposób promieniowania:

1. Zakłócenia dookólne występują wówczas, gdy promieniowanie anteny odbywa się we wszystkich kierunkach z jednakową mocą (rys. 3.3). 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 oraz duże prawdopodobieństwo zagłuszenia własnych środków elektronicznych (rys. 3.3) znajdujących się w zasięgu zakłóceń dookólnych.



Rys. 3.3. Graficzna ilustracja zakłóceń dookólnych

2. Zakłócenia kierunkowe występują wtedy, gdy energia elektromagnetyczna jest promieniowana przez antenę stacji zakłócającej o specjalnie dobranej charakterystyce, w kierunku zakłócanego środka elektronicznego przeciwnika (rys. 3.4). 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.



Rys. 3.4. Graficzna ilustracja zakłóceń kierunkowych

Ze względu na skuteczność⁹⁰ działania:

1. 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 jedynie pewne zniekształce-

⁹⁰ 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 uwzględnić różne czynniki.

nia 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%.

2. 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.

3. Zakłócenia bardzo silne (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.

Problematyka oceny skuteczności zakłócania środków radiowych KF i UKF pracujących na częstotliwościach ustalonych szczegółowo przedstawiona jest w licznych opracowaniach dotyczących walki radioelektronicznej⁹¹.

Skuteczność zakłócania urządzeń radioliniowych (horyzontowych i pozahoryzontowych) oraz radiosatelitarnych związana 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 zdeorganizować pracę środków radioliniowych na głębokość do 200 km.

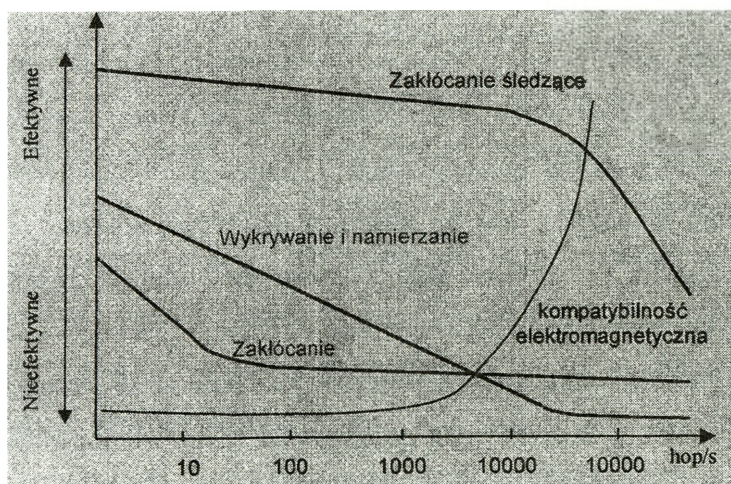
⁹¹ W siłach lądowych USA ocena skuteczności zakłóceń łączności radiowej UKF i KF na fali przyziemnej dokonywana jest przy pomocy zbliżonego aparatu matematycznego zamieszczonego w Communications Jamming Handbook FM 34-40-7. Dużą pomoc świadczą także: podręczny kalkulator GTA 30-6-5 oraz zestaw szablonów ang. The Jampot Fan, będące w wyposażeniu komórek walki elektronicznej.

Z kolei o **skuteczności zakłócania urządzeń radiowych wykorzystujących emisje rozproszone** 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 odpowiedniej 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 rys. 3.5.

Skuteczność zakłócania wyrafinowanymi szybkimi zakłóceniami śledzącymi, posiadającymi zdolność wyszukiwania i zakłócania chwilowych transmisji jest duża dla transmisji na poszczególnych częstotliwościach dłuższych od czasów propagacji sygnału do i od źródła zakłóceń. Jak wynika z rysunku, skuteczność zakłóceń śledzących maleje dopiero powyżej 10000 zmian czę-

stotliwości 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 w zasadzie wszystkie metody zakłóceń: zakłócenia selektywne, wielopunktowe, zaporowe i pływające.



Rys. 3.5. Wpływ częstotliwości skoków na efektywność zakłócania (rozpoznania i namierzania)

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 pasma⁹², 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.

⁹² W radiostacjach ze skokową zmianą częstotliwości jak standard przyjmuje się pasmo 12 MHz (± 6 MHz od częstotliwości środkowej).

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 użycia. 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 szumu. Odpowiednio wysoki poziom szumu w kanale szerokopasmowym, utrudni układowi decyzyjnemu odbiornika sygnałów FH podjęcie prawidłowej decyzji o odebranych sygnałach. 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 zakłó-

canej 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, używającego 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 śledze-

nia 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 urządzeń, szczególnie szerokopasmowych stacji zakłóceń o dużej mocy sygnału, nadajników zakłócających jednorazowego użycia oraz stacji z pływającym (śledzącym) sygnałem, możliwe jest uzyskanie zadowalających efektów zakłócania.

3.2. Zakłócanie systemów (sieci) informatycznych

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 ułatwienie dostępu do danych fałszy-

wych. 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 sterowane są w szerokim zakresie środkami informatycznymi, aby przeprowadzić więc skuteczny atak, wystarczy zdeorganizować pracę komputerów 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 angielskich słów: *malicious software* – oprogramowanie złośliwe)⁹³. 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 uśpionej. Charakteryzują się tym, że po wprowadzeniu do systemu informatycznego podejmują je-

⁹³ S. Garfinkel, G. Spafford, „Bezpieczeństwo w Unixie i Internecie”, Warszawa 1997, s. 31.

dynie 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 okresowo podawały swoją pozycję do przelatującego satelity. Zlokalizowane w ten sposób cele precyzyjnie i bez przeszkód bombardowano.

„Bomby logiczne” są najczęściej „podkładane” w programach przez informatyków, którzy mają legalny dostęp do systemu. Impulsem wyzwającym „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 pro-

gramów, ale mogą przenosić złośliwe kody, które dokonują zmian. Podstawowym zadaniem robaków komputerowych jest wypełnianie pamięci komputerów dużą liczbą 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 uszkodzają 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 reprodukuja się wykładniczo i zajmują ogromną ilość pamięci procesora, przestrzeni dyskowej i innych zasobów, przez co użytkownik nie może z nich dalej korzystać.

3.3. Zakłócanie systemów radionawigacyjnych

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. Powinno być ściśle skoordynowane z zakłócaniem rozpoznania

systemów radionawigacyjnych, które przedstawione zostało w podrozdziale 2.2.1.1.

Przegląd współczesnych systemów radionawigacyjne⁹⁴ umożliwia wydzielenie dwóch charakterystycznych grup:

- 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 zalicza się 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

⁹⁴ 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.

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

Ogólnie podzielić je można – jak przedstawiono w podrozdziale 2.2.1.1. – 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 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 dużą dokładnością. W przypadku systemów kołowych i kołowo-promieniowych takich jak TACAN⁹⁵ i RSBN, oprócz zakłócania odbiorników pokładowych urządzeń zapytujących istnieje również możliwość zakłócania odbiorników radiolaterni. Urządzenia te pracują w paśmie 1000 MHz i mogą być rozpoznawane i zakłócanie 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

⁹⁵ TACAN (ang. Tactical Air Navigation) – system nawigacji taktycznej. Jest połączeniem radiolaterni typu VOR i radiodalmierza DME. Umożliwia pomiar dwóch parametrów nawigacyjnych – azymutu i odległości. Zakres pracy 960 – 1215 MHz. System jest przeznaczony dla lotnictwa wojskowego i cywilnego, a także można wykorzystywać go w nawigacji morskiej.

kilku tysięcy kilometrów. Środki tego systemu pracują zazwyczaj w zakresach średnich, długich i bardzo długich fal radiowych.

Urządzenia pokładowe systemów **Loran**⁹⁶, **Omega**⁹⁷, podobnie jak urządzenia odbiorcze ultrakrótkofalowego systemu **VOR**, mogą być zakłócanie 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 stacji zakłóceń, oblicza się według podobnych zasad, jak w przypadku obezwładnienia zakłóceniami łączności radiowej, odpowiednio zwiększając współczynnik zakłóceń K_z .

⁹⁶ LORAN – C (ang. Long Range Navigation) – system nawigacyjny dalekiego zasięgu, pracujący w zakresie fal długich: $\lambda = 3000$ m ($f = 100$ kHz). Długość bazy między dwoma stacjami tworzącymi parę wynosi 600 – 800 mil morskich. W skład systemu wchodzi 50 stacji naziemnych. Zasięg działania 4000 – 4300 km.

⁹⁷ OMEGA – system fazowy dalekiego zasięgu. W skład systemu wchodzi osiem stacji brzegowych w różnych rejonach świata, oznaczonych literami A, B, C, D, E, F, G, H. Długość linii bazowych między stacjami 8000 – 10 000 km.

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 zagłuszeniu 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 (ko-

smicznego⁹⁸, kontrolnego⁹⁹ i użytkowego¹⁰⁰) najbardziej podatny na zakłócenia jest segment użytkowy. Zakłócenia te mogą powstawać w sposób niezamierzony¹⁰¹ (przypadkowy) w wyniku niekompatybilności różnych urządzeń radioelektronicznych lub też mogą być zamierzone (celowe) sygnały zakłócające emitowane przez komórki walki informacyjnej.

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

⁹⁸ 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° i okrążających Ziemię w ciągu 12 godzin w odległości 20200 km od jej powierzchni.

⁹⁹ 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.

¹⁰⁰ 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.

¹⁰¹ 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.

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 użycia. Są to urządzenia o bardzo małych rozmiarach, których koszt jednostkowy, według amerykańskich szacunków, nie powinien przekraczać 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 wymagać więc będzie uprzedniego dokładnego rozważenia strat i korzyści wynikających z jego zastosowania.

4. ZAKRES I TREŚĆ PRZEDSIĘWZIĘĆ ZAKŁÓCANIA KIEROWANIEM UZBROJENIEM PRZECIWNIKA

Analiza rozwiązań światowych w zakresie uzbrojenia umożliwia wyróżnienie czterech zasadniczych grup kierowania uzbrojeniem:

- zdalne¹⁰²,
- programowe¹⁰³,

¹⁰² 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.

¹⁰³ 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.

- samonaprowadzające¹⁰⁴,
- kombinowane¹⁰⁵.

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 z odległości 1 – 1,5 km może pasywnie naprowadzić się na cel. Zaletą środków bojowych wykorzystujących ra-

¹⁰⁴ „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.

¹⁰⁵ Kierowanie kombinowane jest połączeniem kilku różnych systemów, przy czym każdy system kieruje lotem na określonym odcinku toru, lub pracuje jednocześnie z innymi systemami.

diolokacyjne 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 zamaskowanych¹⁰⁶. Wadą tego systemu jest natomiast 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 oświetlone 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 uzbrojeniem są z reguły

¹⁰⁶ Praktycznie układy te znalazły zastosowanie w wojnie w rejonie Zatoki Perskiej w 1991 r.

urządzeniami wielokanałowymi, umożliwiającymi jednoczesne sterowanie kilkoma obiektami wykonawczymi. Realizację tego zapewniają wyspecjalizowane komputery pokładowe i urządzenia zapewniające wysoką niezawodność oraz skuteczność sterowania.

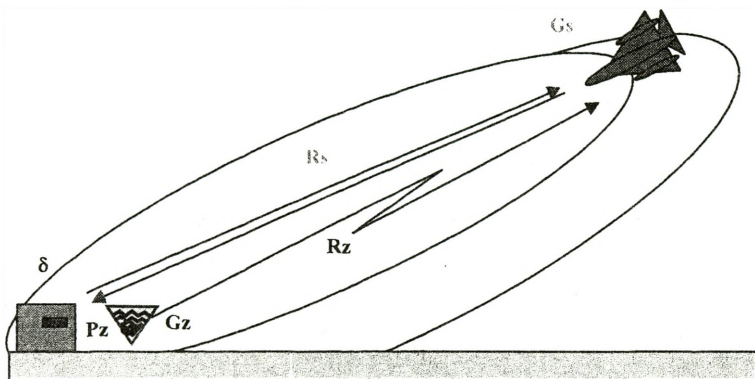
Z praktyki zakłóceń systemów kierowania uzbrojeniem wynika, że **obecnie możliwe jest zakłócanie nieautonomicznych i kombinowanych (częściowo automatycznych) systemów kierowania rakietami**, ponieważ w zestaw sterowania tych rakiet wchodzi urządzenia elektroniczne, które współpracują z naziemnymi środkami 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 doświadczeń minionych konfliktów lokalnych ostatnich lat 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 moż-

liwość zakłócenia zbliżeniowych zapalników radiowych tych rakiet. Oddziaływanie zakłóceniami 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 rakiet nie doleci do zaprogramowanego celu. W wypadku zakłócania zbliżeniowych zapalników radiowych rakiet, stacje zakłócające należy rozmieszczać w rejonach osłanianych obiektów.

Doświadczenia wykazują, że **najkorzystniej jest obezwładniać zakłóceniami urządzenia śledzenia radiolokacyjnego, a także relacji radiowych dowodzenia i automatycznego kierowania (sterowania)**. Zakłócanie urządzeń systemów śledzenia rakiet klasy „powietrze – ziemia” może odbywać się w strefie radiolokacyjnej widzialności i poza nią. Można założyć, że jeśli rakietę 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 potęgę. 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 potęgę. 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 rys. 4.1.



Rys. 4.1. Graficzna interpretacja zakłóceń radiolokacyjnych

Wymienione uwarunkowania można wyrazić następującymi równaniami:

– moc sygnału użytecznego stacji radiolokacyjnej odbitego od celu i odbieranego przez urządzenia odbiorcze stacji¹⁰⁷:

$$P_{\pi} = \frac{P_s G_s^2 \delta \lambda^2}{(4\pi)^2 R_s^4}$$

gdzie:

P_{π} [W] – moc sygnału użytecznego stacji radiolokacyjnej odbitego od celu;

P_s [W] – moc nadajnika stacji radiolokacyjnej (moc stacji);

¹⁰⁷ Por.: K. Kokot, „Podstawy radiolokacji”, wyd. WAT, Warszawa 1968, s. 148.

G_s – zysk kierunkowy anteny stacji radiolokacyjnej;

δ [m^2] – 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 radiolokacyjnej¹⁰⁸:

$$P_{sz} = \frac{P_z G_z G_s \lambda^2}{(4\pi R_z)^2}$$

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 [km] – odległość między stacją zakłócającą a odbiornikiem zakłócanej stacji radiolokacyjnej.

Przy jednakowej mocy stacji radiolokacyjnej i stacji zakłócającej i przy równych odległościach stacji radiolokacyjnej do

¹⁰⁸ Tamże, s. 148.

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 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 ракет 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 ракет w całej strefie śledzenia stacji radiolokacyjnej.

Do zakłócania niszczącego 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). Problematyka ta została przedstawiona w podrozdziale 1.2.3.

ZAKOŃCZENIE

Treści zawarte w niniejszym opracowaniu stanowią 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 elektro-
nicznych oraz specjalistycznych środków niszczenia, a obszar elektromagnetyczny uznawany jest za priorytetowy dla jego pro-
wadzenia.

Autor ma świadomość, że opracowanie nie wyczerpuje cał-
kowicie problematyki zakłócania informacyjnego rozumianego
jako aktywnej formy konfrontacji w sferze informacyjnej walki
zbrojnej. Zdaje sobie również sprawę z wielu ułomności jakie
mogły w sposób niezawiniony wystąpić w znaczeniowym przeka-
zywaniu treści poszczególnych rozdziałów. Będzie wdzięczny
wszystkim czytelnikom za wyrażone swoje opinie i uwagi odno-
śnie zaprezentowanych problemów. Zebrane tą drogą doświad-
czenia posłużą doskonaleniu kolejnych opracowań z zakresu róż-
nych form i metod prowadzenia walki informacyjnej, będącej
ważną sferą konfrontacji w XXI wieku, określanego epoką społeczeństwa informacyjnego.

BIBLIOGRAFIA

1. Antczak St.: „Systemy kierowania i uzbrojenia w polskich siłach powietrznych”, wyd. AON, Warszawa 1997.
2. Campen A. D.: „The first Information War”, Virginia 1992.
3. Ciborowski L.: „Walka informacyjna”, wyd. ECE, Toruń 1999.
4. Globan-Klas T.; Sienkiewicz P.: „Społeczeństwo informacyjne: Szanse, zagrożenia, wyzwania”, wyd. Fundacji Postępu Telekomunikacji, Kraków 1999.
5. Grabau. R.: „Sechs Dimensionen des Kriegers”, w: „Soldat und Technik”, nr 6, 1986.
6. Grafinkel S.; Spafford G.: „Practical Unix and Internet Security”, wyd. II, O'Reilly & Associates, Inc. Sebastopol USA, Opracowanie wersji polskiej Kresak P.: Bezpieczeństwo w Unixie i Internecie, wyd. RM, Warszawa 1997.
7. Janczak J.; Bezoń B.; Scheffs W.: „Walka elektroniczna w działaniach taktycznych wojsk lądowych”, wyd. AON, Warszawa 1999.
8. Janczak J.: „Obrona informacyjna w działaniach wojsk lądowych”, wyd. AON, Warszawa 2000.
9. Janczak J.: „Kierunki rozwoju rozpoznania oraz zakłócania elektronicznego”, wyd. AON, Warszawa 2001.
10. Komow S.A.: „O sposobach i formach prowadzenia walki informacyjnej”, w: Wojenną Mysł, Moskwa 1997.
11. Kozaczuk W.: „Wojna w eterze”. Warszawa 1977.

12. Markiewicz L.: „Ultradźwięki i infradźwięki”, wyd. PWN, Warszawa 1979.
13. Neri F.: „Introduction to Electronic Defense Systems”. Artech House, Inc., 1991.
14. Piekarski H.: „Walka radioelektroniczna”, wyd. MON, Warszawa 1980.
15. Rotkiewicz W.: „Kompatybilność elektromagnetyczna w radiotechnice”, wyd. KiŁ, Warszawa 1978.
16. Schwartz Winn.: „Information Warfare – Cyberterrorism: Protecting Your Personal Security in the Electronic Age”. 1993.
17. Shannon. C. E, Warren. W.: „The Mathematical Theory of Communication”. The University of Illinois Press, Urbana 1949.
18. Starry M. D., Arneson C. W.: Działania informacyjne, w: „Military Review”, nr 6, 1996.
19. Stalings W.: Ochrona danych w sieci i w intersieci, wyd. WNT, Warszawa 1997.
20. Sun Tzu: „Sztuka wojny”, wyd. Wydawnictwo Przedświt, Warszawa 1994.
21. Ścibiorek Z: „Wpływ nowych środków walki na działania bojowe wojsk lądowych”, wyd. AON, Warszawa 1993.
22. 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. Warszawa 1997.

Najnowsze publikacje Akademii Obrony Narodowej

do nabycia w Wydziale Wydawniczym AON
al. gen. A. Chruściela, 00-910 Warszawa, tel./faks 681 37 52

- Robert Bojarski – *Operacja obronna*
- Jan Czaja – *Stolica apostolska wobec integracji europejskiej*
- Marek Gąska, Andrzej Ciupiński – *Międzynarodowe prawo humanitarne*
- Marek Gąska – *Obronność w aktach prawnych Rzeczypospolitej Polskiej*
- Jerzy Groskrejc – *Antropologiczne i aksjologiczne aspekty edukacji oficerów*
- Henryk Herman – *Działania specjalne w wojnach i konfliktach zbrojnych po II wojnie światowej*
- Michał Huzarski (red.) – *Taktyka ogólna wojsk lądowych*
- Kuba Jałoszyński – *Terroryzm antyizraelski*
- Kuba Jałoszyński – *Terroryzm czy terror kryminalny w Polsce?*
- Kuba Jałoszyński – *Zagrożenie terroryzmem w wybranych krajach Europy zachodniej oraz w Stanach Zjednoczonych*
- Tadeusz Jemiolo – *Globalizacja. Szanse i zagrożenia*
- Jarosław Kardas, Krzysztof Loranty – *Wybrane problemy bezpieczeństwa i obronności państwa w opiniach pracowników administracji publicznej*
- Waldemar Kitler (red.) – *Obrona cywilna (niemilitarna) w obronie narodowej III RP*
- Waldemar Kitler – *Obrona narodowa w wybranych państwach demokratycznych*
- Stanisław Korzeniowski – *Żandarmeria wojskowa*
- Mirosław Koziński – *Umowa offsetowa i inne formy udziału państwa w międzynarodowym obrocie gospodarczym*
- Marian Kozub – *Lotnictwo w operacjach połączonych*
- Roman Kwečka – *Informacja w walce zbrojnej*
- Zbigniew Lach, Julian Skrzyp, Andrzej Łaszczuk – *Wojskowo-geograficzna charakterystyka Niemiec*
- Leonard Łukaszuk – *Europejskie prawo pokoju i bezpieczeństwa*
- Józef Marczak (red.) – *Samooorganizacja społeczeństwa na rzecz bezpieczeństwa powszechnego. Samoobrona powszechna III RP*
- Ireneusz Nowak – *Wybrane problemy historii polskiej techniki wojskowej XX wieku. Sprzęt i środki wojsk chemicznych*
- Janusz Płaczek – *Ewolucja polskiej myśli obronno-ekonomicznej w latach 1976–2000*
- Janusz Płaczek (red.) – *Gospodarka obronna Polski w końcu lat dziewięćdziesiątych. Szanse i zagrożenia*
- Adam Rejmak – *Ratownictwo lotnicze*
- Piotr Sienkiewicz – *5 wykładów*
- Aleksandra Skrabacz – *Kobiety w obronie narodowej Polski u progu XXI wieku*
- Katarzyna Słaboń – *Sytuacja jeńców wojennych w konflikcie iracko-irańskim (1980–1988)*
- Marek Sołoucha, Piotr Malinowski – *Użycie artylerii w szczególnych rodzajach działań bojowych*
- Zenon Stachowiak – *Metodyka i metodologia pisania prac kwalifikacyjnych (licencjackich, magisterskich i podyplomowych)*
- Janusz Zuziak – *Dzieje Instytutu Józefa Piłsudskiego w Londynie 1947–1997*

Zamówienia przyjmujemy telefonicznie lub pisemnie

