AKADEMIA
OBRONY NARODOWEJ

AON 5402/2002

Józef JANCZAK

OBRONA INFORMACYJNA W DZIAŁANIACH OBRONNYCH ZWIĄZKU OPERACYJNEGO WOJSK LĄDOWYCH

BIBLIOTEKA GŁÓWNA - ARCHIWUM
Nr ewid.
Akademii Obrony Narodowej
54385

Biblioteka Główna
Akademii Sztuki Wojennej
54385
09-054385-000-0

WARSZAWA 2002

AKADEMIA OBRONY NARODOWEJ

WYDZIAŁ WOJSK LĄDOWYCH

AON 5402/02

Józef JANCZAK

OBRONA INFORMACYJNA W DZIAŁANIACH OBRONNYCH ZWIĄZKU OPERACYJNEGO WOJSK LĄDOWYCH

Praca studyjna



WARSZAWA 2002

Recenzent:

prof. dr hab. Leopold CIBOROWSKI

Druk i oprawa: Akademia Obrony Narodowej – Wydział Wydawniczy, zam. nr 362/2002

SPIS TREŚCI

WSTĘP **5**

1. ISTOTA OBRONY INFORMACYJNEJ W DZIAŁANIACH OBRONNYCH ZWIĄZKU OPERACYJNEGO **19**

1.1. Rola i miejsce obrony informacyjnej w poglądach na prowadzenie działań obronnych związku operacyjnego 19

1.2. Przedmiot, cel i zadania obrony informacyjnej w działaniach obronnych związku operacyjnego 34

1.3. Wnioski 41

2. ZAKRES I TREŚĆ PRZEDSIĘWZIĘĆ OBRONY INFORMACYJNEJ PRZED ROZPOZNANIEM W DZIAŁANIACH OBRONNYCH ZWIĄZKU OPERACYJNEGO **43**

2.1. Obrona informacyjna przed rozpoznaniem bezpośrednim 44

2.1.1. Ochrona kontrwywiadowcza 46

2.1.2. Maskowanie 50

2.1.3. Ubezpieczanie 57

2.2. Obrona informacyjna przed rozpoznaniem pośrednim 59

2.2.1. Obrona informacyjna przed rozpoznaniem elektronicznym 60

2.2.1.1. Maskowanie radioelektroniczne 69

2.2.1.2. Maskowanie radiolokacyjne 99

2.2.1.3. Maskowanie optoelektroniczne 107

2.2.1.4. Maskowanie czujnikowe 112

2.2.1.5. Maskowanie informatyczne 114

2.2.2. Obrona informacyjna przed rozpoznaniem studyjnym 122

2.3. Wnioski 125

3. ZAKRES I TREŚĆ PRZEDSIĘWZIĘĆ OBRONY INFORMACYJNEJ PRZED ZAKŁÓCANIEM W DZIAŁANIACH OBRONNYCH ZWIĄZKU OPERACYJNEGO **129**

3.1. Obrona informacyjna przed zakłócaniem zagłuszającym 131

3.1.1. Obrona antyzagłuszeniowa systemów (sieci) łączności 133

3.1.2. Obrona antyzagłuszeniowa systemów (sieci) teleinformatycznych 146

3.1.3. Obrona antyzagłuszeniowa systemów radionawigacyjnych 151

3.1.4. Obrona antyzagłuszeniowa systemów naprowadzania uzbrojenia 155

3.2. Obrona informacyjna przed zakłócaniem dezinformującym 167
3.3. Obrona informacyjna przed zakłócaniem niszczącym 173
3.4. Zabezpieczenie systemów dowodzenia i naprowadzania uzbrojenia przed niekompatybilnością elektromagnetyczną 182
3.5. Wnioski 190
4. PRZEBIEG PROCESU DECYZYJNEGO POD KĄTEM POTRZEB OBRONY INFORMACYJNEJ W DZIAŁANIACH OBRONNYCH ZWIĄZKU OPERACYJNEGO 193
4.1. Odpowiedzialność funkcyjna za obronę informacyjną 194
4.1.1. Rola dowódcy i szefa sztabu związku operacyjnego 195
4.1.2. Zadania oddziału G 2 sztabu związku operacyjnego w zakresie obrony informacyjnej 197
4.1.3. Zadania oddziału G 3 sztabu związku operacyjnego w zakresie obrony informacyjnej 201
4.1.4. Zadania specjalistów rodzajów wojsk w zakresie obrony informacyjnej .. 202
4.1.5. Powiązania informacyjne w zakresie obrony informacyjnej 203
4.2. Przebieg cyklu decyzyjnego w zakresie obrony informacyjnej 212
4.2.1. Ustalanie położenia w zakresie obrony informacyjnej 214
4.2.2. Planowanie obrony informacyjnej 218
4.2.2.1. Ocena sytuacji w zakresie obrony informacyjnej 219
4.2.2.2. Decyzja i zamiar dowódcy w zakresie obrony informacyjnej 240
4.2.2.3. Opracowanie dokumentów w zakresie obrony informacyjnej 241
4.2.3. Stawianie zadań w zakresie obrony informacyjnej 244
4.2.4. Kontrola wykonania zadań w zakresie obrony informacyjnej 245
4.3. Wnioski 246
ZAKOŃCZENIE 248
BIBLIOGRAFIA 250
ZAŁĄCZNIKI 256

WSTĘP

Problem obrony informacyjnej istniał od zarania dziejów, choć nie postrzegano go z taką jaskrawością jak w obecnych czasach. Wprowadzane wraz z rozwojem społecznym zmiany w sposobach komunikowania się między ludźmi, szczególnie w zakresie zapisu i przesyłania wiadomości, zawsze stwarzały nowe problemy związane z ich ochroną i obroną.

W epoce budowy społeczeństwa informacyjnego[1], w którym dominuje wykorzystanie globalnych systemów informacyjnych (np. Internet), zbudowanych na bazie nowych technologii, wiele państw, instytucji a nawet osób prywatnych ma szeroki dostęp do danych i może je wykorzystać według potrzeb oraz własnego uznania. Prognozuje się, że kraje nie korzystające ze światowych zasobów informacyjnych czeka ekonomiczna oraz technologiczna wegetacja[2].

Nieustannie trwają więc procesy zdobywania i wykorzystania danych w wielu dziedzinach, przede wszystkim na arenie ekonomicznej, politycznej i militarnej. Równocześnie trwa proces ochrony danych[3], szczególnie o znaczeniu militarnym w celu zabezpieczenia ich przed nieautoryzowanym dostępem i modyfikacją. Zdobycie i odpowiednie wykorzystanie informacji np. w dziedzinie militarnej umożliwia bowiem podjęcie uzasadnionej decyzji na

---

[1] T. Globan-Klas, P. Sienkiewicz: „Społeczeństwo informacyjne: Szanse, zagrożenia, wyzwania", wyd. FPT, Kraków 1999.

[2] Ostrzeżenie Unii Europejskiej z tzw. Raportu Bangemanna.

[3] Przynależność Polski do NATO wymaga dostosowania prawnych ram ochrony danych do standardów Sojuszu, przede wszystkim do tzw. minimalnych wymagań w zakresie bezpieczeństwa, określonych w dokumencie C – M/55/15. W uchwalonej przez Sejm RP ustawie „O ochronie informacji niejawnych" z dnia 22.01.1999, DzU nr 11, poz. 95/2000 uwzględnia się wymagania NATO i wprowadza ujednolicone klauzule tajności: „ściśle tajne" (ang. Top Secret), „tajne" (ang. Secret), „poufne" (ang. Confidential), „zastrzeżone" (ang. Restricted), „nieklasyfikowane" (ang. Unclassificed). Ustawa nadaje problemowi ochrony informacji niejawnych charakter ponadresortowy. Wszystkie instytucje, w których są wytwarzane, przetwarzane i przekazywane dane niejawne muszą mieć swoich pełnomocników ochrony, kierujących wyspecjalizowaną komórką organizacyjną ochrony.

polu walki, a tym samym zwiększenie zdolności bojowej wojsk własnych[4] oraz ochronę ich systemów dowodzenia i naprowadzania uzbrojenia przed dezorganizacją pracy, a nawet zniszczeniem.

Powodzenie w konfrontacji zbrojnej w epoce budowy społeczeństwa informacyjnego, której towarzyszy cyfryzacja i informatyzacja pola walki, nie jest więc możliwe bez kompleksowego rozwiązania problemów obrony informacyjnej na wszystkich szczeblach dowodzenia.

Problematyka ta jest dostrzegana w wielu państwach. Odpowiednią rangę nadano jej w siłach zbrojnych przodujących państw NATO. Potwierdzeniem tej tezy są liczne materiały źródłowe [18;37;45;48;57;109;114;121;122;124;145]. Dostrzegana jest również w siłach zbrojnych Federacji Rosyjskiej [40;74;75;77;105]. Mimo wzrastającego zainteresowania tą tematyką na świecie oraz pojawiających się coraz liczniejszych publikacji nawiązujących do tej problematyki, wciąż nie jest ona dostatecznie dostrzegana i interpretowana w naszych siłach zbrojnych. Brak jest na ten temat materiałów naukowych i teoretycznych[5].

Brak kompleksowego rozwiązania dotyczącego obrony informacyjnej w działaniach naszych sił zbrojnych sprawia, że istnieje potrzeba naukowego opracowania tego zagadnienia, z uwzględnieniem różnych związków przyczynowo-skutkowych, mających bezpośredni wpływ na zapewnienie stabilnej pracy i funkcjonowanie systemów dowodzenia i naprowadzania uzbrojenia.

Sytuacja problemowa powstała i ukształtowała się w toku konfrontacji wiedzy teoretycznej i praktycznej autora, nagromadzonej w wyniku osobistych zainteresowań problematyką obrony i ochrony systemów łączności, obrony elektronicznej, obrony informacyjnej systemów dowodzenia i naprowadzania uzbrojenia w warunkach różnorakich zagrożeń na polu walki oraz długoletniej pracy dowódczej, dydaktycznej i naukowej.

Uzyskane doświadczenia i systematycznie pogłębiana wiedza w tym zakresie wyrobiła u autora przekonanie, że obrona informacyjna stanowi jeden z ważniejszych komponentów (filarów) przyszłych działań wojsk związku operacyjnego, zwłaszcza działań obronnych.

Z drugiej strony, zarówno rzeczywistość poznawana podczas ćwiczeń, jak i analiza dokumentów normatywnych utwierdziły autora w przekonaniu, że problem obrony informa-

---

[4] Informacja i technologie cyfrowe tworzą tak synergiczny efekt pomiędzy działającymi systemami, modularnymi strukturami organizacyjnymi wojsk i ich komponentami, że – jak przewidują futurolodzy – możliwości wojsk zostaną niebawem zwiększone o rząd wielkości.

[5] Ogólna teoria walki informacyjnej przestawiona jest w: L. Ciborowski: „Przestrzenie walki informacyjnej", wyd. AON, Warszawa 1997; L. Ciborowski: „Walka informacyjna", wyd. ECE, Toruń 1999; L. Ciborowski, A. Nowak: „Planowanie, organizowanie i prowadzenie walki informacyjnej na szczeblach taktycznych wojsk lądowych", wyd. AON, Warszawa 2000; G. Nowacki: „Walka informacyjna – próba kategoryzacji". Rozprawa doktorska, wyd. AON, Warszawa 1999.

cyjnej w naszych siłach zbrojnych nie jest dostrzegany, bądź traktowany jest formalnie, a więc praktycznie nie rozwiązywany.

Taki stan rzeczy ustalony w ramach poznania przednaukowego skłonił autora do podjęcia tego problemu jako zasadniczego przedmiotu tematycznego pracy studyjnej.

W obecnym stanie wiedzy na temat obrony informacyjnej w działaniach obronnych związku operacyjnego istnieje poważna luka. Pojawiające się nowe zagrożenia towarzyszące cyfryzacji pola walki oraz postępująca integracja w ramach Sojuszu NATO, a wraz z nią oczekiwania i potrzeby towarzyszące złożonemu procesowi zapewnienia interoperacyjności naszym wojskom, również w sferze informacyjnej, wymuszają konieczność przewartościowania poglądów na temat obrony informacyjnej. **Powstają więc pytania: jaka jest istota, przedmiot, cel i zadania obrony informacyjnej oraz zakres i treść przedsięwzięć wykonywanych na jej potrzeby w działaniach obronnych związku operacyjnego wojsk lądowych[6]?**

Treść poznawcza pracy została podporządkowana **osiągnięciu następującego celu**: **Opracować zbiór naukowo uzasadnionych podstaw teorii obrony informacyjnej w działaniach obronnych związku operacyjnego.** Merytoryczne treści wyprowadzić z obszarów poznania obejmujących aktywne i pasywne formy walki informacyjnej, z jednoczesną identyfikacją zakresów i konsekwencji zagrożeń przekładających się na własne systemy dowodzenia wojskami i naprowadzania uzbrojenia oraz na własne procedury tworzenia baz danych i systemy zarządzania zasobami informacyjnymi.

Osiągnięcie powyższego celu zostało zatem połączone z **rozwiązywaniem szeregu problemów** związanych z identyfikowaniem, poznawaniem i ustaleniem:

- po pierwsze – przedmiotu, celu, zadań i struktury obrony informacyjnej w działaniach obronnych związku operacyjnego;
- po drugie – pożądanego zakresu i treści przedsięwzięć obrony informacyjnej przed rozpoznaniem w działaniach obronnych związku operacyjnego;
- po trzecie – pożądanego zakresu i treści przedsięwzięć obrony informacyjnej przed zakłócaniem w działaniach obronnych związku operacyjnego;
- po czwarte – miejsca obrony informacyjnej w strukturach procedur pracy sztabowej oraz przebiegu cyklu decyzyjnego pod kątem jej potrzeb w działaniach obronnych związku operacyjnego.

---

[6] W dalszej części pracy studyjnej występować będzie określenie związek operacyjny.

Rozwiązanie wymienionych problemów badawczych w aspekcie sprecyzowanego wcześniej celu poznania oparto na szeroko rozumianej weryfikacji następującej **hipotezy roboczej:**

Wszechstronnie zaplanowana, zorganizowana i prowadzona obrona informacyjna w działaniach obronnych związku operacyjnego zapewnia stabilną pracę systemów dowodzenia i sterowania środkami walki oraz ochronę ich zasobów i procesów informacyjno-sterujących, co stanowi warunek konieczny osiągnięcia sukcesu na współczesnym i przyszłym polu walki.

W odniesieniu **do pierwszego problemu szczegółowego** przyjęto następującą **szczegółową hipotezę roboczą:**

Sprawność kierowania potencjałem związku operacyjnego w działaniach obronnych uzależniona jest od podejmowanych przez jego wojska odpowiednio skoordynowanych działań w ramach obrony informacyjnej.

Przedmiotem obrony informacyjnej w działaniach obronnych związku operacyjnego są systemy dowodzenia i sterowania środkami walki oraz ich zasoby i procesy informacyjno-sterujące, a jej celem jest zachowanie ciągłości dowodzenia wojskami i naprowadzania uzbrojenia w warunkach kompleksowego rozpoznania i intensywnego zakłócania informacyjnego ze strony potencjalnego przeciwnika.

Cel obrony informacyjnej w działaniach obronnych związku operacyjnego można osiągnąć przez realizację następujących zadań:

- po pierwsze – zabezpieczanie procesów informacyjno-sterujących przed oddziaływaniem informacyjnym przeciwnika;
- po drugie – podwyższanie odporności elementów ugrupowania obronnego związku operacyjnego na ich wykrycie i zakłócenie.

W aspekcie ogólnowojskowym obrona informacyjna stanowi ważny element zabezpieczenia działań związku operacyjnego, a jej strukturę tworzą:

- obrona informacyjna przed rozpoznaniem w działaniach obronnych związku operacyjnego;
- obrona informacyjna przed zakłócaniem w działaniach obronnych związku operacyjnego.

W odniesieniu do **drugiego problemu szczegółowego** przyjęto następującą **szczegółową hipotezę roboczą:**

Identyfikacja zakresu i konsekwencji zagrożeń rozpoznaniem przeciwnika pozwala sądzić, że obrona informacyjna przed nim stanowi zespół skoordynowanych działań dostosowanych do ukrywania zbiorów wszelkich postaci informacji o rzeczywistym stanie, usytuowaniu i zamiarach działania wojsk związku operacyjnego, które mogą być dostępne dla źródeł rozpoznania.

Obrona informacyjna związku operacyjnego przed rozpoznaniem jest ważnym elementem zabezpieczenia działań zarówno w okresie pokoju, jak i podczas kryzysu oraz w stanie wojny, i obejmuje obronę przed rozpoznaniem bezpośrednim oraz obronę przed rozpoznaniem pośrednim prowadzonym przez potencjalnego przeciwnika.

Obronę informacyjną przed rozpoznaniem bezpośrednim w działaniach obronnych związku operacyjnego należy prowadzić różnymi sposobami i metodami. Składają się na nie odpowiednie przedsięwzięcia ochrony kontrwywiadowczej, maskowania i ubezpieczania.

Obrona informacyjna przed rozpoznaniem pośrednim w działaniach obronnych związku operacyjnego obejmuje obronę przed rozpoznaniem elektronicznym (stanowiącą zespół skoordynowanych przedsięwzięć w zakresie maskowania takich jak: ukrywanie, dezinformowanie i pozorowanie) oraz obronę przed rozpoznaniem studyjnym.

W odniesieniu do **trzeciego problemu szczegółowego** przyjęto następującą **szczegółową hipotezę roboczą:**

Identyfikacja zakresu i konsekwencji zagrożeń zakłócaniem informacyjnym przeciwnika pozwala sądzić, że obrona informacyjna związku operacyjnego przed nim ma na celu zabezpieczenie przed niszczeniem zbiorów własnych postaci danych i wnoszeniem do nich takich treści, które mogą powodować wzrost niewiedzy o stanie, usytuowaniu i zamiarach działania wojsk przeciwnika oraz wprowadzać stan chaosu i nieuporządkowania we własnych procesach dowodzenia i naprowadzania uzbrojenia.

Obrona informacyjna związku operacyjnego przed zakłócaniem organizowana w warunkach postępującej elektronizacji oraz automatyzacji pola walki jest problemem wysoce złożonym i stanowi element zabezpieczenia działań podczas kryzysu i w stanie wojny. Przedsięwzięcia planistyczno-organizacyjne należy realizować również w czasie pokoju oraz w okresach poprzedzających zagrożenie bezpośrednie.

Obronę informacyjną przed zakłócaniem w działaniach obronnych związku operacyjnego należy prowadzić różnymi sposobami i metodami. Składają się na nie odpowiednie działania organizacyjne i techniczne (techniczno-eksploatacyjne) podejmowane w ramach:

- obrony informacyjnej przed zakłócaniem zagłuszającym;
- obrony informacyjnej przed zakłócaniem dezinformującym;

– obrony informacyjnej przed zakłócaniem niszczącym;

– zabezpieczenia systemów dowodzenia i naprowadzania uzbrojenia związku operacyjnego przed niekompatybilnością elektromagnetyczną.

W odniesieniu do **czwartego problemu szczegółowego** przyjęto następującą **szczegółową hipotezę roboczą:**

Obrona informacyjna obejmuje przedsięwzięcia i różne formy działalności, które powinny być planowane i organizowane w sposób scentralizowany, a realizowane na zasadzie powszechności (w zakresie zależnym od szczebla dowodzenia i aktualnej sytuacji operacyjno - bojowej).

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

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

Przedmiotem badań niniejszej pracy studyjnej uczyniono obronę informacyjną w działaniach obronnych związku operacyjnego w warunkach wykorzystywania nowych technologii na polu walki.

Na tym tle **obszar badań** został ograniczony do wymiaru informacyjnego pola walki, którego rola i znaczenie systematycznie będzie wzrastać na współczesnym polu walki wraz z coraz szerszym wykorzystaniem globalnych systemów informacyjnych, zbudowanych na bazie technologii cyfrowych.

Do weryfikacji przyjętych hipotez autor wykorzystał empiryczne i teoretyczne **metody badawcze**.

Potraktowanie przedmiotu badań jako systemu[7] o spójnej i wewnętrznie zintegrowanej strukturze, określonych funkcjach oraz stanowiącego jednocześnie część (ściśle zdefiniowany

---

[7] System jest pojęciem desygnującym pewną całość tworzoną przez określony zbiór obiektów (elementów) i powiązań (relacji) między nimi, rozpatrywaną z określonego punktu widzenia (aspektu badań). Jest to wszelki skoordynowany wewnętrznie i wykazujący określoną strukturę układ elementów. Rozpatrywany od zewnątrz jest całością, rozpatrywany od wewnątrz stanowi zbiór, do którego przynależność warunkują związki między wszystkimi jego elementami. Ogół elementów systemu w tym rozumieniu nazywa się składem. Ogół zaś związków (relacji) pomiędzy elementami, które są uwarunkowane przez ich przynależność do systemu, nazywa się strukturą. P. Sienkiewicz: „Podstawy teorii systemów", wyd. AON, Warszawa 1993.

element) systemu nadrzędnego (systemu walki informacyjnej związku operacyjnego) spowodowało, że w procesie badawczym stosowano głównie podejście (ujęcie) systemowe, a także funkcjonalne, informacyjne i logiczne.

Podejście systemowe – zastosowane do rozwiązywania złożonych problemów naukowych i praktycznych przewija się w samym formułowaniu zadań, ich rozwiązywaniu, jak również w organizacji procesu badawczego. Wykorzystując je w pierwszej kolejności, zdefiniowano badany obiekt, a następnie, uwzględniając relacje systemowe, dokonano rozłożenia systemu na podsystemy i podjęto się ich badania.

Szeroki obszar problemowy pracy studyjnej wymagał przyjęcia określonej procedury badawczej, w której kierowano się także **podejściem funkcjonalnym**. Stosując zasadę włączenia, dokonano analizy dwóch systemów funkcjonalnych: ofensywnych działań informacyjnych potencjalnego przeciwnika oraz działań defensywnych związku operacyjnego w tej sferze, tj. obrony informacyjnej.

Analizę prowadzono pod kątem identyfikacji czynników zagrożenia ofensywnymi środkami walki informacyjnej potencjalnego przeciwnika oraz określenia sposobów obrony informacyjnej związku operacyjnego w odniesieniu do ogólnych funkcji badanych systemów – zdolności bojowej walczących stron.

Stosując zasadę wyłączenia – w ramach podejścia funkcjonalnego - oceniano wpływ skuteczności przedsięwzięć obrony informacyjnej na kształtowanie ogólnego stosunku sił w obszarze obrony związku operacyjnego, a więc na właściwości funkcjonowania systemów wyższego rzędu, systemu walki, systemu dowodzenia, systemu sterowania środkami walki, systemu rozpoznania.

Ponieważ związek między różnymi strukturami i odpowiadającymi im funkcjami w badanych systemach nie jest statyczny i zdeterminowany, lecz podlega zmianom dynamicznym, szczególną uwagę zwrócono na ujawnienie i badanie mechanizmów tych zmian.

Ujęcie informacyjne wynikało bezpośrednio z istoty przedmiotu badań oraz potrzeby dokonania głębokiej analizy oraz oceny funkcjonowania systemów dowodzenia i sterowania środkami walki związku operacyjnego, ich zasobów informacyjnych i procesów informacyjno-sterujących postrzeganych jako „źródła", „nośniki", „przetworniki" lub „układy odbierające" bodźców informacyjnych, podtrzymujących i zasilających systemy zasadnicze.

Ujęcie logiczne zastosowano przede wszystkim na etapie badań teoretycznych, umożliwiając rozważenie wszelkich zjawisk charakteryzujących złożony proces decyzyjny w sztabie związku operacyjnego i na tej podstawie doprowadzenie do uogólnień i wniosków na potrzeby obrony informacyjnej.

Przedstawione sposoby podejścia (ujęcia) mają charakter ogólnonaukowy i to one w znacznej mierze umożliwiły przeprowadzenie naukowego „oglądu" otoczenia i samego przedmiotu badań.

Spośród **metod empirycznych** wykorzystano w trakcie prowadzonych badań obserwację naukową (bezpośrednią i pośrednią), modelowanie (matematyczne, komputerowe i symulacyjne) oraz badanie opinii (wywiad i metodę oceny ekspertów). Okazały się one szczególnie pomocne podczas gromadzenia faktów oraz weryfikacji hipotez roboczych.

Źródłem faktów były materiały teoretyczne dotyczące poglądów teoretyków wojskowych najbardziej rozwiniętych państw na walkę informacyjną, sprawozdania z praktycznej realizacji tych poglądów w konfliktach zbrojnych i wojnach lokalnych, a także uwarunkowania operacyjne planowania, organizowania i prowadzenia działań obronnych związku operacyjnego oraz ich wpływ na skuteczność obrony informacyjnej. Dużą rolę odegrały również materiały z ćwiczeń, które prowadzone były w AON w latach 1997 - 2000, szczególnie tych z udziałem przedstawicieli państw NATO. Za pomocą biernej i uczestniczącej obserwacji naukowej badano zjawiska i procesy zachodzące w sferze informacyjnej w toku ćwiczeń, których autor niniejszej pracy był uczestnikiem lub autorem i realizatorem.

Obserwacja naukowa dotyczyła również badań materiałów zamieszczonych w Internecie i specjalistycznej prasie obcojęzycznej, prospektów reklamowych czołowych firm elektronicznych i informatycznych oraz materiałów z ćwiczeń, sprawozdań i relacji z użycia środków i systemów walki informacyjnej w konfliktach i wojnach lokalnych.

Dużą rolę odegrały także badania opinii. Szeroko stosowano wywiad i metodę oceny ekspertów. Badaniami objęto ekspertów z AON, Sztabu Gen. WP, DWLąd, sztabów okręgów wojskowych (związków operacyjnych), a także przedstawicieli uczelni wojskowych innych państw NATO, głównie Bundeswehry, przebywających w AON. Oni to z naukowego punktu widzenia, dostarczyli najbardziej pożytecznych danych dotyczących modelowania cyklu decyzyjnego w zakresie obrony informacyjnej w działaniach obronnych związku operacyjnego pod kątem zapewnienia interoperacyjności naszych wojsk operacyjnych w ramach sojuszu NATO. Opinie te zostały uwzględnione podczas pisemnego opracowywania pracy studyjnej.

Z dużą życzliwością przyjmowano także uwagi, opinie i sugestie oficerów innych rodzajów wojsk oraz specjalistów spoza resortu obrony narodowej biorących udział wspólnie z autorem w konferencjach naukowych[8].

---

[8] Tematyka referatów wygłaszanych przez autora na konferencjach naukowych została zamieszczona w spisie bibliograficznym.

Podczas badań, szczególnie w zakresie modelowania zagrożenia w wymiarze informacyjnym, wykorzystano również modele matematyczne, komputerowe i symulacyjne oceny zagrożenia opracowane przy współudziale autora podczas prowadzonych prac naukowo-badawczych[9]. Autor zaproponował ich wykorzystywanie również w procesie planowania systemu łączności związku operacyjnego.

Spośród **metod teoretycznych** wykorzystano przede wszystkim: analizę, syntezę, abstrahowanie, indukcję, dedukcję, analogię, porównanie, uogólnienie oraz matematyczne metody analityczne. Ich zastosowanie umożliwiło pozyskanie wartościowych przesłanek i ostateczne ustalenie struktury obrony informacyjnej w działaniach obronnych związku operacyjnego oraz przedstawienie jej znaczenia w procesie dowodzenia. Wydatnie wzbogaciły i uzupełniły one zastosowane metody empiryczne.

Zastosowane metody i narzędzia badawcze pozwalają wnioskować, że:

- nie istnieje jedna uniwersalna metoda badawcza, która byłaby pomocna przy rozwiązywaniu danego problemu;
- znajomość metod i narzędzi badawczych pozwala na ich wybór lub opracowanie własnej metody do zbadania określonego problemu;
- metody zastosowane w niniejszej pracy studyjnej wydają się być narzędziami badawczymi użytecznymi i wystarczającymi do rozwiązania zawartych w niej problemów badawczych;
- metody te mogą być stosowane w przyszłości do rozwiązywania podobnych problemów naukowych.

Proces badawczy podzielono na trzy etapy:

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

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

---

[9] Wykaz prac naukowo – badawczych z udziałem autora został zamieszczony w spisie bibliograficznym.

Etap badań właściwych ukierunkowano przede wszystkim na weryfikację hipotez roboczych.

Hipotezę roboczą nr 1 zweryfikowano za pomocą analizy (systemowej, funkcjonalnej i logicznej), porównania i obserwacji pośredniej. Dokonano analizy wewnętrznej dwóch systemów funkcjonalnych: ofensywnych działań informacyjnych potencjalnego przeciwnika oraz działań defensywnych związku operacyjnego w tym wymiarze, tj. obrony informacyjnej. Badania prowadzono pod kątem identyfikacji czynników zagrożenia ofensywnymi środkami walki informacyjnej potencjalnego przeciwnika oraz określenia sposobów obrony informacyjnej w związku operacyjnym w odniesieniu do ogólnych funkcji badanych systemów – zdolności bojowej walczących stron. Przydatna okazała się analiza historyczna i uogólnienia. Po dokonaniu analizy faktów historycznych konfliktów i wojen lokalnych ostatnich lat wykazano, że w przyszłych działaniach obronnych związku operacyjnego istotne znaczenie może mieć wymiar informacyjny prowadzonych działań. W wyniku przeprowadzonych badań zdefiniowano miejsce i rolę obrony informacyjnej w działaniach obronnych związku operacyjnego, a także określono przedmiot, cel, zadania i jej ogólną strukturę.

Wykorzystano przy tym dostępne opracowania krajowe i zagraniczne, publikacje specjalistyczne, opracowania naukowe i prace studyjne oraz sprawozdania i raporty z konfliktu w rejonie Zatoki Perskiej i konfliktu bałkańskiego, które dotyczyły przedmiotu badań i jego otoczenia.

Hipotezę roboczą nr 2 zweryfikowano na podstawie indukcji, dedukcji, analogii, analizy (strukturalnej, systemowej i matematycznej), porównania i uogólnienia oraz pośredniej obserwacji naukowej. Dzięki zastosowanym metodom i narzędziom badawczym wykazano, że obrona informacyjna związku operacyjnego przed rozpoznaniem jest jednym z ważniejszych elementów zabezpieczenia jego działań zarówno w okresie pokoju, podczas kryzysu oraz w stanie wojny. Przeprowadzone badania struktury rozpoznania potencjalnego przeciwnika pozwoliły określić zakres obrony informacyjnej wojsk związku operacyjnego przed jego skutkami.

Ustalono, że składają się na nie odpowiednie przedsięwzięcia i działania podejmowane przez wojska w działaniach obronnych związku operacyjnego w ramach obrony informacyjnej przed rozpoznaniem bezpośrednim (tj. ochrona kontrwywiadowcza, maskowanie i ubezpieczanie) oraz w ramach ich obrony informacyjnej przed rozpoznaniem pośrednim przeciwnika (tj. obrona przed rozpoznaniem elektronicznym oraz obrona przed rozpoznaniem studyjnym).

W toku badań wykorzystano krajowe i zagraniczne wojskowe dokumenty normatywne, materiały naukowe i studyjne oraz opracowania dotyczące najbardziej reprezentatywnych systemów rozpoznawczych, prospekty reklamowe firm o zasięgu globalnym, materiały zamieszczone w Internecie, a następnie weryfikowano je w oparciu o opinie ekspertów oraz opinie zamieszczane w sprawozdaniach z ich użycia w konfliktach i wojnach lokalnych.

Hipotezę roboczą nr 3 zweryfikowano, podobnie jak hipotezę nr 2, na podstawie indukcji, dedukcji, analogii, analizy (strukturalnej, systemowej i matematycznej), porównania, uogólnienia i obserwacji naukowej. Zastosowane metody i narzędzia badawcze umożliwiły wykazanie, że obrona informacyjna związku operacyjnego przed zakłócaniem organizowana w warunkach postępującej automatyzacji oraz elektronizacji pola walki jest problemem wysoce złożonym oraz stanowi ważny element zabezpieczenia jego działań podczas kryzysu i w stanie wojny. Wykazano, że obronę informacyjną przed zakłócaniem w działaniach obronnych związku operacyjnego należy prowadzić różnymi sposobami i metodami. Składają się na nie odpowiednie przedsięwzięcia i działania podejmowane w ramach:

- obrony informacyjnej przed zakłócaniem zagłuszającym;
- obrony informacyjnej przed zakłócaniem dezinformującym;
- obrony informacyjnej przed zakłócaniem niszczącym;
- zabezpieczenia systemów dowodzenia i naprowadzania uzbrojenia przed niekompatybilnością elektromagnetyczną.

W toku badań, podobnie jak podczas weryfikacji hipotezy roboczej nr 2, wykorzystano krajowe i zagraniczne wojskowe dokumenty normatywne, materiały naukowe i studyjne oraz opracowania dotyczące najbardziej reprezentatywnych systemów dowodzenia, naprowadzania uzbrojenia, prospekty reklamowe firm o zasięgu międzynarodowym, materiały zamieszczone w Internecie, a następnie weryfikowano je w oparciu o opinie ekspertów zamieszczane w sprawozdaniach i relacjach z jego użycia w konfliktach i wojnach lokalnych.

Hipotezę roboczą nr 4 zweryfikowano na podstawie indukcji, dedukcji, analogii, analizy (strukturalnej, funkcjonalnej, logicznej), porównania i uogólnienia oraz bezpośredniej i pośredniej obserwacji naukowej, a także modelowania komputerowego[10] i symulacyjnego[11]. Dzięki zastosowanym metodom i narzędziom badawczym wykazano, że przedsięwzięcia

---

[10] Wykorzystano wyniki badań zamieszczone w: A. Barczak, J. Janczak, K. Mamcarz, „Komputerowy model oceny zagrożenia radioelektronicznego perspektywicznego systemu łączności związku operacyjnego wojsk lądowych". Praca naukowo-badawcza, wyd. WSOWŁ, Zegrze 1996.

[11] A. Barczak, J. Janczak, K. Mamcarz, „Model symulacyjny zagrożenia radioelektronicznego systemu łączności związku operacyjnego wojsk lądowych". Praca naukowo-badawcza, wyd. WSOWŁ, Zegrze 1997.

i różne formy działalności podejmowane w toku działań obronnych związku operacyjnego na potrzeby obrony informacyjnej realizowane są przez wielu wykonawców a jej planowanie i organizowanie odbywa się w sposób scentralizowany.

Określono, że odpowiedzialność za całokształt problematyki związanej z obroną informacyjną powinien ponosić dowódca, zaś organizatorem zadań w zakresie jej przygotowania i prowadzenia powinna być komórka G 2, przy znaczącym współudziale komórki G 3 oraz specjalistów rodzajów wojsk i służb.

Wykazano, że cykl decyzyjny na potrzeby obrony informacyjnej jest integralnym elementem procesu dowodzenia, realizowanym przez dowództwo i sztab związku operacyjnego, zgodnie z obowiązującymi procedurami i technikami.

Przedstawiono metodykę pracy sztabu związku operacyjnego oraz przykłady dokumentów opracowywanych na potrzeby obrony informacyjnej.

W toku badań wykorzystano zagraniczne wojskowe dokumenty standaryzacyjne, materiały z ćwiczeń prowadzonych w AON w latach 1997-2000, prace studyjne i materiały dydaktyczne zalecane w procesie dydaktycznym w AON, komputerowe i symulacyjne modele oceny zagrożenia oraz poglądy i opinie zamieszczane na łamach krajowych i zagranicznych periodyków wojskowych.

W **końcowym etapie badań** dokonano weryfikacji wyników badań w toku dyskusji i konsultacji naukowych ze specjalistami krajowymi i oficerami państw członków NATO przebywającymi w AON, podczas konferencji naukowych i seminariów. Rezultatem badań tego etapu jest opracowanie zwarte wraz z wnioskami. Ponadto autor zamierza wyniki badań opublikować w prasie specjalistycznej, poddać weryfikacji na kolejnych konferencjach naukowych, sympozjach i seminariach naukowych oraz wykorzystać do opracowania materiałów dydaktycznych na potrzeby AON i innych placówek dydaktycznych sił zbrojnych RP.

Praca studyjna zawiera wyniki badań istoty, pożądanego zakresu i treści przedsięwzięć obrony informacyjnej w działaniach obronnych związku operacyjnego, miejsca obrony informacyjnej w strukturach procedur pracy sztabowej oraz przebiegu cyklu decyzyjnego pod kątem jej potrzeb na stanowisku dowodzenia związku operacyjnego odnieść również do innych rodzajów sił zbrojnych. Praca studyjna składa się z wstępu, czterech rozdziałów merytorycznych, zakończenia, bibliografii i załączników.

We **wstępie** uzasadniono potrzebę wyboru i konieczność rozwiązania problemu naukowego. Przedstawiono również podstawy metodologiczne, niezbędne do przeprowadzenia badań. Szczególną uwagę zwrócono na cel i zakres badań, metody badawcze, które doprowa-

dziły do weryfikacji hipotez roboczych i osiągnięcia celu badań, oraz ocenę dostępnej literatury przedmiotu badań.

W **rozdziale pierwszym** przedstawiono istotę obrony informacyjnej w działaniach obronnych związku operacyjnego. Analizując dorobek najbardziej reprezentatywnych sił zbrojnych innych państw oraz krystalizujące się stanowisko NATO, określono jej rolę i miejsce w przyszłych działaniach obronnych związku operacyjnego oraz sprecyzowano przedmiot, cel i zadania.

Rozdział drugi obejmuje pożądany zakres i treść przedsięwzięć obrony informacyjnej przed rozpoznaniem (bezpośrednim i pośrednim) w działaniach obronnych związku operacyjnego. W badaniach obrony informacyjnej przed rozpoznaniem bezpośrednim w działaniach obronnych związku operacyjnego wyróżniono ochronę kontrwywiadowczą, maskowanie oraz ubezpieczenie. Natomiast w obronie informacyjnej przed rozpoznaniem pośrednim (elektronicznym i studyjnym) w działaniach obronnych związku operacyjnego skupiono uwagę przede wszystkim na maskowaniu elektronicznym (radioelektronicznym, radiolokacyjnym, optoelektronicznym, czujnikowym i informatycznym). Rozważania teoretyczne i kalkulacje zostały zilustrowane na rysunkach i wykresach, które zamieszczono w załącznikach.

W **rozdziale trzecim** zamieszczono wyniki badań obejmujące pożądany zakres i treść przedsięwzięć obrony informacyjnej przed zakłócaniem w działaniach obronnych związku operacyjnego. Szczególną uwagę zwrócono na obronę systemów dowodzenia i naprowadzania uzbrojenia związku operacyjnego przed zakłócaniem zagłuszającym, zakłócaniem dezinformującym i zakłócaniem niszczącym przeciwnika oraz na zabezpieczenie ich przed niekompatybilnością elektromagnetyczną.

W **rozdziale czwartym** opracowano pożądany przebieg procesu decyzyjnego pod kątem potrzeb obrony informacyjnej w działaniach obronnych związku operacyjnego.

Sprecyzowano odpowiedzialność funkcyjną za obronę informacyjną w związku operacyjnym, określono zadania poszczególnych zespołów funkcjonalnych sztabu w zakresie jej realizacji. Szczególną uwagę zwrócono na przebieg pożądanego cyklu decyzyjnego w zakresie obrony informacyjnej w działaniach obronnych związku operacyjnego oraz formę i treść niezbędnych dokumentów planistycznych i rozkazodawczych. Przykłady dokumentów zilustrowano graficznie oraz zamieszczono w załącznikach.

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

Wyniki badań zamieszczone w pracy studyjnej są adresowane głównie do pracowników naukowych instytucji wojskowych i cywilnych zajmujących się tą problematyką, pracowników dydaktycznych i studentów uczelni wojskowych oraz kadry dowódczo-sztabowej wojsk lądowych, a w części dotyczącej nowych rozwiązań technicznych i organizacyjnych – do osób funkcyjnych Sztabu Generalnego WP, Dowództwa Wojsk Lądowych, sztabów związków operacyjnych oraz wszystkich instytucji mających udział w rozwoju myśli i techniki wojskowej.

1. ISTOTA OBRONY INFORMACYJNEJ W DZIAŁANIACH OBRONNYCH ZWIĄZKU OPERACYJNEGO

1.1. Rola i miejsce obrony informacyjnej w poglądach na prowadzenie działań obronnych związku operacyjnego

Postęp naukowo-techniczny prowadzi do przeobrażeń w wielu dziedzinach życia społecznego. Jest również czynnikiem sprawczym rozwoju nowych środków walki i sposobów prowadzenia działań wojennych. W przeszłości osiągnięcia technologiczne wykorzystywane były przede wszystkim w celu zwiększenia siły (mocy) i skuteczności rażenia wojsk. Imponujące osiągnięcia u schyłku drugiego tysiąclecia w dziedzinie elektroniki, a przede wszystkim rozwój technologii komputerowych i teleinformatycznych spowodował, że główną wartością cywilizacji XXI wieku staje się informacja oraz systemy jej zdobywania, przetwarzania i dystrybucji. Każda sfera funkcjonowania wojsk staje się coraz bardziej zależna od informacji. Informacja i technologie cyfrowe tworzą bowiem tak synergiczny efekt pomiędzy działającymi systemami, modularnymi strukturami organizacyjnymi wojsk i ich komponentami, że – jak przewidują futurolodzy – możliwości wojsk zostaną niebawem zwiększone wielokrotnie. Postępowi temu towarzyszyć będą jednak i nowe zagrożenia. Są podstawy, aby sądzić, iż niewiele osób w naszym kraju dostrzega ten problem. Problem dotyczy walki informacyjnej, ukierunkowanej nie tylko na bezpośrednie zniszczenie przeciwnika, ale przede wszystkim na osiągnięcie celów politycznych bez prowadzenia działań wojennych. Osiągnąć to można w wyniku zdecydowanego złamania woli przeciwnika do przeciwstawiania się, sparaliżowania w początkowym okresie wojny jego organów kierowania państwem i siłami zbrojnymi i tym samym zmuszenia go do pełnej i bezwarunkowej kapitulacji.

Jak wynika z analizy literatury przedmiotu badań, idea strategii tzw. „działań pośrednich" nie jest nowa. Już w V w.p.n.e. chiński teoretyk wojskowy Sun Tzu[1] pisał: : *„Najwyższą sztuką jest zwyciężać armię wroga bez wydania bitwy. Zająć miasta wroga bez oblegania*

[1] Sun Tzu: „Sztuka wojny", wyd. Przedświt, Warszawa 1994, s. 37.

i zająć tereny jego państwa bez inwazji". Niektórzy nasi teoretycy wojskowi, słusznie – zdaniem autora – sądzą, że historia walki informacyjnej jest tak samo długa jak historia prowadzonych dotychczas wojen[2]. Jej rola została w pełni ujawniona podczas wojny w rejonie Zatoki Perskiej[3], gdzie koalicjanci antyiraccy, przede wszystkim Amerykanie, zastosowali na szeroką skalę nowe technologie informacyjne. Pod koniec konfliktu w strefie działań wojennych funkcjonowało ponad trzy tysiące komputerów. Telewidzowie na całym świecie mogli oglądać działanie samolotów, dział i czołgów w obszarze działań wojennych, lecz nie widzieli nieuchwytnego przepływu danych, nieodzownych do wykonania najzwyklejszych funkcji wojskowych. Po wojnie tej ujawniono nową kategorię walki, którą przyjęto nazwać zamiennie walką informacyjną, działaniami informacyjnymi bądź operacjami informacyjnymi.

Z analizy obecnie dostępnych **amerykańskich dokumentów doktrynalnych**[4] wynika, że operacje (działania) informacyjne (ang. Information Operations) – które w czasie wojny nazywane mogą być wprost walką informacyjną – są definiowane jako ciągłe działanie sił zbrojnych w ramach wojskowego środowiska informacyjnego[5]. Przyczyniają się one do zwiększenia możliwości sił własnych w zakresie zdobywania, przetwarzania i przekazywania danych w celu uzyskania przewagi w całym spektrum walki zbrojnej, prowadzonej wewnątrz globalnego środowiska informacyjnego[6]. Jednocześnie ukierunkowane są na obniżenie możliwości w tym zakresie strony przeciwnej.

Celem operacji informacyjnych jest bowiem oddziaływanie na systemy i zasoby informacyjne przeciwnika, a jednocześnie obrona własnych systemów i zasobów przed oddziaływaniem informacyjnym przeciwnika. Dlatego przewiduje się prowadzenie dwóch rodzajów operacji informacyjnych, a mianowicie działania informacyjne ofensywne i działania informacyjne defensywne.

---

[2] L. Ciborowski: „Walka informacyjna", wyd. ECE, Toruń 1999.

[3] „Wojna w rejonie Zatoki Perskiej w 1991 r., nazywana również konfliktem „Pustynna Burza" była wojną, podczas której uncja krzemu w komputerze przyniosła większe efekty niż tona uranu". A. D. Campen: „The first Information War", ed. AFCA International Press Fairfax, Virginia 1992.

[4] W sierpniu 1996 r. Dowództwo Szkolenia i Doktryn TRADOC (ang. Training and Doctrine Command) opublikowało „Regulamin walki sił lądowych USA" (FM–100–6 zawierający m. in. doktrynę (koncepcję) działań (operacji) informacyjnych – ang. Joint Doctrine for Information Operations (Joint Pub 3-13.) oraz doktrynę (koncepcję) walki o przewagę w dowodzeniu – ang. Joint Doctrine for Command & Control Warfare – C2W (Joint Pub 3 – 13.1.).

[5] Wojskowe środowisko informacyjne MIE (ang. Military Information Environment) składa się z systemów informacyjnych i organizacji sił własnych i przeciwnika, zarówno militarnych, jak i pozamilitarnych, które wspierają i wpływają decydująco na działania bojowe wojsk [57].

[6] Globalne środowisko informacyjne GIE (ang. Global Information Environment) – to wszystkie systemy informacyjne (indywidualne, połączone i wojskowe) oraz media i organizacje, które zbierają, opracowują i przekazują wiadomości dla rządów, wojsk, i przedstawicielstw [57].

Eksponuje się również rolę synergicznego efektu obu rodzajów działań w wyniku ich synchronizacji i koordynacji. Zapewnienie synergizmu jest regulaminowym obowiązkiem naczelnych organów odpowiedzialnych za bezpieczeństwo państwa oraz dowódców ogólnowojskowych związków operacyjnych i taktycznych.

Informacyjne działania ofensywne obejmują:

- osłonę działań (ang. Operations Security);
- operacje (działania) psychologiczne (ang. Psychological Operations);
- pozoracje (pozoracje operacyjną, wprowadzanie w błąd) wojskową (ang. Military Deception);
- walkę elektroniczną (ang. Electronic Warfare);
- niszczenie (atak fizyczny) / destrukcję systemów informacyjnych przeciwnika (ang. Physical Attack / Destruction);
- atak informatyczny (ang. Computer Network Attack);
- instytucje rzecznika prasowego i kontaktów z ludnością (ang. Public, Civil Affairs).

Przewiduje się, że poszczególne elementy składowe, będące przedmiotem ostatnich analiz oraz rozważań teoretycznych naszych specjalistów [24;25;26;30;45;96], a także wystąpień na konferencjach naukowych[7] ujmowane będą w planach operacyjnych jako mechanizmy osiągania celów operacji informacyjnych (manipulowanie decyzjami przeciwnika, obezwładnianie zakłóceniami lub zniszczenie jego systemu dowodzenia). Zgodnie z założeniami doktryny, operacje (działania) informacyjne mogą być główne lub wspomagające. Udział poszczególnych mechanizmów działań (elementów składowych) również uzależnia się od szczebla dowodzenia oraz charakteru i stopnia zagrożeń.

Doktrynalnym celem **informacyjnych operacji defensywnych** jest osłanianie i obrona własnego potencjału informacyjnego[8] przed działaniami przeciwnika.

---

[7] J. Janczak: „Walka informacyjna na współczesnym polu walki." Referat w materiałach VII Międzynarodowej Konferencji Telekomunikacji i Informatyki, cz. 1, Zegrze 1998.

[8] Na potencjał informacyjny jako czynnik potencjału militarnego wg Amerykanów składa się:

– utrwalona wiedza faktograficzna (instytucjonalna) związana z wszelkimi czynnikami tego potencjału, tj. aktualne położenie i działania wojsk przeciwnika, jego zamiary (strategiczne, operacyjne, taktyczne), parametry taktyczno-techniczne uzbrojenia i in.;

– utrwalona wiedza uogólniona, a szczególnie wyniki badań związane z obronnością, nowe technologie, metody rozwiązywania problemów operacyjno-taktycznych, metody oceny sytuacji i podejmowania decyzji, i in.;

– ludzie zaangażowani w procesach informacyjnych, tj. zespoły dowódczo-sztabowe, zespoły realizujące prace badawczo rozwojowe i in.;

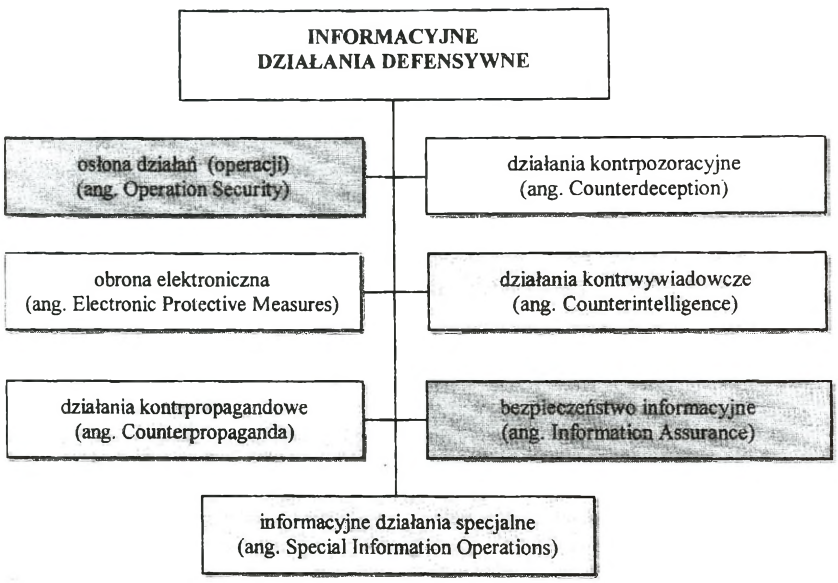
– infrastruktura informacyjna obejmująca sieci sensorowe, telekomunikacyjne, informatyczne, teleinformatyczne i inne związane z bezpieczeństwem państwa i funkcjonujące w ramach systemów C^4I^2/ EW (ang. Computerised, Command, Control, Communication, Intelligence, Interoperability and Electronic Warfare);

– infrastruktura pozamilitarnych segmentów funkcjonowania państwa, tj. administracji państwowej, terenowej, telekomunikacji, transportu, zaplecza naukowo-badawczego i in. [124].

Zakłada się, że działania te są bardzo ważne, mają charakter ciągły i obejmują cztery fazy:

- osłonę środowiska informacyjnego (ang. Information Environment);
- wykrycie ataku (ang. Attack Detection);
- odtwarzanie potencjału (ang. Capability Restoration);
- kontratak (ang. Attack Response).

Podział informacyjnych operacji (działań) defensywnych według poglądów amerykańskich zilustrowano na rysunku 1.1.



Rys. 1.1. Podział informacyjnych operacji (działań) defensywnych wg poglądów amerykańskich

Zadania defensywne wykonywane w ramach osłony działań (operacji) są ściśle powiązane z zadaniami ofensywnymi i mają na celu ukrycie przed przeciwnikiem tych informacji o stanie i możliwościach wojsk własnych oraz zamiarach dowódcy, które warunkują podejmowanie przez niego racjonalnych decyzji. Zakłada się wydłużanie w ten sposób cyklu dowodzenia przeciwnika oraz uniemożliwienie zdobywania przez jego organy rozpoznawcze wiarygodnych danych. Podstawą planowania działań osłonowych jest rozpoznanie kontrwywiadowcze, a zasadnicze działania polegają na blokowaniu informacji o ruchu wojsk.

Zdaniem specjalistów amerykańskich zadania defensywne wykonywane w ramach działań psychologicznych mają na celu oddziaływanie na zachowanie określonych środowisk, grup lub osób przez kontrolowane wpływanie na emocje, motywy działania, percepcje rzeczywistości i rozumowanie. Stosowane mechanizmy uzależnione są od szczebla dowodzenia. Na szczeblu operacyjnym najlepiej sprawdzają się lokalne media. Na szczeblu taktycznym mogą wchodzić w grę również polowe środki propagandowe. W operacjach informacyjnych działania psychologiczne stanowią element pomocniczy i z reguły są traktowane jako wspomagające ważniejsze operacje pozoracyjne.

Amerykanie przyjmują, że zadania defensywne wykonywane w ramach działań kontrpozoracyjnych mają na celu wpływanie na proces decyzyjny przeciwnika przez utrudnianie dostarczania jego systemowi rozpoznawczemu danych niepewnych, bądź nieprawdziwych. Celem operacyjnym tych działań jest przygotowanie takich strumieni wiadomości, aby przeciwnik podejmował działania zgodne ze scenariuszem zaplanowanym przez drugą stronę. Skuteczne kontrpozorowanie w skali operacyjnej jest kosztowne ze względu na konieczność angażowania dodatkowych wojsk i środków walki.

Zadania defensywne wykonywane w ramach obrony elektronicznej mają na celu przeciwdziałanie skutkom ataku elektronicznego przeciwnika oraz ochronę przed wykorzystaniem przez niego widma elektromagnetycznego w celach wywiadowczych lub do naprowadzania środków rażenia. Szczególnym zadaniem obrony elektronicznej jest zapobieganie również skutkom własnych działań elektronicznych (zakłóceniom interferencyjnym).

Założenia doktrynalne działań kontrwywiadowczych reguluje u Amerykanów oddzielna doktryna[9], natomiast informacyjne działania specjalne podlegają procedurom niejawnym. Praktycznie obejmują wszystkie operacje skierowane przeciw ofensywnej walce informacyjnej przeciwnika.

Zadania defensywne wykonywane w ramach działań kontrpropagandowych są realizowane – zdaniem Amerykanów – przede wszystkim przez instytucje rzecznika prasowego i kontaktów z ludnością. Ich rola w operacjach informacyjnych jest pomocnicza i podporządkowana celom operacji psychologicznych.

Zadania wykonywane w ramach bezpieczeństwa informacyjnego są szczególnym obszarem działania amerykańskich komórek kierowania walką informacyjną w operacjach de-

[9] Joint Doctrine and Tactics, Techniques and Procedures for Counterintelligence Support to Operations, Joint Pub 2-01.2.

fensywnych. Bezpieczeństwo informacyjne ma wielosegmentową strukturę, obejmującą następujące składniki:

– legalizację (ang. Authentication) – możliwość weryfikacji źródła wiadomości, autorstwa dokumentu;

– niezaprzeczalność, nioedrzucalność (ang. Nonrepudiation) – możliwość udowodnienia udziału, np. autorstwa, nadania, odbioru i in.;

– dostępność (ang. Availability) – gwarancja udostępnienia wiadomości (dokumentu) każdemu upoważnionemu;

– poufność (ang. Confidentiality) – gwarancja niedostępności wiadomości (dokumentu) dla osób nieupoważnionych;

– integralność (ang. Integrity) – gwarancja ochrony przed zmianami nieautoryzowanymi.

Badania wykazały, że w amerykańskiej doktrynie działań (operacji) informacyjnych położono szczególny nacisk na systematyczne prowadzenie analizy podatności systemów informacyjnych na działania ofensywne różnych podmiotów (nie tylko przeciwnika politycznego, militarnego), oceny ich bezpieczeństwa i planowanie potrzeb. Akcentuje się, że dowódcy oraz sztaby mają obowiązek wykorzystywania do tego celu modeli symulacyjnych i innych narzędzi zaawansowanych technologii z dziedziny bezpieczeństwa informacyjnego INFOSEC (ang. Information Security). Dzielą się one na dwie grupy: COMPUSEC (ang. Computer Security) i COMSEC (ang. Communication Security). Pierwsza z nich obejmuje metody, techniki i procedury bezpieczeństwa w odniesieniu do sprzętu i oprogramowania. Druga dotyczy infrastruktury telekomunikacyjnej. Problematyka ta ma na celu zapewnienie obrony informacyjnej własnych systemów informacyjnych i ich zasobów zgromadzonych w bazach danych.

Zachodni specjaliści NATO określają walkę informacyjną jako rodzaj walki zbrojnej, ukierunkowanej na osiągnięcie przewagi nad przeciwnikiem w wymiarze informacyjnym. Obecnie w środowiskach wojskowych NATO toczy się coraz szersza dyskusja[10] nad problemem zagrożeń wynikających z oddziaływania na systemy i zasoby informacyjne, jako że wiedza faktograficzna i proceduralna dowódców i ich podwładnych z notatek, ksiąg i sejfów została przeniesiona do baz danych i oprogramowania komputerów, a uzależnienie od ciągłości i pewności obiegu informacji stało się czynnikiem krytycznym. Wojskowi teoretycy oraz

[10] Odbyła się ona m. in. na międzynarodowym sympozjum zorganizowanym przez holenderską Królewską Akademię Militarną w grudniu 1999 r., którego myślą przewodnią było „ Informacja jako środek, obiekt ataku i broń. Działania informacyjne co to oznacza?"

praktycy NATO pracują nad koncepcjami i doktrynami działań (operacji) informacyjnych[11]. Działania informacyjne są definiowane jako *„przedsięwzięcia podejmowane w celu wywarcia wpływu na decydentów w ramach wsparcia politycznych i militarnych celów poprzez oddziaływanie na procesy informacyjne innych oraz systemy dowodzenia, kontroli, łączności i informatyczne, przy wykorzystaniu i ochronie własnych systemów oraz procesów informacyjnych".*

W zależności od charakteru prowadzonych operacji wyszczególnia się dwie kategorie działań informacyjnych: defensywne i ofensywne. **Defensywne działania informacyjne** uznaje się za priorytetowe. Przewiduje się – podobnie jak przyjmują specjaliści amerykańscy – następujące ich formy (rysunek 1.1.): osłonę działań (operacji) defensywnych; działania kontrpozoracyjne; działania kontrpropagandowe; działania kontrwywiadowcze; obronę elektroniczną; informacyjne działania specjalne; bezpieczeństwo informacyjne. Zakłada się, że działania te powinny być wspierane przez działania ofensywne, szczególnie w zakresie ochrony środowiska informacyjnego, wykrywania ataków na systemy informacyjne oraz odpowiadania na nie.

Przyjmuje się, że **informacyjne działania ofensywne** powinny obejmować – podobnie jak przyjmują Amerykanie – między innymi: osłonę działań, dezinformację wojskową, działania psychologiczne, walkę elektroniczną, fizyczne niszczenie i atak na sieci komputerowe.

Ze względu na naturę Sojuszu przewiduje się prowadzenie ofensywnych działań informacyjnych w pełnym wymiarze tylko w czasie wojny. W sytuacji kryzysowej przewiduje się ograniczony ich zakres, gdyż wymaga to konsensusu wszystkich suwerennych jego członków, a niektóre ofensywne działania informacyjne uznawane są w wielu państwach za nielegalne. Podkreśla się, że prowadzenie działań ofensywnych w czasie pokoju, jeśli uznano by je za celowe, może być traktowane jako prowokacja lub wrogi akt i dlatego wymaga wyraźnej autoryzacji politycznej przez Radę Północnoatlantycką.

W NATO przewiduje się prowadzenie działań informacyjnych na szczeblu strategicznym, operacyjnym i taktycznym. W zależności od szczebla powinny one stanowić wsparcie działań NATO, wspieranie kampanii w osiąganiu głównych celów operacyjnych oraz wspieranie walk w osiąganiu poszczególnych celów taktycznych. Postuluje się, by działania informacyjne były stałym elementem planowania operacyjnego. A niektóre ich formy, przede

---

[11] Dokument MC 422 pt. „NATO Information Operations Policy"- zaaprobowany przez Komitet Wojskowy NATO 15.12.1998.

wszystkim defensywne (obronne), powinny być stosowane ciągle, tj. od pokoju poprzez kryzys, wojnę i z powrotem do pokoju.

W siłach zbrojnych głównych państw nie należących do NATO np. Federacji Rosyjskiej duże nadzieje pokłada się w informacyjnym oddziaływaniu na przeciwnika i w innych rodzajach „nieśmiercionośnej broni". Specjaliści rosyjscy uważają, że istotą trwającej obecnie „czwartej rewolucji" w sztuce wojennej jest wywalczenie panowania nad przeciwnikiem w dziedzinie informacyjnej[12]. Oznacza to dążenie do stwarzania sytuacji, w której nie tylko baza informacyjna wojsk własnych, ale również cała infrastruktura państwowa stanie się pełniejsza, dokładniejsza, wiarygodniejsza i aktualniejsza niż przeciwnika. W sferze pozawojskowej potrzeba ta argumentowana jest dynamicznym rozwojem bazy informatycznej i nowoczesnych systemów łączności[13]. W sferze wojskowej natomiast koronnym argumentem jest przekonanie, że walka informacyjna umożliwia osiągnięcie zwycięstwa bez potrzeby prowadzenia wyniszczającej i przez to bardzo kosztownej walki zbrojnej. Rosjanie uważają, że w ramach przygotowywania się do tej walki należy w pierwszej kolejności zintegrować wszelkie działania paraliżujące swobodę decyzyjną przeciwnika[14]. Analiza doświadczeń z wojny w rejonie Zatoki Perskiej uświadomiła Rosjanom, że postęp w informacyjnym wsparciu walki zbrojnej zmusza do wydzielenia walki informacyjnej jako samodzielnej dyscypliny sztuki wojennej. W prezentowanych poglądach[15] potrzeba podjęcia tego problemu w siłach zbrojnych argumentowana jest głównie: wzrastającą informatyzacją sił zbrojnych, wzrostem możliwości funkcjonalnych współczesnych systemów łączności, zwiększającym się nasyceniem wojsk nowoczesnymi środkami rozpoznania i coraz częstszym stosowaniem broni precyzyjnego rażenia.

W następstwie tego na początku lat dziewięćdziesiątych zintegrowano już organizacyjnie szereg funkcjonalnych elementów pola walki, w tym szczególnie: ogień, walkę radioelektroniczną, maskowanie operacyjne i strategiczne oraz operacje psychologiczne. Materialnym faktem nadania priorytetu walce informacyjnej stało się powołanie przy urzędzie prezy-

---

[12] Rosjanie twierdzą, że ogniowe środki precyzyjnego rażenia, niejądrowe środki ogniowe do wykonywania głębokich uderzeń i systemy integrujące rewolucjonizują wszystkie aspekty sztuki wojennej i struktur organizacyjnych sił zbrojnych. Twierdzą, że technika informacyjna jest „najważniejszą bronią XXI wieku", a pod względem skuteczności oddziaływania jest porównywana z bronią masowego rażenia [74].

[13] W ramach tego wymieniana jest automatyzacja i komputeryzacja szeregu sfer życia gospodarczego, upowszechnienie systemów łączności cyfrowej, istnienie licznych i różnorodnych baz danych i masowy charakter wykorzystywania komputerów osobistych.

[14] W odniesieniu do sił zbrojnych chodzi o włączenie w zakres walki informacyjnej pozorowania i maskowania, które do tej pory realizowane były według odrębnych planów.

[15] „Poglądy rosyjskich specjalistów na przyszłą wojnę" [w:] Military Review 7/94.

denta Federacji Rosyjskiej Kolegium Federalnej Agencji Łączności i Informacji. Instytucję tę upoważniono prawnie do prowadzenia walki informacyjnej w wymiarze strategicznym.

Generalnie, walka informacyjna lokowana jest przez Rosjan w środowisku funkcjonalnym mieszczącym się pomiędzy wojną „zimną" i „gorącą". Podkreślają, że w porównaniu do zimnej wojny, w której długofalowo stosowane instrumentarium ukierunkowane było na uzyskiwanie głównie określonych efektów ekonomicznych, walka informacyjna jest w stanie spełniać te funkcje, z tą jednak różnicą, że jej efekty mogą być osiągane nie długofalowo, ale prawie natychmiast. Umiejętnie realizowana może doprowadzać do natychmiastowego zrywania wielu żywotnych funkcji współczesnej infrastruktury cywilnej i wojskowej przeciwnika[16]. Rosyjscy specjaliści wojskowi wyróżniają następujące **sposoby** walki informacyjnej[17]: siłową, intelektualną, kombinowaną.

Do kategorii siłowej zaliczają sposoby oparte na prowadzeniu walki informacyjnej różnymi rodzajami ofensywnego uzbrojenia, np. konwencjonalnego, radioelektronicznego, informatycznego. Wykorzystanie sposobów siłowych pozwala – ich zdaniem – uzyskać ilościową przewagę informacyjną, niezbędną do realizacji zadań dowodzenia wojskami i naprowadzania uzbrojenia.

Intelektualne sposoby walki informacyjnej umożliwiają – ich zdaniem – kierowanie działaniami przeciwnika bez użycia siły. Ich zastosowanie pozwala osiągnąć przewagę informacyjną w jakości informacji wykorzystywanej w dowodzeniu wojskami i naprowadzaniu uzbrojenia.

Kombinowane sposoby walki informacyjnej dotyczą osiągania przewagi informacyjnej zarówno w ilości, jak i jakości informacji w dowodzeniu wojskami i w kierowaniu środkami walki.

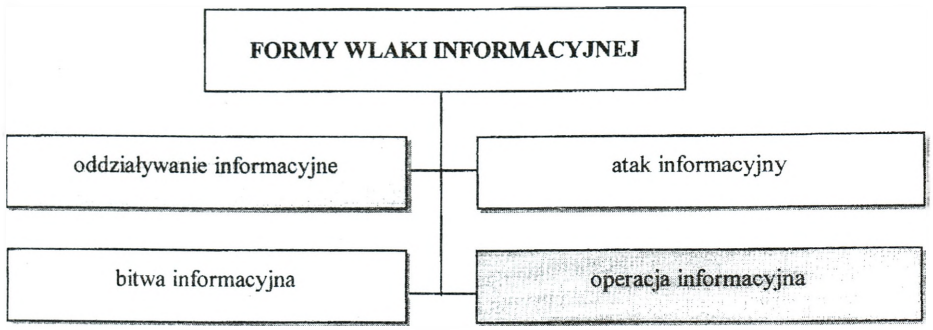
Rosjanie wyróżniają odpowiednie formy prowadzenia walki informacyjnej, które zilustrowano na rysunku 1.2.

Oddziaływanie informacyjne definiują jako zorganizowane użycie sił i środków walki informacyjnej do realizacji zadań mających na celu wywalczenie (utrzymanie) przewagi informacyjnej nad przeciwnikiem.

---

[16] Rosjanie dysponują na przykład niewielkimi urządzeniami dostosowanymi do generowania potężnych impulsów elektromagnetycznych (do 100 MJ) drogą konwencjonalną, które na bardzo dużych obszarach mogą niszczyć wszelkie urządzenie elektroniczne i energetyczne.

[17] S.A. Komow „O sposobach i formach viedienija informacionnoj bor'by", [w:] Vojennaja. Mysl' nr 4, 1997, s. 18 – 22.



Rys. 1.2. Formy prowadzenia walki informacyjnej wg poglądów rosyjskich

Atak informacyjny określają jako całokształt aktywnych informacyjnych oddziaływań sił i środków samodzielnych pododdziałów na element lub grupę elementów systemów informacyjnych dla realizacji szczególnych zadań taktycznych walki informacyjnej.

Bitwa informacyjna, to – zdaniem Rosjan – całokształt różnorodnych oddziaływań informacyjnych i ataków połączonych wspólnym zamiarem, prowadzonych przez specjalnie wydzielone siły i środki ukierunkowane na realizację wspólnego zadania walki informacyjnej.

Operacja informacyjna definiowana jest przez Rosjan jako całokształt uzgodnionych co do celu oddziaływań informacyjnych, ataków i bitew prowadzonych według wspólnego zamiaru i planu dla realizacji zadań walki informacyjnej na kierunku operacyjnym lub na teatrze działań wojennych.

Przyjmuje się, że dla osiągnięcia celów informacyjnych oddziaływań, ataków, bitew i operacji mogą być stosowane wszystkie dostępne sposoby walki informacyjnej, a przede wszystkim:

- uzyskiwanie przewagi nad przeciwnikiem w dziedzinie wywiadu i rozpoznania wojskowego;
- stosowanie zakłócania informacyjnego powodującego paraliżowanie rozpoznawczych systemów informacyjnych, jak również procesów kierowania państwem i dowodzenia wojskami oraz szerzenie w jego szeregach i społeczeństwie demoralizacji stanów osobowych i dezorganizacji życia;
- neutralizowanie przewagi przeciwnika w sferze łączności i informatyki;
- zrywanie procesów informacyjnych przeciwnika oraz obezwładnianie zakłóceniami i niszczenie jego systemów informatycznych i zasobów baz danych;

– wprowadzanie przeciwnika w błąd oraz dezorganizowanie i niszczenie jego infrastruktury informacyjnej;

– wprowadzanie zamieszania i dezorganizowanie lub całkowite zrywanie procesów kierowania państwem i dowodzenia wojskami, szczególnie na wyższych szczeblach dowodzenia[18];

– stwarzanie warunków do szybkiego neutralizowania oporu przeciwnika;

– ochrona własnych, a także sojuszniczych systemów informacyjnych oraz systemów dowodzenia wojskami i kierowania państwem przed rozpoznaniem i wszelkimi działaniami destrukcyjnymi przeciwnika.

Prezentowane są przekonania, że osiągnięcie wymienionych celów powinno skłonić każdego przeciwnika do zrezygnowania z zamiarów prowadzenia klasycznej wojny[19]. Brak realnych perspektyw osiągnięcia taniego sukcesu powinien działać odstraszająco. Uwzględnia się jednak, że jeśli odstraszająca funkcja rosyjskiej walki informacyjnej zawiedzie, to w takiej sytuacji zastosowane zostaną wszystkie inne dostępne metody i środki tej walki służące osiągnięciu zwycięstwa.

Rosjanie zamierzają osiągać wyznaczone na poszczególnych etapach cele walki informacyjnej następującymi **metodami**:

– w okresie pokoju – przez systematyczne stosowanie odstraszania informacyjnego w sferze elektronicznej;

– w okresie kryzysu – przez zmasowane oddziaływania elektroniczne na selektywnie wybrane procesy informacyjne przeciwnika związane z kierowaniem państwem i dowodzeniem wojskami;

– w okresie konfliktu zbrojnego – przez zmasowane użycie wszystkich środków walki informacyjnej, zarówno w odniesieniu do sfery wojskowej, jak i cywilnej przeciwnika[20].

Rosjanie uważają, że współcześnie uzyskanie przewagi w sferze militarnej związane jest bezwzględnie z uzyskaniem dominacji przede wszystkim w kierowaniu państwem, dowodzeniu wojskami oraz w łączności i rozpoznaniu. Co się zaś tyczy bezpośrednio wojska, to zakładają, że najpierw należy uzyskać przewagę i panowanie „w eterze", następnie w powietrzu i przestrzeni kosmicznej, a dopiero w ostatniej kolejności należy uwzględniać użycie potencjału lądowego.

---

[18] Należy sądzić, że w tym zakresie przewidywane jest stosowanie techniki umieszczonej w przestrzeni kosmicznej.

[19] Przewidują, że groźba spowodowania nieodwracalnych szkód w zasobach informacyjnych państwa i w strukturach pozapaństwowych staje się nowym czynnikiem odstraszania w skali globalnej.

[20] Zakładają również użycie środków ogniowych.

W rekapitulacjach tego podkreślają, że współczesne konflikty zbrojne powinny być postrzegane przez pryzmat jakości i zakresu zespolenia ognia i elektroniki ze składową informacyjną[21]. Mocno też podkreślają, że każdy z tych elementów składowych ma własne i specyficzne li tylko dla niego cele, środki i metody działania[22].

Również **nasi teoretycy wojskowi**[23] przyjmują, że współczesny model walki zbrojnej obejmuje trzy zasadnicze czynniki: rażenie (ogień), manewr (ruch) i informację. Informację postrzega się jako czynnik kluczowy na współczesnym polu walki.

Uważa się, że określenie właściwych zależności między czynnikami operacyjnymi[24] zdeterminowane jest posiadaniem informacji dotyczących przeciwnika i sił własnych, obszaru i czasu ich działania. Należy mieć na uwadze, że o wartości informacji decydują: jej treść, wiarygodność i aktualność. Nie chodzi jednak o to, aby wiedzieć wszystko, lecz by wiedzieć wystarczająco dużo, a przede wszystkim więcej niż przeciwnik. Informacja lub jej brak jest czynnikiem decydującym o sukcesie lub porażce. Jest zasadniczym warunkiem umożliwiającym prowadzenie działań, a w określonych sytuacjach staje się czynnikiem samodzielnie decydującym o ich powodzeniu. Starcie dwóch stron jest obecnie w pierwszej kolejności walką o informację. Aby zatem zwyciężyć należy wygrać walkę w sferze informacyjnej (walkę informacyjną).

Walka informacyjna[25] – 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 (rysunek 1.3.).

---

[21] Podkreślają przy tym, że współczesna droga do sukcesu bojowego bardzo kontrastuje z rozwiązaniami stosowanymi w czasie pierwszej i drugiej wojny światowej. Twierdzą, że anachronizmem byłoby dziś przedkładanie ponad walkę informacyjną działalności wojsk lądowych, co było słuszne w czasie pierwszej wojny światowej lub sił powietrznych, co z kolei było najważniejsze w czasie drugiej wojny światowej.

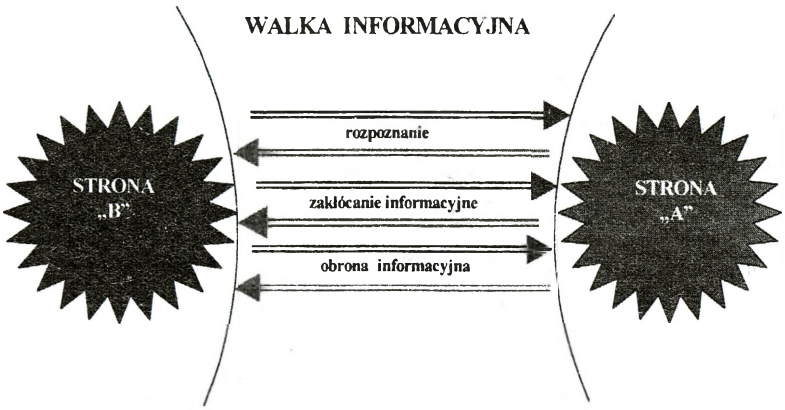
[22] Przez sprzężenia ognia i elektroniki Rosjanie rozumieją równoczesne stosowanie jednych i drugich środków walki. Ich zdaniem może powodować to jednoczesne niszczenie techniki bojowej i siły żywej przeciwnika.
W składowej informacyjnej lokują przede wszystkim możliwości zdobywania danych i ich wykorzystywania w procesie dowodzenia wojskami i naprowadzania uzbrojenia. Z tymi przedsięwzięciami wiążą zwiększenie skuteczności środków ogniowych i walki elektronicznej. Różne formy walki informacyjnej zostały wykorzystane w czasie drugiego konfliktu czeczeńskiego w 1999 r. W wyniku czego działaniom sił zbrojnych na Północnym Kaukazie towarzyszyła aprobata mediów i przyzwolenie Rosjan. Nie znalazły się, w odróżnieniu od konfliktu w latach 1994 – 96, znaczące siły na arenie międzynarodowej, które potępiałyby działania militarne w zbuntowanej republice.

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

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

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

Lokują oni walkę informacyjną – z uwagi na jej charakter – w grupie walk niezbrojnych[26], gdyż jej prowadzenie nie jest bezpośrednio związane z fizycznym niszczeniem i zagrożeniem życia. Powinna być, więc prowadzona wespół z innymi walkami, nie może występować w oderwaniu, bo nigdy też sama dla siebie nie może stanowić celu. Jej cel wynika z celu walki wspieranej.



Rys. 1.3. Ogólny model walki informacyjnej

Rozpatrując walkę informacyjną w aspekcie funkcjonalnym, traktują ją jako pewną „procedurę operacyjną" o wysokim stopniu komplikacji, posiadającą określoną strukturę i składającą się ze:

- sfery rozpoznania;
- sfery zakłócania informacyjnego;
- sfery obrony informacyjnej.

Sferę rozpoznania tworzą źródła zdobywania danych i ich sprzężenia. Źródła te przeznaczone są do wybierania ze zbiorów danych o przeciwniku jak najwięcej takich danych, których posiadanie pozwala identyfikować jego stan aktualny i zamiary działania. Do tej sfery (sfery rozpoznania) są przeciwnie skierowane: sfera obrony informacyjnej przeciwnika i sfera jego zakłócania informacyjnego.

Sfera zakłócania informacyjnego przeznaczona jest do wnoszenia entropii informacyjnej do systemów informacyjnych przeciwnika i destrukcji fizycznej ich nośników, prze-

[26] L. Ciborowski, „Walka informacyjna", wyd. ECE, Toruń 1999, s. 69.

twornikow i układów odbierających. Zakłócanie to możne być prowadzone różnymi sposobami. Najbardziej efektywnie można to jednak czynić przez stosowanie odpowiedniej upływności informacyjnej[27] specjalnie zdeformowanych zbiorów własnych postaci danych, z których podukład rozpoznania przeciwnika czerpie zasilanie informacyjne. Dlatego też do sfery zakłócania informacyjnego jednej strony przeciwnie skierowana jest sfera rozpoznania i sfera obrony informacyjnej strony drugiej.

Sfera obrony informacyjnej przeznaczona jest do ochrony tych postaci danych, które demaskują własny stan rzeczywisty i zamiary dalszego działania. Do niej przeciwnie skierowana jest sfera zakłócania informacyjnego i sfera rozpoznania przeciwnika.

Z powyższego wynika, że w procesie walki informacyjnej każdej sferze jednej strony przeciwstawione są dwie sfery strony drugiej (rysunek 1.4.). Polega to na tym, że:

- prowadzący rozpoznanie musi się liczyć z przeciwdziałaniem w sferze zakłócania informacyjnego i w sferze obrony informacyjnej przeciwnika;
- prowadzący zakłócanie informacyjne musi się liczyć z przeciwdziałaniem w sferze rozpoznania i w sferze obrony informacyjnej przeciwnika;
- prowadzący obronę informacyjną musi się liczyć z przeciwdziałaniem w sferze rozpoznania i w sferze zakłócania informacyjnego przeciwnika.

Wydawać by się, zatem mogło, że destrukcja informacji przeciwnika i ochrona informacji własnej jest jednym z głównych czynników walki informacyjnej. W rzeczywistości cel tego oddziaływania skoncentrowany jest na systemach informacyjnych[28] (informacyjno-sterujących) i ich zasobach, jako że na coś niematerialnego nie można oddziaływać bezpośrednio środkami materialnymi. Informacji[29] nie można ani zakłócić, ani też bezpośrednio zniszczyć. Wynika stąd, że **przedmiotem walki informacyjnej nie jest informacja, ale systemy informacyjno-sterujące i ich zasoby informacyjne wykorzystywane przez walczące strony.**

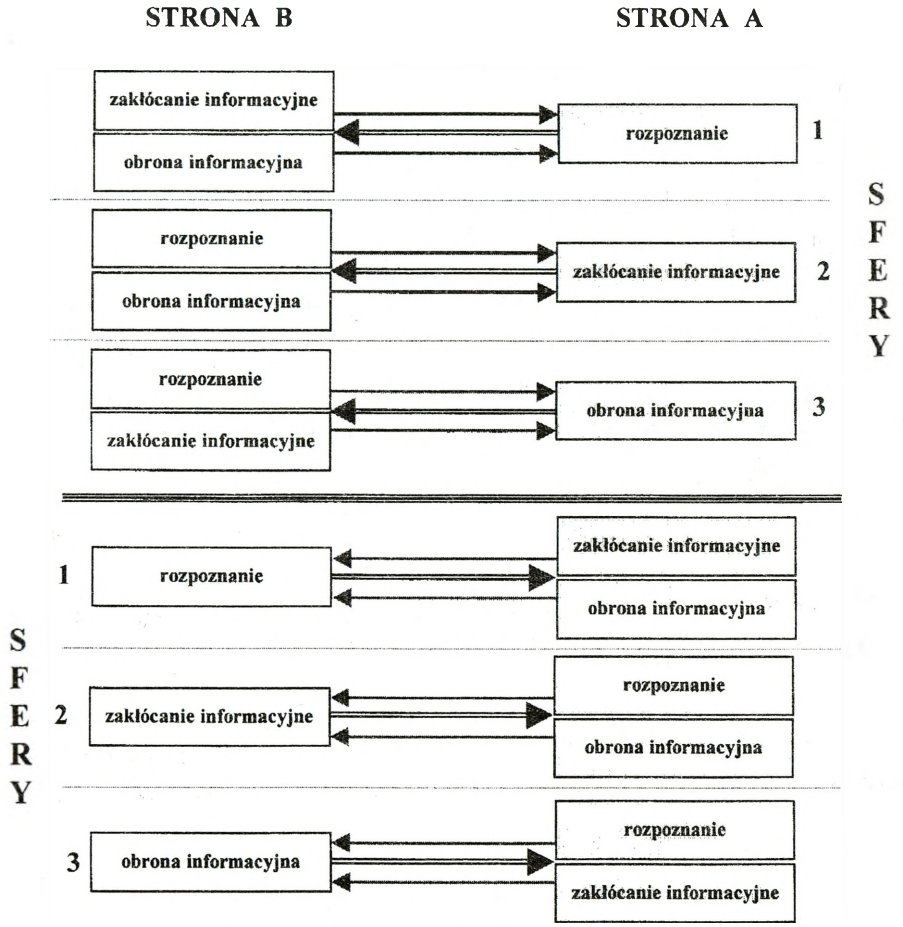
---

[27] Upływność informacyjna to celowe emitowanie takich treści, które wnoszą do systemu rozpoznawczego przeciwnika wiadomości mylące, które powodują zakłócanie jego funkcjonowania.

[28] W otoczeniu występują dwa rodzaje systemów informacyjnych: naturalne i sztuczne. **Systemy naturalne** stworzyła natura. Funkcjonują one poza wpływem i wolą człowieka, są więc odporne na różnorakie jego oddziaływanie. **Sztuczne systemy informacyjne** (ergotransformacyjne) nazywane systemami informacyjno-sterującymi tworzone są i sterowane przez człowieka w aspekcie zaspokojenia konkretnych potrzeb wynikających z zamiaru jego działania celowego. Wyróżnia się systemy gospodarcze i niegospodarcze, wśród których ważną grupę stanowią systemy militarne (wojskowe). Por.: „Systemy i procesy informacyjne", wyd. PWE, Warszawa 1986, s. 35.

[29] Informacją jest wszystko to co nie jest ani energią, ani masą, czyli nie jest zasilaniem. „Mały słownik cybernetyczny", wyd. Wiedza Powszechna. Warszawa 1973, s. 155.

Należy nadmienić, że pojęcie walka informacyjna[30] nie jest dotychczas oficjalnie wyróżniane w dokumentach normatywnych Sztabu Generalnego WP. Potencjał dostosowany do jej prowadzenia nie jest też traktowany jako odrębny rodzaj wojsk. Nie ulega jednak wątpliwości, że taki występuje w strukturze wojsk lądowych i wchodzących w ich skład związków operacyjnych i taktycznych oraz oddziałów. Potencjał ten, według zasad wydzielania rodzajów wojsk[31], ma wszystkie cechy charakterystyczne predestynujące do nazwania go rodzajem wojsk, który dostosowany jest do prowadzenia walki informacyjnej.



Rys. 1.4. Funkcjonalne powiązania walki informacyjnej

[30] Pojęcie „walka informacyjna" zostało zamieszczone w „Regulaminie działań wojsk lądowych", wyd. DWLąd, Warszawa 1999 r.

[31] Rodzajem wojsk nazywa się zbiór takich elementów (oddziałów, pododdziałów i innych komórek organizacyjnych, które odróżniają się od innych specyfiką podstawowego uzbrojenia, wyposażenia technicznego, struktur organizacyjnych, procedur szkolenia i zasad działania na polu walki. „Leksykon wiedzy wojskowej", wyd. MON, Warszawa 1979, s. 369.

Potencjał ten odgrywa ważną rolę w realizowanych przez wojska związku operacyjnego zadaniach zgodnie z przyjętą doktryną obronną RP[32].

Z badań wynika, że **istotą walki informacyjnej jest stwarzanie sytuacji utrudniających przeciwnikowi podejmowanie trafnych decyzji, wykonywanie sprawnych manewrów i precyzyjnych uderzeń ogniowych, przy jednoczesnej obronie przed tym samym wojsk własnych. Ukierunkowana jest na dezorientowanie przeciwnika w sytuacji pola walki, komplikowanie warunków jego działania i w efekcie – zmuszanie go do podejmowania błędnych decyzji.** Innymi słowy jest to niezmiernie złożony proces kierowania działaniami przeciwnika w nieznany mu sposób, a odpowiednio stosowane przedsięwzięcia dezinformujące powinny stwarzać pozory realizmu opracowanego scenariusza działań.

Dlatego też zakres wysiłków podejmowanych dla osiągnięcia tak postawionego celu powinien być precyzyjnie dobierany, a rzeczywiste plany utrzymywane w największej tajemnicy. Nieprzestrzeganie tych reguł najczęściej może doprowadzić do sytuacji, w której własna strona zamiast być reżyserem stanie się nieświadomym narzędziem manipulacji w rękach przeciwnika. Ważną rolę ma do spełnienia w tym zakresie obrona informacyjna. Powinna być prowadzona ciągle, a więc w okresie pokoju[33], podczas zagrożeń (w sytuacjach przedkryzysowych) oraz podczas kryzysu[34] i w czasie wojny[35]. Stwierdzenia te mają więc zastosowanie w całej rozciągłości do działań obronnych związku operacyjnego.

1.2. Przedmiot, cel i zadania obrony informacyjnej w działaniach obronnych związku operacyjnego

Jak wynika z definicji zamieszczonych w literaturze źródłowej **obrona informacyjna stanowi zespół skoordynowanych przedsięwzięć dostosowanych do uniemożliwienia do-**

---

[32] Strategia bezpieczeństwa RP, 4.01.2001r., Internet: www.msz.gov.pl., a ponadto:
- Strategia obronności RP, Departament Systemu Obronnego MON, Warszawa 2000 r.;
- Polityka bezpieczeństwa i strategii obronnej RP. Dokument Komitetu Obrony Kraju, 2 listopada 1992 r.;
- Doktryna obronna RP, luty 1990 r.

[33] Pokój – stan w stosunkach międzynarodowych, w których nie stosuje się przemocy, lecz współpracę sprzyjającą rozwojowi wartości pożądanych przez daną zbiorowość. „Słownik terminów z zakresu bezpieczeństwa narodowego", wyd. AON, Warszawa 1996, s. 70.

[34] Kryzys – sytuacja wewnętrzna lub międzynarodowa, która niesie w sobie zagrożenie dla podstawowych wartości, interesów lub celów strategicznych uwikłanych stron. Tamże, s. 43.

[35] Wojna – konflikt zbrojny między państwami, blokami państw, narodami lub klasami społecznymi; kontynuacja polityki środkami przemocy w celu osiągnięcia określonych interesów politycznych, ekonomicznych lub ideologicznych. Tamże, s. 113.

stępu do zbiorów informacji[36], które odzwierciedlają lub mogą odzwierciedlać stan faktyczny, usytuowanie i zamiary działania wojsk związku operacyjnego oraz ochronę ich procedur dowodzenia i naprowadzania uzbrojenia przed zakłócaniem informacyjnym stosowanym przez przeciwnika.

Postrzegając problem obrony informacyjnej w kategoriach systemowych, należy mieć na uwadze, że w każdym rodzaju działań wojennych organizowane są przez walczące strony różne systemy informacyjno-sterujące[37]. Dostosowane są one do spełnienia trzech podstawowych funkcji:

- zdobywania danych o przeciwniku;
- zbierania danych o własnym potencjale i o jego sytuacji na polu walki;
- kierowania własnym potencjałem walki.

Każda z zaangażowanych stron konfliktu dąży do tego, aby jej systemy informacyjno-sterujące funkcjonowały lepiej od systemów przeciwnika. Efekty tego wyznaczane są skutecznością rozpoznania przeciwnika oraz sprawnością przebiegu kierowania własnym potencjałem.

W procesie **zdobywania danych o przeciwniku** istota walki informacyjnej sprowadza się do tego, że jeden z podmiotów stara się wszelkimi sposobami (za pomocą systemu rozpoznania) zdobyć jak najwięcej danych o stanie, usytuowaniu, zamiarach i możliwych działaniach przeciwnika. Drugi z podmiotów stara się, z podobnym zaangażowaniem, przeciwdziałać osiągnięciu tego celu, tworząc odpowiedni system obrony informacyjnej własnych zbiorów danych i system zakłócania rozpoznania. Procedura ta dotyczy obu walczących stron.

Funkcjonowanie systemu obrony informacyjnej w tym ujęciu sprowadza się do stwarzania warunków uniemożliwiających przeciwnikowi pozyskiwanie danych, szczególnie tych ich postaci, które stanowią najwyższą wartość rozpoznawczą. Nie zawsze jednak istnieje możliwość pełnego osiągnięcia tego celu, tj. ich ukrycia.

---

[36] Informacja – bodziec oddziałujący na układ recepcyjny człowieka, powodujący wytwarzanie w jego wyobraźni przedmiotu myślowego, odzwierciedlającego obraz rzeczy materialnej lub abstrakcyjnej (przedmiotu, procesu, zjawiska, pojęcia itp.), który w jego przekonaniu (świadomości) kojarzy się jakoś z tym bodźcem. Oznacza to, że informacje to tylko te doznania, które inspirują umysł ludzki do pewnej wyobraźni. Jej istnienie jest relatywnie związane z istnieniem człowieka [25].

[37] 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 [24].

Dlatego w ramach obrony informacyjnej przed rozpoznaniem, oprócz ukrywania powinno być stosowane maskowanie danych, które polega na stosowaniu takich rozwiązań, które powodują zmianę wartości potencjału informacyjnego określonych postaci danych.

Zakłócanie informacyjne procesu zdobywania danych może być prowadzone różnymi sposobami i przy wykorzystaniu różnych narzędzi. Służy do wnoszenia entropii informacyjnej do systemu zdobywania danych przeciwnika drogą stosowania szeroko pojętej dezinformacji oraz zagłuszania elektronicznego i fizycznej destrukcji jego elementów technicznych. Procedura destrukcyjnego oddziaływania na proces zdobywania danych, tj. na system rozpoznania przeciwnika, powinna być realizowana w celu uniemożliwienia przeciwnikowi wykorzystania tych postaci danych, do których uda się mu zdobyć dostęp mimo stosowania przedsięwzięć obrony informacyjnej. Działania podejmowane w ramach zakłócania informacyjnego procesu zdobywania danych należy ściśle zsynchronizować z systemem obrony informacyjnej wojsk własnych i powinny one być: scentralizowane, kompleksowe, spójne, wiarygodne, nieszablonowe, skryte, terminowe i ciągłe.

W procesie **zbierania danych o własnym potencjale** walka informacyjna ma nieco inny wymiar niż podczas zdobywania danych o przeciwniku. Skupiona jest przede wszystkim na problematyce zachowywania jego sprawności funkcjonalnej, gdyż sukces na polu walki uwarunkowany jest sprawnością kierowania. Organy kierujące (sterujące) działaniami wojennymi walczących stron zainteresowane są nie tylko wiarygodnymi danymi o przeciwniku. Muszą mieć zapewniony dopływ aktualnych i precyzyjnych danych o rzeczywistym stanie, położeniu i rezultatach działań prowadzonych przez wojska własne[38]. Są one niezbędne do podejmowania trafnych decyzji. Z kolei przeciwnik stara się przeciwdziałać tym działaniom. Proces zbierania danych o własnym potencjale będzie przedmiotem zainteresowania organów rozpoznania przeciwnika oraz obiektem oddziaływania zakłócania informacyjnego. Oznacza to, że proces zbierania danych o własnym potencjale funkcjonuje w pozytywnym otoczeniu własnej obrony informacyjnej i własnego zakłócania informacyjnego oraz w otoczeniu negatywnym rozpoznania przeciwnika i jego zakłócania informacyjnego. **W procesie tym system obrony informacyjnej powinien utrudniać dostęp do danych o wojskach własnych, a celowo dozowana upływność informacyjna ma na celu dezinformowanie organów rozpoznawczych przeciwnika i powinna być ściśle koordynowania z zakłócaniem informacyjnym.**

---

[38] W tym celu należy zorganizować odpowiedni monitoring pola walki.

W procesie **kierowania własnym potencjałem** walka informacyjna powinna skupiać się wokół problematyki rozpoznania i obrony informacyjnej. Odbywa się w nim wymiana danych na potrzeby użycia potencjałów walki zaangażowanych stron. Starają się one, z jednej strony, zdobyć do niego dostęp rozpoznawczy, z drugiej zaś czynią wszystko, aby w stosunku do własnego procesu uniemożliwić to przeciwnikowi, prowadząc kompleksową obronę informacyjną. Istotne jest przy tym, by fakt uzyskania dostępu rozpoznawczego był utrzymany w tajemnicy. Zdemaskowanie tego uniemożliwia zastosowanie dodatkowych przedsięwzięć obronnych (np. w zakresie kontrdezinformacji) przez przeciwnika. Na proces kierowania potencjałem walki można również oddziaływać w ograniczonym zakresie różnymi sposobami w ramach zakłócania informacyjnego. Stosowanie ciągłego zakłócania procesu kierowania potencjałem walki jest jednak niepożądane, gdyż uświadamia przeciwnikowi, że jest dostęp do niego i trzeba podjąć odpowiednie przedsięwzięcia ochronne. Można zatem powiedzieć, że proces kierowania potencjałem walki funkcjonuje w podobnym otoczeniu do procesu zbierania danych o potencjale własnym. Różnica polega na przewartościowaniu znaczenia rozpoznania i zakłócania informacyjnego. W pierwszym wypadku pierwszoplanową rolę odgrywa zakłócanie informacyjne, a rozpoznanie je uzupełnia. Zaś w drugim (chodzi o proces kierowania potencjałem walki) zasadnicze wysiłki walki informacyjnej powinny być ukierunkowane na rozpoznanie, a drugoplanową rolę powinno odgrywać zakłócanie informacyjne.

Szczególną rolę podczas kierowania własnym potencjałem walki mają do odegrania elementy sterujące określonymi procesami[39]. Z reguły wyposażone są one w wysokiej klasy urządzenia elektroniczne wspomagane komputerowo, które wykorzystuje się do gromadzenia i przetwarzania danych oraz wypracowywania decyzji i przekazywania ich podwładnym. Są to najbardziej newralgiczne elementy w strukturze każdego systemu informacyjno-sterującego, a od sprawności ich funkcjonowania w dużej mierze zależy sukces bądź porażka walczących stron. Elementy te, jako przedmioty oddziaływania są szczególnymi obiektami walki informacyjnej. Przeciwnik postrzega je jako obiekty rozpoznania i zakłócania informacyjnego, zaś wojska własne traktują je jako obiekty pieczołowitej obrony informacyjnej.

Dlatego też autor, mając na względzie realizację celu pracy studyjnej, postanowił w dalszych rozważaniach skupić się przede wszystkim na obronie informacyjnej systemów dowodzenia i naprowadzania uzbrojenia w działaniach obronnych związku operacyjnego.

---

[39] W terminologii ogólnowojskowej utożsamiane są z systemami dowodzenia wojskami i naprowadzania uzbrojenia [134].

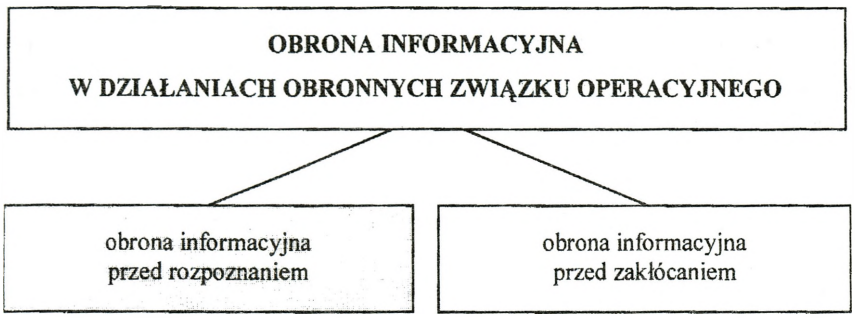
Powyższe oznacza, że **przedmiotem obrony informacyjnej w działaniach obronnych związku operacyjnego są systemy dowodzenia i naprowadzania uzbrojenia oraz ich zasoby informacyjne i procesy informacyjno-sterujące spełniające swoje funkcje w warunkach intensywnego oddziaływania informacyjnego przeciwnika.**

Sprawność kierowania własnym potencjałem uzależniona jest w znacznej mierze od podejmowanych przez wojska związku operacyjnego odpowiednio skoordynowanych działań w ramach obrony informacyjnej. Powinna być ona realizowana różnymi sposobami i narzędziami, a jej **celem powinno być zachowanie ciągłości dowodzenia wojskami i naprowadzania uzbrojenia w warunkach kompleksowego rozpoznania i intensywnego zakłócania informacyjnego ze strony przeciwnika.** To ważny element (filar) działań obronnych związku operacyjnego w wymiarze informacyjnym.

Działania obronne związku operacyjnego w zależności od sposobu dążenia do osiągnięcia celu dzieli się na manewrowe i pozycyjne [15]. W każdej sytuacji działania obronne powinny być aktywne, trwałe, zdolne odeprzeć uderzenia lądowo-powietrznych (powietrzno-morskich) zgrupowań przeciwnika. Z analizy literatury przedmiotu [15;52;69;70;82;86; 129;145] oraz dokumentów normatywnych [85] wynika, że celem działań obronnych związku operacyjnego jest uniemożliwienie przeciwnikowi opanowania terenu, rozbicie zgrupowań uderzeniowych i załamania jego natarcia oraz przejęcie inicjatywy. Podczas planowania działań obronnych związku operacyjnego rozważyć należy nie tylko ich celowość z wojskowego punktu widzenia, lecz również wymiar informacyjny. Wnioski z doświadczeń historycznych wskazują bowiem, że strona która uzyskała przewagę informacyjną z reguły odnosiła sukces.

Walka o przewagę w sferze informacji jest szczególnie istotna wobec stałego zmniejszania liczebności wojsk. Wymiar informacyjny wpływa na stopień poparcia wojska przez społeczeństwo. Często o ocenie działań militarnych nie decyduje rzeczywista sytuacja, lecz jej subiektywne postrzeganie przez media, polityków i społeczeństwo. Poprzez różnego rodzaju oddziaływania w wymiarze informacyjnym wpływa się również na wojska i ludność przeciwnika. Brak akceptacji i negatywna ocena jego społeczeństwa przyczynić się może do niepowodzeń działań i to mimo początkowych sukcesów. Informacja jako czynnik operacyjny jest więc wielkością bezpośrednio stymulującą działania bojowe. Wymaga szczególnej ochrony podejmowanej w ramach obrony informacyjnej.

Z badań wynika, że ogólna struktura[40] obrony informacyjnej w działaniach obronnych związku operacyjnego powinna obejmować elementy zilustrowane na rysunku 1.5.



Rys.1.5. Ogólna struktura obrony informacyjnej w działaniach obronnych związku operacyjnego

Obrona informacyjna przed rozpoznaniem w działaniach obronnych związku operacyjnego ma na celu ukrywanie zbiorów wszelkich postaci danych o rzeczywistym stanie, usytuowaniu i zamiarach działania wojsk związku operacyjnego, które mogą być dostępne dla źródeł rozpoznania potencjalnego przeciwnika.

Obrona informacyjna przed zakłócaniem w działaniach obronnych związku operacyjnego ma na celu zabezpieczenie przed zniszczeniem zbiorów własnych postaci danych i wnoszeniem do nich takich treści, które powodować mogą wzrost niewiedzy o stanie aktualnym, usytuowaniu i zamiarach działania wojsk oraz wprowadzać stan chaosu i nieuporządkowania w procesach dowodzenia i naprowadzania uzbrojenia związku operacyjnego.

Z powyższego wynika, że obronę informacyjną należy organizować i prowadzić zarówno w stosunku do stanów osobowych, jak i urządzeń technicznych (w środowisku osobowym i nieosobowym), jako że obydwie składowe systemów dowodzenia wojskami i naprowadzania uzbrojenia stanowią odpowiednie zespoły powiązanych ze sobą funkcjonalnie i organizacyjnie sił i środków. Tak rozumiana obrona ma do spełnienia **dwa kompleksowe zadania**:

– **zabezpieczenie procesów informacyjno-sterujących w systemach dowodzenia i naprowadzania uzbrojenia związku operacyjnego przed rozpoznaniem i zakłócaniem**

---

[40] Struktura to model zbudowany za pomocą określonych działań upraszczających, które pozwalają utożsamiać różne zjawiska ze wspólnego punktu widzenia. Struktura to zatem całość, części tej całości oraz stosunki pomiędzy tymi częściami. Struktura jest modelem jako system zróżnicowań. Struktura to rozmieszczenie elementów składowych i zespół relacji między tymi elementami, charakterystyczny dla danego układu. „Leksykon techniczny", wyd. WNT, Warszawa 1983, s. 528.

informacyjnym, a także przed przypadkowymi, niezamierzonymi zakłóceniami pochodzącymi z otoczenia, w którym te systemy funkcjonują;

– podwyższenie odporności elementów ugrupowania operacyjnego (bojowego) związku operacyjnego, a zwłaszcza systemów dowodzenia wojskami i naprowadzania uzbrojenia na ich wykrycie i obezwładnienie przez przeciwnika ofensywnymi środkami walki informacyjnej.

Pierwsze z wymienionych zadań powinno być realizowane w celu zapewnienia stabilnej pracy wszystkich systemów dowodzenia wojskami i naprowadzania uzbrojenia związku operacyjnego, szczególnie systemów (sieci) łączności, informatycznych, systemów radionawigacyjnych, rozpoznania, systemów naprowadzania uzbrojenia.

Drugie zadanie powinno być realizowane przez wszystkie elementy ugrupowania operacyjnego związku operacyjnego, a zwłaszcza przez: związki taktyczne pierwszego rzutu; odwód ogólnowojskowy; zgrupowanie oddziałów artylerii; oddział przeciwlotniczy; elementy rozpoznania i zakłócania; odwód przeciwpancerny; oddział zaporowy; stanowiska dowodzenia; oddziały i urządzenia logistyczne; odwody innych rodzajów wojsk. Zadanie to powinno być realizowane także przez oddziały i pododdziały wojsk obrony terytorialnej, straży granicznej oraz innych sił znajdujących się w obszarze odpowiedzialności obronnej związku operacyjnego.

Przedsięwzięcia obrony informacyjnej należy wykonywać w rejonach stałej dyslokacji wojsk, na drogach (pasach) przegrupowania wojsk, w obszarze odpowiedzialności obronnej związku operacyjnego[41], w pasach (rejonach) odpowiedzialności obronnej związków taktycznych.

Czas realizacji poszczególnych zadań obrony informacyjnej związku operacyjnego powinien być uwarunkowany czasem przebywania elementów ugrupowania operacyjnego, systemów dowodzenia i naprowadzania uzbrojenia w zasięgu środków rozpoznania i zakłócania. Realizację tych przedsięwzięć powinno się rozpoczynać z takim wyprzedzeniem czasowym i przestrzennym, aby osiągnąć pełną efektywność podejmowanych działań zanim określone elementy ugrupowania obronnego związku operacyjnego znajdą się w zasięgu oddziaływania określonego środka walki informacyjnej przeciwnika. Szczególną rolę odgrywa czas realizacji przedsięwzięć obrony informacyjnej związku operacyjnego przed rozpoznaniem. Ponieważ wojska związku operacyjnego już w okresie pokoju znajdują się w zasięgu naziem-

[41] Obszar odpowiedzialności obronnej związku operacyjnego obejmuje obszar działań sił osłony, główny obszar działań i tyłowy obszar działań [15].

nych, powietrznych, a przede wszystkim satelitarnych systemów rozpoznania potencjalnego przeciwnika [73], przeciwdziałanie tym systemom powinno być prowadzone w sposób ciągły, a zatem również w okresie pokoju.

Z powyższego wynika, że obrona informacyjna odgrywa szczególną rolę podczas przygotowania i prowadzenia działań obronnych związku operacyjnego. Dobrze zaplanowane i wykonane przedsięwzięcia obrony informacyjnej w sposób zasadniczy mogą wpływać na osiągnięcie celu tych działań. Mimo, że przedsięwzięcia wykonywane w ramach obrony informacyjnej nie są formą działań, która wpływa bezpośrednio destrukcyjnie na siły i środki przeciwnika, to jednak umiejętne wkomponowane w system działań obronnych związku operacyjnego mogą zapewnić wymierne rezultaty.

Pełną skuteczność przedsięwzięć podejmowanych w ramach obrony informacyjnej w związku operacyjnym można osiągnąć tylko pod warunkiem przygotowania już w okresie pokoju sztabów i wojsk do jej prowadzenia. Problematykę przygotowania obrony informacyjnej w działaniach obronnych związku operacyjnego uczyniono przedmiotem oddzielnych badań, a ich wyniki zamieszczono w rozdziale czwartym pracy studyjnej.

1.3. Wnioski

Z przeprowadzonych badań przedmiotu, celu i zadań obrony informacyjnej w działaniach obronnych związku operacyjnego wynika, iż:

1. W siłach zbrojnych głównych państw nie należących do NATO dla osiągnięcia ofensywnych celów oddziaływań informacyjnych, a nawet ataków, bitew i operacji informacyjnych mogą być stosowane wszystkie dostępne sposoby walki informacyjnej. Zakłada się prowadzenie ofensywnej części walki informacyjnej w pełnym wymiarze w czasie kryzysu lub konfliktu (wojny). W tym celu przewiduje się:

- uzyskanie przewagi nad przeciwnikiem w sferze wywiadu i rozpoznania wojskowego;
- wprowadzanie przeciwnika w błąd oraz dezorganizowanie i niszczenie jego infrastruktury informacyjnej;
- stosowanie zakłócania informacyjnego powodującego paraliżowanie systemów rozpoznawczych, jak również procesów kierowania państwem i dowodzenia wojskami oraz szerzenie w jego szeregach i społeczeństwie demoralizacji stanów osobowych, a także dezorganizowanie życia;

– stwarzanie warunków do szybkiego neutralizowania oporu przeciwnika.

2. Defensywny aspekt walki informacyjnej, nazywany również defensywnym przeciwdziałaniem informacyjnym lub wprost obroną informacyjną, odgrywa ważną rolę w zapewnieniu stabilnej pracy własnym systemom informacyjnym. Zakłada się, że działania te są bardzo ważne i mają charakter ciągły. W amerykańskiej doktrynie działań (operacji) informacyjnych wyszczególnia się cztery fazy: osłonę środowiska informacyjnego, wykrywanie ataku informacyjnego, odtwarzanie potencjału informacyjnego, prowadzenie kontrataków informacyjnych.

3. Obecnie w środowiskach wojskowych NATO toczy się coraz szersza dyskusja nad problemem zagrożeń wynikających z oddziaływań na systemy i zasoby informacyjne. Wojskowi teoretycy z wielu państw NATO intensywnie pracują nad koncepcjami i doktrynami działań (operacji) informacyjnych.

4. Przedmiotem obrony informacyjnej w działaniach obronnych związku operacyjnego są systemy dowodzenia i naprowadzania uzbrojenia oraz ich zasoby informacyjne i procesy informacyjno-sterujące spełniające swoje funkcje w warunkach intensywnego oddziaływania informacyjnego potencjalnego przeciwnika;

5. Obrona informacyjna w działaniach obronnych związku operacyjnego ma do spełnienia dwa kompleksowe zadania, tj.:

– zabezpieczenie systemów dowodzenia i naprowadzania uzbrojenia przed rozpoznaniem i zakłócaniem, a także przed przypadkowymi, niezamierzonymi zakłóceniami pochodzącymi z otoczenia, w którym te systemy funkcjonują;

– podwyższenie odporności elementów ugrupowania operacyjnego (bojowego) związku operacyjnego, a zwłaszcza ich elementów dowodzenia wojskami i naprowadzania uzbrojenia na ich wykrycie i obezwładnienie przez przeciwnika ofensywnymi środkami walki informacyjnej;

6. Obronę informacyjną należy realizować zarówno w stosunku do stanów osobowych, jak i urządzeń technicznych, a zatem w środowisku osobowym i nieosobowym.

2. ZAKRES I TREŚĆ PRZEDSIĘWZIĘĆ OBRONY INFORMACYJNEJ PRZED ROZPOZNANIEM W DZIAŁANIACH OBRONNYCH ZWIĄZKU OPERACYJNEGO

Możliwości rozpoznawcze jednej strony zawsze wywierały określony wpływ na treść, a zwłaszcza na formy organizowania i prowadzenia odpowiednich działań przeciwrozpoznawczych[1] drugiej strony. Przykłady i doświadczenia minionych wojen i konfliktów lokalnych dowodzą, że pomiędzy tymi działaniami stron istniała zawsze i nadal będzie istnieć ostra rywalizacja. W wyniku analizy tej rywalizacji nasuwa się wniosek, że najczęściej najpierw następuje rozwój środków rozpoznania, a dopiero potem udoskonala się środki i sposoby obrony przed nim. Aby działania te były skuteczne, należy stale studiować i znać możliwości, charakterystykę oraz zalety i wady sił i środków rozpoznania potencjalnego przeciwnika, które systematycznie są doskonalone wraz z postępem naukowo-technicznym.

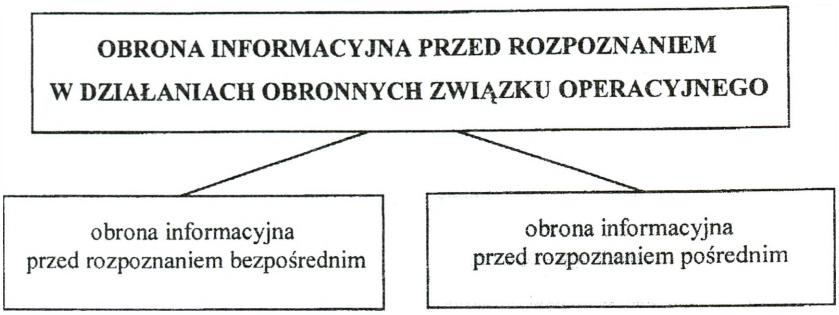
Powyższe oznacza, że **obrona informacyjna przed rozpoznaniem[2] w działaniach obronnych związku operacyjnego jest jednym z ważniejszych elementów zabezpieczenia jego działań. Powinna stanowić zespół skoordynowanych działań dostosowanych do ukrywania zbiorów wszelkich postaci informacji o rzeczywistym stanie, usytuowaniu i zamiarach działania wojsk związku operacyjnego, które znajdą się lub mogą być dostępne dla źródeł rozpoznania przeciwnika.** Dostępność ta może być bezpośrednia (dla zmysłów człowieka) lub pośrednia (dla technicznych środków rozpoznania). Stąd też ogólnie można wyróżnić obronę informacyjną w działaniach obronnych związku operacyjnego przed

---

[1] Wg „Doktryny wojsk lądowych NATO" (ang. Land Force Tactical Doctrine ATP – 35 [B]) działania przeciwrozpoznawcze (ang. Operation Security) są komponentem ubezpieczenia i osłony działań (ang. Security and Protection).

[2] Rozpoznanie - pojęcie używane w rozumieniu czynnościowym i rzeczowym. W rozumieniu czynnościowym - proces poznawczy polegający na wykrywaniu fragmentów wyodrębnionej rzeczywistości i ustalaniu ich przynależności do pewnej znanej klasy lub typu, na podstawie wcześniej zgromadzonej wiedzy o tej rzeczywistości. W rozumieniu rzeczowym – zespół sił i środków służący do spełniania czynnościowych funkcji rozpoznania. Rozpoznanie, ze względu na formę odzwierciedla określony zespół skoordynowanych elementów dostosowany do wydobywania informacji o określonej rzeczywistości ze zbiorów możliwych jej postaci. Elementami tymi są: źródła rozpoznania, przetworniki informacji, nośniki informacji i układy odbierające. Rozpoznanie dzieli się na bezpośrednie i pośrednie [22;59;87].

rozpoznaniem bezpośrednim oraz obronę informacyjną przed rozpoznaniem pośrednim (rysunek 2.1.)



Rys. 2.1. Podstawowy podział obrony informacyjnej przed rozpoznaniem w działaniach obronnych związku operacyjnego

Wnioski z badań szczegółowych poszczególnych komponentów obrony informacyjnej przed rozpoznaniem w działaniach obronnych związku operacyjnego składają się na treść kolejnych podrozdziałów niniejszej pracy studyjnej.

2.1. Obrona informacyjna przed rozpoznaniem bezpośrednim

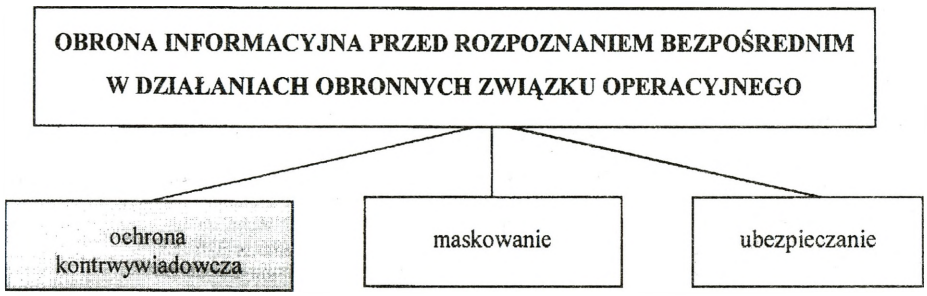
Z badań wynika, że **obrona informacyjna przed rozpoznaniem bezpośrednim w działaniach obronnych związku operacyjnego[3] obejmuje ochronę informacji, które mogą być dostępne dla źródeł rozpoznania przeciwnika przystosowanych do zdobywania danych w postaci bezpośrednio odbieralnej przez układy recepcyjne człowieka.**

Przykłady z historii sztuki wojennej wskazują, że rozpoznanie bezpośrednie jako jedno z najstarszych rodzajów rozpoznania jest prowadzone ciągle. Najważniejszą rolę odgrywa w nim człowiek, utożsamiany najczęściej ze zwiadowcą. Jego zmysły są w stanie wiele rozpoznać, choć obecnie jest on wspomagany przez różnego rodzaju urządzenia. Określone sygnały docierają do niego w formie dla niego bezpośrednio zrozumiałej. Mogą to być dane

[3] Rozpoznanie bezpośrednie stanowi zespół skoordynowanych źródeł rozpoznania dostosowanych do zdobywania informacji w postaci bezpośrednio odbieralnej przez układ recepcyjny człowieka. Określone sygnały docierają do człowieka prowadzącego rozpoznanie w formie bezpośrednio dla niego zrozumiałej (pomiędzy zbiorem możliwych postaci informacji o rzeczy, zjawisku a zbiorem źródeł rozpoznania nie występują żadne przetworniki danych). Dzieli się na rozpoznanie: agenturalne, specjalne i patrolowe. Wraz z rozwojem techniki, a szczególnie elektroniki, zaczęło się rozwijać rozpoznanie pośrednie [22;59;87].

przenoszone w postaci promieniowania widzialnego[4], drgań akustycznych[5], jak również sygnały odbierane dotykowo, smakowo i przez powonienie. Oznacza to, że jest dopuszczalne stosowanie urządzeń wspomagających zasięg i czułość doznań zmysłowych. Uzyskiwane w ten sposób dane są zrozumiałe i nie wymagają przetwarzania do postaci przyswajalnej przez zmysły człowieka.

Analiza struktury i sposobów prowadzenia rozpoznania bezpośredniego [22;59;87] wskazuje, że **obronę informacyjną przed nim należy prowadzić w działaniach obronnych związku operacyjnego ciągle, różnymi sposobami i metodami. Składają się na nie odpowiednie przedsięwzięcia i działania podejmowane przez wojska związku operacyjnego w ramach ochrony kontrwywiadowczej, maskowania i ubezpieczania** (rysunek 2.2.).



Rys. 2.2. Struktura obrony informacyjnej przed rozpoznaniem bezpośrednim w działaniach obronnych związku operacyjnego

Przedstawiona na rysunku 2.2. struktura obrony informacyjnej przed rozpoznaniem bezpośrednim w działaniach obronnych związku operacyjnego stanowiła osnowę dalszych prac badawczych.

---

[4] Promieniowanie widzialne (świetlne) – część promieniowania elektromagnetycznego, która związana jest z widzeniem. Zakres długości fal promieniowania widzialnego zależy od indywidualnych właściwości oka ludzkiego. Jako umowny obszar widzenia przyjmuje się zakres 0,38-0,76 μm. „Ilustrowana encyklopedia dla wszystkich". Fizyka, wyd. WNT, Warszawa 1991, s. 274.

[5] Drgania (fale) akustyczne – zaburzenie rozchodzące się w ośrodku sprężystym, polegające na przenoszeniu energii przez drgające cząsteczki bez zmiany ich średniego położenia. Zaburzenie wywołuje chwilowe zmiany gęstości ośrodka, wskutek czego powstają chwilowe różnice ciśnień, które stają się źródłem zaburzenia cząsteczek przyległych. Wielkościami charakteryzującymi fale akustyczne są: ciśnienie akustyczne, prędkość akustyczna i prędkość fali akustycznej. Tamże, s. 77.

2.1.1. Ochrona kontrwywiadowcza

Problematyka ochrony kontrwywiadowczej była przedmiotem rozważań wielu teoretyków wojskowych. Już Sun Tzu dostrzegał celowość prowadzenia takich działań. Zalecał, aby dane pochodzące z wywiadu traktować priorytetowo i chronić. Jeśli bowiem armia zostanie pozbawiona tajnych agentów, wszelkie działania zbrojne nie mają najmniejszego sensu. Wyróżnia on *pięć rodzajów tajnych agentów (narodowi, wewnętrzni, podwójni, straceni oraz powracający). Jeśli tych pięć typów zatrudnionych agentów pracuje w koordynacji, to nazywani są oni doskonałą siatką i znajdują się pod szczególną opieką władcy. Dlatego też tylko oświecony władca oraz zacny generał są w stanie użyć najinteligentniejszych ludzi jako agentów, a z nimi z pewnością 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*[6].

Jak wykazują doświadczenia minionych wojen [25;74;138;139], ochrona kontrwywiadowcza[7] ma na celu śledzenie i zwalczanie wywiadu[8] przeciwnika. Polega na prowadzeniu odpowiednio zaplanowanych i skoordynowanych akcji przeciwwywiadowczych. Akcje te mają **uniemożliwić służbom wywiadowczym strony przeciwnej rozpoznanie obiektów mających jakiekolwiek znaczenie dla przyszłej wojny, utrudnić rozpoznanie obiektów pod względem wywiadowczym, zapewnić bezpieczeństwo własnych sił zbrojnych (wojsk związku operacyjnego), przeciwdziałać wszelkim przejawom działalności propagandowej i sabotażu ze strony służb wywiadowczych potencjalnego przeciwnika.**

---

[6] Sun Tzu, „Sztuka wojny", wyd. Przedświt, Warszawa 1994, s. 140.

[7] Kontrwywiad wojskowy to działalność zmierzająca do zwalczania szpiegostwa, akcji dywersyjnych i sabotażowych, mająca na celu ochronę tajemnicy wojskowej przed penetracją obcego wywiadu. Ochrona kontrwywiadowcza prowadzona jest w wielu państwach przez służby specjalne, a jej procedury są ściśle tajne [22;59;87].

[8] Wywiad (rozpoznanie agenturalne) to ogół przedsięwzięć organizacyjnych (tajnych), mających na celu zdobywanie różnych materiałów i danych stanowiących tajemnicę państwową i wojskową potencjalnego przeciwnika. Ze względu na dziedzinę zainteresowania można wyróżnić wywiad psychologiczny, polityczny, gospodarczy i wojskowy.
Wywiad wojskowy obejmuje szeroką gamę zagadnień dotyczących całych sił zbrojnych, poszczególnych rodzajów sił zbrojnych, zasobów ludzkich oraz personalia. Z tego też względu wywiad wojskowy dzieli się na: morski; lotniczy, lądowy.
Wywiad lądowy - w obszarze jego zainteresowania znajdują się następujące zagadnienia: topografia, geologiczna struktura i klimat danego kraju; komunikacja, w tym przepustowość dróg kolejowych i samochodowych, możliwości transportowe, mosty, żegluga śródlądowa i jej urządzenia, cywilny transport lotniczy. Stanowi rodzaj rozpoznania strategicznego i operacyjnego. Jest prowadzony nieprzerwanie w okresie pokoju i wojny przez specjalnie wyszkolonych agentów, działających w sposób nielegalny (zakonspirowany). Agenci prowadzący wywiad rekrutują się z różnych środowisk. Są to nie tylko oficerowie, lecz także osoby cywilne zatrudnione w różnych instytucjach. W rejon działania (na terytorium obcego państwa) przerzuca się je kanałami legalnymi i nielegalnymi. Sieć wywiadu organizuje się również przy wykorzystaniu obywateli danego państwa, szczególnie tych, którzy są wysoko postawieni w hierarchii służbowej (wojskowej i cywilnej) i mają dostęp do ważnych informacji państwowych, wojskowych, gospodarczych itp. [22;59;87].

Ze względu na strukturę ugrupowania obronnego [15] związku operacyjnego można wyróżnić z przodu ochronę kontrwywiadowczą **płytką**, realizowaną w obszarze osłony związku operacyjnego oraz **daleką**, realizowaną w głębi operacyjnej. Z kolei analiza metod pozyskiwania informacji wywiadowczych pozwala wyróżnić ochronę kontrwywiadowczą **pasywną i aktywną**.

Pasywną ochronę kontrwywiadowczą w działaniach obronnych związku operacyjnego należy ukierunkować na uniemożliwienie prowadzenia obserwacji (kontrwywiadu obserwacyjnego), na odpowiednie zabezpieczenie dokumentów (kontrwywiad dokumentalny) oraz na ochronę personalną (kontrwywiad personalny).

Kontrwywiad obserwacyjny powinien polegać na wykrywaniu i demaskowaniu agentów, którzy przemieszczając się w obszarze działania związku operacyjnego, metodą obserwacji pozyskują dane o interesujących ich obiektach.

Z kolei kontrwywiad dokumentalny powinien mieć na celu uniemożliwienie zdobywania dokumentów (oryginałów, kopii lub fotografii, plików) traktujących o planach mobilizacyjnych, planach (zamiarach) działania, instrukcjach, projektach urządzeń itp.

Kontrwywiad personalny dotyczy ochrony wyższych dowódców i ważnych osób funkcyjnych związku operacyjnego oraz zaistniałych ciekawszych wydarzeń z ich życia służbowego i prywatnego.

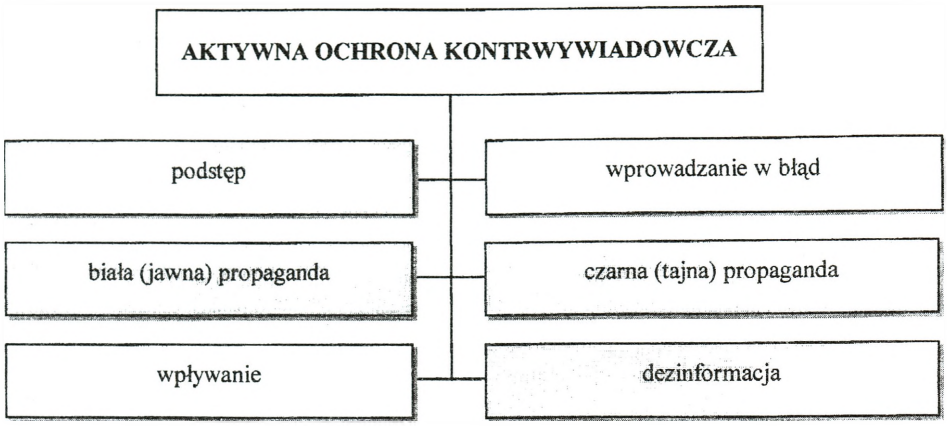
Aktywna ochrona kontrwywiadowcza[9] w działaniach obronnych związku operacyjnego polega na stosowaniu znanych od zarania dziejów metod[10], takich jak (rysunek 2.3.): podstęp, wprowadzanie w błąd, jawna (tzw. biała) propaganda, tajna (tzw. czarna) propaganda oraz wpływanie i dezinformacja.

Podstęp stosowano w wojnie zawsze. Jest on – jak wiadomo – nieodłącznym elementem szermierki, gdyż należy nieustannie grozić przeciwnikowi, żeby zadać mu cios. Wyższa forma podstępu to już działania dezinformujące, polegające na odwróceniu uwagi przeciwnika od miejsca, w którym zamierza się zaatakować. Jeszcze wyższą formą podstępu jest wprowadzanie w błąd. I tak na przykład Grecy nie zadowolili się pozorowaniem wycofania się, lecz ukrywając zbrojnych we wnętrzu konia wmówili Trojanom, że koń jest darem Ateny, bez czego nie zdołaliby wprowadzić go do miasta.

---

[9] Przedsięwzięcia aktywnej ochrony kontrwywiadowczej należy ujmować również w zakłócaniu informacyjnym.

[10] Ich wykładnię dał Wł. Volkoff [w:] „Dezinformacja oręż wojny", wyd. Delikon, Warszawa 1991, s. 6 - 16.



Rys. 2.3. Aktywna ochrona kontrwywiadowcza

Wprowadzanie w błąd (intoksykacja) przeciwnika zawsze było jedną z ulubionych taktyk kontrwywiadu. Nie ma bowiem lepszego sposobu ochrony prawdziwych tajemnic, niż dostarczenie wywiadowi przeciwnika fałszywych danych. Należy mieć na uwadze, że na wyższych szczeblach dowodzenia wprowadzanie w błąd może stać się samodzielnym działaniem na arenie politycznej. Podejmowane wówczas działania są tak ukierunkowane, żeby przeciwnik uwierzył w to, w co powinien uwierzyć, aby działał na własną zgubę na płaszczyźnie politycznej i wojskowej. Np. alianci, podjąwszy decyzję o lądowaniu na Sycylii, postanowili przekonać Hitlera, że zaatakują w Grecji, Sycylia zaś była tylko obiektem pozorowanego ataku. W tym celu wrzucili do morza u wybrzeży Hiszpanii zwłoki brytyjskiego oficera z materiałami mającymi wprowadzić Niemców w błąd. W wyniku tego niemiecka 11 flotylla torpedowców i inne siły opuściły zajmowane pozycje, a alianci wylądowali na Sycylii, niemal nie napotykając oporu.

Biała propaganda, nazywana również propagandą jawną lub oficjalną jest stosowana także w ramach zakłócania informacyjnego. Ma na celu obniżanie morale wojsk przeciwnika oraz wpływanie na nastroje ludności cywilnej. Skuteczność jej oddziaływania jest z reguły niska, ponieważ pochodząc otwarcie ze źródeł znanych przeciwnikowi ma ograniczoną wiarygodność.

Prowadząc czarną (tajną) propagandę, ukrywa się natomiast jej prawdziwe pochodzenie i w ten sposób czyni się wiarygodnymi świadome kłamstwa. Arcymistrzem czarnej propagandy po stronie aliantów w drugiej wojny światowej był, urodzony w Niemczech, Sefton

Delmer[11]. Zorganizował on kilka radiostacji rzekomo prohitlerowskich. Jedna z nich przedstawiała się jako niemiecka rozgłośnia wojskowa „Gustav Siegfried Eins" nadająca muzykę i wiadomości przeznaczone dla „kolegów z Wehrmachtu". Inna posługiwała się bardziej przebiegłą metodą: słuchacze przestrajając odbiornik natrafiali nagle na program jakiejś podziemnej organizacji z przeświadczeniem, że przypadkiem natrafili na audycję przeznaczoną nie dla nich. Radiostacja ta nadawała poufne informacje pochodzące od wiernego i lojalnego zwolennika Hitlera, gardzącego hołotą, która rządzi krajem w imieniu „Führera".

Wpływanie łączy się niekiedy ze stosowaniem technik czarnej propagandy, ale jest metodą nieporównanie subtelniejszą. Agent wpływu jest „rodzajem agitatora w stanie czystym". Zajmuje się agitacją nie w zamiarze zmiany biegu wydarzeń w jakimś określonym kierunku, lecz w sposób ogólniejszy, żeby destabilizować przeciwnika. Nie jest dla niego istotne, czy bezpośrednie skutki jego działań przyniosą korzyści państwu, dla którego pracuje. Rzecz w tym, aby przyniosły one szkodę krajowi, przeciw któremu są wymierzone.

Z powyższego wynika, że wpływanie jest wyrafinowaną techniką, której absolutnie nie należy mylić z jawną propagandą. Co za tym idzie, każda osoba, każda organizacja, która nie kryje się ze swą sympatią dla państwa – mocodawcy, automatycznie wyłącza się z gry. Dlatego, należy zawsze pamiętać, jak radzi Sun Tzu[12], *„żeby w kraju będącym celem działań wywrotowych przeciągać na swoją stronę ludzi mądrych i szlachetnych z otoczenia wrogiego władcy, aby pozbawić go doradców. Czasem wysyła się ludzi zdradzieckich i niebezpiecznych w celu rozbicia jego administracji. Wysyła się też fałszywe informacje, aby odsunąć ministrów od swojego suwerena"*.

Dezinformacja – jako przedsięwzięcie ochrony kontrwywiadowczej może być rozumiana w wąskim lub szerszym znaczeniu. W wąskim tego słowa znaczeniu lokowana jest pomiędzy wprowadzaniem w błąd a wpływaniem. Podczas gdy wprowadzanie w błąd – jako takie jest czynnością jednorazową, związaną z konkretnym zadaniem i dopuszcza pewną amatorszczyznę we wmawianiu pewnych pożądanych zachowań określonym osobom (agentom), to dezinformacja prowadzona jest w sposób systematyczny, fachowy, zawsze za pośrednictwem mediów i jest adresowana do wojsk („opinii publicznej"), a nie sztabów – obiektów działań. Gdy wpływanie przejawia się w działaniach pozornie niezorganizowanych, oportunistycznych, głównie ilościowych, dezinformacja stawia sobie za cel realizację konsekwentnego programu zmierzającego do wytwarzania w świadomości, a przede wszystkim

---

[11] Kozaczuk W., „Wojna w elerze", wyd. RiTV, Warszawa 1977, s. 111 – 132.
[12] Sun Tzu, „Sztuka wojny", wyd. Przedświt, Warszawa 1994, s. 92.

w podświadomości stanów osobowych przeciwnika (ludności cywilnej), będących przedmiotem tych działań, poglądów uznanych za niekorzystne dla dezinformatora, które w gruncie rzeczy są dla niego (dezinformatora) korzystne.

W szerszym tego słowa znaczeniu dezinformacja obejmuje także techniki wpływania, a to z dwóch zasadniczych powodów. Po pierwsze – ci sami ludzie, w ramach tej samej organizacji (na ogół związanej z kontrwywiadem) prowadzą działania w obu tych dziedzinach. Po drugie – obie posługują się analogiczną charakterystyką celu. Zarówno w dezinformacji, jak i we wpływaniu cel widzi się jako „wspólnika".

Dewizą dezinformacji nie jest [1;138]: „*kłamcie, kłamcie, zawsze coś z tego zostanie*", lecz: „*perorujcie, perorujcie, w końcu odpowiednio do tego postąpicie*". Z tego punktu widzenia jedną z najbardziej podstępnych form dezinformacji jest ta, którą można by nazwać logomachią. Polega ona na wynajdywaniu formułek, które przypadłszy najpierw do gustu profesjonalistom od komunikacji masowej są następnie rozpowszechniane przez nich wśród opinii publicznej, która akceptuje je jako prawdziwe, podczas gdy w rzeczywistości są tylko efektowne. Termin „*polowanie na czarownice*" został prawdopodobnie ukuty w takiej właśnie intencji.

Należy mieć na uwadze, że wojska związku operacyjnego , które zamierzają stosować dezinformację jako środek prowadzenia ochrony kontrwywiadowczej[13], powinny powierzać to zadanie służbom specjalnym. Dezinformacja stanowi, bowiem syntezę służby wywiadowczej (zdobywanie wiadomości dotyczących przeciwnika) i kontrwywiadowczej (infiltrowanie jego służb wywiadowczych) dlatego, że umożliwia „zdalne sterowanie" celem za pomocą wcześniej przygotowanych materiałów i to nie poprzez tajne, pełne niewiadomych wpływanie na specjalistyczne organy, lecz przez jawne oddziaływanie na stany osobowe, a poprzez nie na przełożonych i ekspertów, jako że eksperci są uzależnieni od władzy, ta ostatnia zaś – od opinii publicznej.

2.1.2. Maskowanie

Z przeprowadzonych badań wynika, że **maskowanie stanowi zespół przedsięwzięć, działań oraz środków umożliwiających ukrywanie przed przeciwnikiem wszelkich postaci danych o wojskach i obiektach znajdujących się w obszarze odpowiedzialności**

[13] Dezinformacja jest również aktywną formą walki informacyjnej, tj. zakłócania informacyjnego [24;25;26].

obronnej związku operacyjnego, które mogą być dostępne dla jego (przeciwnika) źródeł rozpoznania.

Maskowania jest reakcją na rozpoznanie. To także konsekwencja prawa **akcji i reakcji**. Z jego istoty wynika jednoczesność występowania akcji, tj. rozpoznania i reakcji, tj. maskowania. W praktyce oprócz reakcji związanych z określoną akcją istnieją też działania opóźniające, wyprzedzające i profilaktyczne. Jednakże działania profilaktyczne trudno nazwać reakcją, albowiem jeszcze żadna akcja nie występuje. Oznacza to więc, iż przyczyną działań profilaktycznych jest domniemanie możliwości wystąpienia akcji, czyli – zagrożenia wystąpieniem określonej akcji.

Analogicznie ująć można maskowanie. Prowadzone jest ono przede wszystkim wyprzedzająco, ale i po zakończeniu rozpoznania. Wobec tego również o maskowaniu można mówić, że jest ono reakcją na prowadzone przez przeciwnika rozpoznanie i na zagrożenie nim. Dlatego za przyczynę maskowania uznać można proces rozpoznania oraz przekonanie o zagrożeniu nim. W stwierdzeniu tym znajduje się uzasadnienie zasady ciągłości maskowania. Nakazuje ona prowadzenie działań maskujących we wszystkich etapach walki.

Z powyższego wynika, że maskowanie nie jest celem samym w sobie. Powinno być zamierzonym działaniem sztabu i wojsk związku operacyjnego prowadzonym w ramach obrony informacyjnej w celu ukrycia faktycznego stanu i wprowadzenia w błąd przeciwnika. Stanowi, zatem rodzaj zabezpieczenia działań związku operacyjnego w ramach obrony informacyjnej. W regulaminach wojskowych i instrukcjach wyróżnia się maskowanie operacyjne[14] i bezpośrednie[15].

Kryterium podziału stanowi zakres zadań i celów oraz charakter przedsięwzięć organizacyjnych i wykonawczych. Cechą charakterystyczną jest i to, że można realizować przedsięwzięcia maskowania bezpośredniego autonomicznie, nie realizując zadań maskowania operacyjnego. Sytuacja odwrotna jest niemożliwa, tzn. bez maskowania bezpośredniego nie można mówić o skutecznej realizacji zadań maskowania operacyjnego.

---

[14] Maskowanie operacyjne obejmuje skoordynowane działania mające na celu ukrycie przygotowania do operacji i wprowadzenie w błąd przeciwnika co do zamiaru operacji, sposobu jej realizacji oraz ugrupowania operacyjnego, a także ukrycie opłacalnych celów dla uderzeń ogniowych, w tym systemów dowodzenia rozwiniętych na obszarze kraju oraz charakteru działań wojsk obrony terytorialnej kraju i skierowanie jego uwagi na przedsięwzięcia i obiekty drugorzędne lub pozorowane [54;59;87].

[15] Maskowanie bezpośrednie obejmuje wszystkie czynności zmierzające do ukrycia lub zmiany wyglądu zewnętrznego pojedynczych i zespołowych obiektów, urządzeń, sprzętu, uzbrojenia i ludzi za pomocą środków podręcznych lub etatowych w ramach inżynieryjnego zabezpieczenia działań wojsk. Należy organizować je stale i ciągle bez specjalnych rozkazów i zarządzeń [54;59;87].

Skuteczność maskowania można oceniać na podstawie reakcji przeciwnika, a sposoby i formy jego prowadzenia należy dobierać opierając się na znajomości cech i zwyczajów jego dowódców. Sztab planujący przedsięwzięcia maskowania powinien przyjąć sposób rozumowania adresata tych przedsięwzięć. Można to osiągnąć jedynie przez dokładną znajomość przeciwnika, jego kultury, zwyczajów, psychiki i itp. Znajomość zwyczajów przeciwnika jest niezbędna do osiągnięcia psychologicznego celu maskowania – wprowadzania go w błąd przez uniemożliwienie mu w ogóle spostrzegania, kierowanie jego uwagi na inne (drugorzędne) cele i obiekty, lub doprowadzenie do tego, aby dostrzegane było to, co w rzeczywistości nie istnieje (obiekty pozorne). Jak wskazują doświadczenia minionych wojen [1;138], w maskowaniu powinny obowiązywać następujące zasady psychologiczne:

1. Nic nie widać, nic nie słychać (niedopuszczenie do jakiegokolwiek rozpoznania maskowanego obiektu).

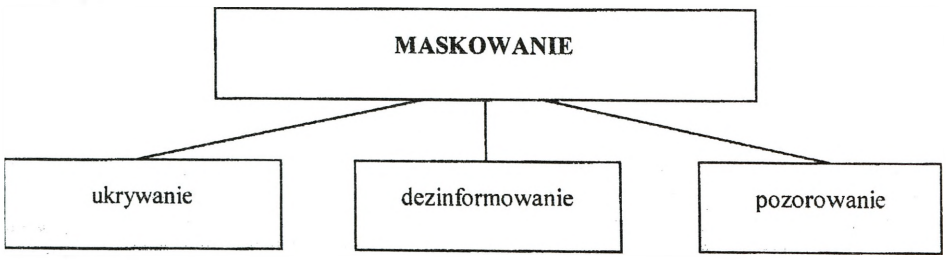
2. Coś widać i słychać, ale nie tam, gdzie znajduje się obiekt (odwrócenie uwagi od zamaskowanego obiektu przez skierowanie jej na inny obiekt).

3. Widać oraz słychać, ale zupełnie coś innego (zniekształcenie obrazu maskowanego obiektu).

Pojęć „widzenie", „słyszenie" nie należy oczywiście rozumieć dosłownie. Zasady te również odnoszą do bodźców dochodzących do środków rozpoznania pośredniego, znajdujących się w wyposażeniu przeciwnika.

Uwzględniając powyższe zasady, rodzaj wykorzystywanych sił i środków oraz cechy charakterystyczne realizacji zadań, można wyróżnić różne formy maskowania, które zilustrowano na rysunku 2.4.

Udział poszczególnych sposobów i przedsięwzięć maskowania w całości podejmowanych działań obronnych związku operacyjnego na poszczególnych szczeblach organizacyj-



Rys. 2.4. Formy maskowania

nych może być różny. **Przeprowadzone badania wskazują, że przedsięwzięcia ukrywania są niezbędne i typowe dla realizacji zadań obrony informacyjnej przed rozpoznaniem bezpośrednim w działaniach obronnych związku operacyjnego. Natomiast przedsięwzięcia dezinformowania i pozorowania powinny mieć swoje odzwierciedlenie również w obronie informacyjnej przed rozpoznaniem pośrednim oraz w zakłócaniu informacyjnym.**

Oznacza to, że wszystkie formy maskowania w działaniach obronnych związku operacyjnego powinny być odpowiednio zsynchronizowane ze sobą w sferze informacyjnej.

Ukrywanie jest to zespół przedsięwzięć i czynności organizacyjnych, mających na celu określenie zasad pracy urządzeń promieniujących energię elektromagnetyczną, zmianę wyglądu zewnętrznego lub maskowanie obiektów, sprzętu, uzbrojenia i ludzi przed rozpoznaniem przeciwnika. Ukrywanie organizuje się stale na wszystkich szczeblach organizacyjnych.

Analiza dostępnej literatury [17;26;52;54;95;138] wskazuje, że ukrywanie uważa się przede wszystkim za domenę maskowania bezpośredniego. Ukrywanie ma na celu uczynienie maskowanego obiektu niewidzialnym. W aspekcie zjawisk psychofizycznych polega ono na dążeniu do uniemożliwienia podmiotom rozpoznania dokonania aktu przedstawienia sobie ukrytych przedmiotów. Istnieją dwa podstawowe sposoby osiągania tego celu.

Pierwszy powinien polegać na fizycznym odizolowaniu maskowanego obiektu od środków rozpoznania przeciwnika. Taki sposób ukrycia charakteryzuje jedną z dwu form ukrywania – **zakrywanie**. Sposób ten pozbawia przeciwnika możliwości spostrzeżenia przedmiotu rozpoznania. Tym samym nie może zaistnieć akt bezpośredniego przedstawienia go sobie. W umyśle prowadzącego rozpoznanie nie powstaje żaden model przedmiotu rzeczywistego, lub powstaje, lecz mocno zniekształcony. Na podstawie takiego przedstawienia podmiot rozpoznania wydaje niewłaściwy sąd o rzeczywistym przedmiocie rozpoznania. Sąd ten znajduje swoje odzwierciedlenie w meldunku rozpoznawczym i w konsekwencji będzie dalej skażał przedstawienia kolejnych podmiotów rozpoznania. A o to przecież chodzi prowadzącemu maskowanie.

Druga forma ukrywania – **kamuflaż** powinna polegać na obniżeniu kontrastu maskowanego przedmiotu poniżej wartości progowej. Powoduje to, najogólniej rzecz biorąc, zlanie się kształtów, barw i wypromieniowanej energii (np. cieplnej) maskowanego przedmiotu z barwą, dominującymi kształtami i energią tła. Efekt kamuflażu jest taki, że obserwator widzi przedmiot rozpoznania, ale go nie postrzega. Oczywiście jest to daleko idące uproszczenie kamuflażu. Podłożem psychofizycznym kamuflażu jest niedoskonałość zmysłów człowieka,

która prowadzi do tego, że sposób, w jaki człowiek przedstawia sobie przedmioty, a wskutek tego i sposób, w jaki o nich sądzi, jest nieuchronnie zależny od jego organizacji. Organizacja ta może być tego rodzaju, iż człowiek dzięki niej wydaje więcej mylnych aniżeli prawdziwych sądów. Swoją niedoskonałą organizację człowiek poprawia stosując różnorodne urządzenia techniczne, dzięki którym stosunkowo łatwo radzi sobie z kamuflażem. Lornetka obniża wartość krytycznego progu kontrastu, kamera termowizyjna pozwala spostrzec różnice temperatur obiektu i tła, a jednoczesna obserwacja wielospektralna komplikuje kamuflaż do potęgi równej liczbie pasm spektrum obserwacji. Jednak mimo tych wszelkich utrudnień, ukrywanie (zarówno zakrywanie, jak i też kamuflaż) odgrywa nadal w maskowaniu rolę szczególną z uwagi na fakt, że dotyczy ono bezpośrednio rzeczywistego przedmiotu rozpoznania. Tym też można tłumaczyć priorytet ukrywania, szczególnie w maskowaniu bezpośrednim. Umożliwia ono bowiem:

- ukrycie sił i środków przed rozpoznaniem patrolowym[16] i specjalnym[17] przeciwnika;
- oszukanie przeciwnika co do położenia wojsk i prowadzonych przez nie działań operacyjnych;
- utrudnienie przeciwnikowi skutecznego oddziaływania elektromagnetycznego i ogniowego oraz podejmowania prawidłowych decyzji.

Ukrywanie w działaniach obronnych związku operacyjnego, w zależności od cech charakterystycznych maskowanych obiektów (urządzeń, ludzi[18], itp.) oraz rodzaju użytych środków celowo jest realizować w wyniku:

---

[16] Rozpoznanie patrolowe to zdobywanie danych o przeciwniku drogą fizycznej (optycznej i akustycznej) penetracji terenu (obszaru) zajmowanego przez przeciwnika. Rozpoznanie patrolowe w związku operacyjnym prowadzą nie tylko etatowe siły i środki, ale i inne rodzaje wojsk, stosownie do potrzeb oraz możliwości. Do elementów ugrupowania patrolowego i elementów patrolowych zalicza się: patrol rozpoznawczy, wóz patrolowy, posterunek obserwacyjny (różnego rodzaju), samolot rozpoznawczy itp. Rozpoznanie patrolowe prowadzone jest przede wszystkim na szczeblu taktycznym [22;59;87].

[17] Rozpoznanie specjalne to prowadzenie działań rozpoznawczych w związku operacyjnym siłami niewielkich grup lub pododdziałów na terenie zajmowanym przez przeciwnika i w ten sposób zdobywanie o nim informacji. Prowadzą je grupy specjalne, grupy specjalne płetwonurków, grupy specjalne kadrowe, grupy rozpoznawcze działające zwykle na tych obszarach przeciwnika, które nie są pokryte innymi rodzajami rozpoznania lub są pokryte, ale w taki sposób, że wiarygodność zdobywanych informacji o przeciwniku jest za mała aby skutecznie kierować wojskami i środkami rażenia. Głębokość usytuowania obszarów rozpoznania specjalnego może być różna, zawsze warunkowana jest możliwościami przerzutu (przenikania) i przetrwania elementów ugrupowania rozpoznawczego. Rozpoznanie specjalne może zdobywać bądź potwierdzać informacje zdobyte z innych źródeł, bez względu na warunki (pogodę, porę roku, doby itp.) i stopień zamaskowania obiektów. Jest w stanie określać rodzaj, charakter, stan i gotowość bojową przeciwnika, a nade wszystko określać dokładne współrzędne wykrywanych obiektów. W szczególnych sytuacjach siły rozpoznania specjalnego mogą być wykorzystywane do wykonywania zadań: dywersyjnych, sabotażowych, psychologiczno-propagandowych i szturmowych, a na własnym terytorium – zadań antyterrorystycznych i przeciwdywersyjnych [22;59;87].

[18] W wyposażeniu współczesnych armii znajduje się wiele środków przeznaczonych do maskowania żołnierzy. Do środków tych można zaliczyć: ubiory maskujące letnie i zimowe (np. mundur polowy z naniesionym wzorem drobnego kamuflażu); siatki maskujące typu peleryny i narzuty; pasty i kremy do nakładania na odsłonięte części ciała.

- maskowania optycznego;
- maskowania akustycznego;
- maskowania termicznego.

Maskowanie optyczne należy stosować przeciw klasycznej, bezpośredniej obserwacji wzrokowej oraz przeciwko środkom walki wyposażonym w aparaturę optyczną wspomaganą techniką laserową i w podczerwieni.

Ukrywanie obiektów przed bezpośrednią obserwacją wzrokową powinno być realizowane przez wykorzystywanie maskujących właściwości terenu oraz stosowanie różnorodnych masek, siatek, powłok absorpcyjnych, dostosowanie obiektów, urządzeń do otaczającego terenu itp. Należy mieć na uwadze, że wykorzystywanie maskujących właściwości terenu oraz jego przystosowanie jest regulaminową powinnością każdego organizatora i uczestnika działań bojowych. Szczególną formą maskowania optycznego jest maskowanie świetlne, które powinno być organizowane przede wszystkim w działaniach nocnych. Dużo zabiegów wymaga maskowanie świateł sprzętu bojowego w czasie marszu. Do jego maskowania należy stosować etatowe komplety urządzeń oraz oprawki zaciemniające wykonane doraźnie z materiałów podręcznych. W rejonach działań sprzęt ten powinien być przygotowany do zaciemnienia wewnętrznego, natomiast obsługi muszą respektować dyscyplinę maskowania oświetlenia zewnętrznego w rejonach ich rozmieszczenia.

W maskowaniu akustycznym należy wykorzystywać maskujące właściwości terenu, szczególnie jego pokrycia (zalesienie, zadrzewienie) i infrastrukturę (budowle i zabudowania). Celowe jest stosowanie przedsięwzięć o charakterze taktycznym, takich jak: unikanie nagłych zmian w natężeniu pracy silników, agregatów prądotwórczych przy dokonywaniu manewru wojsk i zmiany rejonów punktów dowodzenia. Efektywne wykonywanie tego zadania zależy od poziomu wyszkolenia ludzi, a w ślad za tym wyrobienia odpowiednich nawyków w praktycznym działaniu.

Maskowanie termiczne powinno być organizowane w celu przeciwdziałania wykrywaniu obiektów o niewielkiej różnicy temperatur z otoczeniem (około 0,02°C). W tym sposobie maskowania powinny być wykorzystywane ochronne właściwości terenu. Należy stosować maski ochronne zmniejszające kontrast cieplny między obiektami a otoczeniem, a także różnorodne pułapki o prostej konstrukcji, np. zorganizowane paleniska. Można wykorzystywać również makiety wozów bojowych, np. z wmontowanymi silnikami uszkodzonych pojazdów.

Dezinformowanie polega na planowym i systematycznym opracowywaniu i rozpowszechnianiu lub bezpośrednim przekazywaniu przeciwnikowi mylnych wiadomości co do składu, organizacji, zamiaru i struktury obszaru odpowiedzialności obronnej związku operacyjnego. Z badań wynika, że szczególna uwaga powinna być zwrócona na wprowadzenie w błąd przeciwnika odnośnie punktu ciężkości, koncepcji wykorzystania odwodów oraz przyjętego systemu działań obronnych związku operacyjnego (w tym szczególnie ugrupowania operacyjnego i wykorzystania środków rażenia). Przedsięwzięcia dezinformowania powinny stworzyć korzystne warunki dla koncepcji (sposobu) osiągnięcia celu w działaniach obronnych związku operacyjnego. Problematykę dezinformowania jako przedsięwzięcie – przede wszystkim – obrony informacyjnej przed rozpoznaniem pośrednim uczyniono przedmiotem badań szczegółowych, a ich wyniki zamieszczono w podrozdziale 2.2.1.1.

Pozorowanie polega na zorganizowanym działaniu, manewrze i innych przedsięwzięciach o charakterze statycznym lub dynamicznym wojsk w celu stworzenia fałszywego, lecz zbliżonego do rzeczywistości „obrazu" obiektu lub wykonywanych czynności.

W działania obronnych związku operacyjnego pozorowanie powinno spełniać następujące zasadnicze funkcje:

- wprowadzanie w błąd przeciwnika, co do koncepcji wykorzystania elementów systemu obronnego;
- zmuszanie przeciwnika do reakcji pożądanej dla broniących się wojsk związku operacyjnego;
- przygotowanie warunków do wykonania działań rzeczywistych.

Doświadczenia z ćwiczeń oraz rozważania teoretyczne pozwalają przyjąć tezę, że istnieją możliwości wykorzystania przedsięwzięć pozorowania w działaniach obronnych związku operacyjnego. Świadczą one o inicjatywie oraz dążeniu do wykonania zadań kosztem jak najmniejszych strat własnych. Form zastosowania jest wiele. Zależą one od inwencji oficerów sztabu związku operacyjnego, możliwości wojsk, sytuacji operacyjnej, zadania (celu) działań obronnych oraz sposobu ich wykonania (osiągnięcia celu), miejsca i roli w układzie narodowym (koalicyjnym), warunków terenowych itp. Należy pamiętać jednak, że:

- przygotowane i wykonane działania pozorne powinny być w pełni wiarygodne i rzeczywiste;
- nawet najbardziej realne działania pozorne nie mogą wprowadzić w błąd przeciwnika na dłuższy czas;

– zgrupowanie realizujące działania pozorne, w przypadku uzyskania skutków poza planowanymi, winno być zdolne do ich wykorzystania w działaniach bezpośrednich;

– działania pozorne nie mogą być planowane w aspekcie samego działania. Jednocześnie należy planować działania rzeczywiste dla wykorzystania uzyskanej w ten sposób przewagi sytuacyjnej.

Szczegółowe wyniki badań w zakresie pozorowania – jako przedsięwzięcie obrony informacyjnej przed rozpoznaniem pośrednim – zamieszczono w podrozdziale 2.2.1.1.

2.1.3. Ubezpieczanie

Ubezpieczanie stanowi kolejny, niezmiernie ważny element obrony informacyjnej przed rozpoznaniem bezpośrednim w działaniach obronnych związku operacyjnego. W dokumentach normatywnych występuje termin ubezpieczenie[19] jako ważny element zabezpieczenia bojowego działań[20]. Organizuje się je w celu **niedopuszczenia do przenikania elementów rozpoznania przeciwnika do ugrupowania bojowego wojsk oraz zapewnienie im dobrych warunków do przygotowania i prowadzenia działań bojowych.**

Z analizy ćwiczeń prowadzonych w AON w latach 1997 – 2000 wynika, że elementy ugrupowania obronnego związku operacyjnego, przemieszczające się nawet w dużej odległości od granicy państwowej lub będące na postoju, mogą być obserwowane. Mogą też być w każdej chwili obiektami oddziaływania elementów rozpoznania bezpośredniego przeciwnika, grup dywersyjnych, wojsk powietrznodesantowych itp. Szczególnie wrażliwe na ataki grup dywersyjnych są kolumny przemieszczających się wojsk. Również luki w obszarze obrony związku operacyjnego pomiędzy pasami (rejonami) obrony ułatwiają działanie elementom rozpoznawczym, małym pododdziałom i grupom dywersyjnym przeciwnika. Mogą one prowadzić intensywne rozpoznanie bezpośrednie stanowisk dowodzenia i innych elementów ugrupowania obronnego związku operacyjnego oraz niespodziewanie atakować ich wybrane elementy.

---

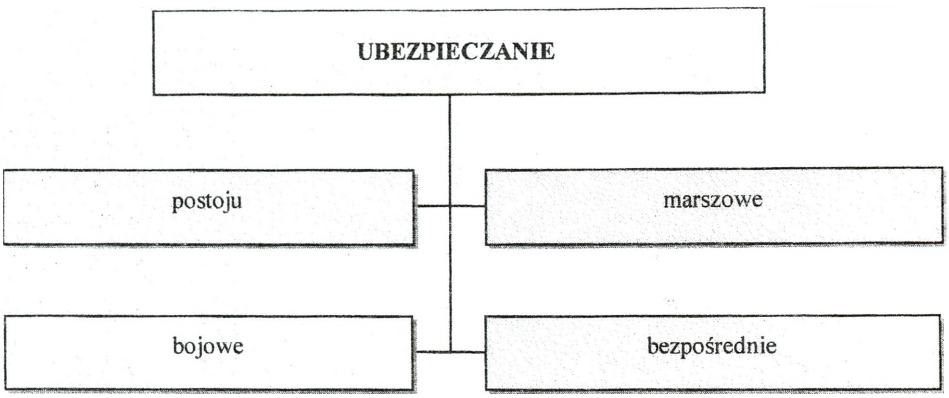
[19] Ubezpieczenie: forma niedokonana – ubezpieczanie to w znaczeniu wojskowym „ochrona wojsk własnych przed niespodziewanym napadem nieprzyjaciela oraz uniemożliwienie mu rozpoznania sił, ilości wojsk". „Słownik języka polskiego", wyd. PWN, Warszawa 1992, tom II, s. 569.

[20] „Regulamin działań wojsk lądowych", wyd. DWLąd, Warszawa 1999.

W zależności od charakteru realizowanych zadań dowództwo i sztab związku operacyjnego oraz dowódcy i sztaby podległych związków taktycznych powinny organizować (rysunek 2.5.):

- w rejonach ześrodkowania (wyjściowym, odpoczynku) – ubezpieczenie postoju.
- w marszu – ubezpieczenie marszowe;
- w walce – ubezpieczenie bojowe.

Dodatkowo w każdej sytuacji należy organizować ubezpieczenie bezpośrednie, którym obejmuje się również stanowiska dowodzenia.



Rys. 2.5. Sposoby ubezpieczania wojsk

Wojska związku operacyjnego znajdujące się w rejonach ześrodkowania powinny ubezpieczać się odpowiednimi elementami ubezpieczenia postoju, tj. oddziałami czat i czatami, wysyłanymi na kierunki ewentualnych zagrożeń ze strony przeciwnika.

Wojska związku operacyjnego wykonujące przegrupowanie powinny ubezpieczać się odpowiednimi elementami ubezpieczenia marszowego, tj. awangardami, ariergardami, szpicami (czołowymi, bocznymi, tylnymi) itp.

Ubezpieczenie bojowe powinno chronić wojska związku operacyjnego przed niespodziewanym atakiem przeciwnika, przenikaniem jego elementów rozpoznania do rejonów działań oraz zmuszać go do wcześniejszego rozwinięcia sił głównych, tj. zgodnie z naszymi zamiarami. Z reguły należy wysyłać je na odległość nie przekraczającą zasięgu ognia środków strzelających na wprost.

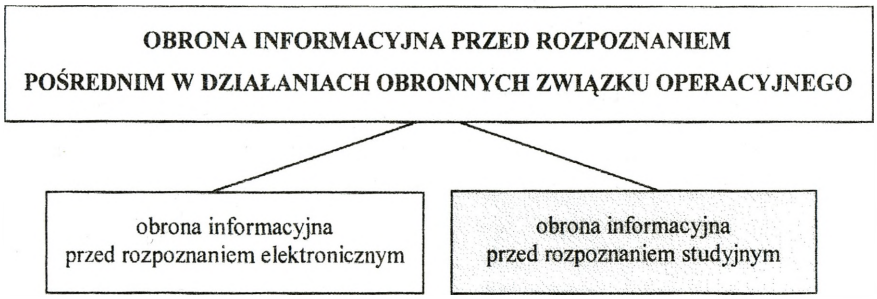
Ubezpieczenie bezpośrednie, pomimo że jest wykonywane najczęściej w działaniach taktycznych, należy organizować również w działaniach obronnych związku operacyjnego

w celu ochrony wybranych elementów ugrupowania operacyjnego np.: stanowisk dowodzenia, naprowadzania uzbrojenia przed niespodziewanym napadem. Należy zapewniać je poprzez aktywne działanie szperaczy, patroli, czujek (podsłuchów), placówek, dyżurnych środków ogniowych, wartowników i in.

2.2. Obrona informacyjna przed rozpoznaniem pośrednim

Jak wynika z analizy literatury przedmiotu badań, **obrona informacyjna przed rozpoznaniem pośrednim w działaniach obronnych związku operacyjnego[21] obejmuje ochronę zbiorów wszelkich postaci danych własnych, które mogą być dostępne dla źródeł rozpoznania przeciwnika, przystosowanych do zdobywania danych w postaci bezpośrednio nieodbieralnej przez układy recepcyjne człowieka.**

Analiza struktury rozpoznania pośredniego przeciwnika [24;59;87] wskazuje, że obrona informacyjna przed nim w działaniach obronnych związku operacyjnego powinna obejmować obronę przed rozpoznaniem elektronicznym oraz ich obronę przed rozpoznaniem studyjnym, co zilustrowane zostało na rysunku 2.6.



Rys. 2.6. Struktura obrony informacyjnej przed rozpoznaniem pośrednim w działaniach obronnych związku operacyjnego

[21] Rozpoznanie pośrednie to zespół skoordynowanych źródeł rozpoznania dostosowanych do zdobywania danych w postaciach bezpośrednio nieodbieranych przez układ recepcyjny człowieka. Pomiędzy zbiorem możliwych postaci danych i zbiorem źródeł rozpoznania występują przetworniki przekształcające ich pierwotnie przechwyconą postać w odbieralną przez układ recepcyjny człowieka. Przetworniki wchodzą w strukturę techniczną źródeł rozpoznania. Istota ich funkcjonowania polega na tym, że zarejestrowany sygnał na wejściu źródła rozpoznania, w formie nieodbieralnej przez człowieka, podawany jest na wejście przetwornika jako wartość sterująca sygnałem odbieranym przez receptory człowieka np. telewizja, gdzie odbierany na wejściu sygnał elektromagnetyczny przetwarzany jest w torze wizyjnym na konkretny obraz, a w torze fonicznym na głos. Zdobywanie danych spoza zasięgu bezpośrednich możliwości recepcyjnych człowieka związane jest z koniecznością wykorzystywania złożonej techniki, rozszerzającej jego możliwości w zakresie widzenia, słyszenia, odczuwania itp. W efekcie tego możliwe jest zdobywanie danych z dużych odległości. Nośnikami danych są najczęściej fale elektromagnetyczne lub efekty akustyczne, sejsmiczne, chemiczne itp., rejestrowane przez różnego rodzaju czujniki, które można przetwarzać w odpowiednio zmodulowane sygnały elektromagnetyczne i przekazywać do układów odbierających. Rozpoznanie pośrednie dzieli się na elektroniczne i studyjne [22;59;66;87].

Wnioski z badań poszczególnych składowych obrony informacyjnej przed rozpoznaniem pośrednim w działaniach obronnych związku operacyjnego stanowią treść kolejnych podrozdziałów pracy studyjnej.

2.2.1. Obrona informacyjna przed rozpoznaniem elektronicznym

W systemach dowodzenia i naprowadzania uzbrojenia związku operacyjnego można wyróżnić wiele różnorodnych i odrębnych elementów. Organizacja i funkcjonowanie tych elementów uwarunkowane jest specyfiką środków technicznych, spełnianą funkcją i przynależnością do określonych dysponentów. Wśród nich ważną rolę spełniają środki elektroniczne, które można podzielić na:

- łączności (radiokomunikacyjne): radiowe (HF[22], VHF[23], radiotelefoniczne, radioliniowe, satelitarne); kablowe (przewodowe, światłowodowe);
- radiolokacyjne;
- radionawigacyjne;
- optoelektroniczne;
- informatyczne.

Tak uszeregowane grupy środków elektronicznych wymagają odpowiedniej, specyficznej ochrony na polu walki. Postęp naukowo-techniczny[24] w dziedzinie elektroniki i informatyki sprawił, że na zakres obrony informacyjnej przed rozpoznaniem elektronicznym duży wpływ ma szereg czynników związanych z powszechną elektronizacją i automatyzacją pola walki, a mianowicie:

- zastosowanie sygnałów elektromagnetycznych o złożonych strukturach widmowych, trudnych do wykrywania przez przeciwnika;
- wykorzystywanie anten o wąskich i zmiennych charakterystykach (z elektronicznym skanowaniem);
- wykonywanie pokryć i środków przeciwradiolokacyjnych oraz dymów pochłaniających i pułapek radiolokacyjnych;

---

[22] HF (ang. High Frequency) – pasmo krótkofalowe: 3 (1,5) – 30 MHz.

[23] VHF (ang. Very High Frequency) – pasmo ultrakrótkofalowe: 30 – 300 MHz.

[24] Szczególnie ważne odkrycia w dziedzinie elektroniki odnotowane zostały w latach sześćdziesiątych XX wieku. W tym okresie zostały opracowane układy scalone, które stanowią podstawę rozwoju w dziedzinie informatyki. Stanowią one również platformę konstrukcyjną źródeł rozpoznania pośredniego nowej generacji. Od tego czasu obserwuje się wyraźną przewagę rozpoznania pośredniego nad bezpośrednim.

– wykorzystywanie detektorów opromieniowania sprzężonych ze środkami imitacji lub maskowania radiolokacyjnego;

– wprowadzanie ograniczeń czasów trwania emisji elektromagnetycznych;

– częste zmiany położenia środków promieniowania energii elektromagnetycznej;

– konieczność zapewnienia bezpieczeństwa systemom i sieciom informatycznym;

– inne czynniki, które powodują konieczność ukrywania zbiorów różnych postaci danych o wojskach własnych.

Obrona informacyjna przed rozpoznaniem elektronicznym[25] w działaniach obronnych związku operacyjnego powinna obejmować zatem **odpowiednio skoordynowane przedsięwzięcia i działania przeciwrozpoznawcze dostosowane do ukrywania pracy systemów i środków elektronicznych oraz zbiorów wszelkich postaci danych o stanie rzeczywistym, usytuowaniu i zamiarach działania w obszarze odpowiedzialności obronnej związku operacyjnego, które są lub mogą być dostępne dla źródeł rozpoznania elektronicznego przeciwnika.**

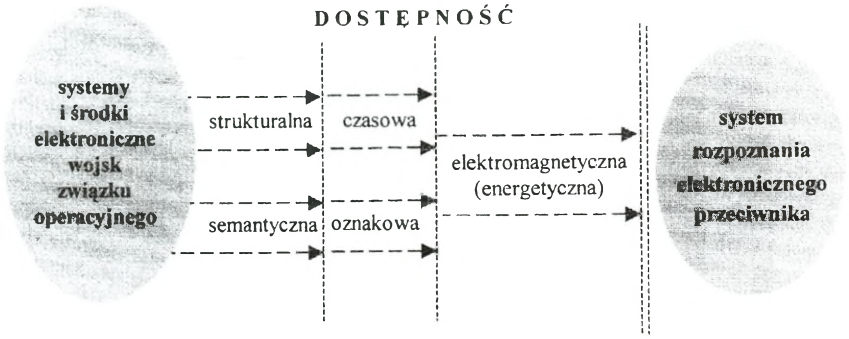
Dostępność systemów i środków elektronicznych dla źródeł rozpoznania elektronicznego przeciwnika w obszarze odpowiedzialności obronnej związku operacyjnego przedstawia rysunek 2.7.

Dostępność elektromagnetyczna (energetyczna) zależy od warunków energetycznych, tj. wymaganego stosunku poziomu sygnału do szumu na wejściu rozpoznawczego urządzenia odbiorczego (w umownym łączu: rozpoznawany nadajnik związku operacyjnego – rozpoznawcze urządzenie odbiorcze przeciwnika).

---

[25] Rozpoznanie elektroniczne zdobywa i przetwarza dane, których nośnikami są fale elektromagnetyczne oraz inne efekty uboczne towarzyszące działaniom zbrojnym (akustyczne, sejsmiczne, magnetyczne, chemiczne, hydroakustyczne, radiacyjne itp.). Rejestracja nośników danych o przeciwniku odbywa się za pomocą odpowiednio skonstruowanych urządzeń elektronicznych. Rozpoznanie elektroniczne w znacznej mierze ma na celu zdobywanie i przetwarzanie tych danych o przeciwniku, których nośnikami są fale elektromagnetyczne (wraz z danymi w nich zawartymi) wypromieniowane przez źródła przeciwnika. Promieniowanie elektromagnetyczne charakteryzuje się długościami fal zawartymi w przedziale 10^{-15} – 10^{8} m. W widmie promieniowania elektromagnetycznego szczególnie wykorzystywana jest druga połowa pasma niższych częstotliwości – od nadfioletu aż do dolnej granicy promieniowania radiowego. Możliwości fal elektromagnetycznych jako nośnika danych są jeszcze bardziej zdumiewające. Tylko w zakresie fal do 100 GHz możliwe jest (przy optymalnym kodowaniu i modulowaniu) przesyłanie w ciągu jednej sekundy 5×10^{10} bitów danych. W tym samym zakresie fal, przy zastosowaniu modulacji częstotliwości (FM), można wykorzystać 2 miliony kanałów przenoszenia. W wyższych zakresach widma elektromagnetycznego, owe możliwości znacznie się zwiększają. W samym zakresie światła widzialnego teoretycznie można przesyłać ilość informacji 1×10^{12} bitów na sekundę. Pełne wykorzystanie właściwości fal elektromagnetycznych, a także uzyskanie w tej dziedzinie określonej przewagi nad przeciwnikiem, daje wiele korzyści w procesie kierowania działaniami na polu walki. Rozpoznanie elektroniczne prowadzi się w każdych warunkach atmosferycznych, czasowych oraz usytuowania bez istotnego zróżnicowania wartości uzyskiwanych efektów. Jest to najszybszy, najbardziej manewrowy i skryty rodzaj rozpoznania wojskowego. Z uwagi na rodzaj rozpoznawanych środków i charakter ich pracy rozpoznanie elektroniczne dzieli się na: radioelektroniczne, radiolokacyjne, optoelektroniczne, czujnikowe, informatyczne [22;59;66;118].

Na przykład: środki łączności radiowej są dostępne elektromagnetycznie w ściśle określonym obszarze, który można określić jako strefę dostępności elektromagnetycznej. Głębokość strefy dostępności elektromagnetycznej zależy przede wszystkim od parametrów równania przepływu mocy w umownym łączu radiowym utworzonym przez ukrywany nadajnik i odbiornik rozpoznawczy przeciwnika.



Rys. 2.7. Dostępność systemów i środków elektronicznych w obszarze odpowiedzialności obronnej związku operacyjnego

Równanie to, uwzględniając najczęściej wykorzystywane w takim łączu rodzaje propagacji fal elektromagnetycznych w działaniach obronnych związku operacyjnego[26] można przedstawić w następujących postaciach:

1. Propagacja fal przyziemnych typu ogólnego (wykorzystywanych przez naziemne środki rozpoznania radiowego przeciwnika podczas rozpoznania naziemnych środków łączności związku operacyjnego):

$$P_o = \frac{P_n G_n G_o}{L_b} \quad (2.1.),$$

[26] Fale rozchodzące się w bliskości powierzchni Ziemi nazywa się **falami przyziemnymi**, spośród których wyróżnia się fale powierzchniowe i fale przestrzenne. **Fale powierzchniowe** są promieniowane przez antenę nadawczą, umieszczoną bezpośrednio na powierzchni Ziemi i rozchodzą się wzdłuż tej powierzchni. **Fale przestrzenne** mogą mieć dwie składowe: bezpośrednią i odbitą. Występują głównie w paśmie VHF, gdy anteny umieszczone są nad powierzchnią Ziemi, co jest możliwe dzięki małym rozmiarom anten wykorzystywanych w tym paśmie częstotliwości. Występują również przy połączeniach między Ziemią a samolotem. Fale, które docierają do odbiorników dzięki odbiciu od jonosfery nazywa się **falami jonosferycznymi** lub **odbitymi**. Por.: D. A Bem, „Anteny i rozchodzenie się fal radiowych", wyd. NT, Warszawa 1973, s. 327.

gdzie:

- P_o - moc sygnału użytecznego przekazywana do odbiornika;
- P_n - moc przekazywana z nadajnika do anteny nadawczej;
- G_n - zysk energetyczny anteny nadawczej;
- G_o - zysk energetyczny anteny odbiorczej;
- L_b - tłumienność trasy radiowej między antenami, określana z zależności:

$$L_b = \frac{R^4}{h_1^2 h_2^2} \quad (2.2.),$$

przy czym:

- R [km] - odległość między antenami nadajnika i odbiornika;
- h_1 [m]- wyniesienie skorygowane anteny nadawczej wyrażane zależnością:

$$h_1 = \sqrt{h_n^2 + h_m^2} \quad 2.3.),$$

- h_2 [m] - wyniesienie skorygowane anteny odbiorczej wyrażane zależnością:

$$h_2 = \sqrt{h_o^2 + h_m^2} \quad (2.4.),$$

- h_n, h_o [m] - wysokość zawieszenia (wzniesienia) anteny nadawczej (odbiorczej) nad ziemią,
- h_m [m] - wyniesienie pozorne anteny przy danej polaryzacji [m] wyrażane zależnością:

$$h_m = \frac{\lambda}{2\pi}\left[(\varepsilon \pm 1)^2 + (60\lambda\sigma)^2\right]^{\pm 1/4} \quad (2.5.),$$

„+"- dla polaryzacji pionowej;

„–" - dla polaryzacji poziomej;

ε, σ - przenikalność elektryczna i konduktywność gruntu na trasie radiowej.

2. Propagacja fal powierzchniowych (wykorzystywanych przez naziemne środki rozpoznania radiowego przeciwnika). W równaniu 2.1. parametr L_b określany jest z zależności:

$$L_b = \frac{R^4}{h_m^4} \quad (2.6.)$$

3. Propagacja fal przestrzennych bezpośrednich (wykorzystywanych przez naziemne środki rozpoznania radiowego podczas rozpoznania powietrznych środków łączności oraz przez powietrzne środki rozpoznania radiowego przeciwnika).

W równaniu 2.1. parametr L_b określany jest z zależności:

$$L_b = \frac{R^4}{h_n^2 h_o^2} \quad (2.7.)$$

4. Propagacja fal odbitych (jonosferycznych) wykorzystywana głównie przez naziemne środki rozpoznania radiowego HF przeciwnika podczas rozpoznania krótkofalowych naziemnych środków łączności związku operacyjnego.

W równaniu 2.1. parametr L_b określany jest z zależności:

$$L_b = \frac{R^4}{h_n^2 h_o^2} \Delta_{Lb} \qquad (2.8.),$$

gdzie:

– Δ_{Lb} - mediana dodatkowej tłumienności [dB] trasy, wywołanej dyfrakcją i rozpraszaniem poza linią horyzontu radiowego [110].

Z równania przepływu mocy 2.1. (postać 1 – 3) wynika, że w łączu radiowym utworzonym przez ukrywany nadajnik i urządzenie rozpoznawcze przeciwnika, głębokość strefy elektromagnetycznej zależy od mocy nadajnika, jego rodzaju pracy oraz wysokości wyniesienia (zawieszenia) anteny nadawczej własnej radiostacji oraz anteny odbiorczej urządzenia rozpoznawczego przeciwnika, długości fali roboczej i jej polaryzacji oraz właściwości elektrycznych gruntu w miejscu i na trasie radiowej (w przypadku propagacji typu ogólnego). Wartości tych parametrów, z wyjątkiem wysokości zawieszenia anteny odbiorczej urządzenia rozpoznawczego przeciwnika, należy odpowiednio kształtować w procesie organizacji i eksploatacji systemów (sieci) łączności szczególnie w obszarze działania sił osłony.

Z analizy warunków propagacji odbitych fal radiowych[27] wynika, że dostępność elektromagnetyczna środków łączności rozmieszczonych w obszarze obrony związku operacyjnego w tym wariancie propagacyjnym (równanie przepływu mocy – postać 4.) jest teoretycznie nieograniczona. W praktyce może być jednak ograniczana dzięki zastosowaniu np. anten kierunkowych zorientowanych równolegle lub w kierunku przeciwnym do przedniego skraju obrony (ang. FEBA[28]).

Dostępność czasową warunkuje czas trwania emisji energii elektromagnetycznej (nadawania) oraz intensywność pracy urządzeń elektronicznych. Jest ona wprost proporcjonalna do wielkości wyżej wymienionych składowych.

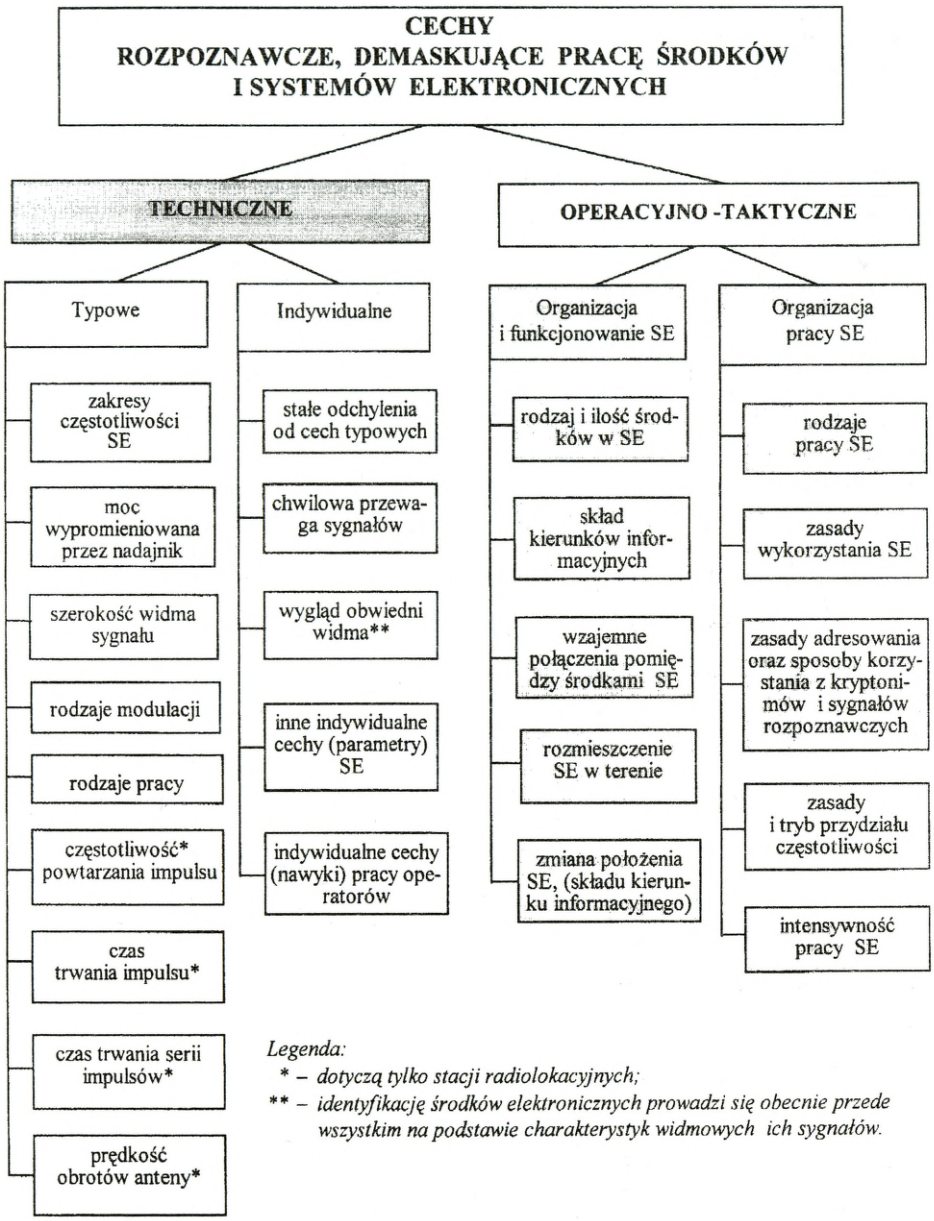
Dostępność oznakowa i strukturalna uwarunkowana jest istnieniem cech (oznak, właściwości) demaskujących pracę środków i systemów elektronicznych (SE). Podział cech rozpoznawczych demaskujących ich pracę przedstawiono na rysunku 2.8.

Techniczne (informacyjne) cechy rozpoznawcze to właściwości urządzeń elektronicznych, które promieniują energię elektromagnetyczną.

---

[27] Tamże, s. 381- 404.
[28] FEBA - ang. Forward Edge the Battle Area.

Wynikają one ze sposobów i rodzajów pracy urządzeń oraz pozwalają jednocześnie na ich rozróżnianie. Można podzielić je na typowe (zbiorowe, ogólne lub grupowe) i indywidualne.



Rys. 2.8. Podział cech demaskujących pracę środków i systemów elektronicznych

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

Indywidualne techniczne cechy rozpoznawcze to wielkości i parametry, według których można określić przynależność środka elektronicznego do rodzaju sił zbrojnych, związku operacyjnego lub taktycznego, do odpowiedniego stanowiska dowodzenia lub dowódcy (osoby funkcyjnej) oraz wyróżnić go spośród tej samej klasy (tego samego typu).

Operacyjno-taktyczne cechy rozpoznawcze to takie charakterystyki, według których określa się zasady organizacji i wykorzystania środka promieniowania elektromagnetycznego w systemach dowodzenia i naprowadzania uzbrojenia. Powyższe cechy pozwalają określić skład bojowy i ugrupowanie wojsk oraz wnioskować o jego działaniach i zamiarach. Można podzielić je na następujące grupy:

- cechy charakterystyczne organizacji i funkcjonowania SE;
- cechy charakterystyczne organizacji pracy SE.

Zaprezentowany podział cech rozpoznawczych, demaskujących pracę środków elektronicznych pozwala postawić tezę, że wynikają one z określonego sposobu wykorzystania tych środków, przynależności do kraju, rodzaju sił zbrojnych, rodzaju uzbrojenia, organu dowodzenia i właściwości pracy w systemach dowodzenia i sterowania środkami walki.

Cechy te umożliwiają organom rozpoznania elektronicznego zidentyfikowanie sygnałów emitowanych przez te środki, a przez to ich lokalizację, określenie składu oraz ich przynależności do szczebla dowodzenia.

Należy mieć na uwadze, że współczesne systemy i środki rozpoznania elektronicznego są przystosowane zarówno do odbioru fal elektromagnetycznych emitowanych przez źródła (urządzenia nadawcze) jak i do prowadzenia analizy technicznej. Wartość rozpoznawczą poszczególnych źródeł ustala się na podstawie określonych w procesie rozpoznania elektronicznego ich cech rozpoznawczych (informacyjnych).

Dostępność semantyczną warunkuje stopień utajnienia wiadomości przekazywanych w systemach elektronicznych (radiokomunikacyjnych, radionawigacyjnych i in.).

Obronę informacyjną przed rozpoznaniem elektronicznym należy ukierunkować na ograniczanie do niezbędnego minimum dostępności elektromagnetycznej (energetycznej), czasowej, oznakowej, strukturalnej i semantycznej nadawczych środków i urządzeń elektronicznych w strefach i sektorach niepożądanych, tj. poza przedni skraj obrony. Istota działań w tym zakresie powinna polegać na ochronie urządzeń nadawczych, promieniujących energię elektromagnetyczną, a także na ochronie treści danych zawartych w tej energii (emitowanych sygnałach). Obrona przed skutkami rozpoznania elektronicznego powinna być działaniem

pierwszoplanowym organizatorów systemów elektronicznych oraz bezpośrednich użytkowników urządzeń wchodzących w ich skład.

Do głównych zadań obrony informacyjnej przed rozpoznaniem elektronicznym w działaniach obronnych związku operacyjnego[29] należy zaliczyć:

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

Niszczenie technicznych środków rozpoznania ich nosicieli oraz punktów zbierania i przetwarzania danych należy traktować jako jedno z ważniejszych zadań na polu walki. Może ono przyjmować formę zakłócania niszczącego[30] (kinetycznego lub elektromagnetycznego). Jest, więc aktywną formą walki informacyjnej (tj. zakłócania informacyjnego), w której część zadań wykonuje się na rzecz obrony informacyjnej. Do zwalczania technicznych środków rozpoznania przeciwnika należy przewidywać wykorzystanie w działaniach obronnych związku operacyjnego: grup specjalnych, oddziałów wydzielonych, wojsk rakietowych i artylerii, lotnictwa wojsk lądowych, desantów oraz innych elementów działających w głębi ugrupowania przeciwnika. Problematyka ta jest przedmiotem szczegółowych badań specjalistów w tej dziedzinie i wykracza poza ramy pracy studyjnej.

Zagłuszanie środków rozpoznania przeciwnika jest również aktywną formą walki informacyjnej (tj. zakłócania informacyjnego), w której część działań wykonuje się na rzecz obrony elektronicznej. Polega na zakłócaniu pracy urządzeń odbiorczych środków elektronicznych systemu rozpoznania przeciwnika.

Jednym z zasadniczych warunków obezwładniania zakłóceniami obiektów elektronicznych jest możliwość przechwycenia i wykrycia ich promieniowania. Niektóre środki rozpoznania elektronicznego[31] nie promieniują energii elektromagnetycznej w przestrzeń, lecz przechwytują promieniowanie rozpoznawanych urządzeń nadawczych. Praca „na odbiór"

---

[29] Należy mieć na uwadze, że ze względu prowadzenie rozpoznania elektronicznego przez potencjalnego przeciwnika w okresie pokoju, kryzysu i w czasie wojny, obrona informacyjna przed nim powinna być prowadzona ciągle. W okresie pokoju i kryzysu obrona informacyjna przed rozpoznaniem elektronicznym powinna polegać na przestrzeganiu zasad wykorzystania urządzeń elektronicznych określonych instrukcjami eksploatacyjnymi oraz przepisami o ochronie informacji niejawnych. Szczególna uwaga powinna być zwrócona na maskowanie wojsk i obiektów przed rozpoznaniem satelitarnym [73], eliminowanie ich cech demaskujących, wykorzystanie maskujących właściwości terenu, warunków atmosferycznych, etatowych i podręcznych środków maskowania itp. Należy również nadać odpowiednią rangę planowaniu i organizowaniu obrony informacyjnej oraz szkoleniu sztabów i wojsk w tym zakresie.

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

[31] Problem dotyczy środków rozpoznania radioelektronicznego.

nadaje im charakter pasywny, uniemożliwia zatem ich wykrycie, a w związku z tym i obezwładnienie zakłóceniami.

Pasywne środki rozpoznania elektronicznego, tj. rozpoznania radioelektronicznego, czujnikowego i informatycznego można obezwładnić zakłóceniami pośrednio. Oznacza to, że uwaga powinna być zwrócona na obezwładnienie zakłóceniami środków elektronicznych kierowania rozpoznaniem, które mogą być autonomiczne lub zewnętrzne, współdziałające z tym systemem rozpoznania. W obu wypadkach zapewniają one kierowanie rozpoznaniem przez:

- przesyłanie danych rozpoznawczych do centrum zbioru i ich opracowanie;
- przesyłanie danych na stanowiska dowodzenia związku operacyjnego, jego związków taktycznych i oddziałów;
- wysyłanie komend do wykonania nowych (kolejnych) zadań rozpoznania.

Elektroniczne środki sterowania rozpoznaniem promieniują i odbierają energię elektromagnetyczną, co pozwala na ich wykrycie, identyfikację i obezwładnienie zakłóceniami.

Aktywne środki rozpoznania elektronicznego, tj. radiolokacyjne i optoelektroniczne wykrywające obiekty wojskowe i technikę bojową działają na zasadzie emisji i odbioru własnej energii elektromagnetycznej. Są zatem możliwe zarówno do wykrycia, jak i zakłócenia.

Zagłuszanie środków rozpoznania elektronicznego przeciwnika powinno być wykonywane w działaniach obronnych związku operacyjnego w ramach zakłócania informacyjnego. Problematyka ta wykracza poza ramy pracy studyjnej.

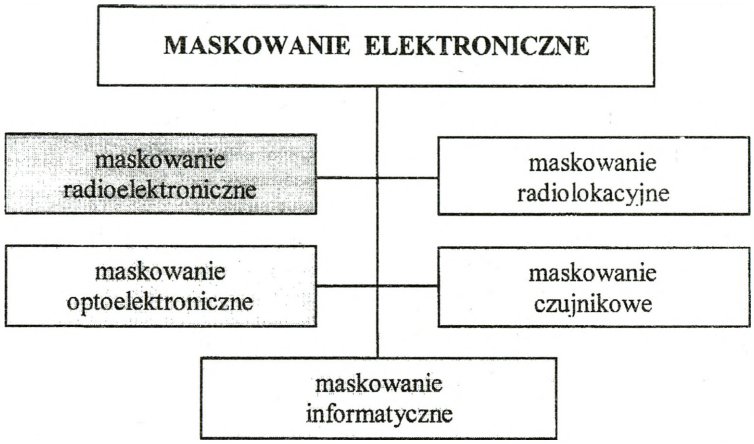
Zapewnienie bezpieczeństwa własnym systemom (środkom) elektronicznym jest głównym zadaniem obrony informacyjnej przed rozpoznaniem elektronicznym w działaniach obronnych związku operacyjnego. Obejmuje ono zespół odpowiednio skoordynowanych przedsięwzięć i działań podejmowanych w związku operacyjnym w ramach maskowania wojsk i obiektów.

Przeprowadzona analiza historyczna dowodzi, że zakres maskowania zmienia się wraz z rozwojem środków rozpoznania i środków rażenia. W okresie pierwszej wojny światowej problem maskowania dotyczył przede wszystkim strefy frontu. W czasie drugiej wojny światowej maskowaniem obejmowano nie tylko obszary zmagań wojennych, lecz także ludność i terytorium poza frontem walczących wojsk. Stosowano wówczas maskowanie strategiczne, operacyjne i taktyczne.

Współcześnie znaczenie maskowania wzrosło jeszcze bardziej. Jest to spowodowane pojawieniem się nowych środków rozpoznania oraz broni precyzyjnego rażenia, umożliwiającej niszczenie małych (punktowych) celów ze znacznych odległości. Przykładem może być wojna w rejonie Zatoki Perskiej (1991), w której maskowanie było jednym z najważniejszych

elementów [1;105;109]. Wojska koalicji antyirackiej stosowały malowanie deformujące sprzętu bojowego (kamuflaż pustynny), pokrycia maskujące (siatki stosowane przede wszystkim do maskowania artylerii i czołgów na stanowiskach ogniowych). Wojska irackie natomiast z powodzeniem stosowały makiety czołgów, dział i wyrzutni rakietowych.

Z powyższego wynika, że maskowanie na współczesnym polu walki powinno być realizowane w szerokim zakresie widma promieniowania elektromagnetycznego. Zakres i charakter tych przedsięwzięć powinien być uzależniony od rodzajów maskowanych obiektów elektronicznych. Wyniki badań przemawiają za tym, aby postrzegać je jako maskowanie elektroniczne o strukturze przedstawionej na rysunku 2.9.



Rys. 2.9. Struktura maskowania elektronicznego

Wnioski ze szczegółowych badań poszczególnych rodzajów maskowania elektronicznego zostały przedstawione w kolejnych podrozdziałach pracy.

2.2.1.1. Maskowanie radioelektroniczne

Jak wynika z analizy literatury przedmiotu badań[32], **maskowanie radioelektroniczne ma na celu utrudnienie lub uniemożliwienie zdobywania i przetwarzania tych danych o wojskach i obiektach związku operacyjnego znajdujących się w obszarze jego odpo-**

[32] Przedstawione treści podrozdziału zostały opracowane na podstawie badań, które zapoczątkowało opracowanie studyjne dotyczące obrony radioelektronicznej. J. Janczak, „Obrona radioelektroniczna", wyd. WSOWŁ, Zegrze 1993.

wiedzialności obronnej, których nośnikami są fale elektromagnetyczne wypromieniowane przez będące w ich wyposażeniu systemy radioelektroniczne.

Maskowanie radioelektroniczne[33] wymaga uwzględnienia na współczesnym polu walki wszelkich środków i sposobów rozpoznania stosowanych przez przeciwnika. Należy również uwzględnić specyfikę maskowanych systemów radioelektronicznych. Ze względu na rodzaj maskowanych systemów radioelektronicznych występujących w związku operacyjnym można wyróżnić:

- maskowanie systemów (sieci) łączności bezprzewodowej: radiowej HF i VHF, radiotelefonicznej, radioliniowej, satelitarnej;
- maskowanie systemów (stacji) radiolokacyjnych;
- maskowanie systemów (stacji) radionawigacyjnych;
- maskowanie systemów rozpoznania radioelektronicznego.

Maskowanie radioelektroniczne – ze względu na cechy charakterystyczne realizacji zadań w działaniach obronnych związku operacyjnego oraz ilość i rodzaj wykorzystywanych sił i środków – podzielono na trzy grupy szczegółowe, nazywane również **formami maskowania[34], tj.: ukrywanie, dezinformowanie, pozorowanie radioelektroniczne** i uczyniono przedmiotami badań w kolejnych podrozdziałach pracy studyjnej.

Problematyka **ukrywania** nabiera szczególnego znaczenia w działaniach obronnych, które w odniesieniu do środków i obiektów radioelektronicznych utożsamiane jest najczęściej z maskowaniem radioelektronicznym[35]. Zapis ten jest mało precyzyjny, ponieważ pojęcie „maskowanie[36] radioelektroniczne" jest pojęciem szerszym, obejmującym ukrywanie oraz dezinformowanie i pozorowanie radioelektroniczne.

Przez **ukrywanie radioelektroniczne należy rozumieć zespół przedsięwzięć organizacyjnych i technicznych, polegających na świadomym wprowadzaniu częściowych lub całkowitych zakazów promieniowania energii elektromagnetycznej przez środki radioelektroniczne w wybranych rejonach, na wybranych kierunkach, w określonych przedziałach czasowych oraz pozbawianie wojsk i obiektów radioelektronicznych cech demaskujących w celu wprowadzenia rozpoznania przeciwnika w błąd co do ugrupowa-**

---

[33] W niektórych publikacjach używa się pojęcia „maskowanie radiowe", nie definiując go. Ograniczane jest wówczas jedynie do maskowania środków radiowych HF i VHF.

[34] Podział maskowania radioelektronicznego autor przyjął na podstawie oceny literatury źródłowej oraz badań własnych [59;66].

[35] Np. instrukcja o maskowaniu wojsk, cz. II, „ Zasady maskowania operacyjnego" wyd. Szt. Gen. WP, Warszawa 1977, s. 11.

[36] Zdefiniowane zostało w podrozdziale 2.1.2. niniejszej pracy studyjnej.

nia, składu i działalności wojsk lub ich zamiarów w obszarze odpowiedzialności obronnej związku operacyjnego.

Istota ukrywania radioelektronicznego polega na dążeniu do całkowitego wyeliminowania możliwości wykrycia przez rozpoznanie radioelektroniczne pojedynczych i zespołowych obiektów radioelektronicznych oraz miejsc ich rozmieszczenia, przemieszczenia oraz zasad pracy urządzeń promieniujących energię elektromagnetyczną. Dotyczyć może całego obszaru obrony związku operacyjnego lub wybranych elementów ugrupowania (rejonów) znajdujących się w tym obszarze.

Przeprowadzone badania upoważniają do podziału ukrywania radioelektronicznego na dwie składowe: operacyjne ukrywanie radioelektroniczne i bezpośrednie ukrywanie radioelektroniczne.

Szereg przedsięwzięć wykonywanych w ramach obu składowych przeplata się i wzajemnie zazębia w obszarze odpowiedzialności obronnej związku operacyjnego, a granica między tymi przedsięwzięciami zaciera się wraz z elektronizacją pola walki. Różnica między tymi rodzajami ukrywania radioelektronicznego wynika z ich celów. O ile operacyjne ukrywanie radioelektroniczne organizuje się w celu ukrycia przygotowań do działań obronnych, ugrupowania operacyjnego, a także ukrycia opłacalnych celów dla uderzeń ogniowych, o tyle bezpośrednie ukrywanie radioelektroniczne będzie obejmować czynności zmierzające do ukrycia pododdziałów, oddziałów i związków taktycznych w ramach zabezpieczenia bojowego ich działań. Z tych względów realizacja zadań bezpośredniego ukrywania radioelektronicznego powinna być regulaminowym obowiązkiem wojsk związku operacyjnego, mających w swoim wyposażeniu środki i urządzenia radioelektroniczne.

Należy nadmienić, że ukrywanie radioelektroniczne trzeba realizować w pełnym wymiarze zarówno w okresie pokoju, kryzysu jak i wojny. Obowiązek ten wynika z zasad prowadzenia współczesnego rozpoznania radioelektronicznego przez przeciwnika [59], które ma największe możliwości zdobywania danych rozpoznawczych właśnie w okresie pokoju, tj. podczas ćwiczeń wojsk, codziennego szkolenia na poligonach, w ośrodkach garnizonowych i w przykoszarowych ośrodkach szkolenia.

Z powyższego wynika, że w okresie tym powinno się dążyć do wprowadzania potencjalnego przeciwnika w błąd odnośnie: planów mobilizacyjnych, składu, przeznaczenia, charakteru działalności, wyszkolenia, zdolności i gotowości bojowej, systemu dowodzenia wojskami, rozmieszczenia rejonów alarmowych, przeznaczenia i możliwości taktyczno-technicznych nowych środków radioelektronicznych wojsk związku operacyjnego.

Doświadczenia z minionych wojen, lokalnych konfliktów zbrojnych i ćwiczeń wojsk wykazują, że przedsięwzięcia **operacyjnego ukrywania radioelektronicznego** podczas działań obronnych związku operacyjnego będą najczęściej miały miejsce:

– w stosunku do systemów radioelektronicznych jednego związku taktycznego pierwszego rzutu (oddziału) w celu wprowadzenia przeciwnika w błąd co do przebiegu rzeczywistego pasa (rejonu) obrony;

– w odniesieniu do elementów systemu dowodzenia i naprowadzania uzbrojenia odwodu ogólowojskowego (lub jego części);

– w celu ukrycia szczególnie ważnych elementów ugrupowania operacyjnego, np. zgrupowań artylerii;

– w celu ukrycia związków (oddziałów) nowo przybyłych w obszar obrony związku operacyjnego itp.

Odrębną kwestią jest zapewnienie dowodzenia ze związkami taktycznymi i oddziałami podlegającymi ukrywaniu operacyjnemu w obszarze obrony związku operacyjnego. Powinien wówczas obowiązywać całkowity zakaz pracy środków radioelektronicznych (promieniujących energię elektromagnetyczną) na nadawanie. Dowodzenie powinno odbywać się poprzez stanowiska znajdujących się w pobliżu jednostek lub skryte podłączenie się ukrywanych jednostek do stacjonarnych elementów operacyjno-taktycznej sieci łączności związku operacyjnego. Wewnątrz ukrywanych jednostek dowodzenie powinno być oparte na wykorzystaniu kablowych (przewodowych, światłowodowych) linii łączności stacjonarnych. Bez względu na odległość od przedniego skraju obrony nie należy stosować środków promieniujących energię elektromagnetyczną. Dotyczy to radiostacji VHF małej mocy, radiotelefonów, a także telefonów komórkowych – w obawie przed rozpoznaniem satelitarnym [73] lub powietrznym rozpoznaniem radioelektronicznym[37].

Z powyższego wynika, że samo operacyjne ukrywanie radioelektroniczne nie przyniesie oczekiwanego rezultatu w obszarze odpowiedzialności obronnej związku operacyjnego, jeżeli nie wykona się innych przedsięwzięć maskowania operacyjnego.

Ważnym elementem działań obronnych związku operacyjnego jest **bezpośrednie ukrywanie radioelektroniczne.** Realizacja przedsięwzięć w tym zakresie powinna odzwierciedlać specyfikę ukrywanych systemów (środków) radioelektronicznych w obszarze obrony związku operacyjnego. Spośród systemów radioelektronicznych związku operacyjnego do-

[37] Podniesienie w górę radioelektronicznego środka rozpoznawczego w zakresie VHF o 1 kilometr zwiększa jego zasięg rozpoznawczy o 124 km [4].

godnymi źródłami dla rozpoznania w pasach (rejonach) obrony związków taktycznych (oddziałów) są przede wszystkim systemy łączności, systemy (stacje) radiolokacyjne oraz systemy rozpoznania radioelektronicznego.

Badania wykazały, że **ukrywanie systemu łączności**[38] **związku operacyjnego** należy ukierunkować na ograniczenie do niezbędnego minimum dostępności[39] elektromagnetycznej (energetycznej), czasowej, oznakowej, strukturalnej i semantycznej wchodzącej w jego skład sieci telekomunikacyjnej[40] w strefach i sektorach niepożądanych, tj. poza obszarem sił przesłaniania związku operacyjnego. Obrona przed skutkami rozpoznania radioelektronicznego powinna być zatem działaniem pierwszoplanowym organizatora systemu (sieci) łączności oraz bezpośrednich użytkowników i załóg środków łączności.

Istota działań w tym zakresie powinna polegać **na ochronie urządzeń nadawczych, promieniujących energię elektromagnetyczną oraz na ochronie danych zawartych w tej energii.** W tym celu należy podjąć szereg przedsięwzięć organizacyjnych i technicznych. Przykładowe przedsięwzięcia organizacyjne w zakresie **ograniczenia dostępności elektromagnetycznej systemu (sieci) łączności** w obszarze odpowiedzialności obronnej związku operacyjnego zostały przedstawione na rysunku 2.10.

Praca środków łączności na minimalnie niezbędnych mocach jest jednym z najprostszych sposobów ograniczania strefy dostępności elektromagnetycznej. Z równania przepływu mocy w łączu radiowym (zależność 2.1.) wynika, że niezależnie od rodzaju propagacji fal radiowych moc nadajnika (P_n) jest wprost proporcjonalna do czwartej potęgi zasięgu łączności (R). Oznacza to, że sygnały nadajnika pracującego z mocą (P_1) mogą być przechwytywane na określonych kierunkach przez urządzenie rozpoznawcze przeciwnika z odległości nie większej niż (R_1). Jest to głębokość strefy dostępności elektromagnetycznej na tych kierunkach. Ograniczając moc nadajnika do (P_2) spowoduje się zmniejszenie strefy dostępności elektromagnetycznej do R_2 zgodnie z zależnością:

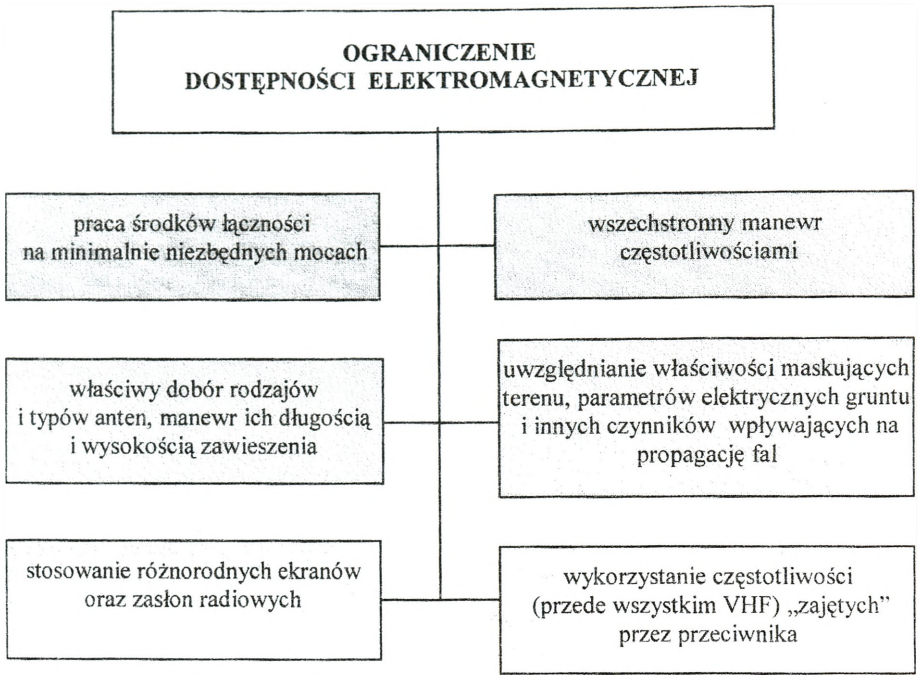
$$R_2 = R_1 \sqrt[4]{\frac{P_2}{P_1}} \quad (2.9.)$$

---

[38] System łączności jest to zespół urządzeń i linii telekomunikacyjnych, środków i linii pocztowych, środków sygnalizacyjnych oraz zasad ich współdziałania. Por.: J. Michniak, Zb. Fiołna, „Sieć łączności państwa", wyd. AON, Warszawa 2001, s. 9.

[39] Problematyka ograniczania dostępności elektromagnetycznej została przedstawiona w podrozdziale 2.2.1.

[40] Sieć telekomunikacyjna to zespół aparatów przetwórczych, linii i stacji teletransmisyjnych, central telefonicznych i telegraficznych, central komutacji pakietów, radiostacji oraz innych urządzeń telekomunikacyjnych znajdujących się na określonym obszarze, powiązanych ze sobą technicznie i przeznaczonych do świadczenia usług telekomunikacyjnych. Sieć telekomunikacyjna związku operacyjnego składa się z węzłów telekomunikacyjnych, linii telekomunikacyjnych oraz elementów nadzoru i zarządzania. Por.: J. Michniak, Zb. Fiołna, „Sieć łączności państwa", wyd. AON, Warszawa 2001, s. 14 - 15.



Rys. 2.10. Ograniczenie dostępności elektromagnetycznej systemu (sieci) łączności w obszarze odpowiedzialności obronnej związku operacyjnego

Ukrywanie systemów (sieci) łączności w działaniach obronnych związku operacyjnego przez zmniejszenie mocy ich nadajników możliwe jest tylko w przypadkach, gdy głębokość strefy dostępności elektromagnetycznej podczas pracy z minimalną mocą jest mniejsza niż odległość miejsca rozwinięcia środków nadawczych od przedniego skraju obrony.

Z powyższego wynika, że dotyczy to środków VHF i urządzeń łączności rozmieszczanych przede wszystkim poza rejonami obrony brygad pierwszorzutowych. Głębokość strefy dostępności elektromagnetycznej powinno się oceniać i określać oddzielnie w odniesieniu do naziemnych i powietrznych środków rozpoznania radiowego przeciwnika.

Dobór właściwego rodzaju i typu anten należy do dowódców elementów łączności; od nich też wymaga się użytkowania właściwych systemów antenowych. Powinni oni dążyć do tego, aby korzystać z anten o najmniejszym zysku energetycznym w umownym łączu: własny nadajnik – odbiornik rozpoznawczy przeciwnika, przy możliwie największej wartości tego parametru w łączu nadajnik – odbiornik korespondenta. Oznacza to, że najkorzystniej jest stosować anteny kierunkowe o wąskim listku głównym charakterystyki promieniowania i jak

najmniejszym poziomie listków bocznych. Wymagane właściwości mają anteny promieniowe z falą bieżącą – w grupie radiostacji małej mocy oraz częściowo anteny stacji radioliniowych.

Z badań wynika [załącznik 1 i 2.], że można skutecznie ukryć przed rozpoznaniem radioelektronicznym: radiostacje małej mocy rozmieszczone w odległości poniżej dwóch kilometrów; stacje radioliniowe szczebla taktycznego rozmieszczone powyżej 5 km i stacje radioliniowe szczebla operacyjnego rozmieszczone powyżej 10 km od przedniego skraju obrony. Jest to możliwe wtedy, gdy topologia systemu (sieci) łączności umożliwia orientowanie anten kierunkowych tych środków łączności w stosunku do przedniego skraju obrony pod takimi kątami, przy których głębokość strefy dostępności elektromagnetycznej będzie mniejsza niż oddalenie od niej ukrywanych radiostacji (stacji radioliniowych). Wartości tych kątów zależą od typu anten i mieszczą się w granicach od 50^0–130^0 do10^0– 170^0.

Mimo niewątpliwych zalet anten kierunkowych (szczególnie anten radiostacji VHF), mają one również szereg wad, mianowicie:

- dużą wrażliwość na zniszczenie środkami ogniowymi;
- możliwość zapewnienia łączności tylko na postoju oraz wówczas, gdy znane są miejsca rozmieszczenia korespondentów;
- konieczność zwijania i rozwijania w celu zmiany ich orientacji (z wyjątkiem anten radioliniowych);
- trudności w zapewnieniu łączności w sieciach radiowych.

Niedostatki te mogą być częściowo usunięte przez wyposażenie radiostacji nowej generacji w tzw. anteny adaptywne, które zapewniają elektroniczne skanowanie wiązki, czyli elektroniczny manewr kierunkiem i wartością energii elektromagnetycznej emitowanej w jednej lub kilku wąskich wiązkach (zależnie od sposobu organizacji łączności) przy silnym stłumieniu sygnałów w obszarze promieniowania niepożądanego.

Wykorzystywanie anten prętowych, w które powszechnie wyposażone są radiostacje VHF związków taktycznych i oddziałów jest niekorzystne z punktu widzenia przeciwdziałania rozpoznaniu radioelektronicznemu przeciwnika. Mają one dookólne charakterystyki promieniowania, a głębokość strefy dostępności elektromagnetycznej środków łączności wykorzystujących te anteny wzrasta z ich zyskiem energetycznym i jest wprost proporcjonalna do zasięgu łączności [załącznik 3.]. Mimo to wykorzystując radiostacje VHF z antenami prętowymi, które z uwagi na ich dużą manewrowość nazywane są coraz częściej radiostacjami pola walki [14] należy przestrzegać następujących zasad:

1. Wartość ich zysku energetycznego rośnie wraz z ich wysokością [załącznik 4.]. Tak, więc w celu ograniczenia dostępności elektromagnetycznej radiostacji należy stosować jak najkrótsze anteny, przy których wykorzystaniu jest możliwe zapewnienie łączności.

2. Jednym z najskuteczniejszych sposobów ograniczenia strefy dostępności elektromagnetycznej jest odkształcenie charakterystyk promieniowania anten dookólnych za pomocą różnorodnych ekranów. W charakterze ekranów mogą być wykorzystywane nieprzezroczyste dla fal elektromagnetycznych obiekty i przedmioty, jeśli przewyższają o ponad 10% wysokość anteny i są oddalone na odległość 12 – 25% długości fali roboczej nadajnika w kierunku przeciwnika [załącznik 5.]. Do odkształcenia charakterystyk promieniowania anten prętowych mogą być wykorzystywane żelazne i żelbetonowe słupy przewodowych linii telekomunikacyjnych, energetycznych linii przesyłowych, elektrycznych trakcji kolejowych oraz mosty, wiadukty, obiekty przemysłowe, zabudowania mieszkalne i inne. W wypadku wozów dowodzenia należy zwrócić uwagę, aby wykorzystywane ekrany nie wykluczały możliwości utrzymania łączności z korespondentami rozmieszczonymi bliżej przedniego skraju obrony (głównie łączności z podwładnymi). Umiejętne stosowanie sztucznych i naturalnych elementów umożliwia ograniczenie głębokości strefy dostępności elektromagnetycznej, np. radiostacji małej mocy z 14 –17 km do rzędu kilkuset metrów [załącznik 6.]. Z powyższego wynika, że przedsięwzięcie to może być skutecznie wykorzystane nawet przez wojska związku operacyjnego prowadzące działania obronne nawet w obszarze sił przesłaniania.

3. Znaczne zmniejszenie głębokości strefy dostępności elektromagnetycznej można uzyskać zmniejszając wysokość zawieszenia anten ukrywanych radiostacji [załącznik 7.]. Gdy dąży się do wyeliminowania dostępności elektromagnetycznej środka łączności, to wówczas należy unikać umieszczania ich anten na masztach, a jeśli jest to konieczne, należy anteny zawieszać na ich najmniejszych wysokościach, przy których jest możliwe zapewnienie łączności.

Kolejnym czynnikiem wywierającym wpływ na głębokość strefy dostępności elektromagnetycznej środków łączności, zwłaszcza z zakresu VHF, są warunki terenowe[41]. Podczas wyboru rejonów i stanowisk do rozwijania środków łączności w obszarze odpowiedzialności obronnej związku operacyjnego powinny być uwzględniane, obok obecności masek naturalnych, również parametry elektryczne gruntu (przenikalność elektryczna i konduktywność

[41] Warunki terenowe powinny być oceniane również pod kątem stref dostępności elektromagnetycznej w toku planowania systemu (sieci) łączności w działaniach obronnych związku operacyjnego. Odpowiedzialność za tę oceną ponosi zespół łączności i informatyki centrum wsparcia dowodzenia SD związku operacyjnego.

gruntu) na trasie radiowej. Parametry te są wielkościami złożonymi i ich wartość zmienia się w miarę struktury powłoki ziemskiej, jej poszycia oraz warunków atmosferycznych. Uśrednione wartości tych parametrów przedstawione są w tabeli 2.1.

Tabela 2.1.

UŚREDNIONE PARAMETRY ELEKTRYCZNE ŚRODOWISKA NATURALNEGO POWŁOKI ZIEMI

Rodzaj powłoki	Przenikalność elektryczna gruntu [ε]	Konduktywność gruntu [σ]
Woda morska	80	4
Woda rzeczna (jeziora)	80	10^{-3}
Gleba bardzo wilgotna	20	10^{-1}
Gleba średnio wilgotna	10	10^{-2}
Gleba sucha	5	10^{-3}
Lasy	-	10^{-3}
Duże miasta, góry	-	$7,5 - 10^{-4}$

Z badań wynika, że głębokość strefy dostępności elektromagnetycznej maleje wraz z pogarszaniem się parametrów elektrycznych gruntu [załącznik 8.]. Zjawisko to jest następstwem zwiększenia się głębokości wnikania fal elektromagnetycznych w grunt w wyniku pogarszania się jego przewodności właściwej, co powoduje wzrost strat wynikających z wytłumienia części emitowanej przez antenę energii w półprzewodzącym środowisku powłoki ziemskiej. Oznacza to, że w celu ograniczenia dostępności elektromagnetycznej środków łączności radiowej należy je rozwijać, jeśli jest to możliwe, w rejonach oddzielonych od przedniego skraju obrony lasami, terenami miejskimi, obiektami przemysłowymi, gruntami piaszczystymi lub skalistymi. Poza tym należy uwzględnić zmienność parametrów elektrycznych gruntu występujących pod wpływem warunków atmosferycznych. Suche piaszczyste gleby oraz średnio wilgotne pola i łąki w okresie wiosennym po mroźnej i śnieżnej zimie, w okresie jesiennym po długotrwałych intensywnych deszczach zmieniają się w bardzo mokre grunty, co wpływa na znaczny wzrost głębokości strefy dostępności elektromagnetycznej ukrywanych środków łączności.

Z kolei długotrwałe mrozy oraz intensywne opady śniegu (ponad 0,5 m na powierzchni ziemi) powodują pogorszenie się parametrów elektrycznych gruntów bardzo i średnio wilgotnych do wartości właściwych gruntu suchego, a zarazem zmniejszenie głębokości strefy dostępności elektromagnetycznej środków rozwiniętych na tych gruntach. Wpływ parametrów elektrycznych gruntu na głębokość strefy dostępności elektromagnetycznej uzależniony jest również od długości fali roboczej [załącznik 9.]. W miarę zmniejszenia się długości fali maleje głębokość przenikania fal elektromagnetycznych w powłokę ziemską. Zmniejsza się wpływ jej parametrów elektrycznych na straty energii emitowanej przez antenę, a więc maleje głębokość strefy dostępności elektromagnetycznej. Przy stałej wartości parametrów elektrycznych gruntu głębokość strefy dostępności elektromagnetycznej maleje w miarę wzrostu częstotliwości roboczej nadajnika wykorzystującego anteny prętowe lub zmniejszania częstotliwości w przypadku wykorzystania anten kierunkowych [załącznik 10.].

Zatem manewr częstotliwości w odniesieniu do środków radiowych pracujących na częstotliwościach ustalonych może być wykorzystany jako kolejne przedsięwzięcie przeciwdziałania środkom rozpoznania radioelektronicznego przeciwnika, pod warunkiem uwzględnienia rodzaju anteny nadawczej i właściwości elektrycznych gruntu. W wypadku radiostacji współpracujących z antenami prętowymi zamocowanymi na nadwoziu (bez wykorzystania masztów) głębokość strefy dostępności elektromagnetycznej maleje w miarę wzrostu częstotliwości nadajnika. Ukrywanym środkom należy, więc przydzielić w tym wypadku najwyższe z przydzielonych do eksploatacji częstotliwości. Natomiast w wypadku współpracy radiostacji z antenami promieniowymi (fala bieżąca) należy przydzielić jak najniższe częstotliwości, gdyż dla tych anten głębokość strefy dostępności elektromagnetycznej maleje wraz z częstotliwością roboczą nadajnika.

W przypadku wykorzystania radiostacji nowej generacji, np. z tzw. skokową zmianą częstotliwości (ang. Frequency Hopping) można używać pseudolosowego ciągu częstotliwości z całego zakresu radiostacji lub też wybranych pasm. Klucz do tego ciągu określany znanym wyrażeniem anglojęzycznym „transec" powinien być przygotowywany według zasad obowiązujących w szyfrowaniu.

Pewne możliwości w zakresie zmniejszenia dostępności elektromagnetycznej stwarza również rozwijanie radiostacji w jak największej odległości od przedniego skraju obrony. Możliwości te powinny być maksymalnie uwzględniane na etapie planowania sieci łączności w działaniach obronnych związku operacyjnego, zwłaszcza, gdy zamierza się przesunąć granicę dostępności elektromagnetycznej przed rubież rozwinięcia środków rozpoznania radioelektronicznego przeciwnika.

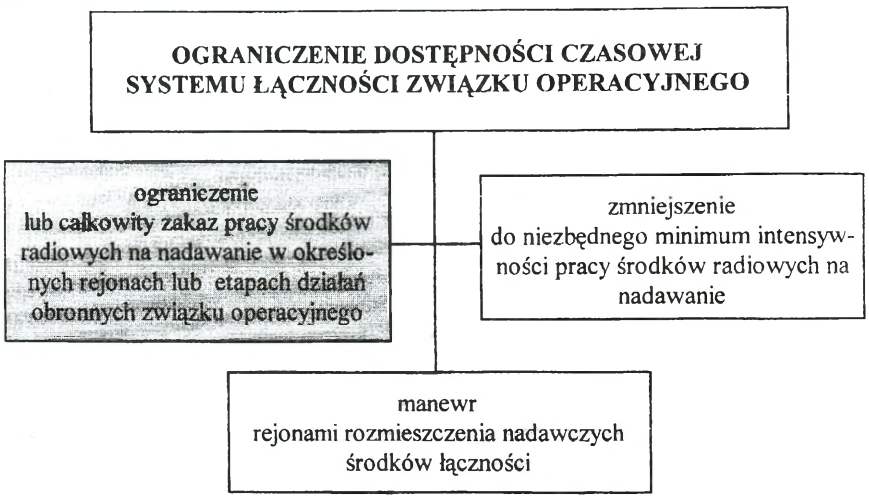
Należy nadmienić, że głębokość strefy dostępności elektromagnetycznej radiostacji VHF w stosunku do powietrznych środków rozpoznania osiąga wielkość 70 – 100 km (radiostacji HF – ponad 300 km). Dostępność elektromagnetyczną tych radiostacji można ograniczyć wykorzystując ekrany wytłumiające energię fal elektromagnetycznych emitowanych przez anteny w kierunku styczności wojsk (stalowe i żelbetonowe mosty, wiadukty, obiekty przemysłowe, itp.).

Ukrywanie środków i sieci łączności radiowej, radiotelefonicznej i radioliniowej jest możliwe w wyniku zwiększenia poziomu zakłóceń na wejściu urządzeń rozpoznawczych (w miejscu ich rozwinięcia). Cel ten można osiągnąć przez tworzenie tak zwanych zasłon radiowych organizowanych za pomocą radiostacji ustawianych w pobliżu przedniego skraju obrony, emitujących energię elektromagnetyczną w kierunku przeciwnika w tym samym czasie i na tych samych częstotliwościach roboczych jak radiostacje ukrywane. Przy czym skuteczność maskowania zasłonami radiowymi jest najwyższa wówczas, gdy wykraczająca poza obszar odpowiedzialności obronnej związku operacyjnego część strefy dostępności elektromagnetycznej ukrywanej radiostacji jest całkowicie pokryta strefą dostępności elektromagnetycznej jednej lub kilku radiostacji maskujących [załącznik 11.] oraz jeżeli stosowany jest taki sam rodzaj pracy radiostacji maskujących jak maskowanych i takie same anteny. Skuteczność maskowania zależy, więc od zachowania odpowiedniej odległości między radiostacją maskującą i maskowaną. Odległość ta powinna być większa niż wartość różnicy między głębokościami stref dostępności elektromagnetycznej tych radiostacji. Warunek ten nie zawsze jest możliwy do spełnienia, gdyż w wielu wypadkach należałoby rozwijać radiostację maskującą w ugrupowaniu operacyjnym (bojowym) przeciwnika. Dlatego też do tworzenia zasłon radiowych powinny być wykorzystywane głównie radiostacje posiadające nadajniki o mocach nie mniejszych niż radiostacje ukrywane (lub mniejsze z dodatkowymi wzmacniaczami mocy). W celu ograniczenia (wyeliminowania) dostępności elektromagnetycznej większej liczby radiostacji rozwiniętych w obszarze obrony związku operacyjnego, pracujących na tych samych częstotliwościach (korespondenci simpleksowych sieci i kierunków radiowych), możliwe jest tworzenie zasłony radiowej w pobliżu przedniego skraju obrony za pomocą kilku radiostacji o mniejszej mocy nadajników. Z praktyki wynika, że liczba radiostacji wydzielonych do tworzenia zasłon radiowych powinna być dwukrotnie wyższa od liczby maskowanych tym sposobem linii łączności [118].

Dostępność elektromagnetyczną środków łączności radiowej pracujących na częstotliwościach ustalonych należy również ograniczać, przydzielając im te częstotliwości, na których występują większe zakłócenia lub te, które są wykorzystywane przez przeciwnika.

Działania tego typu powinny być podejmowane zwłaszcza wtedy, gdy odległości pomiędzy korespondentami są niewielkie i możliwe będzie zapewnienie w miarę stabilnej pracy ukrywanych relacji radiowych. W wypadku większych odległości pomiędzy korespondentami istnieje możliwość wykorzystania częstotliwości o wyższym poziomie zakłóceń lub zajętych przez przeciwnika pod warunkiem, że radiostacje wyposażone będą w anteny kierunkowe.

Bardzo ważnym działaniem w zakresie obrony przed rozpoznaniem radioelektronicznym jest ograniczenie **dostępności czasowej** środków i systemów łączności radiowej, radioliniowej i satelitarnej. Przykładowe przedsięwzięcia w tym zakresie przedstawiono na rysunku 2.11.



Rys. 2.11. Ograniczenie dostępności czasowej systemów łączności w działaniach obronnych związku operacyjnego

Ograniczenie lub całkowity zakaz pracy na nadawanie z wyjątkiem przekazywania sygnałów powiadamiania i alarmowania należy stosować w okresie poprzedzającym działania obronne związku operacyjnego, w trakcie przegrupowania, w rejonach ześrodkowania itp.

Ograniczenia te powinny dotyczyć również związków taktycznych, oddziałów pierwszego rzutu, będących w styczności z przeciwnikiem, lecz nie prowadzących walki (np. podczas organizacji obrony). Działania wojenne na Bliskim Wschodzie w 1967 roku w pełni potwierdziły tę tezę. Strona izraelska przed rozpoczęciem wojny wykorzystywała jedynie łączność przewodową i wojskowej poczty polowej (za pomocą śmigłowców łącznikowych). Dopiero po przekazaniu sygnału o rozpoczęciu wojny uruchomiono łączność radiową na szczeblu operacyjnym. W związkach taktycznych i oddziałach pierwszego rzutu łączność

radiową uruchomiono praktycznie na 15 minut przed rozpoczęciem działań. W ten sposób skutecznie zaskoczono przeciwnika.

Z powyższego wynika, że w czasie prowadzenia działań obronnych związku operacyjnego środki radiowe powinny być wykorzystywane tylko wówczas, gdy niemożliwe jest zapewnienie łączności za pomocą innych środków łączności (kablowych, wojskowej poczty polowej). W szczególnie dynamicznych okresach działań obronnych związku operacyjnego (np. podczas wykonywania kontrataku) środki radiowe można użyć do zapewnienia dowodzenia związkami taktycznymi i oddziałami znajdującymi się w ruchu do dowodzenia grupami rozpoznawczymi oraz elementami, z którymi nie można zapewnić łączności za pomocą innych środków.

W każdej sytuacji należy dążyć do maksymalnego ograniczenia dostępności czasowej, a jeśli jest to możliwe, należy maksymalnie ograniczyć intensywność wymiany korespondencji radiowej. Wzrost intensywności pracy radiostacji wpływa na wzrost prawdopodobieństwa wykrycia przez środki rozpoznania radiowego przeciwnika. Intensywność pracy radiostacji można zmniejszyć, ustalając odpowiednie ograniczenia czasu pracy nadawania. W okresie kiedy łączność radiowa nie jest wykorzystywana, sprawdzenie jakości kanałów radiowych powinno być realizowane jednostronnie (potwierdzenie odbioru w innych kanałach łączności) krótkimi sygnałami i w razie konieczności, ponieważ sieć łączności radiowej powinna zachować pełną gotowość bojową do pracy nawet w okresie całkowitego zakazu wykorzystania środków radiowych.

Zmniejszenie intensywności pracy środków łączności radiowej w działaniach obronnych związku operacyjnego można osiągnąć przez:

- odpowiednie przygotowanie załóg radiostacji oraz dowódców i oficerów sztabu do szybkiej wymiany danych w relacjach radiowych;
- wyprowadzenie korespondentów z sieci do pracy w kierunkach radiowych,
- zdecydowane skracanie do minimum czasu trwania seansów łączności;
- prowadzenie wymiany radiowej bez posługiwania się kryptonimami (sygnałami rozpoznawczymi);
- nadawanie telegramów bez żądania potwierdzenia odbioru;
- przekazywanie rozkazów, zarządzeń i meldunków za pomocą sygnałów;
- wykorzystanie urządzeń transmisji danych.

W badaniach wykazano, że manewr rejonami rozmieszczenia nadawczych środków łączności ma szczególne znaczenie dla skuteczności ich ukrywania, gdyż może wpłynąć za-

równo na ograniczenie dostępności elektromagnetycznej, jak i czasowej. Przedsięwzięcie to powinno mieć szerokie zastosowanie w działaniach obronnych związku operacyjnego o charakterze manewrowym. Kalkulacje przestrzenne w zakresie rozmieszczenia środków taktycznego rozpoznania radioelektronicznego przeciwnika wskazują, że manewr środkami nadawczymi ma istotne znaczenie wówczas, gdy głębokość strefy dostępności elektromagnetycznej przewyższa odległość ich rozmieszczenia od przedniego skraju obrony o wartość rzędu kilku kilometrów, ponieważ pozwala niekiedy wielokrotnie zmniejszyć liczbę urządzeń rozpoznawczych przeciwnika, które mogą przechwytywać sygnały elektromagnetyczne emitowane przez te nadajniki. Powoduje to znaczny spadek prawdopodobieństwa ich wykrycia. Jeśli na przykład głębokość strefy dostępności elektromagnetycznej radiostacji wynosi 15 km, a jest ona rozwinięta w odległości 12 km od przedniego skraju obrony to jej sygnały mogą być przechwytywane przez około 20 urządzeń rozpoznawczych przeciwnika. Przesunięcie tej radiostacji o 2 km w głąb spowoduje, że w jej strefie dostępności elektromagnetycznej mogą pozostać tylko 2 urządzenia rozpoznawcze [55;118]. Zmaleje, zatem prawdopodobieństwo jej wykrycia. Manewr rejonami rozmieszczenia nadawczych środków łączności ma także wpływ na ograniczenie ich dostępności czasowej dla rozpoznania radioelektronicznego, a tym samym na zmniejszenie prawdopodobieństwa ich wykrycia.

Ograniczenie dostępności oznakowej, strukturalnej oraz semantycznej ma na celu maksymalne pozbawianie wojsk i obiektów łączności cech demaskujących w działaniach obronnych związku operacyjnego. Dotyczy to wszystkich sieci łączności, w których wykorzystuje się środki łączności bezprzewodowej (radiowe HF, VHF, radiotelefoniczne i radioliniowe). Pracę tych środków charakteryzuje wiele cech demaskujących, które ułatwiają przeciwnikowi prowadzenie rozpoznania[42]. Przykładowe zestawienie różnorodnych przedsięwzięć organizacyjnych i technicznych w tym względzie zamieszczono na rysunku 2.12.

Spośród **przedsięwzięć organizacyjnych** ważną rolę odgrywa unikanie stosowania szablonowych wariantów sieci łączności mające na celu ograniczenie ich dostępności strukturalnej oraz utrudnianie przeciwnikowi korzystania ze wzorców rozpoznawczych, co powoduje wydłużanie czasu rozpoznania systemu łączności, a w konsekwencji systemu dowodzenia. Specjaliści oddziału dowodzenia i łączności G 6 sztabu związku operacyjnego powinni opracować w okresie pokoju kilka wariantów rozwiązania tego problemu. Zaprojektowane sieci łączności powinny umożliwiać tworzenie wielowariantowych architektur uwzględniających:

[42] Przedstawione zostały na rysunku 2.8.

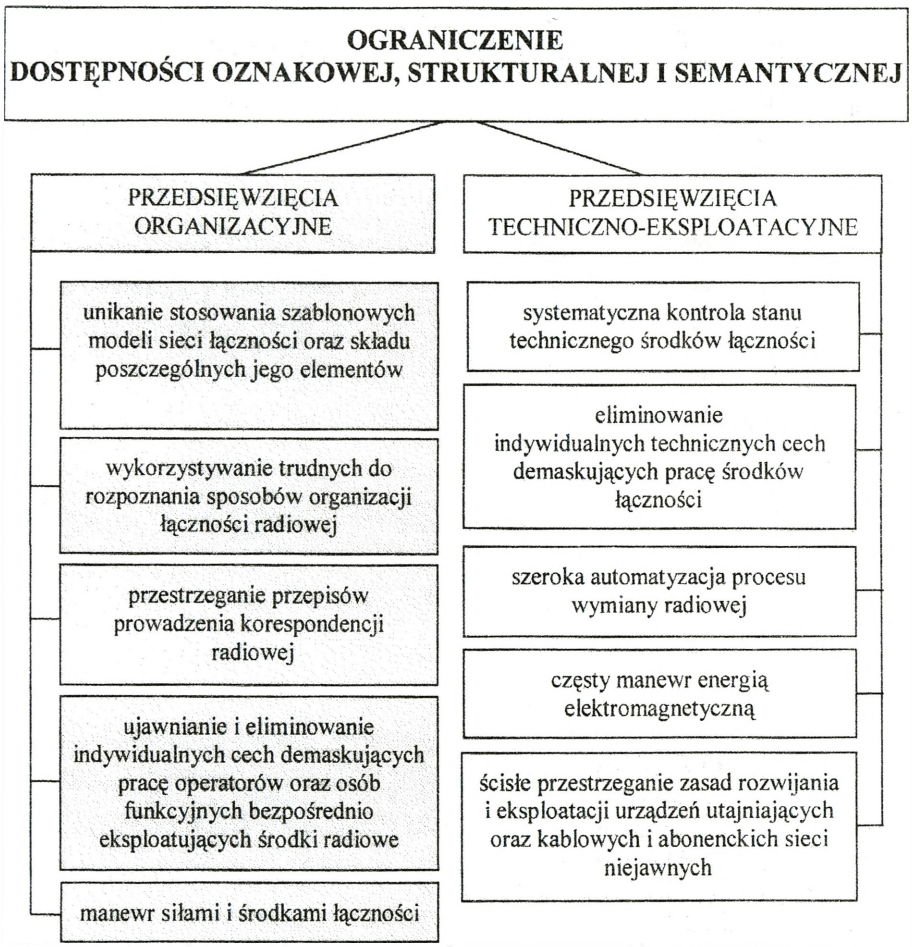
– okresowe zmiany położenia elementów systemu łączności nie związanych bezpośrednio z rozwojem sytuacji operacyjnej i taktycznej;

– tworzenie pośredniczących punktów i okrężnych linii łączności;

– rozmieszczenie grup radiostacji średniej mocy poza węzłami łączności w sposób utrudniający przeciwnikowi ustalenie ich przynależności do określonego węzła łączności;

– organizowanie pozornych węzłów łączności (przez wykorzystanie np. radiostacji wydzielonych do maskowania zasłonami radiowymi);

– różne sposoby wykorzystania sieci telekomunikacyjnych użytku publicznego oraz stacjonarnej sieci łączności.



Rys. 2.12. Ograniczanie dostępności oznakowej, strukturalnej i semantycznej systemu (sieci) łączności w działaniach obronnych związku operacyjnego

Poza tym powinna istnieć możliwość szerokiego stosowania trudnych do rozpoznania sposobów organizacji łączności, na przykład: kombinowane oraz dyżurne sieci radiowe (radiotelefoniczne), częstotliwości dyżurnego odbioru, praca w sieciach radiowych na dwóch częstotliwościach, wyprowadzanie korespondentów z sieci do pracy w kierunkach radiowych (radiotelefonicznych, radioliniowych) z retranslacją lub praca z automatycznym wyborem kanału [4;14]. Wymienione sposoby organizacji łączności powinny być stosowane przede wszystkim w relacjach radiowych dostępnych elektromagnetycznie środkom rozpoznania radiowego przeciwnika (łączność z grupami rozpoznawczymi i innymi pododdziałami rozpoznawczymi działającymi w ugrupowaniu przeciwnika, dowodzenia wojskami walczącymi w obszarze sił przesłaniania oraz zgrupowaniami wykonującymi zwroty zaczepne i inne).

Natomiast zdecydowanie powinno ograniczać się stosowanie „klasycznych" sieci i kierunków radiowych jako sposobów organizacji łączności radiowej najbardziej podatnych na rozpoznanie radioelektroniczne.

Istotne znaczenie dla ograniczania dostępności oznakowej i strukturalnej sieci łączności w działaniach obronnych związku operacyjnego ma rygorystyczne przestrzeganie przepisów prowadzenia korespondencji radiowej oraz utajnianie i eliminowanie indywidualnych cech demaskujących pracę operatorów i innych osób funkcyjnych obsługujących bezpośrednio radiostacje. Wysoka dyscyplina pracy sprzyja sprawnej wymianie radiowej, pozwala uniknąć błędów i powtórzeń, co umożliwia skrócenie czasu transmisji danych, a zatem zmniejszanie prawdopodobieństwa wykrycia radiostacji oraz utrudnienie przeciwnikowi identyfikacji operatorów, radiostacji, węzłów łączności itp.

Indywidualne cechy pracy wyróżniające operatorów i osoby funkcyjne upoważnione do prowadzenia korespondencji radiowej powinny być szczególnie intensywnie eliminowane w procesie szkolenia, a jeśli jest to niemożliwe, osoby obarczone takimi cechami nie powinny być dopuszczane do bezpośredniego przekazywania wiadomości w relacjach radiowych. Praca operatorów demaskuje również ich poziom wyszkolenia. Najlepiej wyszkoleni operatorzy obsługują z reguły radiostacje dowódców, szefów sztabów, co ułatwia przeciwnikowi identyfikację odpowiednich relacji łączności. W celu wyeliminowania tej cechy demaskującej systemu łączności należy organizować już w okresie pokoju proces szkolenia załóg radiostacji (radiotelefonów, stacji radioliniowych) w sposób zapewniający uzyskanie wysokiego, wyrównanego poziomu ich umiejętności w zakresie prowadzenia korespondencji radiowej.

Wysoki poziom wyszkolenia załóg ułatwia maksymalne ograniczenie intensywności pracy linii łączności oraz ścisłe przestrzeganie ustalonych rodzajów pracy. Intensywność pracy bezprzewodowych urządzeń teletransmisyjnych nie powinna demaskować działalności

wojsk. Dotyczy to zwłaszcza urządzeń dostępnych elektromagnetycznie i czasowo środkom rozpoznania radioelektronicznego przeciwnika, tj. radiostacji zapewniających łączność z wojskami działającymi w obszarze działania sił osłony oraz w ugrupowaniu bojowym przeciwnika, środków wydzielonych do tworzenia zasłon radiowych itp. Powinny one rozpocząć pracę po zajęciu rejonów przez wojska i kontynuować ją z intensywnością dobraną w taki sposób, aby nie trzeba było jej zmieniać w toku prowadzenia działań wojennych. Jeśli mimo wszystko zaistnieje konieczność zmiany intensywności pracy tych urządzeń w toku walki, powinna ona następować z pewnym opóźnieniem czasowym w stosunku do zadań realizowanych przez wojska (np. kontratak). Pozbawia się w ten sposób przeciwnika możliwości podjęcia skutecznego przeciwdziałania.

Dostępność strukturalną systemów (sieci) łączności w obszarze odpowiedzialności obronnej związku operacyjnego można ograniczać, stosując manewr sił i środków łączności. Dotychczas kluczowe osoby funkcyjne związku operacyjnego i wojsk podległych (dowódcy, szefowie sztabów, oficerowie rodzajów wojsk) z reguły wykorzystywały przydzielone im „na stałe" radiostacje (wozy dowodzenia) wraz z załogami. Pozwalało to przeciwnikowi na prowadzenie bieżącej analizy zmian w strukturze przestrzennej sieci łączności, a tym samym na prowadzenie właściwej oceny sytuacji radioelektronicznej oraz ustalanie zmian w położeniu wojsk związku operacyjnego.

W celu ograniczenia możliwości przeciwnika w tym zakresie należy, w miarę możliwości, podczas zmiany położenia stanowisk dowodzenia oraz przed zmianą danych radiowych wymieniać między różnymi węzłami łączności i wozami dowodzenia bezprzewodowe urządzenia teletransmisyjne lub załogi. Wymieniane powinny być przede wszystkim te z nich, które były dostępne elektromagnetycznie środkom rozpoznania radiowego przeciwnika, a po wymianie, jeśli jest to możliwe, powinny być wykorzystywane w relacjach łączności umożliwiających wyeliminowanie ich dostępności elektromagnetycznej (w takim wypadku wymiana może być dokonywana w ramach tego samego węzła łączności). Manewr radiostacjami dostępnymi elektromagnetycznie przeciwnikowi przez przemieszczenie ich w inny rejon powinien być okresowo realizowany również bez ścisłego związku z rozwojem sytuacji operacyjnej i taktycznej, wynikającej z przebiegu działań obronnych w celu utrudnienia przeciwnikowi właściwej oceny położenia i aktywności wojsk związku operacyjnego na podstawie danych uzyskanych za pomocą środków rozpoznania radiowego.

Niezmiernie ważny problem stanowi utajnianie wiadomości przekazywanych za pomocą środków radiowych. Sposób utajniania wiadomości powinien uniemożliwić przeciwnikowi ustalenie na podstawie ich treści, składu linii łączności oraz ich przynależności do ro-

dzajów wojsk, służb i szczebli dowodzenia, a także zamiaru podejmowanych działań.

Z powyższego wynika, że w celu ograniczenia dostępności semantycznej sieci łączności w działaniach obronnych związku operacyjnego należy ujednolicić sposób utajniania wiadomości przekazywanych w relacjach radiowych, zwłaszcza, że nowa generacja środków i urządzeń łączności cyfrowej w pełni umożliwia ujednolicenie struktury transmitowanych sygnałów, zapewnia maskowanie początku i zakończenia transmisji oraz utajnianie wiadomości z gwarantowaną mocą kryptograficzną.

W celu podwyższenia skuteczności działań maskujących pracę sieci łączności równocześnie z przedsięwzięciami organizacyjnymi należy realizować również **przedsięwzięcia techniczne** (rys. 2.12.). Szczególnie istotne znaczenie ma systematyczne kontrolowanie parametrów technicznych sprzętu wykorzystywanego w sieciach łączności oraz natychmiastowe usuwanie odchyleń wartości tych parametrów od wymagań instrukcyjnych. W tym zakresie powinna być zwrócona uwaga podczas przygotowywania sprzętu do pracy bojowej na dokładne wyregulowanie torów nadawczych i odbiorczych bezprzewodowych urządzeń teletransmisyjnych oraz stacyjnych i abonenckich urządzeń telefonicznych w celu uzyskania zgodnych z instrukcjami, jednakowych dla wszystkich egzemplarzy danego typu sprzętu wartości takich parametrów, jak: poziom (moc) sygnału; dokładność dostrojenia częstotliwości; szerokość kanału; odległość między kanałami; szybkość transmisji; inne parametry – odpowiednio do typu urządzenia.

Obecnie obserwuje się coraz powszechniejsze wykorzystanie w sieci łączności związku operacyjnego urządzeń pracujących metodą rozpraszania widma sygnału w szerokim paśmie częstotliwości. W szerokopasmowych urządzeniach nowej generacji bardzo ważną rolę odgrywa poziom sygnału użytecznego. Dzięki małej widmowej gęstości mocy nadawanych sygnałów (często poniżej poziomu szumu) stają się one trudne do wykrycia i przechwycenia zawartych w nich danych.

Należy również przestrzegać zaleceń producentów w zakresie okresowej kontroli stanu technicznego urządzeń oraz terminowego kierowania ich do remontów – bez względu na liczbę przepracowanych godzin. Konieczność taka podyktowana jest zmianą z upływem czasu własności niektórych elementów elektronicznych[43]. Realizacja tego przedsięwzięcia pozwala w znacznym stopniu wyeliminować indywidualne techniczne cechy demaskujące bezprzewodowych urządzeń teletransmisyjnych, ograniczyć możliwości przeciwnika w zakresie identyfikacji ich poszczególnych egzemplarzy, zmniejszyć efektywność zautomatyzowanych sys-

[43] Wynikają one z tzw. starzenia się elementów elektronicznych [55;56].

temów rozpoznania przeciwnika, wydłużyć czas niezbędny przeciwnikowi do rozpoznania sieci łączności.

Cechy demaskujące pracę poszczególnych operatorów można ograniczyć, automatyzując wymianę korespondencji radiowej przez wykorzystanie, wszędzie tam gdzie jest to możliwe, technicznych środków eliminujących bezpośredni udział człowieka podczas transmisji danych (komputery, faksy). Środki te powinny być stosowane szczególnie szeroko podczas przekazywania wiadomości, których treść można wcześniej przygotować (np. procedury nawiązywania i sprawdzania łączności, meldunki, zarządzenia, często powtarzające się komendy i sygnały, meldunki od grup rozpoznawczych). Problem eliminowania cech demaskujących pracę urządzeń końcowych i operatorów jest łatwy do rozwiązania w systemie łączności cyfrowej.

Ponadto do przedsięwzięć techniczno – eksploatacyjnych należy również: częsty manewr energią elektromagnetyczną oraz ścisłe przestrzeganie zasad rozwijania i eksploatacji urządzeń utajniających oraz kablowych i abonenckich sieci niejawnych.

Z przeprowadzonych badań wynika, że umiejętne ograniczenie dostępności elektromagnetycznej i czasowej oraz eliminowanie cech demaskujących pracę bezprzewodowych urządzeń teletransmisyjnych w obszarze odpowiedzialności obronnej związku operacyjnego uniemożliwi bądź w znacznym stopniu utrudni wykrycie sieci łączności za pomocą środków (systemów) rozpoznania radiowego. Brakujące dane przeciwnik będzie usiłował zdobyć za pomocą innych środków rozpoznania radioelektronicznego lub rozpoznania powietrznego i naziemnego.

Ważną rolę w działaniach obronnych związku operacyjnego odgrywa również **ukrywanie systemów (stacji) radiolokacyjnych**. Badania wykazały, że powinno ono być organizowane na zasadach analogicznych jak w wypadku ukrywania systemów (sieci) łączności. Z powyższego wynika, że należy realizować odpowiednie przedsięwzięcia organizacyjne i techniczne.

Przedsięwzięcia organizacyjne powinny być ukierunkowane na:

– ścisłe przestrzeganie ustalonych rodzajów pracy podczas przegrupowania i w toku działań obronnych związku operacyjnego;

– stosowanie ograniczeń terytorialnych oraz przestrzennych (wyznaczanie rejonów rozmieszczenia i sektorów pracy zakazanych dla stacji radiolokacyjnych);

– ograniczanie czasu pracy stacji radiolokacyjnych;

– stosowanie manewru: częstotliwościami, sektorami promieniowania oraz częste przebazowania urządzeń radiolokacyjnych. Może to stworzyć znaczne efekty maskujące przez wprowadzenie elementu niepewności i nieoznaczoności w procesie rozpoznania radioelektronicznego prowadzonego przez przeciwnika.

Przedsięwzięcia techniczne powinny obejmować:

– manipulowanie częstotliwościami nośnymi stacji radiolokacyjnych. Zmiany te powinny odbywać się w sposób ustalony programowo (w starszych generacjach urządzeń) lub losowo (stosowane w nowszych generacjach urządzeń), gdzie wykorzystuje się tzw. skokowe zmiany częstotliwości. Utrudnia to radykalnie rozpoznanie stacji radiolokacyjnych oraz czyni je bardziej odpornymi na zakłócenia, głównie szumowe;

– możliwość dokonywania pełnych strojeń stacji radiolokacyjnych, włącznie z nadajnikiem bez emitowania energii wysokiej częstotliwości w przestrzeń. W tym celu należy wykorzystywać sztuczne obciążenia, tzw. ekwiwalenty, przy poziomie mocy rozproszonej gwarantującej niewykrycie przez środki rozpoznania;

– optymalizację zysku kierunkowego anten, które – jak wiadomo – oprócz listka głównego mają listki boczne. Wysoki poziom listków bocznych ułatwia lokalizację stacji przez urządzenia rozpoznawcze[44]. Ten wysoki poziom powinien być minimalizowany za pomocą układów kompensacji listków bocznych oraz układów stabilizacji poziomu fałszywego alarmu. Skutecznym rozwiązaniem powinno być wyposażenie stacji radiolokacyjnych nowej generacji w anteny ścianowe w postaci szyków fazowych, u których poziom listków bocznych powinien wynosić około – 40 dB;

– zagęszczenie pasma (skupienie dużej liczby środków radiolokacyjnych w wąskim paśmie częstotliwości, a zatem występowanie podobieństw częstotliwości)[45], obok mankamentów wynikających z ewentualnych naruszeń kompatybilności elektromagnetycznej[46], powinno powodować znaczne efekty maskujące strukturę pola radiolokacyjnego w obszarze odpowiedzialności obronnej związku operacyjnego.

Badania wykazały, że istotną rolę odgrywa ukrywanie ugrupowania radiolokacyjnych środków obrony przeciwlotniczej związku operacyjnego w okresie przygotowywania działań

---

[44] Dla krajowych konstrukcji stacji radiolokacyjnych poziom listków bocznych anten reflektorowych i szczelinowych jest wysoki i zawiera się w przedziale – 20 do –27 dB w stosunku do głównego listka [29;72].

[45] Pasmo L (podpasma C, D) oraz w pasmo S.

[46] Przez kompatybilność elektromagnetyczną rozumie się w radiokomunikacji prawidłową koegzystencję elektromagnetyczną urządzeń (sieci radiokomunikacyjnych) z innymi urządzeniami (sieciami) oraz ze źródłami zakłóceń naturalnych i technicznych. Por. W. Rotkiewicz, „Kompatybilność elektromagnetyczna w radiotechnice", wyd. KiŁ, Warszawa 1978.

obronnych, gdyż od skuteczności podejmowanych w tym zakresie działań, w znacznym stopniu zależy ich zdolność do odpierania ataków środków napadu powietrznego przeciwnika, od których użycia może on rozpocząć swoje działania wojenne.

Oceniając możliwości **ukrywania systemu rozpoznania radioelektronicznego** stwierdzono, że jest ono utrudnione przede wszystkim w obszarze działania sił osłony. Większość elementów tego systemu jest rozwijana blisko przedniego skraju obrony, a więc znajdują się one w zasięgu środków rozpoznania zarówno bezpośredniego, jak i pośredniego.

Wynika to z faktu, że posterunki rozpoznania systemów radiolokacyjnych rozwijane są w miejscach zapewniających dobry wgląd w teren zajmowany przez przeciwnika (szczyty wzniesień, i ich stoki, obrzeża miejscowości i lasów graniczące z terenem otwartym od strony przeciwnika), co ułatwia ich wykrycie.

Z kolei posterunki rozpoznania radiowego rozwijane są w rejonach zapewniających korzystne warunki propagacji fal elektromagnetycznych w relacji środki łączności radiowej przeciwnika – własne posterunki rozpoznawcze, co stwarza również i przeciwnikowi dogodne warunki do prowadzenia rozpoznania tych systemów. Elementy te wykorzystują intensywnie środki łączności radiowej do obiegu informacji rozpoznawczej, co ułatwia przeciwnikowi wykrycie tych posterunków przez jego systemy rozpoznania radiowego.

Z przedstawionych uwarunkowań wynika, że ukrywanie systemu rozpoznania radioelektronicznego w działaniach obronnych związku operacyjnego powinno obejmować przede wszystkim:

- maskowanie bezpośrednie środków rozpoznania radioelektronicznego;
- okresowe zmiany miejsc rozwinięcia elementów rozpoznania radioelektronicznego;
- wynoszenie środków łączności radiowej jak najdalej poza posterunki rozpoznania;
- wykorzystywanie – wszędzie gdzie jest to możliwe – kablowych linii teletransmisyjnych, a zwłaszcza w relacjach sterowania systemem rozpoznania radioelektronicznego.

Poza tym do ukrywania systemu rozpoznania radioelektronicznego mogą i powinny być stosowane metody i sposoby analogiczne jak w ukrywaniu systemów łączności. Należy dostosować je jednak do konkretnych warunków działań obronnych oraz zasad funkcjonowania systemu rozpoznania radioelektronicznego i jego struktury organizacyjnej.

Pojęcie **dezinformowanie radioelektroniczne** jest często definiowane niejednoznacznie i używane zamiennie z „pozorowaniem radioelektronicznym" [54]. Z kolei w wielu publikacjach traktujących o dezinformowaniu radioelektronicznym [1;25;30;62;101;102; 138;139] istnieje tendencja do utożsamiania go z działaniami dezinformującymi o charakterze

dywersyjnym prowadzonymi przez przeciwnika w ramach zakłócania informacyjnego systemów radioelektronicznych, a przede wszystkim w zagłuszaniu systemów (sieci) łączności związku operacyjnego.

Jak wykazały badania, dezinformowanie radioelektroniczne jest kolejną formą maskowania radioelektronicznego. Może być prowadzone samodzielnie lub uzupełniać przedsięwzięcia pozorowania i ukrywania radioelektronicznego. Dezinformowanie radioelektroniczne **polega na preparowaniu wiadomości fałszywych i rozpowszechnianiu ich lub przekazywaniu rozpoznaniu radioelektronicznemu przeciwnika.** Należy organizować je w celu wprowadzenia dowództw, sztabów i organów rozpoznawczych przeciwnika w błąd co do ugrupowania i rozmieszczenia wojsk związku operacyjnego, zamiaru działań obronnych i innych ważnych danych o charakterze operacyjno-taktycznym.

Ważną zasadą dezinformowania jest przekazywanie danych dezinformujących w bloku danych prawdziwych. Wymaga to zaangażowania wysoko kwalifikowanych specjalistów z różnych dziedzin, m in. wywiadu, propagandy i łączności. Dezinformowanie radioelektroniczne powinno być realizowane zarówno w czynnych, jak i pozornych systemach radioelektronicznych związku operacyjnego oraz w miarę możliwości w lokalnych środkach masowego przekazu (radio, telewizja) i w sieciach teleinformatycznych.

Należy mieć na uwadze, że bezprzewodowe środki teletransmisyjne, a przede wszystkim środki radiowe i radioliniowe należą do typowych i wiarygodnych kanałów dezinformujących. Specyfika tych środków stawia je często ponad innymi kanałami dezinformującymi, takimi jak prasa i agentura.

Radiowe kanały dezinformujące w przeciwieństwie do prasy i agentury mogą wykonywać swoje zadania w bardzo krótkim czasie. Zmiana zadań może być dokonywana dowolnie, w zależności od aktualnej sytuacji operacyjno-taktycznej, a dane dezinformujące mogą docierać do sztabów przeciwnika bezpośrednio, z pominięciem niższych ogniw pośrednich. Poza tym intensywność podawania wiadomości dezinformujących w tych kanałach może być dowolnie regulowana.

Badania wykazały, że do zasadniczych **sposobów dezinformowania radioelektronicznego** można zaliczyć:

- przekazywanie fałszywych wiadomości, komend, rozkazów i meldunków oraz ogłaszanie komunikatów, wywiadów i komentarzy za pomocą czynnych bezprzewodowych urządzeń teletransmisyjnych;
- prowadzenie aktywnej wymiany radiowej w rejonach pozornej dyslokacji.

Efektem realizacji przedsięwzięć dezinformowania radioelektronicznego może być:

- uzyskanie zaskoczenia;
- skłonienie przeciwnika do wcześniejszego ujawnienia swych zamiarów;
- przyjęcie błędnego ugrupowania operacyjnego (bojowego);
- nakłonienie do zużycia amunicji, bomb i rakiet na obiekty nieistotne i in.

Doświadczenia z minionych wojen i konfliktów lokalnych dowodzą, że dezinformowanie radioelektroniczne może przynieść najlepsze efekty, w warunkach prowadzenia przez związek operacyjny działań obronnych o charakterze manewrowym, a więc w sytuacjach niejasnych, gdy potencjalny przeciwnik będzie usilnie dążył do uzyskania informacji o wojskach związku operacyjnego i obszarze jego obrony, zwłaszcza, gdy będzie dążył do ustalenia w krótkim czasie obiektów do uderzeń ogniowych. W takim wypadku wyjście naprzeciw „zapotrzebowaniu" na te informacje będzie przyjmowane z mniejszym krytycyzmem, a wskazane obiekty drugorzędne skutecznie mogą wpłynąć na decyzje przeciwnika. Wynika stąd, że umiejętnie przygotowane, a następnie „udostępnione" w odpowiednim czasie wiadomości dezinformujące mogą stać się ważnym czynnikiem sprzyjającym wprowadzenia przeciwnika w błąd, a tym samym uzyskania zaskoczenia. Działanie takie stanowi – jak podkreślono w rozdziale pierwszym – istotę walki informacyjnej.

Dezinformowanie radioelektroniczne powinno zawierać również wiadomości (sygnały) utwierdzające przeciwnika o prawdziwości przedsięwzięć ukrywania i pozorowania radioelektronicznego. W tym wypadku powinny stanowić dla niego dodatkowy materiał (atut), potwierdzający słuszność prowadzonych ocen. Należy jednak mieć na uwadze, że wiadomości (sygnały) rozpowszechniane za pomocą tych kanałów dezinformujących nie zawsze powinny pokrywać się z przedsięwzięciami maskowania. Mogą być częściowo, a niekiedy całkowicie sprzeczne, ponieważ pełna zgodność może budzić podejrzenia przeciwnika oraz przynieść skutki wręcz odwrotne. Na przykład, jeżeli jest pewne, że pozorowanie związku taktycznego (oddziału) w określonym rejonie, z uwagi na intensywne rozpoznawanie go przez przeciwnika, nie przyniesie zamierzonego efektu, wówczas wiadomość dezinformująca powinna zawierać informacje (sygnały) wskazujące, że rejon ten jest rzeczywiście rejonem pozornym. W takiej sytuacji przeciwnik może nabrać zaufania do wiadomości dezinformujących i łatwo można wprowadzić go w błąd w innym miejscu i czasie w stosunku do innych – lecz ważniejszych, rejonów, obiektów lub zamiarów.

Z doświadczeń minionych wojen i konfliktów lokalnych wynika, że dezinformowanie radioelektroniczne wymaga ścisłej centralizacji planowania i koordynowania, przy czym całość planowanych zamierzeń w tej dziedzinie powinna znać tylko ograniczona liczba osób. Niezmiernie ważnym jego elementem jest preparowanie (przygotowanie) wiadomości (sygnałów) dezinformujących. Powinny być one przygotowywane w pionie G 3, przy współudziale oficerów z pionów G 2 i G 6, a następnie akceptowane przez dowódcę związku operacyjnego. Taka procedura wynika z faktu, że dla uwiarygodnienia danych dezinformujących, oprócz wiadomości (sygnałów) fałszywych powinny znaleźć się i prawdziwe, wynikające z decyzji dowódcy, a na ich ujawnienie może wyrazić zgodę jedynie on sam. Należy liczyć się również z faktem, że określona wiadomość dezinformująca może nie zostać odebrana przez przeciwnika lub zostanie przez niego zignorowana.

Wynika stąd wniosek, że podczas stosowania przedsięwzięć dezinformowania radioelektronicznego należy uwzględnić następujące przypadki:

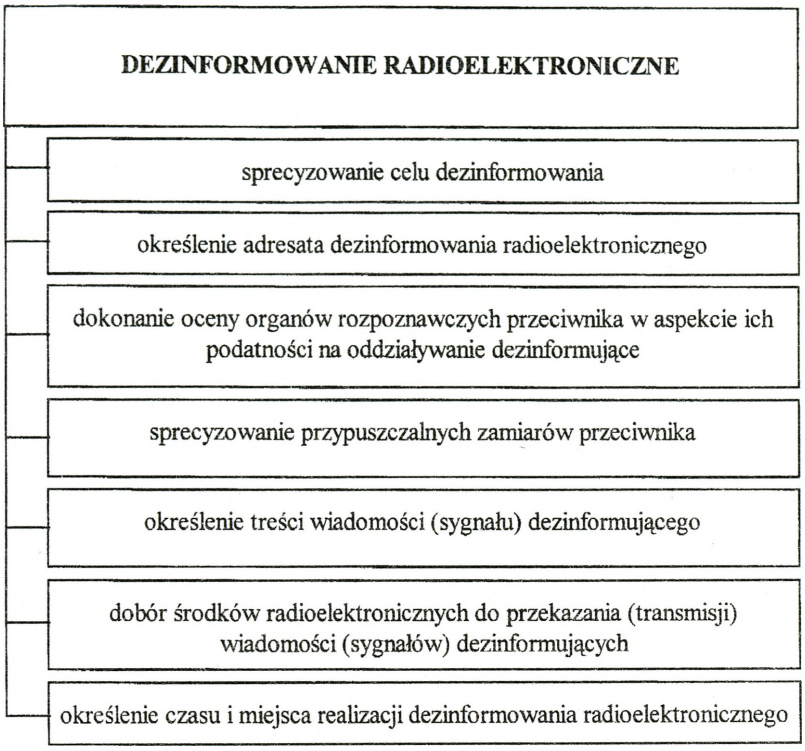
- przeciwnik odebrał wiadomość (sygnał) dezinformującą i postępuje zgodnie z sugestią w niej zawartą;
- przeciwnik odebrał wiadomość (sygnał) dezinformujący i ocenił, że jest wprowadzany w błąd;
- wiadomość (sygnał) nie została odebrana przez rozpoznanie przeciwnika.

Przedstawione okoliczności wymagają odmiennych procedur postępowania. Wybór odpowiedniej powinien być uzależniony od danych uzyskanych przez elementy rozpoznawcze związku operacyjnego. Powinno temu służyć kontrolowanie zachowań przeciwnika na kierunkach lub w rejonach, w których zgodnie z podaną wiadomością dezinformującą powinny zajść oczekiwane zmiany.

Najkorzystniejszy jest oczywiście przypadek pierwszy. Wówczas cel dezinformowania radioelektronicznego jest w pełni osiągnięty.

W przypadku drugim, kiedy przeciwnik rozszyfrował wiadomości dezinformujące, może to wpłynąć na wzmożenie jego czujności, a sposób dezinformowania nie będzie nadawał się do dalszego wykorzystania. Niezbędne będą zmiany w planowaniu działań obronnych, częściowa zmiana rejonów dyslokacji wojsk i sposobów ich wykorzystania. Natomiast dobry efekt może przynieść działanie zgodne lub zbliżone do tego, jakie ujęte zostało w wiadomości dezinformującej. Należy jednak z całą mocą podkreślić, że działanie to nie może być schematyczne.

Podczas przygotowywania wiadomości dezinformujących należy wykorzystać scenariusz zaprezentowany na rysunku 2.13.



Rys. 2.13. Scenariusz przygotowania wiadomości dezinformujących

Realizacja procedury przekazania (transmisji) wiadomości (sygnału) dezinformującej nie powinna odbiegać od obowiązujących w wojskach związku operacyjnego procedur przekazywania wiadomości prawdziwych. Konieczne jest jednak zapoznanie się z zasadami zdobywania danych przez rozpoznanie przeciwnika. Rola użytkowników środków radioelektronicznych powinna w zasadzie ograniczać się do „nieświadomego" przekazania (transmisji) wiadomości (sygnałów) dezinformujących lub do udostępnienia ww. środków oficerom sztabu przekazującym je osobiście.

Jak wykazały badania, podczas prowadzenia dezinformowania radioelektronicznego w działaniach obronnych związku operacyjnego można dopuszczać się kontrolowanych naruszeń:

– zasad ochrony tajemnicy podczas wykorzystania technicznych środków dowodzenia w relacjach jawnych, szczególnie w sytuacjach dynamicznych i skrajnie niejasnych;

– zasad ochrony i wykorzystania technicznych środków utajniających w relacjach niejawnych;

– wykorzystania zdekonspirowanych dokumentów eksploatacyjnych.

Warunkiem koniecznym, który powinien być spełniony podczas realizacji zadań dezinformowania radioelektronicznego jest unikanie szablonowości. O ile szablonowość jest zawsze działaniem szkodliwym, o tyle schematyczne dezinformowanie przeciwnika jest wręcz niedopuszczalne. Może, bowiem przynieść odwrotne skutki, tzn. wykorzystanie wiadomości dezinformujących przez przeciwnika i odwrócenie ich przeciwko nadawcy.

Dezinformowanie radioelektroniczne należy traktować jako najbardziej subtelną formę maskowania operacyjnego. Rola użytkowników środków radioelektronicznych powinna w zasadzie ograniczać się do „nieświadomego" przekazania (transmisji) wiadomości (sygnałów) dezinformujących lub do udostępnienia ww. środków oficerom sztabu przekazującym je osobiście.

Pozorowanie radioelektroniczne jest kolejną formą maskowania organizowaną przede wszystkim na szczeblach operacyjnych. Tworzą je również elementy taktycznego maskowania bezpośredniego. Prowadzi się je **w celu ochrony zasadniczych elementów ugrupowania operacyjnego i bojowego oraz ich obiektów radioelektronicznych przed rozpoznaniem przeciwnika, a także w celu wprowadzenia go w błąd, co do głównego wysiłku działań obronnych i czasu wykonywania uderzeń [54;62;66].**

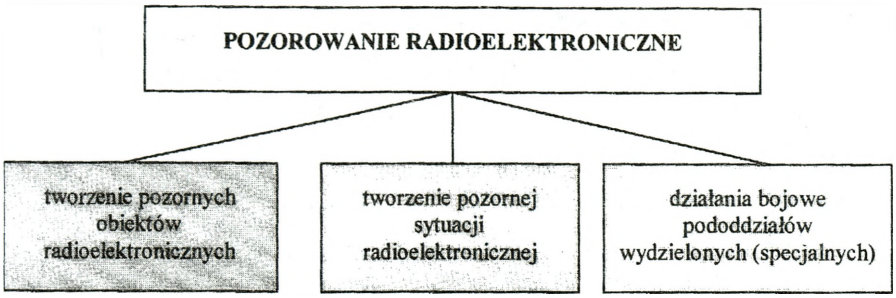
Z powyższego wynika, że pozorowanie radioelektroniczne w działaniach obronnych związku operacyjnego powinno obejmować:

– organizowanie pozornych systemów radioelektronicznych bądź ich elementów, np.: pozornego węzła łączności związku operacyjnego, związku taktycznego lub oddziału; pozornych systemów (stacji) radiolokacyjnych; pozornych systemów naprowadzania rakiet przeciwlotniczych; pozornych systemów wykrywania i naprowadzania lotnictwa; pozornych systemów rozpoznania i zakłócania informacyjnego;

– wprowadzanie przeciwnika w błąd co do możliwości technicznych sprzętu radioelektronicznego lub systemu, w którego skład wchodzi kilka środków;

– wprowadzanie przeciwnika w błąd co do organizacji i sposobów działania poszczególnych systemów radioelektronicznych w różnych etapach działań obronnych związku operacyjnego.

Zasadnicze sposoby prowadzenia pozorowania radioelektronicznego zilustrowano na rysunku 2.14.



Rys. 2.14. Sposoby prowadzenia pozorowania radioelektronicznego

Tworzenie pozornych (fałszywych) obiektów radioelektronicznych umożliwia fakt, że elementy systemów radioelektronicznych, np. systemów łączności, są ze sobą wzajemne powiązane, ale jednocześnie znajdują się w pewnym oddaleniu od siebie. Ta właściwość pozwala na usytuowanie w obszarze odpowiedzialności obronnej związku operacyjnego wśród rzeczywistych (prawdziwych) elementów tych systemów również wielu obiektów pozornych (fałszywych).

W działaniach obronnych związku operacyjnego powinny być tworzone, w razie potrzeby, następujące pozorne obiekty radioelektroniczne:

- ugrupowania obronnego związku taktycznego (oddziału) w rejonie słabo obsadzonym, podczas gdy związek ten (oddział) w rzeczywistości znajduje się na kierunku spodziewanego uderzenia przeciwnika;
- zgrupowania artylerii;
- przepraw, rejonów rozmieszczenia obiektów logistycznych i innych opłacalnych do wykonania uderzeń bronią rakietową.

Pozorowanie przepraw powinno być wykonywane poza rejonem głównego wysiłku obrony i poza rejonami planowanych zwrotów zaczepnych (do tego celu należy stosować odbijacze kątowe do imitacji mostów[47]). Jeżeli natomiast w tym rejonie występują mosty stałe, należy zastosować pojedyncze stacje zakłóceń radiolokacyjnych do ich osłony elektronicznej. Kompleksowe zastosowanie tych środków i sposobów urealni pozorowanie przepraw.

Tworzenie pozornej sytuacji radioelektronicznej obejmuje pozorowanie punktów dowodzenia czynnej sieci łączności oraz pracy stacji radiolokacyjnych i radionawigacyjnych. Elementy pozorne tworzą specyficznie funkcjonujący system radioelektroniczny, który musi

[47] W chwili opracowywania pracy studyjnej występują one w kompanii maskowania, która jest etatowym pododdziałem brygady saperów podległej związkowi operacyjnemu.

mieć powiązanie z systemem rzeczywistym. Do jego ważniejszych przedsięwzięć należy zaliczyć: pozorowanie stanowisk dowodzenia i węzłów łączności w niewielkich odległościach od rzeczywistych lub w zupełnie innych oddalonych rejonach. W pierwszym wypadku organizacja ma miejsce, gdy ukrycie punktu ciężkości obrony i rejonów rozmieszczenia wojsk jest niemożliwe. W drugim wypadku, gdy przeciwnik prawdopodobnie nie zna rejonu rozmieszczenia elementów ugrupowania związku operacyjnego, celem są następujące przedsięwzięcia:

– maskowanie punktu ciężkości obrony, czasu jej gotowości oraz czasu wykonania zwrotów zaczepnych;

– pozorowanie radiowe zmian i przesunięć węzłów łączności stanowisk dowodzenia;

– tworzenie pozornych sieci i kierunków radiowych oraz radioliniowych, a także odpowiednia wymiana danych w tych relacjach;

– tworzenie posterunków rozpoznania elektronicznego przy obiektach pozornych.

Praca środków radioelektronicznych, biorących udział w pozorowaniu powinna mieć charakter działań demonstracyjnych i odbywać się według odpowiedniego scenariusza. Pozorowane elementy powinny mieć określoną liczbę środków elektronicznych, aby stworzyć autentyczność elementu systemu określonego szczebla dowodzenia. Doświadczenia z ćwiczeń z wojskami wskazują, że na użycie środków elektronicznych do budowy pozornego punktu dowodzenia należy przeznaczyć od 30 do 50 % analogicznego rzeczywistego punktu dowodzenia. Przesunięć i zmian stanowisk dowodzenia do nowych rejonów należy dokonywać skrycie. Jednym ze sposobów maskowania jest pozostawienie części środków łączności w dotychczasowym rejonie oraz pozorowanie pracy pozostałych środków w innym miejscu.

Działania bojowe oddziałów wydzielonych lub specjalnych mogą odbywać się wówczas, gdy zamierza się odwrócić uwagę przeciwnika od punktu ciężkości obrony lub kierunku (rejonu) głównego uderzenia wojsk. Powinny obejmować następujące zadania:

– pozorowanie marszu wojsk, podczas gdy faktycznie pozostają one w dotychczasowym rejonie lub maszerują, lecz w zupełnie innym kierunku;

– pozorowanie związków taktycznych i oddziałów w rejonach uprzednio przez nie zajmowanych, podczas gdy wykonują one marsz lub zajmują inny rejon. W tym wariancie należy organizować system dowodzenia oraz pozorne działania pododdziałów specjalnych w rejonach dotychczasowych działań bojowych wojsk.

Stosowanie pozorowania rejonów rozmieszczenia (ześrodkowania) wojsk, rakiet i artylerii, stanowisk dowodzenia, stanowisk ogniowych oraz innych obiektów powinno zapewnić uzyskanie zasadniczych celów maskowania związku operacyjnego. Obiekty pozorne

powinny być jednak upodobnione do obiektów rzeczywistych w takim stopniu, aby przeciwnik – stosując dostępne mu środki rozpoznania – nie mógł dostrzec demaskujących różnic. Muszą, więc mieć wszystkie cechy charakterystyczne dla obiektów rzeczywistych.

W dynamicznie prowadzonych działaniach obronnych, w atmosferze ciągle zmieniającej się sytuacji pola walki działania pozorne nie są przedsięwzięciem prostym w realizacji. Potrzeba utrzymywania odwodów do pogłębiania obrony i narastania oporu, ciągłe odtwarzanie systemu obronnego w miarę osiągania celów pośrednich nie ułatwia zorganizowania i prowadzenia tego rodzaju przedsięwzięć.

Rezultat pozorowania radioelektronicznego powinien być wykorzystany w działaniach obronnych związku operacyjnego do:

– przeniesienia działań w głąb ugrupowania przeciwnika na innym kierunku, szczególnie w wymiarze powietrzno - lądowym, które maskują kierunek głównego wysiłku obrony;

– pozornego uderzenia przez rubieże styczności wojsk dla odtworzenia systemu obronnego na terenie opanowanym przez przeciwnika lub uderzenia z ograniczonym celem – zmylenie co do faktycznego sposobu użycia zgrupowania uderzeniowego, przejścia z manewru pozornego do rzeczywistego;

– odtworzenia systemu obrony na rubieży pośredniej lub umocnienie na opanowanej rubieży – rezultat powstały w wyniku zaniechania potęgowania uderzenia przez przeciwnika – jako konsekwencja zaangażowania jego odwodów przeciw zgrupowaniom pozorującym ich rzeczywiste użycie;

– wycofania zgrupowań z kierunków pasywnych na kolejne rubieże pośrednie (linie koordynacji zadań) – możliwość uderzenia na innym kierunku lub wymuszenia zmiany kierunku głównego uderzenia przeciwnika.

Powodzenie zastosowanych przedsięwzięć pozorowania radioelektronicznego uzależnione jest od przestrzegania odpowiednich reguł jego prowadzenia, do których w działaniach obronnych związku operacyjnego należy zaliczyć:

1. Do pozorowania radioelektronicznego należy dysponować odpowiednią ilością sił i środków oraz wydzielać niezbędną[48] ilość etatowego sprzętu i uzbrojenia znajdującego się w wyposażeniu związku operacyjnego. Obowiązujące regulaminy i dokumenty normatywne w naszych siłach zbrojnych nie precyzują jednak, jaka procentowa część globalnej ilości

[48] Regulaminy zachodnie przewidują wykorzystanie do pozorowania od 10 % nawet do 100 % etatowego sprzętu i uzbrojenia [102].

środków pracujących w systemie rzeczywistym konieczna jest do jego pozorowania[49]. Niecelowe jest natomiast wykorzystywanie środków starszej generacji, wycofanych z wyposażenia, gdyż rozpoznanie przeciwnika może od razu określić ich pozoracyjny charakter na podstawie analizy techniczno-operacyjnej[50].

2. Należy przestrzegać określonych zasad pracy pozornych obiektów radioelektronicznych. W pozorowanych obiektach i systemach intensywność pracy środków radioelektronicznych powinna być cechą świadczącą o aktywności pracy sztabów i działań wojsk i wynikać z sytuacji operacyjno-taktycznej. Intensywność ta nie powinna być przypadkowa, lecz wynikać z planu pozorowania.

3. Rozmieszczenie środków radioelektronicznych pozorowanych obiektów, ich położenie względem siebie lub względem określonych zgrupowań powinno odpowiadać odległościom wynikającym z sytuacji, a także z obowiązujących regulaminów oraz norm operacyjno-taktycznych i wzorców doktrynalnych obowiązujących w działaniach obronnych związku operacyjnego.

4. Pozorowanie obiektów radioelektronicznych może osiągnąć zamierzony cel, jeśli wymiana danych między nimi będzie miała charakter operacyjny. Przekazywanie między nimi np. telegramów ćwiczebnych nie jest wskazane, a często demaskuje te obiekty. Natomiast klucze, dokumenty kodowe oraz pozostałe dokumenty wykorzystywane do utajniania wiadomości powinny być identyczne jak w rzeczywistym systemie dowodzenia.

5. Pozorowanie radioelektroniczne powinno być ściśle zsynchronizowane z ukrywaniem operacyjnym. Można nawet postawić tezę, że warunkiem koniecznym powodzenia zaplanowanych przedsięwzięć pozorowania jest pełna i drobiazgowa realizacja zasad ukrywania radioelektronicznego. Jeśli na przykład przeciwnik wykrył związek taktyczny, który podlegał ukrywaniu operacyjnemu, to wysiłki pozorowania, choćby najbardziej przekonujące, będą nieskuteczne.

6. Należy mieć na uwadze, że pozorowanie radioelektroniczne nie powinno być jedynym sposobem maskowania. Trzeba przestrzegać zasady, że każdy obiekt, czy też pozorowane działanie powinno kompleksowo oddziaływać na system rozpoznawczy przeciwnika. Oprócz pracy środków radioelektronicznych konieczne jest, na przykład do pozorowania działalności sztabów, wykonanie niezbędnych prac ziemnych o niepełnym profilu, dokonanie deformacji

---

[49] Prowadzone badania w AON dowodzą, że dla pozorowania obiektów związku operacyjnego szczególnie ważnych należy wydzielać 80 % ogólnej ilości sprzętu, natomiast dla pozostałych 20–30 % [118].

[50] Współczesne rozpoznanie ma w swoich bazach danych wzorce widm środków radioelektronicznych.

radiolokacyjnej terenu[51] oraz ożywienie[52] wszystkich obiektów wydzielonymi do tego celu siłami i środkami.

7. Siły i środki wydzielone do realizacji przedsięwzięć pozorowania radioelektronicznego będą realizowały swoje zadania z pełnym natężeniem w określonych etapach działań obronnych związku operacyjnego, głównie zaś w okresie przygotowawczym i w ich początkowej fazie. Wynika stąd, że w pozostałych okresach mogą wykonywać zadania realne, wynikające z potrzeb operacyjno-taktycznych. Nawet podczas pracy w systemie pozorowanym mogą one w skrajnych przypadkach (w razie wyższej konieczności) przerwać – na ustalony sygnał – wykonywane zadania i rozpocząć (kontynuować) pracę w systemie rzeczywistym. Mogą stanowić, więc niekiedy swoisty odwód sił i środków radioelektronicznych.

2.2.1.2. Maskowanie radiolokacyjne

Maskowanie radiolokacyjne ma na **celu uniemożliwienie zdobywania oraz przetwarzania tych danych o wojskach i obiektach związku operacyjnego znajdujących się w obszarze jego odpowiedzialności obronnej, których nośnikami są fale elektromagnetyczne wypromieniowane przez środki (stacje) radiolokacyjne[53] przeciwnika i odbite od obiektów związku operacyjnego.**

Analiza stanu oraz tendencji rozwojowych środków (stacji) radiolokacyjnych potencjalnego przeciwnika – w kontekście działań obronnych związku operacyjnego – pozwala na sformułowanie następujących wniosków:

– najbardziej rozpowszechnione są naziemne stacje radiolokacyjne do wykrywania obiektów pola walki, które pracują z reguły w paśmie 3 cm (8 – 12 GHz);

– powietrzne środki walki wykorzystują stacje radiolokacyjne pracujące najczęściej w paśmie 2 i 3 cm (8 – 20 GHz);

---

[51] W ramach zakłócania informacyjnego [24;25;66].

[52] Przeprowadzone badania wskazują, że do pozorowania funkcjonowania obiektów radioelektronicznych należy użyć pododdziałów o stanach równych 10-25 % etatowej ilości pozorowanego elementu [118].

[53] Środki radiolokacyjne przeznaczone są do wykrywania i określania położenia obiektów za pomocą odpowiednio emitowanych i odbieranych fal elektromagnetycznych. Termin „radiolokacja" pochodzi od łacińskich słów radius (promień) i locus (miejsce), jego zaś odpowiednik RADAR pochodzi od angielskiego określenia: Radio Aids for Defence and Reconnaissance (radiowe pomoce do obrony i rozpoznania). Ze względu na sposób uzyskiwania sygnału rozróżnia się radiolokację: 1) aktywną – z pasywną lub aktywną odpowiedzią; 2) półaktywną, 3) pasywną [59;62;66].

– moce stacji radiolokacyjnych z reguły dostosowywane są do potrzeb w zakresie głębokości rozpoznania;

– należy liczyć się również z możliwością wykorzystywania przez potencjalnego przeciwnika radarów pasywnych, wykrywających obiekty na podstawie ich własnego promieniowania w paśmie mikrofalowym. Typowe „okna" wykorzystywane w radiolokacji pasywnej to: 34 – 36 GHz; 75 – 95 GHz; 140 i 225 GHz.

Prowadzone przez przeciwnika rozpoznanie radiolokacyjne[54] obejmuje zatem: systemy rozpoznania obszaru powietrznego, systemy nadzorowania pola walki, systemy naprowadzania uzbrojenia, systemy obrony przeciwlotniczej, pokładowe systemy obserwacji bocznej SLAR[55] i in. Systemy te umożliwiają:

– dostarczenie radiolokacyjnych obrazów odpowiednich sektorów przestrzeni powietrznej, terenu (lądu) oraz akwenów morskich;

– lokalizowanie obiektów wojskowych i środków walki (czołgów, transporterów, samolotów, śmigłowców, armat, rakiet i in.);

– określenie tras przelotu samolotów oraz miejsc rozmieszczenia celów ruchomych (czołgów, transporterów opancerzonych, samochodów, pododdziałów oraz pojedynczych żołnierzy) w warunkach braku widoczności (noc, mgła, opady atmosferyczne, zadymienie, kurz) itp.;

– wykrywanie rejonów zgrupowania wojsk wyposażonych w ww. środki walki, obserwację ruchu wojsk, rozpoznawanie dróg dowozu i ewakuacji;

– wskazywanie celów i kierowanie ogniem broni pokładowej, szczególnie śmigłowców oraz samolotów lotnictwa wojsk lądowych.

Badania wykazały, że maskowanie radiolokacyjne w działaniach obronnych związku operacyjnego powinno obejmować odpowiednie przedsięwzięcia i działania w zakresie ukrywania wojsk i obiektów związku operacyjnego przed rozpoznaniem radiolokacyjnym przeciwnika, a także w zakresie dezinformowania i pozorowania radiolokacyjnego. W zależności od szczebla organizacyjnego udział poszczególnych składowych w całości wykonywanych przedsięwzięć w obszarze obrony związku operacyjnego powinien być różny, np. w maskowaniu bezpośrednim podstawę powinno stanowić ukrywanie radiolokacyjne, a w maskowaniu operacyjnym – pozorowanie.

---

[54] Chociaż występuje już od czasów II wojny światowej, nie ujmowane jest w dokumentach normatywnych i podręcznikach jako oddzielny rodzaj rozpoznania. Często utożsamiane jest z rozpoznaniem radiotechnicznym a nawet technicznym [59;87].

[55] SLAR - ang. Side-Looking Airborne Radar.

Przedsięwzięcia wykonywane w ramach maskowania radiolokacyjnego powinny być podzielone na **organizacyjne i techniczne.** Należy jednak mieć na uwadze, że przedsięwzięcia te powinny być ze sobą ściśle powiązane i uzupełniać się wzajemnie w obszarze odpowiedzialności obronnej związku operacyjnego w zależności od wykonywanych zadań, warunków naturalnych, prowadzonego rozpoznania przeciwnika i możliwości w tym zakresie wojsk związku operacyjnego.

Przedsięwzięcia organizacyjne – dotychczas stosowane najczęściej – mają na celu ukrywanie[56] różnych obiektów w obszarze odpowiedzialności obronnej związku operacyjnego. Polegają na odpowiednim wykorzystaniu w tym celu masek naturalnych, właściwości terenu i przedmiotów terenowych, pory doby (nocy) pogody (mgły) oraz innych warunków meteorologicznych mających wpływ na obniżenie efektywności środków rozpoznania radiolokacyjnego.

Najlepszymi ukryciami naturalnymi dla wojsk i obiektów związku operacyjnego mogą być tylne zbocza wzniesień o kącie nachylenia większym niż 10^{o}, wąskie doliny, wąwozy i jary, lecz tylko w wypadku odpowiedniego ich usytuowania względem kierunków rozpoznania[57]. Wszelkiego rodzaju fałdy terenowe o odpowiedniej wysokości i stromości mogą tworzyć tzw. cienie radiolokacyjne, zmniejszając lub eliminując oddziaływanie rozpoznawczych środków radiolokacyjnych przeciwnika.

Podobną rolę mogą odgrywać kompleksy leśne (zarówno iglaste jak i liściaste) z gęstym poszyciem i wysokością drzew powyżej 2 m. Jednak odsunięcie wojsk i obiektów od skraju w głąb lasu o gęstości drzew 20 – 25 na 100 m^2 w okresie letnim powinno być nie mniejsze niż 20 – 25 m, w zimie natomiast 30 – 35 m. Wysokość maski naturalnej nie powinna być mniejsza niż 0,5 m od ukrywanych obiektów.

Duże znaczenie w ochronie przed oddziaływaniem tych środków mogą mieć rejony zurbanizowane [17;52], przede wszystkim duże i średnie aglomeracje o różnorodnej strukturze wewnętrznej, a także osiedla i wioski. Stwarzają one specyficzne warunki do osłony wojsk przed rozpoznaniem. Dotyczy to zwłaszcza ekranizujących właściwości różnorodnych budowli tworzących również cienie radiolokacyjne. Na przykład moc sygnałów odbitych od powierzchni materiałów budowlanych (w porównaniu z odbiciem od metalu) zmniejsza się:

---

[56] Niektóre źródła podają, że ukrycie obiektu przed obserwacją następuje w warunkach, kiedy różnica odbijania obiektu i tła nie przekracza 1,5 – 3 m^2 [62;66].

[57] Fale elektromagnetyczne wykorzystywane w radiolokacji rozprzestrzeniają się prostoliniowo, a zatem możliwości wykrywania są ograniczone m in. ukształtowaniem terenu i obecnością różnych obiektów i przedmiotów terenowych [62].

od cegły 8 – 10 razy; od betonu 3 – 5 razy; od konstrukcji drewnianych 4 – 8 razy. Pozwala to również w znacznym stopniu ochronić wybrane elementy ugrupowania obronnego związku operacyjnego przed bezpośrednimi uderzeniami środków ogniowych. **Umiejętne wykorzystanie ochronnych i maskujących właściwości terenu pozwala zmniejszyć możliwości rozpoznania oraz skutki uderzeń ogniowych o 10 – 50 % i więcej** [66].

Niekorzystne warunki atmosferyczne i pogodowe, a szczególnie obecność w atmosferze śniegu, deszczu, mgły, dymów oraz kurzu zwiększa tłumienność rozprzestrzeniania się energii elektromagnetycznej oraz utrudnia wykrycie małokontrastowych[58] obiektów. Przenikalność centymetrowych fal radiowych i krótszych podlega silnemu obniżeniu podczas silnych deszczów, mgieł i śnieżyc. W zależności od intensywności zjawisk atmosferycznych zasięg środków radiolokacyjnych może się zmniejszyć o 35 – 60 %.

Podczas organizacji **przedsięwzięć technicznych** maskowania radiolokacyjnego należy uwzględniać, że technika bojowa i obiekty wojskowe są „widziane" przez stacje radiolokacyjne przeciwnika w określonych tłach i mogą być przez nie wykryte w przypadku wystarczającego kontrastu radiolokacyjnego obiektów z tłami, na których występują.

Na podstawie analizy rozwiązań światowych oraz badania opisów patentowych można wnioskować, że wysiłki specjalistów w tej dziedzinie koncentrują się nie tylko na opracowaniu materiałów maskujących, lecz przede wszystkim na obniżaniu skutecznej powierzchni odbicia obiektów. W tym celu wykorzystywane są (rysunek 2.15.) pokrycia specjalne pochłaniające lub rozpraszające energię elektromagnetyczną oraz wszelkiego rodzaju ekrany radiolokacyjne i sztuczne urządzenia odbijające (odbijacze kątowe i dipolowe) itp.



Rys. 2.15. Podział technicznych środków maskowania radiolokacyjnego w działaniach obronnych związku operacyjnego

[58] Kontrast na ekranie radiolokatora jest rezultatem zróżnicowania właściwości odbijających dla fal elektromagnetycznych obiektu i tła [29].

Osłabiają[59] one natężenie odbitych od nich sygnałów echa.

Pokrycia pochłaniające (rozpraszające) energię elektromagnetyczną należy wykorzystywać do maskowania techniki bojowej oraz obiektów stałych[60]. Powinny być wykorzystywane do rozpraszania i wytłumiania energii elektromagnetycznej radiolokatorów, docierającej do rozpoznawanego obiektu. Zmniejszają one skuteczną powierzchnię odbicia poszczególnych środków walki. Pokrycia te, często nazywane pokryciami przeciwradiolokacyjnymi, powinny być wytwarzane jako siatki maskujące (maty), farby, pokrycia z tworzyw sztucznych. Mogą one być selektywne lub szerokopasmowe.

Pokrycia selektywne (na wybrane pasmo częstotliwości) jest łatwiej zbudować, jednak na polu walki nie zawsze mogą spełniają swoje zadanie. Selektywne pokrycia przeciwradiolokacyjne wykonuje się jednowarstwowo. Zapewniają one wytracenie energii elektromagnetycznej o określonej częstotliwości. Tego rodzaju pokrycia należy umieszczać bezpośrednio na powierzchni celu. Podczas opromieniowania powierzchni pokrycia, część energii elektromagnetycznej odbija się, a część przenika w głąb i załamuje się. Załamane fale elektromagnetyczne docierają do powierzchni obiektu, odbijają się od niej i wracają w kierunku powierzchni pokrycia przeciwradiolokacyjnego. Fale odbite od powierzchni pokrycia i odbite od powierzchni celu sumują się z różnicą fazy o 180^{O}. W rezultacie następuje wytłumienie sygnału. Tego rodzaju pokrycia zapewniają współczynnik odbicia 1 – 2 % przy nieznacznej grubości materiału.

W pokryciach szerokopasmowych przenikalność dielektryczna materiału i straty energii elektromagnetycznej w warstwie pokrycia rosną stopniowo w miarę przenikania fal w głąb. Znaczną zmianę przenikalności i wartości strat można uzyskać przez zastosowanie kilku warstw wykonanych z różnych materiałów pochłaniających. Wielowarstwowe, grube pokrycia pracują w dość szerokim zakresie. Można wykonać je z mas plastycznych, z rozproszonymi w określony sposób materiałami ferromagnetycznymi. Między poszczególnymi warstwami mogą się też znajdować specjalne błony pochłaniające energię elektromagnetyczną. Ponadto pokryciami tego typu mogą też być wielowarstwowe koce i siatki maskujące. Liczba warstw izolujących i przewodzących powinna być uzależniona od szerokości pasma i zakresu częstotliwości, które ma tłumić.

---

[59] Całkowite ukrycie obiektów wojskowych przed obserwacją radiolokacyjną jest bardzo trudne. Zadawalające wyniki maskowania można osiągnąć dopiero wówczas, gdy natężenie sygnałów odbitych od obiektów zostanie zmniejszone setki a nawet tysiące razy. Trudność tę pogłębia fakt, że urządzenia rozpoznawcze pracują w szerokim zakresie częstotliwości i dysponują znacznym dynamicznym potencjałem wykrycia [29;62].

[60] Powinny być dostosowane także do maskowania obiektów przed rozpoznaniem optoelektronicznym [62].

Jednym ze sposobów wykonania pokryć przeciwradiolokacyjnych może być wykorzystanie, jako warstwy pochłaniającej, magnetodielektryków. Przy ich zastosowaniu można stworzyć dobre pokrycia przeciwradiolokacyjne dla zakresu fal centymetrowych i milimetrowych w postaci konstrukcji dwuwarstwowych o grubości około 1 cm i współczynniku odbicia fal elektromagnetycznych 6 – 8 %. Przy zastosowaniu wielodyspersyjnych proszków drobnoziarnistych żelaza karbonylonowego można uzyskać jeszcze cieńsze pokrycia odznaczające się współczynnikiem odbicia 1 – 2 %.

Dodatkowym czynnikiem, który umożliwia osłabienie odbicia od materiału pochłaniającego, jest odpowiedni kształt jego powierzchni zewnętrznej. Powierzchnia chropowata sprzyja zmniejszeniu odbicia energii elektromagnetycznej w kierunku stacji radiolokacyjnej. Także odpowiedni kształt celu może zmniejszać ilość energii odbijanej w kierunku stacji radiolokacyjnej.

Ważną rolę mają do spełnienia szerokopasmowe pokrycia nowej generacji, które zapewniają 20–krotne osłabienie sygnału odbitego w zakresie 0,8 – 12 cm. Pokryciem tym może być włóknista mata przesycona gumą z dodatkami sadzy węglowej i elementów ferromagnetycznych. Ponadto każdy włos jest pokryty cienką warstwą półprzewodzącą. Tego rodzaju pokrycia osłabiają odbicie od powierzchni metalowej dla zakresu fal 10 cm – 100 razy, dla fal 3 i 2 cm – 300 razy, dla zakresu około 1cm – 1000 razy. Technologia osłabiania odbicia radiolokacyjnego otrzymała anglojęzyczną nazwę „stealth".

Ekrany radiolokacyjne - wykonane z tkanin metalizowanych lub grafitowych – mogą służyć do maskowania wojsk związku operacyjnego w rejonach ześrodkowania, zajmujących pozycje (rejony) obrony, samolotów na lotniskach, składów amunicji i innych obiektów typu stałego lub znajdujących się na postoju. Pokrycia maskujące tego typu powinny zmieniać współczynnik odbicia ukrywanych obiektów tak, aby zmniejszyć nie mniej niż o 50 % odległość ich wykrycia przez stację radiolokacyjną przeciwnika. Tłumienie odbić kompletów maskujących powinno być nie mniejsze niż 20 dB (stukrotne) w całym zakresie długości fal. Struktura sygnałów odbitych od zamaskowanego obiektu nie powinna w istotny sposób różnić się od tzw. odbić naturalnych otaczającego terenu. Analiza dostępnej literatury specjalistycznej upoważnia autora do postawienia tezy, że obecnie w kraju nie są eksploatowane pokrycia maskujące spełniające te wymagania[61].

---

[61] Natomiast na szczególną uwagę zasługuje pokrycie firmy Barrakudaverken AB (Szwecja). Ma ono strukturę trójwarstwową, przy czym warstwy zewnętrzne są zabarwione w sposób odpowiadający maskowaniu optycznemu. Środkowa warstwa maskująca jest wykonana z materiału syntetycznego metalizowanego lub zawierającego folię, siatkę metalową lub metalowe cienkie włókna różnej długości. W celu zwiększenia efektu maskowania dla różnych kątów obserwacji – powłoce materiału nadaje się formę przestrzenną poprzez jej nacięcia [26;97].

Do pozorowania[62] i dezinformowania radiolokacyjnego należy wykorzystywać sztuczne urządzenia odbijające i rozpraszające energię elektromagnetyczną: odbijacze kątowe i dipole odbijające (zakłócające).

Odbijacze kątowe wywołują zwiększoną liczbę obiektów na ekranach stacji radiolokacyjnych, tworząc przez to obraz nieczytelny i niewiarygodny. Służą, więc do pozorowania obiektów, obecności wojsk i techniki bojowej w obszarze odpowiedzialności obronnej związku operacyjnego[63]. Za ich pomocą można pozorować mosty stałe i pontonowe, przeprawy promowe, drogi, wyrzutnie rakiet, różne pojazdy bojowe, lotniska i samoloty na nich, bazy morskie, zmieniać linie brzegową i naturalne dozory radiolokacyjne. Istnieje możliwość pozorowania obiektów ruchomych, co ma szczególnie duże znaczenie przy wykorzystaniu przez przeciwnika radiolokacyjnych stacji dopplerowskich.

Odbijacze kątowe wykonane z dużą dokładnością są urządzeniami wąskopasmowymi. Ich skuteczna powierzchnia odbicia jest odwrotnie proporcjonalna do kwadratu długości padającej fali elektromagnetycznej. Oznacza to, że podczas użycia przez przeciwnika stacji radiolokacyjnej pracującej na niższych częstotliwościach skuteczna powierzchnia odbicia (SPO) odbijaczy tego typu maleje. Wykonuje się je z blach metalowych lub środków metalizowanych, ponieważ wnikanie energii elektromagnetycznej w głąb metalu jest niewielkie, a współczynnik odbicia duży. Ścianki odbijaczy kątowych mogą mieć różne wymiary i kształty: kwadratowe, sektorowe, trójkątne, kompensujące. Odbijacze kątowe mogą być również wykonywane z siatek metalowych, w których czynnikiem określającym zdolność odbijania energii elektromagnetycznej przez siatkę jest wymiar jej oczek. Właściwością odbijaczy kątowych jest zdolność odbijania energii elektromagnetycznej stacji radiolokacyjnej w kierunku przeciwnym do jej padania. Największą kierunkowość działania mają odbijacze kątowe o ściankach kwadratowych, odbijacze o ściankach trójkątnych mają zaś charakterystyki bardziej równomierne. Szerokości robocze charakterystyk odbicia są następujące: dla odbijaczy o ściankach kwadratowych – 25°, o ściankach trójkątnych – 40°, sektorowe (o ściankach wykroju ćwiartki koła) – 35°.

---

[62] Istotną wadą urządzeń radiolokacyjnych jest trudność odróżnienia na ekranie wskaźnika celów rzeczywistych od pozornych, jeżeli analogiczna jest ich skuteczna powierzchnia odbicia. Przez skuteczną powierzchnię odbicia celu rozumie się taką ekwiwalentną powierzchnię zorientowaną normalnie do kierunku padania fali, która promieniując we wszystkich kierunkach całkowitą padającą na nią mocą pola pierwotnego wywołuje w punkcie odbioru (położenia radiolokatora) taką samą gęstość strumienia mocy jak rzeczywisty cel [29;72].

[63] Odbijacze kątowe są postrzegane również jako pasywne środki zakłócania. Z tych względów taktyka ich użycia ulokowana jest w zakłócaniu informacyjnym [62].

W celu uzyskania bardziej równomiernego rozkładu odbicia energii elektromagnetycznej w szerokim zakresie zmienności kątów opromieniowania mogą być stosowane tzw. „kompensacyjne" lub wieloselekcyjne (cztero – lub ośmiosekcyjne) odbijacze kątowe.

Analiza rozwiązań światowych wskazuje, że należy wyposażyć wojska związku operacyjnego[64] w różnego typu odbijacze kątowe, które mogą mieć konstrukcję stałą, składaną lub nadmuchiwaną. Bez względu na konstrukcję należy nie tylko stawiać je, jak ma to miejsce obecnie, ale również ciągnąć po ziemi, w powietrzu i w razie potrzeby – po wodzie. Należy mieć na uwadze, że działania obronne związku operacyjnego, szczególnie o charakterze pozycyjnym umożliwiają szerokie zastosowanie tego typu konstrukcji.

Dipole odbijające[65] stosowane są dotychczas przede wszystkim do maskowania samolotów oraz pozorowania celów powietrznych i nawodnych. Idea ich wykorzystania polega na tym, że dipole pod wpływem dochodzącej do nich energii elektromagnetycznej ze stacji radiolokacyjnej przeciwnika – powodują wtórne jej promieniowanie (zachowują się jak antena). W wyniku tego zjawiska powstają na ekranach wskaźników tych stacji fałszywe znaki, imitujące rzeczywiste cele (zaśmiecanie ekranów). Odbicia te mają dość wąskie pasmo fluktuacji.

Współczesne dipole odbijające powinny być zbudowane z metalizowanych włókien szklanych[66] lub taśm (albo jeszcze innych materiałów) o długości połowy fali elektromagnetycznej zakłócanych stacji radiolokacyjnych lub stanowiących wielokrotność połowy długości tej fali. Charakteryzują się: skuteczną powierzchnią odbicia, szybkością opadania (i zaniku zakłóceń) i koncentracją dipoli w jednostce objętości.

Skuteczna powierzchnia odbicia to miara energii elektromagnetycznej, która powraca do urządzenia odbiorczego stacji radiolokacyjnej i jest sumą odbić pojedynczych elementów dipolowych. Wyrażana jest w metrach kwadratowych. Przy maskowaniu celu skuteczna powierzchnia odbicia obłoku dipolowego powinna przewyższać 3 – 5 razy skuteczną powierzchnię odbicia celu.

---

[64] Należy nadmienić, że w wyposażeniu jednostek inżynieryjnych operacyjnego przeznaczenia wojsk lądowych są trzy zasadnicze typy składanych odbijaczy kątowych: **08 - 33** – o zarysie okrągłym i średnicy koła 13 cm, złożony z 8 trójściennych rożków do maskowania i pozorowania na lądzie pojazdów mechanicznych, małych samolotów i in.; **T8-62/L (mały)** – o trójkątnych kształtach zmian, złożony z 8 trójściennych rożków o długości krawędzi trójkąta 62 cm (SPO = 15 – 20 m^2) do maskowania i pozoracji różnych obiektów wojskowych; **T8-62/W (duży)** – o trójkątnych kształtach zmian, złożony z 8 trójściennych rożków o długości krawędzi trójkąta 62 cm (SPO = 40-60 m^2) do pozoracji budynków, mostów stalowych, pontonowych itp. Por.: Wł. Ślemp, W. Kawka, „Informator sprzętu inżynieryjnego wojsk własnych", wyd. AON, Warszawa 1999.

[65] Przeznaczone są głównie do pasywnego zakłócania pracy stacji radiolokacyjnych przeciwnika [62].

[66] Włókno szklane o grubości 17,5 – 50 μm pokrywane jest 2,5 μm powłoką z aluminium lub cynku [62].

Szybkość opadania decyduje o czasie utrzymywania się celu pozornego, który jest zarazem czasem maskowania obiektu rzeczywistego. Warunki atmosferyczne, takie jak: średnia prędkość wiatru, średnia temperatura warstwy powietrza, turbulencja atmosfery mają zasadniczy wpływ na rozprzestrzenianie się obłoku dipolowego. W polskich warunkach atmosferycznych przeciętna szybkość opadania wynosi 25 – 50 m/min, a obłok powiększa się do swojego maksimum w czasie 1 – 3 minut i wielkość tę utrzymuje przez około 1,5 – 3 minut.

Koncentracja dipoli w jednostce objętości decyduje o wytłumieniu fali elektromagnetycznej, a przez to o zmniejszeniu zasięgu stacji radiolokacyjnej. Wyraża się ją liczbą dipoli w 1 m^3 powietrza. Dziesięciokrotne zmniejszenie zasięgu stacji radiolokacyjnej odpowiada tłumieniu 40 dB. Dla fali o długości 3 cm osiąga się taki stan przy 30 dip/m^3.

Pozorowanie radiolokacyjne w działaniach obronnych związku operacyjnego za pomocą dipoli odbijających powinno polegać – analogicznie do innych rodzajów wojsk – na wystrzeliwaniu przez specjalne wyrzutnie zamontowane na środkach walki[67] (czołgach, transporterach opancerzonych, armatach, rakietach) pocisków dipolowych lub na wyrzucaniu z samolotów paczek z dipolami w chwili wykrycia ich opromieniowania)[68]. Liczba tych pocisków powinna być każdorazowo dostosowywana do potrzeb.

2.2.1.3. Maskowanie optoelektroniczne

Maskowanie optoelektroniczne ma na **celu uniemożliwienie zdobywania oraz przetwarzania tych danych o wojskach i obiektach znajdujących się w obszarze odpowiedzialności obronnej związku operacyjnego, których nośnikami są fale elektromagnetyczne pasma optycznego[69].** Należy zauważyć, że do pracy w tym paśmie skonstruowano całą rodzinę urządzeń optoelektronicznych[70], pozwalających na prowadzenie rozpoznania

---

[67] Przykładem mogą być wyrzutnie dipoli „Jastrząb" montowane na okrętach Marynarki Wojennej RP. Por.: M. Zieliński, „Porównanie systemów biernej obrony przeciwrakietowej będących na uzbrojeniu Marynarki Wojennej RP", w materiałach I konferencji NT „Systemy Rozpoznania i WRE, wyd. WAT, Żegiestów 1995, s.137.

[68] W tym celu środki walki należy wyposażyć – podobnie jak samoloty i okręty – w indywidualne odbiorniki ostrzegające o opromieniowaniu radiolokacyjnym. Koncepcja takiego odbiornika przedstawiona jest w materiałach IV konferencji NT „Systemy Rozpoznania i WRE", wyd. BIL-GRAL s.c. Babice Stare 1999, s. 228.

[69] Pasmo optyczne widma elektromagnetycznego (zakres optyczny) stanowią promieniowania: ultrafioletowe (długość fali: 0,01 – 0,38 μm), widzialne (długość fali: 0,38 – 0,76 μm) i podczerwone (długość fali: 0,76 – 1000 μm) [59;87].

[70] Optoelektronika to dział elektroniki, którego przedmiotem jest łączne wykorzystanie optycznego i elektrycznego sposobu przetwarzania i przekazywania sygnałów. Podstawą optoelektroniki są fizyczne procesy warunkujące przetwarzanie sygnałów elektrycznych na optyczne i sygnałów optycznych na elektryczne oraz procesy wytwarzania, przesyłania, przetwarzania i magazynowania informacji niesionych przez światło [59;87].

w ultrafiolecie, w zakresie promieniowania widzialnego, a także w zakresie bliskiej, średniej, dalekiej i skrajnej podczerwieni.

Z analizy wyposażenia wielu systemów rozpoznania potencjalnego przeciwnika wynika, że w ich składzie mogą znaleźć się m.in.: różnego rodzaju urządzenia rozpoznawcze, m.in.: telewizyjne termowizyjne, noktowizyjne oraz laserowe.

Dane pozyskiwane w wyniku rozpoznania prowadzonego za pomocą tych środków mają charakter obrazowy. Mogą, więc być szeroko wykorzystywane do monitorowania pola walki. Wynika stąd potrzeba podejmowania skutecznych przedsięwzięć przeciwrozpoznawczych w tym zakresie; ważną rolę powinno tu odgrywać maskowanie optoelektroniczne.

Problematyka maskowania optoelektronicznego w działaniach obronnych związku operacyjnego powinna być ściśle powiązana z maskowaniem radiolokacyjnym i rozwiązywana za pomocą ukrywania, dezinformowania i pozorowania optoelektronicznego. W zależności od szczebla organizacyjnego udział poszczególnych składowych w całości wykonywanych przedsięwzięć powinien być różny, np. w maskowaniu bezpośrednim podstawę powinno stanowić ukrywanie optoelektroniczne.

Przedsięwzięcia wykonywane w ramach maskowania optoelektronicznego powinny być podzielone na **organizacyjne i techniczne.** Należy jednak mieć na uwadze, że składowe te powinny być ze sobą ściśle powiązane i uzupełniać się wzajemnie w obszarze odpowiedzialności obronnej związku operacyjnego w zależności od rodzaju wykonywanych zadań, warunków naturalnych, prowadzonego rozpoznania przeciwnika i możliwości w tym zakresie wojsk związku operacyjnego.

Przedsięwzięcia organizacyjne mają na celu ukrywanie różnych wojsk i obiektów znajdujących się w obszarze odpowiedzialności obronnej związku operacyjnego. Powinny polegać na odpowiednim wykorzystaniu ukryć naturalnych i wynikają z właściwości terenu i przedmiotów terenowych, pory doby (nocy) pogody (mgły), zastosowania zasłon dymnych, oraz innych warunków meteorologicznych mających wpływ na obniżenie efektywności środków rozpoznania optoelektronicznego. Przedsięwzięcia te powinny być ściśle skoordynowane i prowadzone według zasad obowiązujących w maskowaniu radiolokacyjnym[71].

Badania wykazały, że znaczny wpływ na obniżenie efektywności środków rozpoznania optoelektronicznego mają zasłony dymne. Uniemożliwiają one lub znacznie utrudniają przeciwnikowi prowadzenie nie tylko obserwacji optycznej, lecz również laserowej i termowizyjnej. Właściwości maskujące dymów przedstawiono w tabeli 2.2.

---

[71] Problematyka ta zawarta została w poprzednim podrozdziale.

Tabela 2.2.

MASKUJĄCE WŁAŚCIWOŚCI DYMÓW

Lp.	Rodzaj rozpoznania	Zakres fal roboczych	Zastosowanie	Skuteczność maskowania
1.	optyczno-wzrokowe	– pasmo widzialne (0,38 – 0,76 μm)	broń strzelecka	10–15 –krotne zmniejszenie skuteczności ognia broni strzeleckiej i pokładowej
			środki przeciwpancerne	8–10 –krotne zmniejszenie skuteczności środków przeciwpancernych
			bombardowanie lotnicze	5–7 –krotne zmniejszenie skuteczności bombardowania
2.	termowizyjne (pasywne)	– pasmo 3 – 5 μm; – pasmo 10 – 13 μm.	lotnicze i naziemne systemy rozpoznania pola walki oraz systemy naprowadzania śmigłowców przeciwpancernych	2–3 –krotne zmniejszenie skuteczności rozpoznania i rażenia
3.	noktowizyjne (aktywne)	– 0,76 – 1,5 μm – bliska podczerwień; – 1,5–5,6 μm – średnia podczerwień; – 5,6 – 1000 μm – daleka podczerwień.	naziemne systemy rozpoznania pola walki	2–3 –krotne zmniejszenie skuteczności rozpoznania i rażenia
4.	laserowe	– od ultrafioletu (0,1 – 0,38 μm) do dalekiej podczerwieni (5,6 – 1000 μm)	lotnicze, artyleryjskie i czołgowe celowniki i dalmierze	całkowite przeciwdziałanie tym środkom

Z przedstawionych w tabeli danych liczbowych wynika, że skuteczność maskowania zasłonami dymnymi jest wysoka i w zależności od typu środka rozpoznania optoelektronicznego waha się od się 2 – 3 - krotnego zmniejszenia jego skuteczności do całkowitego przeciwdziałania mu. Ważną rolę w maskowaniu dymami odgrywa wypracowanie sposobów stawiania zasłon dymnych ze względu na ich ograniczony czas efektywnego zadymiana. Czas zadymiania, w zależności od rodzaju środka dymnego, waha się od kilku minut (świeca dymna, ręczny granat dymny) do zasłon długotrwałych wytwarzanych przez lotnicze i naziemne wytwornice (generatory) dymu. **W celu podniesienia efektywności maskowania dymami należy dążyć do opracowania nowych środków umożliwiających m in. stosowanie aero-**

zolowych zasłon dymnych, wytwarzanie tzw. dymów metalizowanych, a także odpowiednie wyposażenie wojsk związku operacyjnego w takie urządzenia dymotwórcze.

Realizacja **przedsięwzięć technicznych** maskowania optoelektronicznego jest z kolei związana ze stosowaniem różnego rodzaju etatowych i podręcznych środków maskujących oraz odpowiednich materiałów. Należy podkreślić fakt, że stosowanie środków etatowych, w odróżnieniu od podręcznych, pozwala na znaczne skrócenie czasu wykonania zadań, a ponadto uniezależnia od warunków naturalnych oraz zapewnia lepsze warunki przeciwdziałania środkom rozpoznania przeciwnika. Dlatego też rozwojowi tych środków maskowania powinno się nadać odpowiednią rangę, zwłaszcza że wraz z rozwojem technologicznym środków rozpoznania optoelektronicznego obserwuje się tendencję do stopniowego zmniejszania udziału przedsięwzięć organizacyjnych w maskowaniu optoelektronicznym organizowanym w działaniach obronnych związku operacyjnego.

Obecnie w wyposażeniu związku operacyjnego znajdują się różnego rodzaju maski przeznaczone do maskowania bezpośredniego obiektów nieruchomych (na postoju). Są to głównie maski poliamidowe: czołgowe, samochodowe, artyleryjskie i piechoty. Charakteryzują się one zaledwie dostatecznymi zdolnościami maskującymi w zakresie widma widzialnego oraz w bliskiej podczerwieni. Stają się one coraz mniej przydatne w maskowaniu optoelektronicznym. Zdaniem autora powinny być jak najszybciej zastąpione pokryciami termicznymi (metalizowanymi ekranami).

Poważne braki odczuwa się ponadto w zakresie bezpośredniego maskowania żołnierzy. Niezbędne staje się wyposażenie stanów osobowych w metalizowane umundurowanie, metalizowane narzutki maskujące lub kombinezony, odpowiednie pasty lub kremy ochronne oraz odpowiednie okulary (gogle), zabezpieczające ich wzrok przed oślepianiem laserowym[72].

Rozwój współczesnych środków rozpoznania optoelektronicznego wymusza podjęcie działań w zakresie maskowania mobilnych elementów ugrupowania operacyjnego (bojowego) oraz sprzętu technicznego będącego w ruchu[73]. Ważną rolę odgrywa, zatem ograniczenie kontrastu cieplnego, związanego z pracą takich elementów jak silnik, prądnica (agregat prądotwórczy), układy odprowadzania spalin[74], układy jezdne, nadajniki emitujące energię elek-

---

[72] Miniaturowe urządzenia tego typu wykorzystywane są obecnie przez kibiców na stadionach do oślepiania zawodników (bramkarzy) na boisku. Zdarzają się również przypadki uszkodzeń wzroku przez dzieci bawiące się zabawkami sprowadzanymi z Dalekiego Wschodu.

[73] Opracowanie zestawów do kompleksowego maskowania sprzętu technicznego powinno mieć miejsce w fazie projektowania lub podczas jego modernizacji.

[74] Należy zaznaczyć, że gazy spalinowe i ciepłe powietrze nie mają – mimo wysokiej temperatury – istotnego wpływu na charakterystykę cieplną obiektu ze względu na niski współczynnik emisyjności i szybką dyfuzję w otaczającym powietrzu. Powodują natomiast nagrzewanie się elementów znajdujących się w pobliżu [55;56].

tromagnetyczną i in. Jednym ze sposobów zmniejszania kontrastu między nagrzanymi elementami a tłem powinno być stosowanie pokryć – ekranów termicznych w postaci pokrowców na nagrzewające się elementy (zespoły) pojazdów oraz osłon i filtrów szerokopasmowych tych urządzeń.

Również maskowanie przed oddziaływaniem generatorów promieniowania mikrofalowego dużej gęstości mocy powinno polegać na uodpornieniu i izolowaniu układów, aby nie powstawała w nich energia cieplna.

Ważnym i – jak wykazuje praktyka ostatnich wojen i konfliktów lokalnych – skutecznym środkiem maskowania jest malowanie maskujące[75], którego podstawowe rodzaje to:

- malowanie ochronne (ukrywające);
- malowanie pozorujące;
- malowanie deformujące.

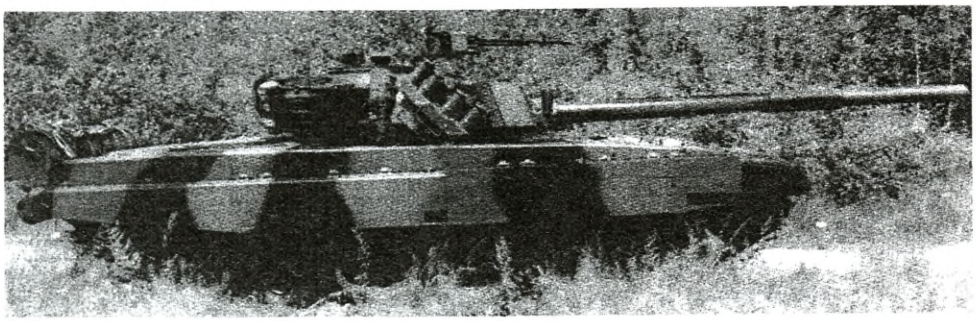
W malowaniu ochronnym, wykonywanym podczas przygotowania wojsk związku operacyjnego do działań obronnych, należy wykorzystać specjalne farby, które powodowałyby w czasie obserwacji celu w podczerwieni powstawanie złudzeń polegających na zlewaniu się widma podczerwieni obserwowanego celu z widmem tła. Farby takie, nazywane metamorficznymi powodują bowiem zmianę koloru pod wpływem warunków zewnętrznych (temperatury, natężenia oświetlenia).

Malowaniem pozorującym należy objąć obiekty pozorne, których kolorystyka i charakterystyki spektralne nie powinny odbiegać od obiektów rzeczywistych. Środki umożliwiające budowę obiektów pozornych powinny być zatem o zbliżonych do rzeczywistych charakterystykach wizualnych, termalnych i elektromagnetycznych. Takie możliwości ma np. system DECEPTION – szwedzkiej firmy Barracuda [26;97]. W większości są to obiekty wykonane w skali 1:1, pozorujące sprzęt bojowy, systemy rakietowe, mosty, bazy lotnicze itp. Obiekty te są szczególnie efektywne przy ataku z powietrza, ponieważ pilot ma zaledwie kilka sekund na identyfikację obiektu i podjęcie decyzji. Prawdopodobieństwo przeprowadzenia ataku na cel pozorny przy zastosowaniu właściwej techniki pozoracji jest bardzo duże. Rozproszenie wysiłku rozpoznawczego przeciwnika zwiększa szansę na przetrwanie elementów rzeczywistych. Należy sądzić, że środki te będą ulegały ciągłemu rozwojowi, ponieważ pozwalają przy niskich nakładach finansowych znacząco zmniejszyć straty własne. Średnio ich koszt nie przekracza 0,25 % ceny pozorowanego obiektu.

---

[75] Jednak w naszych wojskach lądowych nie ma etatowych zestawów do malowania maskującego, a przygotowanie stanów osobowych do jego wykonania jest niewystarczające.

Na szczególną uwagę zasługuje malowanie deformujące, nazywane również kamuflażowym. Na jego potrzeby należy wykorzystać różnego rodzaju farby nitrocelulozowe, olejne, kazeinowe oraz farby nowej generacji oparte na dyspersji koloidowej, poliuretanowej i farby rozpuszczalne w wodzie. Należy opracować wzorcowe przykłady wymalowań sprzętu technicznego na różne pory roku[76]. Przy doborze rodzaju tych farb należy zwrócić uwagę na ich kolorystykę i charakterystyki spektralne w zależności od uśrednionego tła terenu[77] (wzór malowania deformującego czołgu przedstawiono na rysunku 2.16.).



Rys. 2.16. Wzór malowania deformującego czołgu

2.2.1.4. Maskowanie czujnikowe

Maskowanie czujnikowe ma na **celu uniemożliwienie zdobywania i przetwarzania danych o wojskach i obiektach znajdujących się w obszarze odpowiedzialności obronnej związku operacyjnego , których nośnikami są fale sprężyste[78] (infradźwięki[79], ultradź-**

---

[76] Obecnie w siłach zbrojnych czołowych państw NATO malowanie maskujące odbywa się bezpośrednio na liniach produkcyjnych sprzętu lub w specjalnie przygotowanych punktach wyposażonych w urządzenia do programowania wzorów malowania. Farby używane do malowania sprzętu są odporne na działania substancji chemicznych. Pojazd pomalowany taką farbą sprawia wrażenie znikania. Najbardziej rozpowszechnioną techniką malowania maskującego są trójbarwne wzory komponowane z dużych plam brązowych, zielonych i czarnych.

[77] Według danych amerykańskich, sprzęt bojowy oraz obiekty i urządzenia inżynieryjne maluje się jednocześnie czterema ustalonymi kolorami. Sprzyja to lepszemu ich ukryciu (ogółem w wojskach amerykańskich wykorzystuje się 12 kolorów maskujących).

[78] Fale sprężyste – zaburzenia rozchodzące się w ośrodku sprężystym, polegające na drganiu cząsteczek wokół punktu równowagi. „Ilustrowana encyklopedia dla wszystkich. Fizyka", wyd. WNT, Warszawa 1991, s. 77.

[79] 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 oraz eksplozji na polu walki. Tamże, s. 112.

więki[80]) oraz wszelkiego rodzaju uboczne efekty towarzyszące działaniom bojowym, na przykład: termiczne, sejsmiczne, naciskowe, magnetyczne, chemiczne, zapachu.

Przeprowadzone badania dowiodły, że do postrzegania materii pola walki przez pryzmat fal sprężystych oraz w zakresie efektów magnetycznych i chemicznych środowiska potencjalny przeciwnik może wykorzystać całą gamę urządzeń czujnikowych z szerokim zastosowaniem elektronicznej przemiany rejestrowanych efektów [25;59;89;133]. W wyniku prowadzonego rozpoznania czujnikowego przeciwnik ma możliwość pozyskiwania danych z niedostępnych stref[81] w czasie zbliżonym do rzeczywistego. Może również nadzorować:

- aktywność wojsk związku operacyjnego w wybranych rejonach, w których zostały rozmieszczone odpowiednie czujniki;
- natężenie ruchu i aktywność wojsk wzdłuż wybranych tras;
- aktywność wojsk w rejonach rozmieszczenia jego zapór i pól minowych;
- aktywność wojsk w rejonach przepraw rzecznych, mostów i brodów;
- rejony zaplanowane jako strefy lądowania lub zrzutu wojsk desantowo–szturmowych;
- zmiany w funkcjonowaniu elementów ugrupowania wojsk związku operacyjnego, ich stanowisk dowodzenia, węzłów łączności, elementów naprowadzania uzbrojenia, punktów zaopatrywania. itp.;
- wskazywanie celów.

Maskowanie czujnikowe w działaniach obronnych związku operacyjnego stanowi perspektywiczny rodzaj maskowania elektronicznego. Problematyka ta może być rozwiązywana za pomocą ukrywania, pozorowania czujnikowego i niszczenia. W zależności od szczebla organizacyjnego udział poszczególnych składowych w całości wykonywanych przedsięwzięć w obszarze odpowiedzialności obronnej związku operacyjnego powinien być różny. Podstawę powinno stanowić – z uwagi na szerokie użycie środków czujnikowych na szczeblach taktycznych – ukrywanie czujnikowe.

Przedsięwzięcia wykonywane w ramach maskowania czujnikowego powinny być podzielone na **organizacyjne i techniczne.** Należy jednak pamiętać, że powinny one być ze sobą ściśle powiązane i uzupełniać się wzajemnie w obszarze odpowiedzialności obronnej

---

[80] Ultradźwięki - fale sprężyste o częstotliwościach większych iż 20 kHz, a więc leżące powyżej zakresu ludzkiej słyszalności. Mogą być wykorzystane do rejestracji efektów akustycznych (odgłosów) pola walki. Tamże, s. 293.

[81] W przyszłości mogą być wysyłane w powietrze lub rozmieszczane na lądzie tysiące maleńkich czujników. Miniaturowe czujniki zapachu mogą nawet wyczuć przeciwnika, bowiem unoszące się w powietrzu biosensory będą mogły śledzić żołnierzy na podstawie zapachu ich oddechów lub potu [59].

związku operacyjnego w zależności od rodzaju wykonywanych zadań, warunków naturalnych, prowadzonego rozpoznania przeciwnika i możliwości w tym zakresie wojsk związku operacyjnego.

Przedsięwzięcia maskowania czujnikowego należy ukierunkować na ochronę przed rozpoznaniem, a w ślad za nim i zakłócaniem własnych detektorów, które wykorzystują energię odpowiadającą parametrami sygnałom bodźcowym, charakterystycznym dla środowiska – akustycznego, magnetycznego, elektrycznego, chemicznego.

Charakterystyczne dla środowiska akustycznego na polu walki są: odgłosy wybuchów, wstrząsy, warkot pojazdów mechanicznych i zespołów prądotwórczych. Maskowanie źródeł hałasu powinno sprowadzać się do wykorzystania maskujących właściwości terenu oraz stosowania okryć tłumiących hałas. Ponadto należy zapewnić unifikację środków transportu techniki bojowej, co zapobiega wykrywaniu i identyfikowaniu ich przez system czujnikowy przeciwnika. Problematyka ta sygnalizowana była w poprzednim podrozdziale.

Obrona przed generatorami infradźwieków powinna opierać się na budowaniu tzw. miękkich zasłon, w celu absorpcji energii fali dźwiękowej, oraz tworzeniu tzw. pól aktywnego hałasu. Istota ich działania polega na wytworzeniu fali dźwiękowej o tej samej długości, co fala atakująca, lecz odwróconej w fazie (o 180^0). Zasadniczym problemem w stosowaniu tego typu obrony jest stworzenie odpowiedniego zestawu specjalistycznych głośników oraz wzmacniaczy, które wymagają m.in. bardzo wydajnych układów chłodzenia.

2.2.1.5. Maskowanie informatyczne

W przyszłych działaniach obronnych związku operacyjnego należy liczyć się z systematycznym wzrostem wykorzystania rozległych i lokalnym sieci teleinformatycznych[82], które obsługiwać będą zautomatyzowane systemy dowodzenia, zautomatyzowane systemy rozpoznania oraz zautomatyzowane systemy naprowadzania uzbrojenia. Już w chwili obecnej sieci informatyczne są bogatymi źródłami danych o wojskach walczących stron. Wartościowe wia-

[82] Teleinformatyka jest dziedziną obejmującą użytkowanie sprzętu informatycznego przez odległych abonentów za pośrednictwem urządzeń telekomunikacyjnych. Oferowanie usług informatycznych przez sieć telekomunikacyjną czyni ją niejako automatycznie siecią teleinformatyczną. Mając do czynienia z nowoczesnymi sieciami zintegrowanymi i dysponując zaawansowanym technicznie terminalem abonenckim, korzysta się w zasadzie (praktycznie poza klasyczną usługa telefoniczną) z usług teleinformatycznych.

domości ulokowane są również w promieniowaniu komputerowym. W razie braku odpowiednich mechanizmów ochronnych możliwy staje się dostęp do ich baz danych[83].

Zgromadzone w nich zasoby informacyjne są narażone na rozpoznanie, penetrację i modyfikację. Możliwość włączania się do nich użytkowników nieupoważnionych staje się w obecnych czasach coraz bardziej prawdopodobna. Mogą oni śledzić, podsłuchiwać i przechwytywać dane oraz prowadzić dezinformację. Stąd też problem ochrony informacji w sieciach informatycznych nabiera szczególnego znaczenia. Aby zapewnić tę ochronę w pełnym zakresie, konieczne staje się wprowadzenie mechanizmów chroniących bazy danych przed szpiegostwem, piractwem oraz przypadkowym zniszczeniem lub modyfikowaniem [30;122]. Dotyczy to wszystkich poziomów *„działań na informacjach"*, a więc ich przetwarzania, przesyłania i przechowywania. Działania te narażone są na **podsłuch bierny**, stanowiący zagrożenie dla niejawności oraz na **podsłuch aktywny**, zagrażający autentyczności danych.

Podsłuch bierny – dotyczy przechwytywania przez przeciwnika danych, zwykle bez wykrywania tego faktu przez podsłuchiwanego. Podsłuch służy najczęściej do zapoznania się z treścią wiadomości, a w sieciach komputerowych do monitorowania przepływu informacji w celu ustalenia struktury sieci łączności. Podsłuch bierny (zagrożenie niejawności informacji) może odbywać się poprzez: przeglądanie, przenikanie i wnioskowanie.

Przeglądanie – polega na przeszukiwaniu sieci komputerowej w celu uzyskania informacji. Jest to proces podobny do śledzenia w sieciach łączności, przy czym istnieją tu dwie istotne różnice. Po pierwsze w sieciach komputerowych dane są przechowywane znacznie dłużej i dlatego przeglądanie jej jest zdecydowanie większym zagrożeniem niż śledzenie w sieciach łączności. Po drugie, wiadomości przesyłane w sieciach łączności są narażone nawet wtedy, kiedy dostęp do systemu jest zabroniony. Przeglądanie natomiast jest możliwe jedynie wówczas, gdy użytkownik ma prawo dostępu do sieci i do wybranych obszarów pamięci systemów komputerowych.

Przenikanie – zwane też przeciekaniem, dotyczy przepływu danych do nieuprawnionych użytkowników podczas procesów realizowanych z legalnym dostępem do danych.

Wnioskowanie – dotyczy procesów ustalenia danych niejawnych obejmujących wybrany element całości charakteryzowanej danymi jawnymi. Na przykład: przechwycenie

---

[83] 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. Przykładem w tym zakresie mogą być międzynarodowi piraci komputerowi (ang. hackers), którzy bez większych przeszkód włamują się do odpowiednio zabezpieczonych systemów komputerowych m in. Pentagonu. Nie trzeba zatem „być ani wielkim, ani bogatym", aby skutecznie prowadzić rozpoznanie informatyczne.

przez przeciwnika danych ze służby zapatrzenia żywnościowego dotyczącej ilości zamawianej żywności umożliwia określenie liczby żołnierzy danej jednostki.

Podsłuch aktywny (zniekształcanie) – dotyczy rozmyślnych modyfikacji wykonywanych na strumieniach danych. Celem tego działania może być pozyskiwanie danych połączone z zastąpieniem ich treści innymi. Działania takie są szczególnie niebezpieczne dla wojskowych sieci komputerowych, gdyż przeciwnik jest w stanie zinterpretować i wykorzystać pozyskane dane. Na przykład może wprowadzić do sieci błędne komunikaty i polecenia. Jeżeli dane będą zmieniane w minimalnym zakresie, to takie zniekształcenie będzie bardzo trudne do wykrycia. Do możliwych zagrożeń autentyczności (integralności) danych zaliczyć należy: zniekształcanie, podszywanie się, zniszczenia przypadkowe.

Zniekształcanie (modyfikacja) danych w sieciach komputerowych jest odpowiednikiem podsłuchu aktywnego w sieciach łączności. Zniekształcanie może być użyte do wykonywania określonych zmian w bazach danych. Innym celem może być zamazywanie dotychczasowych danych lub usuwanie całych plików.

Podszywanie się jest odpowiednikiem dywersyjnych działań dezinformujących w sieciach łączności. Jest to sytuacja, w której przeciwnik podszywa się pod uprawnionego użytkownika sieci i w ten sposób uzyskuje dostęp do plików i zbiorów. Odmianą takiej sytuacji jest przypadek, gdy przeciwnikowi uda się wprowadzić program stymulujący funkcje systemu, dzięki czemu przez pozyskanie haseł dostępu może uzyskać dostęp do najbardziej zastrzeżonych wiadomości.

Zniszczenia przypadkowe – dotyczą niezamierzonego zamazania lub usunięcia danych. Niezamierzone zamazywanie może być spowodowane wadliwym oprogramowaniem lub usterką sprzętu, a także pomyłką użytkownika.

W specjalistycznej literaturze informatycznej z reguły operuje się pojęciami: ochrona informacji w sieciach teleinformatycznych lub bezpieczeństwo komputerowe. Używa się również obu tych pojęć zamiennie lub jednocześnie. Pojęcie **ochrona informacji**[84] definiuje się jako zespół sił i środków, procedur i metod służących do zapewnienia bezpieczeństwa systemom teleinformatycznym i zautomatyzowanym systemom dowodzenia oraz danym w nich przetwarzanym, przechowywanym i przesyłanym. Z kolei uważa się, że **bezpieczeństwo komputerowe** nie jest zestawem sztuczek, ale rozwijającą się dziedziną wiedzy. Obejmuje ona techniki wspomagające ochronę systemów komputerowych przed ludźmi – zarówno

[84] W. Stalings, „Ochrona danych w sieci i w intersieci", wyd. WNT, Warszawa 1997.

z zewnątrz, jak i wewnątrz środowiska roboczego – których motywacje są z założenia destrukcyjne lub którzy są po prostu ignorantami[85].

Problematyka ochrony systemów teleinformatycznych związku operacyjnego przed penetracją z zewnątrz (tj. przed ich rozpoznaniem przez przeciwnika) powinna mieć swoje odzwierciedlenie również w maskowaniu zarówno – operacyjnym, jak i bezpośrednim, które z uwagi na specyfikę maskowanych obiektów należy postrzegać jako **maskowanie informatyczne.**

Maskowanie informatyczne ma na celu uniemożliwienie zdobywania oraz przetwarzania tych danych o wojskach i obiektach znajdujących się w obszarze jego odpowiedzialności obronnej związku operacyjnego , których nośnikami są sieci teleinformatyczne (rozległe i lokalne) obsługujące systemy dowodzenia, rozpoznania oraz naprowadzania uzbrojenia.

Maskowanie informatyczne w działaniach obronnych związku operacyjnego jest, zatem również **perspektywicznym rodzajem maskowania elektronicznego. Problematyka maskowania informatycznego w działaniach obronnych związku operacyjnego powinna być rozwiązywana za pomocą ukrywania, dezinformowania i pozorowania informatycznego.** W zależności od szczebla organizacyjnego udział poszczególnych składowych w całości wykonywanych przedsięwzięć powinien być różny.

Przedsięwzięcia wykonywane w ramach maskowania informatycznego celowo jest podzielić na **organizacyjne i techniczne**. Należy jednak mieć na uwadze, że powinny one być ze sobą ściśle powiązane w obszarze odpowiedzialności obronnej związku operacyjnego i uzupełniać się wzajemnie w zależności od rodzaju wykonywanych zadań, prowadzonego rozpoznania przeciwnika i możliwości w tym zakresie wojsk związku operacyjnego.

Przedsięwzięcia organizacyjne, nazywane również administracyjnymi, powinny zawierać określone procedury postępowania obowiązujące podczas „działań na informacjach", a w szczególności: regulacje prawne w zakresie ochrony kryptograficznej; zbiory przepisów dotyczących organizacji i funkcjonowania służb ochrony systemów; normy w zakresie bezpieczeństwa sieci teleinformatycznych; zbiory procedur i algorytmów postępowania w celu odtworzenia systemów po awariach i dekonspiracji.

W tym celu powinny być ustalone odpowiednie zasady dostępu, sposób korzystania z zasobów informacyjnych sieci komputerowych. *„Działanie na informacjach"* niejawnych

---

[85] S. Grafinkel, G. Spafford, „Practical Unix and Internet Security", wyd. 2, O'Reilly & Associates, Inc. Sebastopol USA, opracowanie wersji polskiej P. Kresak. „Bezpieczeństwo w Unixie i Internecie", wyd. RM, Warszawa 1997, s. 6.

powinno odbywać się w miejscach pracy do tego przystosowanych oraz zabezpieczonych przed dostępem fizycznym dla osób nieuprawnionych. Praktycznie na każdym stanowisku dowodzenia (określonego szczebla dowodzenia), gdzie dokonuje się wymiany danych niejawnych, powinny być zorganizowane miejsca pracy odpowiednio wyposażone w sprzęt komputerowy. Sprzęt ten powinien spełniać wymogi norm krajowych[86] lub wymogi amerykańskiej technologii – TEMPEST[87]. Dla takich stanowisk należy zorganizować ochronę fizyczną polegającą na:

- wyznaczeniu strefy ochronnej oraz prowadzeniu nadzoru pomieszczeń oraz sprzętu (np. za pośrednictwem: kart magnetycznych, telewizji przemysłowej, rejestracji ruchu osób w sztabach);
- ograniczeniu dostępu do informacji, przez wprowadzenie zakresu uprawnień i haseł dostępu dla poszczególnych użytkowników.

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

Spośród **przedsięwzięć technicznych** ważną rolę powinny odgrywać programowe metody ochrony[88] danych budowane na podstawie komputerowych programów ochrony i będące z zasady integralnym elementem systemu operacyjnego. Chronią one przed nieuprawnionym dostępem do całych sieci lub ich fragmentów.

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

---

[86] Norma Polska PN-92 T-20001/02 pt. „Współdziałanie systemów otwartych (OSI). Podstawowy Model Odniesienia. Architektura Zabezpieczeń".

[87] W latach osiemdziesiątych w USA opracowano system certyfikujący o nazwie TEMPEST. Jego zadaniem jest ocena podatności systemów komputerowych na monitorowanie za pośrednictwem fal radiowych. Opracowane normy są tak skutecznie chronione, że ich treść nie jest dokładnie znana poza USA [37].

[88] Programowa ochrona danych związana jest z klasą stosowanych urządzeń, a jako standard przyjęto klasyfikację opracowaną przez National Computer Security Centre (NCSC) w 1985 r. i opublikowaną w tzw. Pomarańczowej Księdze (The Orange Book) na zamówienie Ministerstwa Obrony USA. Kryteria bezpieczeństwa systemów komputerowych podzielono na 4 kategorie, od D – najniższej; C (C1, C2); B (B1, B2, B3); do A (A1) – najwyższej [48].

– szyfrowanie danych niejawnych przesyłanych w sieciach teleinformatycznych w sposób zapewniający ich integralność. Postęp technologiczny umożliwił wysokiej jakości szyfrowanie informacji u źródła i deszyfrowanie dopiero u jej ujścia w wielu nowoczesnych sieciach. Zminiaturyzowane urządzenia elektroniczne, realizujące odpowiednie algorytmy szyfrowania stanowią integralną część nowoczesnych abonenckich urządzeń łączności, a proces szyfrowania i deszyfrowania odbywa się w czasie rzeczywistym.

– wiarygodną identyfikację stacji informatycznych i użytkowników oraz sprawdzanie ich uprawnień;

– maskowanie ruchu w sieciach teleinformatycznych, co uniemożliwia identyfikację na jego podstawie ważnych stanowisk dowodzenia i obiektów;

– ochronę zasobów informacyjnych zgromadzonych w bazach danych.

Problematyka związana z szyfrowaniem, z uwagi na jej złożoność i obszerność, wykracza poza ramy pracy studyjnej.

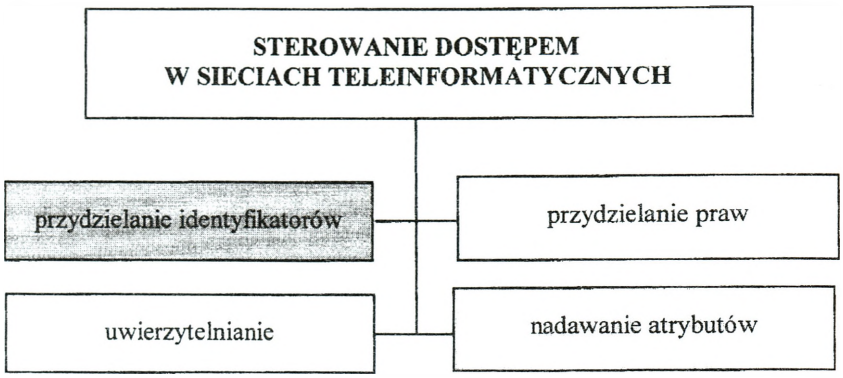
Ochrona programowa danych dotyczy również zastosowania metod i środków programowych zapewniających ich bezpieczeństwo podczas przechowywania i przetwarzania w systemach komputerowych, a także podczas ich przesyłania w sieciach teleinformatycznych. Obejmuje ona **cztery rodzaje sterowania: sterowanie szyfrowaniem; sterowanie dostępem; sterowanie przepływem danych; sterowanie wnioskowaniem.**

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

Sterowanie dostępem powinno polegać na opracowaniu odpowiednich mechanizmów zapewniających legalność dostępu 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 teleinformatycznych obejmuje czynności przedstawione na rysunku 2.17.

Użytkownikowi należy przydzielić identyfikator, dzięki któremu sieć potrafi określić jego tożsamość i przynależność do określonej jednostki organizacyjnej. Identyfikator powinien być podawany przy każdej próbie rejestracji w sieci, która identyfikuje użytkownika i jednocześnie określa zakres przysługujących mu praw.

Czynnością pozwalającą sprawdzić, czy osoba podająca identyfikator jest tą, za którą się podaje, jest uwierzytelnianie realizowane za pomocą **hasła.**



Rys. 2.17. Sterowanie dostępem w sieciach teleinformatycznych

Wpisywane hasło nie powinno być widoczne na ekranie. Jest to zabezpieczenie przed odczytem przez osoby nieupoważnione. Po podaniu hasła program zarządzający powinien przechodzić do wykonywania poleceń związanych z realizacją początku sesji. Warto podkreślić, że procedura sprawdzania poprawności hasła nie powinna odbywać się w komputerze (ze stacji dysków), lecz w serwerze. W tej sytuacji nie będzie odbywać się transmisja hasła z serwera do stacji. Nie jest zatem możliwe odczytanie go ani programowo, ani sprzętowo na zasadzie analizy danych przesyłanych z serwera. Jedynymi miejscami, w których hasło „istnieje" powinny być: serwer i pamięć użytkownika. W przyszłości uwierzytelnianie powinno odbywać się za pomocą **kart indentyfikacyjnych.** Podczas ich wprowadzania należy wykorzystać bogate doświadczenia sektora finansowego zdobyte przy użytkowaniu kart bankomatowych.

Elementem ochrony niejawności danych powinno być nadanie odpowiednich uprawnień (praw) użytkowników przez zarządcę sieci. Prawa określają, jakiego rodzaju operacje mogą być wykonywane na zbiorach (np.: prawo do czytania, zapisywania, zakładania, modyfikacji lub ich przeszukiwania).

Prawa dzielą się na dwa rodzaje:

- prawa użytkownika – przyznaje je zarządca sieci;
- prawa katalogu – określa się w nich maksymalny zakres dopuszczalnych operacji użytkowników katalogu.

Kolejnym mechanizmem ochrony niejawności informacji może być nadawanie atrybutów plikom i katalogom. Atrybuty należy przydzielać zbiorom i powinny one być jednakowe dla wszystkich użytkowników (przykładowo – plik tylko do odczytu lub systemowy nie może być kopiowany).

Sterowanie przepływem danych dotyczy praw rozchodzenia się danych, bez względu na to, jakie obiekty je zawierają. Sterowanie przepływem powinno ustalać legalne kanały dla transmisji danych. Bardzo istotną rolę odgrywa ochrona niejawności danych w sieciach komputerowych mająca na celu zabezpieczenie jej przed niesankcjonowanym dostępem i ujawnieniem. Szerokie wykorzystanie niezabezpieczonej techniki informatycznej do przetwarzania danych faktycznie prowadzi do ujawnienia danych stanowiących tajemnicę, drogą emisji ujawniającej (przewodzonej i wypromieniowanej). Niecelowe jest wówczas stosowanie metod przedstawionych powyżej, gdyż dane przesyłane mogą być ujawnione przez niebezpieczne środki informatyczne.

Emisja ujawniająca przewodzona i promieniowana jest podstawowym zagrożeniem, jakie niesie za sobą zastosowanie informatyki w procesach przesyłania danych niejawnych. Dane przechowywane w pamięci komputerów oraz przesyłane mogą ulec przypadkowemu, niezamierzonemu zniszczeniu. Może to być spowodowane niesprawnością sprzętu, zanikiem zasilania lub wpływem obcego pola magnetycznego. W urządzeniu takim jak komputer promieniują prawie wszystkie elementy (procesor, dysk twardy, stacja dysków, klawiatura, monitor). Złe obudowy, odkryte łącza krawędziowe komputerów i urządzeń peryferyjnych (np. drukarek) mogą być antenami emitującymi promieniowanie elektromagnetyczne w czasie przetwarzania danych. Promieniowanie to ma różny zasięg w zależności od zastosowanych elementów i zawiera się w granicach 50 – 1500 m. Istnieją udokumentowane przypadki[89] przechwytywania przez specjalne urządzenia (oddalone nawet o kilkadziesiąt metrów) komunikatów wyświetlanych na monitorze lub przekazywanych łączami telefonicznymi.

Przy tak dużym zasięgu emisji ujawniającej konieczne jest zastosowanie odpowiednich przedsięwzięć ochronnych w celu zmniejszenia zasięgu tego promieniowania, takich jak:

- stosowanie tylko sprzętu atestowanego o obniżonym poziomie emisji i spełniającego wymogi norm krajowych lub wykonanego w technologii TEMPEST;
- stosowanie odpowiednich osłon i kabin ekranujących (w warunkach polowych można stosować namioty z tkaniny ekranującej) oraz urządzeń identyfikujących i alarmujących;
- stosowanie utajnionych linii transmisyjnych (łączy światłowodowych);

---

[89] W trakcie międzynarodowego zjazdu hackerów (uczestniczyło ponad 2000 osób) w Almere (Holandia) prof. E. Moeller z politechniki w Aachen pokazał, jak za pomocą zwykłego telewizora, prostej anteny oraz nieco zmodyfikowanego odbiornika można bez trudu (na odległość do kilkuset metrów) odczytywać zawartość monitorów. Odczyt z monitora nie nastręcza żadnej trudności nawet wtedy, kiedy pracuje kilka komputerów obok siebie. Do odbioru wykorzystywano w trakcie pokazu 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 [37].

– odpowiednie rozmieszczanie środków informatycznych, t.j. poza strefami ich dostępności dla rozpoznania (np. w środku stanowisk dowodzenia i jego zespołów funkcjonalnych).

Sterowanie wnioskowaniem dotyczy przypadków, kiedy dane pozyskiwane ze źródeł poufnych powinny być odtajnione i udostępnione do szerszej dystrybucji. Celem sterowania wnioskowaniem powinno być uruchomienie dodatkowych mechanizmów kontroli przepływu, a tym samym zagwarantowanie, że udostępnianie przez bazę danych nie doprowadzi do ujawnienia danych poufnych.

Badania wykazały, że przedsięwzięcia techniczne maskowania informatycznego w odróżnieniu od innych rodzajów maskowania elektronicznego powinny być ukierunkowane na zastosowanie programowych metod ochrony danych. Są one na pewnych etapach procesu przetwarzania danych jedynymi metodami, które mogą zapewnić ich bezpieczeństwo przez:

a) kontrolę dostępu do sprzętu informatycznego, a w tym:
- identyfikację i nadawanie uprawnień: haseł i kart identyfikacyjnych dostępu;
- monitorowanie pracy w czasie sesji użytkownika;
- ewidencję zdarzeń w systemie;
- hierarchiczny dostęp do danych;
- zabezpieczenie indywidualne (specjalistyczne oprogramowanie),

b) ochronę danych, a w tym:
- zabezpieczenie przed modyfikacją danych;
- kontrolę zmian dokonywanych w programach;
- kontrolę transmisji danych;
- przechowywanie danych w postaci zaszyfrowanej,

c) kontrolę systemową, a w tym:
- szyfrowanie programów użytkowników;
- adresowanie logiczne programów.

2.2.2. Obrona informacyjna przed rozpoznaniem studyjnym

Powszechnie panuje przekonanie, że prowadzenie rozpoznania związane jest najczęściej tylko z działalnością elementów rozpoznawczych. Takie podejście jest wielkim uproszczeniem. 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 całość fragmentarycznych danych dostarczanych przez elementy (podsystemy) rozpoznawcze. Działalność ta ma charakter studyjny, stąd też często proces ten określany jest mianem rozpoznania studyjnego[90]. W okresie pokoju rozpoznanie studyjne odgrywa najważniejszą rolę w działalności sztabowych komórek rozpoznawczych. Płynne przejście do działań zbrojnych zależy od jakości prowadzonego rozpoznania studyjnego właśnie w okresie pokoju.

Specyfiką rozpoznania studyjnego – odróżniającą je od innych rodzajów rozpoznania – jest to, że nie zdobywa ono danych w sposób bezpośredni, a wykorzystuje informacje zdobyte przez elementy i podsystemy rozpoznawcze wojsk własnych, sąsiadów i przełożonych. Typowym efektem studyjnej działalności rozpoznawczej jest prognoza zagrożenia (przewidywane warianty działań przeciwnika) przedstawiana dowódcy i sztabowi w procesie planowania operacji. Rozpoznanie studyjne rozpatruje się jako:

- studiowanie różnorodnych danych o przeciwniku;
- wytwarzanie danych o przeciwniku (na podstawie ich studiowania) bardziej przydatnych do wykorzystania w procesie przygotowania i prowadzenia działań zbrojnych.

Rozpoznanie studyjne ma dwoisty charakter. Dwoistość ta wyraża się w tym, że rozpoznanie studyjne występuje jako proces zasilający sztab w wiadomości oraz jako ogniwo funkcjonalne (personel, osoby funkcyjne) rozpoznania danego szczebla organizacyjnego. Ważną rolę w rozpoznaniu studyjnym odgrywa dysponowanie bankami danych, które ułatwiają (ukierunkowują) proces jego prowadzenia. Od ich jakości oraz umiejętnego wykorzystania zależą w znacznej mierze rezultaty pracy sztabowych komórek oraz jednostek wydzielających elementy i podsystemy rozpoznawcze.

Z przedstawionych uwarunkowań funkcjonowania rozpoznania studyjnego wynika, że obrona informacyjna przed nim w działaniach obronnych związku operacyjnego jest niezmiernie ważnym, ale zarazem bardzo trudnym do realizacji przedsięwzięciem. Jej **celem powinno być utrudnianie gromadzenia, analizowania i przetwarzania wszelkich danych zdobywanych przez inne rodzaje rozpoznania (najczęściej fragmentarycznych) oraz przeciwdziałanie w opracowywaniu (wytwarzaniu) informacji nowych o znacznie większej wiarygodności i wartości użytecznej.** Powinna być prowadzona ciągle, niezależnie od

---

[90] Rozpoznanie studyjne to rodzaj rozpoznania wojskowego przygotowany fachowo i dostosowany technicznie do gromadzenia, analizowania i przetwarzania wszelkich informacji rozpoznawczych (najczęściej fragmentarycznych) i na tej podstawie opracowywanie informacji nowych o znacznie większej wartości użytkowej. Niezależnie od uwarunkowań sytuacyjno-czasowych ma ono charakter ciągły [59;87].

uwarunkowań sytuacyjno-czasowych, w obszarze odpowiedzialności obronnej związku operacyjnego.

Skuteczność obrony informacyjnej przed rozpoznaniem studyjnym w działaniach obronnych związku operacyjnego uwarunkowana jest skutecznością działań przeciwrozpoznawczych podejmowanych przede wszystkim w ramach maskowania. **Powinny być wykorzystywane wszystkie jego formy dostępne w działaniach obronnych związku operacyjnego , tj. pozorowanie, dezinformowanie i ukrywanie, lecz ukierunkowane na wprowadzanie w błąd organów sztabowych przeciwnika.** Szczególna uwaga powinna być zwrócona na odpowiednie oddziaływanie na proces gromadzenia danych o wojskach związku operacyjnego, który obejmuje: zbieranie, rejestrację oraz selekcję i przechowywanie. W tym celu należy wykorzystać cały arsenał środków zaprezentowany przez autora w poprzednich podrozdziałach, lecz skierowany na wprowadzenie w błąd organów sztabowych przeciwnika, zmylenie ich co do zdolności bojowej, morale i inwencji sił własnych, a w szczególności:

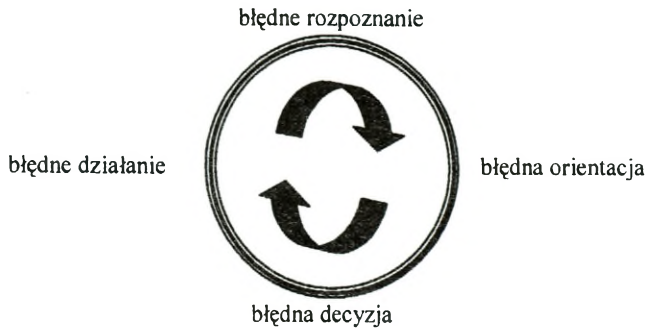
- powodowanie, aby przeciwnik podejmował działania, które w istocie będą dla niego niekorzystne;
- przeciążenie organów sztabowych (grup analizy danych) przeciwnika nadmiarem bezwartościowych danych;
- prowokowanie przeciwnika do stosowania określonych wzorców zdarzeń, które powodować będą małą skuteczność jego działań;
- powodowanie utraty mocy bojowej przeciwnika na skutek występowania opóźnień lub podejmowania niewłaściwych działań.

Aby działania takie odniosły pożądany skutek, należy spowodować stan, w którym przeciwnik:

- nie zauważy przedsięwzięć wprowadzających go w błąd (mylących);
- oceni działania mylące – po analizie – jako prawdziwe;
- podejmie działania przeciwko pozorowanym celom i sytuacjom.

Efekty tego rodzaju działania można zobrazować w postaci modelu błędnego koła, w którym (rysunek 2.18.):

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



Rys. 2.18. Model błędnego koła

Innymi słowy, działania te mają spowodować, aby organy rozpoznawcze przeciwnika niewłaściwie oceniły sytuację na polu walki, a jego dowódca podjął błędną decyzję.

W konkluzji prowadzonych rozważań można stwierdzić, że ważną rolę odgrywają ćwiczenia z udziałem obserwatorów zagranicznych organizowane w okresie pokojowym, gdzie powinny być wykorzystane aplikacyjne warianty działania związku operacyjnego.

Wnioski z takich ćwiczeń powinny budzić wątpliwość i podważać prawdziwość (lub utwierdzać w przekonaniu, jeśli są błędne) dotychczasowych opracowań organów rozpoznawczych przeciwnika[91], komunikatów, meldunków, zestawień, itp., zawierających określone zbiory odpowiednio opracowanych wiadomości rozpoznawczych.

2.3. Wnioski

Z przeprowadzonych badań wynika, że obrona informacyjna przed rozpoznaniem w działaniach obronnych związku operacyjnego jest jednym z ważniejszych elementów zabezpieczenia jego działań. Stanowi zespół skoordynowanych działań dostosowanych do ukrywania zbiorów wszelkich postaci informacji o rzeczywistym stanie, usytuowaniu i zamiarach działania wojsk związku operacyjnego, które znajdą się lub mogą być dostępne

[91] Wiadomo, że w okresie pokoju opracowywane są odpowiednie wzorce doktrynalne, natomiast w okresie działań wojennych możliwa jest ich korekta (na podstawie systematycznie powtarzających się wiadomości o stosowanych środkach walki lub rozwiązaniach taktyczno–operacyjnych) [59;66].

dla źródeł rozpoznania przeciwnika. W związku z powyższym wyróżniono ogólnie obronę informacyjną w działaniach obronnych związku operacyjnego przed rozpoznaniem bezpośrednim oraz obronę informacyjną przed rozpoznaniem pośrednim, a ponadto wykazano iż:

1. Obronę informacyjną przed rozpoznaniem bezpośrednim należy prowadzić w działaniach obronnych związku operacyjnego ciągle, różnymi sposobami i metodami. Składają się na nie odpowiednie przedsięwzięcia i działania podejmowane przez wojska związku operacyjnego w ramach ochrony kontrwywiadowczej, maskowania i ubezpieczania.

√ Ochrona kontrwywiadowcza w działaniach obronnych związku operacyjnego ma na celu śledzenie i zwalczanie wywiadu przeciwnika i powinna obejmować przedsięwzięcia pasywne i aktywne. Pasywną ochronę kontrwywiadowczą należy ukierunkować na uniemożliwienie prowadzenia obserwacji (kontrwywiadu obserwacyjnego), na odpowiednie zabezpieczenie dokumentów (kontrwywiad dokumentalny) oraz na ochronę personalną (kontrwywiad personalny). Aktywna ochrona kontrwywiadowcza powinna polegać na stosowaniu znanego od zarania dziejów arsenału metod, takich jak: podstęp, wprowadzanie w błąd, jawna (tzw. biała) propaganda, tajna (tzw. czarna) propaganda oraz wpływanie i dezinformacja.

✓ Maskowanie jest reakcją na rozpoznanie. Z uwagi na charakterystyczne cechy realizacji zadań w tym zakresie wyróżniono: ukrywanie, dezinformowanie, pozorowanie. Przedsięwzięcia ukrywania uznano za niezbędne i typowe dla realizacji zadań obrony informacyjnej przed rozpoznaniem bezpośrednim. W zależności od cech charakterystycznych ukrywanych wojsk i obiektów w obszarze odpowiedzialności obronnej związku operacyjnego (urządzeń, ludzi, sprzętu itp.) oraz rodzaju użytych środków wyróżniono: maskowanie optyczne; maskowanie akustyczne; maskowanie termiczne.

✓ Ubezpieczanie, w zależności od charakteru wykonywanych zadań w obszarze obrony związku operacyjnego obejmuje: w rejonach ześrodkowania (wyjściowym, odpoczynku) – ubezpieczenie postoju; w marszu – ubezpieczenie marszowe; w walce – ubezpieczenie bojowe. Dodatkowo w każdej sytuacji uznano za konieczne organizowanie ubezpieczenia bezpośredniego, którym należy również objąć stanowiska dowodzenia związku operacyjnego i punkty naprowadzania uzbrojenia.

2. Obrona informacyjna przed rozpoznaniem pośrednim w działaniach obronnych związku operacyjnego obejmuje: obronę przed rozpoznaniem elektronicznym oraz obronę przed rozpoznaniem studyjnym.

✓ Obronę informacyjną przed rozpoznaniem elektronicznym ukierunkowano na ograniczenie do niezbędnego minimum dostępności nadawczych środków i urządzeń elektronicz-

nych w strefach i sektorach niepożądanych, szczególnie poza obszarem odpowiedzialności obronnej związku operacyjnego oraz na zapewnienie ich bezpieczeństwa.

✓ Zapewnienie bezpieczeństwa systemom elektronicznym w działaniach obronnych związku operacyjnego stanowi główne zadanie obrony informacyjnej związku operacyjnego przed rozpoznaniem elektronicznym realizowane w ramach maskowania elektronicznego, tj.: radioelektronicznego, radiolokacyjnego, optoelektronicznego, czujnikowego i informatycznego.

✓ Maskowanie radioelektroniczne ma na celu utrudnienie lub uniemożliwienie zdobywania i przetwarzania tych danych o wojskach i obiektach związku operacyjnego znajdujących się w obszarze jego odpowiedzialności obronnej, których nośnikami są fale elektromagnetyczne wypromieniowane przez będące w ich wyposażeniu systemy radioelektroniczne. Maskowanie radioelektroniczne – ze względu na cechy charakterystyczne realizacji zadań w działaniach obronnych związku operacyjnego oraz ilość i rodzaj wykorzystywanych sił i środków – podzielono na trzy grupy szczegółowe, nazywane również formami maskowania, tj.: ukrywanie radioelektroniczne; dezinformowanie radioelektroniczne; pozorowanie radioelektroniczne.

✓ Maskowanie radiolokacyjne ma na celu uniemożliwienie zdobywania oraz przetwarzania tych danych o wojskach i obiektach związku operacyjnego znajdujących się w obszarze jego odpowiedzialności obronnej, których nośnikami są fale elektromagnetyczne wypromieniowane przez środki (stacje) radiolokacyjne przeciwnika i odbite od obiektów związku operacyjnego.

✓ Maskowanie optoelektroniczne ma na celu uniemożliwienie zdobywania oraz przetwarzania tych danych o wojskach i obiektach związku operacyjnego znajdujących się w obszarze jego odpowiedzialności obronnej, których nośnikami są fale elektromagnetyczne pasma optycznego, tj. w ultrafiolecie, w zakresie promieniowania widzialnego, a także w zakresie bliskiej, średniej, dalekiej i skrajnej podczerwieni.

✓ Maskowanie czujnikowe ma na celu uniemożliwienie zdobywania i przetwarzania danych o wojskach i obiektach związku operacyjnego znajdujących się w obszarze jego odpowiedzialności obronnej, których nośnikami są fale sprężyste oraz wszelkiego rodzaju uboczne efekty towarzyszące działaniom bojowym, na przykład: termiczne, sejsmiczne, naciskowe, magnetyczne, chemiczne, zapachu.

✓ Maskowanie informatyczne ma na celu uniemożliwienie zdobywania oraz przetwarzania tych danych o wojskach i obiektach związku operacyjnego znajdujących się w obszarze

jego odpowiedzialności obronnej, których nośnikami są sieci teleinformatyczne (rozległe i lokalne), obsługujące systemy dowodzenia, rozpoznania oraz sterowania środkami walki.

- Skuteczność obrony informacyjnej przed rozpoznaniem studyjnym uwarunkowana jest skutecznością przedsięwzięć przeciwrozpoznawczych podejmowanych przede wszystkim w ramach maskowania. Podczas realizacji tych przedsięwzięć należy wykorzystać wszystkie formy dostępne w działaniach obronnych związku operacyjnego, tj. pozorowanie, dezinformowanie i ukrywanie, lecz ukierunkowane na wprowadzanie w błąd organów sztabowych przeciwnika.

3. ZAKRES I TREŚĆ PRZEDSIĘWZIĘĆ OBRONY INFORMACYJNEJ PRZED ZAKŁÓCANIEM W DZIAŁANIACH OBRONNYCH ZWIĄZKU OPERACYJNEGO

Wnioski z minionych wojen lokalnych i konfliktów zbrojnych[1] wskazują, że w przyszłych działaniach obronnych wojska związku operacyjnego mogą wykonywać zadania w warunkach intensywnego zakłócania informacyjnego[2]. Najbardziej intensywnego oddziaływania informacyjnego należy spodziewać się w okresie poprzedzającym ewentualny konflikt zbrojny oraz w początkowym okresie wojny. Oddziaływanie to z różnym nasileniem będzie towarzyszyć, więc prowadzonym działaniom w obszarze odpowiedzialności obronnej związku operacyjnego. Rezultatem zakłócania informacyjnego może być maksymalne ograniczenie napływu wiarygodnych wiadomości i powodowanie przez to zniekształcanie obrazu pola walki w całym obszarze odpowiedzialności obronnej związku operacyjnego. Ten fałszywy obraz pola walki ma bezpośrednie przełożenie na podejmowane decyzje w obszarze działań sił osłony oraz na rozstrzygającą walkę obronną (na głównym obszarze operacji obronnej), obejmującą odparcie uderzenia przeciwnika i uniemożliwienie przełamania przez niego głównego obszaru obrony oraz wzbronienie zgrupowaniom uderzeniowym przeciwnika rozwinięcia powodzenia. W tej sytuacji zachodzić będzie potrzeba podejmowania odpowiednich środków zaradczych w postaci odpowiednio zorganizowanej obrony informacyjnej przed zakłócaniem.

Obrona informacyjna przed zakłócaniem w działaniach obronnych związku operacyjnego organizowana w warunkach postępującej elektronizacji oraz automatyzacji pola walki

---

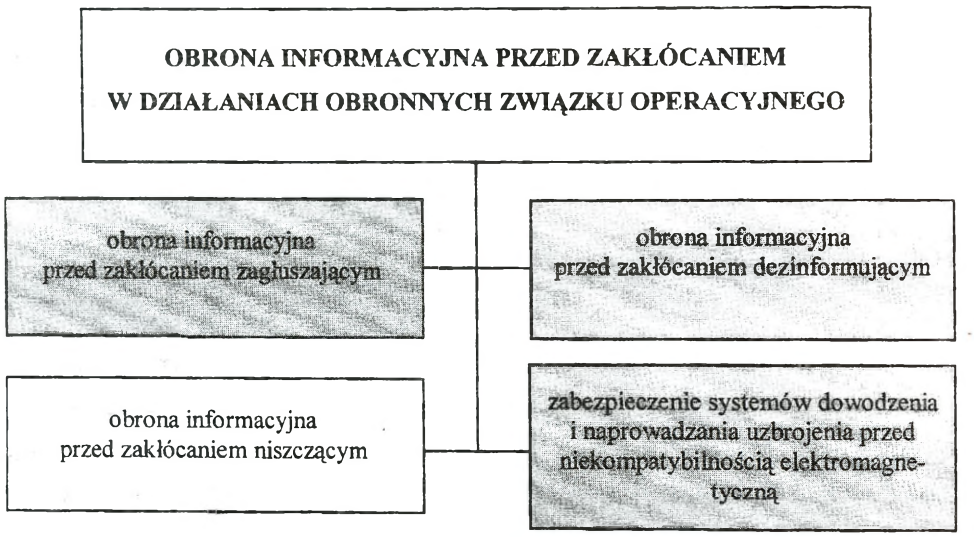
[1] Szczególnie konflikt bałkański w 1998 r., wojna w Zatoce Perskiej w 1991 r.

[2] Zakłócanie informacyjne jest elementem składowym walki informacyjnej. Jest to zespół skoordynowanych przedsięwzięć i działań, które dostosowane są do zakłócania procesów dowodzenia wojskami i sterowania środkami walki przeciwnika. Zakłócanie informacyjne przeciwdziała również rozpoznaniu. „Regulamin walki wojsk lądowych", wyd. DWLąd, Warszawa 1999, s. 62.

jest problemem wysoce złożonym. Powinna być jednym z ważniejszych elementów zabezpieczenia jego działań[3].

Ma ona **na celu zabezpieczenie przed zniszczeniem zbiorów własnych postaci danych i wnoszeniem do nich takich treści, które powodować mogą zmniejszenie wiedzy (wzrost entropii informacyjnej[4]) o stanie aktualnym, usytuowaniu i zamiarach działania wojsk oraz wprowadzać stan chaosu i nieuporządkowania w procesach dowodzenia i naprowadzania uzbrojenia związku operacyjnego.**

Analiza struktury zakłócania informacyjnego [24;25;26;62;66;97] wskazuje, że obronę przed nim w działaniach obronnych związku operacyjnego należy prowadzić różnymi sposobami i metodami. Składają się na nie odpowiednie przedsięwzięcia i działania, których ogólny podział zilustrowano na rysunku 3.1.



Rys. 3.1. Podstawowy podział obrony informacyjnej przed zakłócaniem w działaniach obronnych związku operacyjnego

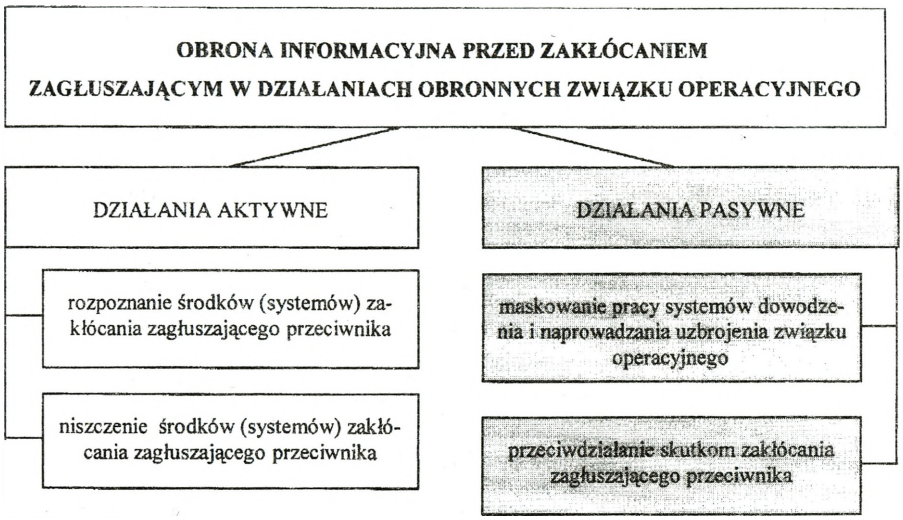
[3] Przedsięwzięcia planistyczno-organizacyjne należy podejmować również w czasie pokoju oraz podczas kryzysu i w okresach poprzedzających zagrożenie bezpośrednie.

[4] Entropia informacyjna – jest to entropia będąca miarą nieokreśloności zdarzeń stanowiących źródła danych przy określonym stanie niewiedzy o tych zjawiskach. Jest ona ściśle związana z wiadomością zawartą np. w odebranym komunikacie, gdyż za miarę uzyskanej tą drogą przez odbiorcę informacji przyjmuje się stopień zmniejszenia nieokreśloności. W odróżnieniu od entropii fizycznej, która jest całkowicie określona przez istniejący obiektywnie rozkład prawdopodobieństwa danego stanu, pojęcie entropia informacyjna uwzględnia dodatkowo nieokreśloność spowodowaną niepełną wiedzą odbiorcy o statystyce zjawisk zachodzących w źródle danych. Dlatego też entropia informacyjna, którą odbiorca przypisuje określonemu zjawisku, może być co najmniej równa entropii fizycznej tego zjawiska lub większa od niej. Tylko w przypadku, gdy odbiorca jest poinformowany o statystycznej naturze zjawiska, wartości entropii fizycznej i informacyjnej pokrywają się [25;26].

Wnioski z badań poszczególnych składowych obrony informacyjnej przed zakłóceniem w działaniach obronnych związku operacyjnego stanowią treść kolejnych podrozdziałów niniejszej pracy studyjnej.

3.1. Obrona informacyjna przed zakłócaniem zagłuszającym

Zakres i treść zagłuszania informacyjnego oraz sposoby jego prowadzenia wskazują, że obrona informacyjna przed skutkami jego oddziaływania w działaniach obronnych związku operacyjnego powinna obejmować zespół skoordynowanych działań aktywnych i pasywnych, które przedstawiono na rysunku 3.2.



Rys. 3.2. Podział obrony informacyjnej związku operacyjnego przed zakłócaniem zagłuszającym w działaniach obronnych związku operacyjnego

Rozpoznanie środków zakłócania zagłuszającego – to zadanie realizowane w ramach szeroko rozumianego rozpoznania wojskowego[5]. Umożliwia wykrycie środków zakłócania przeciwnika i rejonów dyslokacji z dokładnością umożliwiającą określenie współrzędnych wymaganych do skutecznego ich obezwładnienia zakłóceniami lub zniszczenia. Stanowi ono aktywną formę walki informacyjnej (w tym wypadku rozpoznania wojskowego), prowadzonej w ramach walki ogólnowojskowej, w której część zadań wykonuje się na rzecz obrony

[5] Problematyka ta przedstawiona jest w [25;97].

informacyjnej. Duże moce nadajników zakłóceń (800, 1000, 2000, 5000 i więcej watów) ułatwiają ich zlokalizowanie za pomocą środków rozpoznania elektronicznego oraz zidentyfikowanie rozmieszczonych w ich pobliżu bezprzewodowych środków łączności zapewniających wymianę danych w tych systemach. Środki te należy natychmiast obezwładnić zakłóceniami, a po zdobyciu niezbędnych danych do porażenia ogniowego – zniszczyć razem ze stacjami zakłóceń. Szczegółowe badania tej problematyki wykraczają poza ramy pracy studyjnej.

Niszczenie środków (systemów) zakłócania zagłuszającego przeciwnika, a przede wszystkim ośrodków dowodzenia wojskami i elementów naprowadzania uzbrojenia, grup stacji zakłóceń wraz ze środkami łączności należy traktować jako najważniejsze zadanie w zakresie ich zwalczania na polu walki. Poszczególne elementy systemów zakłócania przeciwnika stanowią samodzielne obiekty rozwinięte na niewielkich powierzchniach, co ułatwia ich zwalczanie za pomocą broni precyzyjnego rażenia, przede wszystkim pocisków naprowadzających się na źródła promieniowania energii elektromagnetycznej, oraz przez pododdziały działające w głębi ugrupowania przeciwnika (grupy specjalne, grupy rozpoznawcze, oddziały wydzielone i in.). Niszczenie stanowi zatem inną aktywną formę walki informacyjnej (zakłócanie informacyjne), prowadzoną w ramach walki ogólnowojskowej, w której część zadań wykonuje się na rzecz obrony informacyjnej.

Z analizy literatury źródłowej [15;130;131] wynika, że zorganizowany charakter prowadzenia działań obronnych związku operacyjnego oraz zapewnienie warunków wykonania zadań oparte są na efektywnym zaplanowaniu systemu rażenia wszystkich środków będących w dyspozycji jego dowódcy. Ogień poszczególnych komponentów systemu rażenia powinien być zsynchronizowany w jeden spójny system, który zapewnia maksymalną skuteczność w dowolnym czasie oraz w dowolnym obszarze działań związku operacyjnego (operacja głęboka, bezpośrednia i w obszarze tyłowym). Szczegółowe badania problematyki niszczenia przedstawione są w literaturze naukowej[6].

Maskowanie pracy systemów dowodzenia i naprowadzania uzbrojenia w działaniach obronnych związku operacyjnego – jest przedsięwzięciem mieszczącym się zarówno w obronie informacyjnej przed rozpoznaniem, jak i w obronie przed zakłócaniem. Należy pamiętać o tym, że wszechstronna realizacja zadań obrony informacyjnej przed rozpoznaniem w działaniach obronnych związku operacyjnego zapewnia również skuteczność ich maskowania, a zatem i realizację przedsięwzięć obrony informacyjnej przed zakłócaniem. Masko-

---

[6] Problematyka niszczenia w procedurze zakłócania informacyjnego jest przedstawiona w pracy badawczej pt. „Zakłócanie informacyjne w operacjach wojsk lądowych", wyd. AON, Warszawa 2001, której autor jest kierownikiem.

wanie pracy własnych systemów dowodzenia i naprowadzania uzbrojenia jest pasywną formą walki informacyjnej i ma na celu zapewnienie bezpieczeństwa tym systemom w ramach walki informacyjnej prowadzonej przez przeciwnika. Treść tego przedsięwzięcia przedstawiono w poprzednim rozdziale.

Przeciwdziałanie skutkom zakłócania zagłuszającego powinno obejmować zespół działań organizacyjnych i techniczno-eksploatacyjnych podejmowanych przez elementy ugrupowania obronnego związku operacyjnego w celu ochrony wchodzących w ich skład systemów dowodzenia i naprowadzania uzbrojenia przed celowym destrukcyjnym oddziaływaniem przeciwnika odpowiednio dobranymi sygnałami zakłócającymi. Zakres i charakter tych przedsięwzięć, tworzących w istocie obronę antyzagłuszeniową, zależy od rodzajów środków elektronicznych wykorzystywanych w tych systemach. Ze względu na rodzaj i specyfikę środków elektronicznych poddano odrębnym badaniom w aspekcie obrony antyzagłuszeniowej:

- systemy (sieci) łączności;
- systemy (sieci) teleinformatyczne;
- systemy radionawigacyjne;
- systemy naprowadzania uzbrojenia.

3.1.1. Obrona antyzagłuszeniowa systemów (sieci) łączności

Obronę antyzagłuszeniową systemów łączności[7] należy podejmować zarówno na etapie organizacji, jak i eksploatacji sieci łączności w działaniach obronnych związku operacyjnego. Powinna **stanowić odrębną grupę przedsięwzięć organizacyjnych i technicznych służących ochronie urządzeń odbiorczych bezprzewodowych środków teletransmisyjnych przed oddziaływaniem celowych, aktywnych zakłóceń radiowych[8] emitowanych przez środki walki informacyjnej przeciwnika.**

---

[7] Treść podrozdziału została opracowana na podstawie badań, które zapoczątkowało opracowanie studyjne dotyczące obrony radioelektronicznej. J. Janczak, „Obrona radioelektroniczna", wyd. WSOWŁ, Zegrze 1993.

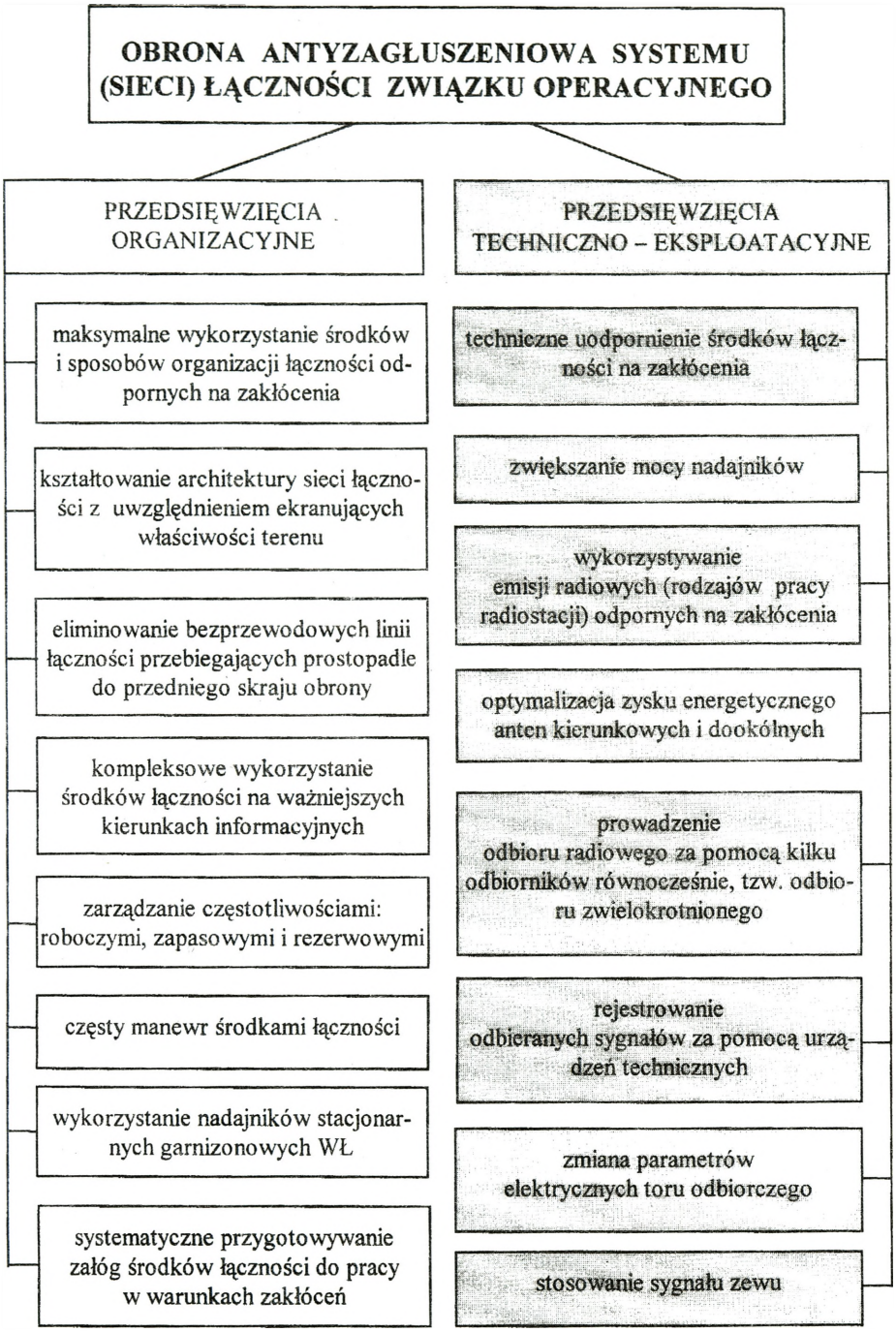
[8] Zakłócenia radiowe polegają na celowym promieniowaniu zakłócającej energii elektromagnetycznej powodującej utrudnienie pracy środków radiowych. Osiąga się je przez stosowanie nadajników emitujących aktywne sygnały zakłócające. W teorii zakłóceń radiowych wyróżnia się zakłócenia selektywne (wąskopasmowe, punktowe, kierunkowe) dużej mocy emitowane z ugrupowania bojowego potencjalnego przeciwnika, o strukturze zbliżonej do sygnałów zakłócanych (użytecznych) oraz szerokopasmowe zakłócenia dookólne małej mocy, emitowane przez nadajniki zakłóceń jednorazowego użytku umieszczane w pobliżu urządzeń zagłuszanych. Zakłócenia radiowe mogą całkowicie zdezorganizować funkcjonowanie sieci łączności radiowej. Są w stanie uniemożliwić odbiór sygnałów, pogorszyć słyszalność, spowodować nieprawidłowe działanie urządzeń końcowych, wprowadzić w błąd operatorów lub zwiększyć błędy urządzeń transmisji danych [62].

Obrona ta ma charakter pasywny, a wykonane przedsięwzięcia powinny wchodzić w zakres obowiązków organizatora systemu łączności związku operacyjnego (wydziału łączności i informatyki oddziału wsparcia dowodzenia G 6) oraz bezpośrednich użytkowników wchodzących w jego skład urządzeń łączności. Zbiór działań w tym zakresie przedstawiono na rysunku 3.3. Ważnym **przedsięwzięciem organizacyjnym** w zakresie podwyższania odporności sieci łączności związku operacyjnego na oddziaływanie radioelektroniczne przeciwnika jest wykorzystanie środków łączności kablowej (przewodowej, światłowodowej), środków wojskowej poczty polowej oraz technicznych środków sygnalizacyjnych.

Nieodzowna jest jednak modernizacja tych środków i sposobów ich wykorzystania, aby i tam gdzie jest to możliwe, zdolne były zastąpić bezprzewodowe urządzenia teletransmisyjne, które w decydujących momentach walki mogą być obezwładnione zakłóceniami.

Sposoby wykorzystania tych środków regulują odpowiednie instrukcje łączności[9] oraz przyjęte w wielu armiach państw NATO stałe procedury operacyjne [2;14;48]. Należy nadmienić, że działania obronne związku operacyjnego, głównie o charakterze pozycyjnym umożliwiają realizację tego przedsięwzięcia w pełnym wymiarze. Powinna być przygotowana więc przed rozpoczęciem tych działań trwała (dobrze zabezpieczona pod względem inżynieryjnym) sieć łączności kablowej (przewodowej lub światłowodowej). Przykładowe struktury takiej sieci przedstawione są w literaturze przedmiotu [14;78;91]. W wypadku stosowania silnych zakłóceń radiowych należy maksymalnie wykorzystywać do przekazywania wiadomości i dokumentów bojowych środki wojskowej poczty polowej. Zachodzi konieczność umiejętnego rozwiązywania problemu skrytego przemieszczania się środków wojskowej poczty polowej, zwłaszcza w rejonach przylegających do miejsc rozmieszczenia stanowisk dowodzenia. Wymagane jest również należyte zabezpieczenie poszczególnych środków poruszających się po naziemnych marszrutach przed grupami dywersyjnymi i rozpoznawczymi przeciwnika w głębi ugrupowania obronnego związku operacyjnego. W dynamicznych momentach działań obronnych związku operacyjnego należy szeroko wykorzystywać techniczne środki sygnalizacyjne, które niekiedy mogą pozostać – jak w minionych wojnach – jedynymi środkami zdolnymi do zapewnienia dowodzenia. Środki te jednak muszą być sukcesywnie udoskonalane.

[9] „Organizacja łączności na szczeblach taktycznych", wyd. MON. Warszawa 1986.



Rys. 3.3. Zakres obrony antyzagłuszeniowej systemu (sieci) łączności w działaniach obronnych związku operacyjnego

Duży wpływ na skuteczne przeciwdziałanie środkom zagłuszania zakłócającego ma architektura sieci łączności wykorzystywana w obszarze odpowiedzialności obronnej związku operacyjnego. Należy ją tak projektować [14;78;91], aby maksymalnie wykorzystać ekranujące właściwości terenu przy zachowaniu jak najmniejszych odległości między korespondentami i jak najmniejszej liczby bezprzewodowych linii łączności organizowanych w kierunku przeciwnika (pod kątem zbliżonym do 90^0 do linii styczności wojsk). Zachodzi potrzeba szerszego wykorzystania na tych kierunkach polowych linii kablowych (światłowodowych, przewodowych), a także linii stacjonarnej sieci telekomunikacyjnej państwa.

Duże znaczenie będzie tu miało umiejętne wykorzystywanie ekranów naturalnych i sztucznych[10], które w wielu wypadkach pozwalają uodpornić środki radioelektroniczne na oddziaływanie urządzeń zakłócających przeciwnika. Znając potencjalne możliwości przeciwnika, można wybrać z mapy prawdopodobne pozycje rozmieszczenia jego środków zakłóceń. Komputerowa analiza tzw. profili ścieżek PPA (ang. – Path Profile Analysis) powinna ułatwić rozwiązanie tego zadania. Należy zatem dobierać miejsca rozwijania środków łączności za ekranami do których przylega teren płaski o ubogim poszyciu. Najkorzystniejszym miejscem rozmieszczenia stanowisk dowodzenia i innych obiektów wykorzystujących środki łączności są – z tego punktu widzenia – małe miejscowości, do których przylegają pola orne z niskopiennymi uprawami czy też rozległe łąki.

Kompleksowe wykorzystanie środków łączności na ważniejszych kierunkach informacyjnych, tj. radiostacji HF, VHF, stacji radioliniowych oraz środków kablowych (światłowodowych, przewodowych) pozwala skutecznie uodpornić systemy łączności na oddziaływanie radioelektroniczne przeciwnika. Dobre efekty można uzyskać wykorzystując radiostacje pośredniczące oraz organizując okrężne linie łączności z wykorzystaniem radiostacji różnych elementów systemu dowodzenia rozmieszczonych w sąsiednich rejonach, przy jednoczesnej pracy w różnych zakresach częstotliwości (np.: HF i VHF). Ważną rolę odgrywają także nowe, nieszablonowe i tym samym trudne do wykrycia i zakłócenia sposoby organizacji łączności[11], organizowanie służbowych i skrytych relacji radiowych (radioliniowych, radiotelefonicznych) jak również szerokie wykorzystanie częstotliwości dyżurnego odbioru lub praca

[10] Przedstawione w podrozdziale 2.2.1.1.

[11] Problematyka ta szczegółowo przedstawiona jest m in. w „Organizacja łączności na szczeblach taktycznych", wyd. MON, Warszawa 1986.

radiostacji nowej generacji z automatycznym wyborem kanału[12]. W ten sposób utrudnia się przeciwnikowi rozpoznanie zaplanowanych relacji radiowych, a ponadto wydatnie zmniejsza się prawdopodobieństwo jednoczesnego ich obezwładniania zakłóceniami.

Jeśli wystąpią silne zakłócenia równocześnie w relacjach pracujących w różnych zakresach częstotliwości (HF i VHF), należy wykorzystać do przekazania wiadomości częstotliwości dyżurnego odbioru oraz rzadziej zakłócane, służbowe sieci radiowe. Gdy większość zasadniczych częstotliwości zostanie zakłócona, a realizowane różnorodne przedsięwzięcia nie poprawiają sytuacji, to wówczas wskazane jest odtwarzanie łączności w skrytych, niewykorzystywanych i nieznanych przeciwnikowi relacjach radiowych lub – jeśli jest to możliwe – wykorzystanie nadajników stacjonarnych węzłów łączności rozmieszczonych w pobliżu walczących wojsk.

Skuteczność obrony przed zagłuszaniem zakłócającym w obszarze odpowiedzialności obronnej związku operacyjnego zależy w dużym stopniu od właściwego zarządzania częstotliwościami. W nasyconym i gęstym środowisku elektromagnetycznym odpowiedni przydział częstotliwości oddanych do dyspozycji wojsk związku operacyjnego, ich związków taktycznych i oddziałów stanowi poważny problem. Proces ten powinien być dość elastyczny i odbywać się na każdym z wymienionych ogniw dowodzenia w stosunku do podległych wojsk. Czynności planistyczne powinny być wspomagane komputerowo. Bezwzględnie należy uwzględnić uwarunkowania obszaru obrony związku operacyjnego oraz jego ugrupowanie

---

[12] Sieci radiowej nie przydziela się ustalonej częstotliwości roboczej, lecz indywidualny jej numer i numer zbioru częstotliwości. Programowo zbiór taki składa się np. dla radiostacji SEM – 93 z 16 częstotliwości, które mogą być wykorzystane jednocześnie przez nie więcej niż 16 sieci. W metodzie tej wyróżnia się procesy:

– **wyszukiwania**, w którym radiostacja wyszukuje wśród różnych sygnałów swój własny, przypisany numerowi jej sieci radiowej. Po rozpoznaniu oczekiwanej cyfrowej sygnalizacji radiostacja przechodzi na odbiór;

– **nadawania**, w którym po naciśnięciu przycisku rozmownego następuje wyszukiwanie wolnego kanału w obszarze najmniejszej ich zajętości. W wyszukanym kanale radiostacja wysyła (jako wywołanie) sygnał numeru własnej sieci radiowej, który jest „rozpoznawany" przez inne radiostacje tej sieci. Po przyjęciu sygnału radiostacje przełączają się na odbiór, co oznacza gotowość do rozpoczęcia wymiany radiowej;

– **odbioru**, w którym wszyscy użytkownicy sieci radiowej znajdują się na jednej częstotliwości danego zbioru. W tym stanie pozostają wszyscy korespondenci, także podczas trwania wymiany radiowej. Dopiero po krótkim czasie od zakończenia wymiany radiowej w sieci ponownie rozpoczyna się proces wyszukiwania.

Procesy te dotyczą jednocześnie różnych sieci, w których wykorzystuje się wprawdzie ten sam zbiór częstotliwości, lecz wydzielane są do prowadzenia wymiany danych w różnych przedziałach czasowych. Radiostacje danej sieci reagują tylko na numer własnej sieci. Metoda ta umożliwia ekonomiczne wykorzystanie deficytowych częstotliwości, pozwalając na jednoczesne ich wykorzystanie przez wiele sieci radiowych. Radiostacja steruje automatycznie wszystkimi procesami w taki sposób, że użytkownik nie zauważa różnic w porównaniu z pracą radiostacji na częstotliwości ustalonej. Zwiększoną odporność na zakłócenia osiąga się metodą **„rozpraszania widma częstotliwości"**. Podczas eksploatacji radiostacji ze skokową zmianą częstotliwości FH (ang. Frequency Hopping) definiuje się każdą sieć radiową za pomocą odpowiedniego generatora kodowego, wytwarzającego jednoznaczny kryptologicznie ciąg. Oprogramowanie komputerowe grupuje będące do dyspozycji częstotliwości w taki sposób, aby nie było „kolizji" z radiostacjami innej sieci. Jest praktycznie niemożliwe, aby w różnych zbiorach powtórzyły się te same częstotliwości. Dla zwiększenia skuteczności ww. metody rozdziela się „skaczące częstotliwości" w szerokim paśmie oraz określa się krótki czas ich zajętości [4;14].

operacyjne. Jako częstotliwości robocze należy przydzielać te częstotliwości, na których zwykle występują zakłócenia przypadkowe, umożliwiające jednak dokonywanie wymiany radiowej. Przyjęcie takiego założenia w wielu przypadkach utrudni przeciwnikowi wykrycie już zakłóconych relacji łączności. Natomiast częstotliwości zapasowe powinny zapewniać jak najkorzystniejsze warunki propagacji fal radiowych. Pracę na częstotliwościach zapasowych należy rozpoczynać po wyczerpaniu wszystkich możliwości zapewnienia łączności na częstotliwościach roboczych. Wskazane jest, by podczas przechodzenia do pracy na częstotliwościach zapasowych kontynuować pracę (próbować odtwarzać łączność) na częstotliwościach roboczych. Łączność na częstotliwościach zapasowych w takich sytuacjach należy nawiązywać za pomocą innych radiostacji (na przykład odwodowych).

Wszystkie przedstawione zabiegi zmuszą przeciwnika do zaangażowania większej liczby sił i środków rozpoznania oraz zakłócania, a w konsekwencji uniemożliwią prowadzenie skoncentrowanych zakłóceń relacji łączności określonych stanowisk dowodzenia.

Odporność systemu (sieci) łączności związku operacyjnego na oddziaływanie radioelektroniczne przeciwnika podwyższa stan przygotowania załóg łączności oraz osób funkcyjnych do pracy w warunkach zakłóceń. Problem ten nie powinien być pomijany podczas szkolenia wojsk[13]. Szkolenie powinno być progresywne, realistyczne i kompleksowe. Należy prowadzić je na różnych poziomach i obejmować nim jednostki wojskowe oraz użytkowników środków łączności.

Szkolenie stanu osobowego wszystkich jednostek wojskowych podczas przygotowywania działań obronnych związku operacyjnego powinno odbywać się na zasadzie powszechności i obejmować wszystkich użytkowników środków elektronicznych. W jego toku należy przedstawić zagrożenia wynikające z możliwości taktyczno–bojowych środków walki informacyjnej, określić podatność wszystkich urządzeń radioelektronicznych na zakłócenia, włączając w to środki cywilne, urządzenia zobrazowania i środki nieradiowe oraz zaprezentować procedury postępowania na wypadek ich wystąpienia. W szkoleniu stanu osobowego powinno chodzić o to, aby każdy użytkownik środka łączności był przekonany o tym, że pomimo radioelektronicznego oddziaływania przeciwnika zawsze zachowa się szansę skutecznego realizowania wymiany radiowej.

W szkoleniu indywidualnym operatorów powinna być zwracana uwaga na zagrożenia środkami zakłóceń urządzeń przez nich obsługiwanych oraz na metody, sposoby i procedury

---

[13] Szkolenie w tym zakresie jest często lekceważone z powodu braku zainteresowania i posiadania niewystarczającej wiedzy z zakresu zagrożeń, jakie niosą współczesne środki walki informacyjnej [56].

likwidacji skutków zakłócania. Należy zwracać uwagę na właściwy sposób nadawania, prawidłowe trzymanie mikrofonu, dobrą dykcję, dwukrotne (w razie potrzeby) powtórzenia i in. Z praktyki ćwiczeń z wojskami wynika, że dobrze wyszkoleni operatorzy potrafią odbierać sygnały nadawane przez korespondentów nawet wtedy gdy zakłócenia przewyższają ich poziom. Szczególną uwagę należy zwracać na te relacje łączności, w których po przekazanej komendzie następuje natychmiastowe wykonanie zadania (np. w sieciach radiowych dowódców, sterowania ogniem artylerii, naprowadzania lotnictwa, obrony przeciwlotniczej).

Istotny wpływ na skuteczność obrony przed zakłócaniem radioelektronicznym wywiera perfekcyjna realizacja **przedsięwzięć techniczno-eksploatacyjnych**.

Najskuteczniejszym z nich jest techniczne uodpornienie środków radioelektronicznych na zakłócenia. Baza materialna sieci łączności związku operacyjnego powinna być wyposażona w środki łączności nowej generacji[14] zawierające wyspecjalizowane moduły (układy) przeciwzakłóceniowe COMSEC (ang. Communication Security). Moduły te wraz z modułami bezpieczeństwa transmisji TRANSEC (ang. Transmission Security) zapewniają standaryzację zabezpieczeń systemów w ramach NATO[15]. O odporności na zakłócanie środków łączności nowej generacji np. wykorzystujących modulacje szerokopasmowe FH decydują ich parametry charakterystyczne. Zalicza się do nich m.in.: pasmo skoków częstotliwości, liczbę i zestaw częstotliwości skaczących, szybkość zmian, system synchronizacji, kodowanie zmian częstotliwości. Odporność na zakłócenia determinowana jest w zasadzie przez pasmo skoków częstotliwości i liczbę oraz zestaw częstotliwości skaczących.

Ważnym przedsięwzięciem jest również celowe zwiększenie mocy nadajnika tej radiostacji, której sygnały są obezwładniane zakłóceniami. Nadajniki radiowe nowej generacji mają możliwość autonomicznego sterowania mocą w zależności od warunków odbioru sygnałów, tj. w zależności od potrzeb wynikających z uwarunkowań energetycznych poszczególnych linii łączności w punktach (miejscach) odbioru w obszarze obrony związku operacyjnego. W wielu nadajnikach starszej generacji przedsięwzięcie to można wykonywać ręcznie. Podwyższenie mocy nadajnika jest sprzeczne, jak wykazano w podrozdziale 2.2.1.1., z zasadami jego obrony przed rozpoznaniem radioelektronicznym. Należy jednak mieć na uwadze, że przeciwnik decyduje się na zakłócenie danej relacji radiowej wówczas, gdy zo-

---

[14] Powinny to być radiostacje, radiotelefony i stacje radioliniowe pracujące ze skokową zmianą częstotliwości w różnych postaciach i z różnymi prędkościami lub wykorzystujące widmo rozproszone, w którym sygnał jest rozczepiony w pseudolosowy sposób i ukryty w szumie. Por.: B. Bezoń, J. Janczak, „Analiza współczesnych systemów łączności w kontekście integracji SZ RP z NATO", wyd. AON, Warszawa 1999.

[15] Są to standardowe moduły stosowane w NATO, co pozwala na wymianę radiową pomiędzy partnerami Sojuszu.

stała ona w wystarczającym stopniu rozpoznana. Zatem dalsze ukrywanie jej pracy z chwilą pojawienia się zakłóceń niewiele pomoże.

W wielu środkach radiowych, emitujących energię elektromagnetyczną istnieje możliwość, oprócz podwyższenia mocy, wykorzystania rodzajów pracy, dzięki którym emitowana energia jest bardziej odporna na zakłócenia. Badania literatury źródłowej [56;118] wskazują, że odporność relacji łączności, a zatem i sieci łączności związku operacyjnego na zakłócenia radioelektroniczne można określić za pomocą współczynnika ochronnego, którego wielkość wynika z cech oddziałujących na siebie sygnałów na wejściu urządzeń odbiorczych, tj. użytecznego i zakłócającego. Niektórzy autorzy posługują się podczas oceny odporności na zakłócenia jedynie współczynnikiem zakłóceń[16] (K_z), wykorzystywanym do oceny skuteczności środków walki informacyjnej. Powinni jednak zdawać sobie sprawę z tego, że współczynnik ten stanowi minimalny stosunek natężenia pola elektrycznego zakłócającego do użytecznego, przy którym następuje pełne lub w wymaganym stopniu naruszenie pracy środka radioelektronicznego z zadanym prawdopodobieństwem [56;118]. Zatem przytaczane przez tych autorów wartości liczbowe współczynnika zakłóceń dotyczą sytuacji, w której następuje całkowite obezwładnienie zakłóceniami bezprzewodowej linii łączności. W tych warunkach odbiór nadawanych przez korespondenta sygnałów jest niemożliwy lub znacznie utrudniony, zakłócenia bowiem są silne bądź bardzo silne (tłumiące)[17].

Posługiwanie się tym współczynnikiem nie znajduje, zatem uzasadnienia, gdyż celem oceny odporności linii łączności na zakłócenia jest przecież określenie warunków, w których relacja łączności przestaje spełniać stawiane przed nią wymagania.

Do tego rodzaju ocen należy wykorzystać współczynnik ochronny emisji (p). Współczynnik ten stanowi minimalną wartość stosunku natężenia pola elektrycznego użytecznego (E_s) do zakłócającego (E_z) w miejscu odbioru, przy którym możliwe jest jeszcze prawidłowe przekazywanie wiadomości [55;56;57;118]. Można przedstawić go za pomocą zależności matematycznej:

$$p = \frac{E_s}{E_z}\left[\frac{\mu V/m}{\mu V/m}\right] \qquad (3.1.),$$

lub w mierze logarytmicznej:

---

[16] P. Gryciuk, „Doskonalenie metod oceny zagrożenia radioelektronicznego i uodpornienia systemu łączności dywizji (DZ, DPanc.) z wykorzystaniem symulacji komputerowej". Rozprawa doktorska, wyd. ASG WP, Warszawa 1987.

[17] Klasyfikacja zakłóceń radioelektronicznych przedstawiona jest w opracowaniu „Walka elektroniczna w działaniach taktycznych wojsk lądowych", wyd. AON, Warszawa 1999.

$$p = 20\log\frac{E_s}{E_z}\ [dB] \qquad (3.2.)$$

Wartość liczbowa współczynnika ochronnego p, nazywanego niekiedy współczynnikiem wymaganym zależy od rodzaju emisji radiowej wykorzystywanej w radiostacji i rodzaju emisji zakłócającej. Wykaz wartości wymaganych współczynników ochronnych (p) dla wybranych emisji radiowych zamieszczono w załączniku 12[18].

Z danych zamieszczonych w załączniku wynika, że najbardziej odporne na zakłóccnia radioelektroniczne są rodzaje pracy bezprzewodowych środków łączności oparte na emisji z manipulacją amplitudy (F1A) p = 1,5 – 2, a w dalszej kolejności:

- z manipulacją częstotliwości (F1B) p = 2,23 –3 ,98;
- z modulacją częstotliwości (F3E) p = 2,51 – 3,16;
- emisji jednowstęgowej (J3E) p = 3,98 – 5,62;
- emisji dwuwstęgowej z modulacją amplitudy (A3E) p = 5,6 – 7,08;
- emisji z modulacją częstotliwości wykorzystywanych w telefonicznych relacjach utajnionych (F3E – telefon utajniony p = 7,9);
- emisji jednowstęgowej z modulacją amplitudy wykorzystywanych w telefonicznych relacjach utajnionych (J3E – telefon utajniony p = 15,8).

Podczas oceny odporności na zakłócenia konkretnej bezprzewodowej linii łączności należy pamiętać o konieczności spełnienia wymagań energetycznych w punktach odbioru, wyrażonych za pomocą właściwego dla tej linii rzeczywistego współczynnika ochronnego (p_{rz}). Dla ustalenia rzeczywistej wartości współczynnika ochronnego należy wykorzystać zależności matematyczne [55;56;60;65;66;110;118], które określają wartość natężenia pola elektrycznego dla odpowiedniej propagacji fal radiowych[19].

Przedstawione w wyżej wymienionej literaturze przedmiotu zależności matematyczne, umożliwiają organizatorowi łączności uwzględnianie uwarunkowań energetycznych w punktach odbioru. Powodują one w wielu sytuacjach pola walki znaczne trudności w zapewnieniu ciągłej łączności w razie wystąpienia zakłóceń celowych. Dla ułatwienia procedury obliczeniowej można wykorzystać narzędzia informatyczne, np. arkusz kalkulacyjny EXCEL z pakietu MS OFFICE.

---

[18] Na podstawie – Polska Norma – PN-90 T-04500/04: „Metody pomiarów odbiorników radiofonicznych różnych rodzajów emisji". W europejskich zaleceniach: Recomendation ITU – R SM 669 – 1 (wcześniej CCiR) współczynniki ochronne podawane są dla 6 klas wierności (dla sygnałów analogowych) oraz 3 wartości elementowej stopy błędów w wypadku odbioru sygnałów cyfrowych).

[19] Rodzaje propagacji fal elektromagnetycznych wykorzystywanych w działaniach obronnych związku operacyjnego scharakteryzowano w podrozdziale 2.2.1.

Uwarunkowania matematyczne, wyniki symulacji zagrożenia radioelektronicznego sieci łączności związku operacyjnego [65] oraz analiza danych liczbowych zamieszczonych w tabeli [załącznik 3.] sugerują, iż w wielu wypadkach zmiana rodzaju pracy, a w ślad za nim i rodzaju emisji radiowej bezprzewodowego środka łączności umożliwia eliminowanie zakłóceń radioelektronicznych w stopniu zapewniającym stabilną pracę danej bezprzewodowej linii łączności, a pośrednio i całej sieci łączności.

Niezmiernie ważną rolę odgrywa również przygotowanie rezerwowych rodzajów pracy środków łączności. Powinny stanowić one w tym względzie rezerwę, uruchomianą na wypadek faktycznych działań wojennych. Istnienie i szczegóły związane z tymi rodzajami pracy środków łączności powinny być utrzymywane w ścisłej tajemnicy. Należy nadmienić, że w naszych siłach zbrojnych utrzymuje się sprzęt rezerwowy jako zapas nienaruszalny. Są to jednak środki tej samej generacji co będące w użytku bieżącym lub przestarzałe, niejednokrotnie wycofane z eksploatacji.

Kolejnym działaniem umożliwiającym poprawę odporności bezprzewodowych linii łączności jest optymalizacja zysku energetycznego anten. Optymalizacja zysku energetycznego powinna być prowadzona w taki sposób, aby w umownym łączu radiowym utworzonym przez nadajnik zakłócający przeciwnika i obezwładniany odbiornik wojsk własnych parametr ten miał jak najniższą wartość, natomiast w łączu utworzonym przez obezwładniany odbiornik wojsk własnych i nadajnik korespondenta – wartość ta powinna być nie mniejsza niż niezbędna do zapewnienia prawidłowego funkcjonowania linii łączności. Przedsięwzięcie to powinno być realizowane w sposób analogiczny do sposobu organizacji maskowania radioelektronicznego, lecz należy ukierunkować je na ochronę urządzeń odbiorczych[20].

Szczególną uwagę należy zwrócić na jak najszersze wykorzystanie anten kierunkowych oraz poziomej polaryzacji fal elektromagnetycznych. Wykorzystanie anten kierunkowych, a zwłaszcza anten adaptacyjnych[21] z elektronicznym skanowaniem wiązki energii elektromagnetycznej uodparnia bezprzewodowe linie łączności na oddziaływanie nadajników zakłócających (w tym jednorazowego użytku) rozmieszczanych w stosunku do urządzeń odbiorczych na innych kierunkach niż ten, na którym znajduje się korespondent.

Zastosowanie polaryzacji poziomej zwiększa odporność bezprzewodowych linii łączności wykorzystujących propagację fal typu ogólnego na oddziaływanie nadajników zakłócających przede wszystkim w obszarze sił osłony związku operacyjnego, gdyż składowa pozioma pola

---

[20] Problematyka ta została przedstawiona w podrozdziale 2.2.1.1.
[21] Są to anteny nowej generacji [56;71].

elektromagnetycznego jest silniej tłumiona przez grunt niż składowa pionowa, a zatem przy takim samym oddaleniu i tej samej mocy nadajnika zakłócającego poziom sygnału zakłóceń na wejściu obezwładnianego odbiornika jest mniejszy w wypadku wykorzystania polaryzacji poziomej [66]. Wykorzystanie polaryzacji poziomej fal elektromagnetycznych wpływa również na uodpornienie bezprzewodowych linii łączności na oddziaływanie nadajników zakłóceń jednorazowego użytku, wyposażonych głównie w anteny prętowe, pracujące z polaryzacją pionową. Należy nadmienić, że działania obronne związku operacyjnego, szczególnie o charakterze pozycyjnym umożliwiają realizację tego przedsięwzięcia w szerokim zakresie.

Odporność bezprzewodowych linii łączności na zakłócenia można podwyższyć również przez obniżenie wysokości zawieszenia anteny odbiorczej przy jednoczesnym zwiększeniu wysokości zawieszenia anteny nadawczej radiostacji korespondenta. Pogorszeniu ulegają wówczas warunki propagacji fal elektromagnetycznych w umownym łączu radiowym tworzonym przez nadajnik zakłócający i obezwładniany odbiornik, tym samym zmniejsza się poziom sygnału zakłóceń na wejściu odbiornika, a poziom sygnału użytecznego praktycznie nie powinien się zmienić.

W niektórych sytuacjach istnieją możliwości dokonywania zmian ukierunkowania anteny. Antena prętowa ustawiona pionowo odbiera sygnały emitowane ze wszystkich kierunków jednakowo. Każda zmiana kąta nachylenia anteny powoduje taką zmianę jej charakterystyki, że z jednego kierunku będzie odbierać sygnały dobrze, a z innych słabo lub wcale. Zmieniając kąt nachylenia anteny w kierunku korespondenta, można znaleźć takie jej położenie, w którym sygnały użyteczne będą odbierane względnie dobrze, natomiast zakłócające bardzo słabo.

Innym sposobem przeciwdziałania środkom zakłócania radioelektronicznego przeciwnika może być prowadzenie wymiany radiowej za pomocą kilku radiostacji (odbiorników radiowych) równocześnie, tzw. zwielokrotnionego odbioru. Realizacja tego przedsięwzięcia wymaga jednego nadajnika i co najmniej dwóch, w miarę możliwości jak najbardziej oddalonych od siebie odbiorników. Zwielokrotniony odbiór powinien być stosowany wówczas, gdy istnieją możliwości rozmieszczenia odbiorników w odległości nie mniejszej niż zasięg skutecznego oddziaływania nadajników zakłóceń przeciwnika na daną bezprzewodową linię łączności. Zwielokrotniony odbiór powinien być stosowany na wyższych szczeblach dowodzenia oraz tam, gdzie istnieje możliwość wykorzystania połączonych liniami kablowymi odbiorników, oddalonych od siebie o kilka kilometrów [55;56].

Podczas występowania słabych i silnych zakłóceń w relacjach radiowych celowe jest prowadzenie wymiany korespondencji z równoczesnym rejestrowaniem odbieranych sygnałów za pomocą technicznych urządzeń końcowych. Pozwala to na wielokrotne ich przesłuchiwanie, co w wielu wypadkach umożliwia prawidłową interpretację sygnałów nie rozszyfrowanych podczas odbioru bezpośredniego.

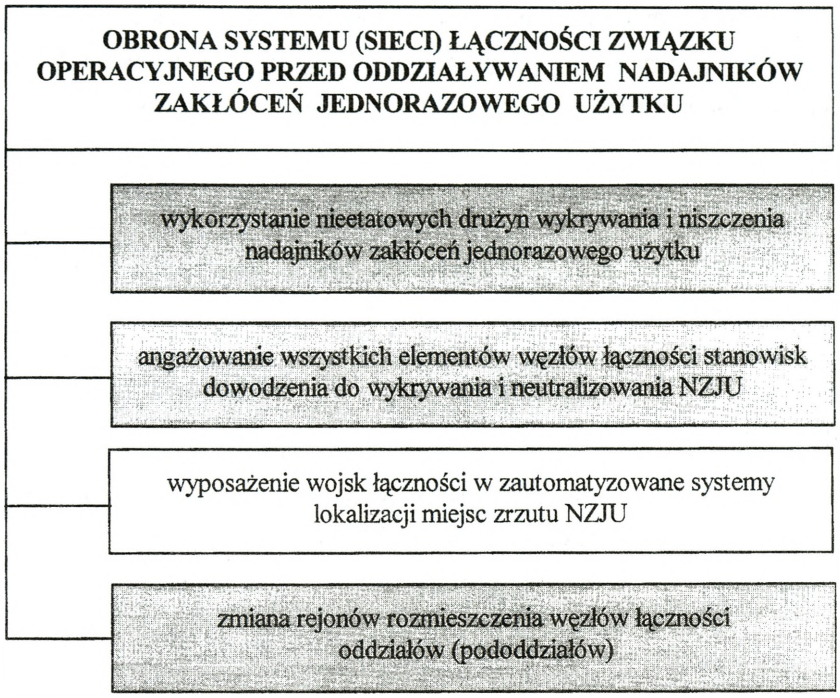
Skuteczność zakłóceń radiowych można również obniżyć przez zmianę parametrów elektrycznych toru odbiorczego radiostacji. W przypadku stosowania przez przeciwnika zakłóceń zaporowych celowe jest zawężenie pasma przepuszczania odbiornika, z kolei przy zakłóceniach selektywnych poprawę warunków odbioru można uzyskać przez nieznaczne odstrojenie odbiornika od częstotliwości roboczej. Należy mieć na uwadze również to, że oddziaływanie zakłóceń zależy od częstotliwości roboczej. Im wyższa częstotliwość robocza, tym mniejsza jest skuteczność zakłóceń [66]. Zależność ta występuje jednak wyłącznie przy suchej i słonecznej pogodzie. Przy pogodzie pochmurnej, mżawkach i opadach deszczu lub śniegu mniej przydatne na zakłócenia są niższe częstotliwości. Przy pogodzie mglistej, a zwłaszcza we wczesnych godzinach popołudniowych, występują dodatkowe wahania sygnału, których nie można w żaden sposób ograniczyć.

Jeżeli radiostacje wyposażone są w urządzenia zewowe, to istnieje możliwość wykorzystania sygnału zewu do przekazywania niektórych umówionych sygnałów. Ponieważ sygnał zewu może przytłumić sygnały zakłócające, możliwe jest przekazywanie umówionego sygnału za jego pomocą. Niezbędne przy tym jest, aby w dokumentach łączności wyraźnie określić zasady posługiwania się sygnałem zewu. Np.: dwukrotny sygnał zewu może oznaczać: "tak, potwierdzam"; czterokrotny: „nie, nie odebrałem".

Szczególnie trudnym zadaniem, wymagającym rozwiązań zarówno organizacyjnych, jak i technicznych jest **walka z nadajnikami zakłóceń jednorazowego użytku (NZJU).** Załogi łączności powinny umieć je wykrywać, niszczyć lub neutralizować, bądź też wychodzić poza strefy ich skutecznego oddziaływania. Możliwy wykaz działań w tym zakresie przedstawiono na rysunku 3.4.

Jednym ze sposobów przeciwdziałania NZJU powinno być organizowanie na węzłach łączności stanowisk dowodzenia nieetatowych zespołów (drużyn) wykrywania i niszczenia NZJU. Biorąc jednak pod uwagę czas pracy tych nadajników (średnio od kilkunastu do kilkudziesięciu minut) oraz prawdopodobny sposób ich użycia (umieszczanie w rejonie obezwładnianego obiektu kilkunastu do kilkudziesięciu nadajników zakłócających w taki sposób, aby nowo umieszczane nadajniki rozpoczynały pracę wcześniej niż zakończą ją znajdujące się już w tym rejonie), możliwość ich wcześniejszego zaminowania, a także stosunkowo długi czas

i sposób wykonania zadania przez nieetatową drużynę, należy sądzić, że przedstawiony sposób obrony może być wykorzystany na węzłach łączności rozmieszczanych w głównym obszarze działań związku operacyjnego.



Rys. 3.4. Zakres obrony systemu (sieci) łączności związku operacyjnego przed oddziaływaniem nadajników zakłóceń jednorazowego użytku (NZJU)

Natomiast o obszarze działań sił osłony może okazać się nieskuteczny. Poza tym należy zakładać, że w składzie takiej drużyny powinni być również saperzy, którymi jednostki dowodzenia związku operacyjnego nie dysponują.

Bardziej skutecznym sposobem może okazać się zaangażowanie wszystkich elementów węzłów łączności do wykrywania i neutralizowania NZJU. Neutralizowanie polega na ich ekranowaniu za pomocą np. lekkich metalizowanych siatek, cienkich arkuszy folii aluminiowej lub odpowiednio wysokich prętów metalowych wbitych w ziemię wokół poszczególnych nadajników. Spowoduje to natychmiastowe skuteczne ograniczenie rozprzestrzeniania się energii elektromagnetycznej emitowanej przez NZJU. Czynność ta jest mniej czasochłonna niż niszczenie, gdyż nie wymaga angażowania wyspecjalizowanych sił i środków.

Najskuteczniejszym sposobem, umożliwiającym natychmiastowe i precyzyjne lokalizowanie nowo pojawiających się źródeł energii elektromagnetycznej w rejonie węzłów łączności i przyległym terenie jest wyposażenie wojsk łączności w zautomatyzowane systemy pelengacyjne. Systemy te powinny mieć możliwość odróżniania sygnałów pochodzących z NZJU od sygnałów emitowanych przez nadajniki własnych korespondentów.

Z kolei zmiane rejonów rozmieszczenia węzłów łaczności należy przewidywać przede wszystkim w obszarze działania sił osłony z chwilą pojawienia się zakłóceń emitowanych przez NZJU.

3.1.2. Obrona antyzagłuszeniowa systemów (sieci) teleinformatycznych

Z analizy literatury przedmiotu badań wynika, że obrona antyzagłuszeniowa systemów (sieci) teleinformatycznych stanowi perspektywiczne przedsięwzięcie w działaniach obronnych związku operacyjnego w zakresie przeciwdziałania skutkom zakłócania informacyjnego przeciwnika. Obiektami oddziaływania zagłuszającego mogą być rozległe i lokalne sieci teleinformatyczne[22] związku operacyjnego, a przede wszystkim wchodzące w ich skład komputery wraz z oprogramowaniem oraz zbiory danych w nich gromadzone i przetwarzane. W odróżnieniu od innych systemów, oddziaływanie na środki informatyczne jest osiągalne prawie dla każdego[23].

Oddziaływanie to może być realizowane przy wykorzystaniu różnorodnych „programów złośliwych", które powodują wymazywanie w krótkim czasie dużej liczby zbiorów danych, spowalnianie pracy programów użytkowych i in. Programem złośliwym są specjalne kody wyrządzające szkody w urządzeniach i sieciach informatycznych. Niektórzy specjaliści [37;48] posługują się również określeniem *malware* (zlepek słów pochodzących z języka angielskiego Malicious Software – oprogramowanie złośliwe). Potocznie określane są również jako wirusy komputerowe CVW (ang. Computer Virus Weapon).

Jak wskazują doświadczenia, niektóre wirusy podejmują działania natychmiast po wprowadzeniu do systemu, a niektóre wprowadzone są w postaci odpowiednio zaszyfrowanej

---

[22] Por.: podrozdział 2.2.1.5.

[23] W odróżnieniu od konfliktu nuklearnego przyszłą wojnę może prowadzić każdy „uzdolniony komputerowiec". Używając terminologii anglojęzycznej, można działania takie określić jako „hackerwar" i „cyberwar". Hackerwar mają najczęściej wymiar lokalnych akcji dezinformujących w sieciach komputerowych. Cyberwar jest o wiele groźniejsze, gdyż są to przede wszystkim zorganizowane działania – tzw. „cyberataki" prowadzone w określonym celu przeciwko konkretnym osobom, organizacjom, siłom zbrojnym, m.in. w ramach walki informacyjnej [18;30;57;114;124].

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

Koncepcja zastosowania *„wirusów"* wprowadzanych do systemów komputerowych przeciwnika w celu zakłócenia pracy systemów dowodzenia i naprowadzania uzbrojenia na szeroką skalę została sprawdzona w czasie wojny w rejonie Zatoki Perskiej w 1991 r., a przykłady ich użycia opisywane były nawet w prasie codziennej.

Z badań wynika, że obrona antyzagłuszeniowa systemów (sieci) teleinformatycznych w działaniach obronnych związku operacyjnego powinna mieć **na celu ochronę zautomatyzowanych miejsc pracy na stanowiskach dowodzenia wojskami i punktach naprowadzania uzbrojenia, a przede wszystkim komputerów oraz zbiorów danych w nich zgromadzonych i przetwarzanych przed ich modyfikowaniem czy zniszczeniem.** Obronę tę należy ściśle zsynchronizować z maskowaniem informatycznym[24], która w razie potrzeby powinna stanowić jego uzupełnienie.

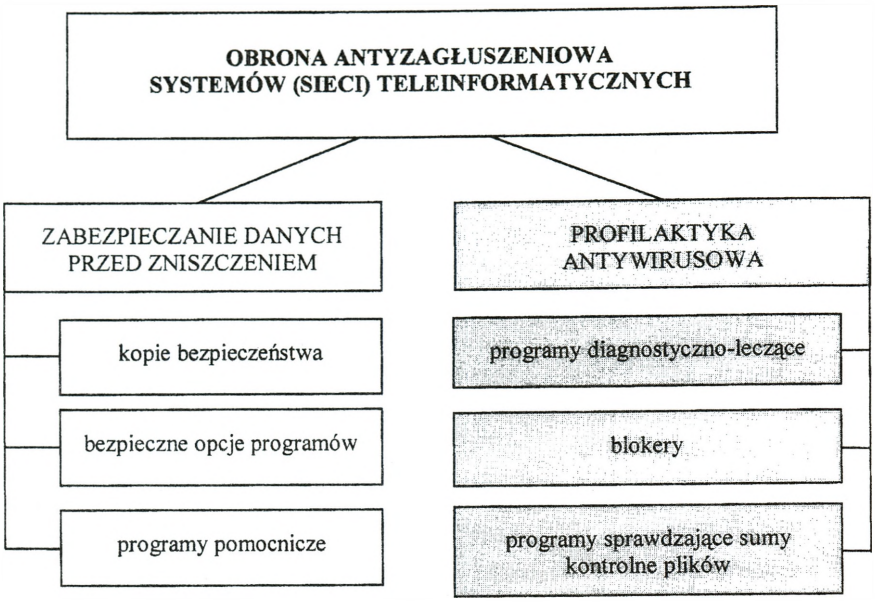
Z powyższego wynika, że obrona antyzagłuszeniowa systemów (sieci) teleinformatycznych związku operacyjnego obejmuje odpowiednie przedsięwzięcia organizacyjno- techniczne zilustrowane na rysunku 3.5., które powinny być ze sobą ściśle powiązane w działaniach obronnych związku operacyjnego i uzupełniać się w zależności od wykonywanych zadań oraz zagrożeń wynikających z oddziaływania środkami zakłócania informacyjnego przeciwnika.

Kopie bezpieczeństwa są podstawowym warunkiem pozwalającym zachować pewien margines bezpieczeństwa podczas pracy z komputerem. Bezwzględnie należy kopiować zbiory przed wykonaniem operacji takich, jak: przeformatowanie, konwersja do innego formatu czy też testowanie zmodyfikowanego programu.

Bezpieczne opcje posiada większość programów użytkowych. Mają one pewne mechanizmy ochrony danych, na których operuje użytkownik. Część funkcjonuje automatycznie, część zaś dostępna jest po wybraniu odpowiednich opcji programu (przykładowo – żądanie potwierdzenia skasowania plików, okresowe składowanie danych na dysku, składowanie danych na dysku przed wykonaniem operacji przedstawionych powyżej).

---

[24] Wyniki badań w zakresie maskowania informatycznego zamieszczone zostały w podrozdziale 2.2.1.5.



Rys. 3.5. Obrona antyzagłuszeniowa systemów (sieci) teleinformatycznych w działaniach obronnych związku operacyjnego

Z powyższego wynika, że osoby funkcyjne stanowisk dowodzenia związku operacyjnego, mając do dyspozycji zautomatyzowane miejsca pracy powinny w jak najszerszym zakresie wykorzystywać bezpieczne opcje ich oprogramowania oraz serwery bazowe, które umożliwiają bieżąca archiwizację danych, a zarazem stanowią tzw. gorącą rezerwę.

Istnieje również cała gama programów pomocniczych, które pozwalają osobom funkcyjnym zautomatyzowanych miejsc pracy stanowisk dowodzenia na zabezpieczenie przed utratą danych, na których wykonywane są operacje. Są to zwykle programy chroniące przed:

- skasowaniem poprzedniego zbioru przez zapamiętanie go na pewien czas w poprzednim (starym) miejscu;
- przypadkowym sformatowaniem dysku lub dyskietki przez zapamiętanie pewnych informacji o dysku i specjalne formatowanie.

Mogą to być programy rezydentne, zmieniające sposób działania pewnych nieplanowanych operacji (np. zamieniające operacje kasowania na przenoszenie do specjalnego katalogu – z którego można odtworzyć dane). Zasada działania tych programów może opierać się także na zmianie pewnych nieodwracalnych operacji na łagodniejsze, których skutki są możliwe do usunięcia (np. programy formatujące dysk w odwracalny sposób).

Niezmiernie ważnym przedsięwzięciem w obronie antyzagłuszeniowej systemów (sieci) teleinformatycznych jest profilaktyka antywirusowa. Wirus jest programem złośliwym celowo napisanym przez człowieka. Jego głównym zadaniem jest powielanie własnego kodu i umieszczanie go w określonych miejscach na dysku lub w programach. Dodatkową czynnością większości wirusów jest także realizowanie określonego zadania, począwszy od pokazów (takich jak generowanie komunikatów i dźwięków) poprzez fałszowanie i niszczenie plików, aż do fizycznego zniszczenia sprzętu. Jak wskazują doświadczenia, należy liczyć się następującymi programami złośliwymi: „koń trojański"[25], „bomba logiczna[26]", „mikroby" (robaki komputerowe)[27], „bakterie" (króliki)[28] oraz wiele im podobnych, które mogą się pojawić przy przesyłaniu danych w postaci jawnej, przede wszystkim w sieciach lokalnych (LAN).

Jak wynika z analizy literatury przedmiotu badań [24;30;37;48;97;119], profilaktyka antywirusowa powinna polegać przede wszystkim na niedopuszczaniu do uruchomiania oprogramowania systemowego z dyskietek nieznanego pochodzenia. Podczas uruchamiania komputera należy pamiętać o tym, aby w stacjach dysków nie było żadnych dyskietek, na których mogą rezydować wirusy. Innym rozwiązaniem może być odpowiednia konfiguracja startowa komputera, wyposażona w funkcję, która umożliwia wybranie pierwszego dysku, z którego ma się uruchamiać system. Dzięki tej funkcji nawet pozostawiona w stacji przenośnej dyskietka z wirusem przestaje być groźna.

---

[25] Koń trojański otrzymał swoją nazwę ze względu na analogię ze znanym mitem greckim. Jest on podprogramem, który (wmontowany np. w oryginalne programy użytkowe, np. gry, arkusze kalkulacyjne czy edytory) może na określony sygnał lub komendę wymazywać dane z dysków. Użytkownik może na przykład sądzić, 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 [24;30;37;97].

[26] Bomba logiczna jest zazwyczaj „podkładana" w programach przez informatyków, którzy mają legalny dostęp do systemu. Impulsem wyzwalającym „wybuch bomby" może być obecność odpowiednich plików, określona data, czy jakiś użytkownik uruchamiający aplikację. Uruchomiona 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 zakupionego oprogramowania z chwilą utraty ważności licencji użytkownika [24;30;37;97].

[27] 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. Same robaki nie zmieniają programów, ale mogą przenosić złośliwy kod, który to robi. Ich podstawowym zadaniem jest wypełnianie pamięci komputerów taką ilością przypadkowo generowanych danych, że prowadzi to do istotnego spowolnienia pracy sieci lub wręcz jej zablokowania [24;30;37;97].

[28] Bakterie, zwane również królikami to programy, które nie uszkadzają plików wprost. Ich jedynym zadaniem jest rozmnażanie. Typowy program - bakteria lub program - królik może nie robić nic innego jak dzielić się na dwie kopie i uruchamiać je w środowisku zasobów. Może też tworzyć dwa nowe pliki, z których każdy jest kopią programu wyjściowego. Oba nowe programy będą się następnie dalej mnożyły, tworząc kolejne „potomstwo". Bakterie reprodukują się wykładniczo i zajmują ogromną ilość czasu procesora, pamięci, przestrzeni dyskowej i innych zasobów, przez co użytkownik nie może z nich dalej korzystać [24;30;37;97].

Najlepszą metodą unikania konia trojańskiego jest nieuruchamianie żadnego programu, dopóki nie przeczyta się dokładnie całego pliku. Do czytania pliku należy stosować program czy edytor, który wyświetla kody sterujące w sposób widoczny. Nie należy również uruchamiać programu, którego czytanie nie wyjaśnia pojawiających się wątpliwości.

Ochrona przed złośliwymi bombami logicznymi polega na nieinstalowaniu oprogramowania bez wcześniejszego dokładnego przetestowania i przeanalizowania kodu źródłowego. Należy przeprowadzać regularne archiwizacje, aby w razie wystąpienia problemów można było powrócić do stanu sprzed awarii.

Metodą obrony przed mikrobami (robakami) jest regularne sprawdzanie integralności ważnych plików, nowego oprogramowania, zwłaszcza z nieznanych lub słabo znanych źródeł. Innymi słowy, jeśli komputer jest zabezpieczony przed nieautoryzowanym dostępem, powinien być odporny na każdego robaka. Jeśli robak znajduje się już w systemie, zerwanie połączeń sieciowych może nie dopuścić do jego dalszego rozprzestrzeniania oraz przesyłania prywatnych danych na zewnątrz sieci lokalnej.

Ochrona przed bakteriami (królikami) polega na zachowaniu ostrożności w stosunku do importowanych programów w postaci kodów źródłowych, jak i w postaci skompilowanej.

Z badań wynika, że nie istnieje żaden kompleksowy sposób ochrony przed wirusami. Spowodowane jest to tym, że wirusy jako zjawisko rozwijają się bardzo szybko. Powstające oprogramowanie antywirusowe jest zawsze krok do tyłu. Oprócz tego różnorodność wirusów jest tak wielka, że jakakolwiek ogólna metoda antywirusowa nie może być w pełni skuteczna. Tylko od stosowanych przez użytkowników środków ostrożności zależy, jakie będą skutki zetknięcia się z wirusem. Chcąc zminimalizować ryzyko „zainfekowania" komputera wirusem, a tym samym zmniejszyć skutki jego działania, należy:

- używać oprogramowania dostarczonego przez zarządcę sieci, gdyż minimalizuje ono prawdopodobieństwo wykorzystania programów zawierających wirusy;
- tworzyć i pieczołowicie chronić kopie zapasowe, gdyż umożliwiają one odzyskanie danych po zniszczeniu oprogramowania przez wirusy;
- stosować odpowiednie oprogramowania antywirusowe, gdyż sygnalizuje ono obecność znanych wirusów, a także możliwość usunięcia skutków ich działania;
- sprawdzać dyskietki pochodzące od innych użytkowników sieci, a także te, do których miały dostęp inne osoby;

– mieć dyskietki systemowe, ponieważ wirusy z zainfekowanego komputera można usunąć uruchamiając system z nie zawirusowanej dyskietki i zastępując zainfekowany sektor startowy sektorem czystym.

Badania opinii informatyków wyrażane w praktyce oraz na łamach pism informatycznych sugerują, że najsilniejszym narzędziem, jakie powstało do walki z wirusami są właśnie odpowiednie programy antywirusowe wyszczególnione na rysunku 3.5.

Programy diagnostyczno – leczące stanowią grupę programów wykorzystywanych do poszukiwania na dysku i w pamięci znanych już wirusów i w razie wykrycia zmian umożliwiają usuwanie skutków ich działania. Programy te są najczęściej stosowane w praktyce, niestety są nieskuteczne w wypadku zainfekowania systemu wirusami nieznanymi. Należy przewidywać, że właśnie takie wirusy potencjalny przeciwnik będzie wykorzystywał w pierwszej kolejności wobec systemów (sieci) informatycznych w działaniach obronnych związku operacyjnego.

Jedynymi programami próbującymi przeciwstawić się „infekcji" wirusowej są blokery. Zasadą ich działania jest monitorowanie poczynań uruchamianych programów i w przypadku odkrycia „podejrzanych" operacji alarmowanie użytkownika. Jest to znakomita metoda, ale niestety nowo powstające wirusy są wyposażone w mechanizmy uniemożliwiające wyodrębnienie z nich operacji „podejrzanych". Poważną wadą blokerów jest także zwalnianie działania komputera i zajmowanie pamięci operacyjnej.

Istotą działania programów sprawdzających sumy kontrolne plików jest zakładanie bazy danych, zawierającej pewne cechy zbiorów dyskowych i „newralgicznych" obszarów dysku. Te programy, przy systematycznym stosowaniu, umożliwiają wykrycie źródła infekcji wirusowej, a czasami odzyskanie bezpowrotnie części utraconych plików.

3.1.3. Obrona antyzagłuszeniowa systemów radionawigacyjnych

Rozwój nowych technologii oraz taktyki działania sił zbrojnych spowodował konieczność poszukiwania dokładniejszych sposobów nawigowania oraz przesyłania danych na jego potrzeby. Wśród różnorodnych systemów pozwalających człowiekowi lub komputerowi określić położenie na powierzchni Ziemi czy też w przestrzeni kosmicznej są współczesne

satelitarne systemy radionawigacyjne[29]. Obecnie państwa sojusznicze NATO wprowadzają do wojsk i wykorzystują w ostatnich konfliktach lokalnych[30] system GPS NAVSTAR jako jednolity system nawigacyjny dla wszystkich rodzajów sił zbrojnych. Obserwuje się jednocześnie znaczne zmniejszenie zainteresowania dotychczas wykorzystywanymi systemami radionawigacyjnymi typu TACAN[31], OMEGA[32] i LORAN–C[33], dającymi dużo mniejszą dokładność określania położenia i mającymi często jedynie zasięg lokalny.

Wobec coraz szerszego wykorzystania systemu GPS NAVSTAR również w siłach zbrojnych RP oraz planowanego wprowadzenia tego systemu do związku operacyjnego[34] problem określenia jego podatności na zakłócenia oraz organizacji obrony antyzagłuszeniowej nabiera ważnego znaczenia.

Badania wykazały, że spośród trzech segmentów systemu GPS NAVSTAR (kosmicznego[35], kontrolnego[36] i użytkowego[37]) najbardziej podatny na zakłócenia jest segment użytkowy. Zakłócenia te mogą powstawać w sposób niezamierzony[38] (przypadkowy) w wyniku

---

[29]GPS NAVSTAR (ang. Global Positioning System Navigation Satellite Providing Time and Range) – amerykański globalny system wyznaczania pozycji; GLONASS (ros. Глобальная Навигационная Сателлитная Система) – rosyjski globalny system nawigacji satelitarnej; GNSS (ang. Global Navigation Satellite System) – globalny system nawigacji satelitarnej. Zsynchronizowany system GPS i GLONASS. Przewiduje się, że w przyszłości GNSS stanie się jedynym globalnym systemem nawigacyjnym na świecie, który będzie wykorzystywany do nawigacji obszarowej przede wszystkim na potrzeby lotnictwa cywilnego [16;61].

[30] Np. wojna w rejonie Zatoki Perskiej w 1991 r. [18;124].

[31] TACAN (ang. Tactical Air Navigation) – system nawigacji taktycznej. Jest połączeniem radiolatarni 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 [16;61].

[32] 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 [16;61].

[33] LORAN – C (ang. Long Range Navigation) – system nawigacyjny dalekiego zasięgu, pracujący w zakresie fal długich: λ = 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 [16;61].

[34] Badania w zakresie możliwości wykorzystania systemu w wojskach lądowych RP przedstawiono w pracy naukowo-badawczej p.k. „GPS-1", której autor pracy studyjnej był kierownikiem, wyd. AON, Warszawa 1999.

[35] Segment kosmiczny obejmuje 24 satelity (w tym i 6 zapasowych) poruszających się po 6 różnych orbitach nachylonych do płaszczyzny równika pod kątem 55^0 i okrążających Ziemię w czasie 12 godzin w odległości 20200 km od jej powierzchni [16;61].

[36] Segment kontrolny 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 [16;61].

[37] Segment użytkowy 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 [16;61].

[38] 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. [16;61].

niekompatybilności elektromagnetycznej[39] różnych urządzeń radioelektronicznych lub też mogą to być zamierzone (celowe) sygnały zakłócające emitowane przez elementy walki informacyjnej przeciwnika[40].

Zakłócenia niezamierzone (przede wszystkim typu technicznego): harmoniczne, listki boczne, efekty intermodulacji wzajemnej oraz te, których nie udaje się ustalić przy pomocy tradycyjnych metod kontroli częstotliwości. Są one groźne dla systemu GPS NAVSTAR z tego powodu, że nawet nadajniki małych mocy mogą zakłócić odbiorniki GPS w promieniu do 10 km. Przegląd opinii użytkowników systemu [16;61] sugeruje, że system GPS NAVSTAR jest podatny na zakłócenia emitowane nawet przez przenośne nadajniki zakłóceń (dostępne na rynku lub montowane przez amatorów). Podatność odbiorników systemu GPS NAVSTAR na zakłócenia emitowane przypadkowo przez podręczne nadajniki jest sprawą ewidentną, co wpływa niekorzystnie na działania operacyjne w oddalonych obszarach (rejonach). Pracę tych odbiorników mogą zakłócać na przykład telefony komórkowe. Wykorzystują one sygnały radiowe do synchronizacji w pracy multipleksowej, powodując zakłócenia w torze odbiorczym systemu nawigacji. Jak się okazuje, telefon komórkowy może zakłócić sygnał GPS, a nie odwrotnie.

Dla ochrony odbiorników GPS przed zakłóceniami firmy produkujące je proponują dodatkowe zabezpieczenia techniczne. Na przykład firma ERI[41] wyposaża odbiornik GPS w moduł eliminujący zakłócenia ISU (ang. Interference Suppresion Unit).

Składa się on z urządzenia elektronicznego i anteny. Przeprowadzone testy – zarówno przy zakłócaniu wąskopasmowym, jak i szerokopasmowym – wykazały wysoką skuteczność urządzenia przy stosowaniu kodu odbiornika, wykorzystywanego do dokładnego serwisu pozycyjnego PPS[42] (dla użytkowników uprawnionych) oraz do standardowego serwisu pozycyjnego (SPS)[43]. Moduł elektroniczny, który może być rozmieszczony w pewnej odległości od odbiornika systemu GPS NAVSTAR (według zaleceń producenta), jest zbudowany z gotowych elementów. System jest udoskonalany dzięki zastosowaniu kart komputerowych, wykonywanych z elementów mikroelektronicznych, które mają gwarantować bezpieczeństwo. Moduł eliminujący zakłócenia (ISU) zapewnia – zdaniem producenta – ochronę dla

---

[39] Wyniki badań w zakresie zabezpieczenia przed niekompatybilnością systemów dowodzenia i naprowadzania uzbrojenia związku operacyjnego przedstawiono w podrozdziale 3.4.

[40] Problematyka ta była podejmowana przez autora w opracowaniach naukowych [59;62] oraz materiałach studyjnych i dydaktycznych [55;56].

[41] ERI – ang. Electro-Radiation, Incorporated, Fairfield, New Jersey.

[42] PPS – ang. Precise Positioning Service.

[43] SPS – ang. Standard Positioning Service.

podatnych na zakłócenia (nie zabezpieczonych) odbiorników radiowych systemu GPS NAVSTAR .

Do obezwładnienia zakłóceniami zamierzonymi (celowymi) segmentu użytkowego systemu GPS NAVSTAR wykorzystywanego w obszarze odpowiedzialności obronnej związku operacyjnego przeciwnik może użyć masowo przenośnych nadajników zakłócających jednorazowego użytku. Są to urządzenia o bardzo małych rozmiarach, których koszt, według szacunków Amerykanów, nie powinien przekraczać 100 dolarów. Sytuacja ta może stać się poważnym zagrożeniem podczas wykorzystywania systemu GPS NAVSTAR w działaniach obronnych związku operacyjnego[44].

Z badań wynika, że **obrona antyzagłuszeniowa systemów radionawigacyjnych przed oddziaływaniem celowych sygnałów zakłócających potencjalnego przeciwnika powinna być organizowana w działaniach obronnych związku operacyjnego według zasad przedstawionych w podrozdziale 3.1.1.** Z uwagi na przewidywane masowe wykorzystywanie segmentu użytkowego przez różnych jego użytkowników, bardzo ważne staje się techniczne uodpornienie odbiorników GPS NAVSTAR na celowe zakłócenia radioelektroniczne. W wypadku niezbyt intensywnego oddziaływania zakłóceniami na system GPS NAVSTAR w obszarze działań obronnych związku operacyjnego skutecznym przedsięwzięciem może okazać się wykorzystanie modułu przeciwzakłóceniowego (np. ISU). Jak twierdzą konstruktorzy urządzenia[45], unika ono programowo skomplikowanych zakłóceń. Możliwości zintegrowanego systemu przeciwzakłóceniowego wynoszą: 95 – 100 dB tłumienności przy zakłóceniach szerokopasmowych oraz 105 – 110 dB tłumienności przy zakłóceniach wąskopasmowch. Urządzenie ISU nie musi być kierunkowo sterowane za pomocą dodatkowych urządzeń.

Aby wykluczyć możliwość wykorzystania systemu GPS NAVSTAR przez przeciwnika, producent wprowadził odpowiednie zabezpieczenia, dzięki którym zakłócani są odbiorcy niepożądani systemu GPS NAVSTAR. Urządzenie ISU eliminując bowiem zakłócenia jednego odbiornika GPS, może samo być źródłem zakłóceń dla innych użytkowników systemu nawigacyjnego. W niektórych sytuacjach można wykorzystywać zatem moduły ISU do zakłócania odbiorników GPS przeciwnika w tym samym czasie, gdy własne odbiorniki odbie-

---

[44]Nadajniki zakłóceń jednorazowego użytku mogą pracować w dowolnym paśmie fal elektromagnetycznych i dlatego mogą zakłócać również odbiorniki radiowe systemu GPS [61].

[45]Urządzenie testowano przy stosowaniu kodów: serwis SPS (C/A) i serwis PPS (P/Y). Scenariusz testu obejmował stosowanie od jednego do dwóch nadajników zakłóceń o osiągach 35 – 40 dB przy zakłóceniu szerokopasmowym i 45 – 50 dB przy zakłóceniu wąskopasmowym. Skuteczna tłumienność urządzenia przy dwu rozstawionych oddzielnie nadajnikach zakłóceń wynosi powyżej 45 dB i jest zależna od typu nadajnika [61].

rają sygnały z satelitów. Moduły pracują bowiem w zakresie częstotliwości radiowych i umożliwiają zmianę rodzajów pracy odbiorników GPS. Zmiana sposobu pracy w paśmie częstotliwości radiowych w celu zakłócenia odbiorników przeciwnika odbywa się przez zastosowanie odpowiedniego algorytmu kodowania. Dekodowanie, które następuje w odbiornikach sił własnych pozwala na przechwytywanie sygnałów nawigacyjnych w systemie GPS NAVSTAR przy równoczesnym stosowaniu zakłóceń. Moduł ISU może być zatem wykorzystany do ochrony przed zakłóceniami zarówno wojskowych, jak i cywilnych naziemnych stacji końcowych, pracujących w satelitarnych systemach łączności.

Dodatkowo przeciwko zakłóceniom wąskopasmowym może być wykorzystana metoda filtrowania kompleksowego. W metodzie tej zakłada się, że nie jest ważne fizyczne eliminowanie nadajnika zakłóceń, lecz ulepszenie możliwości selekcji sygnału w odbiorniku, poprzez technikę eliminacji zakłóceń wieloczęstotliwościowych. Metoda ta może być skuteczna przeciwko wielofunkcyjnym nadajnikom zakłóceń. Polega na wykorzystaniu wysokiej czułości odbiornika i ułamkowym czasie reakcji na odbiór sygnału, co umożliwia odbiór danych w warunkach zakłóceń pasmowych. A zatem odbiorniki, w których zastosowano technikę kompleksowego filtrowania, nie są podatne na zakłócenie wielopasmowe i nie wymagają stosowania wzorcowych sygnałów synchronizowanych częstotliwościowo lub amplitudowo.

W sytuacjach, kiedy konieczne jest wykluczenie sił przeciwnika z dostępu do systemu w obszarach, w których nie przewiduje się wykorzystania go przez elementy ugrupowania obronnego związku operacyjnego (np. w tyłowym obszarze działań związku operacyjnego) należy przewidzieć rozwinięcie systemów zakłóceń, które będą współpracować z pasmem częstotliwości systemu GPS NAVSTAR. Problem ten należy rozwiązywać w ramach zakłócania informacyjnego.

3.1.4. Obrona antyzagłuszeniowa systemów naprowadzania uzbrojenia

Z badań wynika, że obrona antyzagłuszeniowa systemów naprowadzania uzbrojenia w działaniach obronnych związku operacyjnego stanowi również perspektywiczne przedsięwzięcie w zakresie przeciwdziałania skutkom zakłócania informacyjnego przeciwnika. Obiektami oddziaływania zagłuszającego systemów naprowadzania uzbrojenia związku operacyjnego mogą być różne układy naprowadzania uzbrojenia. Analiza rozwiązań światowych przeprowadzona na podstawie dostępnych materiałów źródłowych [3;16;52;62;66;69;83;136]

umożliwia **wyróżnienie czterech zasadniczych grup naprowadzania uzbrojenia: zdalne**[46], **programowe**[47], **samonaprowadzanie**[48], **kombinowane**[49]. W każdej grupie wyróżnia się różnorodne urządzenia techniczne wykorzystujące fale elektromagnetyczne, zjawiska świetlne, dźwiękowe, magnetyczne, cieplne, bezwładnościowe, żyroskopowe i inne. W większości systemów naprowadzania uzbrojenia wykorzystuje się urządzenia radiolokacyjne, telewizyjne, termowizyjne, laserowe oraz radiowe.

W naprowadzaniu 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 radiolokacyjne systemy naprowadzania jest możliwość ich stosowania w nocy oraz w prawie 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 automatycznie, a w starszych systemach – półautomatycznie lub ręcznie.

---

[46] Naprowadzanie zdalne realizowane jest z wykorzystaniem specjalnych urządzeń dokonujących automatycznie pomiaru wzajemnego położenia celu i środka rażenia, przetwarzania tych danych na sygnały sterowania (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 [3;66;134].

[47] Naprowadzanie 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 naprowadzanie: programowe automatyczne, astronawigacyjne, radionawigacyjne, bezwładnościowe [3;66;93;134].

[48] Samonaprowadzanie polega na samoczynnym naprowadzaniu 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 wówczas, gdy istnieje możliwość wyróżnienia celu z otaczającego tła, czyli gdy istnieje tzw. kontrastowość celu, którą system może uchwycić. Z uwagi na miejsce pierwotnego źródła energii wykorzystywanego do pracy układu naprowadzania wyróżnia się samonaprowadzanie: pasywne, półaktywne i aktywne [3;66;93;134].

[49] Naprowadzanie kombinowane jest połączeniem kilku różnych systemów, przy czym każdy system kieruje lotem na określonym odcinku toru, lub pracuje jednocześnie z innymi systemami [3;66;93;134].

Wadą telewizyjnego systemu naprowadzania jest jego niska efektywność w warunkach złej lub ograniczonej widoczności. Można zakłócić go stosując również zasłony dymne.

Systemy naprowadzania w podczerwieni (termowizyjne) uzupełniają układy telewizyjne. Umożliwiają, bowiem zwalczanie celów w nocy oraz w warunkach ograniczonej widoczności. Zasada działania termowizyjnych systemów naprowadzania jest zbliżona do wykorzystywanej w naprowadzaniu telewizyjnym, z tym że w systemach termowizyjnych kamera umieszczona w głowicy pocisku widzi obraz termiczny atakowanego obiektu formowany na podstawie różnicy temperatur celu i otaczającego go środowiska. Dodatkową zaletą tego układu jest dwukrotnie większy (niż przy laserowym lub telewizyjnym układzie) zasięg wykrywania celu oraz możliwość wykrywania celów ukrytych i zamaskowanych[50]. Wadą tego systemu jest natomiast jego podatność na działanie pułapek termicznych, które mogą skutecznie pozorować obiekty rzeczywiste.

W **laserowych systemach naprowadzania (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 naprowadzania zapewniają wysoką celność sterowanej amunicji. Nie są jednak odporne na działanie zakłóceń pasywnych.

Ponieważ każdy z systemów naprowadzania ma swoje zalety, ale również i wady, to zazwyczaj do naprowadzania środków 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 naprowadzania są z reguły urządzeniami wielokanałowymi, umożliwiającymi jednoczesne sterowanie kilkoma obiektami wykonawczymi. Realizację tego zapewniają wyspecjalizowane komputery pokładowe i urządzenia charakteryzujące się wysoką niezawodnością oraz skutecznością sterowania.

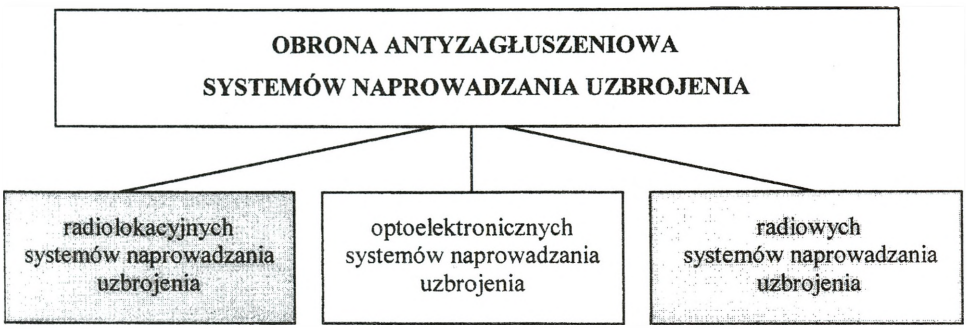
Z powyższego wynika, że **obrona antyzagłuszeniowa systemów naprowadzania uzbrojenia związku operacyjnego powinna obejmować zespół przedsięwzięć organizacyjnych oraz technicznych mających na celu ochronę odbiorczych urządzeń radiolokacyjnych, optoelektronicznych i radiowych przed oddziaływaniem aktywnych oraz pa-**

---

[50] Praktycznie układy te znalazły zastosowanie w wojnie w rejonie Zatoki Perskiej w 1991 r. [3;18;114].

sywnych zakłóceń emitowanych przez środki walki informacyjnej przeciwnika (rysunek 3.6.).

Działania podejmowane w ramach obrony antyzagłuszeniowej systemów naprowadzania uzbrojenia w obszarze odpowiedzialności obronnej związku operacyjnego powinny być ściśle zsynchronizowane – w zależności od sposobu naprowadzania i rodzaju wykorzystywanych środków technicznych z maskowaniem[51] radioelektronicznym, radiolokacyjnym, optoelektronicznym i informatycznym, lecz ukierunkowane przede wszystkim na zapewnienie stabilnej pracy urządzeń odbiorczych w warunkach intensywnego stosowania zakłóceń elektronicznych przez przeciwnika.



Rys. 3.6. Obrona antyzagłuszeniowa systemów naprowadzania uzbrojenia w działaniach obronnych związku operacyjnego

Z badań wynika, że w obronie **antyzagłuszeniowej radiolokacyjnych systemów naprowadzania uzbrojenia** szczególną uwagę należy zwrócić na **przedsięwzięcia techniczno - organizacyjne** które odgrywają rolę pierwszoplanową w planowaniu użycia wyżej wymienionych systemów w działaniach obronnych związku operacyjnego. Polegają one na:

- odpowiednim doborze parametrów technicznych stacji radiolokacyjnych;
- stosowaniu specjalnych układów przeciwzakłóceniowych;
- należytym wyszkoleniu specjalistycznym obsług.

[51] Problematyka ta była przedmiotem rozważań w rozdziale 2 niniejszej pracy studyjnej.

Ważnym przedsięwzięciem, umożliwiającym zwiększenie odporności stacji radiolokacyjnej na **zakłócenia**[52] **aktywne** jest stabilizacja poziomu fałszywego alarmu (SPFA). Zastosowane we współczesnych stacjach radiolokacyjnych tzw. układy SPFA są absolutnie niezbędnym środkiem przeciwzakłóceniowym. Należy podkreślić, że SPFA nie likwiduje wpływu zakłóceń na wykrywanie sygnałów użytecznych. O tym, czy echo zostanie wykryte, decyduje stosunek mocy echa do sumy mocy zakłóceń i szumu własnego.

Spośród parametrów technicznych stacji radiolokacyjnych wykorzystywanych do naprowadzania uzbrojenia dużą rolę odgrywa dobór częstotliwości ich pracy oraz przestrajanie na inne częstotliwości nośne. Z teorii propagacji fal elektromagnetycznych wynika, że im wyższy zakres wykorzystywanych częstotliwości, tym trudniejsze jest wykrycie i rozpoznanie danej stacji (wąskie wiązki antenowe, małe moce nadajników).

Utrudnione jest również zakłócanie, ponieważ anteny te mają bardzo małe listki boczne. Z uwagi na okna transmisji w atmosferze stacje tego typu powinny pracować w zakresie częstotliwości: 34 – 36 GHz[53]; 75 – 95 GHz; 140 GHz, 225 GHz.

Możliwość szybkiego przestrajania współczesnych stacji radiolokacyjnych na inną częstotliwość nośną jest nieodzownym ich atrybutem w walce z celowymi zakłóceniami aktywnymi. Jeżeli stacja radiolokacyjna pracuje na stałej częstotliwości, staje się łatwą „ofiarą" nadajnika zakłóceń, który może promieniować w wąskim paśmie częstotliwości i odpowied-

---

[52] Zakłócenia radiolokacyjne to niepożądane sygnały, zniekształcające lub zakłócające sygnały użyteczne, stanowiące nośniki informacji w systemach radiolokacyjnych. Ze względu na sposób powstawania dzielą się na celowe i przypadkowe. Zakłócenia celowe wytwarza się za pomocą specjalnych środków i urządzeń technicznych, zaś przypadkowe powstają wskutek odbicia energii elektromagnetycznej od obiektów terenowych (miejscowych), chmur, kropli deszczu lub wskutek promieniowania słonecznego, kosmicznego i z urządzeń przemysłowych. Zalicza się do nich także zakłócenia w postaci szumów własnych odbiornika i zakłócenia interferencyjne (wzajemne) urządzeń. Zakłócenia celowe wytwarza się dla zmniejszenia efektywności lub całkowitego sparaliżowania pracy systemów radiolokacyjnych. Ze względu na sposób wytwarzania dzieli się je na aktywne i pasywne. Do wytwarzania **zakłóceń aktywnych** służą z reguły stacje zakłóceń radiolokacyjnych. Ze względu na szerokość widma i sposób promieniowania energii elektromagnetycznej dzieli się je na: zaporowe, przestrajanie w częstotliwości (quasi - zaporowe), wąskopasmowe, ciągłe i impulsowe. Zakłócenia zaporowe mają widmo częstotliwości wielokrotnie przekraczające pasmo przenoszenia odbiornika. Pozwalają one na jednoczesne zakłócenie wielu stacji radiolokacyjnych pracujących na różnych częstotliwościach. Zakłócenia wąskopasmowe wytwarzane są w wąskim paśmie częstotliwości; są one zwykle skuteczniejsze od zakłóceń zaporowych, ponieważ wykorzystuje się ich całą energię, ale w tym wypadku niezbędna jest znajomość dokładnej wartości częstotliwości nośnej stacji radiolokacyjnej. Zakłócenia impulsowe mogą być odzewowe (jednokrotne lub wielokrotne) albo niezależne (nieodzewowe). Ze względu na sposób oddziaływania na zakłócane urządzenia rozróżnia się zakłócenia maskujące i imitujące (dezinformujące). Do pierwszej grupy zalicza się zakłócenia, które utrudniają lub uniemożliwiają wykrycie i obróbkę sygnału użytecznego. Zakłócenia imitujące wprowadzają do zakłócanego systemu nieprawdziwe dane. Za ich pomocą można wytworzyć na ekranie wskaźnika stacji radiolokacyjnej zobrazowanie celu na takim azymucie i odległości, gdzie nie ma celów rzeczywistych. **Zakłócenia pasywne** są wytwarzane w celu wywołania silnych odbić elektromagnetycznych wysłanych przez stacje radiolokacyjne. Stanowią one odbicia od sztucznych obiektów (dipoli, reflektorów rogowych oraz innych sztucznych elementów odbijających, pułapek radiolokacyjnych) lub naturalnych niejednorodności, takich jak hydrometeory, opadów atmosferycznych powierzchni wody, lądu i in. [62;97].

[53] Pasmo to wykorzystywane jest powszechnie w stacjach radiolokacyjnych do naprowadzania uzbrojenia, zainstalowanych na śmigłowcach uzbrojonych i samolotach taktycznego wsparcia pola walki.

nio maksymalizować promieniowaną gęstość mocy. Natomiast stacja radiolokacyjna szybko zmieniająca częstotliwość nośną[54] zmusza nadajnik zakłóceń do rozłożenia dysponowanej mocy w odpowiednio szerszym paśmie, a w konsekwencji do wielokrotnego obniżenia gęstości mocy emitowanego sygnału zakłóceń. Szybkie przestrajanie, czyli tzw. „ucieczka od zakłóceń" może okazać się skuteczną metodą w walce z zakłóceniami wąskopasmowymi. W wypadku zastosowania przez przeciwnika zakłóceń szerokopasmowych należy wykorzystać ideę zasygnalizowaną przez profesora Yu Hai Mao z Chin [29] polegającą na „śledzeniu" częstotliwości interferencyjnych zaników zakłóceń, a następnie na adaptacyjnym przestrajaniu stacji radiolokacyjnej na te częstotliwości.

W celu zwiększenia odporności stacji radiolokacyjnych na zakłócenia często stosuje się przedsięwzięcie polegające na zwiększaniu mocy nadajnika radiolokatora. Taka metoda przeciwdziałania zakłóceniom, zwana popularnie „przepalaniem zakłóceń" jest jednak nieefektywna, zważywszy iż nadajnik zakłóceń radiolokacyjnych ma z natury taką przewagę nad stacją radiolokacyjną. Jego sygnał zmienia się z odległością (R) proporcjonalnie do $1/R^2$, podczas gdy echo radarowe – proporcjonalnie do $1/R^4$ [29]. Jednak w połączeniu z innymi czynnikami niewątpliwie każdy dodatkowy kilowat mocy nadajnika może być cenny dla maksymalizacji sygnalizowanego wyżej stosunku sygnału do zakłóceń.

Z powyższego wynika, że **problem pożądanego zasięgu radiolokacyjnej stacji naprowadzania uzbrojenia w działaniach obronnych związku operacyjnego powinien być uwzględniany na etapie ich planowania.** Zwiększając moc nadajnika stacji radiolokacyjnej można również częściowo rekompensować sztuczne zmniejszenie skutecznej powierzchni odbicia celu (przykładem tego mogą być pokrycia wykonane w nowej technologii, określanej anglojęzyczną nazwą stealth) i w ten sposób można zwiększyć zasięg jego wykrycia.

W walce z zakłóceniami uczestniczy również na kilka sposobów antena stacji radiolokacyjnej. Zwiększenie zysku kierunkowego anteny oznacza zmniejszenie szerokości charakterystyki kierunkowej anteny. Jest ono celowe nie tylko ze względu na przeciwdziałanie zakłóceniom aktywnym, lecz i pasywnym, których efektywność zależy od tzw. przestrzeni nierozróżniania.

Ważnym parametrem anteny jest również poziom listków bocznych. Przy niskim poziomie listków bocznych anteny (poniżej – 40 dB) można z powodzeniem realizować zadania w znakomicie przeważającej części obszaru obserwacji, poza wąskim sektorem obserwacji, kiedy jej wiązka ukierunkowana jest wprost na źródło zakłóceń. Dla obniżenia poziomu listków bocznych anten należy stosować ich kompensację. Przedsięwzięcie to polega na wyposa-

[54] Np. stacja radiolokacyjna ze skokową zmianą częstotliwości nośnej.

żeniu stacji radiolokacyjnej w dodatkowe anteny kompensacyjne (bezkierunkowe) wraz z dodatkowymi odbiornikami i układami porównującymi. Dzięki temu na wyjściu odbiornika stale będą występowały odbierane zakłócenia impulsowe, które z kolei można wykorzystać do blokowania odbiornika radiolokatora na czas odbioru zakłóceń lub do ich kompensacji. Utworzony system kompensacji akceptuje tylko sygnały odebrane wiązką główną, eliminując sygnały odebrane listkami bocznymi. Podobnie można blokować zakłócenia pochodzące od blisko położonych stacji radiolokacyjnych.

Szybsze wykrycie sygnału użytecznego na tle zakłóceń można uzyskać przez zastosowanie anten dających eliptyczną polaryzację fali. Polaryzacja eliptyczna charakteryzuje się trzema podstawowymi parametrami: kątem przestrzennej orientacji elipsy polaryzacji, współczynnikiem eliptyczności i kierunkiem wirowania wektora natężenia pola elektrycznego. Jeżeli zatem parametry polaryzacji fali zakłócającej będą różnić się od parametrów polaryzacyjnych sygnału użytecznego, to już w układzie antenowym takiego radiolokatora będzie zachodziła selekcja sygnałów. Z powyższego wynika, że największy wpływ na efektywność selekcji ma różnica kierunków wirowania wektorów natężenia pola elektromagnetycznego, przy czym im współczynnik eliptyczności bardziej różni się od jedności, tym większy jest ten wpływ.

Odporność radiolokatora na zakłócenia może być podwyższona również w wyniku zwiększenia dynamiki układu odbiorczego. Zapobiega ona bowiem przesterowaniu odbiornika silnymi zakłóceniami – zarówno aktywnymi, jak i pasywnymi. Ważną rolę odgrywają również wskaźniki z bezwładnością świetlną ekranu, którymi ograniczają wpływ zakłóceń asynchronicznych i szumowych dzięki integracji sygnału użytecznego.

Ważną rolę w obronie antyzagłuszeniowej radiolokacyjnych systemów naprowadzania uzbrojenia spełniają układy przeciwzakłóceniowe, w których wykorzystuje się zazwyczaj różnice między parametrami sygnału użytecznego i zakłócającego. Parametrami, którymi różnią się te sygnały, są: częstotliwość nośna, szerokość widma, częstotliwość powtarzania, czas trwania impulsów, faza, amplituda, polaryzacja i in. Układy przeciwzakłóceniowe powinny być dostosowane do rodzaju zakłóceń stosowanych przez potencjalnego przeciwnika. Z tych też względów wyróżnia się:

- układy przeciw zakłóceniom impulsowym;
- układy przeciw zakłóceniom ciągłym;
- układy przeciw zakłóceniom impulsowym i ciągłym;
- układy (środki) przeciwdziałania zakłóceniom pasywnym.

W wypadku stosowania przez przeciwnika asynchronicznych zakłóceń impulsowych sygnał użyteczny różni się od sygnału zakłócającego przede wszystkim częstotliwością (okre-

sem) powtarzania impulsów. Układami skierowanymi przeciw takim zakłóceniom mogą być selektory częstotliwości (okresu powtarzania impulsów). W wyniku zastosowania takiego selektora wraz z linią opóźniającą impulsy zakłóceń o okresie powtarzania różnym od czasu opóźnienia linii (który odpowiada impulsom odbitym od celu) nie zostają przenoszone przez ten układ, co jest równoznaczne z ich tłumieniem.

Z kolei do ograniczania szerokopasmowych zakłóceń impulsowych należy wykorzystać układ z dodatkowym odbiornikiem dostrojonym do częstotliwości nieco różniącej się od częstotliwości sygnału użytecznego. W wyniku zastosowania odpowiednich układów kompensacji, do dalszej obróbki można – w idealnej sytuacji – uzyskać sygnał użyteczny obarczony jedynie własnym szumem odbiornika. Można również zastosować odpowiednie układy selekcji, gdy zakłócenia impulsowe mają bardzo szerokie widmo przesunięte w stosunku do widma sygnału użytecznego.

Przeciwdziałanie silnym zakłóceniom ciągłym niemodulowanym lub modulowanym powinno być realizowane przede wszystkim z punktu widzenia ochrony odbiornika przed przesterowaniem napięciem sygnałami zakłócającymi. W tym celu odbiorniki radiolokacyjne powinny być wyposażone w odpowiednie układy przeciwzakłóceniowe, tj. wzmacniacze pośredniej częstotliwości o dużej dynamice, z logarytmiczną charakterystyką amplitudową, układy natychmiastowej automatycznej regulacji wzmocnienia[55], układy automatycznej regulacji wzmocnienia uzależnionej od częstotliwości fałszywych alarmów (w razie zakłóceń szumowych), obwody różniczkujące, filtry optymalne, integratory cyfrowe i in. Układy te zwiększają odporność radiolokatora nie tylko na silne zakłócenia ciągłe niemodulowane i modulowane amplitudowo i częstotliwościowo, lecz także na zakłócenia w postaci impulsów o długim czasie trwania.

Z analizy właściwości zakłóceń pasywnych [29;62;68] wynika, że mają one charakter ciągły (w wypadku odbić od lądu, morza itp.) lub postać długich impulsów (w razie odbić od hydrometeorów lub źródeł sztucznych, np. chmur dipoli). Jeśli ich moc jest duża, może dochodzić do przesterowania odbiornika radiolokacyjnego. Do przeciwdziałania zakłóceniom pasywnym należy, zatem wykorzystywać układy umożliwiające wykrywanie wśród nich sygnałów użytecznych. Wykrywanie takie jest możliwe przez stosowanie układów automatycznej regulacji wzmocnienia oraz specjalnych charakterystyk amplitudowych odbiorników lub na zasadzie wykorzystania różnic[56] między właściwościami sygnału użytecznego i zakłócają-

---

[55] Układ natychmiastowej automatycznej regulacji wzmocnienia powoduje zmniejszenie wzmocnienia wzmacniacza pośredniej częstotliwości urządzenia odbiorczego, gdy tylko pojawi się silny sygnał zakłócający [60;68].

[56] Przyczyną wpływającą na powyższe różnice są na ogół różne szybkości celu i źródła pasywnych zakłóceń, w wyniku czego, zgodnie ze zjawiskiem Dopplera, częstotliwość nośna sygnału użytecznego będzie się różnić od częstotliwości nośnej zakłóceń pasywnych. Istota tego zjawiska polega na tym, że przy zbliżaniu się obiektów ruchomych obserwuje się zwiększanie częstotliwości, przy oddalaniu natomiast jej zmniejszanie [60].

cego. Podstawowym sposobem eliminacji zakłóceń pasywnych w nowoczesnych stacjach radiolokacyjnych 3D (trójwspółrzędnych) jest filtracja dopplerowska[57], dzięki której wykrywany obiekt, np. samolot przelatujący przez chmurę dipoli jest wykrywany. W stacjach tych następuje utrata wykrywania tylko w jednej „wiązce" (lub w dwóch sąsiednich), podczas gdy pozostałe wiązki praktycznie nie widzą zakłóceń i pozwalają wykrywać obiekty pod i nad chmurą dipoli.

Do przeciwdziałania zakłóceniom pasywnym można wykorzystywać również różnice w polaryzacyjnych właściwościach sygnałów odbitych od celów i źródeł zakłóceń pasywnych. W tym celu należy stosować anteny dające kołową polaryzację fali promieniowanej. Selekcję polaryzacyjną należy stosować w celu zmniejszenia efektywności zakłóceń pochodzących np. od reflektorów rogowych lub opadów atmosferycznych. Fale odbite od takich obiektów będą spolaryzowane kołowo, lecz skierowane w odwrotnym kierunku niż fala padająca, w wyniku czego nie zostaną odebrane przez układ antenowy radiolokatora. Cele rzeczywiste mają różnorodne kształty i dlatego polaryzacja fal od nich odbitych staje się eliptyczna o składowej natężenia pola elektrycznego wirującej zgodnie lub przeciwnie w stosunku do fali padającej, dzięki czemu część energii sygnału odbitego przechodzi przez układ antenowy i sygnał taki może być wyróżniony na tle tego typu zakłóceń pasywnych.

Aby zwiększyć odporność stacji radiolokacyjnej na zakłócenia pasywne, należy dobierać również możliwie mały czas trwania impulsu, ponieważ obszar odbicia jest wprost proporcjonalny do czasu jego trwania. Należy mieć na uwadze, że pociąga to za sobą zmniejszenie jego energii przy ustalonej mocy impulsowej.

Ciągły rozwój automatyzacji radiolokacyjnych systemów naprowadzania uzbrojenia stwarza warunki, w których rola obsługi stacji w zakresie obrony antyzagłuszeniowej jakby malała. W tych systemach operator występuje często w roli decydenta lub kontrolera środków automatyzacji. Okazuje się jednak, że nawet w pełni automatyczne urządzenie nie jest w stanie całkowicie zastąpić dobrze przygotowanego operatora. Urządzenie takie może poprawnie funkcjonować tylko wówczas, jeśli a priori znane są rodzaje stosowanych przez przeciwnika zakłóceń. I tylko wtedy jego efektywność będzie duża. Jeśli zmieni się natomiast rodzaj zakłóceń, przestaje ono należycie spełniać swoje zadanie. Natomiast dobrze wyszkolony operator, dzięki umiejętnościom dostosowania się do nowych, niekiedy nieoczekiwanych sytuacji i rodzajów zakłóceń, może lepiej niż zaprogramowany automat wykorzystać dostępne środki przeciwdziałania zakłóceniom, w jakie wyposażony jest radiolokator. Przede wszystkim po-

[57] W literaturze specjalistycznej określana jest mianem przestrzennej filtracji zakłóceń [29].

winien on umieć rozróżniać sygnały prawdziwe od fałszywych, aby uniknąć pomyłek stanowiących cel niektórych rodzajów zakłóceń. Z powyższego wynika potrzeba ciągłego doskonalenia umiejętności szkolenia operatorów w warunkach różnorodnych zakłóceń, które są i będą nieodłącznym atrybutem elektronicznego pola walki.

Z badań wynika, że obrona **antyzagłuszeniowa optoelektronicznych systemów naprowadzania uzbrojenia w działaniach obronnych związku operacyjnego powinna obejmować zespół przedsięwzięć organizacyjno-technicznych zapewniających stabilną pracę układów naprowadzania telewizyjnego, termowizyjnego i laserowego w warunkach prowadzenia przez przeciwnika zakłócania optoelektronicznego**[58]. Powinna być skoordynowana z maskowaniem optoelektronicznym, które było przedmiotem rozważań w podrozdziale 2.2.1.3.

Ważną rolę w obronie antyzagłuszeniowej optoelektronicznych systemów naprowadzania uzbrojenia ma wyposażenie zarówno powietrznych, jak i naziemnych środków walki związku operacyjnego w odpowiednie odbiorniki ostrzegawcze pracujące w podczerwieni

---

[58] Zakłócanie optoelektroniczne polega na dezorganizacji pracy lub niszczeniu urządzeń rozpoznania pola walki oraz naprowadzania pocisków na cel. Zasada ich działania opiera się na emisji promieniowania elektromagnetycznego o długości fali i natężeniu wiązki zdolnej do (najczęściej czasowego) zakłócania pracy czujników lub porażenia wzroku żołnierza obsługującego broń. Do tej grupy należą: broń laserowa małej mocy; promienniki równokierunkowe i kierunkowe; środki mylące w podczerwieni (naboje i rakiety – flary); generatory promieniowania mikrofalowego dużej mocy i in. **Broń laserowa małej mocy** może być stosowana we wszystkich rodzajach sił zbrojnych. W związku operacyjnym może występować jako środek przenośny (zestawy indywidualne, podwieszane pod karabinkiem i in.) lub przewoźny. W laserach małej mocy wykorzystuje się promieniowanie o różnej długości fali, co zwiększa skuteczność jego działania. Najczęściej stosowane jest promieniowanie ultrafioletowe, czerwone, niebieskie i żółte. Urządzenia impulsowe promieniowania laserowego są również stosowane do wytwarzania plazmy i fali uderzeniowej, służących do niszczenia czujników i porażenia załóg wozów bojowych. Wykorzystuje się zjawisko ablacji (stopniowego niszczenia, kruszenia), zachodzące w wypadku uderzenia promienia laserowego w atakowaną powierzchnię oraz tworzenie fali uderzeniowej i powstawanie odłamków z materiału pancerza. Plazma może uszkodzić czujniki, układy kontrolno - pomiarowe i obserwacyjne. Broń tego typu może być wykorzystana do obezwładniania lekko opancerzonych oraz lekkich wozów bojowych. **Promienniki równokierunkowe** lub izotropowe wykorzystywane do celów wojskowych 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 (ksenon, cez, argon i in.). Do rozgrzania gazu i doprowadzenia go do stanu plazmy wykorzystuje się energię detonacji materiału wybuchowego w kształcie stożka wypełnionego gazem szlachetnym. **Promienniki kierunkowe**, w odróżnieniu od równokierunkowych, są dodatkowo wyposażone w urządzenia ukierunkowujące strumień promieniowania (np. lampy błyskowe, wypełnione ww. gazami szlachetnymi). Pod względem konstrukcyjnym różnią się też umiejscowieniem ładunku wybuchowego. Charakteryzują się one większą sprawnością i mniejszym prawdopodobieństwem przypadkowego porażenia celów własnych. Środki mylące (głównie naboje i rakiety – flary) są wykorzystywane do „ściągania na siebie" układów sterowania pocisków naprowadzających się głównie na podczerwień, uniemożliwiając im trafienie w cel. Zazwyczaj są to mieszanki łatwo palne wystrzeliwane ze specjalnych urządzeń umieszczanych w zasobnikach razem z dipolami służącymi do zakłócania promieniowania radiolokacyjnego. **Generatory promieniowania mikrofalowego i laserowego dużej mocy**, nazywane również superśrodkami zakłócającymi wykorzystywane są do zakłócania łączności radioliniowej oraz do niszczenia układów elektronicznych samolotów, śmigłowców, pocisków rakietowych, jak również do niszczenia satelitów bojowych i telekomunikacyjnych, a także pokryć wykonanych w technologii ang. „stealth" [59;97].

i odbiorniki ostrzegawcze laserowe, służące do wykrywania bezpośredniego ich zagrożenia oraz podjęcia – z reguły automatycznie – odpowiednich przedsięwzięć ochronnych (manewru, wprowadzania w błąd, rozpoczęcia zakłóceń, zadymiania i in.).

W wypadku wykrycia przez odbiornik ostrzegawczy, pracujący w podczerwieni, bezpośredniego zagrożenia pociskami rakietowymi przeciwnika należy stosować flary emitujące promieniowanie cieplne, które z kolei mają na celu zmylenie pocisków potencjalnego przeciwnika naprowadzanych na źródło ciepła. Są one najbardziej skuteczne, gdy realistycznie naśladują ślad cieplny obiektu i gdy się używa wraz z systemami ostrzegania o zbliżaniu pocisku. Mogą one być wystrzeliwane ze specjalnie skonstruowanych zasobników. Zastosowana w nich mieszanka łatwo palna spala się w odległości 50 do 200 m od osłanianego obiektu w czasie od 0,5 do kilku sekund (około 4 s) i daje emisję cieplną w paśmie 14 mikrometrów, a wytworzony impuls ma moc rzędu 22 kW/s [66].

Laserowe odbiorniki ostrzegawcze wykrywają promieniowanie widzialne i podczerwone dalmierzy i oświetlaczy laserowych przeciwnika. Są w stanie ostrzec załogę powietrznego (np. śmigłowca) lub naziemnego środka walki (np. wozu bojowego) o opromieniowaniu wiązką laserową i automatycznie uruchomić urządzenia odpalające świece dymne, które z kolei w kilka sekund zakrywają cel obłokiem dymu i umożliwiają dokonanie skrytego manewru. Odbiorniki te mogą być przydatne wojskom działającym w obszarze sił przesłaniania związku operacyjnego.

Rozwój systemów optoelektronicznych pracujących w układzie pasywnym, a zatem trudno wykrywalnych wymusza konieczność poszukiwania nowych środków przeciwdziałania. Jednym z najskuteczniejszych sposobów przeciwdziałania jest maskowanie środków walki za pomocą siatek maskujących optycznie i termicznie oraz malowanie ochronne[59]. Pojawienie się urządzeń do wykrywania w podczerwieni doprowadziło do stosowania farb o niskim współczynniku emisyjności, obniżających do minimum kontrast temperatury pomiędzy powierzchnią obiektu a otoczeniem. W czasie obserwacji celu w podczerwieni może powstawać w ten sposób złudzenie polegające na zlaniu się widma podczerwieni obserwowanego celu z widmem tła, zastosowanie bowiem środków metamorficznych powoduje zmianę koloru pod wpływem warunków zewnętrznych (temperatury, natężenia oświetlenia). Należy zauważyć, że pokrycia takie są najskuteczniejsze, wtedy gdy emisyjność poszczególnych plam barwnych jest zróżnicowana, co powoduje pozorne rozdzielenie sylwetki obserwowanego obiektu w podczerwieni. Szczególna uwaga powinna być zwrócona na wykorzystanie

[59] Problemy te były przedmiotem rozważań w podrozdziale 2.2.1.3.

osłon izolacyjnych (np. na silniki, układy wydechowe i in.) i filtrów szerokopasmowych na urządzenia pracujące w tym zakresie promieniowania elektromagnetycznego.

Jak wskazują doświadczenia, osiągnięcie różnicy temperatur 2^{o}– 6^{o} C obiektu względem tła obniży w dużym stopniu prawdopodobieństwo wykrycia celu. Stąd też już na etapie projektowania środków walki należy ograniczać wartości różnorodnych składowych pól fizycznych mających wpływ na ograniczenie ich współczynnika emisyjności.

Możliwość wykorzystania przez przeciwnika nowoczesnych optoelektronicznych środków wymusza konieczność stosowania zasłon wielospektralnych, ograniczających efektywność ich użycia. Zasłony te powinny stanowić kombinację absorpcji rozproszenia i odbić tworzonych przez odpowiednie środki dymotwórcze i dipolowe, zapewniające skuteczną osłonę przed obserwacją w podczerwieni, w zakresie światła widzialnego oraz przed obserwacją radiolokacyjną. Mogą one być wykorzystywane również do stosowania zakłóceń pasywnych, tłumiących skutecznie energię wiązki laserowej.

Obrona przed oddziaływaniem generatorów promieniowania mikrofalowego i laserowego dużej mocy stanowi przedsięwzięcie perspektywiczne i powinna polegać na zastosowaniu odpowiednich rozwiązań technicznych i organizacyjnych, umożliwiających uodpornienie układów wrażliwych na przegrzane i izolowanie ich przed nadmierną energią cieplną. Należy zaznaczyć, że skutkiem oddziaływania tego promieniowania może być zapalenie lub topnienie atakowanych celów, dzięki zjawisku zamiany w napromieniowanym materiale energii promieniowania mikrofalowego w energię cieplną. Przedsięwzięcia techniczne powinny mieć swoje odzwierciedlenie w wymaganiach stawianych środkom walki nowo wprowadzanym do uzbrojenia związku operacyjnego. Przedsięwzięcia organizacyjne obrony przed oddziaływaniem generatorów promieniowania mikrofalowego i laserowego dużej mocy powinny być przedmiotem odrębnych, szczegółowych badań – w miarę wprowadzania do wyposażenia wojsk tego rodzaju broni.

Z badań wynika, że obrona **antyzagłuszeniowa radiowych systemów naprowadzania uzbrojenia** w działaniach obronnych związku operacyjnego powinna obejmować odpowiednie przedsięwzięcia techniczno-eksploatacyjne oraz organizacyjne, przedstawione w ramach przeciwdziałania skutkom zakłócania systemów (sieci) łączności związku operacyjnego (podrozdział 3.1.1.).

3.2. Obrona informacyjna przed zakłócaniem dezinformującym

Częste wykorzystywanie aktywnych działań dezinformujących[60] w minionych wojnach i konfliktach zbrojnych dowodzi, że i w przyszłych działaniach obronnych mogą one również odgrywać ważną rolę. Zakłada się, że działania te będą służyć osiągnięciu celów strategicznych, operacyjnych i taktycznych. Przewiduje się, że znaczenie działań dezinformujących wzrośnie, głównie ze względu na rozmach prowadzonych operacji i walk, w których dowodzenie wojskami i naprowadzanie uzbrojenia będzie realizowane na dużych przestrzeniach i przede wszystkim za pomocą środków technicznych wspomaganych środkami informatycznymi.

Wysoka dynamika i manewrowość działań obronnych związku operacyjnego będzie często stwarzać trudne sytuacje, w których dowództwo, sztab, związki taktyczne i oddziały nie będą miały ciągłej łączności lub jej utrzymanie będzie utrudnione.

Ponadto duże możliwości rażenia i niszczenia przez lotnictwo, wojska rakietowe i artylerię, desanty i grupy dywersyjno-rozpoznawcze środków i obiektów elektronicznych będą przyczyną częstego „wypadania" elementów (korespondentów) z poszczególnych relacji dowodzenia (łączności) bez wiedzy dowództw i sztabów, co stworzy bardzo korzystne warunki do prowadzenia dezinformowania, którego główną formą jest – jak wiadomo – podszywanie się pod nieczynne w danym okresie środki elektroniczne.

Przekazywanie przez przeciwnika wiadomości nieprawdziwych np. w relacjach łączności i kanałach radionawigacyjnych może być przyczyną różnego rodzaju nieporozumień, niepewności, nieskoordynowanych działań i w konsekwencji może przynieść większe efekty niż zakłócanie zagłuszające[61]. Sytuacja taka może mieć miejsce również w działaniach obronnych związku operacyjnego. Zachodzi zatem konieczność przeciwdziałania temu zagrożeniu w ramach obrony przed zakłócaniem dezinformującym, która utożsamiana jest z obroną kontrdezinformacyjną[62].

---

[60] Aktywne działania dezinformujące stanowią szczególną formę celowego oddziaływania przeciwnika. Tego rodzaju działania mają wybitnie charakter dywersyjny i umożliwiają uzyskanie stosunkowo wysokiego stopnia dezorganizacji dowodzenia i naprowadzania uzbrojenia. Problemowi temu poświęca się wiele uwagi w siłach zbrojnych wielu państw. W siłach zbrojnych Rosji działania te utożsamiane są głównie z działaniami dywersyjnymi prowadzonymi w stosunku do systemów radioelektronicznych (radiowych, radionawigacyjnych). W siłach zbrojnych głównych państw NATO operuje się pojęciem „mylenie", które w odniesieniu do środków elektronicznych obejmuje manipulowanie, imitowanie i symulowanie elektroniczne [59;62;97].

[61] Szerzej problematyka ta przedstawiona jest w wielu opracowaniach naukowych [101;102] oraz w literaturze beletrystycznej [79]. Podejmowana była również przez autora w [60].

[62] Problem ten postrzegany jest również jako obrona przeciwdezinformacyjna [24;25;26].

Z badań wynika, że **obrona kontrdezinformacyjna w działaniach obronnych związku operacyjnego powinna być realizowana zarówno w stosunku do stanów osobowych, jak i urządzeń technicznych. Można, zatem wyróżnić obronę kontrdezinformacyjną osobową i nieosobową (techniczną).**

Osobową obronę kontrdezinformacyjną należy ściśle zsynchronizować z ochroną kontrwywiadowczą[63] i skupiać na:

- zachowaniu czujności i realizacji przedsięwzięć w sztabach i w wojskach związku operacyjnego w celu zapobiegania obcej działalności wywiadowczej (akcjom sabotażowym, dywersyjnym itp.);
- niedopuszczaniu do sytuacji, w której człowiek utraci wolę walki i podda się depresji.

Osobowa obrona kontrdezinformacyjna[64] powinna obejmować zespół przedsięwzięć i działań mających na celu zachowanie czujności wobec działalności wywiadowczej, akcji dywersyjnych i sabotażowych oraz uodparniających wojska związku operacyjnego na działania mylące przeciwnika. Innymi słowy, jej realizacja powinna polegać na niedopuszczeniu do niedoboru lub nadmiaru danych napływających z obszaru obrony związku operacyjnego. Zarówno niedobór, jak i nadmiar wpływają źle na psychikę ludzi, powodując niepokój, lęk, niepewność podejmowania decyzji. Dowódcy i sztaby znające aktualną sytuację będą miały świadomość realności pola walki. Ich orientacja co do sytuacji będzie polegała na czynnym poszukiwaniu i wykorzystaniu różnych zmian w środowisku pola walki jako nośników sygnałów informacyjnych. Posiadanie aktualnej wiedzy będzie zatem w znaczny sposób wpływać na ich dobry stan psychiczny oraz na zmniejszenie ryzyka podejmowania błędnych decyzji.

Należy mieć na uwadze, że niedobór (ograniczenie dopływu) danych może spowodować, że decydenci nie zaspokoją swoich potrzeb poznawczych. Konieczność odbioru i przetwarzania bardzo dużej liczby danych, jak również ich niedobór, może zakłócić czynności umysłowe i wywołać takie negatywne skutki, jak napięcie, lęk, zmęczenie. Postęp współczesnej cywilizacji oparty na zdobywaniu, gromadzeniu i wykorzystaniu danych wydaje się być hamowany ich nadmiarem z powodu ograniczonych możliwości percepcji człowieka. Zasadniczą rolę w tej działalności odgrywają czynniki osobowe, między innymi właśnie możliwości percepcyjne człowieka (pamięć), jego stan psychiczny, umiejętności, zdolności, doświadczenie, potrzeby. Stawianie zbyt wysokich wymagań może powodować zakłócenia obiektyw-

---

[63] Wyniki badań ochrony kontrwywiadowczej zostały przedstawione w podrozdziale 2.1.1.

[64] Nazywana jest również ochroną psychologiczną [88;97]. Jako część działań psychologicznych wchodzi w zakres zakłócania informacyjnego [24;25;66].

ne (nieosiągnięcie zakładanego celu) lub subiektywne (obniżenie zdolności działania, znużenie, nerwice). Maksymalna ilość danych, jaką otrzymuje układ (człowiek) ze wszystkich receptorów wynosi 10^9 bit/s, a uświadomionych zostaje tylko 10^2 bit/s. W cybernetyce ilość informacji oznacza ciąg sygnałów przekazywanych od nadajnika do odbiornika w kanale łączności, którego najważniejszą cechą jest zdolność przepustowa, wyrażona właśnie w liczbie bitów na sekundę. Sprawność funkcjonowania układu człowiek - komputer zależy od szybkości przepływu w tym układzie. Szybkość ta nie może przewyższać zdolności przepustowej „wejścia sensorowego" człowieka. Podobnie szybkość wprowadzania rozkazów (poleceń) nie może być wyższa niż zdolność przepustowa „wyjścia motorycznego" człowieka. W wypadku przeciążenia dodatkowymi wiadomościami mylącymi, które z reguły powstaje po przekroczeniu „zdolności przepustowej" zmysłów i układu nerwowego człowieka, trudno jest jednoznacznie odpowiedzieć na pytanie, ile tych danych człowiek może spostrzec, zrozumieć i odrzucić w określonym czasie.

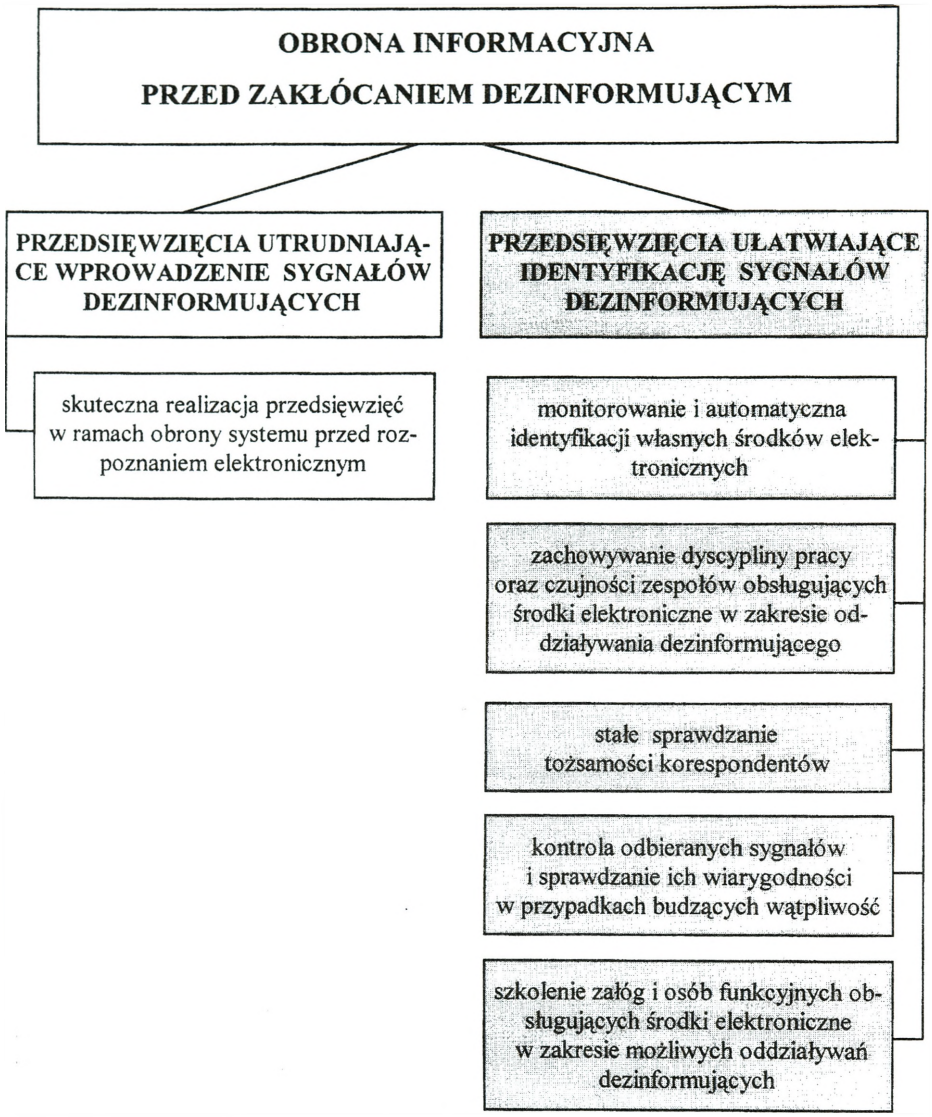
Zakres i charakter przedsięwzięć osobowej obrony kontrdezinformacyjnej – jak pokreślono wcześniej powinien być ściśle zsynchronizowany z przedsięwzięciami ochrony kontrwywiadowczej i podejmowany w działaniach obronnych związku operacyjnego w powszechnym wymiarze przez sztab i stan osobowy związku operacyjnego.

Techniczna obrona kontrdezinformacyjna[65] ma na celu wszechstronne zabezpieczenie środków elektronicznych wykorzystywanych w systemach dowodzenia i naprowadzania uzbrojenia związku operacyjnego przed wprowadzeniem fałszywych sygnałów, tj. rozkazów, zadań, sygnałów powiadamiania i ostrzegania oraz sygnałów sterujących, itp.

Z analizy sposobów prowadzenia dezinformowania technicznego wynika, że przeciwdziałanie jemu w obszarze odpowiedzialności obronnej związku operacyjnego powinno obejmować przedsięwzięcia uniemożliwiające lub utrudniające przeciwnikowi wprowadzenie wiadomości mylących, przede wszystkim do relacji łączności i kanałów radionawigacyjnych związku operacyjnego, oraz działania ułatwiające identyfikację tych danych. Zespół odpowiednio skoordynowanych przedsięwzięć w tym względzie przedstawiono na rysunku 3.7.

---

[65] Zakres i możliwości prowadzenia dezinformacji technicznej uzależnione są od sposobów organizacji przez wojska związku operacyjnego systemów elektronicznych oraz zastosowanych zabezpieczeń kryptograficznych. Zgodnie z obowiązującą teorią do zasadniczych zadań dezinformacji technicznej można zaliczyć:
- przekazywanie nieprawdziwych meldunków, rozkazów, komunikatów, sygnałów sterujących itp.;
- przeciążanie relacji łączności i kanałów radionawigacyjnych;
- utrzymywanie dowództw i sztabów w niepewności co do wiarygodności danych oraz zmuszanie do upewniania się co do wiarygodności przekazywanych danych;
- wprowadzenie chaosu i zamieszania w dowodzenie wojskami i naprowadzaniu uzbrojenia [62;101;102].



Rys. 3.7. Zakres przedsięwzięć kontrdezinformacyjnych w działaniach obronnych związku operacyjnego

Badania wykazały, że najskuteczniejszym sposobem uniemożliwiania (utrudniania) przeciwnikowi oddziaływania sygnałami dezinformacyjnymi na systemy dowodzenia i naprowadzania uzbrojenia w działaniach obronnych związku operacyjnego jest skuteczna realizacja przedsięwzięć obrony informacyjnej przed rozpoznaniem elektronicznym[66]. Przeciwnik

[66] Wyniki badań w tym zakresie zamieszczono w podrozdziale 2.2.1.

nie może wprowadzić wiadomości mylących do tych systemów i ich elementów (relacji łączności), których nie wykrył. Szczególną uwagę należy zwrócić na ograniczanie dostępności elektromagnetycznej i semantycznej bezprzewodowych urządzeń teletransmisyjnych poza obszar odpowiedzialności obronnej związku operacyjnego. Wyeliminowanie dostępności elektromagnetycznej środków łączności wyklucza praktycznie możliwość prowadzenia przez przeciwnika dezinformacji w tworzonych przez nie relacjach łączności. Jednak wyeliminowanie dostępności elektromagnetycznej wszystkich środków łączności nie jest możliwe.

Dotyczy to zwłaszcza środków zapewniających łączność z pododdziałami działającymi w głębi ugrupowania przeciwnika oraz w obszarze sił przesłaniania związku operacyjnego. Nie zawsze też można wyeliminować dostępność semantyczną z uwagi na udokumentowane historycznie „łamanie" szyfrów[67], kodów i kluczy.

Zastosowane dokumenty tajnego dowodzenia oraz techniczne urządzenia utajniające, szczególnie starszej generacji, nie zawsze mają wystarczającą moc kryptograficzną. W wielu relacjach łączności wymiana danych może być realizowana fonicznie tekstem jawnym. Dogodne warunki do prowadzenia dezinformacji będą istniały w relacjach naprowadzania lotnictwa, sterowania ogniem artylerii, naprowadzania rakiet przeciwlotniczych, ostrzegania i alarmowania, w których przekazywane są komendy (sygnały sterujące) do natychmiastowego wykonania. Dlatego też zachodzi konieczność podejmowania działań ułatwiających identyfikację sygnałów dezinformujących.

W celu zapewnienia odpowiedniej skuteczności przeciwdziałania dezinformacji technicznej przeciwnika konieczne jest monitorowanie i automatyczna identyfikacji własnych środków elektronicznych w obszarze obrony związku operacyjnego. Środki elektroniczne nowej generacji powinny być wyposażone w specjalne układy bezpieczeństwa transmisji, np. TRANSEC (ang. Transmition Security)[68] identyfikujące nadajnik (nadajniki) korespondentów na podstawie wprowadzonych do ich pamięci wzorców (np.: widma odbieranych sygnałów, jednolitego czasu operacyjnego, itp.).

Operatorzy dysponujący takimi środkami (wraz z modułami) sprawdzaliby tożsamość korespondenta tylko w wypadku negatywnego wyniku porównania z wzorcem. Zidentyfikowanie wiadomości mylącej wprowadzonej przez przeciwnika do poszczególnych relacji łączności pozwalałoby na właściwą ich interpretację. Powinno stanowić również ostrzeżenie, że relacja łączności została rozpoznana. Następnie należy zrealizować odpowiednio skuteczne

---

[67] Por.: F.W. Winterbotham, „The Ultra Secret", London 1974.

[68] Są to standardowe moduły stosowane w NATO, co pozwala na wymianę radiową pomiędzy partnerami Sojuszu [14].

przedsięwzięcia obrony przed rozpoznaniem elektronicznym przeciwnika, a rozpoznane relacje łączności wykorzystać do pozorowania lub zaniechać w nich dalszej pracy.

Pozostałe przedsięwzięcia (rysunek 3.7.) mające na celu identyfikację sygnałów mylących przeciwnika mają charakter organizacyjny i powinny polegać na:

- zachowywaniu dyscypliny pracy oraz czujności zespołów, obsługujących środki elektroniczne w zakresie oddziaływania dezinformującego;
- stałym sprawdzaniu tożsamości korespondentów;
- kontroli odbieranych sygnałów i sprawdzaniu ich wiarygodności w przypadkach budzących wątpliwość;
- szkoleniu załóg i osób funkcyjnych, obsługujących środki elektroniczne, w zakresie możliwych oddziaływań dezinformujących.

Powyższe działania mogą okazać się w niektórych sytuacjach mało skuteczne. Sytuacje takie mogą występować zwłaszcza w relacjach współdziałania, dowodzenia lotnictwem, sterowania środkami rażenia oraz w innych – podczas przekazywania komend (sygnałów) wymagających natychmiastowej reakcji. W wypadku blokowania przez przeciwnika relacji radiowych przez długotrwałe nadawanie na ich częstotliwościach roboczych różnorodnych sygnałów konieczne może się okazać zastosowanie przedsięwzięć typowych dla obrony przed zakłóceniami celowymi[69].

Analiza ćwiczeń wojsk łączności[70] dowodzi, że obrona kontrdezinformacyjna traktowana jest często formalnie lub całkowicie pomijana w procesie szkolenia wojsk, a niekiedy również podczas organizacji maskowania radioelektronicznego w działaniach obronnych związku operacyjnego. Jest to zjawisko bardzo niebezpieczne, ponieważ skuteczność przeciwdziałania dezinformacji technicznej zależy w wielu wypadkach od nawyków operatorów, załóg środków łączności, a nawyki można wyrobić tylko w procesie systematycznego, długotrwałego szkolenia. Ważne jest, by w trakcie szkolenia zwrócić uwagę, że cykl oddziaływania dezinformującego rozpoczyna się skrytym włączaniem radiostacji przeciwnika do czynnej sieci łączności w działaniach obronnych związku operacyjnego. Scenariusz takiego cyklu może obejmować:

- utożsamianie się i przejęcie roli jednej z radiostacji sieci, najczęściej tej, która z różnych powodów nie zgłasza się lub okresowo „wyszła" z sieci;
- wejście do sieci po kolejnej zmianie częstotliwości roboczej, jeśli nie zgłosiły się wszystkie podległe radiostacje;
- włączenie się do sieci kryptonimem radiostacji wyższego szczebla;
- zgłoszenie się w sieci jako nowy korespondent.

---

[69] Problematyka ta została przedstawiona w podrozdziale 3.1.1.

[70] Autor był kierownikiem zespołu kontroli radioelektronicznej i dywersji radiowej podczas ćwiczeń z wojskami łączności organizowanymi w WSOWŁ w latach 1990 – 1995.

Należy mieć na uwadze, że podstawowym warunkiem dywersyjnego, nie zauważonego przeniknięcia do danej relacji radiowej związku operacyjnego jest jej wcześniejszy dokładny nasłuch.

3.3. Obrona informacyjna przed zakłócaniem niszczącym

Doświadczenia ze współczesnych konfliktów i wojen lokalnych oraz ćwiczeń prowadzonych z wojskami, a także tendencje rozwojowe środków walki sygnalizują skalę zagrożeń w stosunku do poszczególnych uczestników przyszłego pola walki. Trwałe i ciągłe dowodzenie wojskami i naprowadzanie uzbrojenia w znacznej mierze uzależnione jest od żywotności poszczególnych ich komponentów. Mogą one być obiektami szczególnego zainteresowania potencjalnego przeciwnika w działaniach obronnych związku operacyjnego, gdyż są opłacalnymi i dogodnymi celami[71] rozpoznania, ataku i niszczenia środkami rażenia.

Należy liczyć się zatem z możliwością oddziaływania zakłócania niszczącego na systemy dowodzenia i naprowadzania uzbrojenia związku operacyjnego. Elementy funkcjonalne i techniczne tych systemów mogą być celem **ataku i niszczenia kinetycznego** środkami broni precyzyjnego rażenia o zwiększonej sile działania i dokładności rażenia[72]. Elementy te mogą być także obiektami **ataku i niszczenia elektromagnetycznego** przeciwnika za pomocą broni energii bezpośredniej[73].

---

[71] Problematyka ta była przedmiotem rozważań autora w opracowaniu: „Model ocenowy odporności sieci łączności radioliniowo-przewodowej związku taktycznego na oddziaływanie ogniowe i radioelektroniczne". Praca naukowo - badawcza, wyd. WIŁ, Zegrze 1997, współautorzy: A. Barczak., K. Mamcarz.

[72] Tempo rozwoju współczesnych technologii może spowodować, że już niebawem każdy rodzaj broni będzie posiadał wszystkie cechy broni precyzyjnego rażenia [55;129;133].

[73] Od dłuższego czasu trwają prace nad bronią energii bezpośredniej, które mogą doprowadzić do uzyskania „broni idealnej" zdolnej do zniszczenia każdego celu. Prace te koncentrują się na:

– **broni laserowej**, tj. działach opartych na laserach małej (1 kW), średniej (40 kW) i dużej (powyżej 400 kW) mocy zdolnych do niszczenia celów przez „oślepianie" załóg i urządzeń czujnikowych wskutek zapalenia lub wypalenia otworów w obudowie i aparaturze wewnętrznej. Prace nad tą bronią są najbardziej zaawansowane.

– **broni wiązkowej cząstek elementarnych**, gdzie nośnikiem energii są naładowane lub neutralne cząsteczki. Działa akceleratorowe, niszczące cele mechanicznie i promieniowaniem wtórnym mogą okazać się skuteczniejsze od broni laserowej. Cząsteczki elementarne przenikają w bardzo krótkim czasie (w przeciwieństwie do lasera) przez obudowę urządzeń, powodując uszkodzenie układów elektronicznych, eksplozję ładunków wybuchowych głowic lub zapłon paliwa napędowego.

– **broni fal elektromagnetycznych**, tj. broni mikrofalowej, generatorów (dział) impulsu elektromagnetycznego oraz broni modulowanych sygnałów impulsowych. Broń mikrofalowa może zakłócać pracę urządzeń radioelektronicznych (radiowych, radiolokacyjnych), podobnie jak czynią to współczesne środki walki elektronicznej, tylko przy zastosowaniu ogromnych mocy promieniowania (tysiące razy większej). Emitowane silne sygnały zakłócające mogą dodatkowo niszczyć układy elektroniczne, zasoby informatyczne, a także inne mechanizmy środków bojowych w wyniku ich przegrzewania. Broń ta stanowić ma superśrodek zakłócający, przystosowany również do zwalczania celów wykonanych w technice „stealth". Generatory impulsu elektromagnetycznego, oparte na konwencjonalnej technice wybuchowej mogą być wykorzystane do zakłócania, powodowania uszkodzeń, lub niszczenia środków łączności, komputerów, czułych elementów sterowania siecią energetyczną, itp. Dobór parametrów generatorów ma zapewnić selektywne oddziaływanie na określony rodzaj urządzeń. Broń modulowanych sygnałów impulsowych (odpowiednio dobranych co do częstotliwości, kształtu, czasu narastania i czasu trwania) jest przeznaczona do zaburzeń pracy poszczególnych organów ludzkich, np. pracy mózgu, serca, nerek, paraliż, przegrzewanie stawów. Broń ta może być zaliczona do broni masowego rażenia [62;129;133].

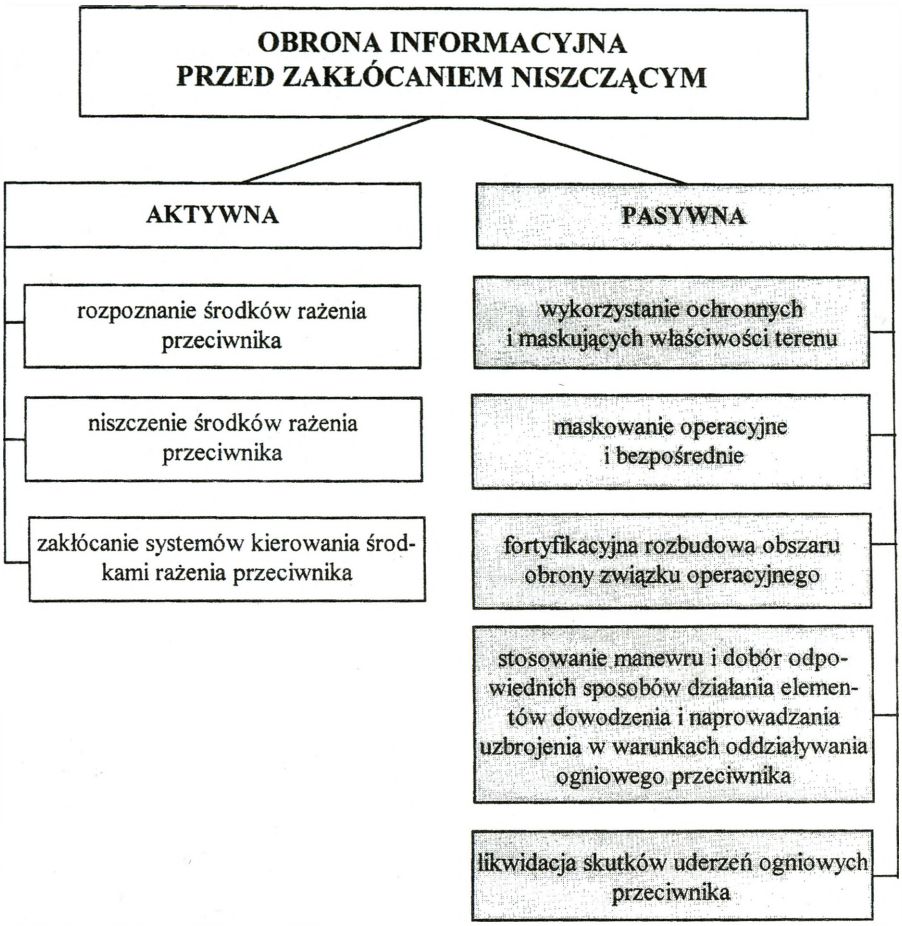
Użycie poszczególnych rodzajów broni pozostawać będzie zależało od sytuacji operacyjnej, będzie także dostosowane do różnych obiektów w celu uzyskania maksymalnych efektów. Obiektami oddziaływania niszczącego są elementy ugrupowania obronnego związku operacyjnego przede wszystkim w obszarze jego działań bezpośrednich, a wśród nich stanowiska dowodzenia, węzły łączności, posterunki oraz stacje radiolokacyjne wykorzystywane do wykrywania oraz śledzenia celów powietrznych i in.

Z badań wynika, **że obrona informacyjna przed zakłócaniem niszczącym w działaniach obronnych związku operacyjnego powinna obejmować odpowiednie przedsięwzięcia aktywne i pasywne w celu zachowania żywotności wojsk oraz ich systemów dowodzenia i naprowadzania uzbrojenia na polu walki** (rysunek 3.8.).

W **aktywnej obronie informacyjnej przed zakłócaniem niszczącym** należy skoncentrować wysiłek na rozpoznaniu i niszczeniu środków rażenia przeciwnika oraz na zakłócaniu tych urządzeń elektronicznych systemów naprowadzania uzbrojenia przeciwnika, które są najbardziej wrażliwe na sygnały zagłuszające.

Problematyka rozpoznania i niszczenia środków rażenia przeciwnika, chociaż dotyczy systemów dowodzenia i naprowadzania uzbrojenia, wykracza poza nakreślone ramy pracy studyjnej i jest przedmiotem badań szczegółowych innych specjalistów. Wielu spośród nich sądzi, że wysiłek uderzeniowy, szczególnie lotnictwa przeciwnika, będzie skierowany przede wszystkim na niszczenie posterunków radiolokacyjnych, stacji radiolokacyjnych wykrywania i śledzenia celów powietrznych, urządzeń radionawigacyjnych oraz stacji radiolokacyjnych naprowadzania rakiet i sterowania ogniem artylerii przeciwlotniczej, a następnie na stanowiska dowodzenia i węzły łączności związku operacyjnego.

Ze względu na możliwość powszechnego stosowana przez przeciwnika pocisków rakietowych do niszczenia głównych obiektów związku operacyjnego i ich obiektów elektronicznych szczególną uwagę należy zwrócić na zakłócanie pracy systemów naprowadzania uzbrojenia.



Rys. 3.8. Obrona informacyjna przed zakłócaniem niszczącym w działaniach obronnych związku operacyjnego

Ocena wykorzystywanych systemów naprowadzania rakiet [3;62;136] wykazuje, że obecnie możliwe jest zakłócanie[74] nieautonomicznych i kombinowanych (częściowo automatycznych) systemów naprowadzania rakietami, ponieważ w zestaw sterowania tych rakiet wchodzą urządzenia elektroniczne, które współpracują z naziemnymi środkami elektronicznymi rozwiniętymi na określonych punktach kierowania szczebla operacyjnego i taktycznego. Konieczność elektronicznej współpracy w relacjach: „ziemia – powietrze" i „powie-

[74] W tym wypadku przedsięwzięcie to realizowane jest na korzyść obrony systemów dowodzenia i naprowadzania uzbrojenia w ramach zakłócania informacyjnego [22;24;25].

trze – ziemia" czyni wszystkie te urządzenia wrażliwymi na rozpoznanie i zakłócanie elektroniczne.

Z przeprowadzonych analiz [62] wynika, że obecnie niemożliwe jest zakłócanie elektroniczne autonomicznych, najczęściej z góry zaprogramowanych systemów naprowadzania rakiet. W systemach tych program lotu rakiet ustala się przed ich wystrzeleniem i steruje za pomocą urządzeń znajdujących się na ich pokładach, niezależnie od ośrodków naziemnych. Dzięki temu są one niewrażliwe na zakłócania elektroniczne wytwarzane z zewnątrz (przez fałszywy cel lub pułapki radiolokacyjne z ziemi albo z pokładu samolotu). Istnieje jednak możliwość zakłócenia zbliżeniowych zapalników radiowych tych rakiet. Oddziaływanie 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, rakieta nie doleci do zaprogramowanego celu. W wypadku zakłócania zbliżeniowych zapalników radiowych rakiet należy rozmieszczać stacje zakłócające w rejonie osłanianych obiektów.

Prowadzone badania wykazują, że najkorzystniej jest obezwładniać zakłóceniami urządzenia śledzenia radiolokacyjnego, a także relacji radiowych dowodzenia i automatycznego naprowadzania (sterowania). Do zakłócania urządzeń radiolokacyjnego śledzenia można wykorzystywać naziemne lub samolotowe stacje zakłóceń radiolokacyjnych, wytwarzające zakłócenia szumowe i impulsowo – odzewowe.

Zakłócenia urządzeń systemów śledzenia rakiet klasy „powietrze – ziemia" mogą się odbywać w strefie radiolokacyjnej widzialności i poza nią. Można założyć, że jeśli rakieta jest śledzona radiolokacyjnie i sterowana na całej trasie lotu, to zakłócenie urządzenia śledzącego, np. samolotu nosiciela rakiety przeciwnika jest możliwe na całej trasie jego lotu, tj. od rubieży startu rakiety (pocisku kierowanego) do rubieży jej naprowadzania na obiekt naziemny.

Środki śledzenia radiolokacyjnego rakiet klasy „ziemia – ziemia" można skutecznie obezwładniać za pomocą samolotowych stacji zakłócających, odznaczających się dużą mocą zakłóceń. Zakłócanie może być przeprowadzone na trasach lotu rakiet w całej strefie śledzenia stacji radiolokacyjnej.

Do zakłócania niszczącego elementów elektronicznych zarówno systemów dowodzenia, jak i naprowadzania uzbrojenia (systemów termowizyjnych, czujników laserowych, i in.)

można będzie w przyszłości wykorzystać bomby impulsu elektromagnetycznego bądź urządzenia mikrofalowe o dużej gęstości mocy (lasery)[75].

W **pasywnej obronie informacyjnej przed zakłócaniem niszczącym** w działaniach obronnych związku operacyjnego wysiłek należy skierować (rysunek 3.8.) na: wszechstronne wykorzystanie ochronnych właściwości terenu; realizację przedsięwzięć maskowania operacyjnego i bezpośredniego; systematyczną rozbudowę fortyfikacyjną; dobór odpowiednich sposobów działania elementów dowodzenia i naprowadzania uzbrojenia w warunkach rażenia środkami ogniowymi przeciwnika, a także likwidację skutków uderzeń ogniowych.

Najprostszym sposobem obrony elementów systemów dowodzenia i naprowadzania uzbrojenia przed zakłócaniem niszczącym jest umiejętne wykorzystanie ochronnych i maskujących właściwości terenu w obszarze odpowiedzialności obronnej związku operacyjnego. Przedsięwzięcie to powinno być realizowane według zasad obowiązujących w maskowaniu operacyjnym i bezpośrednim[76]. Umiejętna realizacja przedsięwzięć w tym zakresie pozwala zmniejszyć rezultaty rozpoznania oraz skutki niszczenia ogniowego przeciwnika tych elementów o 20 – 30% i więcej [41;42;118].

Fortyfikacyjna rozbudowa obszaru obrony związku operacyjnego[77] jest jedną z podstawowych form obrony elementów systemów dowodzenia i naprowadzania uzbrojenia przed oddziaływaniem środków rażenia przeciwnika. W toku realizacji tego przedsięwzięcia należy uwzględnić również wykorzystanie istniejącej infrastruktury, zwłaszcza zabudowań w aglomeracjach miejskich i rejonach zurbanizowanych. W nowoczesnym budownictwie przemysłowym stosuje się bowiem konstrukcje stalowe lub żelbetowe, odporniejsze na oddziaływanie środków ogniowych, a dachy pokryte blachą stanowią trwałą zasłonę przed promieniowaniem elektromagnetycznym lub – odpowiednio wykorzystane – są naturalnymi reflektorami eliminującymi sygnały zakłócające przeciwnika. Powierzchnie wysokich budynków tworzą tzw. cienie radiolokacyjne, w których zasięgu opromieniowanie radiolokacyjne nie jest skuteczne.

Ważnym przedsięwzięciem obrony pasywnej jest stosowanie manewru oraz dobór odpowiednich sposobów działania elementów dowodzenia i naprowadzania uzbrojenia w warunkach oddziaływania ogniowego przeciwnika, do których można zaliczyć:

---

[75] Problematyka ta jest przedmiotem badań szczegółowych wielu specjalistów [27;118], w tym i autora niniejszej pracy studyjnej [55;56].

[76] Wyniki badań w tym zakresie zostały przedstawione w podrozdziałach: 2.1.2. i 2.2.1.

[77] Rozbudowa fortyfikacyjna prowadzona jest w ramach zabezpieczenia inżynieryjnego. Przewiduje się prace pierwszej, drugiej i następnej kolejności. „Regulamin działań wojsk lądowych", wyd. DWLąd, Warszawa 1999, s. 233.

– rozśrodkowanie;

– dublowanie obiektów dowodzenia (systemów łączności oraz innych systemów radioelektronicznych);

– osłonę radioelektroniczną ważniejszych elementów ugrupowania obronnego (m in. stanowisk dowodzenia) związku operacyjnego;

– okresową zmianę rejonów rozmieszczenia;

– wyprowadzanie wojsk i obiektów z rejonów uderzeń.

Wyszczególnione działania powinny być realizowane przy uwzględnieniu i wykorzystaniu ochronnych oraz maskujących właściwości terenu. W rejonach operacyjnego rozwinięcia poszczególne elementy ugrupowania obronnego związku operacyjnego, a także urządzenia i środki techniczne powinny być rozśrodkowane w taki sposób, aby przede wszystkim zapewnić wymagane warunki bezpieczeństwa oraz możliwość ciągłego dowodzenia nimi, sprawnego współdziałania i wykonania manewru wewnątrz zajmowanego rejonu lub po wcześniej zaplanowanych drogach. Każde rozśrodkowanie powinno przebiegać sprawnie, niezależnie od warunków i sytuacji. Uwzględniając możliwości systemów broni precyzyjnego rażenia, należy przy rozśrodkowaniu elementów dowodzenia związku operacyjnego w rejonach wyjściowych (ześrodkowania), a także w czasie marszu utrzymywać odstęp 1 – 1,5 km między pododdziałami i 100 – 200 metrów pomiędzy wozami bojowymi i pojazdami.

Rozśrodkowanie w odniesieniu do stanowisk i punktów dowodzenia związku operacyjnego powinno uwzględniać specyfikę wykorzystania wojsk oraz środków elektronicznych. Polega ono na:

– rozwijaniu środków emitujących energię elektromagnetyczną poza rejonami rozmieszczenia tych stanowisk;

– zmniejszeniu liczby aparatowni na stanowiskach i punktach dowodzenia;

– stosowaniu nieliniowego sposobu rozmieszczania elementów węzłów łączności;

– maksymalnym odsuwaniu anten od nadajników.

W rejonie jednego węzła łączności związku operacyjnego należy poszczególne aparatownie rozmieszczać w sposób gniazdowy, po 3 – 4 w „gnieździe". Odległość między nimi powinna wynosić 10 – 15 m, między „gniazdami" 50 – 70 m, między grupami 200 – 300 m. Taki sposób rozmieszczenia wyklucza możliwość porażenia dwóch grup jednym pociskiem kasetowym małej mocy o promieniu rażenia nie większym niż 200 m. Środki wypromieniowujące energię elektromagnetyczną, pracujące w grupach aparatowni teletransmisyjnych (np. stacje radioliniowe) należy rozmieszczać w odległości nie mniejszej niż 400 – 600 m od apa-

ratowni komutacyjnych. Odległość między środkami wypromieniowującymi tę energię powinna wynosić 800 – 1000 m. Takie oddalenie wyklucza możliwość jednoczesnego ich porażenia jednym pociskiem kasetowym. Poza tym należy maksymalnie odsuwać anteny od nadajników oraz wyposażyć je w komplety rezerwowe. Rozmieszczenie poszczególnych elementów węzłów łączności w sposób rozśrodkowany oraz rozwinięcie środków nadawczych poza stanowiskami dowodzenia (grup nadajników na szczeblu związku operacyjnego 3 – 5 km, związku taktycznego 1 – 3 km, oddziału 1 – 1,5 km) powinno zapewnić ich ochronę przed środkami rażenia i rozpoznania przeciwnika. Natomiast nieliniowe rozmieszczenie elementów węzła łączności w połączeniu z przedsięwzięciami maskowania i pozorowania przyczyni się do zmniejszenia prawdopodobieństwa ich rażenia do 10 – 20 %.

Ważnym przedsięwzięciem obrony informacyjnej przed zakłócaniem niszczącym, szczególnie w czasie działań obronnych związku operacyjnego jest dublowanie obiektów dowodzenia, elementów systemów łączności oraz innych systemów elektronicznych (zwłaszcza rozpoznania i obrony przeciwlotniczej). W tym celu należy przewidzieć tworzenie i wykorzystanie obiektów zapasowych (np. zapasowych systemów i stacji radiolokacyjnych), aby w razie zniszczenia jednego z nich drugi mógł go zastąpić. Bardzo korzystne jest dublowanie kablowych linii łączności liniami bezprzewodowymi (radiowymi, radioliniowymi, radiotelefonicznymi). Podwyższa ono zdecydowanie odporność systemu łączności na ogniowe oddziaływanie przeciwnika. Żywotność systemów dowodzenia w działaniach obronnych związku operacyjnego można przedłużyć wykorzystując odpowiednią ilość środków elektronicznych do zdublowania stanowisk dowodzenia oraz odpowiednio weryfikując dyslokację miejsc pracy osób funkcyjnych. Podobnie powinny być rozwiązywane problemy dublowania w systemach rozpoznania i obrony przeciwlotniczej, gdyż ich elementy są celami pierwszej kolejności rażenia bronią precyzyjnego rażenia.

Ważniejsze elementy ugrupowania obronnego związku operacyjnego, m. in. stanowiska dowodzenia powinny być osłaniane radioelektroniczne przed rozpoznaniem i niszczeniem bronią precyzyjnego rażenia. Z analizy zasad bojowego wykorzystania pododdziałów zakłóceń radiolokacyjnych wynika, że mogą one prowadzić:

– osłonę zgrupowania uderzeniowego – wokół osłanianego elementu ugrupowania operacyjnego, gdzie stacje rozmieszcza się co 8 – 10 km naokoło;

– osłonę obiektową, gdzie stacje rozmieszcza się nie dalej niż 4 – 6 km od obiektu na kierunku przewidywanego nalotu lotnictwa przeciwnika;

– osłonę strefową, gdzie strefę (linię) od strefy (linii) oddala się na odległość 20 – 25 km, a stacje w strefie rozmieszcza się co 8 – 10 km;

– osłonę strefowo – obiektową, gdzie wykorzystuje się kombinowany sposób osłony.

Skutecznym sposobem obrony przed oddziaływaniem niszczącym może być wykonywanie nieoczekiwanego manewru elementami ugrupowania operacyjnego, ich stanowiskami dowodzenia (węzłami łączności) oraz obiektami techniczno-specjalnymi. Określając odległość przesunięcia (okresowej zmiany rejonów rozmieszczenia), należy uwzględnić wielkość powierzchni rozpoznania i rażenia danym systemem broni precyzyjnego rażenia, tak aby zapewnić odpowiednie ukrycie elementów ugrupowania lub obiektu. Manewr ten najlepiej wykonywać jest w nocy lub w innych warunkach ograniczonej widoczności z wykorzystaniem tzw. cieni radiolokacyjnych. Przemieszczanie stanowisk dowodzenia i innych obiektów powinno odbywać się zespołami (grupami środków), przy zachowaniu odległości między kolumnami 2 – 3 km. Kolumny powinny przemieszczać się grupami, po 3 – 4 środki w każdej grupie, zachowując odległości między nimi 100 – 150 m, a między środkami w grupie – do 70 m. Stanowiska dowodzenia związku operacyjnego, podległych związków taktycznych i oddziałów powinny być przegrupowywane, jeśli jest to możliwe, po kilku drogach. Należy unikać wyboru długich odcinków prostoliniowych, dobrze widocznych z dużej odległości. Na drogach marszu powinna znajdować się mała liczba możliwie krótkich odcinków odkrytych pod względem radiolokacyjnym. Większa liczba (do 10) odkrytych odcinków może kilkakrotnie powiększyć straty w sprzęcie. Odkryte odcinki drogi powinno się pokonywać z większą prędkością, przy zachowaniu odległości między pojazdami 100 – 150 m. Zwiększając prędkość marszu z 20 do 70 km/h, można zmniejszyć straty od kilku do kilkunastu razy. Natomiast w strefach cieni radiolokacyjnych pojazdy powinny poruszać się z prędkością 20 – 30 km/h, z zachowaniem odległości między nimi równej 30 – 50 m.

Z manewrem (okresową zmianą rejonów ześrodkowania) związane jest wyprowadzanie elementów z rejonów uderzeń. Przedsięwzięcia tego rodzaju powinny być realizowane przede wszystkim przez te obiekty, które zostały rozpoznane, lub co do których istnieje przypuszczenie, że ich położenie jest znane przeciwnikowi. Wyprowadzenie ich z rejonów uderzeń bronią precyzyjnego rażenia należy realizować przy ścisłym przestrzeganiu zasad maskowania i wykorzystaniu maskujących właściwości terenu, zwłaszcza tzw. cienia radiolokacyjnego oraz w warunkach ograniczonej widoczności. Odległość nowego rejonu powinna być dostosowana do powierzchni pola rozpoznania stacji radiolokacyjnej pracującej w trybie rozpoznania szczegółowego. Wyprowadzanie elementów systemów dowodzenia i naprowadza-

nia uzbrojenia z rejonów uderzeń ogniowych będzie zależeć również od czasu potrzebnego na zwijanie elementów ugrupowania bojowego w rejonie zajmowanym dotychczas. W każdej sytuacji działanie to powinno być na tyle racjonalne, aby nie doprowadziło do naruszenia ciągłości dowodzenia oraz systemu ognia. Szczególne znaczenie ma odpowiedni wybór i zamaskowanie dróg marszu oraz zamaskowanie i rozbudowa inżynieryjna rejonów zapasowych. Kierując się potrzebami zachowania ciągłości dowodzenia, celowe jest uprzednie zorganizowanie kablowych linii łączności do rejonów zapasowych. Poza tym trzeba najpierw wyprowadzić te elementy, które bezpośrednio wpływają na utrzymanie ciągłości działania, a następnie pozostałe. Opuszczone rejony należy wykorzystać jako rejony pozorne. Realizacja przedsięwzięć w ramach wyprowadzania elementów systemu dowodzenia i naprowadzania uzbrojenia spod uderzeń broni precyzyjnego rażenia pozwala, w dogodnych warunkach, zmniejszyć straty o 75% i więcej.

Zakres zasadniczych działań mających na celu odtwarzanie zdolności bojowej i likwidacje skutków uderzeń ogniowych powinien obejmować:

- odtworzenie naruszonego systemu dowodzenia i naprowadzania uzbrojenia;
- ustalenie skutków użycia broni precyzyjnego rażenia (rozpoznanie rejonów uderzeń);
- sprecyzowanie zadań dla tych sił, które nie utraciły zdolności bojowej;
- realizację przedsięwzięć ratunkowo-ewakuacyjnych;
- ustalenie możliwości i warunków przebywania wojsk w dotychczas zajmowanych rejonach oraz wykonania przez nie zadań bojowych;
- rozpoznanie dróg manewru oraz przegrupowanie części sił i środków;
- uzupełnianie stanów osobowych, sprzętu i środków materiałowych.

Elementy dowodzenia i naprowadzania uzbrojenia związku operacyjnego powinny odtwarzać zdolność bojową – w zasadzie przy wykorzystaniu ocalałych sił i środków – bezpośrednio po wykonaniu uderzenia, bez oczekiwania na zarządzenie szczebla nadrzędnego. Innym sposobem odtworzenia zdolności bojowej może być uzupełnienie tych elementów zapasowymi środkami materiałowymi, sprzętem specjalistycznym oraz stanem osobowym. Celowe jest zatem posiadanie odwodu (rezerwowych środków) w związku operacyjnym i wykorzystywanie go w sytuacjach krytycznych.

Ważnym czynnikiem, który może ograniczyć skutki uderzeń ogniowych, będzie terminowe powiadamianie o zagrożeniu ich użyciem. Terminowość powiadamiania o zagrożeniu zależy od jakości i dokładności rozpoznania prowadzonego kompleksowo przez wszystkie szczeble dowodzenia, własnymi siłami i środkami. Powiadamianie powinno odbywać się

w związku operacyjnym w specjalnie zorganizowanych do tego celu sieciach powiadamiania (relacjach łączności). Ponadto w wojskach związku operacyjnego – na podstawie sygnałów uzyskanych z sieci powiadamiania oraz z własnych źródeł – powinno być organizowane i prowadzone ostrzeganie oddziałów o zagrożeniu z powietrza. Ważną rolę w powiadamianiu i ostrzeganiu powinny odgrywać jednostki dowodzenia organizujące odpowiednie relacje łączności.

3.4. Zabezpieczenie systemów dowodzenia i naprowadzania uzbrojenia związku operacyjnego przed niekompatybilnością elektromagnetyczną

Zabezpieczenie systemów dowodzenia i naprowadzania uzbrojenia przed niekompatybilnością elektromagnetyczną w działaniach obronnych związku operacyjnego jest ważnym przedsięwzięciem w zakresie zabezpieczenia trwałości i stabilności pracy wchodzących w ich skład komponentów. Problematyka ta – sygnalizowana dotąd w ramach zapewnienia kompatybilności elektromagnetycznej[78] poszczególnych systemów radioelektronicznych powinna znaleźć odzwierciedlenie również w obronie informacyjnej związku operacyjnego. Tym mianem określa się prawidłową koegzystencję systemów elektronicznych i ich elementów w środowisku elektromagnetycznym. W środowisku tym mogą występować szkodliwe i niepożądane zjawiska zakłóceń interferencyjnych (wzajemnych) zarówno zewnętrznych, jak i wewnętrznych. Z badań wynika, że do głównych przyczyn powstawania zakłóceń interferencyjnych (wzajemnych) w działaniach obronnych związku operacyjnego można zaliczyć:

- masowe użycie urządzeń elektronicznych;
- ograniczoną pojemność i nierównomierne wykorzystanie widma częstotliwości;
- wzrost potencjału energetycznego urządzeń nadawczych;
- wzrost czułości urządzeń odbiorczych;
- niestabilność częstotliwości;
- niedoskonałość innych cech technicznych środków elektronicznych;
- niewłaściwe rozmieszczenie środków elektronicznych w terenie.

[78] Kompatybilność elektromagnetyczna – to zdolność zapewniająca prawidłowe funkcjonowanie środków elektronicznych (z założoną jakością) w otaczającym środowisku elektromagnetycznym, bez wywierania szkodliwego wpływu na to środowisko [55;56;110].

Masowe użycie urządzeń elektronicznych wynika z wysokiego stopnia nasycenia wojsk różnorodnymi środkami elektronicznymi[79]. Do środków tych należą: stacje radiolokacyjne, radiostacje, radiotelefony, stacje radioliniowe i troposferyczne, stacje zakłóceń, namierniki, urządzenia odbiorcze itp. Duża liczba tych środków dowodzenia w związku operacyjnym oraz gęstość ich rozmieszczenia w ugrupowaniu bojowym, a także prawdopodobieństwo jednoczesnej pracy, stanowi jedną z poważniejszych przyczyn występowania zakłóceń interferencyjnych (wzajemnych).

Ograniczona pojemność i nierównomierne wykorzystanie widma częstotliwości wynika z nienasyconych potrzeb zagospodarowania całego pasma przez potencjalnych użytkowników środków elektronicznych. Często zachodzi bowiem konieczność kilkakrotnego używania tych samych częstotliwości przez różne urządzenia elektroniczne. Z widma częstotliwości natomiast wykorzystuje się w całości i bardzo nierównomiernie pasmo od 10 kHz do 40 GHz. Stanowi to przesłankę występowania zakłóceń interferencyjnych (wzajemnych).

Wzrost potencjału energetycznego urządzeń nadawczych i wzrost czułości urządzeń odbiorczych to wynik założonych oczekiwań zwiększenia zasięgu emisji elektromagnetycznej. Współczesne układy nadawcze urządzeń elektronicznych mogą emitować dziesiątki i setki kilowatów mocy podczas pracy ciągłej i impulsowej, przy bardzo dużych współczynnikach zysku kierunkowego anten.

Zwiększenie potencjału energetycznego układów nadawczych i czułości urządzeń odbiorczych, z jednej strony prowadzi do zwiększenia zasięgu i niezawodności, z drugiej zaś – zwiększa obszar, w którym urządzenia elektroniczne mogą się wzajemnie zakłócać.

Niestabilność częstotliwości roboczych i niedoskonałość innych charakterystyk technicznych objawia się oddziaływaniem promieniowania niepożądanego (pozapasmowego, bocznego) jednych urządzeń na podstawowy kanał odbiorczy innych urządzeń. Promieniowanie pozapasmowe (na częstotliwościach harmonicznych) urządzeń nadawczych jest zbędne i szkodliwe, ponieważ zakłóca urządzenia odbiorcze. Poziom zaś emisji niepożądanych zależy od rodzaju i parametrów urządzeń elektronicznych, typu generatorów i rodzaju modulacji oraz obecności filtrów na wyjściu układów nadawczych (moc emisji na częstotliwościach harmonicznych w niektórych urządzeniach nadawczych jest tylko o 20 – 30 dB mniejsza od częstotliwości podstawowej). Boczne kanały urządzeń odbiorczych nie są wykorzystywane do emisji sygnałów użytecznych, jedynie pogarszają selektywność, ponieważ ich czułość jest

[79] Szacuje się, że tylko w rejonie obrony jednego związku taktycznego może być rozmieszczonych około 14000 różnorodnych źródeł promieniujących energię elektromagnetyczną [4].

kilkadziesiąt decybeli mniejsza od czułości kanału podstawowego. Wysokie poziomy sygnałów bocznych i tylnych listków urządzeń antenowych, pogarszające możliwości selekcji przestrzennej, są przyczyną występowania zakłóceń interferencyjnych (wzajemnych). Istnieje bowiem możliwość zarówno emitowania, jak i odbioru zakłóceń z dowolnego kierunku.

Niewłaściwe rozmieszczenie środków elektronicznych w terenie powoduje również wzajemne zakłócenia środków. Środki radiowe, radioliniowe i radiolokacyjne o dużej mocy emisji wytwarzają wokół siebie pole elektromagnetyczne. Obecność innych urządzeń w takim obszarze powoduje natomiast występowanie zakłóceń w ich pracy, mimo iż częstotliwości robocze będą różne. Bliskie sąsiedztwo stacji zakłócających oraz środków systemu dowodzenia i naprowadzania uzbrojenia tworzy więc warunki wzajemnych zakłóceń. Niewłaściwe rozmieszczenie środków elektronicznych jest zaliczane do tzw. błędów taktycznych.

Badania wykazały[80], że **problem eliminacji zakłóceń interferencyjnych (wzajemnych) należy rozwiązywać w dwóch płaszczyznach: kompatybilności zewnętrznej (prawidłowa koegzystencja elektromagnetyczna pomiędzy poszczególnymi podsystemami elektronicznymi, a także ze źródłami zakłóceń przypadkowych[81], t.j. naturalnych i technicznych) w obszarze obrony związku operacyjnego oraz kompatybilności wewnętrznej (prawidłowa koegzystencja elektromagnetyczna obiektów jednego systemu).**

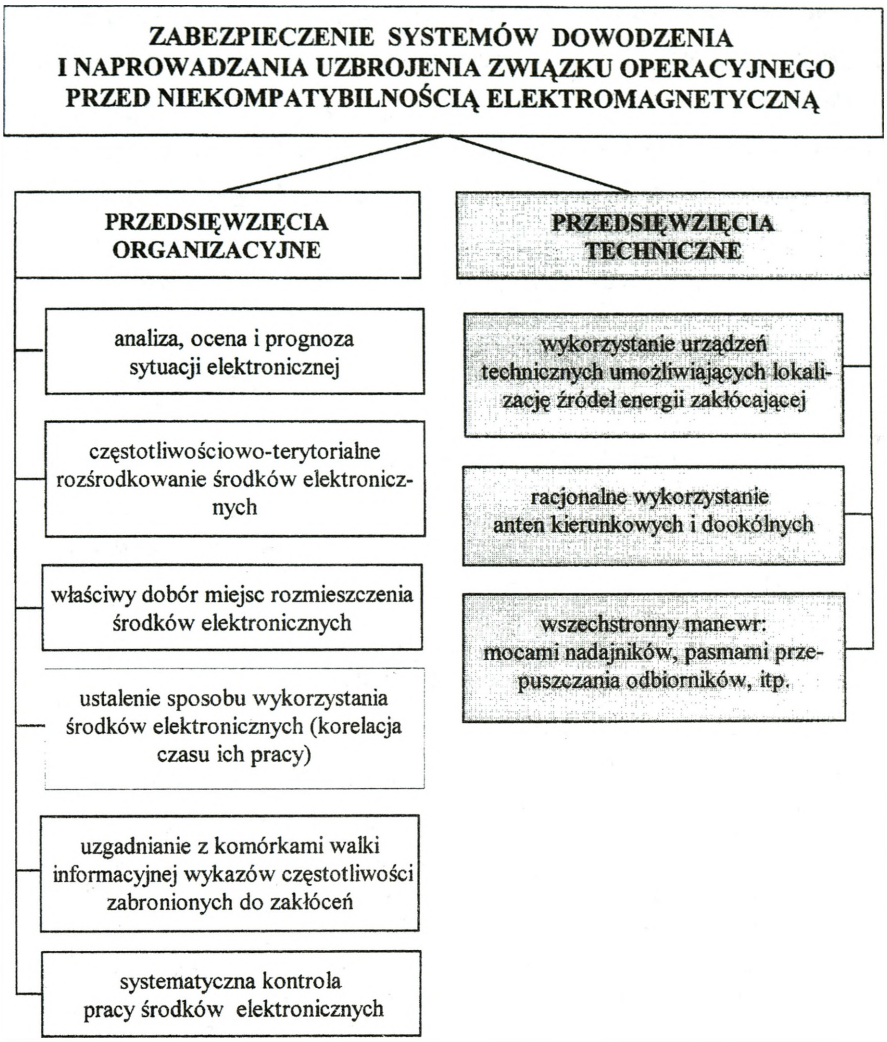
Ochrona systemów i środków elektronicznych przed zakłóceniami interferencyjnymi (wzajemnymi) powinna zmierzać do wyeliminowania lub maksymalnego zmniejszenia niepożądanego oddziaływania jednych systemów (środków) na drugie. Zdolność tę można uzyskać przez wcześniejsze uzgodnienia w zakresie wykorzystania środków i systemów elektronicznych związku operacyjnego. W tym celu należy organizować odpowiednie **przedsięwzięcia organizacyjne i techniczne** (eksploatacyjne), które powinny być skoordynowane w obszarze odpowiedzialności obronnej związku operacyjnego z przedsięwzięciami i działaniami podejmowanymi w ramach obrony antyzagłuszeniowej (podrozdział 3.1.). Zestawienie przedsięwzięć w celu zabezpieczenia związku operacyjnego przed niekompatybilnością elektromagnetyczną przedstawiono na rysunku 3.9.

Jak wynika z analizy literatury przedmiotu badań [14;43;50;58;72;110;118] **przedsięwzięcia organizacyjne** należy planować i realizować w sztabie związku operacyjnego w sposób scentralizowany.

---

[80] Treści podrozdziału zostały opracowane na podstawie badań, które zapoczątkowało opracowanie studyjne dotyczące obrony radioelektronicznej. J. Janczak, „Obrona radioelektroniczna", wyd. WSOWŁ, Zegrze 1993.

[81] Badania w tym zakresie przedstawione w podrozdziale 3.2.1.



Rys. 3.9. Zakres przedsięwzięć zabezpieczających systemy dowodzenia i naprowadzania uzbrojenia przed niekompatybilnością elektromagnetyczną w działaniach obronnych związku operacyjnego

Analiza, ocena i prognoza sytuacji elektronicznej[82] określa zakres pracy dla wykonawców – dysponentów środków elektronicznych. Prace analityczno-prognostyczne należy prowadzić począwszy od pary pojedynczych typów środków elektronicznych wchodzących w skład ugrupowania obronnego związku operacyjnego, a skończywszy na wszystkich środkach elektronicznych tego ugrupowania.

[82] Ocena sytuacji elektronicznej powinna być dokonywana podczas planowania działań obronnych związku operacyjnego w ramach elektronicznego przygotowania pola walki [21].

Analizie i ocenie powinny podlegać więc warunki wykorzystania pasma częstotliwości, propagacji elektromagnetycznej, rejonów rozmieszczenia i czasu pracy wszystkich środków elektronicznych w walce. Określane powinny być warunki optymalnego wykorzystania środków, a także ograniczenia i zastrzeżenia, co do ich wykorzystania. Ważną rolę w tym względzie odgrywa dobór częstotliwości roboczych dla środków elektronicznych, który powinien być dokonywany w celu zaspokojenia potrzeb w zakresie wykorzystania częstotliwości i umożliwiać pracę środków elektronicznych bez zakłóceń interferencyjnych (wzajemnych). Przedsięwzięcie to polega na przydzieleniu poszczególnym użytkownikom związku operacyjnego, związkom taktycznym i oddziałom limitu częstotliwości oraz wyznaczaniu częstotliwości dla konkretnych środków elektronicznych (lub określaniu, które z nich są już zajęte ze względu na właściwości konstrukcyjne sprzętu).

Rozdział częstotliwości roboczych jest zasadniczym sposobem zapewnienia kompatybilności elektromagnetycznej bezprzewodowych środków łączności i innych urządzeń elektronicznych. Należy podkreślić, że systematycznie wzrasta ranga rozdziału częstotliwości ze względu na powszechny ich deficyt, duże zagęszczenie środków elektronicznych w rejonach działania wojsk związku operacyjnego i przyległych do nich (zwłaszcza przed przednim skrajem obrony oraz w rejonach rozmieszczenia pierwszego rzutu), a także duży i trudny do przewidzenia wpływ środków i systemów elektronicznych przeciwnika na sytuację elektroniczną.

Problem rozdziału oraz zarządzania częstotliwościami roboczymi i kluczami nabrał znaczenia wraz z pojawieniem się środków elektronicznych pracujących ze skokową zmianą częstotliwości (ang. Frequency Hopping).

Istotne dla zapewnienia kompatybilności elektromagnetycznej jest częstotliwościowo – terytorialne rozśrodkowanie obiektów elektronicznych. Wybór miejsca pracy środków elektronicznych obejmuje wykorzystanie właściwości terenu (ukształtowanie, pokrycie i infrastrukturę) w celu zmniejszenia występowania zakłóceń interferencyjnych z najbardziej zagrożonych kierunków. Warunki terenowe w rejonie rozwijania środków elektronicznych mogą zmniejszać wielokrotnie gęstość mocy energii elektromagnetycznej w przestrzeni, na której są przeszkody, np. las, zabudowa, konstrukcje metalowe. Umiejętne wykorzystanie terenu pozwoli obniżyć poziom zakłóceń interferencyjnych lub całkowicie je wyeliminować. Rozwiązanie tego problemu powinno sprowadzać się do rygorystycznego przestrzegania przewidzianych dokumentami normatywnymi odległości między środkami elektronicznymi, a zwłaszcza pomiędzy radiostacjami średniej mocy i stacjami radioliniowymi, rozwijanymi

w obrębie tego samego stanowiska dowodzenia (węzła łączności) związku operacyjnego lub w sąsiednich rejonach. Odległości te powinny być nie mniejsze niż:

- między radiostacjami średniej mocy a stacjami radioliniowymi: 1500 – 2000 m;
- między stacjami radioliniowymi: 200 – 300 m;
- między radiostacjami średniej mocy HF i VHF: 300 – 400 m;
- w grupie powyżej 4 radiostacji średniej mocy: 800 – 1000 m;
- pozostałe elementy węzłów łączności powinny być rozśrodkowane z zachowaniem odstępów 50 – 70 m;
- grupy środków radiowych powinny być rozmieszczane w odległości: WŁ SD ZO 3 – 5 km i więcej; WŁ SD ZT i oddziału do 3 km; WŁ SD.

Należy przestrzegać również odpowiednich odstępów między częstotliwościami wykorzystywanymi przez różne środki elektroniczne, głównie środki łączności, które zgrupowane są niejednokrotnie w małych rejonach, na stanowiskach dowodzenia i węzłach łączności, wewnątrz wozów dowodzenia i środków walki. Wyniki badań w tym zakresie zamieszczone zostały w tabeli 3.1[83].

Wybór miejsca rozwijania środków elektronicznych powinien mieć również duże znaczenie dla eliminowania zakłóceń interferencyjnych. Idealne z punktu widzenia kompatybilności elektromagnetycznej miejsce do rozwijania środków elektronicznych powinno umożliwiać ekranowanie anteny odbiorczo – nadawczej w obszarze promieniowania niepożądanego z wykorzystaniem ekranów naturalnych oraz stwarzać korzystne warunki propagacji fal elektromagnetycznych w obszarze promieniowania pożądanego. Optymalnym miejscem rozwijania elementów systemów łączności, przede wszystkim szczebla taktycznego, są małe miejscowości.

Ze względu na niekontrolowany wpływ środków i systemów elektronicznych przeciwnika, powszechny deficyt częstotliwości, duże zagęszczenie środków elektronicznych oraz inne uwarunkowania wynikające z zasad obecnie stosowanego sposobu podziału częstotliwości, mogą występować nieprzewidziane zakłócenia kompatybilności elektromagnetycznej. Dlatego też konieczne jest ustalanie sposobu wykorzystania środków elektronicznych według częstotliwości, czasu i kierunków informacyjnych. Realizacja ww. ustaleń (przedsięwzięć) ogranicza w pewnym stopniu przepustowość systemu łączności. Powinny być podejmowane

---

[83] J. Janczak, „Obrona radioelektroniczna mobilnych systemów łączności", wyd. AON, Warszawa 1998.

zatem w ostateczności, gdy niemożliwe jest usunięcie przyczyn naruszenia kompatybilności elektromagnetycznej innymi sposobami.

Tabela 3.1.

WIELKOŚĆ
ODSTROJENIA CZĘSTOTLIWOŚCI W ZALEŻNOŚCI OD ODLEGŁOŚCI MIĘDZY WYBRANYMI ŚRODKAMI ŁĄCZNOŚCI

Odległość między środkami łączności	**Odstrojenie częstotliwości (± kHz)**						
	25 kHz	50 kHz	100 kHz	200 kHz	300 kHz	400 kHz	500 kHz
między radiostacjami (radiotelefonami) małej mocy (1 W)	350 m	125 m	65 m		25 m		
między radiostacjami pokładowymi (20 W) a radiostacjami małej mocy		300 m	125 m			25 m	
między radiostacjami pokładowymi ze wzmacniaczem (75 W) mocy a radiostacjami małej mocy		550 m	225 m	100 m			25 m

Ważnym przedsięwzięciem, eliminującym wpływ zakłóceń pochodzących od wojsk własnych, jest uzgodnienie z komórkami zakłócania informacyjnego częstotliwości zabronionych do zakłóceń[84]. Przy czym należy podkreślić, że osoby odpowiedzialne za organizację i eksploatację systemów elektronicznych powinny zabiegać o dostarczenie wykazów częstotliwości, rejonów i sektorów zabronionych do zakłóceń do odpowiednich komórek walki informacyjnej.

Ustalenie sposobów wykorzystania środków elektronicznych (korelacja czasu ich pracy) jest jednym z warunków kompatybilnej pracy środków elektronicznych w sytuacji, gdy niemożliwe jest zapewnienie odstępu częstotliwościowo–terytorialnego. Powinno polegać na rozłożeniu w różnym okresie pracy środków elektronicznych lub zakazie ich wykorzystania w określonym czasie. Należy pamiętać o tym, aby zakazem lub ograniczeniem pracy były obejmowane te środki, które w danym okresie nie są związane bezpośrednio z prowadzeniem działań bojowych lub ich wyłączenie nie wpłynie ujemnie na możliwości bojowe wojsk.

[84] Wykazy takie powinny być zamieszczone w formie apendyksów do odpowiednich aneksów.

Sprawną eliminację przyczyn naruszenia kompatybilności elektromagnetycznej można osiągnąć w wyniku systematycznej kontroli pracy środków elektronicznych i warunków propagacji fal elektromagnetycznych. Jest to podstawowe zadanie organów zarządzania systemami elektronicznymi i powinno być realizowane przez specjalistyczne komórki sztabu związku operacyjnego. Kontrola elektroniczna powinna być prowadzona w celu wykrycia i eliminowania cech demaskujących pracę własnych środków elektronicznych oraz sprawdzenia przestrzegania regulaminu i ustalonych zasad pracy. Powinna umożliwiać ponadto określenie głębokości stref rozpoznania przeciwnika i sprawdzenie skuteczności przedsięwzięć maskowania elektronicznego. Pod względem formy i treści kontrola ta powinna dzielić się na kontrolę radiową, radiotechniczną, optoelektroniczną i inną.

Kontrolę radiową należy organizować przede wszystkim w jednostkach dowodzenia związku operacyjnego. W tym celu powinny być wyznaczane zespoły oficerskie oraz odpowiednie siły i środki. W składzie węzła łączności związku operacyjnego i dywizji powinny znaleźć się (i funkcjonować) aparatownie kontroli radiowej.

Kontrola radiotechniczna i optoelektroniczna powinna być organizowana i prowadzona w związku operacyjnym, a w miarę możliwości również w dywizjach. Jej zadanie to sprawdzenie technicznych norm pracy środków elektronicznych takich, jak: stabilność częstotliwości, szerokość pasma jednej emisji, wielkość mocy sygnałów. Do tego niezbędny jest specjalistyczny sprzęt techniczny: aparatownie kontrolne i analizatory komputerowe oraz wyszkolone zespoły osób funkcyjnych. Należy mieć na uwadze, że prawdopodobieństwo naruszenia kompatybilności elektromagnetycznej, np.: w działaniach taktycznych dywizji I rzutu wynosi około 0,9999997 [118]. Jeśli uwzględni się wpływ innych środków przeciwnika i własnych oraz zakłóceń naturalnych i technicznych, to łączne prawdopodobieństwo wystąpienia naruszeń kompatybilności elektromagnetycznej będzie jeszcze wyższe. W wypadku drastycznych naruszeń kompatybilności elektromagnetycznej należy przewidzieć wyłączanie mniej ważnych środków elektronicznych lub podejmowanie innych działań.

Z badań wynika, że **przedsięwzięcia techniczne** powinny być realizowane zdecentralizowanie przez zespoły obsługujące wszystkie środki elektroniczne. W ramach działań technicznych należy przede wszystkim wyposażyć je w urządzenia umożliwiające identyfikację i lokalizację źródeł energii zakłóceniowej, poprzez ciągłe śledzenie źródeł emitujących energię elektromagnetyczną na częstotliwościach przydzielonych środkom elektronicznym. Pozostałe przedsięwzięcia techniczne mające na celu eliminację zakłóceń interferencyjnych (wzajemnych) powinny być podejmowane analogicznie do sposobu organizacji obrony antyzagłuszeniowej.

3.5. Wnioski

W wyniku przeprowadzonych badań określono zakres i treść zasadniczych przedsięwzięć obrony informacyjnej przed zakłócaniem w działaniach obronnych związku operacyjnego. Uznając, że w warunkach postępującej elektronizacji i automatyzacji pola walki jest to problem wysoce złożony wykazano, że:

1. Obrona informacyjna przed zakłócaniem w działaniach obronnych związku operacyjnego ma na celu zabezpieczenie przed zniszczeniem zbiorów własnych postaci danych i wnoszeniem do nich takich treści, które powodować mogą wzrost niewiedzy o stanie aktualnym, usytuowaniu i zamiarach działania wojsk oraz wprowadzać stan chaosu i nieuporządkowania w procesach dowodzenia i naprowadzania uzbrojenia związku operacyjnego. Ogólna struktura obrony informacyjnej przed zakłócaniem w działaniach obronnych obejmuje: obronę informacyjną przed zakłócaniem zagłuszającym, dezinformującym i niszczącym (środków rażenia), a także zabezpieczenie systemów dowodzenia i naprowadzania uzbrojenia przed niekompatybilnością elektromagnetyczną.

2. Przeciwdziałanie skutkom zakłócania zagłuszającego jest głównym zadaniem obrony informacyjnej przed zakłócaniem informacyjnym w działaniach obronnych związku operacyjnego i obejmuje zespół działań organizacyjnych i techniczno-eksploatacyjnych podejmowanych przez wszystkie elementy ugrupowania operacyjnego (bojowego) związku operacyjnego, stanowiska dowodzenia i punkty kierowania środkami rażenia dla ochrony swoich systemów dowodzenia i naprowadzania uzbrojenia przed celowym destrukcyjnym oddziaływaniem przeciwnika odpowiednio dobranymi sygnałami zakłócającymi. Zakres i charakter tych przedsięwzięć uzależniono od rodzajów środków elektronicznych, w wyniku czego wyróżniono obronę antyzagłuszeniową: systemów (sieci) łączności; systemów (sieci) teleinformatycznych; systemów radionawigacyjnych oraz systemów naprowadzania uzbrojenia.

√ Obrona antyzagłuszeniowa systemów (sieci) łączności stanowi odrębną grupę działań organizacyjnych i technicznych w celu ochrony urządzeń odbiorczych bezprzewodowych środków teletransmisyjnych przed oddziaływaniem celowych, aktywnych zakłóceń radiowych emitowanych przez środki walki informacyjnej przeciwnika. Obrona ta ma charakter pasywny, a wykonywane przedsięwzięcia powinny wchodzić w zakres obowiązków organizatora systemu łączności oraz jego bezpośrednich użytkowników.

√ Obrona antyzagłuszeniowa systemów (sieci) teleinformatycznych związku operacyjnego stanowi perspektywiczne przedsięwzięcie i nabiera coraz większego znaczenia. Ko-

nieczne staje się wprowadzenie systemowej usługi „ochrony informacji", mającej na celu zapewnienie bezpieczeństwa systemów przetwarzania i przesyłania danych na potrzeby związku operacyjnego, polegającej na przeciwstawianiu się atakom przy użyciu odpowiednich mechanizmów zabezpieczających.

√ Obronę antyzagłuszeniową systemów radionawigacyjnych przed oddziaływaniem celowych sygnałów zakłócających potencjalnego przeciwnika należy organizować analogicznie do sposobu obrony antyzagłuszeniowej systemów łączności.

√ Obrona antyzagłuszeniowa systemów naprowadzania uzbrojenia związku operacyjnego stanowi ważne przedsięwzięcie, które należy realizować wielospektralnie w ramach: maskowania, ostrzegania, zakłócania i niszczenia.

3. Obronę informacyjną przed zakłócaniem dezinformującym w działaniach obronnych związku operacyjnego należy realizować zarówno w stosunku do stanów osobowych, jak i urządzeń technicznych. Wyróżniono obronę kontrdezinformacyjną osobową i nieosobową (techniczną).

√ Osobową obronę kontrdezinformacyjną należy ściśle zsynchronizować z ochroną kontrwywiadowczą i skupiać na: zachowaniu czujności i realizacji przedsięwzięć w celu zapobiegania obcej działalności wywiadowczej (akcjom sabotażowym, dywersyjnym itp.); niedopuszczaniu do sytuacji, w której człowiek utraci wolę walki i podda się depresji.

√ Techniczna obrona kontrdezinformacyjna ma na celu wszechstronne zabezpieczenie środków elektronicznych wykorzystywanych w systemach dowodzenia i naprowadzania uzbrojenia związku operacyjnego przed wprowadzeniem fałszywych sygnałów, tj. rozkazów, zadań, sygnałów powiadamiania i ostrzegania oraz sygnałów sterujących, itp. Przeciwdziałanie jej obejmuje przedsięwzięcia uniemożliwiające lub utrudniające przeciwnikowi wprowadzenie wiadomości mylących przede wszystkim do relacji łączności i kanałów radionawigacyjnych wykorzystywanych przez wojska związku operacyjnego oraz działania ułatwiające ich identyfikację.

4. Obrona informacyjna przed zakłócaniem niszczącym w działaniach obronnych związku operacyjnego obejmuje odpowiednie działania aktywne i pasywne w celu zachowania żywotności wojsk oraz ich systemów dowodzenia i naprowadzania uzbrojenia na polu walki.

√ W aktywnej obronie informacyjnej związku operacyjnego przed zakłócaniem niszczącym wysiłek należy skoncentrować na rozpoznaniu i niszczeniu środków ogniowych przeciwnika oraz na zakłócaniu tych urządzeń elektronicznych systemów naprowadzania rakiet przeciwnika, które są najbardziej wrażliwe na sygnały zagłuszające.

√ Zasadniczą kwestią wymagającą rozwiązania przez elementy systemów dowodzenia i naprowadzania uzbrojenia związku operacyjnego w ramach działań pasywnych jest ukrywanie swoich obiektów przed rozpoznaniem satelitarnym oraz nowymi systemami radiolokacyjnymi sprzężonymi niejednokrotnie z bronią o precyzyjnym naprowadzaniu na cele. Planując rozmieszczenie wojsk i obiektów w obszarze obrony związku operacyjnego, należy uwzględnić wpływ własności terenu na ich ochronę oraz maskowanie przede wszystkim przed obserwacją boczną.

√ Główne sposoby przeciwdziałania skutkom niszczenia ogniowego przeciwnika – to: wykorzystanie nowych generacji środków maskowania (tzw. osłon termicznych, powłok pochłaniających, itp.) i imitacji, budowa odpowiednio „ożywionych" obiektów pozornych, osłona radioelektroniczna ugrupowania oraz racjonalne działanie wojsk.

5. Zabezpieczenie systemów dowodzenia i naprowadzania uzbrojenia przed niekompatybilnością elektromagnetyczną w działaniach obronnych związku operacyjnego jest ważnym działaniem w zakresie zabezpieczenia trwałości i stabilności pracy wchodzących w ich skład systemów i środków elektronicznych. W tym celu należy podejmować odpowiednie działania organizacyjne i techniczne, które powinny być odpowiednio zsynchronizowane z przedsięwzięciami ochrony antyzagłuszeniowej.

√ Przedsięwzięcia organizacyjne należy planować i realizować w sposób scentralizowany na poszczególnych szczeblach dowodzenia. Wśród nich ważną rolę odgrywa: analiza, ocena i prognoza sytuacji elektronicznej, częstotliwościowo – terytorialne rozśrodkowanie środków elektronicznych oraz kontrola pracy własnych środków elektronicznych.

√ Przedsięwzięcia techniczne należy realizować w sposób zdecentralizowany przez zespoły obsługujące wszystkie środki elektroniczne. W ramach działań technicznych należy przede wszystkim wyposażyć je w urządzenia umożliwiające identyfikację i lokalizację źródeł energii zakłóceniowej poprzez ciągłe śledzenie źródeł emitujących energię elektromagnetyczną na częstotliwościach przydzielonych środkom elektronicznym. Pozostałe techniczne działania mające na celu eliminację zakłóceń interferencyjnych (wzajemnych) powinny być podejmowane analogicznie do sposobu organizacji obrony antyzagłuszeniowej.

√ Konieczne jest również wdrażanie urządzeń technicznych umożliwiających: ciągłe śledzenie sytuacji elektronicznej, automatyzację przydziału częstotliwości i manewr częstotliwościami, elektroniczne kształtowanie charakterystyk promieniowania anten.

4. PRZEBIEG PROCESU DECYZYJNEGO POD KĄTEM POTRZEB OBRONY INFORMACYJNEJ W DZIAŁANIACH OBRONNYCH ZWIĄZKU OPERACYJNEGO

Z analizy literatury przedmiotu badań [23;26;42;82;92;126;142;148;149] wynika, że proces decyzyjny w zakresie przygotowania[1] i prowadzenia działań informacyjnych jest w chwili opracowywania pracy studyjnej w stadium dyskusji oraz zgłaszania postulatów w siłach zbrojnych wielu państw. Trwa również wymiana poglądów w tym zakresie pomiędzy armiami państw NATO[2]. Zakłada się, że działania informacyjne, a szczególnie defensywne (obrona informacyjna) powinny stanowić wsparcie działań NATO na szczeblu strategicznym, operacyjnym oraz taktycznym i być stosowane ciągle, tj. od pokoju poprzez kryzys, wojnę i z powrotem do pokoju. Postuluje się, aby działania informacyjne były stałym elementem planowania operacyjnego.

Mając na uwadze, iż w siłach zbrojnych RP przyjmuje się, że związek operacyjny[3] jest podstawowym szczeblem, na którym realizuje się planowanie operacyjne, autor w swoich rozważaniach skupił się właśnie na tym ogniwie dowodzenia, zwracając szczególną uwagę na określenie zakresu kompetencji osób funkcyjnych oraz opracowanie wpływu potrzeb obrony informacyjnej na cykl decyzyjny w działaniach obronnych związku operacyjnego.

Rozważania przedstawione w tym rozdziale stanowią również swoisty udział autora w tej dyskusji, a opracowane wnioski mogą posłużyć decydentom do argumentowania podejmowanych w przyszłości decyzji.

---

[1] W państwach zachodnich jest to proces wypracowywania decyzji i planowania (ang. Decision Making and Planning). Por.: J. Kręcikij, „Przygotowanie działań taktycznych w NATO", wyd. AON, Warszawa 1996, s. 6.

[2] Szerzej problematykę tę autor przedstawił w podrozdziale 1.1.

[3] Przeznaczony jest do prowadzenia samodzielnych operacji na dużych obszarach we współdziałaniu z lotnictwem taktycznym i siłami morskimi. Realizuje założenia operacji połączonych. „Regulamin działań wojsk lądowych", wyd. DWLąd, Warszawa 1999, s. 27.

4.1. Odpowiedzialność funkcyjna za obronę informacyjną

Z analizy podstaw teorii organizacji i kierowania wynika, że funkcje dowodzenia, jako funkcje szczególnego rodzaju kierowania, mieszczą się w cyklu działania zorganizowanego, na który składają się według J. Zielenieckiego[4]: określenie celu, planowanie, organizowanie (wykonanie) i kontrola. Z kolei w nowszych opracowaniach[5] spotyka się bardziej adekwatne funkcje kierowania występujące w procesie decyzyjnym: planowanie[6], organizowanie[7], przewodzenie[8], kontrolowanie[9].

Przebieg procesu decyzyjnego **w zakresie obrony informacyjnej należy postrzegać jako integralny element procesu dowodzenia[10], realizowanego przez sztab związku operacyjnego, zgodnie z obowiązującymi procedurami i technikami w celu oceny sytuacji, tj. określenia tego co się dzieje, zdecydowania co robić, jakie podjąć działania oraz postawienia zadań i kontroli ich wykonania.**

Jak przedstawiono w podrozdziale 1.2., odpowiedzialność za całokształt problematyki związanej z obroną informacyjną powinien ponosić dowódca. Ze względu na to, że obrona informacyjna obejmuje różnorakie przedsięwzięcia i różne formy działalności, które w toku działań obronnych realizowane będą przez wielu wykonawców, jej planowanie i organizowanie powinno odbywać się w sposób scentralizowany.

Z analizy powiązań funkcjonalnych obrony informacyjnej z poszczególnymi komponentami walki informacyjnej (przedstawionymi w podrozdziale 1.1.) oraz z głoszonych opinii ekspertów[11] wynika, że organizatorem zadań w zakresie jej przygotowania i prowadzenia powinna być komórka G 2[12], przy znaczącym współudziale komórki G 3[13].

---

[4] J. Zieleniewski, „Organizacja zespołów ludzkich. Wstęp do teorii organizacji i kierowania", wyd. PWE, Warszawa 1992.

[5] James A. F. Stoner, Edward R. Freeman, Daniel R. Gilbert (przekład [z jęz. ang.] A. Ehrlich), „Kierowanie", wyd. PWE, Warszawa 1998.

[6] Planowanie to proces ustalania celów i odpowiednich działań by je osiągnąć. Tamże, s. 25.

[7] Organizowanie to proces doprowadzania dwóch i więcej osób do współpracy w ramach określonej struktury stosunków, aby osiągnąć określony cel lub zbiór celów. Tamże, s. 25;

[8] Przewodzenie to proces kierowania działaniami członków grupy lub całej organizacji, związanymi z wykonaniem zadań oraz wywieranie na nie wpływu. Tamże, s. 26.

[9] Kontrolowanie to proces zmierzający do zapewnienia, by rzeczywiste działania były zgodne z planowanymi. Tamże, s. 26.

[10] Nazywany jest również procesem informacyjno-decyzyjnym lub cyklem decyzyjnym, który stanowi całokształt przedsięwzięć organizacyjnych związanych z cyklicznym zbieraniem i opracowaniu danych oraz przetwarzaniem ich w decyzje, precyzowaniem zadań oraz stawieniem ich do realizacji.

[11] L. Ciborowski, A. Nowak, „Planowanie, organizowanie i prowadzenie walki informacyjnej na szczeblach taktycznych wojsk lądowych", wyd. AON, Warszawa 2000.

[12] Podobny zapis jest w: „Regulamin działań wojsk lądowych", wyd. DWLąd, Warszawa 1999, s. 62.

[13] W myśl zapisów w starszych dokumentach normatywnych wydanych przez Sztab Generalny WP pion operacyjny (zarząd, oddział) jest organizatorem maskowania operacyjnego [54], które, jak wykazano w pracy studyjnej, jest komponentem obrony informacyjnej związku operacyjnego przed rozpoznaniem.

Organami wykonawczymi sztabu w zakresie planowania i organizowania obrony informacyjnej związku operacyjnego, która z upływem czasu może być utożsamiona z powszechną obroną informacyjną[14], powinny być również komórki specjalistyczne rodzajów wojsk i służb w ramach określonych im obowiązków w zakresie planowania użycia swoich wojsk oraz zabezpieczenia działań bojowych. Ważną rolę w procesie realizacji (wykonania) zadań obrony informacyjnej mają do spełnienia również bezpośredni użytkownicy środków i systemów rozpoznania, dowodzenia i naprowadzania uzbrojenia.

4.1.1. Rola dowódcy i szefa sztabu związku operacyjnego

Jak wykazano w rozdziale pierwszym, odpowiedzialność za całokształt problematyki związanej z planowaniem i prowadzeniem obrony informacyjnej w związku operacyjnym powinien ponosić jego dowódca. Otrzymując zadanie operacyjne ma już niektóre informacje o przeciwniku i dlatego, stawiając zadania oficerowi G 2, powinien określić, jakie dane i w jakim terminie chciałby otrzymać dodatkowo oraz w jakiej formie powinny one być mu przedstawione i w jaki sposób należy je chronić. Poza tym dowódca – niezależnie od wniosków meldowanych przez oficera rozpoznawczego – osobiście ocenia zagrożenie ze strony przeciwnika i wnioskuje o jego możliwościach również w sferze informacyjnej.

Dowódca związku operacyjnego, chcąc podjąć decyzję dotyczącą prowadzenia działań obronnych jest zobowiązany do uwzględnienia aspektu informacyjnego. Powinien określić wysiłek, cel i zadania obrony informacyjnej oraz sposób i czas ich wykonania przez podległe mu wojska. Określając zadania w sferze informacyjnej, powinien wskazać m.in. sposoby i czas zdezorganizowania systemów rozpoznania, dowodzenia i naprowadzania uzbrojenia przeciwnika oraz zapewnienia stabilnej pracy analogicznym systemom wojsk własnych.

Dowódca (szef sztabu) powinien postawić zadania oficerowi G 2, dotyczące:

- zdobycia danych umożliwiających kierowanie przebiegiem działań obronnych;
- zakłócenia procesów rozpoznania, dowodzenia wojskami i naprowadzania uzbrojenia przeciwnika, a przez to dezorientowania go w sytuacji pola walki, komplikowania jego warunków działania i zmuszania go do błędnych decyzji i działań;

---

[14] W analogiczny sposób dokonała się ewolucja pojęcia „powszechna obrona przeciwlotnicza".

– obrony systemów dowodzenia i naprowadzania uzbrojenia związku operacyjnego oraz ich zasobów informacyjnych i procesów informacyjno-sterujących przed ofensywnym oddziaływaniem informacyjnym przeciwnika.

Zadania te spełniają rolę usługową w stosunku do zadania głównego określonego w decyzji i stanowią podstawę organizowania działań w zakresie rozpoznania, zakłócania i obrony informacyjnej w obszarze odpowiedzialności obronnej związku operacyjnego. Dostosowane do charakteru decyzji, obligują skupienie wysiłku w zakresie walki informacyjnej zgodnie z wysiłkiem wojsk, tak w stosunku do kierunku ich działania, jak i zadań (etapów).

Nie można ustalić żadnych reguł i zasad, według których należy określić, jakich danych i w jaki sposób w określonej sytuacji należy szukać. Najlepiej jest formułować braki informacyjne w postaci pytań. Forma pytająca pobudza bowiem do myślenia wszystkich zainteresowanych i wskazuje na ważność poszczególnych informacji dla danego dowódcy.

Stawiane pytania muszą być jasne, krótkie i sformułowane zwięzłym i prostym językiem. Pytania te powinny dotyczyć rozpoznania (zdobywania informacji)[15], zakłócania informacyjnego[16] i obrony informacyjnej. W **sferze obrony informacyjnej** powinny skupiać się na poniższych problemach:

1. Gdzie bronić?
2. Kiedy bronić?
3. Czego bronić?
4. Czym bronić?
5. Czego oczekiwać w następstwie obrony?

Dowódca, dając ogólna koncepcją prowadzenia działań obronnych związku operacyjnego powinien akceptować szczegółowe propozycje oficerów sztabu w sferze obrony informacyjnej, a ponadto:

– nadzorować procesu biernego[17] oraz czynnego[18] informacyjnego przygotowania pola walki;

---

[15] W sferze rozpoznania (zdobywania informacji) powinny brzmieć: 1. Gdzie szukać?; 2. Kiedy szukać?; Czego szukać?; Czym szukać?; Czego oczekiwać? [26].

[16] W sferze zakłócania informacyjnego: 1. Gdzie zakłócać?; 2. Kiedy zakłócać?; Co zakłócać?; Czym zakłócać?; Czego oczekiwać w następstwie zakłócania? [26].

[17] Przedsięwzięcia bierne związane z informacyjną preparacją pola walki to usystematyzowany proces analityczny ukierunkowany na dokonywanie wiarygodnych ocen przeciwnika w zakresie: możliwości jego działania na polu walki, ustalenia wrażliwych miejsc w jego usytuowaniu i możliwościach, demaskowania jego prawdopodobnych zamiarów co do dalszego działania. Podczas biernego (analitycznego) informacyjnego preparowania pola walki uwzględnia się cztery aspekty problemu skoncentrowane wokół: obszaru działania, terenu, pogody, zagrożeń [26;66].

[18] Przedsięwzięcia czynne, związane z informacyjną preparacją pola walki, to procedury realizacyjne tego wszystkiego, co wcześniej zostało ustalone do wykonania, pod kątem walki informacyjnej podczas biernego (analitycznego) preparowania pola walki.

- podjąć decyzję i ogłosić zamiar w zakresie obrony informacyjnej;
- terminowo stawiać zadania w zakresie obrony informacyjnej;
- współuczestniczyć w kontroli realizacji postawionych zadań.

Precyzując zadania dla wojsk dowódca powinien postawić również zadania dla elementów rozpoznania ogólnowojskowego i specjalnego, zakłócania informacyjnego, a także określić obiekty własne, które powinny podlegać obronie informacyjnej. **Dowódca związku operacyjnego powinien decydować o treściach niektórych wiadomości dezinformujących i podstawowych działaniach związanych z pozorowaniem obiektów rzeczywistych**. Sprecyzowane przez dowódcę zadania dla wojsk powinny mieć swoje odzwierciedlenie w rozkazie operacyjnym i w odpowiednich aneksach.

Pracą sztabu bezpośrednio kieruje **szef sztabu**. Powinien on określić zasadnicze zadania komórki G 2 i innych ogniw organizacyjnych sztabu oraz rodzajów wojsk i służb w zakresie zbierania i opracowywania wiadomości rozpoznawczych, a także ustalić czas oraz sposoby meldowania (przekazywania) danych o przeciwniku zainteresowanym odbiorcom i wzajemnej wymiany danych wewnątrz sztabu. Szef sztabu powinien zapoznać się również z oceną przeciwnika dokonaną przez oficera rozpoznania.

Szef sztabu powinien także kontrolować pracę komórki rozpoznawczej i pozostałych komórek organizacyjnych sztabu, które partycypują w całokształcie pracy informacyjnej. Kontrola powinna sprowadzać się nie tylko do wyszukiwania braków i niedociągnięć, ale i do pomocy w ich likwidacji, a także do wyzwolenia większej inicjatywy w zdobywaniu, opracowywaniu, rozpowszechnianiu i ochronie danych.

4.1.2. Zadania oddziału G 2 sztabu związku operacyjnego w zakresie obrony informacyjnej

Podstawowym zadaniem komórki G 2 na każdym szczeblu dowodzenia jest, aby przez kompleksowe użycie różnorodnych sił i środków jak najszybciej uzyskać dane zapewniające możliwość określenia położenia przeciwnika i wynikających z niego zagrożeń. Powinno to pozwolić dowódcy na podjęcie odpowiednich decyzji, co do użycia właściwych sił i środków we właściwym czasie i miejscu oraz zapewnienia bezpieczeństwa ich działań.

Z badań wynika, że obecnie komórką wykonawczą sztabu związku operacyjnego, powołaną do planowania, organizowania i kierowania rozpoznaniem i walką radioelektroniczną

jest **oddział rozpoznania G 2**[19], w którego skład wchodzi: wydział planowania i analiz, wydział topograficznej oceny terenu, wydział bezpieczeństwa wojsk, wydział informacyjny. Komórka G 2 odpowiada za:

- przygotowanie i prowadzenia działań rozpoznawczych;
- przeciwrozpoznanie;
- szkolenie rozpoznawcze.

Z uwagi na określoną w poprzednim podrozdziale odpowiedzialność funkcyjną i realizowane zadania przez oddział G 2 również w zakresie zakłócania informacyjnego oraz obrony informacyjnej autor przyjął do dalszych rozważań strukturę organizacyjną zilustrowaną na rysunku 4.1. Taka struktura jest niezbędna do realizacji zadań przez oddział G 2 w sferze informacyjnej.



Rys. 4.1. Struktura oddziału G 2 związku operacyjnego

Problematyka obrony informacyjnej powinna być rozwiązywana również w określonym zakresie w sztabach dywizji i brygad ogólnowojskowych. W G 2 związku taktycznego[20] powinna znajdować się sekcja obrony informacyjnej, natomiast w S 2 oddziału[21] powinien być specjalista ds. obrony informacyjnej. Elementy te wraz z elementami związku operacyj-

[19] J. Michniak, i inni: „Metody i treść pracy zespołów funkcjonalnych na stanowisku dowodzenia wojsk lądowych", wyd. AON, Warszawa 2000, s. 18.
[20] Tamże, s. 20.
[21] Tamże, s. 21.

nego stanowią odpowiedni system, który w wyniku efektu synergicznego powinien służyć osiągnięciu pożądanych efektów.

Wydział obrony informacyjnej, podlegając szefowi G 2[22], powinien być komórką odpowiedzialną za zapewnienie bezpieczeństwa wojskom związku operacyjnego w warunkach prowadzenia przez przeciwnika walki informacyjnej. Do głównych zadań wydziału należy:

– sprawowanie nadzoru nad prawidłowym funkcjonowaniem systemów informacyjnych oraz ich ochrony przed zagrożeniem ze strony środków walki informacyjnej przeciwnika;

– sprawowanie nadzoru nad właściwym zabezpieczeniem wiadomości niejawnych oraz ich właściwą klasyfikacją, wytwarzaniem i obiegiem;

– prowadzenie kontroli w zakresie bezpieczeństwa oraz ochrony tajemnicy;

– opiniowanie, czy publikowane materiały oraz ich udostępnianie i rozpowszechnianie odpowiadają przepisom bezpieczeństwa;

– ochrona kontrwywiadowcza oraz koordynowanie zadań w zakresie bezpieczeństwa, wykonywanych przez inne komórki organizacyjne;

– współdziałanie z innymi komórkami organizacyjnymi związku operacyjnego oraz z komórkami Urzędu Ochrony Państwa, Policji i Straży Granicznej w zakresie zapewnienia bezpieczeństwa związku operacyjnego i podległych mu związków taktycznych, oddziałów i pododdziałów;

– przesłuchiwanie jeńców, dezerterów i innych osób oraz przedstawianie uzyskanych istotnych wiadomości do szefa G 2;

– gromadzenie i ocena danych o potencjale walki informacyjnej przeciwnika;

– studiowanie zdobytych danych o przeciwniku, opracowywanie wniosków z nich wynikających;

– przygotowanie koncepcji w zakresie obrony informacyjnej przed rozpoznaniem w działaniach obronnych związku operacyjnego;

– przygotowanie koncepcji obrony informacyjnej przed zakłócaniem w działaniach obronnych związku operacyjnego;

– opracowanie planu i kierowanie realizacją szkolenia pionu G 2 w zakresie obrony informacyjnej.

---

[22] Zdaniem autora możliwe jest – w zależności od przyjętej struktury organizacyjnej sztabu związku operacyjnego oraz określonego zakresu kompetencyjnego jej elementów – podporządkowanie tej komórki szefowi G 6 (oddziału wsparcia dowodzenia), a niekiedy szefowi G 3 (oddziału operacyjnego) lub bezpośrednio dowódcy (szefowi sztabu) związku operacyjnego.

Wydział obrony informacyjnej, z uwagi na zadania stojące przed nim, powinien mieć określoną strukturę organizacyjną, która przedstawiona została na rysunku 4.2.



Rys. 4.2. Struktura wydziału obrony informacyjnej

Działalność wydziału obrony informacyjnej **powinna mieć charakter ciągły i być odpowiednio zróżnicowana w zależności od sytuacji i sposobów realizacji ww. zadań w okresie pokoju[23], kryzysu[24] oraz w czasie wojny, a zatem i w czasie działań obronnych związku operacyjnego.**

W toku działań obronnych związku operacyjnego wydział obrony informacyjnej powinien realizować dwie zasadnicze grupy zadań:

- obrona informacyjna w działaniach obronnych związku operacyjnego przed rozpoznaniem (przeciwdziałanie realizacji zadań rozpoznawczych przez przeciwnika);

---

[23] W **okresie pokoju**[23] obrona informacyjna powinna polegać na przestrzeganiu zasad wykorzystania technicznych środków rozpoznania, dowodzenia i naprowadzania uzbrojenia określonych instrukcjami eksploatacyjnymi oraz przepisami o ochronie tajemnicy. Szczególna uwaga powinna być zwrócona na ukrywanie wojsk i obiektów, eliminowanie ich cech demaskujących, wykorzystanie maskujących właściwości terenu, warunków atmosferycznych, etatowych i podręcznych środków maskowania itp. Należy również nadać odpowiednią rangę ochronie kontrwywiadowczej oraz szkoleniu sztabów i wojsk w tym zakresie. W okresie pokoju prowadzone jest również rozpoznanie (zdobywanie informacji) o potencjalnym przeciwniku. Tworzone są bazy danych o jego siłach i środkach oraz wzorce doktrynalne.

[24] W okresie **kryzysu** przedsięwzięcia obrony informacyjnej, odpowiednio skoordynowane z rozpoznaniem, powinny być realizowane przede wszystkim w celu uniemożliwienia przeciwnikowi określenia czasu osiągnięcia gotowości do prowadzenia działań wojennych. Szczególną uwagę należy zwracać na zachowanie w tajemnicy osiągania przez wojska związku operacyjnego wyższych stanów gotowości bojowej. Główny wysiłek powinien być skierowany na: ukrycie przedsięwzięć związanych z rozwijaniem mobilizacyjnym związku operacyjnego; zachowanie w tajemnicy planów prowadzenia operacji i walki, w tym szczególnie planów prowadzenia walki informacyjnej; realizację na szeroką skalę przedsięwzięć obrony informacyjnej wszelkimi dostępnymi siłami i środkami.

– obrona informacyjna systemów dowodzenia i naprowadzania uzbrojenia przed zakłócaniem.

Obrona informacyjna w działaniach obronnych związku operacyjnego przed rozpoznaniem powinna być planowana i organizowana przez wydział obrony informacyjnej, natomiast prowadzona, zgodnie z opracowanymi planami, przez szeroki krąg wykonawców. Obrona ta powinna polegać między innymi na stosowaniu szeregu przedsięwzięć przeciwrozpoznawczych[25], udaremniających lub utrudniających zdobywanie danych przez siły i środki rozpoznania przeciwnika.

Obrona informacyjna przed zakłócaniem w działaniach obronnych związku operacyjnego powinna być planowana i organizowana przez organy obrony informacyjnej, natomiast prowadzona, zgodnie z opracowanymi planami, przez wybrany krąg wykonawców[26].

4.1.3. Zadania oddziału G 3 sztabu związku operacyjnego w zakresie obrony informacyjnej

Badania wykazały, że w procesie planowania i organizowania obrony informacyjnej czynnie powinny uczestniczyć organy operacyjne[27]. Biorą one udział w koordynowaniu zadań rozpoznania, zakłócania i obrony informacyjnej z zadaniami związku operacyjnego, związków taktycznych i oddziałów. Ustalają (wspólnie z G 2) rejony rozwinięcia sił i środków rozpoznania, zakłócania, działań psychologicznych i działań specjalnych, ich przegrupowanie, drogi i czas marszu oraz wszystkie inne przedsięwzięcia związane z wykonywaniem manewru.

Organy operacyjne **powinny uczestniczyć w przygotowaniu treści komunikatów do prowadzenia dezinformacji, a problemy związane z pozorowaniem należy wzajemnie uzgadniać.**

---

[25] Zakres i treść przedsięwzięć obrony informacyjnej w działaniach obronnych związku operacyjnego przed rozpoznaniem przedstawiono w rozdziale 2 pracy studyjnej.

[26] Zakres i treść przedsięwzięć obrony informacyjnej w działaniach obronnych związku operacyjnego przed zakłócaniem przedstawiono w rozdziale 3 pracy studyjnej.

[27] W świetle dotychczasowych rozwiązań w siłach zbrojnych RP organy operacyjne są odpowiedzialne za planowanie i organizowanie maskowania operacyjnego [54;92]. Jak wykazano jednak w rozdziale 2 pracy studyjnej, problematyka maskowania jest komponentem obrony informacyjnej związku operacyjnego przed rozpoznaniem, powinna być zatem rozwiązywana przede wszystkim w komórce G 2.

Pomiędzy organami G 3 a organami G 2 powinny być koordynowane również problemy realizacji zadań rozpoznania, zakłócania oraz obrony informacyjnej z zadaniami związków taktycznych i oddziałów. Współpraca ta powinna dotyczyć m.in.:

- koordynowania działania środków ostrzegawczych z działaniami przeciwrozpoznawczymi;
- przygotowania działań pozornych, przez ocenę:
  a) środków przetwarzania danych przeciwnika;
  b) szczebla dowodzenia przeciwnika mogącego podjąć działania pozorne;
  c) proponowania „scenariusza" działań pozornych;
  d) reakcji przeciwnika na określone działania przydatne w planowaniu przyszłych działań pozornych;
- przygotowania wspólnie z G 2 i G 6 koncepcji działań dezinformujących, mających na celu wprowadzenie przeciwnika w błąd oraz nadzorowania i koordynowania realizowanych przedsięwzięć w tym zakresie;
- nadzorowania przestrzegania zasad ochrony wymiany danych;
- w razie konieczności proponowanie wprowadzenia cenzury.

4.1.4. Zadania specjalistów rodzajów wojsk w zakresie obrony informacyjnej

Dokumenty normatywne zobowiązują specjalistów rodzajów wojsk do ciągłej znajomości sytuacji rozpoznawczej w interesującym ich zakresie, prowadzenia osobistej oceny przeciwnika i jego możliwości oddziaływania na podległe im siły i środki. Powinni oni ponadto uzyskane przez podległe im wojska dane rozpoznawcze (w tym bojowe, po ich wykorzystaniu) niezwłocznie przekazywać do oddziału G 2, który jako jedyny jest kompetentny do ich globalnej oceny merytorycznej.

Informowanie o przeciwniku jest obowiązkiem wszystkich komórek organizacyjnych, a zwłaszcza tych, które mają możliwości uzyskania określonych danych o jego potencjale z dodatkowych źródeł. Zdobyte przez nie dane niezależnie od ich wykorzystania na własne potrzeby, powinny być przekazane, po wstępnym opracowaniu, komórkom rozpoznawczym.

Wstępne opracowanie danych i przekazanie ich do G 2 z odpowiednimi wnioskami jest potrzebne dlatego, że wnioski te będą miały z reguły charakter specjalistyczny i fachowy, a ich ocena może pomóc elementom rozpoznawczym w dogłębnym zrozumieniu ich treści.

Również oddział G 2 obowiązany jest nie tylko do ogólnej oceny przeciwnika[28], którą przedstawia zainteresowanym komórkom sztabu związku operacyjnego, ale także do szczegółowej jego oceny służącej planowaniu użycia własnych sił i środków rozpoznania.

Wszystkie przedsięwzięcia planistyczne z zakresu rozpoznania, wykonywane przez specjalistów rodzajów wojsk i służb, winny znajdować odzwierciedlenie w planie rozpoznania związku operacyjnego.

Specjaliści rodzajów wojsk i służb powinni uczestniczyć ponadto w szczegółowym planowaniu zadań w zakresie obrony informacyjnej. W opracowywanych koncepcjach użycia wojsk **osoby te – we współpracy z organami G 2 i G 3 – powinny być zobowiązane do przedstawienia wszystkich zaplanowanych przedsięwzięć w zakresie maskowania bezpośredniego, maskowania pośredniego, obrony elektronicznej oraz innych zamierzeń, współzależnych z realizacją zadań obrony informacyjnej.** Poza tym, specjaliści rodzajów wojsk i służb powinni być bezpośrednio odpowiedzialni za ustalenie priorytetów pracy, jak również rodzajów i czasu pracy środków elektronicznych, określenie sposobu eliminacji ich wzajemnych zakłóceń, zasad i sposobów rozmieszczenia tych środków w ugrupowaniu wojsk oraz ustalenie sposobu kontroli elektronicznej w toku działań. W swoich dokumentach planistycznych powinni ujmować własne działania, które realizują ze środkami zakłócania, uwzględniając czas i sposób działania oraz harmonogram współdziałania.

Specjaliści rodzajów wojsk i służb powinni nadzorować realizację zadań obrony informacyjnej w swoich wojskach oraz wnosić, w razie potrzeby, niezbędne korekty.

4.1.5. Powiązania informacyjne w zakresie obrony informacyjnej

Z analizy struktury wewnętrznej stanowiska dowodzenia (SD) związku operacyjnego[29] wynika, że oddział G 2 wchodzi w skład centrum dowodzenia (CD) i tworzy zespół rozpoznania. Zespół ten, w świetle stojących przed nim zadań należy nazwać **zespołem działań**

---

[28] Decydującą i koordynującą rolę w pracy informacyjnej o przeciwniku spełniają komórki G2, które zbierają i opracowują dane napływające z różnych źródeł. Nie oznacza to jednak, że powyższe czynności stanowią wyłączną domenę komórek rozpoznawczych [26].

[29] J. Michniak i inni, „Metody i treść pracy zespołów funkcjonalnych na stanowisku dowodzenia wojsk lądowych", wyd. AON, Warszawa 2000, s. 26.

informacyjnych. Powinien składać się z następujących grup: planowania, badań i informacji, rozpoznania, zakłócania informacyjnego, obrony informacyjnej oraz topograficznej oceny terenu.

Odpowiedni zespół (sekcja) działań informacyjnych powinien być również wydzielany na tyłowym stanowisku dowodzenia (TSD) związku operacyjnego, w którego składzie powinien być specjalista w zakresie obrony informacyjnej.

Z analizy metod i treści pracy zespołów funkcjonalnych na stanowisku dowodzenia związku operacyjnego wynika, że występują między nimi odpowiednie powiązania informacyjne wewnętrzne oraz powiązania informacyjne zewnętrzne ze szczeblem nadrzędnym, podwładnymi i współdziałającymi. W ramach tych powiązań i więzi powinny być rozwiązywane również problemy w zakresie obrony informacyjnej.

Wewnętrzne powiązania informacyjne zespołu działań informacyjnych centrum dowodzenia stanowiska dowodzenia związku operacyjnego (tworzonego na bazie oddziału G 2) powinny obejmować praktycznie wszystkie elementy stanowiska dowodzenia (rysunek 4.3.). Wynika to z faktu, że praktycznie wszyscy muszą korzystać z danych posiadanych przez zespół działań informacyjnych dotyczących przeciwnika, obszaru działania oraz czynników wpływających na wykonanie zadania. Jednocześnie zespół ten powinien korzystać ze wszystkich danych uzyskanych przez poszczególne elementy stanowiska dowodzenia.

Z powyższego wynika, że należy wyróżnić następujące powiązania informacyjne:

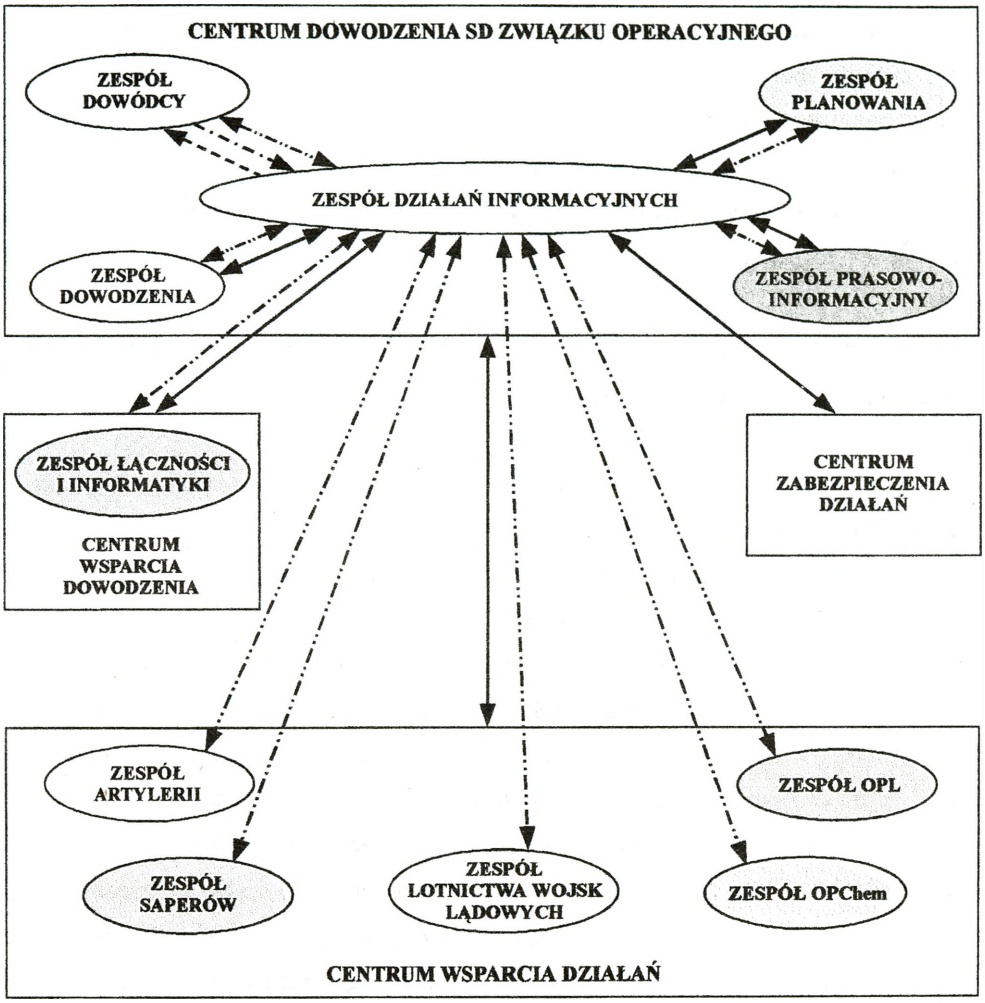
1. W ramach centrum dowodzenia:

a) z zespołem dowódcy:

- otrzymywanie zadań w zakresie rozpoznania, zakłócania i obrony informacyjnej;
- meldowanie ocen i wyników rozpoznania, zakłócania i obrony informacyjnej w poszczególnych fazach cyklu dowodzenia oraz według potrzeb;
- proponowanie koncepcji rozpoznania, zakłócania i obrony informacyjnej.

b) z zespołem planowania:

- informowanie o przeciwniku i terenie;
- uzgodnienia w zakresie opracowania wariantów działania przeciwnika i wojsk własnych;
- uzgodnienia w zakresie rozwinięcia, rozmieszczenia i działania podległych sił i środków rozpoznania i zakłócania oraz niezbędnych zagadnień związanych z bezpieczeństwem działania elementów rozpoznawczych;



LEGENDA:

- zadania;
- meldowanie;
- informowanie, uzgodnienia;
- współdziałanie.

Rys. 4.3. Powiązania informacyjne zespołu działań informacyjnych na SD związku operacyjnego

– przekazanie niezbędnych danych do opracowania oleatu wsparcia decyzji i planu działań obronnych;

– współdziałanie w zakresie przeciwdziałania realizacji zadań rozpoznawczych przez przeciwnika (w zakresie działań przeciwrozpoznawczych);

– współdziałanie w zakresie realizacji zadań obrony informacyjnej elementów ugrupowania związku operacyjnego przed zakłócaniem.

c) z zespołem dowodzenia:

– informowanie o przeciwniku i terenie;

– przekazywanie niezbędnych danych do rozkazu operacyjnego i zarządzeń (aneksy[30]: rozpoznanie; zakłócanie; obrona informacyjna; apendyksy; wstawki dotyczące przeciwnika i terenu);

– ustalenia w zakresie kierowania wojskami oraz realizacją zadań obrony informacyjnej.

d) z zespołem prasowo-informacyjnym:

– informowanie o przeciwniku i terenie;

– współdziałanie w zakresie przekazywania wiadomości dezinformujących i mylących.

2. Z centrum wsparcia dowodzenia:

a) z zespołem łączności i informatyki:

– informowanie o przeciwniku i terenie;

– uzgodnienie w zakresie funkcjonowania systemu łączności i informatyki oraz wymiany danych na potrzeby rozpoznania i zakłócania informacyjnego (przydział częstotliwości i organizacja sieci łączności oraz zabezpieczenia wymiany danych o przeciwniku w związku operacyjnym, ze sztabem przełożonego oraz sztabami sąsiednimi i współdziałającymi);

– uzgodnienia w zakresie kontroli przestrzegania zasad pracy na urządzeniach łączności oraz współdziałania w wykrywaniu i eliminowaniu niekompatybilności elektromagnetycznej;

– współdziałanie w zakresie prowadzenia dezinformacji oraz organizacji pozornych elementów (węzłów łączności SD) ugrupowania operacyjnego związku operacyjnego;

– uzgodnienia częstotliwości zabronionych do zakłócania oraz w zakresie realizacji pozostałych przedsięwzięć obrony informacyjnej przed zakłócaniem.

---

[30] Zdaniem autora docelowo będzie opracowywany jeden aneks – walka informacyjna.

3. Z centrum wsparcia działań:

a) z zespołem artylerii:

- informowanie o przeciwniku i terenie;
- określenie punktów i obszarów (rejonów) zainteresowania celami;
- określenie kolejności i sposobów rozpoznania celów dla artylerii;
- uzgodnienie sposobów wskazywania celów;
- koordynacja wysiłku rozpoznania z rozpoznaniem artyleryjskim w zakresie:
  - √ miejsc rozmieszczenia punktów obserwacyjnych (stanowisk dowódczo-obserwacyjnych) artylerii, środków rozpoznania radiolokacyjnego i dźwiękowego oraz ich zadania, czas rozwinięcia, kolejne rubieże działania i sposób przegrupowania;
  - √ elementów rozpoznawczych, do których należy włączyć zwiadowców artylerii (miejsce i czas włączenia);
  - √ sposobów organizacji łączności i przekazywania (wymiany) zdobytych danych rozpoznawczych;
- koordynacja wysiłku zakłócania z porażeniem ogniowym, a szczególnie:
  - √ rażenie uderzeniami rakiet i ogniem artylerii stanowisk (punktów) dowodzenia oraz kierowania środkami walki przeciwnika;
  - √ przenoszenie w rejony węzłów łączności stanowisk dowodzenia przeciwnika nadajników zakłóceń jednorazowego użytku (według danych i na sygnał z zespołu działań informacyjnych centrum dowodzenia SD K);
- uzgodnienie niezbędnych zagadnień w zakresie zapewnienia bezpieczeństwa elementów rozpoznawczych przed własnym porażeniem ogniowym;

b) z zespołem obrony przeciwlotniczej (OPL):

- uzgodnienie oceny przeciwnika powietrznego;
- określenie miejsc rozmieszczenia posterunków obserwacji powietrznej, ich zadań oraz sposobów współdziałania z elementami rozpoznawczymi, zakłócania i obrony informacyjnej;
- uzgodnienie sposobów przekazywania sygnałów alarmowych o przeciwniku powietrznym;
- uzgodnienie sposobu organizacji łączności i przekazywania (wymiany) zdobytych danych rozpoznawczych;
- uzgodnienia w zakresie organizacji współdziałania sił i środków OPL oraz zakłócania informacyjnego na okres osłony wybranych (nakazanych) obiektów ugrupowania obronnego związku operacyjnego;

c) z zespołem saperów:

– uzgodnienia w zakresie oceny przeciwnika i terenu;

– uzgodnienie miejsc rozmieszczenia inżynieryjnych posterunków obserwacyjnych oraz ich zadań;

– określenie czasu wysłania samodzielnych inżynieryjnych patroli rozpoznawczych (IPR) i ich zadań;

– uzgodnienie sposobów współdziałania w zakresie realizacji zadań rozpoznawczych, zakłócania i obrony informacyjnej z elementami inżynieryjnymi;

– wytypowanie odcinków i czasu naziemnego fotografowania obrony przeciwnika;

– wydzielanie saperów – zwiadowców do elementów rozpoznawczych (ogólnowojskowych i działań specjalnych) podczas przygotowywania i prowadzenia rozpoznania;

– uzgodnienie sposobu organizacji łączności i przekazywania (wymiany) zdobytych danych rozpoznawczych;

– współdziałanie w realizacji przedsięwzięć przeciwradiolokacyjnego maskowania wojsk i obiektów oraz realizacji pozornych obiektów elektronicznych dowodzenia (węzłów łączności SD, itp.) przy wykorzystaniu podległych pododdziałów;

d) z zespołem obrony przeciwchemicznej:

– uzgodnienie miejsc rozmieszczenia posterunków obserwacji skażeń w okresie przygotowawczym do działań, ich zadania i czas rozwinięcia;

– określenie sposobów, dróg, kierunków i czasu ich przegrupowania w toku działań obronnych związku operacyjnego;

– wytypowanie rejonów wejścia i kierunków działania patroli rozpoznania skażeń;

– możliwości i potrzeb włączenia sił i środków rozpoznania skażeń w skład ogólnowojskowych elementów rozpoznawczych (kto?, gdzie? i kiedy?);

– uzgodnienie sposobu utrzymania łączności i przekazywania (wymiany) danych rozpoznawczych;

– uzgodnienie realizacji przedsięwzięć przeciwdziałania optoelektronicznym środkom rozpoznania przeciwnika przez podległe pododdziały;

e) z zespołem lotnictwa wojsk lądowych:

– planowanie działań śmigłowców i bezpilotowych samolotów rozpoznawczych;

– koordynowanie powietrznych działań rozpoznawczych;

– uzgodnienie sposobu wymiany danych z rozpoznania powietrznego;

– uzgodnienia w zakresie wykorzystania śmigłowców transportowych na potrzeby przerzutu grup specjalnych (rozpoznawczych);

– uzgodnienia w zakresie dezorganizacji systemu dowodzenia i naprowadzania uzbrojenia przeciwnika poprzez:

√ oddziaływanie ogniowe na punkty dowodzenia oraz obiekty kierowania środkami walki;

√ ogniowe niszczenie środków rozpoznania obrony powietrznej;

√ przenoszenie w rejony węzłów łączności stanowisk dowodzenia przeciwnika nadajników zakłóceń jednorazowego użytku[31] według danych i na sygnał z zespołu działań informacyjnych centrum dowodzenia stanowiska dowodzenia związku operacyjnego.

4. Z centrum zabezpieczenia działań:

– uzgadnianie możliwości zaopatrzenia wojsk rozpoznawczych w niezbędne środki (medyczne, techniczne, żywnościowe, materiały pędne i smary, specjalne, maskowania itp.)[32];

– dokonywanie ustaleń co do sposobu (miejsc, terminów) logistycznego zabezpieczenia działań rozpoznawczych;

– uzgadnianie spraw kadrowych.

Zewnętrzne powiązania informacyjne zespołu działań informacyjnych centrum dowodzenia związku operacyjnego w zakresie rozwiązywania problemów obrony informacyjnej zilustrowano na rysunku 4.4.

Należą do nich powiązania:

– z zespołem działań informacyjnych centrum dowodzenia stanowiska dowodzenia dowództwa wojsk lądowych;

– z sąsiadami;

– z zespołami działań informacyjnych centrum dowodzenia SD podległych dywizji;

– z batalionem elektronicznym[33] oraz z siłami i środkami rozpoznania lądowego, działań specjalnych i działań psychologicznych;

---

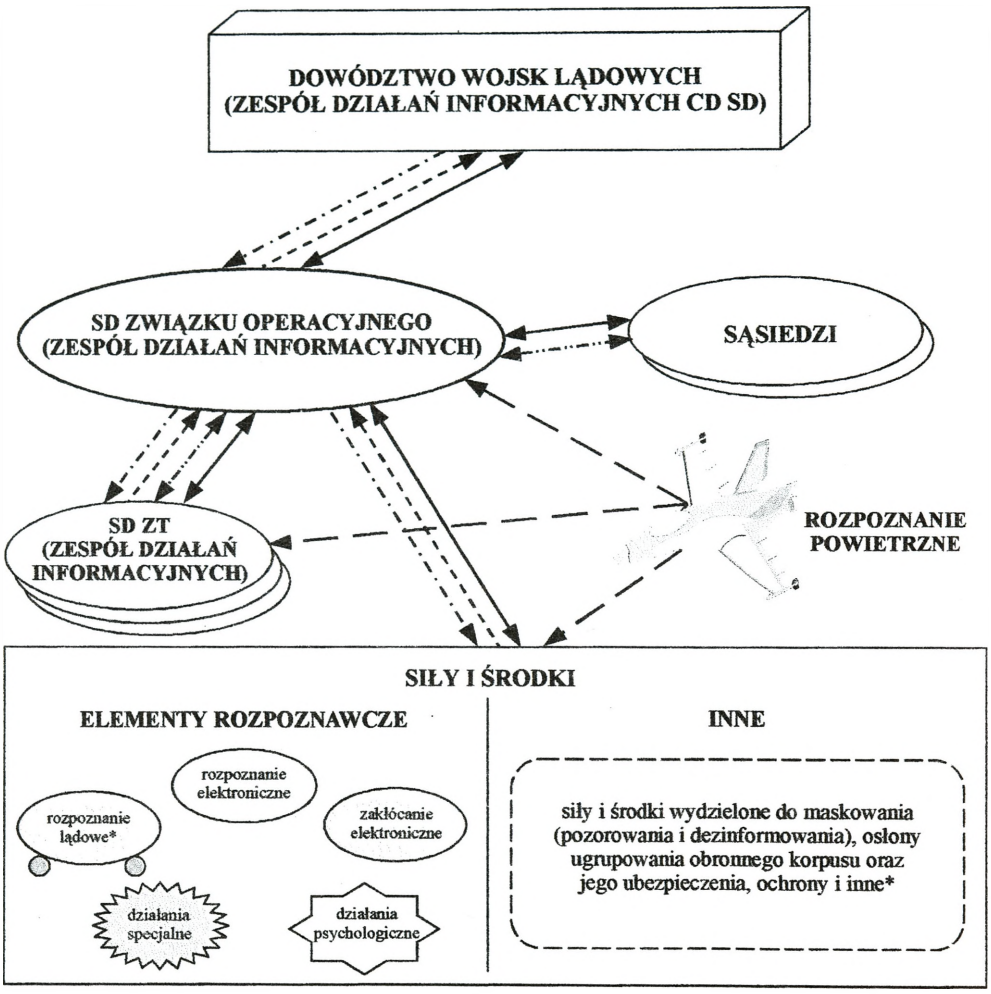
[31] W wypadku posiadania tego typu nadajników.

[32] Formalne zapotrzebowanie składa dowódca jednostki rozpoznawczej.

[33] Zgodnie z nową koncepcją reorganizacji SZ RP do roku 2003 w związku operacyjnym wystąpi batalion elektroniczny (radioelektroniczny). Przewiduje się również jednostki wsparcia rozpoznania, których struktura nie jest bliżej określona. Konferencja metodyczna kierowniczej kadry rozpoznania wojsk lądowych, w której autor czynnie uczestniczył. Lidzbark Warmiński, 11 – 14.12.2000.

Powiązania informacyjne utrzymywane z zespołem działań informacyjnych dowództwa wojsk lądowych powinny zapewnić:

– terminowe otrzymywanie zadań w zakresie rozpoznania, zakłócania i obrony informacyjnej;



LEGENDA:

- zadania;
- meldowanie;
- informowanie, uzgodnienia;
- współdziałanie;
- odbiór danych z rozpoznania powietrznego;
- * zgodnie z aneksem A - podział sił.

Rys. 4.4. Zasadnicze powiązania zewnętrzne zespołu działań informacyjnych związku operacyjnego

– terminowe składanie meldunków (w tym doraźnych);

– bieżące kierowanie i koordynację działań w zakresie rozpoznania, zakłócania i obrony informacyjnej w działaniach obronnych związku operacyjnego;

– bieżące otrzymywanie komunikatów rozpoznawczych od przełożonego oraz składanie na nie zapotrzebowań.

W ramach tej więzi informacyjnej, ze względu na specyfikę działań i potrzebę bieżącego współdziałania (koordynacji działań), powinna być utrzymywana ciągła i niezawodna łączność na potrzeby rozpoznania, zakłócania i obrony informacyjnej.

Powiązania informacyjne z sąsiadami powinny zapewnić możliwość współdziałania w wypadku wykonywania wspólnych zadań oraz bieżące informowanie się o sytuacji. Ta więź informacyjna może mieć również duże znaczenie dla rozwiązywania problemów obrony informacyjnej, zapewnia bowiem wymianę danych o przeciwniku z sąsiadami, a tym samym zwiększa możliwości w zakresie oceny zagrożeń, zwłaszcza blisko linii rozgraniczenia z sąsiadami związku operacyjnego i podległych związków taktycznych oraz umożliwia organizację współdziałania w zakresie realizacji przedsięwzięć obrony informacyjnej.

Powiązania informacyjne utrzymywane z zespołami działań informacyjnych centrum dowodzenia SD podległych dywizji powinny zapewnić:

– terminowe stawianie zadań w zakresie rozpoznania, zakłócania i obrony informacyjnej;

– terminowe otrzymywanie meldunków (w tym doraźnych);

– bieżące kierowanie i koordynację działań w zakresie rozpoznania, zakłócania i obrony informacyjnej w działaniach obronnych związku operacyjnego;

W ramach tej więzi informacyjnej, ze względu na specyfikę działań i potrzebę bieżącego współdziałania oraz informowania, powinna być utrzymywana ciągła i niezawodna łączność na potrzeby rozpoznania, zakłócania i obrony informacyjnej.

Z elementami rozpoznawczymi powinna być utrzymywana również ciągła więź informacyjna w zakresie:

– stawiania zadań rozpoznawczych oraz na potrzeby zakłócania i obrony informacyjnej;

– terminowego otrzymywania meldunków rozpoznawczych (w tym doraźnych) oraz o prowadzonym zakłócaniu;

– bieżącego kierowania i koordynacji działań rozpoznawczych, zakłócania i obrony informacyjnej;

– bieżącego informowania podwładnych o sytuacji.

Dodatkowo, w celu zapewnienia ciągłego kierowania, koordynowania działań oraz wymiany danych rozpoznawczych, na potrzeby zakłócania i obrony informacyjnej winna być zapewniona niezawodna łączność służąca realizacji zadań:

– rozpoznania bezpośredniego (łączność z siłami i środkami rozpoznania lądowego) oraz w razie potrzeby łączność z poszczególnymi elementami rozpoznania patrolowego i specjalnego[34];

– rozpoznania elektronicznego (łączność z dowództwem i sztabem batalionu) oraz w razie potrzeby łączność z poszczególnymi jego elementami;

– zakłócania informacyjnego (łączność z dowództwem i sztabem batalionu) oraz w razie potrzeby łączność z poszczególnymi jego elementami;

– obrony informacyjnej we wszystkich czynnych relacjach łączności.

Z siłami i środkami wydzielonymi do maskowania (pozorowania i dezinformowania), osłony radioelektronicznej ugrupowania obronnego związku operacyjnego oraz jego ubezpieczenia i ochrony powinna być utrzymywana więź informacyjna w specjalnie organizowanych do tego celu relacjach łączności.

Z elementami rozpoznania powietrznego powinna być utrzymywana również więź informacyjna. W tym celu zespoły działań informacyjnych centrum dowodzenia SD związku operacyjnego oraz podległych dywizji, a także elementów rozpoznawczych powinny uruchamiać odbiorniki do odbioru danych z rozpoznania powietrznego[35].

4.2. Przebieg cyklu decyzyjnego w zakresie obrony informacyjnej

Jak wynika z analizy dostępnej autorowi literatury przedmiotu badań [23;26;41;42; 56;82;92;126;142;149], całokształt przedsięwzięć związanych z dowodzeniem realizowanym przez komórki organizacyjne i osoby funkcyjne składa się na proces dowodzenia[36], który z operacyjnego punktu widzenia traktowany jest jako cykl decyzyjny jednakowy na wszystkich szczeblach. Ramowy układ cyklu decyzyjnego, zalecany w Akademii Obrony Narodowej do rozwiązywania problemów dowodzenia przedstawiono na rysunku 4.5[37].

---

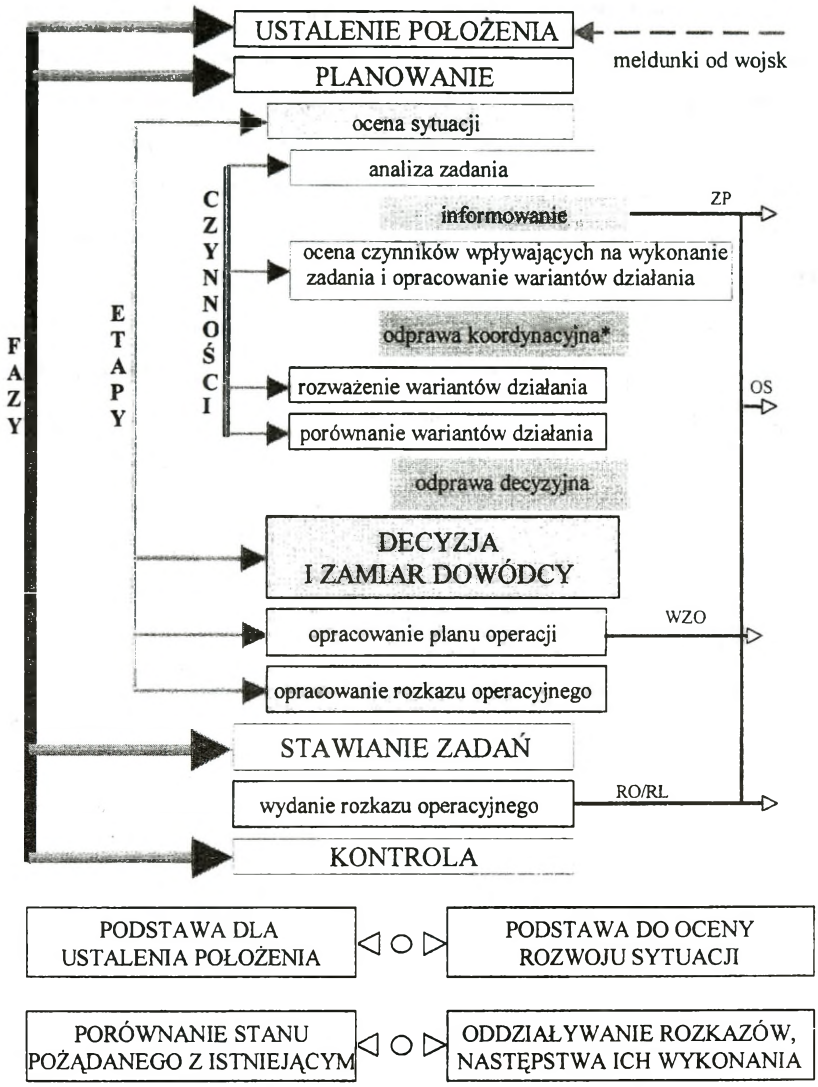
[34] W celu skrócenia czasu wymiany informacji.

[35] Taki odbiornik jest dotychczas umieszczany w rozpoznawczych wozach dowodzenia.

[36] Proces ten symbolicznie można przedstawić w postaci koła, które utrzymywane jest w ruchu przez ciągłe zdobywanie, przetwarzanie i wykorzystywanie danych, stanowiących podstawę do powzięcia decyzji i opracowania planu działania oraz opracowania zadań (dyrektyw, rozkazów, zarządzeń) i przekazania ich wykonawcom.

[37] Opracowano na podstawie: J. Michniak i inni, „Metody i treść pracy zespołów funkcjonalnych na stanowisku dowodzenia wojsk lądowych", wyd. AON, Warszawa 2000, s. 29.

Cykl ten jest zgodny ze stałymi procedurami operacyjnymi obowiązującymi w siłach zbrojnych głównych państw NATO oraz uwzględnia dorobek polskiej myśli wojskowej.



LEGENDA:

ZP - zarz' dzenie przygotowawcze;
OS - orientowanie w sytuacji;
WZO - wstępne zarządzenie operacyjne;
RO/RL - rozkaz operacyjny / logistyczny;
* - liczba, miejsce i cele odpraw koordynacyjnych określa dowódca lub szef sztabu.

Rys. 4.5. Ramowy układ cyklu decyzyjnego

Z powyższego wynika, że **cykl decyzyjny w zakresie obrony informacyjnej powinien być nierozerwalnie związany z procesem dowodzenia, realizowanym przez komórki organizacyjne i osoby funkcyjne na stanowiskach dowodzenia związku operacyjnego w ramach systemu dowodzenia.** W procesie tym **najważniejsze zadania realizuje zespół działań informacyjnych centrum dowodzenia**[38]. Udział biorą także zespoły planowania i dowodzenia centrum dowodzenia oraz zespół łączności i informatyki centrum wsparcia dowodzenia. Uczestniczą w nim również zespoły funkcjonalne centrum wsparcia działań w ramach nałożonych na nich obowiązków w zakresie planowania i zabezpieczenia działań bojowych.

Cykl decyzyjny w zakresie obrony informacyjnej przebiega w czterech łączących się i przenikających się nawzajem fazach: ustalenia położenia, planowania, stawiania zadań, kontroli. Jego celem jest określenie kolejności, sposobów i terminów wykonania zadań z zakresu obrony informacyjnej w działaniach obronnych związku operacyjnego.

4.2.1. Ustalanie położenia w zakresie obrony informacyjnej

Ustalenie położenia jest punktem wyjściowym całego cyklu dowodzenia. Faza ta rozpoczyna się z chwilą otrzymania zadania, niekiedy meldunku w formie prośby lub wiadomości w ramach prowadzonej stałej obserwacji i napływu danych o sytuacji, ale także w wyniku zaistniałej sytuacji i nie dającego się przewidzieć jej rozwoju.

Przedmiotem działań na tym etapie jest – w związku z poszukiwaniem odpowiednio ukierunkowanej decyzji – przede wszystkim zebranie wszystkich istotnych faktów oraz określenie czynników wywierających wpływ na daną sytuację, ich ocenę i uporządkowanie. Występują tutaj różne formy pracy sztabowej z wykorzystaniem technicznych środków przetwarzania danych. W wielu wypadkach regułą będzie, że z powodów czasowych i dużej objętości materiału etap ten będzie musiał zostać zrealizowany wcześniej. Ważne jest, aby podczas oceny otoczenia właściwie zdecydować, kiedy zajdzie potrzeba zdobycia nowych danych, a kiedy posiadana baza danych wystarczy w dalszym postępowaniu. Tylko w nielicznych wypadkach taki podział i segregowanie danych osiągać będzie wystarczający stopień pewności.

---

[38] Pożądaną odpowiedzialność funkcyjną za przygotowanie i prowadzenie obrony informacyjnej przedstawiono w podrozdziale 4.1. niniejszej pracy studyjnej.

Ustalenie położenia jest najczęściej zapoczątkowywane przez **informowanie o położeniu**. Ma ono na celu poinformowanie dowódcy i sztabu związku operacyjnego o zaistniałej sytuacji i określenie dalszego algorytmu postępowania. Faza ustalenia położenia dla zespołu działań informacyjnych na centrum dowodzenia SD związku operacyjnego jest **początkiem procesu informacyjnego przygotowania pola walki**[39]. W procesie tym należy rozpatrywać również problemy obrony informacyjnej (rysunek 4.6.).

Do głównych zadań, jakie w tej fazie powinien realizować **zespół działań informacyjnych** [40] **w zakresie obrony informacyjnej** należą:

- zebranie, uporządkowanie, a następnie zobrazowanie danych o położeniu i ukompletowaniu sił i środków walki informacyjnej przeciwnika oraz ich wykorzystywaniu w dotychczasowych działaniach;
- zebranie i uporządkowanie danych o otoczeniu pola walki (o obszarze działań, terenie, pogodzie, warunkach demograficznych itp.), mającym wpływ na wymiar informacyjny działań;
- określenie braków informacyjnych, luk w wiedzy o przeciwniku i terenie w sferze informacyjnej;
- zebranie i uporządkowanie danych o położeniu i realizowanych zadaniach przez potencjał walki informacyjnej (rozpoznania, zakłócania i obrony informacyjnej) związku operacyjnego;
- ukierunkowanie cyklu realizowanych przedsięwzięć zgodnie z zadaniami postawionymi przez dowódcę;
- wykonywanie bieżących czynności wynikających z zadań.

Podczas pracy w fazie ustalanie położenia zespół działań informacyjnych centrum dowodzenia SD związku operacyjnego powinien sporządzić wstępną ocenę sytuacji, dającą sztabowi niezbędne dane do dalszej pracy. Wnioski w tej fazie należy zobrazować w takich dokumentach, jak: mapa informacyjna lub sytuacyjna (oleat sytuacji bojowej), zarządzenie przygotowawcze, rozkaz operacyjny i inne.

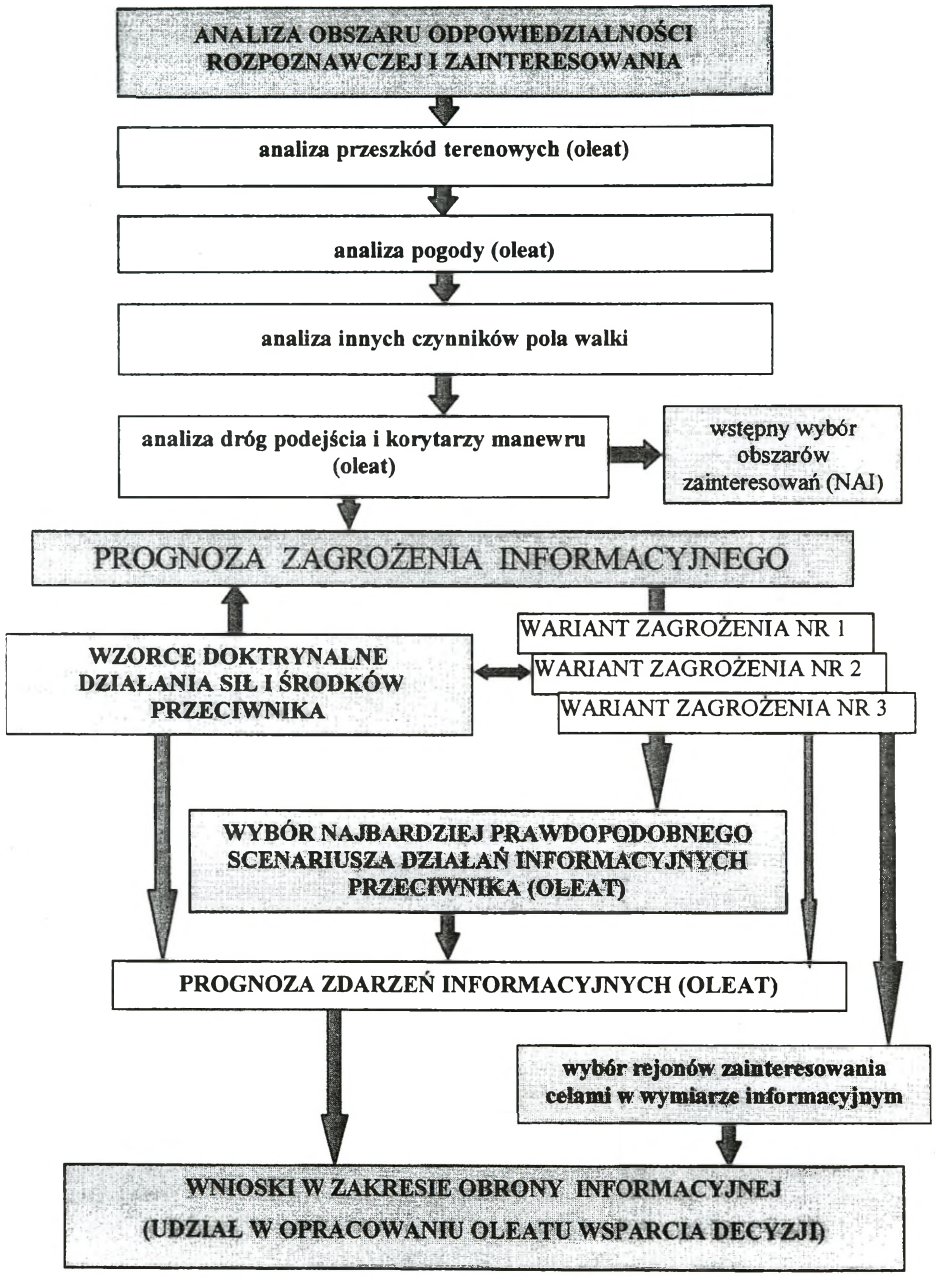
Celem ustalenia położenia na potrzeby obrony informacyjnej jest **zebranie, uporządkowanie, a następnie zobrazowanie danych o położeniu i potencjale walki informacyjnej**

---

[39] Problematyka informacyjnego (rozpoznawczego) przygotowania pola walki (ang. Intelligence Preparation of the Battlefield), której ważnym komponentem jest elektroniczne przygotowanie pola walki (ang. Electronic Preparation of the Battlefield) jest przedmiotem opracowań studyjnych w AON, w których autor również uczestniczył [60;62]. Stanowi ona ważną procedurę planowania działań wojsk sojuszniczych NATO [21;23].

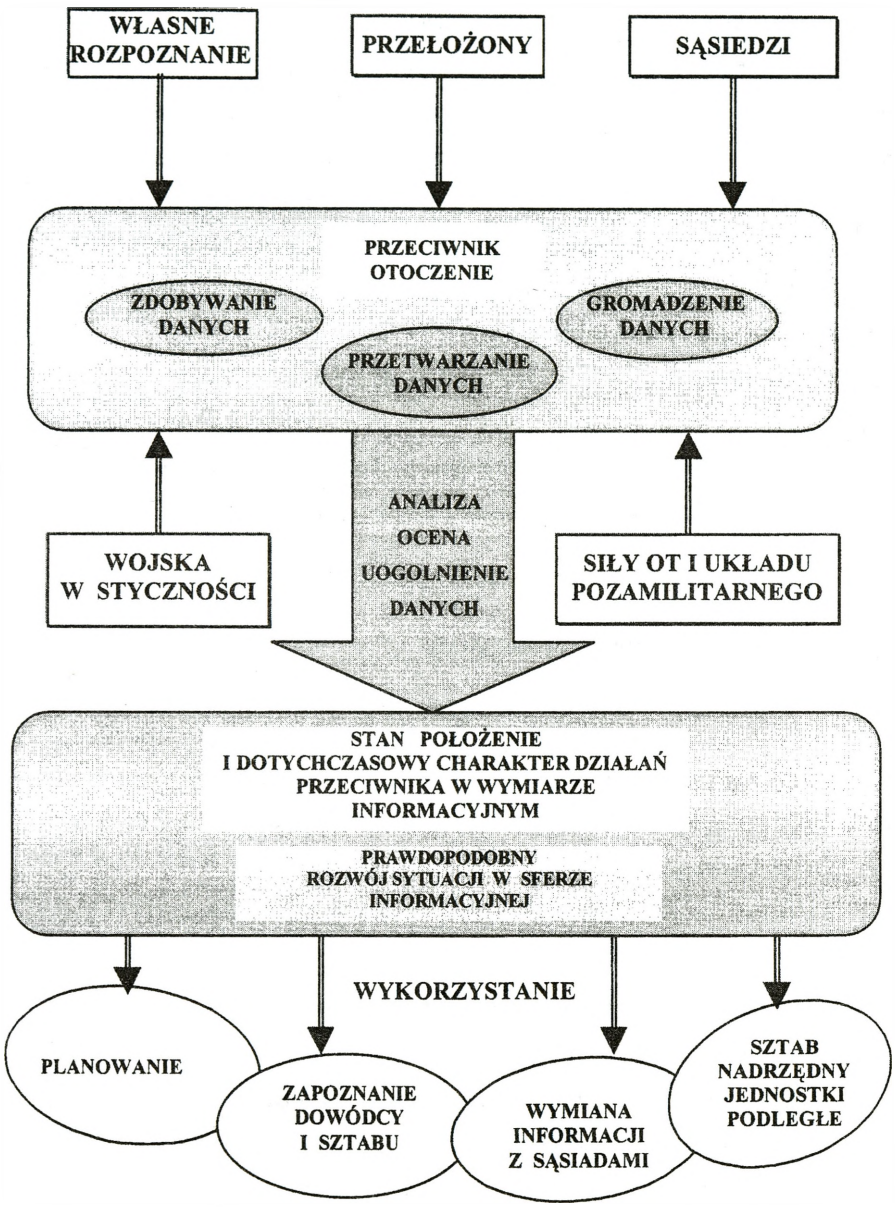
[40] Zadania realizowane w jej zakresie wykonuje przede wszystkim wydział obrony informacyjnej, którego strukturę przedstawiono na rysunku 4.2.

przeciwnika, a głównie o dotychczasowych działaniach jego systemów rozpoznania i zakłócania oraz o środowisku pola walki (o terenie, pogodzie, warunkach demograficznych, warunkach propagacji fal elektromagnetycznych itp.).



Rys. 4.6. Informacyjne przygotowanie pola walki w zakresie obrony informacyjnej

Należy ocenić również położenie oraz dotychczasowe działania wojsk własnych w sferze informacyjnej (rysunek 4.7.).



Rys. 4.7. Przebieg fazy ustalania położenia

Podstawę do ustalenia położenia przeciwnika powinny stanowić meldunki wojsk w styczności, rozkazy operacyjne i komunikaty szczebla nadrzędnego, meldunki od własnego potencjału rozpoznania (jeśli był lub jest w działaniu), informacje uzyskane od sąsiadów, sił obrony terytorialnej oraz układu pozamilitarnego.

Położenie sił i środków związku operacyjnego, głównie elementów systemu dowodzenia i naprowadzania uzbrojenia oraz rozpoznania i zakłócania informacyjnego, należy ustalać z kolei na podstawie meldunków od podwładnych. Zebrane dane powinny być porządkowane i ewidencjonowane oraz poddawane wstępnej analizie, ocenie i uogólnieniu. Opracowane w ten sposób dane stają się materiałem wyjściowym do procesu planowania obrony informacyjnej. Mogą być zasilane nimi również podległe wojska, sąsiedzi, specjaliści rodzajów wojsk i służb oraz inni uprawnieni zainteresowani.

Cechą szczególną fazy ustalania położenia z punku widzenia obrony informacyjnej jest to, że ma ona charakter działania ciągłego, podczas którego dane szczątkowe i rozpoznawcze poddaje się stałej weryfikacji. Jest przez to możliwa ich aktualizacja, uwiarygodnianie oraz poszerzanie obszaru wiedzy (rozpoznania).

4.2.2. Planowanie obrony informacyjnej

Z badań wynika, że spośród czterech faz cyklu decyzyjnego, faza druga – planowanie[41] obrony informacyjnej w działaniach obronnych związku operacyjnego odgrywa rolę szczególną, która związana jest z jej określoną specyfiką wynikającą z celu, zadań i nietypowych sposobów ich realizacji.

Zgodnie z ramowym układem cyklu decyzyjnego faza ta powinna być **podzielona na trzy następujące po sobie w logicznej kolejności etapy:**

- **ocena sytuacji na potrzeby obrony informacyjnej;**
- **decyzja i zamiar dowódcy w zakresie obrony informacyjnej;**
- **opracowanie dokumentów w zakresie obrony informacyjnej.**

Podstawowe czynności realizowane w ramach planowania obrony informacyjnej powinny być zatem zgodne z ramowym układem cyklu decyzyjnego w sztabie związku operacyjnego.

---

[41] Planowanie jest skoordynowanym i złożonym procesem sztabowym, ukierunkowanym na wypracowanie najlepszej metody wykonania postawionych zadań lub zadań możliwych do wykonania w przyszłości.

4.2.2.1. Ocena sytuacji w zakresie obrony informacyjnej

Z praktyki działania sztabów wynika, że etap ten zajmuje w fazie planowania działań specjalne miejsce. Ocenę sytuacji w sferze informacyjnej należy postrzegać jako ważny element ogólnej oceny sytuacji operacyjnej i położenia wojsk. W jej ramach określany jest obszar działań, dokonywana jest ocena środowiska pola walki (terenu, warunków meteorologicznych, spektrum elektromagnetycznego) oraz ocena zagrożeń (środków i systemów rozpoznania i zakłócania informacyjnego przeciwnika, zasad ich organizacji, eksploatacji i wykorzystania podczas działań bojowych), jak również ocena położenia, wyposażenia, stanu gotowości bojowej i możliwości własnych sił i środków walki informacyjnej. Pod względem zakresu może być ona ogólna[42] i szczegółowa.

Ocena szczegółowa polega na wszechstronnej analizie i prawidłowej ocenie wszystkich podstawowych czynników mających wpływ na pracę środków i działanie systemów informacyjnych oraz wyciągnięcie właściwych wniosków, co do zakresu prowadzenia przez przeciwnika aktywnych działań w sferze informacyjnej oraz możliwości obrony przed nimi przez wojska związku operacyjnego.

Ocena sytuacji w zakresie obrony informacyjnej powinna **obejmować:**

- **analizę zadania;**
- **informowanie operacyjne;**
- **ocenę czynników wpływających na wykonanie zadania i opracowanie koncepcji obrony informacyjnej dla poszczególnych wariantów działania związku operacyjnego;**
- **rozważenie i porównanie koncepcji prowadzenia obrony informacyjnej w poszczególnych wariantach działania związku operacyjnego.**

W toku **analizy zadania**[43] jako czynności w procesie oceny sytuacji precyzuje się, co i w jakim celu należy wykonać, aby zrealizować otrzymane zadanie.

---

[42] **Ocena ogólna** dokonywana jest w czasie pokoju, kryzysu i w okresie wojny. W ramach oceny ogólnej należy rozpatrzyć wszystkie posiadane dane o systemach walki informacyjnej przeciwnika oraz wojsk własnych, jak również o właściwościach ich pracy i eksploatacji. Dane o ogólnej sytuacji w sferze informacyjnej należy wykorzystać podczas planowania i organizowania całego kompleksu przedsięwzięć walki informacyjnej. Podczas rozwiązywania problemów obrony informacyjnej stają się one niezbędne również do określenia warunków, zasad i rodzajów pracy systemów dowodzenia wojskami i naprowadzania uzbrojenia oraz do ustalania wzajemnego wpływu pracy wchodzących w ich skład środków i systemów elektronicznych w procesie eksploatacji, jak też zapewnienia kompatybilności elektromagnetycznej podczas rozmieszczania środków o różnych parametrach taktyczno-technicznych w ugrupowaniu związku operacyjnego.

[43] Należy udzielić odpowiedzi na następujące pytania:
- jaki jest zamiar przełożonego oraz jaka jest rola związku operacyjnego w realizacji jego planu obrony informacyjnej?
- czego wymaga przełożony i jakie zadania należy wykonać dla zrealizowania jego zamiaru?
- jakie istnieją ograniczenia swobody działania (obszar, czas, siły)?
- jakie znaczące zmiany sytuacji nastąpiły od momentu podpisania rozkazu przez przełożonego?

Podczas analizy zadania dokonywanej w **zespole działań informacyjnych** prowadzona jest wstępna ocena posiadanych wiadomości o przeciwniku oraz środowisku pola walki i wskazanie luk w rozpoznaniu (wiedzy o przeciwniku). Analiza zadania to proces intelektualny zespołu, mający na celu rozpatrzenie również zadań walki informacyjnej, której ważnym komponentem jest obrona informacyjna. Powinna umożliwiać określenie **zadań obrony informacyjnej oraz sposobów ich wykonania na tle sytuacji operacyjnej i taktycznej, otrzymanych zadań ogólnowojskowych i ograniczeń swobody działania (czasu, obszaru[44] oraz sił)[45].**

Do głównych zadań zespołu działań informacyjnych podczas analizy zadania należy:

- wstępna analiza i ocena posiadanych wiadomości o środowisku działań oraz o siłach i środkach walki informacyjnej przeciwnika;
- wypracowanie wstępnej oceny przeciwnika;
- wypracowanie wniosków do dalszej pracy w procesie informacyjnego przygotowania pola walki;
- wypracowanie wniosków do dalszej pracy w zakresie planowania rozpoznania, zakłócania i obrony informacyjnej;
- wykonywanie bieżących zadań.

W toku **informowania operacyjnego** w sztabie związku operacyjnego szef zespołu działań informacyjnych przedstawia ogólną sytuację przeciwnika wraz z wstępną jego oceną i pierwszymi możliwymi wariantami jego działania, przeciwstawiającymi się wykonaniu zadania własnego.

W wyniku informowania operacyjnego szef zespołu działań informacyjnych zapoznawany jest z kolei z wieloma zagadnieniami, które mają znaczny wpływ na dalszy przebieg cyklu decyzyjnego, a mianowicie:

- sprecyzowane zadanie własne związku operacyjnego;
- myśl przewodnia dowódcy;
- kryteria do porównania wariantów działania;
- wytyczne do pracy sztabu wynikłe z wstępnej kalkulacji czasu.

---

[44] Obszar pola walki dla walczących wojsk dzieli się na strefę działania, strefę oddziaływania i strefę zainteresowania. W poszczególnych strefach należy uwzględnić różne wymiary pola walki: szerokość, głębokość, wysokość lub przestrzeń powietrzną, czas, spektrum elektromagnetyczne. Należy mieć na uwadze, że spektrum elektromagnetyczne nie jest ograniczone żadną strefą, lecz warunkami propagacji fal, a jego rozpatrywanie odnosi się zarówno do wymiaru lądowego, jak i powietrznego, w którym będzie działać przeciwnik [26;62].

[45] Problematyka ta powinna być przedmiotem zainteresowania przede wszystkim specjalistów **z grupy obrony informacyjnej**, która – jak przedstawiono w podrozdziale 4.15. – wchodzi w skład zespołu działań informacyjnych.

W sprecyzowanym zadaniu związku operacyjnego i myśli przewodniej dowódcy powinny **znaleźć odzwierciedlenie również problemy związane z osiąganiem zakładanych celów w ramach obrony informacyjnej.**

Etap ten kończy się postawieniem zadań przez szefa zespołu działań informacyjnych do dalszego przebiegu procesu informacyjnego przygotowania pola walki. Treścią tych zadań może być na przykład: liczba wariantów działania oraz aspektów oceny zagrożenia (również w sferze informacyjnej); terminy i forma wypracowania ocen; zakres i metody poszukiwania brakujących wiadomości; źródła danych itp.

Po tym etapie powinny być również wysłane zarządzenia przygotowawcze do wojsk; należy w nich ująć także problemy obrony informacyjnej.

Problematyka obrony informacyjnej powinna znaleźć odzwierciedlenie także w zadaniach i wytycznych specjalistów rodzajów wojsk i służb w ramach ich obowiązków w zakresie planowania i zabezpieczenia działań bojowych.

Celem **oceny czynników wpływających na wykonanie zadania przez związek operacyjny** jest ich zidentyfikowanie i szczegółowa analiza oraz określenie, w jaki sposób będą one wpływać na wykonanie zadań, a także ustalenie kilku realnych sposobów (wariantów) działania.

Z badań wynika, że **ocena czynników wpływających na wykonanie zadania w sferze informacyjnej obejmuje:**

- **środowisko pola walki (warunki terenowe, atmosferyczne, propagacyjne, stan bezpieczeństwa informacyjnego w obszarze przyszłych działań i in.);**
- **zagrożenie w sferze informacyjnej ze strony przeciwnika;**
- **położenie wojsk związku operacyjnego i ich obiektów podatnych na oddziaływanie ofensywnymi środkami walki informacyjnej;**
- **inne, które należy uwzględnić, np. czas.**

Do **oceny środowiska pola walki w sferze informacyjnej** zespół działań informacyjnych centrum dowodzenia SD związku operacyjnego powinien wykorzystać przytaczaną wcześniej procedurę informacyjnego przygotowania pola walki, w której powinny być uwzględniane również problemy rozwiązywane w ramach obrony informacyjnej[46], a mianowicie:

[46] Por.: rysunek 4.6.

– wpływ warunków terenowych na realizację przedsięwzięć obrony informacyjnej, zwłaszcza ze względu na możliwości techniczne środków rozpoznania i zakłócania przeciwnika oraz systemów dowodzenia i naprowadzania uzbrojenia związku operacyjnego. W tym celu należy wykorzystać oleat oceny terenu[47] (przeszkód terenowych), na którym zaznaczone są obszary trudno przejezdne, nieprzejezdne i ograniczające swobodę manewru. Dodatkowo należy określić obszary zakryte dla rozprzestrzeniania się energii elektromagnetycznej, w tym zakryte dla prowadzenia rozpoznania elektronicznego, rejony niesprzyjające rozmieszczeniu środków elektronicznych i walki informacyjnej [załącznik 13.].

– wpływ warunków atmosferycznych[48] na realizację przedsięwzięć obrony informacyjnej. W tym celu należy wykorzystać oleat oceny warunków atmosferycznych [załącznik 14.] sporządzony w zespole działań informacyjnych. Dodatkowo specjaliści z grupy obrony informacyjnej, wchodzącej w skład tego zespołu[49], powinni rozważyć wpływ pogody na teren i prowadzone działania oraz na rozmieszczenie i funkcjonowanie systemów dowodzenia i naprowadzania uzbrojenia, a także funkcjonowanie elementów rozpoznania i zakłócania wojsk własnych i przeciwnika.

– określenie dróg podejścia i korytarzy manewru. W tym celu należy wykorzystać oleat dróg podejścia i korytarzy manewru, który wykonuje się dla całego zespołu działań informacyjnych centrum dowodzenia SD związku operacyjnego. Specjaliści z grupy obrony informacyjnej, analizując oleaty dróg podejścia powinni dodatkowo określić przeszkody terenowe, które utrudnią lub uniemożliwią manewr siłami i środkami walki informacyjnej przeciwnika (rozpoznania i zakłócania) [załącznik 15.]. Obok lądowych dróg podejścia analizie należy poddać korytarze i drogi podejścia w przestrzeni powietrznej [62;64]. Specjaliści z grupy obrony informacyjnej powinni wykorzystać w tym celu ilustracje korytarzy powietrznych i dróg podejścia samolotów i śmigłowców przygotowane przez oficerów z zespołu lotnictwa wojsk lądowych, [załączniki 16,17,18.]. Wnioski z analizy dróg podejścia i korytarzy manewru pozwalają na wstępne określenie obszarów zainteresowania.

---

[47] Wykonywany jest dla całego sztabu przez zespół oficerów z grupy topograficznej oceny terenu. Specjaliści z grupy obrony informacyjnej mogą korzystać z oleatów i opisów przeszkód terenowych wykonanych przez tę grupę, a specjalistyczną ocenę terenu mogą prowadzić samodzielnie lub z udziałem specjalistów grupy topograficznej oceny terenu [26;62;64].

[48] Analizę tę wykonują oficerowie grupy prognozy pogody. Specjaliści z grupy obrony informacyjnej korzystają z opracowanej już prognozy i wyciągają wnioski dotyczące wpływu warunków atmosferycznych na pracę przede wszystkim technicznych środków dowodzenia i naprowadzania uzbrojenia oraz wchodzących w ich skład urządzeń elektronicznych [26;62;64].

[49] Struktura zespołu działań informacyjnych centrum dowodzenia SD związku operacyjnego przedstawiona została w podrozdziale 4.1.5.

Ocena czynników środowiska pola walki prowadzi do sformułowania następujących problemów dotyczących realizacji zadań obrony informacyjnej:

– w jaki sposób zamaskować rzeczywiste rejony rozmieszczenia wojsk, a przede wszystkim elementy systemów dowodzenia i naprowadzania uzbrojenia i gdzie zorganizować ich rejony pozorne?

– gdzie i w jakim stopniu pozorować przegrupowanie wojsk, a przede wszystkim elementy systemów dowodzenia i naprowadzania uzbrojenia dla osiągnięcia jego celu?

– jakie są możliwości wykorzystania warunków terenowych oraz zasobów miejscowych do realizacji przedsięwzięć bezpośredniej obrony informacyjnej?

Z przeprowadzonych analiz wynika, że **prognoza zagrożenia w sferze informacyjnej** stanowi część składową prognozy zagrożenia ogólnego, a w procesie wypracowywania koncepcji obrony informacyjnej jest jednym z filarów służących poprawnemu jej opracowaniu. Należy przy tym uwzględnić dwa aspekty. **Pierwszym** jest rozpatrywanie zagadnień związanych z położeniem, stanem i możliwościami oddziaływania informacyjnego oraz przewidywanym charakterem działań sił walki informacyjnej przeciwnika. **Drugim** – praktyczna wiedza o przygotowywaniu i prowadzeniu działań bojowych przez pododdziały walki informacyjnej przeciwnika. Poziom tej wiedzy często decyduje o skutkach prowadzonej obrony informacyjnej. W okresie pokoju przygotowaniem odpowiednich materiałów służących poszerzeniu wiedzy o siłach i środkach walki informacyjnej przeciwnika powinien zajmować się wydział badań i informowania[50]. Dane te powinny być uzupełniane na bieżąco z własnych źródeł rozpoznawczych i otrzymywanych od przełożonego.

Z badań wynika, że do zasadniczych **wymagań** stawianych zespołowi działań informacyjnych centrum dowodzenia SD związku operacyjnego prowadzącemu prognozę zagrożenia w sferze informacyjnej należą:

– szczegółowa i wnikliwa znajomość sił i środków walki informacyjnej przeciwnika;

– znajomość i świadomość celu działania;

– ciągłość i systematyczność pracy;

– umiejętność prognozowania zagrożenia;

– bazowanie na wiarygodnych danych;

– uwzględnienie wszystkich zależności i czynników, mogących mieć wpływ na przyszłe działania sił i środków walki informacyjnej przeciwnika;

---

[50] Problematyka ta była przedmiotem rozważań w podrozdziale 4.1.4.

- zachowanie w wynikach prognozy proporcji między szczegółowością i ogólnością;
- przestrzeganie terminowości podczas dokonywania prognozy;
- formułowanie wniosków z przeprowadzonej prognozy.

Prognoza zagrożenia w sferze informacyjnej powinna polegać na określeniu podstawowych danych dotyczących możliwości bojowych sił i środków walki informacyjnej przeciwnika. Dane dotyczące stanu etatowego i rodzajów środków walki informacyjnej, stanowisk dowodzenia poszczególnych szczebli, środków naprowadzania uzbrojenia, ugrupowania środków rozpoznania i zakłócania, a także środków elektronicznych, jakie mogą wystąpić na każdym szczeblu dowodzenia i w każdej jednostce organizacyjnej przeciwnika, powinny być gromadzone na bieżąco w komputerowych bazach danych. Z punktu widzenia obrony informacyjnej dokumenty oceny zagrożenia w sferze informacyjnej należy wykonywać w postaci tabel, schematów, wykresów oraz graficznie na oleatach ugrupowania sił i środków walki informacyjnej. Prognoza zagrożenia powinna znaleźć odzwierciedlenie również w aneksie „obrona informacyjna" do rozkazu operacyjnego związku operacyjnego oraz w rozkazach bojowych jednostek elektronicznych.

Wynika stąd, że **prognoza zagrożenia w sferze informacyjnej powinna obejmować**[51]**:**

- **analizę wzorców doktrynalnych działania sił i środków walki informacyjnej;**
- **opracowanie oleatu sytuacyjnego w sferze informacyjnej;**
- **wariantowanie zagrożeń w sferze informacyjnej;**
- **opracowanie oleatu zdarzeń w sferze informacyjnej;**
- **udział w opracowaniu oleatu wsparcia decyzji.**

Doktrynalne wzorce działań środków walki informacyjnej[52] powinny zawierać wszystkie dane o sposobach działania i sprzęcie przeciwnika, zawarte w regulaminach i instrukcjach taktyczno-technicznych. W czasie pokoju wzorce te są tworzone w formie graficznej i aktualizowane na podstawie obserwacji ćwiczeń dowódczo-sztabowych, ćwiczeń z wojskami, treningów, a także ze względu na zmiany w metodach szkolenia jednostek potencjalnego przeciwnika. Każda baza danych o siłach i środkach przeciwnika powinna być modyfikowana, szczególnie gdy stwierdza się wprowadzenie nowego sprzętu do jednostek przeciwnika, głównie jednostek walki informacyjnej.

---

[51] Por.: rysunek 4.6.

[52] Głównymi składowymi rozpatrywanymi w czasie przygotowania dowolnego wzorca doktrynalnego są: sposób prowadzenia działań przez przeciwnika w każdym etapie walki (marsz, natarcie, obrona); sposób zabezpieczenia i wsparcia logistycznego działań; struktura organizacyjna; sprzęt i wyposażenie [62;64].

Oprócz danych dotyczących systemów i środków walki informacyjnej należy gromadzić charakterystyki osobowo-zawodowe dowódców poszczególnych szczebli dowodzenia (jednostek walki informacyjnej i jednostek elektronicznych), co pozwoli na ustalenie, jakich decyzji należy spodziewać się po określonym dowódcy, i właściwą prognozę działań przeciwnika. Technika ich tworzenia jest różna w czasie pokoju i wojny. W czasie pokoju dane o przeciwniku powinny być dostarczane przez przełożonego, a w czasie wojny nowe informacje, potwierdzające działanie przeciwnika, jako pierwsze uzyskują pododdziały prowadzące rozpoznanie. Jest to więc obieg danych odwrotny w stosunku do pokojowego.

W obydwu sytuacjach grupa obrony informacyjnej zespołu działań informacyjnych centrum dowodzenia SD związku operacyjnego powinna być zobowiązana do posiadania aktualnej bazy danych o przeciwniku. Wzorce doktrynalne powinny być przechowywane w specjalnych bankach danych. Po rozpoczęciu działań wojennych wzorce opisujące siły i środki walki informacyjnej przeciwnika powinny być wykorzystywane do wskazywania ważnych obiektów, które należy rozpoznać lub zakłócić. Służą one także do wskazania celów, które powinny być niszczone środkami ogniowymi.

Informacje zawarte we wzorcach działań informacyjnych powinny być potwierdzane w zespole działań informacyjnych centrum dowodzenia SD związku operacyjnego, do którego napływają dane od jednostek pełniących dyżury bojowe lub od przełożonego. Zweryfikowane dane służą do opracowania modeli doktrynalnych w czasie oceny zagrożenia przed rozpoczęciem działań wojennych, a w czasie jej trwania – do ich korekty w zależności od zmian w ugrupowaniu przeciwnika. W zespole działań informacyjnych centrum dowodzenia SD związku operacyjnego tworzy się kilka oddzielnych wzorców działań informacyjnych przeciwnika. Pierwszy zawiera dane o węzłach łączności, drugi dotyczy pozostałych urządzeń emitujących energię elektromagnetyczną (np. stacji radiolokacyjnych), a trzeci określa zasady użycia sił i środków walki informacyjnej, za który bezpośrednią odpowiedzialność powinni ponosić specjaliści z grupy obrony informacyjnej. Przykładowy oleat – walka informacyjna (rozpoznanie i zakłócanie) w działaniach zaczepnych przeciwnika zamieszczono w załączniku 19[53].

Do pełnego zobrazowania zagrożenia w sferze informacyjnej niezbędna jest również analiza działań przeciwnika powietrznego i systemów przeciwlotniczych. Dlatego ze szczególną uwagą powinno się analizować wzorce doktrynalne działań samolotów (śmigłowców)

[53] Wykonując wzorce doktrynalne systemów walki informacyjnej przeciwnika należy dokonać oceny zagrożenia o jeden szczebel w dół, gdy wojska własne są w obronie, a o dwa szczeble w dół, gdy prowadzi się natarcie [62].

i elementów obrony przeciwlotniczej. W razie potrzeby należy wykonać odpowiednie wzorce porównawcze zasięgów wybranych stacji radiolokacyjnych związku operacyjnego w odniesieniu do środków napadu powietrznego przeciwnika [62;64].

Oleat sytuacyjny w sferze informacyjnej[54] powstaje wyniku połączenia: oleatu oceny terenu; oleatu kierunków podejścia i korytarzy manewru; wzorca doktrynalnego sposobu działania przeciwnika. Oleat ten wykonuje grupa obrony informacyjnej na podstawie:

- danych o sytuacji bieżącej (z rozpoznania i zakłócania informacyjnego);
- wiadomości od przełożonego;
- danych od jednostek osłonowych i sąsiadów;
- innych źródeł (np. uchodźców, dezerterów, wojsk obrony terytorialnej, układu pozamilitarnego).

Dokument ten powinien odzwierciedlać graficzny obraz sytuacji bojowej w sferze informacyjnej połączony z koncepcją doktrynalną, zgodną z obowiązującymi zasadami rozmieszczenia sił i środków oraz prawdopodobnym zamiarem przeciwnika, w odniesieniu do terenu i warunków meteorologicznych. Tak przygotowany oleat powinien stanowić podstawę do dalszych rozważań nad prawdopodobnym działaniem sił i środków walki informacyjnej przeciwnika[55].

Oleat należy sporządzać w takiej skali jak wykorzystywane mapy[56]. Wiadomości z banków danych (wzorce ugrupowania) należy przerysowywać na oleaty z zachowaniem norm, a następnie się je uaktualnia na podstawie bieżących danych. Dla przejrzystego zobrazowania sytuacji wszystkie potwierdzone wiadomości o przeciwniku uzyskane od przełożonego i podwładnych należy traktować jako pewne i nanosić je linią ciągłą, natomiast położenie jednostek walki informacyjnej wynikające z zasad doktrynalnego działania należy przedstawić liniami przerywanymi. W ten sposób powstanie prawdopodobny obraz aktualnego położenia elementów walki informacyjnej wojsk przeciwnika.

Oleat sytuacyjny w sferze informacyjnej [załącznik 20.] powinien stanowić dla specjalistów grupy obrony informacyjnej pomocnicze narzędzie, niezbędne do określenia potrzeb w zakresie uzupełnienia danych o elementach walki informacyjnej.

---

[54] Opracowanie tego oleatu rozpoczyna wg poglądów amerykańskich kolejny etap informacyjnego przygotowania pola walki, który nazywany jest integracją zagrożeń. L. Ciborowski, R. Polko, „Planowanie i organizowanie walki zbrojnej według poglądów NATO, cz. II: Informacyjna preparacja pola walki", wyd. AON Warszawa 1996, s. 29.

[55] W zespole G 2 mogą być wykonywane jeszcze dwa oleaty bieżącej sytuacji: na potrzeby rozpoznania i zakłócania informacyjnego.

[56] L. Ciborowski, R. Polko, „Planowanie i organizowanie walki zbrojnej wg poglądów NATO, cz. II. Informacyjna preparacja pola walki", AON, Warszawa 1996, s. 36.

Podczas oceny sytuacji w sferze informacyjnej należy poddać analizie i w miarę możliwości ustalić:

– ogólną liczbę obiektów walki informacyjnej przeciwnika w strefie odpowiedzialności rozpoznawczej związku operacyjnego;

– liczbę obiektów rozpoznania przeciwnika w strefie odpowiedzialności rozpoznawczej związku operacyjnego z podziałem na pasma częstotliwości i rodzaje środków;

– liczbę obiektów zakłócania przeciwnika w obszarze działania związku operacyjnego (w jego strefie odpowiedzialności rozpoznawczej) z podziałem na pasma częstotliwości i rodzaje środków;

– liczbę i rodzaj obiektów walki informacyjnej przeciwnika, które ze względu na promieniowaną energię mogą się znaleźć w zasięgu rozpoznania w trakcie realizacji zadania przez związek operacyjny.

W zakończeniu oceny sytuacji w sferze informacyjnej należy sprecyzować wnioski wynikające z potrzeb obrony informacyjnej. Niezbędne jest określenie liczby obiektów i źródeł, których rozpoznanie jest konieczne (lub pożądane) z uwagi na zadania obronne realizowane przez związek operacyjny. Ponadto należy ustalić priorytety rozpoznawcze z grupą rozpoznania zespołu G 2 co do poszczególnych obiektów i źródeł.

Kolejny etap pracy specjalistów grupy obrony informacyjnej powinien obejmować wypracowanie prawdopodobnych wariantów działania przeciwnika w sferze informacyjnej. Wypracowane warianty należy udostępnić pozostałym grupom zespołu działań informacyjnych, oficerom zespołu planowania centrum dowodzenia SD związku operacyjnego, a także specjalistom zespołu dowodzenia i łączności z centrum wsparcia dowodzenia oraz zespołom specjalistycznym z centrum wsparcia działań do koordynowania działań jednostek wykonujących zadania bojowe.

Wariantowanie zagrożeń w sferze informacyjnej powinno być prowadzone z uwzględnieniem oceny przygotowanej przez specjalistów z grupy rozpoznania[57] zespołu działań informacyjnych centrum dowodzenia SD związku operacyjnego. Na tej podstawie specjaliści z grupy obrony informacyjnej powinni określić prawdopodobny wariant działania przeciwnika w sferze informacyjnej oraz sprecyzować potrzeby w zakresie uzupełniania brakujących danych. W wypracowanym wariancie powinno się uwzględnić wpływ pogody i terenu na działania przeciwnika oraz w określonym czasie opisowo lub w sposób graficzny

[57] Zakres tej oceny przedstawiono w podrozdziale 4.1.5.

prognozować, jak jego siły i środki będą wykonywać manewr (np. wzdłuż jakich dróg podejścia i korytarzy manewru, z wykorzystaniem jakich środków łączności). Ponadto należy brać pod uwagę, w jakim zakresie działanie przeciwnika może odbiegać od wzorców doktrynalnych lub w jaki sposób przeciwnik może zmieniać szerokość i głębokość ugrupowania oraz rozmieszczenie elementów ugrupowania bojowego, aby sprostać wymaganiom pogody i terenu.

Rozważając wpływ pogody i terenu na działania przeciwnika odbiegające od wzorców doktrynalnych, należy dokonać analizy jego możliwości w zakresie zapewnienia łączności, wykrywania celów, kierowania ogniem, rozpoznania i zakłócania informacyjnego. Opracowywany wariant zagrożenia w sferze informacyjnej powinien uwzględniać dane z rozpoznania, które pozwolą na ustalenie środków walki informacyjnej przeciwnika oraz potencjalnych rejonów ich rozmieszczenia.

Należy rozważyć także działania przeciwnika mające na celu maskowanie stanowisk dowodzenia (punktów obserwacyjnych) przed rozpoznaniem i zakłócaniem. W obrębie danego segmentu korytarza manewru należy analizować przewidywane rozmieszczenie jednostek przeciwnika (węzłów łączności) oraz innych środków emitujących energię elektromagnetyczną. W trakcie wariantowania zdarzeń w sferze informacyjnej powinny zostać rozważone sposoby i możliwości działania przeciwnika, szczególnie te, które powodują uzyskanie korzystnego stosunku sił, tempa działań oraz zaskoczenia. Analiza danych z rozpoznania i wariantów zdarzeń informacyjnych powinna być skoncentrowana na określeniu linii widzialności optycznej i radiowej w pasach (rejonach) działań pierwszorzutowych związków taktycznych. Ponadto należy ustalić obszary nadające się do ukrycia i maskowania bądź ugrupowania wojsk, bowiem zmniejszają one możliwość rozpoznania. Należy określić także obszary, które wojska własne mogą wykorzystać do tych samych celów. Analiza musi uwzględniać rejony, z których przeciwnik może uzyskać jak największy zasięg rozpoznania i zakłócania.

W wariantach zdarzeń w sferze informacyjnej należy ujmować również charakterystyki emisji elektromagnetycznych poszczególnych elementów oraz ich umiejscowienie. Pogoda i teren mają wpływ na wykorzystanie systemów rozpoznania i zakłócania przeciwnika, przede wszystkim zaś na pracę urządzeń emitujących energię elektromagnetyczną, wpływając na rozmieszczenie poszczególnych elementów tych systemów. Warianty użycia źródeł energii elektromagnetycznej powinny uwzględniać przyszłe działania i zmieniać się w zależności od czasu i miejsca na polu walki. Specjaliści grupy obrony informacyjnej powinni dokonywać analiz systemów elektronicznych i węzłów objętych wzorcami doktrynalnymi, współdziałając z grupami rozpoznania i zakłócania informacyjnego.

Po rozpoczęciu zbierania danych przez własne systemy rozpoznawcze, do poszczególnych komórek zespołu działań informacyjnych powinny być przekazywane aktualne dane o ugrupowaniu przeciwnika oraz o jego działaniach również w sferze informacyjnej. Specjaliści z grupy obrony informacyjnej powinni wstępnie opracowywać napływające dane i porównywać je z danymi zawartymi w wariantach sytuacji oraz we wzorcach zagrożeń. Pozwala to na:

- przekazywanie aktualnych danych przełożonemu i podległym jednostkom w trakcie wymiany wiadomości o przeciwniku;
- dokonywanie korekty wariantów zagrożenia w sferze informacyjnej;
- dokonywanie przez grupę wraz ze współpracującymi specjalistami z innych rodzajów służb identyfikacji emiterów energii elektromagnetycznej;
- korygowanie lokalizacji obiektów walki informacyjnej przeciwnika na podstawie ich cech identyfikacyjnych, ustalenie linii rozgraniczenia wojsk oraz wyselekcjonowanie pod względem informacyjnym ważnych celów (obiektów).

Warianty działania przeciwnika powinny być poddawane weryfikacji za pomocą komputerowych i symulacyjnych modeli oceny zagrożenia w sferze informacyjnej[58], w trakcie gier wojennych (taktycznych) itp.

Efektem pracy specjalistów z grupy obrony informacyjnej powinno być opracowanie prawdopodobnego wariantu działania przeciwnika w sferze informacyjnej, po czym należy dokonać jego ostatecznej weryfikacji podczas spotkań roboczych zespołu działań informacyjnych i zespołu planowania centrum dowodzenia SD związku operacyjnego. Finalnym efektem tych spotkań powinien być **wybór wariantu zagrożenia w sferze informacyjnej**[59] (wariant powinien uwzględniać działania przeciwnika przewidywane przez grupę rozpoznania z zespołu działań informacyjnych). Na jego podstawie należy przystąpić do szczegółowego planowania obrony informacyjnej oraz użycia własnych pododdziałów walki informacyjnej. Jeśli wariant zagrożenia proponowany przez zespół działań informacyjnych nie zostanie zaakceptowany, należy rozpatrzyć pozostałe warianty, wcześniej odrzucone.

---

[58] Do oceny zagrożenia radioelektronicznego, np. systemu łączności związku operacyjnego można wykorzystać modele komputerowe i symulacyjne: A. Barczak, J. Janczak, K. Mamcarz, „Komputerowy model oceny zagrożenia radioelektronicznego perspektywicznego systemu łączności związku operacyjnego wojsk lądowych". Praca naukowo-badawcza, Zegrze: WSOWŁ 1996; A. Barczak, J. Janczak, K. Mamcarz, „Model symulacyjny zagrożenia radioelektronicznego systemu łączności związku operacyjnego wojsk lądowych". Praca naukowo-badawcza, Zegrze WSOWŁ, 1997.

[59] Wynikiem analizy są wnioski – odpowiedzi na pytania: co?, kiedy?, gdzie?; jak?, w jakim celu?

Przy wariantowaniu działań przeciwnika powinien również powstać plan alternatywny (zapasowy), który powinien znacząco odbiegać od wzorców doktrynalnych. Taki wariant działania przeciwnika, zazwyczaj przeczy logice działania i czasami jest sprzeczny z dotychczas znanymi zasadami walki. Planem alternatywnym może być także odrzucony wariant zagrożenia z niektórymi elementami działania przeciwnika sprzecznymi z obowiązującymi normami. Przykładowy wariant zagrożeń w sferze informacyjnej na kierunku działania pierwszorzutowej dywizji związku operacyjnego ilustruje załącznik 21.

Oleat zdarzeń w sferze informacyjnej powinien być sporządzany przez specjalistów grupy obrony informacyjnej (w uzgodnieniu z grupą rozpoznania i grupą zakłócania zespołu działań informacyjnych) na podstawie wybranego wariantu działania. Swoją formą nie powinien odbiegać od oleatu zdarzeń wykonywanego przez oficerów z grupy rozpoznania[60]. **W grupie obrony informacyjnej powinno być eksponowane położenie sił i środków walki informacyjnej przeciwnika, zazwyczaj w określonych odstępach czasowych.** Oleat zdarzeń powinien być sporządzany na podstawie najbardziej prawdopodobnego wariantu działania przeciwnika. Położenie wojsk przeciwnika, w zależności od szczebla na jakim się rozpatruje stopień zagrożenia, należy oceniać według linii czasowych (co 1, 2, a nawet co 4 godziny lub według zasięgu środków ogniowych[61]). Linie czasowe (TPL)[62] powinny uwzględniać i ujmować wszystkie drogi podejścia i korytarze manewru. Nowe położenie przeciwnika należy zaznaczać przewidywaną rubieżą w terenie, niekiedy rubież ta powinna otrzymać nazwę własną. Poza tym należy określić rejony (obszary) szczególnego zainteresowania (NAI)[63]. Są to z zasady takie obszary, w których elementy rozpoznania są w stanie określić sposób działania przeciwnika. W ramach obszarów NAI należy wyznaczyć punkty kontrolne, w stosunku do których trzeba rozmieścić elementy rozpoznawcze. Połączenie danych z własnych elementów rozpoznawczych oraz z rozpoznania przełożonego, pozwala na określenie ważnych zdarzeń na polu walki oraz wytypowanie elementów walki informacyjnej, które dostarczają danych na temat kierunków działań prowadzonych przez przeciwnika i celów, jakie pragnie osiągnąć. **Specjalista grupy obrony informacyjnej dokonujący analizy powinien dostrzec różnicę pomiędzy zdarzeniami, które już nastąpiły i zostały rozpoznane, a tymi, które są tylko przewidywane. Ponadto powinien kontrolować działania przeciwnika zmierzające do wprowadzania w błąd, aby nie dopuścić do skupienia wysiłku własnych jednostek rozpoznania na obiektach (obszarach) pozornych.**

---

[60] W wypadku ograniczonego czasu na planowanie może być wykonywany wspólny oleat zdarzeń dla całego zespołu działań informacyjnych SD związku operacyjnego.

[61] W armii amerykańskiej co godzinę, dwie, lub cztery w zależności od szczebla dowodzenia, a w Bundeswehrze ilość czasu określana jest wg zasięgu środków ogniowych.

[62] TPL – ang. Time Phase Line.

[63] NAI – ang. Named Areas of Interest.

Po rozpoczęciu działań bojowych wiedza o tym, gdzie i kiedy może nastąpić istotne zdarzenie na polu walki, może zostać wzbogacona[64]. Należy mieć na uwadze, że rejony zainteresowania celami w sferze informacyjnej nie zawsze będą się znajdować na drogach podejścia. Często występować będą poza nimi ze względu na specyfikę pracy oraz możliwości bojowe sprzętu, głównie elektronicznego. Rejony te są jednak ważne, gdyż znajdują się w najbardziej prawdopodobnych miejscach decydujących zdarzeń czy też działań na polu walki oraz mogą w nich występować cele wysoko opłacalne[65].

Rejony zainteresowania powinny stanowić podstawę do wariantowania zdarzeń w sferze informacyjnej, ponieważ wskazują kierunki działania przeciwnika, ogniskują zbieranie danych oraz są uwzględniane w opracowaniu wymagań wobec informacji pozyskiwanych przez rozpoznanie. Aby trafnie określić zamiary przeciwnika, jego aktywność w obrębie drogi podejścia lub obszaru określonego jako NAI może być porównana ze wskaźnikami aktywności występującymi w obszarze innego NAI, w obrębie innej drogi podejścia. Poziom aktywności może również stanowić dla rozpoznania i zakłócania informacyjnego wskazówkę o istnieniu jakiegoś urządzenia w obrębie obszaru niekontrolowanego. Rejony zainteresowania są bowiem celami dla zakłócania informacyjnego. Numeracja NAI powinna być ustalona podczas spotkań koordynacyjnych wewnątrz zespołu działań informacyjnych. Ustalenia te są niezbędne dla wyeliminowania błędów i dwuznaczności w oznaczeniach lub oznaczeń dublujących, ponieważ niektóre obszary NAI mogą się pokrywać w tym samym miejscu w różnych zespołach. Przykład oleatu zdarzeń w sferze informacyjnej w pasie działania pierwszorzutowej dywizji związku operacyjnego przedstawiono w załączniku 22[66].

Oleat wsparcia decyzji w zasadzie wykonuje zespół planowania centrum dowodzenia SD związku operacyjnego, przy współudziale zespołu działań informacyjnych oraz zespołu artylerii z centrum wsparcia działań[67]. **Specjalista zespołu działań informacyjnych powinien wrysować na oleat wsparcia decyzji zaakceptowany wariant działania przeciwnika (w którym należy uwzględnić również potencjał jego walki informacyjnej), dający podstawy do jego wykonania.**

Oleat wsparcia decyzji – jak określono w materiałach źródłowych [23;62; 64;92] jest końcowym i zarazem najważniejszym dokumentem procesu informacyjnego przygotowania pola walki. Wykonywany jest na potrzeby śledzenia prognozowanej sytuacji przeciwnika i powinien być pomocny dowódcy w procesie podejmowania decyzji. Oleat wsparcia decyzji nie ogranicza kompetencji dowódcy, lecz wskazuje wydarzenia oraz możliwe działania przeciwnika, w określonym miejscu i czasie, które wymagać będą podjęcia określonych decyzji.

---

[64] Przeciwnik będzie dążyć do ograniczenia strumienia danych o swoim działaniu i stan naszej wiedzy może nie zmienić się mimo rozpoczęcia działań.

[65] Cele o znaczeniu decydującym dla działania wojsk przeciwnika.

[66] Koncepcja rozwoju sytuacji elektronicznej po stronie przeciwnika powinna znaleźć również odzwierciedlenie w aneksie „Obrona informacyjna" (pkt 3b).

[67] Jego wykonanie jest „podstawową funkcją wyznaczonej w tym celu przez dowódcę triady".

Temu właśnie służą określone na oleacie wsparcia decyzji tzw. obszary zainteresowania celami (TAI[68]), punkty decyzyjne (DP[69]) i linie czasowe. Przykład oleatu wsparcia decyzji w pasie działania pierwszorzutowej dywizji związku operacyjnego z uwzględnieniem stery informacyjnej przedstawiono w załączniku 23.

Z oceny zagrożeń w sferze informacyjnej wypływają odpowiedzi na pytania[70]:

– w jakim rejonie (kierunku) i w jakim czasie – z uwagi na działanie przeciwnika – należy określić punkt ciężkości w zakresie realizacji przedsięwzięć obrony informacyjnej?

– przeciwko jakim rodzajom i środkom walki informacyjnej należy przede wszystkim zaplanować przedsięwzięcia obrony informacyjnej?

– w jaki sposób najskuteczniej wprowadzić poszczególne elementy rozpoznania przeciwnika w błąd?

– jakie środki walki informacyjnej należy zniszczyć, jakie obezwładnić zakłóceniami, lub jakie zastosować przeciwko nim przedsięwzięcia obrony informacyjnej?

Ocena wojsk związku operacyjnego w zakresie obrony informacyjnej powinna obejmować, jak wskazują doświadczenia z ćwiczeń prowadzonych w AON w latach 1996 – 2000, poszczególne komponenty systemów dowodzenia i naprowadzania uzbrojenia związku operacyjnego, a w szczególności systemy (sieci) łączności i informatyki, systemy radionawigacyjne, systemy naprowadzania uzbrojenia i systemy walki informacyjnej. Należy prowadzić ją we współdziałaniu z zespołem planowania centrum dowodzenia SD związku operacyjnego, z zespołem dowodzenia i łączności centrum wsparcia dowodzenia oraz z zespołami specjalistycznymi centrum wsparcia działań. Ponadto należy dokonać oceny czynnika czasu oraz warunków i możliwości zabezpieczenia logistycznego (materiałowego i technicznego).

W **ocenie systemów (sieci) łączności i informatyki**[71] – w uzgodnieniu z zespołem dowodzenia i łączności centrum wsparcia dowodzenia stanowiska dowodzenia związku operacyjnego – należy rozpatrzyć:

---

[68] TAI – ang. Target Areas of Interest.

[69] DP – ang. Decision Point.

[70] Proces prognozowania działań kończy się z chwilą podjęcia decyzji przez dowódcę i ogłoszenia zamiaru. Zespół G 2, niezależnie od tego jak obszerna i dokładna wydaje się być dokonana analiza i ocena terenu i pogody, zawsze musi liczyć się z innym, odmiennym od przyjętych schematów działaniem przeciwnika oraz zawsze musi być przygotowany do powtórzenia cyklu ocen i przeprowadzenia analiz od początku.

[71] W specjalistycznej literaturze informatycznej systemy łączności i informatyki określane są jako systemy teleinformatyczne [45;48;122].

– rodzaj i liczbę stanowisk dowodzenia i węzłów łączności, ich przestrzenne rozmieszczenie, strukturę oraz sposób rozwinięcia w terenie, system ochrony i obrony;

– rodzaj i liczbę kanałów transmisji (relacji) między poszczególnymi węzłami łączności i indywidualnymi użytkownikami oraz ich strefy dostępności elektromagnetycznej i podatność na rozpoznanie[72];

– wykorzystanie poszczególnych pasm widma elektromagnetycznego (poszczególnych częstotliwości), rodzajów środków i zasady ich eksploatacji podczas walki;

– parametry techniczne określonych rodzajów środków łączności rzutujące na możliwości ich rozpoznania i zakłócania;

– sposoby i zakres utajniania wiadomości, możliwości maskowania i pozorowania elementów sieci łączności oraz inne dane rzutujące na pracę środków łączności;

– podatność stacjonarnej sieci łączności sił zbrojnych, sieci telekomunikacyjnej państwa, a także rozgłośni radiowych i telewizyjnych na oddziaływanie informacyjne.

Ocenie poddawany powinien być także stan bezpieczeństwa środków informatycznych będących w wyposażeniu zespołów funkcyjnych poszczególnych stanowisk dowodzenia. W tym celu powinny być analizowane dokumenty normatywne z zakresu bezpieczeństwa i przepisy prawne obowiązujące w wojskach własnych.

Wnioski z oceny systemów (sieci) łączności i informatyki powinny dotyczyć: oceny stopnia zagrożenia poszczególnych systemów, możliwości organizacji obrony przed rozpoznaniem i zakłócaniem jego najważniejszych elementów składowych, a także przed niszczeniem węzłów łączności, kablowych linii łączności (przewodowych i światłowodowych) oraz ważnych środków łączności, zapewnienia kompatybilności elektromagnetycznej obszaru odpowiedzialności obronnej związku operacyjnego oraz sposobów współdziałania w realizacji tych zadań z innymi rodzajami wojsk.

W **ocenie systemów radionawigacyjnych** – w uzgodnieniu z zespołem lotnictwa wojsk lądowych centrum wsparcia działań stanowiska dowodzenia związku operacyjnego – należy rozpatrzyć:

– rodzaj i przeznaczenie systemu, zasięg jego funkcjonowania, powiązanie między systemami oraz urządzeniami autonomicznymi;

– parametry taktyczno–techniczne systemów i ich wpływ na sposoby prowadzenia działań bojowych i taktykę użycia środków walki;

---

[72] Metodykę określania stref dostępności elektromagnetycznej przedstawiono w podrozdziale 2.2.1.1.

– liczbę i dyslokację punktów radionawigacyjnych, jeśli są one rozmieszczone w rozpatrywanym obszarze działań.

Dużą wagę należy przywiązywać do oceny satelitarnych systemów radionawigacyjnych ze względu na ich bardzo duży zasięg i szerokie wykorzystanie przez różne rodzaje sił zbrojnych i wojsk.

Wnioski z oceny powinny dotyczyć określenia stopnia zagrożenia poszczególnych rodzajów systemów, możliwości obrony przed rozpoznaniem, zakłócaniem oraz niszczeniem poszczególnych jego elementów. Mogą także dotyczyć ustalenia wpływu funkcjonowania tych systemów na sposób prowadzenia działań obronnych przez związek operacyjny.

W **ocenie systemów i środków naprowadzania uzbrojenia** oraz środków identyfikacji celów – w uzgodnieniu z zespołami specjalistycznymi centrum wsparcia działań stanowiska dowodzenia związku operacyjnego – należy rozpatrzyć:

– rodzaj systemów, ich zasięg, warunki, w jakich mogą pracować, techniki stosowane w sterowaniu;

– częstotliwości i zakresy pasm, na których pracują;

– możliwości zmiany warunków sterownia;

– punkty kierowania i ich wrażliwość na rozpoznanie, zakłócanie oraz niszczenie ogniowe;

– posiadane zabezpieczenia.

Podczas oceny systemów kierowania i sterowania należy zwrócić uwagę na dużą różnorodność ich elementów nawet w jednym rodzaju środków. Często głowica jest wymienna, każdy zaś rodzaj głowicy ma inny system naprowadzania. Należy też zwrócić uwagę na warunki, w jakich poszczególne rodzaje środków mogą być użyte. Niewłaściwe warunki terenowe lub atmosferyczne mogą uniemożliwić użycie określonego rodzaju systemu.

Wnioski z takiej oceny powinny dotyczyć: określenia stopnia zagrożenia poszczególnych rodzajów środków walki; możliwości ich obrony przed rozpoznaniem, szczególnie w zakresie maskowania i pozorowania celów; możliwości ich obrony przed zakłócaniem; możliwości wykorzystania warunków terenowych i atmosferycznych do ograniczenia użycia broni precyzyjnego rażenia.

W **ocenie systemów i środków walki informacyjnej** – w uzgodnieniu z grupą rozpoznania i zakłócania zespołu działań informacyjnych centrum dowodzenia SD związku operacyjnego – należy rozpatrywać odporność systemów rozpoznania i zakłócania na oddziaływanie informacyjne przeciwnika.

W **ocenie systemów i środków rozpoznania** należy uwzględnić:

- rodzaj środków rozpoznania radioelektronicznego, radiolokacyjnego, optoelektronicznego, czujnikowego i informatycznego;
- przewidywany ich zasięg i możliwości rozpoznawcze;
- parametry taktyczno–techniczne poszczególnych rodzajów środków i ich odporność na oddziaływanie ogniowe i elektroniczne;
- ich cechy rozpoznawcze, ochronę i obronę;
- taktykę ich użycia podczas walki, możliwości zastąpienia innymi środkami oraz powiązanie systemów rozpoznania z innymi środkami walki.

Ocenie tej powinny podlegać zarówno środki naziemne, jak i powietrzne, a w obszarze nadmorskim – także środki sił morskich.

W **ocenie środków i systemów zakłócania** należy uwzględnić:

- rodzaj i liczbę systemów w obszarze odpowiedzialności obronnej związku operacyjnego oraz sił powietrznych;
- ich możliwości bojowe i techniczne, warunki, czas i sposoby użycia;
- rejony rozwinięcia (strefy dyżurowania samolotów), obszary oraz głębokość oddziaływania;
- możliwości niszczenia obiektów zakłócania przeciwnika za pomocą broni samosterującej naprowadzonej na źródło promieniowania energii elektromagnetycznej;
- możliwości i przewidywany zasięg użycia środków pasywnych oraz warunki atmosferyczne sprzyjające użyciu tego rodzaju środków;
- możliwości użycia broni elektromagnetycznej (powodującej niszczenie układów elektronicznych), obszary jej użycia oraz zasięg zniszczeń.

Przy ocenie środków zakłócania należy uwzględnić też rodzaj tych środków, które mogą być najbardziej zagrożone.

Wnioski z oceny powinny dotyczyć określenia punktów ciężkości, na których należy skupić główny wysiłek sił i środków zakłócania. Stanowią ponadto podstawę do sprecyzowania zadań w zakresie niszczenia poszczególnych, ważnych obiektów przeciwnika w okresie działań bojowych i operacji oraz przewidywanych zadań wojsk. Mają niezmiernie istotne znaczenie w związku z potrzebą wykonania przedsięwzięć w zakresie obrony informacyjnej własnych, czynnych systemów dowodzenia wojskami i zabezpieczenia kompatybilności elektromagnetycznej środków elektronicznych różnych rodzajów wojsk.

Ponadto w uzgodnieniu z zespołem saperów centrum wsparcia działań SD związku operacyjnego należy określić specjalistyczne zadania wchodzące w zakres fortyfikacyjnej rozbudowy przedstawionych wyżej komponentów systemu dowodzenia i naprowadzania uzbrojenia, a także zakres inżynieryjnej rozbudowy oraz niezbędną liczbę makiet i odbijaczy do pozorowania tych komponentów.

Ocena czynnika czasu ma szczególne znaczenie dla rozwiązywania problemu zsynchronizowania trzech elementów: sił, przestrzeni i czasu, to znaczy zidentyfikowania rozwiązań pozwalających na rozmieszczenie wystarczających sił we właściwym obszarze oraz w nakazanym czasie. Jest czynnikiem ograniczającym swobodę działania. Dotyczy to również realizacji przedsięwzięć obrony informacyjnej. Wnioski wynikające z oceny czasu powinny dotyczyć:

- określenia czasu niezbędnego na zaplanowanie szczegółowych zadań obrony informacyjnej w działaniach obronnych związku operacyjnego;
- czasu rozpoczęcia i okresów organizowania przedsięwzięć pozornych z punktu widzenia faktycznych działań wojsk;
- rozpoczęcia i zakończenia realizacji poszczególnych zadań obrony informacyjnej;
- czasu prowadzenia kontroli zaplanowanych przedsięwzięć obrony informacyjnej.

Oceny warunków i możliwości zabezpieczenia logistycznego powinna być dokonywana w uzgodnieniu z zespołem materiałowym i technicznym centrum zabezpieczenia działań stanowiska dowodzenia związku operacyjnego. Podczas tej oceny należy rozpatrywać:

- ilość, rodzaj uzbrojenia, sprzętu zdobycznego i uszkodzonego oraz możliwości wykorzystania go do realizacji przedsięwzięć obrony informacyjnej (w ramach maskowania);
- ilość, rodzaj etatowych środków i materiałów maskowania niezbędnych do realizacji poszczególnych zadań obrony informacyjnej (w ramach maskowania)[73];
- ilość środków niezbędnych do prowadzenia kontroli obrony informacyjnej.

Uogólnione wnioski z oceny przedstawionych wyżej czynników powinny prowadzić do wypracowania koncepcji prowadzenia obrony informacyjnej w odniesieniu do ustalonych w zespole planowania centrum dowodzenia SD związku operacyjnego i zaprezentowanych w toku **odprawy koordynacyjnej** wariantów działań obronnych związku operacyjnego.

---

[73] Niezbędna ilość sił i środków do wykonania maskowania i pozorowania obiektów wojskowych zamieszczona jest w: „Instrukcji o maskowaniu wojsk", cz. II. „Zasady maskowania operacyjnego", wyd. Szt. Gen. WP, Warszawa 1977, załącznik 1 do 6.

Wnioski te powinny dotyczyć m.in.[74]:

– określenia elementów ugrupowania obronnego związku operacyjnego, które należy ukryć przede wszystkim, oraz miejsca punktu ciężkości obrony informacyjnej;

– sposobów wykorzystania faktycznych działań wojsk związku operacyjnego (przemarsze, rejony rozmieszczenia wojsk, stanowisk dowodzenia, węzłów łączności i in.) do realizacji przedsięwzięć obrony informacyjnej;

– określenia sił i środków jednostek bojowych, jakie powinny być wykorzystane do realizacji przedsięwzięć obrony informacyjnej (w uzgodnieniu ze specjalistami zespołu planowania centrum dowodzenia SD związku operacyjnego);

– określenia możliwości związku operacyjnego w zakresie wykonania zadań pozorowania i dezinformowania w ramach obrony przed rozpoznaniem;

– określenia możliwości związku operacyjnego w zakresie wykonania zadań obrony przed zakłócaniem informacyjnym;

– wyspecyfikowania zadań, które należy postawić związkom taktycznym i oddziałom;

– określenia sił i środków przeznaczonych do kontroli realizacji przedsięwzięć obrony informacyjnej.

W wyniku szczegółowego rozważenia poszczególnych czynników wpływających na wykonanie zadania oraz po zapoznaniu się z przyjętymi wariantami działań obronnych związku operacyjnego grupa obrony informacyjnej (specjalista odpowiedzialny na ocenę wojsk własnych) powinna opracować **koncepcje obrony informacyjnej dla poszczególnych wariantów**. Oznacza to, że w ramach tej czynności powinno powstać, niejako równolegle, kilka przyszłych planów prowadzenia obrony informacyjnej w działaniach obronnych związku operacyjnego.

Badania literatury źródłowej [23;26;92] oraz materiały z ćwiczeń prowadzonych w AON[75] wskazują, że **koncepcja obrony informacyjnej dla określonego wariantu powinna zawierać:**

– **określenie punktu (punktów) ciężkości w zakresie wprowadzenia przeciwnika w błąd,**

– **przedsięwzięcia niezbędne do realizacji zadań obrony informacyjnej w działaniach obronnych związku operacyjnego;**

---

[74] Wnioski z oceny wojsk własnych należy ujmować w apendyksie do aneksu „obrona informacyjna".
[75] W latach 1997 – 2000.

– **podział (wstępny) sił i środków przeznaczonych do realizacji zadań obrony informacyjnej;**

– **sposób ugrupowania i rozwinięcia systemów pozornych oraz powiązanie ich z systemami rzeczywistymi.**

Koncepcje takie należy przygotować dla wszystkich rozpatrywanych wariantów. W miarę posiadanego czasu należy wzbogacić je, np. tabelami podziału zadań na potrzeby obrony informacyjnej oraz schematami (oleatami) zawierającymi dane dające się zilustrować. Należy mieć na uwadze, że szczególnie ważne zadania obrony informacyjnej przed rozpoznaniem (z zakresu pozorowania i dezinformowania) nie powinny być ujawniane bez zgody dowódcy, a zatem i bezpośrednio odzwierciedlane w tych dokumentach.

Rozważenie koncepcji prowadzenia obrony informacyjnej w poszczególnych wariantach działań obronnych związku operacyjnego jest kolejną czynnością w zakresie planowania, której celem jest określenie zalet i wad poszczególnych wariantów wykonania zadania w sferze informacyjnej w konfrontacji z prawdopodobnym sposobem działania przeciwnika. Najczęściej stosowaną techniką powinna być symulacja[76] przyszłych działań zgodnie z przyjętymi wariantami, będąca próbą określenia przyszłych zdarzeń zgodnie **z zasadą: akcja – reakcja – przeciwreakcja.** Uczestnikami symulacji powinni być członkowie zespołu planowania (po stronie wojsk własnych) oraz zespołu działań informacyjnych (po stronie przeciwnika) centrum dowodzenia SD związku operacyjnego. Uczestniczyć w niej powinni również przedstawiciele zespołów z centrum wsparcia dowodzenia, centrum wsparcia działań i innych komórek (w tym specjalista grupy obrony informacyjnej) stosownie do ustaleń szefa sztabu. W miarę rozważania kolejnych wariantów działania (symulacji) przedstawiciel G 2 (grupy obrony informacyjnej) powinien dokonać zestawienia zalet i wad każdego wariantu z punktu widzenia prowadzenia obrony informacyjnej.

W trakcie symulacji powinny być identyfikowane również fakty i przewidywania niezbędne do sporządzenia planu synchronizacji działań (wstępnego zarysu graficzno-tabelarycznego), po jednym dla każdego wariantu działania. **W planach tych powinny być skoordynowane również przedsięwzięcia obrony informacyjnej. W tym celu specjaliści rodzajów wojsk i służb, przygotowując koncepcje użycia swych wojsk, powinni uwzględniać również problemy obrony informacyjnej wchodzących w ich skład komponentów systemów dowodzenia i naprowadzania uzbrojenia.**

---

[76] Etapy postępowania w trakcie przygotowywania i przeprowadzania symulacji oraz podstawowe techniki rozważania wariantów działania (wg etapów, kierunków, obiektów) są wystarczająco przedstawione w literaturze przedmiotu [26;56;104].

Sformułowane w wyniku symulacji wnioski i oceny poszczególnych wariantów działania, a wraz z nimi i koncepcji prowadzenia obrony informacyjnej powinny być wykorzystane do ich porównania, a zatem do ich przyjęcia, zmodyfikowania bądź wręcz odrzucenia jako nie spełniające wymaganych kryteriów.

Porównanie koncepcji prowadzenia obrony informacyjnej w poszczególnych wariantach działań obronnych związku operacyjnego powinno polegać na rzeczowej ocenie przygotowanych i rozważonych koncepcji oraz na wyłonieniu tego wariantu, który będzie rekomendowany dowódcy. Proces porównania dokonywany jest w toku **odprawy koordynacyjnej**, a jej przebieg jest ustalany przez szefa sztabu, który jest jej organizatorem. W jej trakcie poszczególne zespoły funkcjonalne SD w formie krótkich meldunków powinny przedstawić wyniki swojej pracy.

W toku swoich wystąpień szef zespołu działań informacyjnych centrum dowodzenia SD związku operacyjnego, oprócz oceny środowiska pola walki oraz przeciwnika, powinien przedstawić koncepcje prowadzenia rozpoznania, zakłócania i obrony informacyjnej[77] we wszystkich rozpatrywanych wariantach działania[78]. **Istotą jego wystąpienia w odniesieniu do obrony informacyjnej powinno być precyzyjne wyartykułowanie zalet i wad poszczególnych wariantów wpływających na sposób wykonania zadań obrony informacyjnej.** Odprawa koordynacyjna powinna zatem doprowadzić do jeszcze większej koordynacji zarysu planu działań obronnych związku operacyjnego z opracowaną koncepcją prowadzenia w ich toku obrony informacyjnej.

Końcowym przedsięwzięciem odprawy koordynacyjnej jest porównanie wariantów działania, które w zależności od decyzji szefa sztabu może być realizowane metodą rozważenia wad i zalet, metodą głosowania lub metodą kryteriów (określonych przez dowódcę podczas analizy zadania). Należy mieć na uwadze, że porównanie wariantów działania jest jedną z najważniejszych czynności w procesie pracy sztabu. Ma bowiem na celu wyłonienie wariantu rekomendowanego dowódcy. Kończy ono również etap oceny sytuacji.

---

[77] Koncepcje prowadzenia obrony informacyjnej we wszystkich rozpatrywanych wariantach działania przygotowuje grupa obrony informacyjnej zespołu G 2.

[78] W wypadku ograniczonego czasu trwania odprawy koordynacyjnej może zaistnieć sytuacja, kiedy będzie musiał wskazać jedynie wariant najkorzystniejszy z punktu widzenia wykonania zadań obrony informacyjnej.

4.2.2.2. Decyzja i zamiar dowódcy w zakresie obrony informacyjnej

Zgodnie z ramowym układem cyklu decyzyjnego podjęcie przez dowódcę decyzji i ogłoszenie zamiaru do działań obronnych związku operacyjnego odbywa się podczas **odprawy decyzyjnej**[79]. Za jej przebieg i organizację ponosi odpowiedzialność szef sztabu[80]. Na odprawie decyzyjnej prezentowane są wyniki pracy sztabu, a szef sztabu wskazuje rekomendowany wariant działania.

W trakcie swoich wystąpień szef zespołu działań informacyjnych oprócz oceny środowiska pola walki oraz wojsk przeciwnika powinien przedstawić **propozycję** prowadzenia rozpoznania, zakłócania i **obrony informacyjnej**[81] w działaniach obronnych związku operacyjnego, a ponadto powinien być w gotowości do udzielenia odpowiedzi na ewentualne pytania dowódcy w celu wyjaśnienia wszelkich wątpliwości wykonania zadań obrony informacyjnej.

Propozycja ta **stanowi rozwinięcie koncepcji prowadzenia obrony informacyjnej dla wariantu rekomendowanego.** Powinna zatem zawierać:

- przedsięwzięcia niezbędne do realizacji zadań obrony informacyjnej w działaniach obronnych związku operacyjnego;
- podział sił i środków przeznaczonych do realizacji zadań obrony informacyjnej;
- określenie punktu (punktów) ciężkości w zakresie wprowadzenia przeciwnika w błąd;
- sposób ugrupowania i rozwinięcia systemów pozornych oraz powiązanie ich z systemami rzeczywistymi;
- priorytety w zakresie realizacji zadań obrony informacyjnej przed zakłócaniem.

Końcową czynnością odprawy decyzyjnej jest dokonanie przez dowódcę wyboru jednego z przedstawionych przez sztab wariantów działania i ogłoszenie go jako swojej decyzji. Na bazie tej decyzji dowódca ogłasza swój zamiar działania[82]. Wskazuje w nim między innymi priorytety we wsparciu i zabezpieczeniu działań. Uwzględniona powinna być również sfera informacyjna.

---

[79] W odprawie tej uczestniczą kierownicy zespołów organizacyjno – funkcjonalnych stanowiska dowodzenia.

[80] Przykład układu odprawy decyzyjnej przedstawiony jest w: [26;85;92].

[81] Propozycję prowadzenia obrony informacyjnej w działaniach obronnych związku operacyjnego przygotowuje grupa obrony informacyjnej zespołu działań informacyjnych.

[82] Struktura zamiaru ogłaszanego przez dowódcę na koniec odprawy decyzyjnej nie jest sformalizowana. Zamiar działania może zawierać: podział sił; sposób działania; elementy dowodzenia i koordynacji; ugrupowanie; podział odpowiedzialności w obszarze tyłowym; priorytety we wsparciu i zabezpieczeniu działań; łączność. „Regulamin działań wojsk lądowych", wyd. DWLąd, Warszawa 1999, s. 55.

Bezpośrednio po odprawie decyzyjnej szef zespołu działań informacyjnych powinien zapoznać z zamiarem dowódcy podległy zespół oraz wydać końcowe wytyczne do planowania szczegółowego oraz opracowania dokumentów planistycznych i rozkazodawczych, określając czas jego zakończenia. Dopiero w wyniku sprecyzowania powyższych danych grupa obrony informacyjnej ma podstawy do ostatecznego opracowania dokumentów na potrzeby obrony informacyjnej w działaniach obronnych związku operacyjnego.

4.2.2.3. Opracowanie dokumentów w zakresie obrony informacyjnej

Opracowanie dokumentów na potrzeby obrony informacyjnej stanowi końcowy etap fazy planowania działań obronnych związku operacyjnego. Do czasu opracowania niniejszej pracy studyjnej nie zostały wypracowane wzory dokumentów na potrzeby obrony informacyjnej. Z badań wynika, że **dokumenty te powinny w formie i treści być zbliżone do dokumentów opracowywanych w sztabie związku operacyjnego i obowiązujących w wojskach.** Nie informuje się bowiem bezpośrednich wykonawców o pozorowanym, dezinformującym czy też mylącym charakterze ich działań. Powinni oni i muszą być przekonani, że pracują w systemach rzeczywistych. Stąd też przez analogię można określić **dokumenty jakie powinny być opracowywane na potrzeby obrony informacyjnej, tj.:**

1. Planistyczne – „Plan prowadzenia obrony informacyjnej w działaniach obronnych związku operacyjnego" wraz z załącznikami.
2. Rozkazodawcze – Aneks „Obrona informacyjna" wraz z apendyksami.
3. Inne dokumenty (robocze, sprawozdawcze) – w zależności od potrzeb.

Plan prowadzenia obrony informacyjnej w działaniach obronnych związku operacyjnego należy opracować na podstawie ogłoszonego przez dowódcę zamiaru działania oraz wcześniejszych ustaleń zawartych w koncepcji i propozycji obrony informacyjnej. Bezpośrednią odpowiedzialność za jego opracowanie powinien ponosić szef grupy obrony informacyjnej[83] zespołu działań informacyjnych centrum dowodzenia SD związku operacyjnego.

---

[83] W starszych dokumentach sygnowanych przez Sztab Generalny WP („Instrukcja o maskowaniu wojsk", cz. II. „Zasady maskowania operacyjnego", wyd. Szt. Gen. WP, Warszawa 1977, s. 46) widnieje zapis odnośnie planu maskowania operacyjnego, który opracowuje zarząd (oddział) operacyjny frontu (armii) przy współudziale szefostw rodzajów wojsk i służb. Jak wykazano w podrozdziale 2.2. oraz 3.2.2. pracy studyjnej, maskowanie (bezpośrednie i operacyjne) jest komponentem obrony informacyjnej przed rozpoznaniem. Zdaniem autora obrona informacyjna jest zatem problemem nadrzędnym wobec maskowania operacyjnego. Poglądy takie mają również amerykańscy specjaliści w tej dziedzinie [114;124].

Plan obrony informacyjnej[84] w działaniach obronnych związku operacyjnego powinien być opracowywany w formie opisowo – tabelarycznej i uzupełniony załącznikami w formie tabelarycznej, np. wykaz wiadomości dezinformujących (mylących)[85], harmonogram kontroli realizacji zadań obrony informacyjnej oraz graficznej, np. plan pozorowania – wykonany na oleacie wg potrzeb.

W części **tabelarycznej planu** należy umieścić [załącznik 24.]:

- etapy lub okresy działań;
- rodzaje zadań obrony informacyjnej w poszczególnych etapach;
- rodzaje przedsięwzięć wykonywanych podczas realizacji poszczególnych zadań;
- sposoby ich wykonania;
- odpowiedzialność funkcyjną za realizację poszczególnych przedsięwzięć;
- terminy realizacji zadań obrony informacyjnej;
- sposób prowadzenia kontroli w zakresie realizacji zadań obrony informacyjnej;
- uwagi dotyczące współdziałania organów obrony informacyjnej z organami rozpoznania i zakłócania, a także z elementami wsparcia dowodzenia i działań.

Część graficzna planu (plan pozorowania) powinna być dostępna dla ściśle określonego grona osób: dowódcy, szefa sztabu, szefa zespołu działań informacyjnych (kierownika grupy obrony informacyjnej), szefa zespołu planowania centrum dowodzenia SD związku operacyjnego. Przykład planu pozorowania zilustrowano graficznie w załączniku 25.

Problematyka obrony informacyjnej powinna mieć również odzwierciedlenie w planach użycia rodzajów wojsk i służb (w częściach graficznych, opisowych) oraz w odpowiednich apendyksach do aneksów. Należy w nich uwzględnić, np.:

- wnioski z zagrożenia w sferze informacyjnej dla danego rodzaju wojsk lub służb;
- wnioski z oceny wojsk związku operacyjnego na potrzeby obrony informacyjnej;
- zakres realizacji zadań obrony informacyjnej przewidzianych dla danego rodzaju wojsk lub służb;

---

[84] Plan obrony informacyjnej jest jednym z trzech dokumentów planistycznych jakie powinny być wykonywane w G 2 w zakresie walki informacyjnej. Na potrzeby rozpoznania opracowuje się „Plan zbierania informacji", a na potrzeby zakłócania powinien być opracowywany „Plan zakłócania informacyjnego". Poza tym podczas opracowywania planu działań obronnych oficerowie zespołu G 2 SD związku operacyjnego wrysowują rekomendowany wariant działania przeciwnika dający podstawy do wykonania oleatu wsparcia decyzji (w wyniku wypracowanych zagadnień w informacyjnym przygotowaniu pola walki) [23;26].

[85] Na szczeblu centralnym oraz na potrzeby Dowództwa Wojsk Lądowych należy opracowywać plan dezinformowania.

– kalkulację sił i środków koniecznych do realizacji planowanych zadań, w tym etatowych środków maskowania i sprzętu bojowego;

– czynności (przedsięwzięcia) pozorne i zgranie ich z faktycznym działaniem danego rodzaju wojsk, czy służb;

– główne przedsięwzięcia przeciwrozpoznawcze;

– procedury postępowania podczas wystąpienia zakłóceń celowych lub interferencyjnych (wzajemnych);

– inne – wg potrzeb.

Sporządzenie planu obrony informacyjnej umożliwia przygotowanie wstępnego zarządzenia operacyjnego sztabu związku operacyjnego, które może być wysłane do wojsk biorących udział w realizacji przedsięwzięć obrony informacyjnej. Umożliwia ono wcześniejsze postawienie zadań, zwłaszcza, jeżeli czas na przygotowanie działań jest ograniczony. Układ wstępnego zarządzenia operacyjnego jest taki sam jak rozkazu operacyjnego[86]. Punkty, których nie można na tym etapie opracować, należy pozostawić puste.

Aneks „N – obrona informacyjna"[87] do rozkazu operacyjnego opracowywany jest równolegle z rozkazem operacyjnym związku operacyjnego. Bezpośrednią odpowiedzialność za jego sporządzenie powinien ponosić szef grupy obrony informacyjnej. Układ aneksu pod względem formy i treści [załącznik 26.] powinien być zgodny z aneksami[88] opracowywanymi w zespole działań informacyjnych i w innych zespołach specjalistycznych SD związku operacyjnego.

Do aneksu powinny być opracowywane niezbędne apendyksy, np.:

– prognoza zagrożeń w sferze informacyjnej;

– wnioski z oceny wojsk związku operacyjnego na potrzeby obrony informacyjnej;

– tabelaryczny plan koordynacji przedsięwzięć w zakresie obrony informacyjnej;

---

[86] W sporządzeniu rozkazu operacyjnego biorą udział również oficerowie zespołu działań informacyjnych, opracowując punkt 1 (sytuacja), 3c (zadania dla elementów wspierających), 3d (wytyczne koordynujące i współdziałanie w zakresie obrony informacyjnej) oraz zasilają w niezbędne informacje inne punkty rozkazu.

[87] Niektóre źródła (J. Michniak i inni, „Metody i treść pracy zespołów funkcjonalnych na stanowisku dowodzenia wojsk lądowych", wyd. AON, Warszawa 2000, s. 87) wyszczególniają aneks „I – maskowanie", który opracowywany jest przez zespół planowania centrum dowodzenia. Nie przedstawiono jednak jego układu i treści. W materiale tym nie uwzględniono jednak problematyki walki informacyjnej w ogóle, a zatem i obrony informacyjnej. Zdaniem autora obydwa aneksy nie wykluczają się. W wypadku posiadania wystarczających sił i środków materiałowych, a także i czasu, mogą być wykonywane obydwa, a podejmowane przedsięwzięcia odpowiednio skoordynowane.

[88] W zespole działań informacyjnych powinny być opracowywane:

– w grupie rozpoznania – aneks **„B – rozpoznanie"** do rozkazu operacyjnego wraz z apendyksami;

– w grupie zakłócania informacyjnego – aneks **„H – zakłócanie informacyjne"** do rozkazu operacyjnego wraz z apendyksami.

- rejony i częstotliwości zastrzeżone;
- dokumenty normatywne z zakresu bezpieczeństwa informacyjnego;
- inne, według potrzeb.

Z analizy wzorów dokumentów rozkazodawczych, wykonywanych podczas ćwiczeń w AON i dokumentów standaryzacyjnych NATO wynika, że apendyksy mogą mieć formę tekstową, graficzną lub tekstowo – graficzną. W gruncie rzeczy zależy ona od wykonawcy danego dokumentu.

4.2.3. Stawianie zadań w zakresie obrony informacyjnej

Sposób postawienia zadań może być różny i będzie zależał od wielu czynników (m. in.: od posiadanego czasu, stopnia doświadczenia i wyszkolenia dowództw, stanu posiadania i poziomu technicznych środków łączności i wspomagania procesu dowodzenia).

Formalne przekazanie wykonawcom zadań wynikających z decyzji dowódcy rozpoczyna się po zakończeniu opracowania pełnego rozkazu operacyjnego[89] wraz z niezbędnymi aneksami i apendyksami. Zgodnie jednak z przyjętą procedurą dowodzenia podwładni mogą otrzymać zadania bojowe wcześniej w formie zarządzenia przygotowawczego (ZP), wstępnego zarządzenia operacyjnego (WZO).

Postawienie zadań może odbyć się na SD związku operacyjnego (przyjmuje wówczas formę odprawy koordynacyjnej poświęconej temu problemowi) lub na SD podwładnych. W drugim wypadku wykorzystuje się do tego celu zastępcę dowódcy, innych oficerów sztabu (w tym i z zespołu działań informacyjnych) lub (oraz) oficerów łącznikowych.

Z powyższego wynika, że **szef zespołu działań informacyjnych nie ma kompetencji do bezpośredniego stawiania zadań. Uczestnicząc jednak w tym przedsięwzięciu, może wyjaśniać niezbędne dane ujęte w rozkazie operacyjnym, dotyczące przeciwnika, terenu oraz prowadzenia rozpoznania, zakłócania informacyjnego i obrony informacyjnej.** Zwłaszcza, że po postawieniu zadań z reguły odbywa się koordynacja działań pomiędzy podległymi jednostkami. Czynność ta odgrywa bardzo ważną rolę w koordynowaniu zadań obrony informacyjnej wykonywanych przez różne jednostki.

---

[89] „Organizacja dowodzenia jednostkami operacyjnymi wojsk lądowych", cz. 3, wyd. AON, Warszawa 1998.

4.2.4. Kontrola wykonania zadań w zakresie obrony informacyjnej

Kontrola stanowi ostatnią fazę cyklu decyzyjnego procesu dowodzenia[90]. Jednocześnie zapewnia ona ciągłość tego procesu, gdyż jej rezultaty stanowią postawę do uaktualniania posiadanych danych o sytuacji, a głównie ustalania położenia i realizacji kolejnych faz cyklu.

Z badań wynika, że za realizację procesu kontroli odpowiedzialny jest dowódca każdego szczebla dowodzenia. Kontrola powinna być realizowana przez: ustanowienie elementów kontroli; organizację synchronizacji działań, monitorowanie sytuacji, podejmowanie działań mających na celu zmniejszenie różnicy pomiędzy stanem zaplanowanym a rzeczywistym.

Kontrola wykonania zadań w zakresie obrony informacyjnej jest więc **istotną częścią działań podejmowanych w tej fazie cyklu, a jej cechą szczególną jest to, że należy postrzegać ją w dwóch aspektach: przeciwnik – wojska własne.**

W pierwszym wypadku konieczne jest określenie, w jaki sposób realizowane przedsięwzięcia mogą oddziaływać na funkcjonowanie organów walki informacyjnej przeciwnika, a tym samym uzyskanie odpowiedzi na pytania:

- w jaki sposób przeciwnik ocenia nasze działania w zakresie obrony informacyjnej, a głównie w zakresie obrony przed rozpoznaniem?
- do jakich wniosków mogą lub powinny go skłonić dane przedsięwzięcia obrony informacyjnej?

W drugim wypadku należy wykryć i usunąć niedociągnięcia powstałe w czasie realizacji zadań obrony informacyjnej przez wojska własne.

Z powyższego wynika, że bardzo ważną rolę podczas kontroli realizacji zadań obrony informacyjnej odgrywa **monitorowanie sytuacji**. W tym celu powinny być wykorzystywane dane:

- z meldunków od wojsk;
- z wizyt dowódcy (oficerów sztabu, a w tym i z zespołu działań informacyjnych) u podległych mu wojsk;
- od wysyłanych grup kontrolnych;
- z elementów kontroli organizowanej po linii funkcjonalnej przez specjalistów rodza-

---

[90] Por.: rysunek 4.5.

jów wojsk[91] (działalność grup rozpoznawczych, kontrola radiowa, radiolokacyjna, optoelektroniczna, informatyczna i in.).

Do głównych zadań zespołu działań informacyjnych w tej fazie w zakresie obrony informacyjnej powinno należeć:

- bieżące informowanie dowódcy o sytuacji przeciwnika i działalności rozpoznawczej;
- kontrola efektów zaplanowanych działań w zakresie obrony informacyjnej i ewentualne ich korygowanie oraz stawianie zadań dodatkowych, wynikających z rozwoju sytuacji (według opracowanego harmonogramu, stanowiącego załącznik do planu obrony informacyjnej);
- bieżące prowadzenie dokumentacji na potrzeby obrony informacyjnej (mapy sytuacyjnej, dokumentów pomocniczych, uaktualniania baz danych itp.).

Cechą typową procesu kontrolowania powinno być wykraczanie poza ramy konkretnych działań związku operacyjnego, tzn. że kontrola powinna być prowadzona w okresach przygotowawczych, w toku prowadzenia działań obronnych, jak i po ich zakończeniu. Wynika to z faktu, że przedsięwzięcia realizowane w fazie kontroli na potrzeby działań bieżących, muszą być również ukierunkowane na prowadzenie przez związek operacyjny przewidywanych przyszłych działań. Pozwoli to na przystąpienie do kolejnego cyklu decyzyjnego z określonym potencjałem danych na potrzeby kolejnego ustalenia położenia.

4.3. Wnioski

W wyniku przeprowadzonych badań pożądanego przebiegu procesu decyzyjnego pod kątem potrzeb obrony informacyjnej w działaniach obronnych związku operacyjnego wykazano, że:

1. Odpowiedzialność za całokształt problematyki związanej z obroną informacyjną ponosi dowódca związku operacyjnego, zaś organizatorem zadań w zakresie jej przygotowania i prowadzenia jest oddział G 2, przy znaczącym współudziale oddziału G 3 i specjalistów rodzajów wojsk i służb.

---

[91] Bardzo ważnym elementem kontroli obrony informacyjnej może być lotnictwo wojsk lądowych wyposażone w urządzenia rozpoznania fotograficznego, radiowego, radiolokacyjnego i optoelektronicznego. Może prowadzić zatem w określonej sytuacji pola walki monitoring zarówno wojsk własnych, jak i przeciwnika.

2. Celowe jest utworzenie w centrum dowodzenia SD związku operacyjnego zespołu działań informacyjnych, w którego składzie należy przewidzieć grupę obrony informacyjnej.

3. Przebieg cyklu decyzyjnego w zakresie obrony informacyjnej jest integralnym elementem procesu dowodzenia, realizowanym przez dowództwo i sztab związku operacyjnego, zgodnie z obowiązującymi procedurami i technikami.

4. Metodyka pracy sztabu związku operacyjnego w zakresie obrony informacyjnej oparta jest na ramowym układzie cyklu obowiązującego w sztabie związku operacyjnego.

5. Forma i treść dokumentów wykonywanych na potrzeby obrony informacyjnej jest zgodna z wzorami obowiązującymi w sztabie związku operacyjnego. Mogą być one wykonywane sposobem tradycyjnym bądź z wykorzystaniem pakietu grafiki operacyjnej.

ZAKOŃCZENIE

Przeprowadzone w ramach dysertacji badania ugruntowały przekonanie autora o potrzebie i aktualności ich podjęcia. Dorobek teorii obrony informacyjnej – jedynie o ogólnym stopniu opracowania – wymagał uporządkowania, rozwinięcia i syntetycznego przedstawienia problemów wynikających z potrzeb uwzględnienia sfery informacyjnej w przyszłych działaniach obronnych związku operacyjnego.

W toku badań uzyskano odpowiedzi na sformułowane, w postaci pytań, problemy badawcze, które w stopniu wyczerpującym wyjaśniły interesujące zdarzenia, potwierdziły trafność przyjętych hipotez roboczych i umożliwiły uzyskanie zamierzonych celów badawczych.

Celem dysertacji nie było stworzenie gotowych reguł (recept), lecz poszukiwanie i analiza mechanizmów sterujących obroną informacyjną w działaniach obronnych związku operacyjnego. Identyfikacja i opisanie tych zjawisk stanowi zasadniczy wkład w rozwój teorii walki zbrojnej w sferze informacyjnej. U podstaw zaproponowanych rozwiązań legło przekonanie, iż jedynie twórcze ich wykorzystanie pozwoli na osiągnięcie sukcesu w działaniach obronnych związku operacyjnego. Stanowią one jednocześnie zbiór pożądanych zasad, których nieuwzględnienie będzie nieuchronnie prowadzić do klęski na przyszłym, cyfrowym polu walki.

W procedurze poznawczej wykorzystywane były metody badań (teoretyczne i empiryczne) dostosowane do poznawania zjawisk złożonych. Podejście systemowe i funkcjonalne oraz zastosowane narzędzia badawcze pozwoliły na uzyskanie nowych efektów poznawczych, dotyczących:

1. Istoty, przedmiotu, celu, zadań i struktury obrony informacyjnej w działaniach obronnych związku operacyjnego.

2. Pożądanego zakresu i treści przedsięwzięć obrony informacyjnej związku operacyjnego przed rozpoznaniem.

3. Pożądanego zakresu i treści przedsięwzięć obrony informacyjnej związku operacyjnego przed zakłócaniem.

4. Pożądanego przebiegu procesu decyzyjnego pod kątem potrzeb obrony informacyjnej w działaniach obronnych związku operacyjnego.

Przeprowadzone badania potwierdziły ważność i aktualność zagadnień obrony informacyjnej w epoce budowy społeczeństwa informacyjnego. Obecnie, kiedy zarówno w życiu cywilnym, jak i wojskowym na szeroką skalę wykorzystywane są systemy informacyjne, problematyka ta nabrała szczególnego znaczenia i wyrazistości. Potencjalny przeciwnik może spowodować poważne straty bez użycia tradycyjnych sposobów walki oraz narażania własnych sił i środków. Oddziałując na systemy informacyjne, przeciwnik może obezwładnić zakłóceniami czy wręcz zniszczyć środkami ogniowymi nowej generacji istotne elementy systemów dowodzenia i naprowadzania uzbrojenia. Atakujący przeciwnik ma również możliwość ukrycia swojej tożsamości, a zaatakowane wojska mogą nie być w stanie jednoznacznie wskazać agresora. Wynika z tego, że walka w sferze informacyjnej staje się realnym zagrożeniem dla realizacji zadań stojących przed naszymi siłami zbrojnymi. Powodzenie konfrontacji zbrojnej w tej sferze nie jest możliwe zatem bez kompleksowego rozwiązania problemów obrony informacyjnej na wszystkich szczeblach dowodzenia. Problematyka ta jest dostrzegana w wielu państwach.

Zdaniem autora, niniejsza praca studyjna stanowi znaczący wkład w rozwiązanie tych problemów w działaniach obronnych związku operacyjnego wojsk lądowych. Zawiera wyniki badań, które w większości wypadków można odnieść do całych wojsk lądowych jak również do innych rodzajów sił zbrojnych. Przedstawione oceny i wnioski zawarte w poszczególnych rozdziałach są odpowiedzią na postawione problemy badawcze. Wynikają one z analizy literatury przedmiotu badań, z analizy konfliktów lokalnych ostatnich lat (wojna w rejonie Zatoki Perskiej, wojna na Bałkanach, wojna w Czeczenii) oraz z analizy rozwiązań aplikacyjnych przyjmowanych w czasie ćwiczeń w AON. Na ich treść istotny wpływ wywarły również opinie uzyskane w czasie narad, konferencji naukowych, sympozjów i szkoleń oraz oceny ekspertów.

Treści przedstawione w pracy studyjnej nie stanowią jednak pełnego i wyczerpującego rozwiązania problemów obrony informacyjnej na przyszłym, cyfrowym polu walki. Przedstawione poglądy i rozwiązania stanowią bazę do budowania pełniejszych koncepcji działań w sferze informacyjnej. Konieczność ta wynika zarówno z charakteru głównego problemu badawczego, który jest problemem otwartym, jak też z istnienia w jego otoczeniu wielu nie opracowanych naukowo problemów. Zdaniem autora w pierwszej kolejności dalszymi badaniami należy objąć problem planowania szczegółowego oraz organizowania obrony informacyjnej w operacjach połączonych oraz w poszczególnych rodzajach działań wojsk lądowych.

BIBLIOGRAFIA

1. Ackerman R. K., Sztuka wprowadzania w błąd, w: Signal nr 4, 1988.
2. AJP - 1 (A) Allied Joint Operations Doctrine, August 1994.
3. Antczak St., Systemy kierowania i uzbrojenia w polskich siłach powietrznych, wyd. AON, Warszawa 1997.
4. Amanowicz M., Modelowanie profesjonalnych systemów radiokomunikacji ruchomej lądowej, wyd. WAT, Warszawa 1989.
5. Armante J., The Automated Battle, a Feasible Dream, w: Military Review nr 5, 1992.
6. Asmus R. D., NATO. Koncepcja bezpieczeństwa XXI wieku, Warszawa 1997.
7. Balcerowicz B., Sojusz, a obrona narodowa, wyd. Bellona, Warszawa 1999.
8. Barczak A., Janczak J., Mamcarz K., Komputerowy model oceny zagrożenia radioelektronicznego perspektywicznego systemu łączności związku operacyjnego wojsk lądowych. Praca naukowo-badawcza, wyd. WSOWŁ, Zegrze 1996.
9. Barczak A., Janczak J., Mamcarz K., Komputerowy model oceny zagrożenia radioelektronicznego mobilnego systemu łączności, w: materiałach III Krajowej Konferencji KOWBAN'96. Komputerowe wspomaganie badań naukowych (cz. 1), wyd. Wrocławskie Towarzystwo Naukowe, Polanica Zdrój 1996.
10. Barczak A., Janczak J., Mamcarz K., Model symulacyjny zagrożenia radioelektronicznego systemu łączności związku operacyjnego wojsk lądowych. Praca naukowo-badawcza, wyd. WSOWŁ, Zegrze 1997.
11. Barczak A., Janczak J., Mamcarz K., Model ocenowy odporności sieci łączności radioliniowo-przewodowej związku taktycznego na oddziaływanie ogniowe i radioelektroniczne. Praca naukowo-badawcza, wyd. WIŁ Zegrze 1997.
12. Bartosiewicz St., Mańkowski R., Logistyka wojsk lądowych, wyd. AON, Warszawa 2000.
13. Berg A. I., Informacja i cybernetyka, wyd. WNT, Warszawa 1970.
14. Bezoń B., Janczak J., Analiza współczesnych systemów łączności w kontekście integracji SZ RP z NATO, wyd. AON, Warszawa 1999.
15. Bojarski R., Operacja obronna, wyd. AON, Warszawa 1999.
16. Bordon W., Bodziński R., Fellner A., Ligęza S., System GPS NAVSTAR, wyd. DWLiOP, Poznań 1997.
17. Bujak A., Działania bojowe w specyficznych środowiskach pola walki. Rozprawa habilitacyjna, wyd. AON, Warszawa 2000.
18. Campen A. D., The first Information War, ed. AFCA International Press Fairfax, Virginia 1992.
19. Castells M., End of Millennium, ed. Blackwell, Oxford 1998.
20. Chajtman S., Systemy i procesy informacyjne, wyd. PWE, Warszawa 1986.
21. Ciborowski L., Informacyjna preparacja pola walki, referat w materiałach III KNTWRE, wyd. WAT, Żegiestów 1997.
22. Ciborowski L., Rola i miejsce rozpoznania w systemie obronnym RP, wyd. AON, Warszawa 1993.

23. Ciborowski L., Polko M., Planowanie i organizowanie walki zbrojnej wg poglądów NATO, wyd. AON, Warszawa 1996.
24. Ciborowski L., Przestrzenie walki informacyjnej, wyd. AON, Warszawa 1997.
25. Ciborowski L., Walka informacyjna, wyd. ECE, Toruń 1999.
26. Ciborowski L., Nowak A., Planowanie, organizowanie i prowadzenie walki informacyjnej na szczeblach taktycznych wojsk lądowych, wyd. AON, Warszawa 2000.
27. Cieślar P., Wsparcie inżynieryjne działań operacyjnych wojsk lądowych, wyd. AON, Warszawa 1998.
28. Courter J., Thompson L., Army Vision and the Transformation of Land Power in the Next Country, w: Strategic Review nr 3, 1997.
29. Czekała Zb., Parada radarów, wyd. Bellona, Warszawa 1999.
30. Czerwiński J., Problemy bezpieczeństwa systemów dowodzenia a walka informacyjna, w: Myśl Wojskowa nr 3, 2000.
31. Dando M., Biotechnology, Weapons and Humanity, ed. Hardwood Academic Publishers, 1992.
32. Daniels D. J., Surface Penetrating Radar. The Institution of Electrical Engineers, London 1996.
33. Dęga Cz., Uzbrojenie i pole walki wojsk lądowych do 2020 roku, wyd. Bellona, Warszawa 1995.
34. Doctrine for Joint Operations". Joint Pub 3-0. Brussels, February 1995.
35. Dunkier B., Nachrichtengewinnung und Aufklarung im Heer, w: Europ. Sichercheit nr 2, 1998.
36. Dyrda M. Psychologia dowodzenia, wyd. AON, Warszawa 1996.
37. Egmont R.; Sperber K., Sperber J., Die Datenmafia, wyd. Rewohlt Vering GmbH, Heinbek bei, Hamburg 1995. Tłumaczenie z języka niemieckiego: Ratajski R., Infomafia, wyd. URAEUS, Gdynia 1997.
38. Elie B., La direction du renseignement militarie, w: Def. Nat. nr 1, 1993.
39. Faucon F., Guerre de l'information ou operations d'information, w: Def. Nat. nr 3, 1998.
40. Fitzgerald M. C., Russian views on information warfare, w: Army nr 5, 1994.
41. Findeisen W., Analiza systemowa – podstawy i metodologia, wyd. PWN, Warszawa 1985.
42. Flanek Cz., Ficoń K., Symulacyjny model potencjału obronnego państw sąsiadujących z Polską, wyd. AON, Warszawa 1998.
43. Gajewski P., Karasek R., Procedury alokacji kanałów w systemach radiokomunikacji ruchomej, w: materiałach IV Konferencji Naukowej KNSŁ – 95 (cz. 1), wyd. WSOWŁ Zegrze 1995.
44. Gier P., Information Warfare, w: Air Force Magazine nr 3, 1995.
45. Globan-Klas T., Sienkiewicz P., Społeczeństwo informacyjne: Szanse, zagrożenia, wyzwania, wyd. Fundacji Postępu Telekomunikacji, Kraków 1999.
46. Gołąb Z., Wojna a system obronny państwa, wyd. MON, Warszawa 1984.
47. Grabau R., Sechs Dimensionen des Krieges, w: Soldat und Technik nr 6, 1986.
48. 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.
49. Grant S., Tomorrow's Battlefield, Jane's Defence, 1997.
50. Gryciuk P., Doskonalenie metod oceny zagrożenia radioelektronicznego i uodpornienia systemu łączności dywizji (DZ, DPanc) z wykorzystaniem symulacji komputerowej. Rozprawa doktorska, wyd. ASG WP, Warszawa 1987.
51. Herman H., Operacja w sztuce wojennej, wyd. AON, Warszawa 1992.
52. Huzarski M., Zagadnienia taktyki wojsk lądowych, wyd. ECE, Toruń 1999.

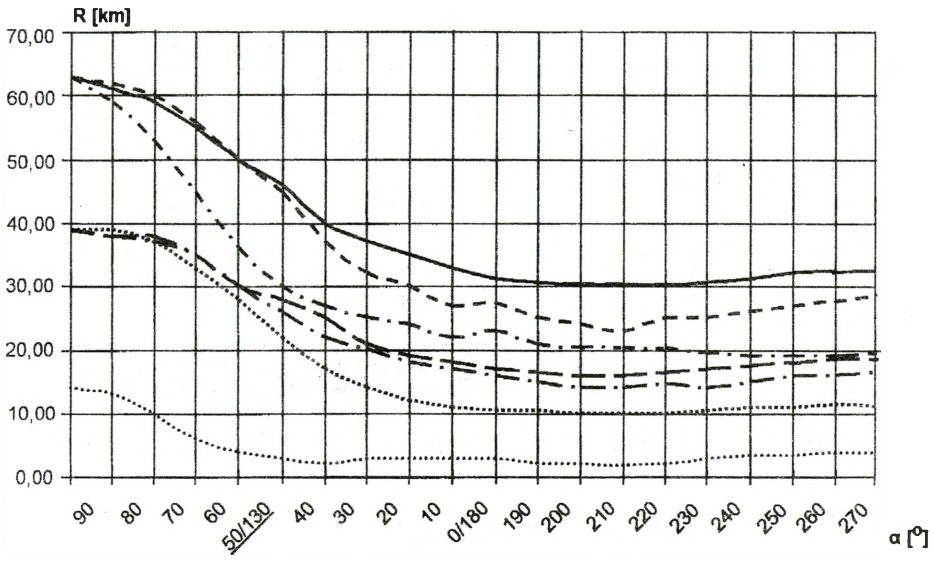
53. Idzikiewicz A. Z., Ochrona informacji w procesie przetwarzania, wyd. PWE, Warszawa 1979.
54. Instrukcja o maskowaniu wojsk, cz. II – zasady maskowania operacyjnego, wyd. Szt. Gen. WP, Warszawa 1976
55. Janczak J., Obrona radioelektroniczna, wyd. WSOWŁ, Zegrze 1993.
56. Janczak J., Obrona radioelektroniczna mobilnych systemów łączności, wyd. AON, Warszawa 1998.
57. Janczak J., Walka informacyjna na współczesnym polu walki, w: materiałach VII Międzynarodowej Konferencji i Wystawy WKTiI'98 (cz. 1), wyd. WIŁ, Zegrze 1998.
58. Janczak J., Kompatybilność elektromagnetyczna mobilnych systemów łączności, w: materiałach VII Międzynarodowa Konferencja i Wystawa WKTiI'98 (cz. 1), wyd. WIŁ, Zegrze 1998.
59. Janczak J., Analiza informacji o siłach i środkach przeciwnika w kontekście budowy komputerowej bazy danych, wyd. AON, Warszawa 1998.
60. Janczak J., Walka radioelektroniczna w działaniach wojsk lądowych. Praca naukowo-badawcza, wyd. AON, Warszawa 1998.
61. Janczak J., Nowacki G., Scheffs W., Możliwości wykorzystania systemu globalnej nawigacji satelitarnej GPS NAWSTAR w wojskach lądowych RP. Praca naukowo-badawcza, wyd. AON, Warszawa 1999.
62. Janczak J., Bezoń B., Scheffs W., Walka elektroniczna w działaniach taktycznych wojsk lądowych. Praca naukowo-badawcza, wyd. AON, Warszawa 1999.
63. Janczak J., Zmiany w teorii walki radioelektronicznej w świetle zapewnienia interoperacyjności SZ RP z NATO, w materiałach Konferencji Naukowo-Technicznej KNTWRE'1999, wyd. WAT, Rynia 1999.
64. Janczak J. i inni, Walka elektroniczna w działaniach taktycznych związku taktycznego. Materiał studyjny, wyd. AON, Warszawa 2000.
65. Janczak J., Modelowanie symulacyjne zagrożenia elektronicznego mobilnego systemu łączności związku operacyjnego wojsk lądowych, wyd. AON, Warszawa 2000.
66. Janczak J., Obrona informacyjna w działaniach obronnych korpusu. Rozprawa habilitacyjna, wyd. AON, Warszawa 2001.
67. Janczak J., Kierunki rozwoju rozpoznania oraz zakłócania elektronicznego, wyd. AON, Warszawa 2001.
68. Janczak J., Bezoń B., Zakłócanie informacyjne w operacjach wojsk lądowych. Praca badawcza, wyd. AON, Warszawa 2001.
69. Jarecki Cz., Sołoducha M., Zadania, sposoby użycia i działania WRiA w operacji obronnej wojsk lądowych, wyd. AON, Warszawa 1998.
70. Kaczmarek W., Nowe środki walki i ich wpływ na zmiany w taktyce, wyd. AON, Warszawa 1997.
71. Killen H. B., Transmisja cyfrowa w systemach światłowodowych i satelitarnych, wyd. KiŁ, Warszawa 1992.
72. Kokot K., Podstawy radiolokacji, cz. 2. Zasięg urządzeń radiolokacyjnych oraz przeciwdziałanie ich pracy, wyd. WAT, Warszawa 1968.
73. Kołosowski Wł. i inni., Rozpoznanie satelitarne i przeciwdziałanie rozpoznaniu na terenie Polski, referat w materiałach IV KNTWRE, wyd. WAT, Rynia 1999.
74. Komow S. A., Informacionnaja bor'ba v sovremennnoj vojne: voprosy teorii, w: Vojen. Mysl' nr 3, 1996.
75. Komow S. A., O sposobach i formach viedienija informacionnoj bor'by, w: Vojen. Mysl' nr 4, 1997.
76. Konieczny J., Inżynieria systemów działania, wyd. WNT, Warszawa 1983.
77. Kostin H. A., Obścije osnovy teorii informacionnoj bor'by, w: Vojen. Mysl' nr 3, 1997.

78. Kowalewski M., Janczak J., Kowalczyk B., Systemy łączności i informatyki sił zbrojnych RP w perspektywie integracji z NATO. Praca naukowo-badawcza, wyd. WSOWŁ, Zegrze 1996.
79. Kozaczuk W., Wojna w eterze, wyd. Radio i TV, Warszawa 1977.
80. Koziej S., Teoria sztuki wojennej, wyd. AON, Warszawa 1993.
81. Krajewski W., Prawa nauki, wyd. KiW, Warszawa 1982.
82. Krauze M., Szulc B., Sztuka wojenna. Konteksty teoretyczne i praktyczne, wyd. ECE, Toruń 2000.
83. Krzemień T., Biernacik R., Operacyjno-taktyczna ocena skuteczności wsparcia ogniowego wojsk w działaniach bojowych, wyd. AON, Warszawa 1995.
84. Kurnal J., Teoria organizacji i zarządzania, wyd. PWN, Warszawa 1979.
85. Land Forces Tactical Doctrine . ATP 35 (B), MAS 1995.
86. Lidwa W., Współdziałanie w walce lądowej, wyd. ECE, Toruń 2000.
87. Łokociejewski M., Taktyczny system rozpoznania i walki elektronicznej wojsk lądowych, wyd. AON, Warszawa 2000.
88. Maliszewski W., Oddziaływanie psychologiczne w operacji obronnej. Rozprawa doktorska, wyd. AON, Warszawa 1998.
89. Markiewicz L., Ultradźwięki i infradźwięki, wyd. PWN, Warszawa 1979.
90. Mazur M., Jakościowa teoria informacji, Warszawa 1970.
91. Michniak J., Podstawy teorii kierowania polowymi systemami łączności wojsk lądowych. Rozprawa habilitacyjna, wyd. AON, Warszawa 1997.
92. Michniak J. i inni, Metody i treść pracy zespołów funkcjonalnych na stanowisku dowodzenia wojsk lądowych, wyd. AON, Warszawa 2000.
93. Miszalski Wł., NATO, poradnik logistyki. Red. meryt. i tłum. z jęz. ang., wyd. Inst. Techn. WL, 1997.
94. Mitiugow W., Fizyczne podstawy teorii informacji, wyd. PWN, Warszawa 1980.
95. Neri F., Introduction to Electronic Defence Systems, ed. Artech House, Inc., 1991.
96. Nowak E., Komunikacje i wojna, wyd. Bellona, Warszawa 1994.
97. Nowacki G., Walka informacyjna – próba kategoryzacji. Rozprawa doktorska, wyd. AON, Warszawa 1999.
98. Panecki T., Wojsko Polskie w działaniach koalicyjnych, wyd. AON, Warszawa 2000.
99. Perelman M., Class Warfare in the Information Age, ed. St. Matin's Press, New York 1998.
100. Petersen K., Pracht U., Information Warfare, w: Sold. Techn. Nr 12, 1995.
101. Piekarski H., Istota i charakter walki radioelektronicznej w SZ RP, wyd. AON, Warszawa 1993.
102. Piekarski H., Walka radioelektroniczna, wyd. MON, Warszawa 1980.
103. Pierce J. R., Symbole, sygnały i szumy, wyd. PWN, Warszawa 1967.
104. Popper K. R., Logika odkrycia naukowego, wyd. PWN, Warszawa 1977.
105. Priumov V. S., Rodinov M. A., Niekotoryje aspiekty informacionnoj bor'by, w: Vojen. Mysl' nr 5, 1997.
106. Pytkowski W., Organizacja badań i ocena prac naukowych, wyd. PWN, Warszawa 1985.
107. Ravier E., Informatique et novel echelon strategique, w Def. Nat. nr 11, 1997.
108. Robinson C., A., Electronic Combat Techniques Provide Information, w: Signal nr 5, 1997.
109. Ross J. D., Information War, w: Army nr 2, 1994.
110. Rotkiewicz W., Kompatybilność elektromagnetyczna w radiotechnice, wyd. KiŁ, Warszawa 1978.
111. Różański G., Zintegrowane systemy informacyjne w środowisku systemów otwartych, referat w materiałach (cz. 1) IV Konferencji Naukowej KNSŁ – 95, wyd. Zegrze 1995.

112.Rutkowski C., Podstawowe pojęcia z dziedziny bezpieczeństwa i obronności państwa, w: Myśl Wojskowa nr 2, 1996.
113.Scales R., Future warfare, Carlisle Barracks, 1999.
114.Schwartau Winn., Information Warfare – Cyberterrorism: Protecting Your Personal Security in the Electronic Age, 1993.
115.Seidlar. J., Nauka o informacji. T I, II, wyd. WNT, Warszawa 1983.
116.Shannon C. E, Warren W., The Mathematical Theory of Communication. The University of Illinois Press, Urbana 1949.
117.Sienkiewicz P., Analiza systemowa: metodologia modelowania systemowego; przykłady modeli systemowych; podstawy metodologiczne teorii, analizy i inżynierii systemów, wyd. AON, Warszawa 1994.
118.Sikorski K., Doskonalenie obrony radioelektronicznej DZ w początkowym okresie wojny. Rozprawa doktorska, wyd. ASG WP, Warszawa 1989.
119.Sokołowski A., Ochrona informacji komputerowych, wyd. MON, Warszawa 1987.
120.Stankiewicz W., Ekonomika wojenna, wyd. MON. Warszawa 1981.
121.Starry M. D., Arneson C. W., Działania informacyjne, w: Military Review nr 6, 1996.
122.Stalings W., Ochrona danych w sieci i w intersieci, wyd. WNT, Warszawa 1997.
123.Stępień R., System bezpieczeństwa Polski, wyd. AON, Warszawa 1995.
124.Stokarski A., Amerykańska doktryna operacji informacyjnych, w: Myśl Wojskowa nr 2, 2000.
125.Sun Tzu, Sztuka wojny, wyd. Przedświt, Warszawa 1994.
126.Szulc B., Walka zbrojna w kontekście ogólnej teorii walki i teorii konfliktów, wyd. AON, Warszawa 1996.
127.Szulc B., Nauka i sztuka wojenna na przełomie wieków. Wykład, wyd. AON, Warszawa 1999.
128.Szydłowski A., O psychologicznym podłożu maskowania, w: Myśl Wojskowa nr 4/96.
129.Ścibiorek Z., Karczmarek W., Przyszła wojna – jaka?, wyd. Bellona, Warszawa 1995.
130.Ścibiorek Z., Działania opóźniające, wyd. Bellona, Warszawa 1996.
131.Ścibiorek Z., Wojna czy pokój, wyd. Ossolineum, Wrocław 1999.
132.Śladkowski St. i inni, Obrona przeciwchemiczna wojsk lądowych, wyd. AON, Warszawa 1999.
133.Świątnicki W. Z., Bronie inteligentne, wyd. ISBN, Warszawa 1992.
134.Tarasiuk B., Zautomatyzowane systemy dowodzenia wojsk lądowych, wyd. AON, Warszawa 1992.
135.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.
136.Tomaszewski A., Krzemień T. i inni, Rażenie ogniowe i elektroniczne, wyd. AON, Warszawa 1996.
137.Tomaszewski A. i inni, Struktura organizacyjno-funkcjonalna systemu dowodzenia wojsk lądowych, tom 2, wyd. AON, Warszawa 1997.
138.Wołkow Wł., Dezinformacja oręż wojny, wyd. Delikon, Warszawa 1991.
139.Volkoff Vl., Petite histoire de la desinformation, du cheval de Troie a Internet. Monaco: Editions du Rocher, cop. 1999.
140.Waltz E., Information warfare principles and operations, ed. Artech House, Boston, London 1998.
141.Wehner D. R., High Resolution Radar, ed. Artech House, Norwood, MA, 1995.
142.Wiatr M., Między strategią a taktyką, wyd. ECE, Toruń 1999.
143.Wilson J. R., Waging the Infowar, w: Int. Def. Rev. Dod. Nr 4, 1977.

144. Wróblewski R., Ciborowski L., Zagrożenia kryzysowe i wojenne Polski w kontekście jej członkostwa, wyd. AON, Warszawa 1999.
145. Wymagania CCITT. Zielona księga, tom III, wyd. KiŁ, Warszawa 1976.
146. Zacher L (red.), Polska a globalne społeczeństwo informacyjne. Ekspertyza zbiorowa (K. Doktrowicz, T. Globan-Klas, K. Krzysztofek, F. Mączyński) dla Komitetu Badań Naukowych, Warszawa 1997.
147. Zabłocki E., Koncepcja wojskowych systemów eksperckich, wyd. AON, Warszawa 1995.
148. Zieleniewski J., Podstawowe pojęcia teorii systemów, organizacja, sterowanie i zarządzanie. Współczesne problemy zarządzania, wyd. PWN, Warszawa 1985.
149. Zieliński J. i inni, Podstawowe założenia operacji połączonych, wyd. AON, Warszawa 2000.

GŁĘBOKOŚĆ STREFY DOSTĘPNOŚCI ELEKTROMAGNETYCZNEJ (R) W FUNKCJI WARTOŚCI KĄTA (α) POMIĘDZY OSIĄ KIERUNKOWĄ ANTENY A LINIĄ ŁĄCZĄCĄ ANTENĘ Z NAJBLIŻSZYM PUNKTEM LINII STYCZNOŚCI WOJSK



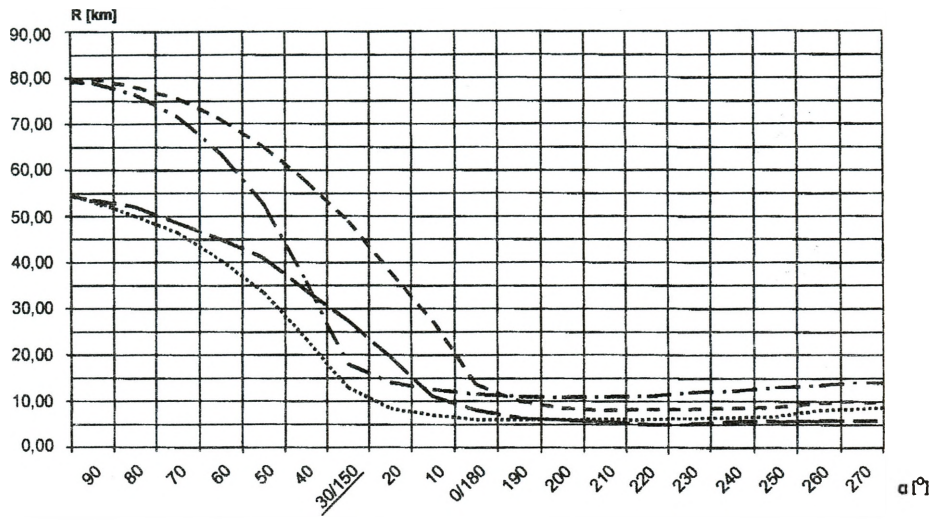
Legenda: — — — A ——— B — · — · C — · — A' — — — B' ····· C' ····· D

A – antena logarytmiczno-periodyczna; P_N=22,5 W;
B,C – anteny z płaskim reflektorem do pracy w podzakresach B i C;
A',B',C' – jak wyżej – podczas pracy z obniżoną mocą P_N=3 W;
D – antena promieniowa z falą bieżącą 40m/1m, moc nadajnika P_N=1 W, częstotliwość robocza f_{rob}=40 MHz.

Warunki:

- pomiędzy anteną nadawczą i anteną odbiorczą teren odkryty, spełniający warunek bezpośredniej widoczności anten;
- gleba średnio wilgotna (ε=10,σ =10^{-2}).

GŁĘBOKOŚĆ STREFY DOSTĘPNOŚCI ELEKTROMAGNETYCZNEJ (R) W FUNKCJI WARTOŚCI KĄTA (α) POMIĘDZY OSIĄ KIERUNKOWĄ ANTENY A LINIĄ ŁĄCZĄCĄ ANTENĘ Z NAJBLIŻSZYM PUNKTEM LINII STYCZNOŚCI WOJSK



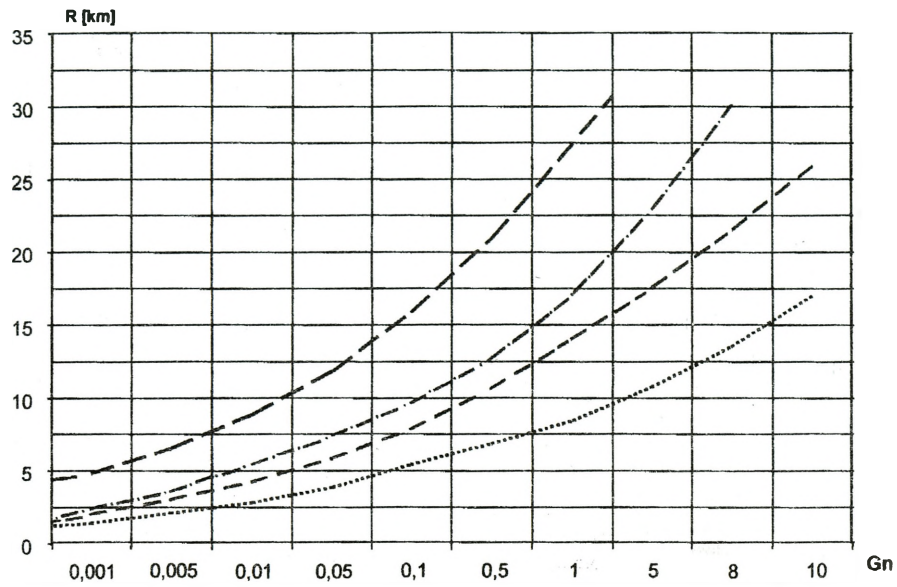
Legenda: — — A - - - B ····· C — · — D

A – antena typu kanał falowy (Yagi), P_N=2,5 W;
B – jak wyżej – praca ze wzmacniaczem mocy, P_N=25 W;
C – antena kątowa, P_N=1,5 W;
D – jak wyżej – praca ze wzmacniaczem mocy, P_N=10 W.

Warunki:

- pomiędzy anteną nadawczą i anteną odbiorczą teren odkryty, spełniający warunek bezpośredniej widoczności anten;
- gleba średnio wilgotna (ε=10,σ =10^{-2}).

GŁĘBOKOŚĆ STREFY DOSTĘPNOŚCI ELEKTROMAGNETYCZNEJ (R) W FUNKCJI ZYSKU ENERGETYCZNEGO ANTENY NADAWCZEJ (G_N)



Legenda: — — A – · – · B – – – C ····· D

A – polaryzacja pionowa, antena nie zawieszona na maszcie;
B – praca kluczem telegraficznym;
C – praca fonem;
D – polaryzacja pozioma, antena zawieszona na wysokości 1 m.

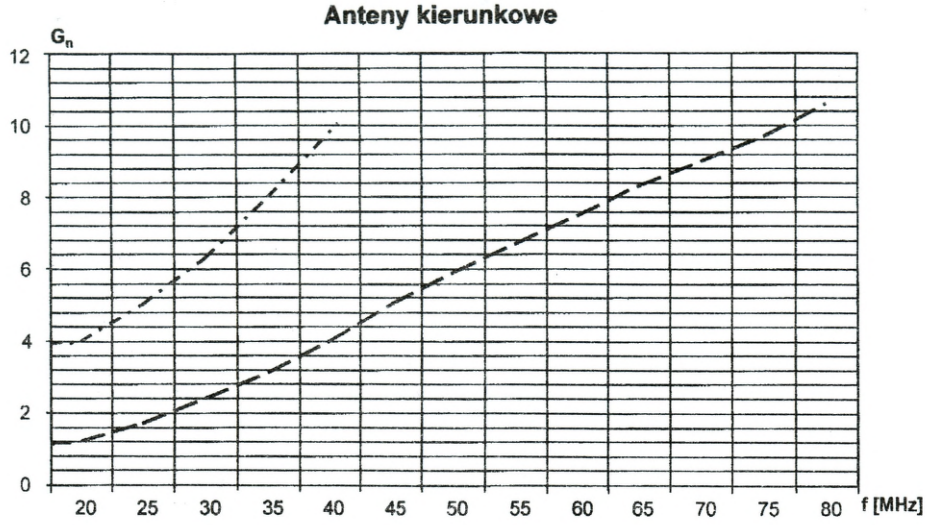
Linie przerywane pozwalają określić orientacyjny zasięg nadajnika podczas jego pracy z antenami prętowymi.

Warunki:

- moc nadajnika P_N=1 W;
- antena rozwinięta w terenie odkrytym o ubogiej morfologii;
- gleba średnio wilgotna (ε=10, $\sigma = 10^{-2}$);
- antena odbiorcza – pręt 1,5 m zawieszony na maszcie h=16,5 m;
- moc zakłóceń na wejściu odbiornika rozpoznawczego $P_Z = 5 \times 10^{-14}$ W.

ZYSK ENERGETYCZNY ANTENY (G_N) W FUNKCJI CZĘSTOTLIWOŚCI (f)

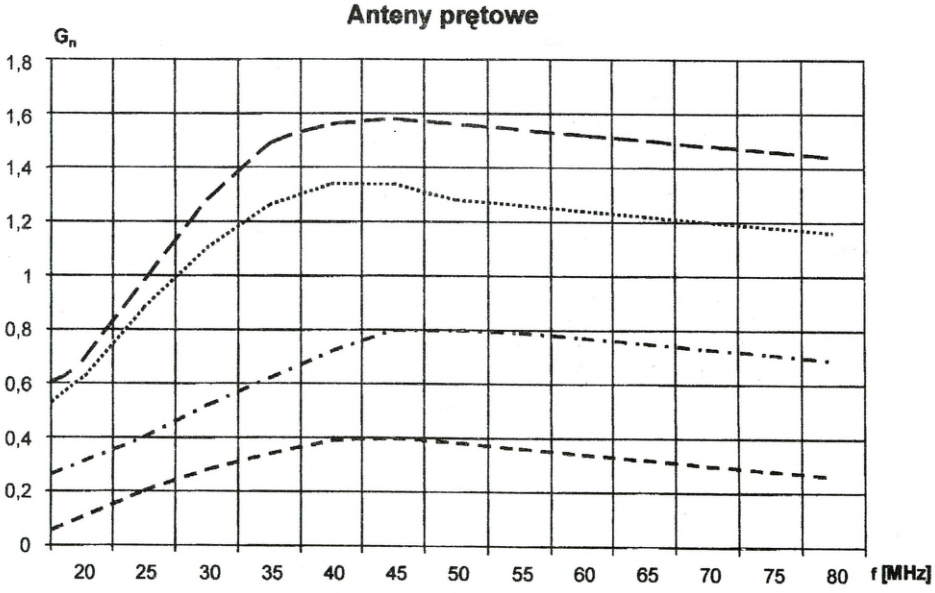
Anteny kierunkowe



Legenda: — · — A — — B

A – półromb pionowy;
B – antena z falą bieżącą o długości 40 m i wysokości zawieszenia 1 m.

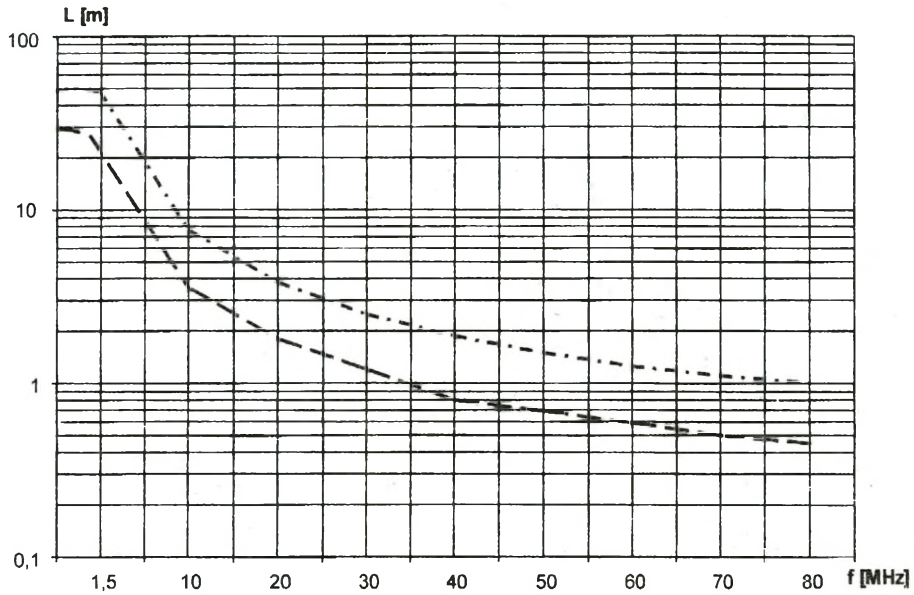
Anteny prętowe



Warunki: — — 4 m ·····3,4 m — · — 2,7 m — — — 1,5

- radiostacja rozwinięta w terenie odkrytym o średniej wilgotności.

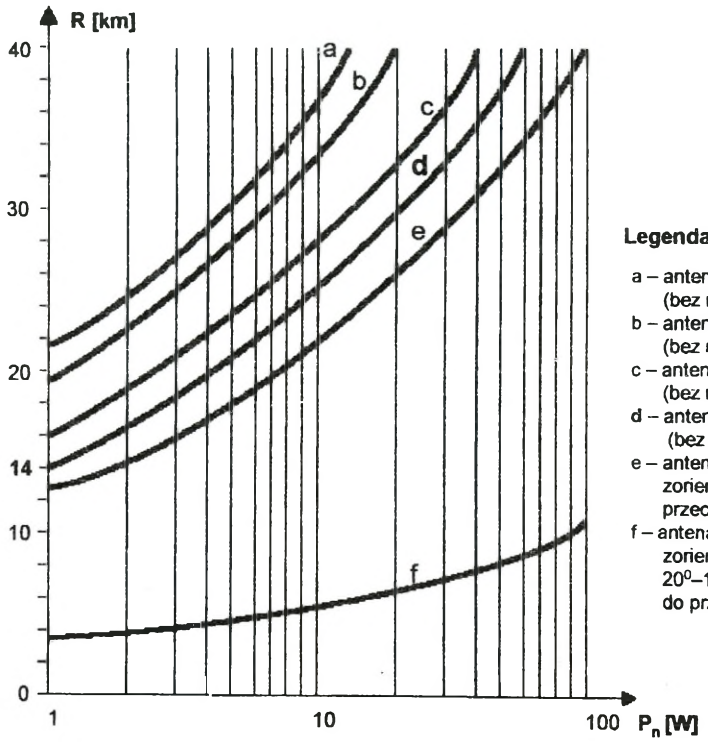
OPTYMALNA ODLEGŁOŚĆ POMIĘDZY ANTENĄ PRĘTOWĄ A EKRANEM (L) W FUNKCJI DŁUGOŚCI FALI ROBOCZEJ NADAJNIKA



Warunki: – · – 25% — — 12%

- odległość pomiędzy ekranem a anteną powinna wynosić 12 – 25% długości fali (λ) oraz być dobierana z określonego na wykresie obszaru w ten sposób, aby odpowiadała jak największej liczbie częstotliwości wykorzystywanych przez nadajnik lub częstotliwości, na których przewidywana jest praca z wykorzystaniem danej anteny;
- dla zakresu VHF optymalna jest odległość 1 m, która pozwala skutecznie ekranować antenę bez względu na długość fali roboczej.

GŁĘBOKOŚĆ STREFY DOSTĘPNOŚCI ELEKTROMAGNETYCZNEJ (R) RADIOELEKTRONICZNYCH ŚRODKÓW ŁĄCZNOŚCI W FUNKCJI MOCY NADAJNIKA (P_N) Z UWZGLĘDNIENIEM WYBRANYCH TYPÓW ANTEN



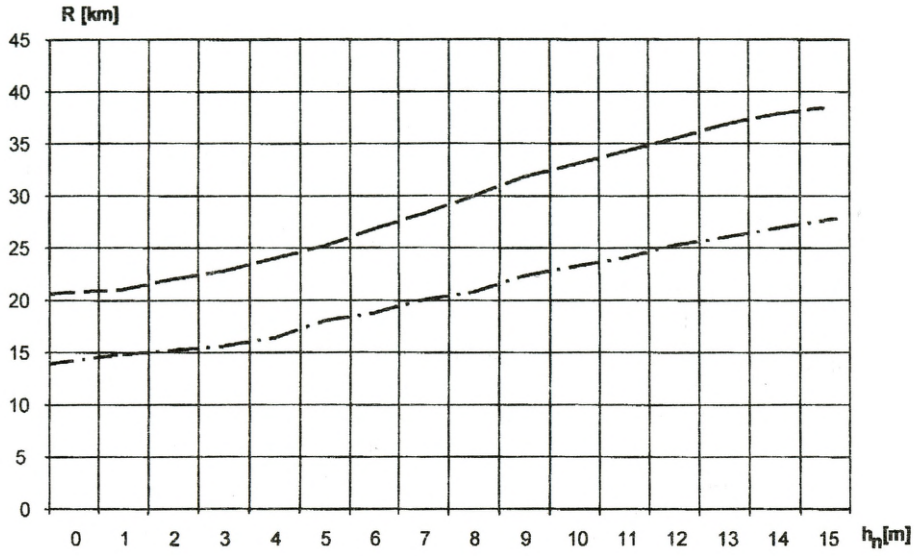
Legenda:

a – antena prętowa 4 m (bez masztu);
b – antena prętowa 3,4 m (bez masztu);
c – antena prętowa 2,7 m (bez masztu);
d – antena prętowa 1,5 m (bez masztu);
e – antena z falą bieżącą zorientowana w kierunku przeciwnika;
f – antena z falą bieżącą zorientowana pod kątem 20^0–160^0 w stosunku do przedniego skraju obrony.

Warunki:

- radiostacja rozwinięta w terenie odkrytym o ubogiej morfologii;
- gleba średnio wilgotna (ε=10, $\sigma = 10^{-2}$);
- częstotliwość robocza 40 MHz;
- antena odbiorcza prętowa 1,5 m zawieszona na maszcie 16,5 m;
- moc zakłóceń na wejściu odbiornika $P_Z = 5 \times 10^{-14}$ W.

WPŁYW WYSOKOŚCI ZAWIESZENIA ANTENY (h_n) NA GŁĘBOKOŚĆ STREFY DOSTĘPNOŚCI ELEKTROMAGNETYCZNEJ DLA RÓŻNYCH ANTEN PRĘTOWYCH

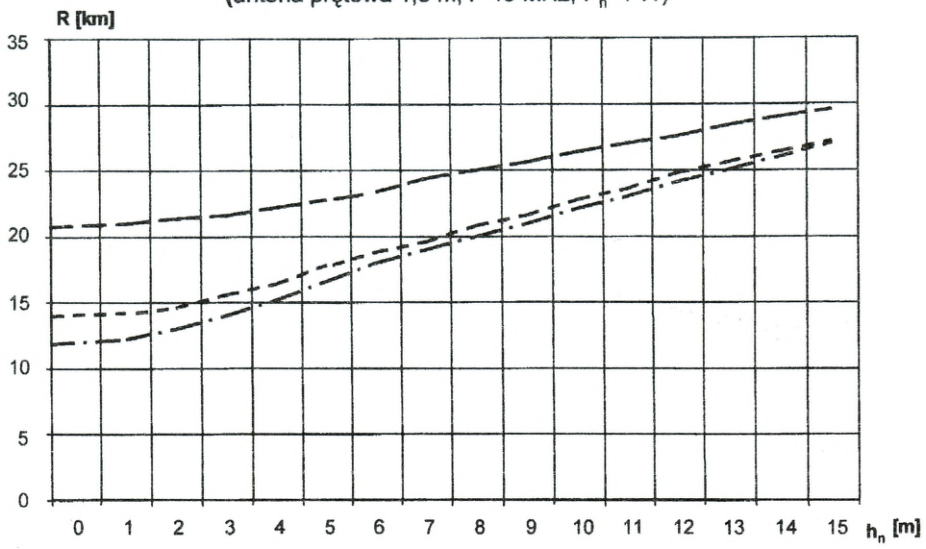


Legenda: — — A — · — B

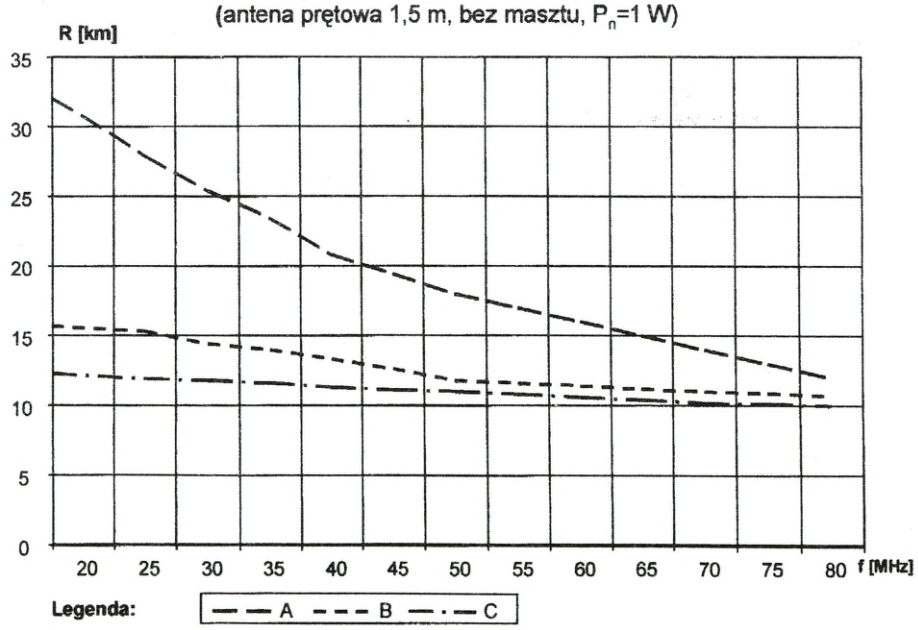
A – antena prętowa 4 m;
B – antena prętowa 1,5 m.

GŁĘBOKOŚĆ STREFY DOSTĘPNOŚCI ELEKTROMAGNETYCZNEJ (R) Z UWZGLĘDNIENIEM PARAMETRÓW ELEKTRYCZNYCH GRUNTU

w funkcji wysokości wzniesienia anteny
(antena prętowa 1,5 m, f=40 MHz, P_n=1 W)

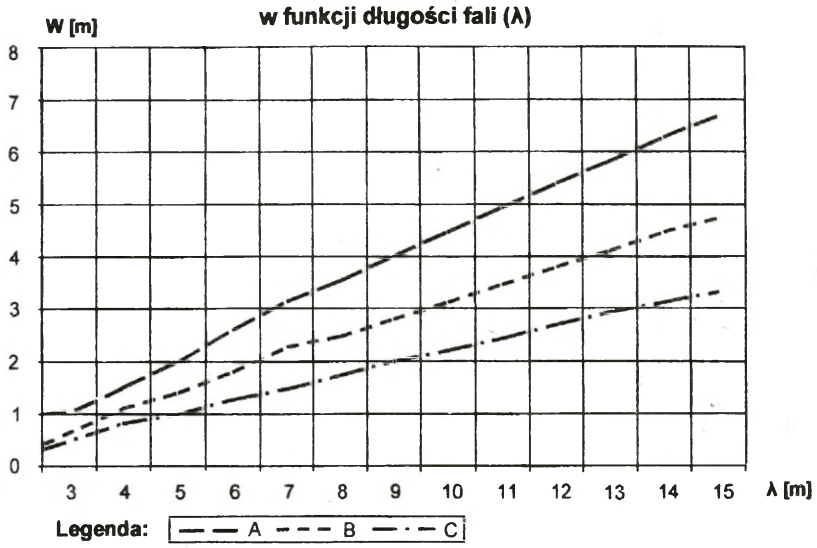


w funkcji częstotliwości roboczej nadajnika
(antena prętowa 1,5 m, bez masztu, P_n=1 W)

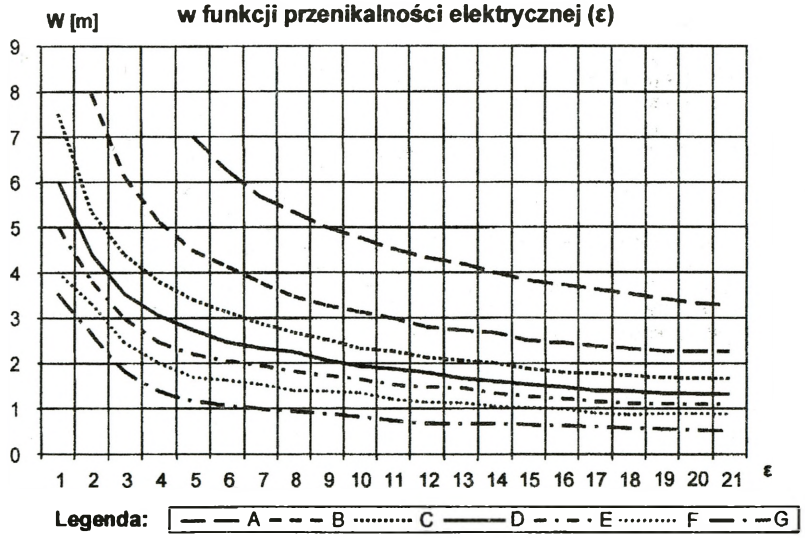


A – grunt bardzo mokry (bagna, błota, jeziora, rzeki);
B – grunt średnio wilgotny (lasy, łąki);
C – grunt suchy.

WPŁYW PARAMETRÓW ELEKTRYCZNYCH GRUNTU NA GŁĘBOKOŚĆ PRZENIKANIA FAL ELEKTROMAGNETYCZNYCH NA POWŁOKĘ ZIEMSKĄ (W)

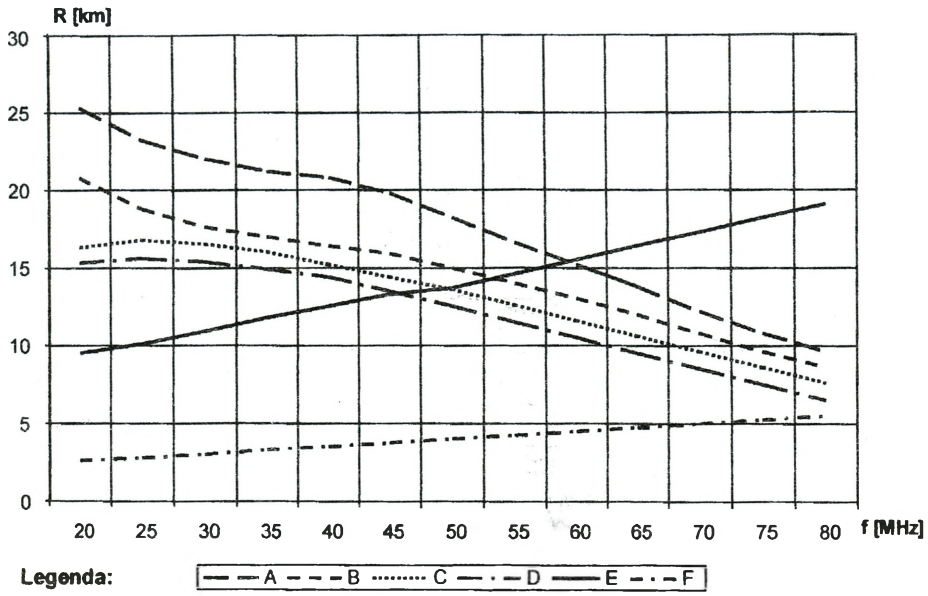


A – ε = 5 (grunt suchy);
B – ε = 10 (grunt średnio wilgotny);
C – ε = 20 (grunt bardzo wilgotny).



A – λ = 15 m; (f = 20 MHz);
B – λ = 10 m; (f = 30 MHz);
C – λ = 7,5 m; (f = 40 MHz);
D – λ = 6 m; (f = 50 MHz);
E – λ = 5 m (f = 60 MHz);
F – λ = 4,29 m; (f = 70 MHz);
G – λ = 3,75 m; (f = 80 MHz).

GŁĘBOKOŚĆ STREFY DOSTĘPNOŚCI ELEKTROMAGNETYCZNEJ (R) W FUNKCJI CZĘSTOTLIWOŚCI ROBOCZEJ NADAJNIKA Z UWZGLĘDNIENIEM RÓŻNYCH ANTEN



A – antena prętowa 4 m;
B – antena prętowa 2,7 m;
C – antena prętowa 2 m;
D – antena prętowa 1,5 m;
E – antena promieniowa 40/1 m, $\alpha = 0^0$;
F – antena promieniowa 40/1 m, $\alpha = 110 \div 250^0$.

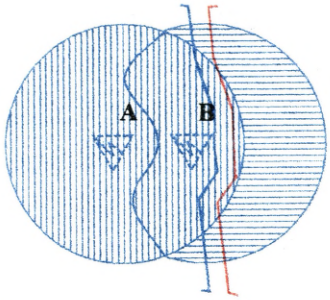
Warunki:

α - kąt pomiędzy osią kierunkową anteny a linią łączącą antenę z najbliższym punktem linii styczności wojsk;
- anteny prętowe nie zawieszone na masztach;
- moc nadajnika 1 W;
- grunt średnio wilgotny ($\varepsilon = 10$, $\sigma = 10^{-2}$).

Załącznik 11

MASKOWANIE PRACY RADIOSTACJI ZASŁONĄ RADIOWĄ

1. Za pomocą radiostacji maskującej o identycznej mocy

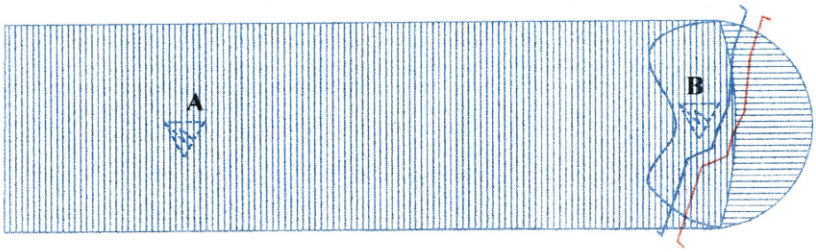


LEGENDA:
A - miejsce rozwinięcia radiostacji ukrywanej;
B - miejsce rozwinięcia radiostacji maskującej;

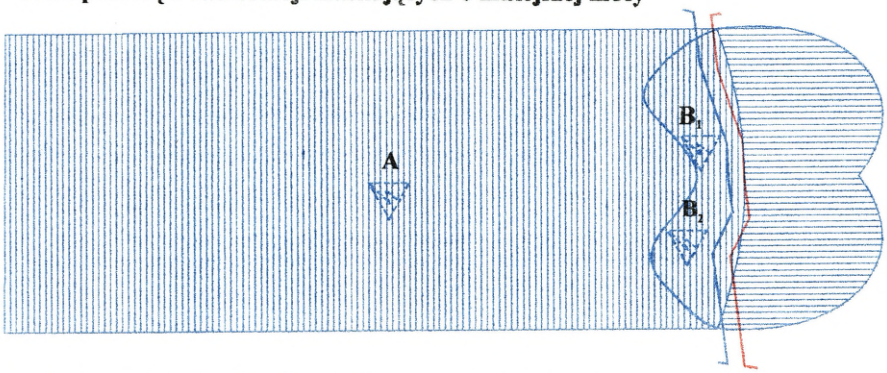
Strefa dostępności elektromagnetycznej radiostacji ukrywanej;

Strefa dostępności elektromagnetycznej radiostacji maskującej.

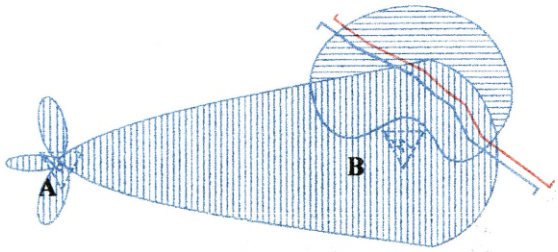
2. Za pomocą radiostacji maskującej o mniejszej mocy



3. Za pomocą 2 radiostacji maskujących o mniejszej mocy



4. Podczas ukrywania radiostacji pracującej z anteną kierunkową



Załącznik 12

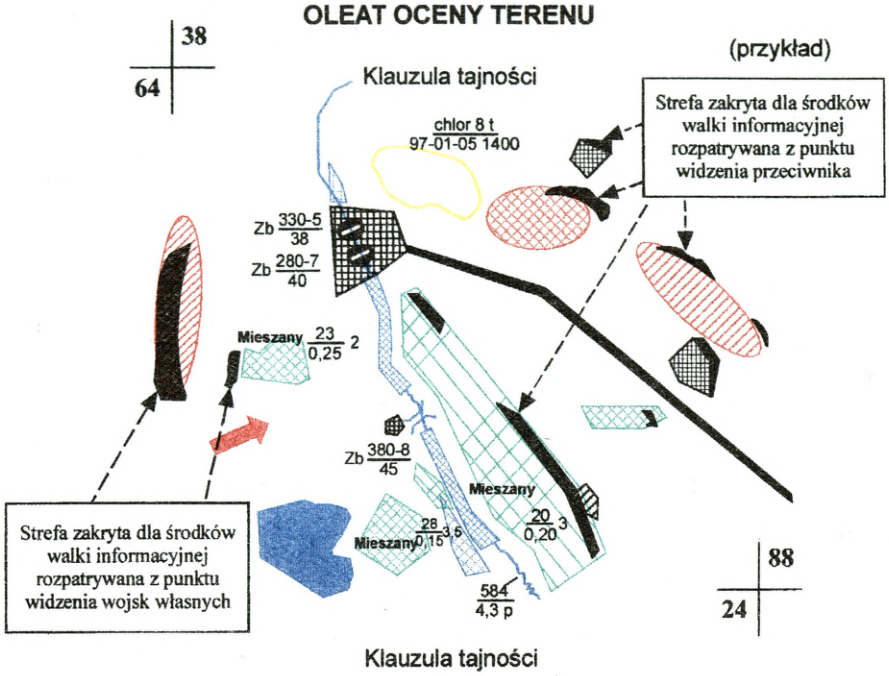
WYKAZ
WARTOŚCI WYMAGANYCH WSPÓŁCZYNNIKÓW OCHRONNYCH (p) DLA WYBRANYCH EMISJI RADIOWYCH*

Nazwa emisji użytecznych	Wartość współczynnika p w zależności od rodzaju emisji zakłócającej											
	A-3E			J-3E			F-3E			F-1B		
	dB	$\frac{E_s}{E_z}$	$\frac{P_s}{P_z}$	dB	$\frac{E_s}{E_z}$	$\frac{P_s}{P_z}$	dB	$\frac{E_s}{E_z}$	$\frac{P_s}{P_z}$	dB	$\frac{E_s}{E_z}$	$\frac{P_s}{P_z}$
J-3E telef. utajn.				24	15,8	251						
F-3E telef. utajn.	18	7,9	63,1				18	7,9	63,1			
A-3E	15 do 17	5,62 do 7,08	31,6 do 50,1				12	3,98	15,8			
J-3E				12 do 15	3,98 do 5,62	15,8 do 31,6						
F-3E	10	3,16	10				8 do 10	2,51 do 3,16	6,3 do 10			
F-1B	8	2,51	6,3	12	3,98	15,8				7	2,23	5,01

* Przedstawione wyżej wartości współczynnika (p) w pełni gwarantują niezakłóconą pracę linii radiowych. Wartości te nie zawsze będzie można osiągnąć w działaniach bojowych. Toteż w wypadkach szczególnych powinno się przyjmować ich wartości nawet mniejsze o 30 %, wiedząc, iż linie radiowe pracujące w tych warunkach będą spełniać swoje zadanie, lecz czas przekazywania komunikatu może się wydłużyć w związku z koniecznością powtarzania go dla osiągnięcia wymaganej wierności.

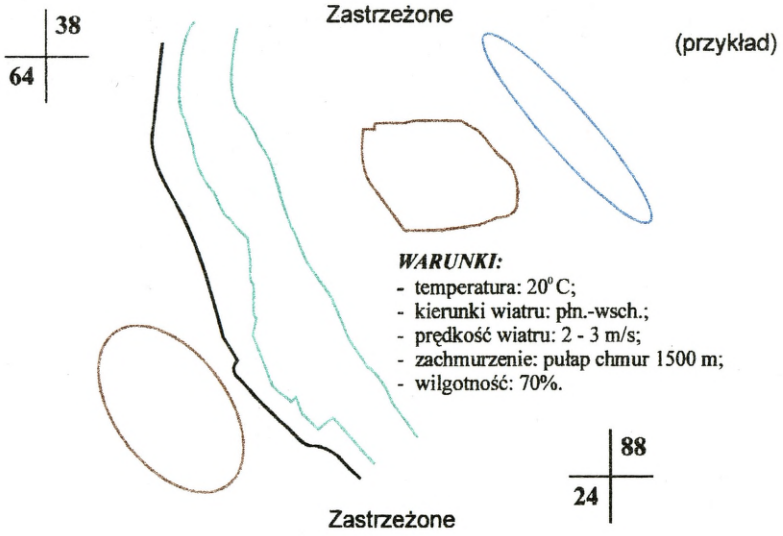
Załącznik 13*

OLEAT OCENY TERENU



Załącznik 14*

OLEAT WARUNKÓW METEOROLOGICZNYCH

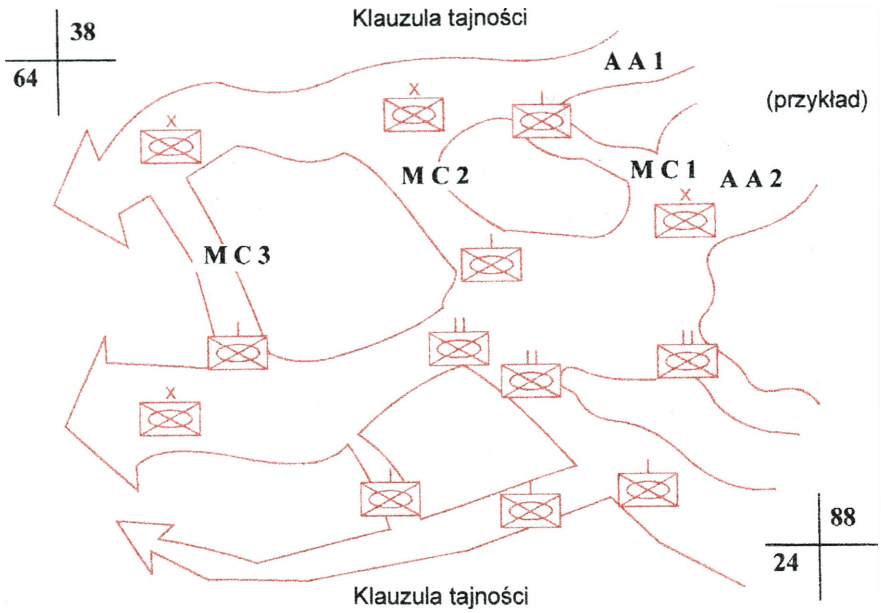


* Opracowano na podstawie: J. Janczak, B. Bezoń, W. Scheffs, „Walka elektroniczna w działaniach taktycznych wojsk lądowych". Praca naukowo-badawcza, wyd. AON, Warszawa 1999, s. 147.

* Tamże, s. 154.

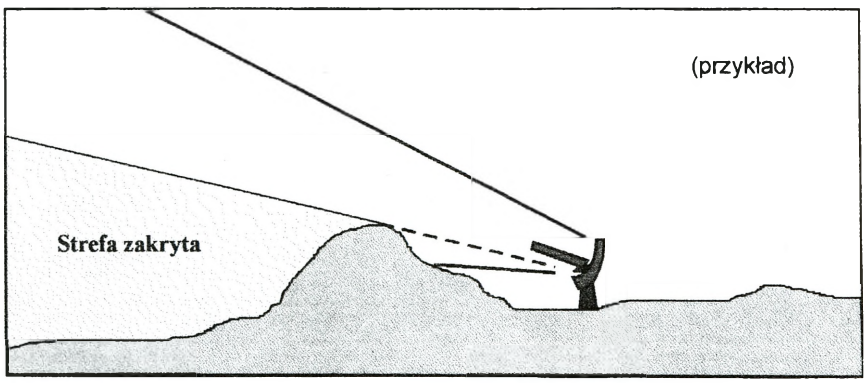
Załącznik 15*

OLEAT DRÓG PODEJŚCIA I KORYTARZY MANEWRU DLA DYWIZJI PIERWSZEGO RZUTU



Załącznik 16*

ILUSTRACJA UKOŚNEJ LINII WIDOCZNOŚCI Z ZIEMI

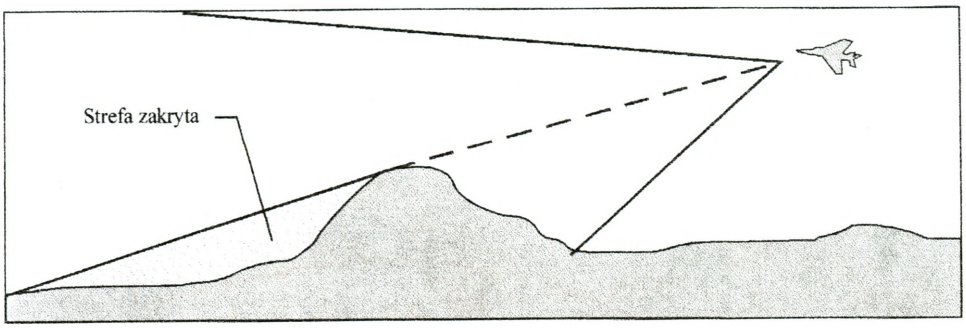


* Tamże, s. 148.
* Tamże, s. 149.

Załącznik 17*

ILUSTRACJA UKOŚNEJ LINII WIDOCZNOŚCI Z POWIETRZA

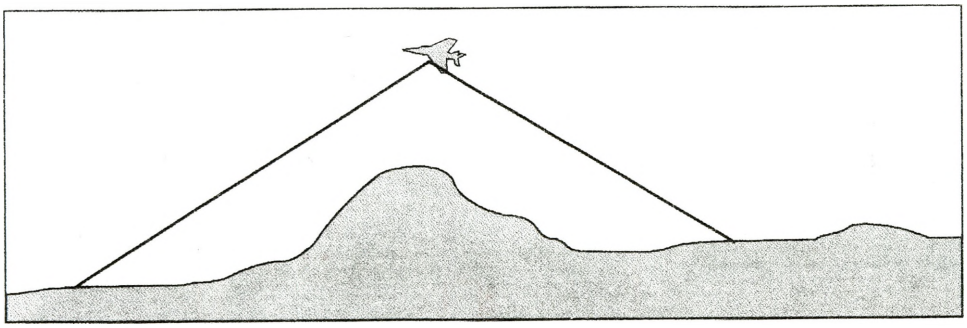
(przykład)



Załącznik 18*

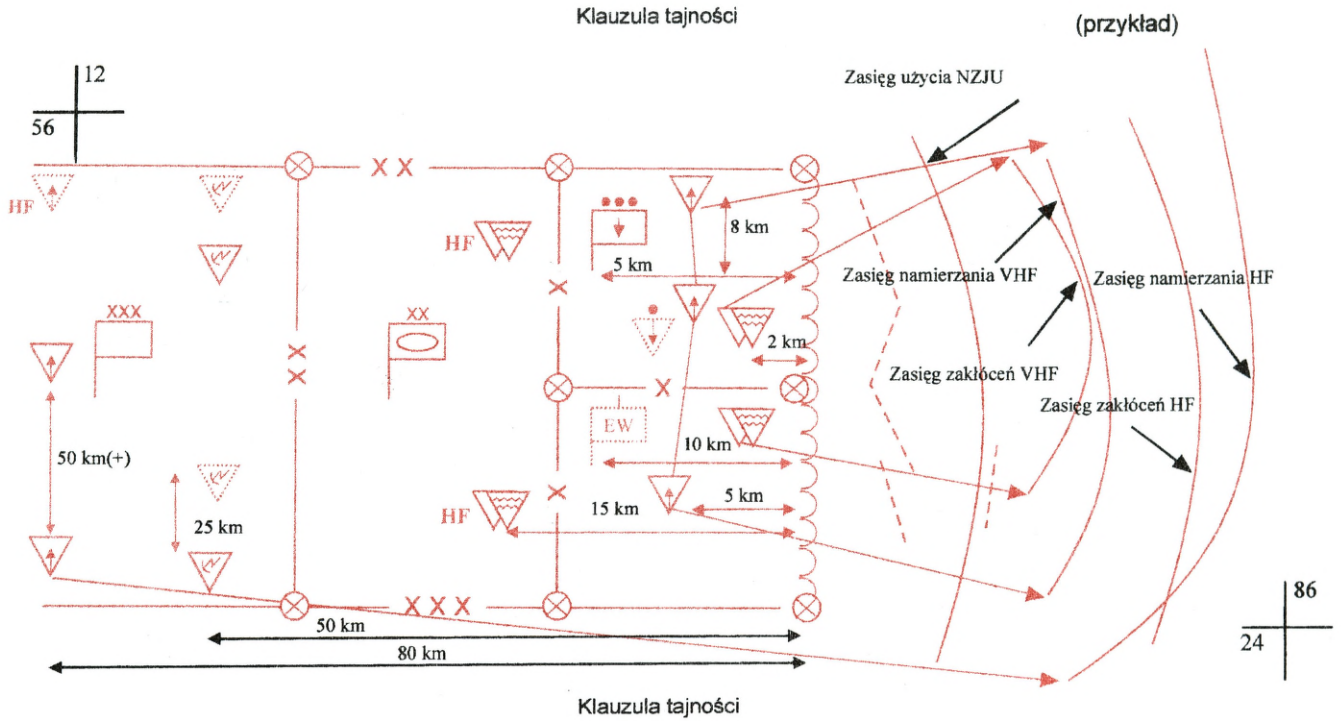
ILUSTRACJA PIONOWEJ LINII WIDOCZNOŚCI Z POWIETRZA

(przykład)



* Tamże, s. 149.
* Tamże, s. 149.

OLEAT - WALKA INFORMACYJNA (ROZPOZNANIE I ZAKŁÓCANIE) W DZIAŁANIACH ZACZEPNYCH PRZECIWNIKA

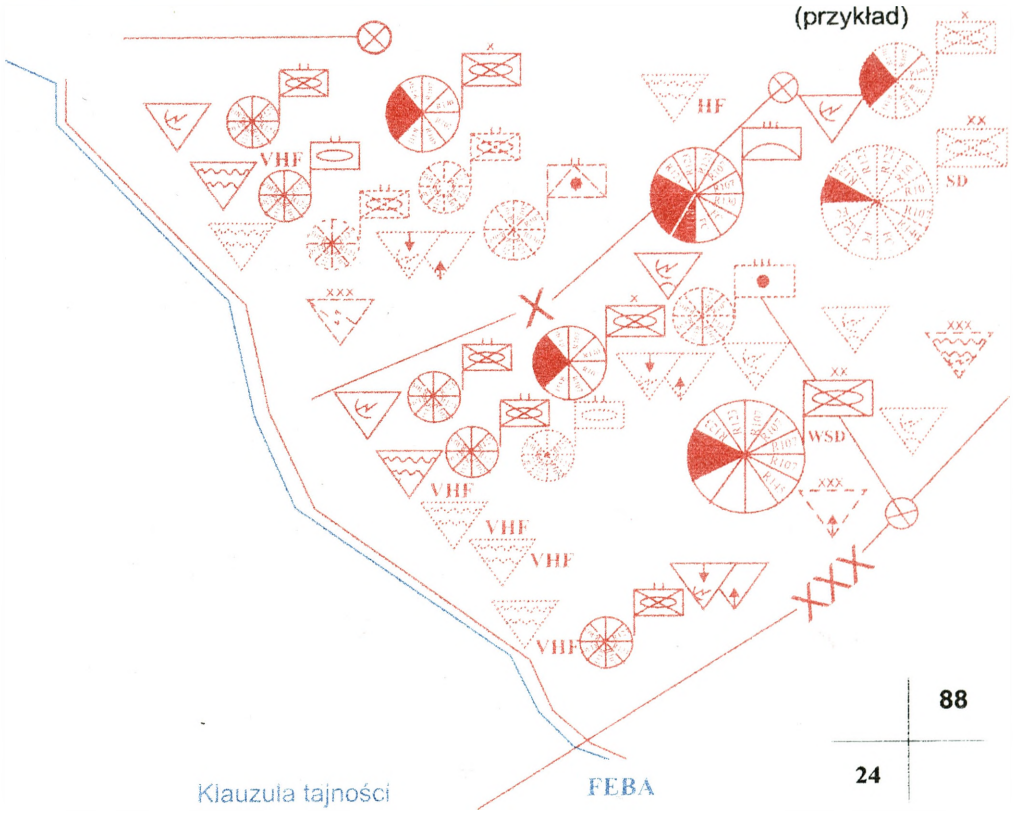


* Tamże, s. 229.

Załącznik 20

OLEAT SYTUACYJNY W SFERZE INFORMACYJNEJ*

(przykład)



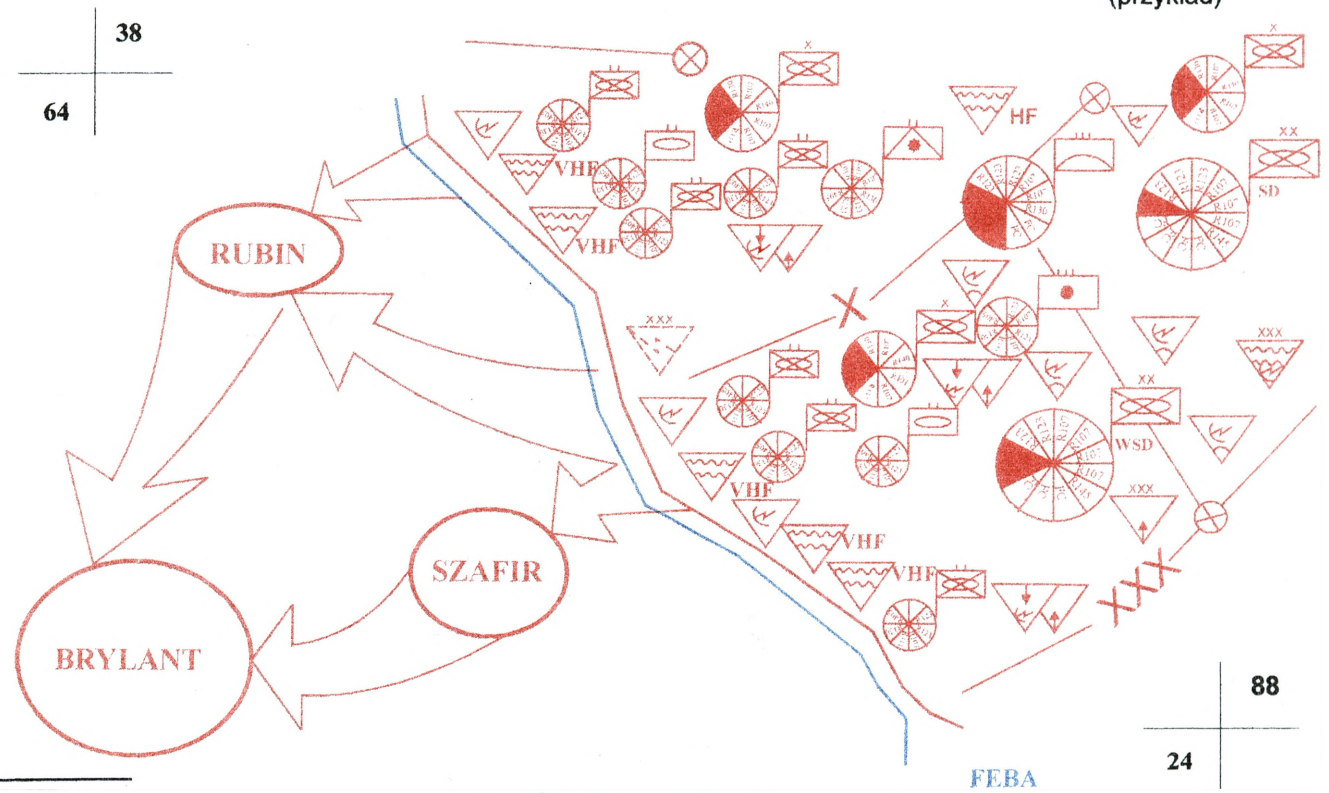
*Tamże, s. 221.

Klauzula tajności

Załącznik 21

OLEAT ZAGROŻEŃ INFORMACYJNYCH NA KIERUNKU DZIAŁANIA PIERWSZORZUTOWEJ DYWIZJI
(wariant nr..)

(przykład)

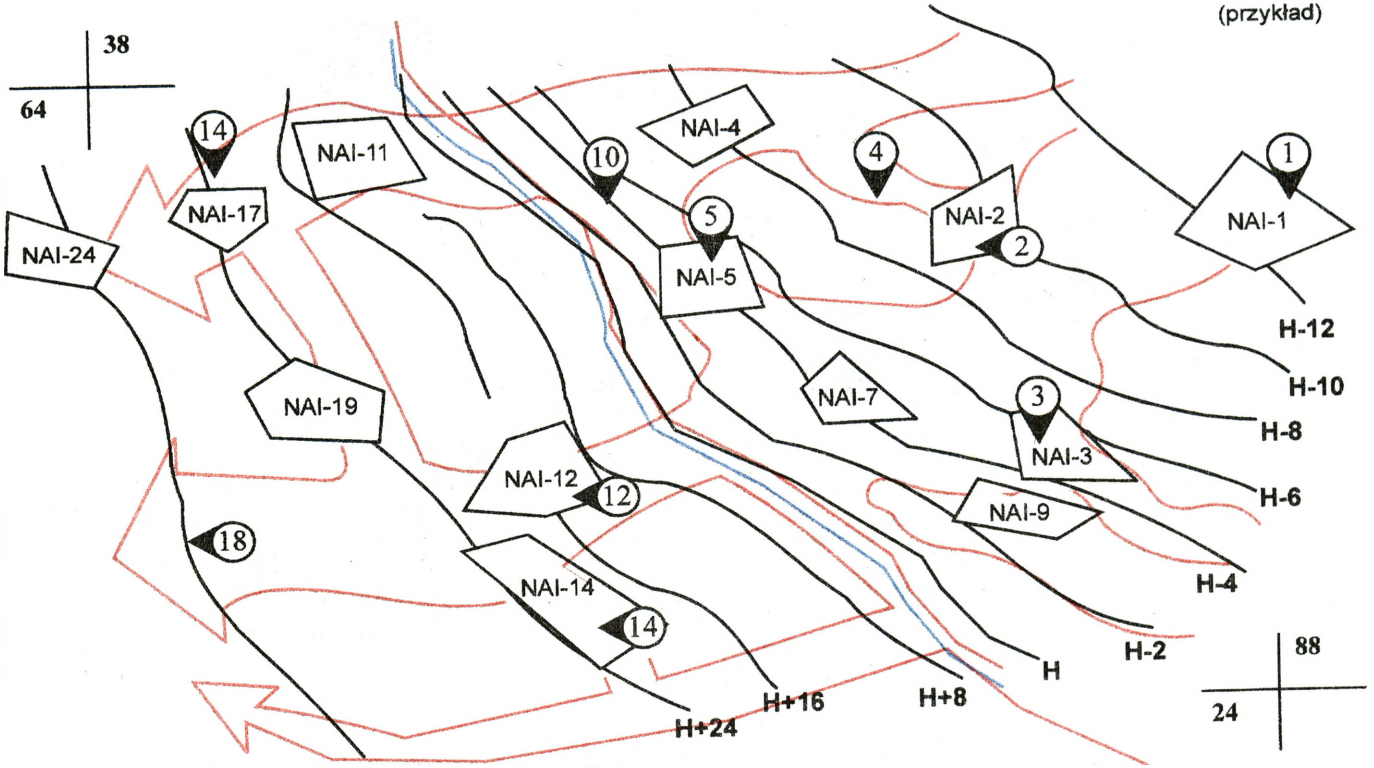


*Tamże, s. 222.

Klauzula tajności

OLEAT ZDARZEŃ INFORMACYJNYCH W PASIE DZIAŁANIA PIERWSZORZUTOWEJ DYWIZJI

(przykład)



Klauzula tajności

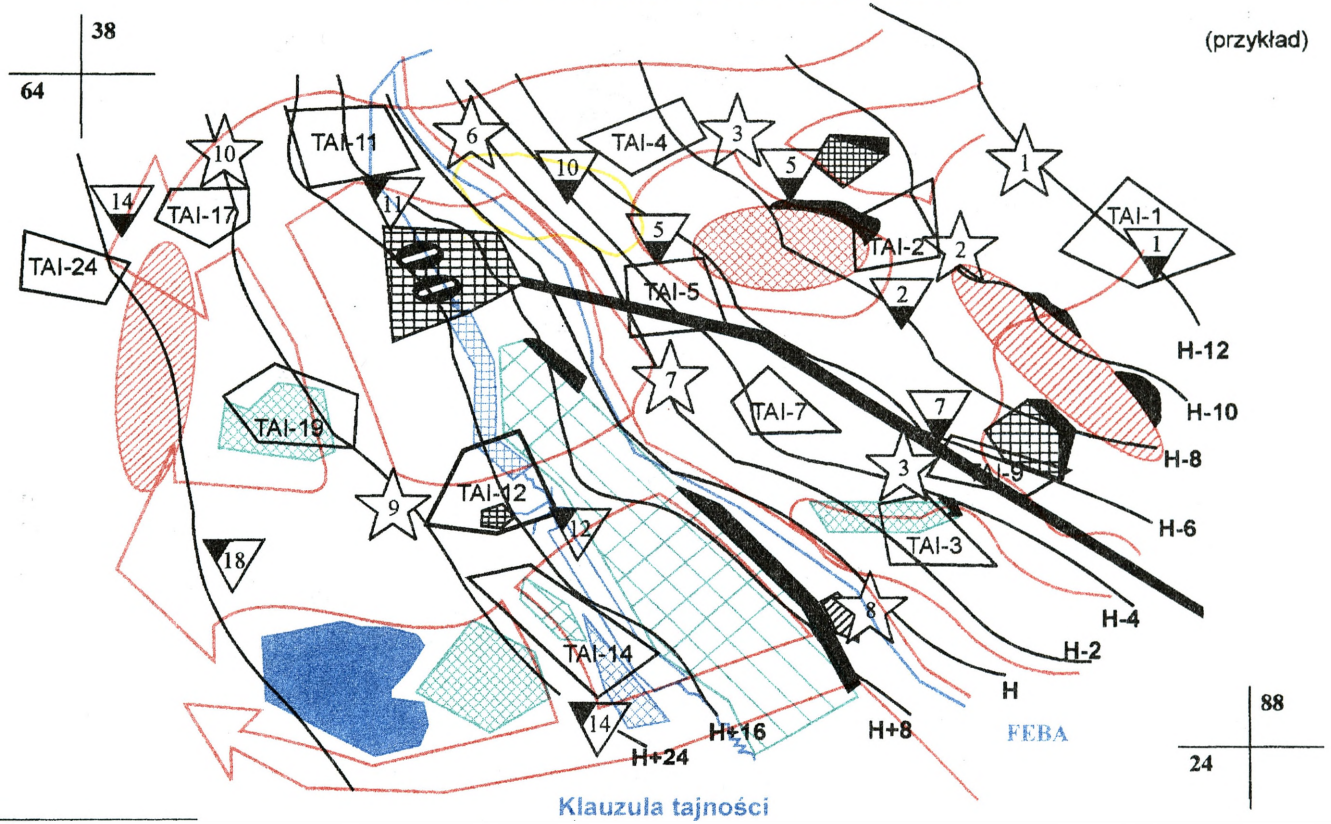
*Tamże, s. 225.

Załącznik 23

Klauzula tajności

OLEAT WSPARCIA DECYZJI W PASIE DZIAŁANIA PIERWSZORZUTOWEJ DYWIZJI
Z UWZGLĘDNIENIEM SFERY INFORMACYJNEJ

(przykład)



Klauzula tajności

*Tamże, s. 226.

Załącznik 24

PLAN OBRONY INFORMACYJNEJ W DZIAŁANIACH OBRONNYCH ..... ZWIĄZKU OPERACYJNEGO

(przykład)

Lp.	Rodzaj zadania	Rodzaj przedsięwzięcia	Treść przedsięwzięcia	Termin realizacji	Sposób wykonania	Odpowiedzialność funkcyjna	Sposób kontroli	Uwagi
I. W czasie organizowania działań obronnych związku operacyjnego								
1.	Obrona informacyjna wojsk ZO przed rozpoznaniem	Dezinformowanie (wprowadzanie w błąd)	1. Informowanie w środkach masowego przekazu o ruchach wojsk w innych rejonach niż rzeczywiste. 2. Doniesienia mylące w prasie lokalnej. 3. Utwierdzanie przeciwnika o przygotowaniach wojsk ZO do obrony w innym obszarze niż ogłoszony w zamiarze dowódcy. 4. Inne.	W okresach poprzedzających organizowanie działań obronnych. Podczas organizowania działań obronnych. G-	Wg planu dezinformowania przełożonego. Krótkie informacje prasowe. Przeprowadzanie pozornego rekonesansu w rejonie	Sztab przełożonego. Sztab ... ZO. Sztab ... BZ.	Wg harmonogramu.	
		Pozorowanie	1. Prowadzenie wymiany informacji między sztabami biorącymi udział w pozorowaniu. 2. Działalność demonstracyjna w rejonie..... 3. Inne.	G- .... Wg planu pozorowania związku operacyjnego.	Wymiana telegramów ćwiczebnych. Zajmowanie rejonu.	Kierownik zespołu łączności i informatyki SD... ZO. Wydzielone środki ruchome.	Wg harmonogramu. Wg harmonogramu.	

		Ukrywanie	1. Skryte wyprowadzenie wojsk ZO z rejonów wyjściowych.	Podczas wyprowadzania wojsk z rejonów wyjściowych.	Zgodnie z zasadami maskowania bezpośredniego.	Dowódcy związków taktycznych, i oddziałów.	Szef sztabu i organa regulacji ruchu.	
			2. Ochrona kontrwywiadowcza wojsk związku operacyjnego.	W rejonach wyjściowych i podczas marszu.	Zgodnie z obowiązującymi procedurami.	Oficer grupy obrony informacyjnej.	Szef G 2 ... ZO	
			3. Ubezpieczenie marszu wojsk związku operacyjnego.	Podczas wykonywania marszu.	Zgodnie z obowiązującymi regulaminami.	Dowódcy związków taktycznych, i oddziałów.	Szef sztabu ... ZO.	
			4. Maskowanie elektroniczne.	W rejonach wyjściowych i podczas marszu.	Realizacja przedsięwzięć maskowania elektronicznego.	Użytkownicy środków elektronicznych.	Specjaliści rodzajów wojsk i służb.	
			5. Ukrywanie przygotowań obszaru obrony związku operacyjnego.	W rejonach rozmieszczenia stanowisk dowodzenia i punktów kierowania ogniem.	Ograniczenie ruchu wojsk oraz zakaz pracy SE na nadawanie.	Specjaliści rodzajów wojsk.	Wg harmonogramu.	
			6. Inne.					
2.	Obrona informacyjna wojsk ZO przed zakłócaniem	Obrona informacyjna wojsk ZO przed oddziaływaniem dezinformującym	1. Zachowanie czujności i realizacja przedsięwzięć w celu zapobiegania obcej działalności dezinformującej, dywersyjnej i sabotażowej.	W czasie dezorganizacji podejścia przeciwnika.	Stałe sprawdzanie tożsamości korespondentów	Użytkownicy środków łączności i informatyki.	Kierownik zespołu łączności i informatyki SD... ZO.	

			2. Podejmowanie działań utrudniających wprowadzenie sygnałów dezinformujących do systemów dowodzenia i naprowadzania uzbrojenia. 3. Inne	W rejonach wyjściowych i podczas marszu.	Wykonanie przedsięwzięć kontrdezinformacyjnych.	Użytkownicy technicznych środków dowodzenia i naprowadzania uzbrojenia.	Wg harmonogramu.	
		Obrona informacyjna wojsk ZO przed zakłócaniem zagłuszającym	1. Rozpoznanie środków (systemów) zakłócania zagłuszającego przeciwnika. 2. Maskowanie pracy własnych systemów dowodzenia i naprowadzania uzbrojenia. 3. Inne.	W czasie dezorganizacji podejścia przeciwnika. W rejonach wyjściowych i podczas marszu.	Wg planu rozpoznania elektronicznego. Wykonanie przedsięwzięć obrony antyzagłuszeniowej.	Elementy rozpoznania elektronicznego ..ZO. Specjaliści rodzajów wojsk i służb.	Wg harmonogramu. Wg harmonogramu.	
II. W czasie obrony w obszarze działań sił osłony								
1.	Obrona informacyjna wojsk ZO przed rozpoznaniem	Ukrywanie	1. Ukrywanie przedniego skraju obrony oraz elementów ugrupowania obronnego sił głównych związku operacyjnego. 2..Ochrona rejonów, obiektów, stanowisk dowodzenia i punków kierowania ogniem przed penetracją grup rozpoznawczo-dywersyjnych.	Po zajęciu rejonów obrony. Po zajęciu rejonów obrony.	Maskowanie bezpośrednie.. Wzmocnienie ubezpieczenia wojsk związku operacyjnego.	Dowódcy wszystkich szczebli dowodzenia. Dowódcy elementów ochrony i komendanci stanowisk dowodzenia.	Wg harmonogramu. Szef sztabu ... ZO.	

			3. Maskowanie elektroniczne.	Po zajęciu rejonów obrony.	Ograniczenie dostępności elektromagnetyczne i czasowej SE.	Użytkownicy środków radioelektronicznych.	Specjaliści rodzajów wojsk i służb.	
			4. Maskowanie radiolokacyjne optoelektroniczne i czujnikowe	Po zajęciu rejonów obrony.	Wykonanie przedsięwzięć organizacyjnych i technicznych.	Dowódcy związków taktycznych, i oddziałów.	Wg harmonogramu.	
			5. Maskowanie informatyczne	Po zajęciu rejonów obrony.	Wykonanie przedsięwzięć organizacyjnych i technicznych.	Użytkownicy systemów dowodzenia i naprowadzania uzbrojenia.	Wg harmonogramu.	
			6. Inne					
		Pozorowanie	1. Pozorowanie SD .....BZ, w rejonie	G -	Wykorzystanie makiet i środków podręcznych.	Wojska osłonowe.	Wg harmonogramu.	W uzgodnieniu z G 3.
			2. Działalność demonstracyjna po trasie	Wg planu pozorowania związku operacyjnego.	Pozorowany przemarsz.	Wydzielone środki ruchome.	Szef sztabu ... ZO.	
			3. Prowadzenie wymiany informacji między sztabami biorącymi udział w pozorowaniu.....	Podczas organizacji systemów dowodzenia, łączności i informatyki.	Wiadomości mylące w sieci radioliniowo-kablowej.	Jednostki dowodzenia ... ZO.	Wg harmonogramu.	W uzgodnieniu z G 3.
			4. Inne					

		Dezinformowanie (wprowadzanie w błąd)	1. Przekazywanie sprzecznych informacji w środkach masowego przekazu.	G -	Wg planu dezinformowania szczebla nadrzędnego.	Sztab przełożonego.		
			2. Działalność ulotkowa (wpływanie na postawy żołnierzy przeciwnika).	G -	Wg planu działań psychologicznych.	.....G.Dz.Psych.	Wg harmonogramu.	W uzgodnieniu z G 3.
			3. Skierowanie uderzeń przeciwnika w rejon głównego wysiłku obrony.	W czasie prowadzenia działań osłonowych	Kontrolowana utrata dokumentu mylącego w rejonie	Sztab .....BZ.	Wg harmonogramu.	
			4. Inne					
2.	Obrona informacyjna wojsk ZO przed zakłócaniem	Obrona informacyjna wojsk ZO przed oddziaływaniem dezinformującym	1. Zachowanie czujności i realizacja przedsięwzięć ułatwiających identyfikację obcej działalności dezinformującym, dywersyjnej i sabotażowej.	W czasie prowadzenia działań osłonowych.	Stałe sprawdzanie tożsamości korespondentów i inne przedsięwzięcia.	Użytkownicy środków łączności i informatyki.	Wg harmonogramu.	
			2. Podejmowanie działań utrudniających wprowadzenie sygnałów mylących do systemów dowodzenia i naprowadzania uzbrojenia.	W czasie prowadzenia działań osłonowych.	Ścisłe przestrzeganie zasad eksploatacji technicznych środków dowodzenia i naprowadzania uzbrojenia.	Użytkownicy technicznych środków dowodzenia i naprowadzania uzbrojenia.	Wg harmonogramu.	
			3. Inne.					

		Obrona informacyjna wojsk ZO przed zakłócaniem zagłuszającym	1. Rozpoznanie środków (systemów) zakłócania zagłuszającego przeciwnika. 2. Maskowanie pracy systemów dowodzenia i naprowadzania uzbrojenia sił głównych. 3. Inne.	W czasie prowadzenia działań osłonowych. W czasie prowadzenia działań osłonowych.	Wg planu rozpoznania elektronicznego. Realizacja przedsięwzięć obrony informacyjnej przed zakłóceniem.	Siły i środki rozpoznania elektronicznego ..ZO. Użytkownicy systemów elektronicznych.	G 2.... ZO. Wg harmonogramu.	
III. Podczas odparcia uderzenia i uniemożliwienia przełamania głównego obszaru obrony związku operacyjnego								
1.	Obrona informacyjna wojsk ZO przed rozpoznaniem	Ukrywanie	1. Ukrywanie sił wzmocnienia, blokowania i prowadzenia kontrataku. 2. Ochrona rejonów, obiektów, stanowisk dowodzenia i punków kierowania ogniem przed penetracją grup rozpoznawczo-dywersyjnych. 3. Osłona radiolokacyjna SD ... ZO. Inne.	W czasie walki o utrzymanie przedniego skraju obrony. Po zajęciu rejonów obrony. Po zajęciu rejonu obrony	Realizacja przedsięwzięć maskowania bezpośredniego. Realizacja przedsięwzięć ubezpieczenia wojsk związku operacyjnego. Wg planu zakłócania.	Dowódca odwodu ogólnowojskowgo. Dowódcy elementów ochrony i komendanci stanowisk dowodzenia. Elementy zakłócania radiolokacyjnego.	Wg harmonogramu. Szef sztabu związku operacyjnego. Wg harmonogramu.	
		Pozorowanie	1. Pozorowanie ugrupowania obronnego BZ w rejonie	G +....	Ustawienie makiet i wykorzystanie odbijaczy kątowych	....Bsap. i wydzielone siły i środki.	Wg harmonogramu.	W uzgodnieniu z G 3.

			2. Organizacja pozornych stanowisk ogniowych artylerii w rejonie		Ustawienie makiet i odbijaczy kątowych.	Bsap. i wydzielone i środki.	Wg harmonogramu.	W uzgodnieniu z G 3.
			3. Pozorowanie przegrupowania batalionu po drodze	G + ...	Wykonanie marszu.	Wydzielone siły i środki bp i regulacji ruchu.	Wg harmonogramu. Szef logistyki.	
			4. Organizacja pozornych obiektów logistycznych w rejonie	G + ...	Inżynieryjna rozbudowa rejonu bzaop.	Wydzielone siły i środki ..... Bsap.	Wg harmonogramu.	W uzgodnieniu z G 3.
			5. Prowadzenie intensywnej wymiany informacji między sztabami biorącymi udział w pozorowaniu.	G + ...	Wiadomości mylące w sieci łączności radiowej.	Kierownik zespołu łączności i informatyki SD... ZO.		
			6. Inne.	G + ...				
		Dezinformowanie (wprowadzanie w błąd)	1. Przekazywanie sprzecznych informacji w środkach masowego przekazu.	G + ...	Wg planu dezinformowania przełożonego.	Sztab przełożonego.		W uzgodnieniu z G 3.
			2. Działalność ulotkowa (wpływanie na motywacje wojsk przeciwnika).	G + ...	Wg planu działań psychologicznych.	...G.Dz..Psych.	Wg harmonogramu.	
			3. Utwierdzanie przeciwnika o przygotowaniach do kontrataku w rejonie innym niż w działaniach rzeczywistych.	Podczas walk o utrzymanie przedniego skraju obrony	Kontrolowana utrata dokumentu.	Sztab ...DZ.	Wg harmonogramu.	
			4. Inne.					

2.	Obrona informacyjna wojsk ZO przed zakłócaniem	Obrona informacyjna wojsk ZO przed oddziaływaniem dezinformującym	1. Zachowanie czujności i realizacja przedsięwzięć ułatwiających identyfikację działalności dezinformującej, dywersyjnej i sabotażowej. 2. Podejmowanie działań utrudniających wprowadzenie sygnałów dezinformujących do systemów dowodzenia i naprowadzania uzbrojenia. 3. Inne.	W czasie prowadzenia działań obronnych. Z chwilą pojawienia się zagrożenia.	Stałe sprawdzanie tożsamości korespondentów. Ścisłe przestrzeganie zasad eksploatacji systemów dowodzenia i naprowadzania uzbrojenia.	Użytkownicy środków łączności i informatyki. Użytkownicy technicznych środków dowodzenia i naprowadzania uzbrojenia.	Wg harmonogramu. Wg harmonogramu.	
		Obrona informacyjna wojsk ZO przed zakłócaniem zagłuszającym	1. Rozpoznanie środków (systemów) zakłócania zagłuszającego przeciwnika. 2. Maskowanie pracy systemów dowodzenia i naprowadzania uzbrojenia sił głównych. 3. Niszczenie środków zakłócania zagłuszającego przeciwnika. 4. Przeciwdziałanie skutkom zakłócania zagłuszającego. 5. Inne.	W czasie prowadzenia działań obronnych. W czasie prowadzenia działań obronnych. Po wykryciu. Z chwilą pojawienia się zakłóceń.	Wg planu rozpoznania elektronicznego. Przedsięwzięcia organizacyjne i techniczne. WRiA, LWL, użytkownicy SE w odniesieniu do NZJU. Przedsięwzięcia techniczno-eksploatacyjne.	Siły i środki rozpoznania elektronicznego .....ZO. Specjaliści rodzajów wojsk i służb. Specjaliści rodzajów wojsk i służb. Użytkownicy systemów elektronicznych.	Wg harmonogramu. Wg harmonogramu. Wg harmonogramu. Wg harmonogramu.	

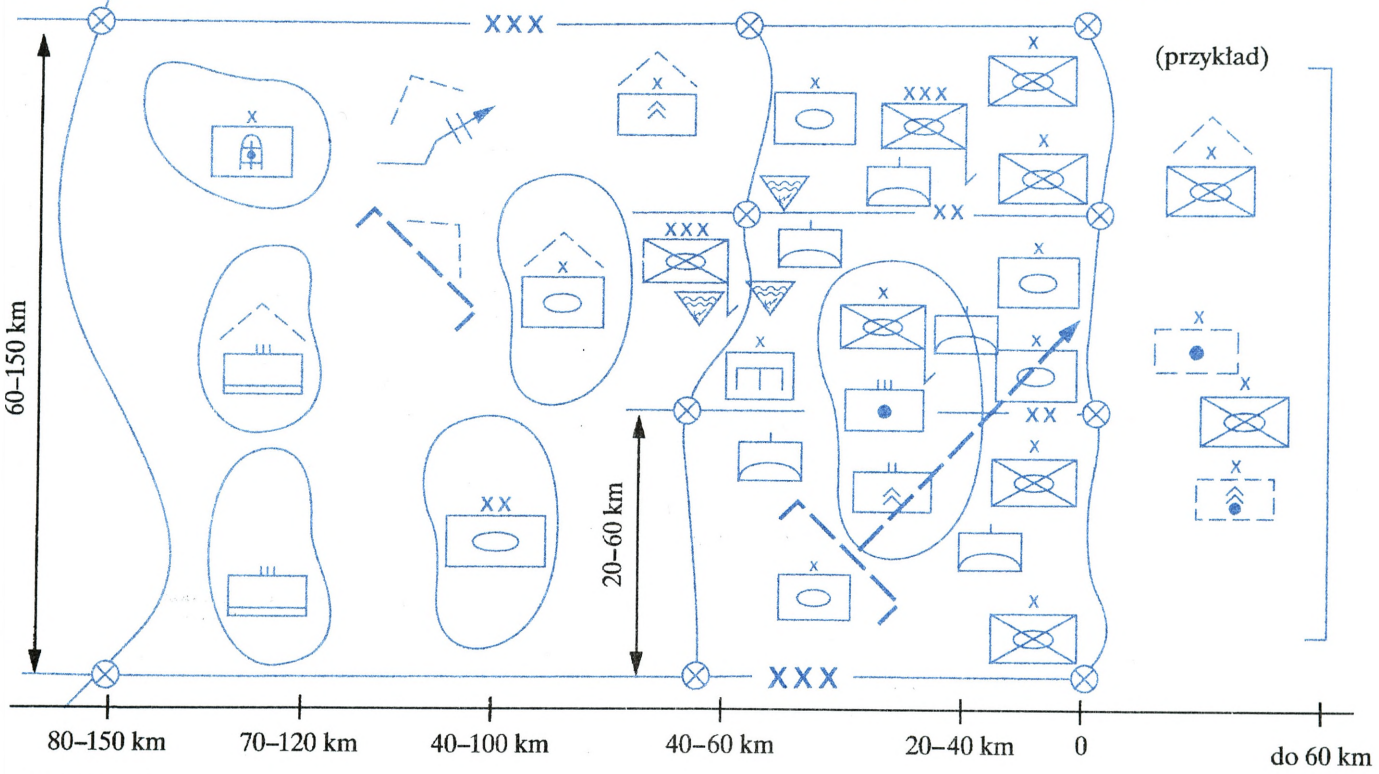
		Obrona informacyjna wojsk ZO przed oddziaływaniem niszczącym	Zapewnienie żywotności komponentów systemów dowodzenia i naprowadzania uzbrojenia.	W toku działań obronnych.	Przedsięwzięcia aktywne i pasywne.	Dowódcy wszystkich szczebli dowodzenia.	Wg harmonogramu.	
		Zabezpieczenie systemów dowodzenia i naprowadzania uzbrojenia ZO przed niekompatybilnością EM	Zapewnienie prawidłowej koegzystencji systemów dowodzenia i naprowadzania uzbrojenia w środowisku elektromagnetycznym.	Z chwilą pojawienia się zakłóceń interferencyjnych.	Przedsięwzięcia organizacyjne i techniczne.	Użytkownicy systemów elektronicznych.	Wg harmonogramu.	
IV. Podczas wzbronienia zgrupowaniom uderzeniowym przeciwnika rozwinięcia powodzenia								
	.....	.....	.....	.....	.....	.....	.....	.....
	.....	.....	.....	.....	.....	.....	.....	.....
Inne etapy – wg potrzeb								
	.....	.....	.....	.....	.....	.....	.....	.....
	.....	.....	.....	.....	.....	.....	.....	.....

mjr Z. Rydwan

Załączniki:

1. Plan pozorowania – oleat (mapa, szkic) – [załącznik 25.],
2. Wykaz wiadomości dezinformujących (mylących),
3. Podział sił – zgodnie z aneksem A (podział sił) do rozkazu operacyjnego ....ZO).
4. Harmonogram kontroli realizacji zadań obrony informacyjnej,
5. Inne – wg potrzeb.

OLEAT PLANU POZOROWANIA W DZIAŁANIACH OBRONNYCH ....ZO



LEGENDA:

– w połączeniu ze znakiem podstawowym oznacza obiekt pozorowany

Załącznik 26

Informacje umieszczane tylko w wypadku przesłania aneksu osobno poza rozkazem[1]	**Numer kopii:** Wydający rozkaz: Miejsce wydania: Grupa data-czas: Nr wychodzący:	Egz. ... z .... (.....) .....

ANEKS N – OBRONA INFORMACYJNA – DO ROZKAZU OPERACYJNEGO Nr...

Dokumenty odniesienia: *stosowne dokumenty (pisemne i graficzne)*

(Mapa 1: ..., godła ..., wydanie ...)

(Komunikat rozpoznawczy nr ...)

Strefa czasowa: *właściwa dla rozkazu (dla obszaru Polski – ALFA).*

1. SYTUACJA

a. Siły przeciwnika

(1) Siły główne – *odesłanie do: Aneks B (rozpoznanie) do planu działania .....ZO.*

(2) Systemy walki informacyjnej przeciwnika - *uogólniona charakterystyka wykorzystywanych przez przeciwnika systemów rozpoznania i zakłócania przeciwnika.*

(3) Przewidywane przedsięwzięcia przeciwnika – *przedsięwzięcia z zakresu walki informacyjnej jakie może zastosować przeciwnik w operacji.*

(4) Spodziewane nowe systemy i środki walki informacyjnej – *krótka charakterystyka użycia nowych systemów walki informacyjnej w toku prowadzonych działań.*

(5) Przewidywana taktyka użycia środków walki informacyjnej przez przeciwnika.

[1] Legenda:
Jeżeli aneks jest wysyłany oddzielnie od rozkazu, musi być opisany tak jak rozkaz (strona tytułowa, podpis, rozdzielnik). Natomiast w sytuacji gdy jest on integralną częścią rozkazu i jest rozprowadzany według tego samego rozdzielnika, wystarczy sam tytuł dokumentu – wówczas na początku aneksu nie umieszcza się tekstu zaznaczonego ramkami.

b. Wojska własne

Przedsięwzięcia obrony informacyjnej realizowane przez przełożonego – *wymienia się, jakie przedsięwzięcia z zakresu obrony informacyjnej realizował będzie przełożony na kierunku działania związku operacyjnego.*

(1) Wsparcie sił powietrznych w zakresie obrony informacyjnej – *wymienia się, jakie przedsięwzięcia z zakresu obrony informacyjnej realizowane będą przez inne rodzaje sił zbrojnych – lotnictwo, siły morskie.*

(2) Przedsięwzięcia sąsiadów – *przedsięwzięcia w zakresie obrony informacyjnej realizowane przez sąsiadów.*

(3) Przydział wzmocnienie – *wymienia się, jakie siły i środki na potrzeby obrony informacyjnej wydziela (przydziela) się, jakie podporządkowuje się czasowo.*

c. Zmiany w podporządkowaniu

Podział sił – odnośnik do aneksu A. W razie potrzeby określa się od kiedy obowiązują ewentualne zmiany w podporządkowaniu.

2. ZADANIA W ZAKRESIE OBRONY INFORMACYJNEJ

Zadania z zakresu obrony informacyjnej (przed rozpoznaniem i zakłócaniem) realizowane w działaniach obronnych ....ZO.

3. REALIZACJA

a. Koncepcja działania (myśl przewodnia) w zakresie obrony informacyjnej.

Określenie głównego wysiłku obrony informacyjnej w działaniach obronnych związku operacyjnego.

b. Zadania dla elementów ugrupowania obronnego

W kolejnych podpunktach stawiane są zadania z zakresu obrony informacyjnej dla poszczególnych elementów ugrupowania obronnego w poszczególnych ich etapach (w kolejności, w jakiej są wymienione w rozkazie operacyjnym), przewidziane zarówno do działań bojowych, jak i pozornych.

c. Wytyczne koordynujące

Wyszczególnienie informacji dotyczących dwóch i więcej elementów ugrupowania bojowego i podanie niezbędnych współrzędnych, linii koordynacyjnych. Terminy, czasy i sposoby współdziałania z rodzajami wojsk i służb. Czasy gotowości do działań – mogą być powtórzone. Inne dane.

4. ZABEZPIECZENIE LOGISTYCZNE

a. Zaopatrywanie w środki maskowania

Odwołanie do aneksu „Plan zabezpieczenia logistycznego".

b. Zabezpieczenie techniczne środków pozorowania

Odwołanie do aneksu „Plan zabezpieczenia logistycznego".

c. Uzupełnianie

Odwołanie do aneksu „Plan zabezpieczenia logistycznego".

5. DOWODZENIE I ŁĄCZNOŚĆ

a. Dowodzenie

Rozmieszczenie wysuniętego i głównego SD, własnego i przełożonego oraz jednostek współdziałających. Ich kolejne miejsca rozwinięcia.

b. Łączność

Odesłanie do aneksu łączność Aneks L (łączność i informatyka) do planu działania.

6. INNE DANE

Opracowywane według ustaleń i potrzeb G 2 (może zawierać wszystkie nie ujęte w sposób sformalizowany treści aneksu).

.....

[podpis dowódcy]
[nazwisko dowódcy]
[stopień dowódcy]

ZA ZGODNOŚĆ:

(podpisuje upoważniony przez dowódcę oficer, w miejscu podpisu dowódcy umieszcza się stopień i nazwisko).

[stopień, nazwisko]

APENDYKSY:

1. Prognoza zagrożeń w wymiarze informacyjnym;
2. Wnioski z oceny wojsk związku operacyjnego w zakresie obrony informacyjnej;
3. Tabelaryczny plan koordynacji przedsięwzięć w zakresie obrony informacyjnej;
4. Plan obrony informacyjnej w działaniach obronnych ...ZO;
5. Rejony i częstotliwości zastrzeżone;
6. Dokumenty normatywne z zakresu bezpieczeństwa informacyjnego i in;
7. Inne –wg potrzeb.

Rozdzielnik:

Zewnętrzny	Egz. nr ....
Do realizacji:	
1 DZ	1
.....	...
.....	...
.....	...
a/a	...
kancelaria	...

BIBLIOTEKA GŁÓWNA - ARCHIWUM
Akademii Obrony Narodowej
Nr ewid. 54385

PUBLIKACJE AKADEMII OBRONY NARODOWEJ

do nabycia w Wydziale Wydawniczym AON
al. gen. A. Chruściela 103, bl. 2
00-910 Warszawa, tel./faks 681 37 52

- H. Binkowski, A. Ciupiński – **Polityka obronna i siły zbrojne partnerów Polski z Grupy Wyszehradzkiej**
- R. Bojarski – **Operacja obronna**
- R. Bojarski – **Główne problemy działań operacyjnych**
- J. Brzozowski – **Metodyka zajęć grupowych**
- A. Ciupiński, R. Białoskórski – **Wczesne ostrzeganie i zapobieganie współczesnym konfliktom zbrojnym w strategii Sojuszu Północnoatlantyckiego**
- J. Czaja – **Stolica apostolska wobec integracji europejskiej**
- A. Dawidczyk – **Nowe wyzwania, zagrożenia i szanse dla bezpieczeństwa Polski u progu XXI w.**
- W. Drążczyk – **Logistyka sił powietrznych w działaniach wielonarodowych**
- **Działania (operacje) połączone.** Materiały z konferencji naukowej
- M. Gąska, A. Ciupiński – **Międzynarodowe prawo humanitarne**
- M. Gąska – **Obronność w aktach prawnych RP**
- J. Gotowała – **Lotnictwo XXI wieku**
- J. Groskrejc – **Antropologiczne i aksjologiczne aspekty edukacji oficerów**
- J. Groskrejc – **Nauczyciel w edukacji. Funkcje – kompetencje – koncepcje kształcenia**
- J. Halik – **Metodyka opracowania pracy magisterskiej i studyjnej**
- H. Herman – **Działania specjalne w wojnach i konfliktach zbrojnych po II wojnie światowej**
- M. Huzarski (red.) – **Taktyka ogólna wojsk lądowych**
- K. Jałoszyński – **Terroryzm antyizraelski**
- K. Jałoszyński – **Terroryzm czy terror kryminalny w Polsce?**
- K. Jałoszyński – **Zagrożenie terroryzmem w wybranych krajach Europy Zachodniej oraz w Stanach Zjednoczonych**
- J. Janczak – **Zakłócanie informacyjne**
- T. Jemioło – **Globalizacja. Szanse i zagrożenia**
- J. Kardas, K. Loranty – **Wybrane problemy bezpieczeństwa i obronności państwa w opiniach pracowników administracji publicznej**
- J. Kardas – **Edukacja kadr administracji publicznej na Wyższych Kursach Obronnych**
- W. Kitler (red.) – **Obrona cywilna (niemilitarna) w obronie narodowej III RP**
- W. Kitler – **Obrona narodowa w wybranych państwach demokratycznych**
- Z. Klawitter – **Wybrane aspekty systemu dowodzenia brygady zmechanizowanej (pancernej) w działaniach taktycznych**
- S. Korzeniowski – **Żandarmeria wojskowa**
- M. Koziński – **Umowa offsetowa i inne formy udziału państwa w międzynarodowym obrocie gospodarczym**
- M. Kozub – **Lotnictwo w operacjach połączonych**
- S. Kurinia – **Współczesna brytyjska myśl obronno-ekonomiczna**
- R. Kwećka – **Informacja w walce zbrojnej**
- Z. Lach, J. Skrzyp, A. Łaszczuk – **Wojskowo-geograficzna charakterystyka Niemiec**
- L. Łukaszuk – **Europejskie prawo pokoju i bezpieczeństwa**
- J. Marczak (red.) – **Samoorganizacja społeczeństwa na rzecz bezpieczeństwa powszechnego. Samoobrona powszechna III RP**
- Z. Maślak, K. Kozłowski, P. Krawczyk – **Podstawy użycia lotnictwa myśliwskiego**
- W. Michalak – **Dominacja z powietrza**
- G. Nowacki – **Strategiczne siły jądrowe wybranych państw**
- I. Nowak – **Wybrane problemy historii polskiej techniki wojskowej XX wieku. Sprzęt i środki wojsk chemicznych**
- M. Obrusiewicz – **Wielonarodowe połączone siły zadaniowe CJTF**
- J. Pawłowski, A. Ciupiński (red.) – **Umiędzynarodowiony konflikt wewnętrzny**
- J. Płaczek – **Ewolucja polskiej myśli obronno-ekonomicznej w latach 1976–2000**
- J. Płaczek (red.) – **Gospodarka obronna Polski w końcu lat dziewięćdziesiątych. Szanse i zagrożenia**
- K. Przeworski – **Ewakuacja jako sposób ochrony ludności**
- A. Radomyski – **Zagrożenie śmigłowcowe dywizji zmechanizowanej**
- A. Rejmak – **Ratownictwo lotnicze**
- S. Sadowski – **Podstawowe zagadnienia teorii walki zbrojnej**
- P. Sienkiewicz – **5 wykładów**
- A. Skrabacz – **Kobiety w obronie narodowej Polski u progu XXI w.**

- Z. Skwarek – **Powietrzne systemy wczesnego wykrywania i powiadamiania**
- K. Słaboń – **Sytuacja jeńców wojennych w konflikcie iracko-irańskim (1980–1988)**
- J. Słowik – **Dowodzenie brygadą zmechanizowaną (pancerną) w natarciu**
- **Słownik terminów z zakresu psychologii** (praca zbiorowa)
- M. Sołoducha, P. Malinowski – **Użycie artylerii w szczególnych rodzajach działań bojowych**
- H. Spustek – **Wybrane zagadnienia badań operacyjnych i modelowania liniowego**
- Z. Stachowiak – **Metodyka i metodologia pisania prac kwalifikacyjnych (licencjackich, magisterskich i podyplomowych)**
- R. Stępień (red.) – **Edukacja w wyższych szkołach wojskowych**
- M. Strzoda, N. Prusiński – **System dowodzenia. Terminologia. Część I**
- R. Szpyra – **Powietrzna sztuka operacyjna wybranych państw**
- E.A. Wesołowska, A. Szerauc (red.) – **Patriotyzm – Obronność – Bezpieczeństwo**
- J. Wołejszo, Z. Fiołna – **Dowodzenie brygadą zmechanizowaną (pancerną) w obronie**
- J. Wojtasik (red.) – **Studia z dziejów polskiej techniki wojskowej od XVI do XX wieku**
- W. Zawadzki, T. Majewski, N. Prusiński – **Informacyjne uwarunkowania procesu decyzyjnego**
- J. Zieliński (red.) – **Podstawowe założenia dydaktyki sztuki operacyjnej**
- J. Zuziak – **Dzieje Instytutu Józefa Piłsudskiego w Londynie 1947–1997**

Zamówienia przyjmujemy telefonicznie lub pisemnie