R G B WH GR BL Grey Scale #13 C M Y K
A 1 2 3 4 5 6 M 8 9 10 11 12 13 14 15 B 17 18 19

Colour Chart #13
Inches Centimetres
Blue Cyan Green Yellow Red Magenta White 3/Color Black

AKADEMIA
OBRONY NARODOWEJ

AON 5210/2000

WALKA ELEKTRONICZNA W DZIAŁANIACH TAKTYCZNYCH ZWIĄZKU TAKTYCZNEGO

Praca studyjna

BIBLIOTEKA GŁÓWNA AKADEMII Akademii Obrony Narodowej
Nr ewid. II
52515

WARSZAWA 2000

AKADEMIA OBRONY NARODOWEJ

WYDZIAŁ WOJSK LĄDOWYCH

AON 5210/2000

WALKA ELEKTRONICZNA W DZIAŁANIACH TAKTYCZNYCH ZWIĄZKU TAKTYCZNEGO

Praca studyjna

BIBLIOTEKA GŁÓWNA - ARCHIWUM
Nr ewid. 52515
II
Akademii Obrony Narodowej

WARSZAWA **2000**

Opracował zespół autorów w składzie:

płk dr inż. Józef JANCZAK - kierownik
płk dr inż. Bogdan BEZOŃ
ppłk dr inż. Gabriel NOWACKI
mjr dypl. inż. Waldemar SCHEFFS
mjr mgr inż. Wiesław BŁAŻEJCZYK

Redaktor
mgr Teresa PIĄTEK

Redaktor techniczny
Beata KLAROWSKA

Korekta
Kazimiera KRZEŚNIAK
Jolanta PUCHALSKA

Skład, druk i oprawa
Akademia Obrony Narodowej – Wydział Wydawniczy
Zam. nr 775/99

SPIS TREŚCI

WSTĘP 5

1. ISTOTA WALKI ELEKTRONICZNEJ W DZIAŁANIACH TAKTYCZNYCH ZWIĄZKU TAKTYCZNEGO 6

1.1. Rola i miejsce WE w działaniach taktycznych 6

1.2. Podstawowe zasady WE 10

2. ROZPOZNANIE ELEKTRONICZNE 13

2.1. Istota rozpoznania elektronicznego 13

2.2. Rozpoznanie radioelektroniczne 15

2.2.1. Rozpoznanie radiowe 19

2.2.2. Rozpoznanie systemów radiolokacyjnych 21

2.2.3. Rozpoznanie systemów radionawigacyjnych 32

2.3. Rozpoznanie radiolokacyjne 33

2.4. Rozpoznanie optoelektroniczne 39

2.5. Rozpoznanie czujnikowe 40

2.6. Rozpoznanie informatyczne 40

3. ZAKŁÓCANIE ELEKTRONICZNE 42

3.1. Istota zakłócania elektronicznego 42

3.2. Aktywne zakłócenia elektroniczne 43

3.3. Pasywne zakłócenia elektroniczne 45

3.4. Zagłuszanie elektroniczne 47

3.5. Pozorowanie elektroniczne 52

3.6. Neutralizacja 53

3.7. Znaczenie zakłócania elektronicznego 54

4. OBRONA ELEKTRONICZNA 56

4.1. Istota obrony elektronicznej 56

4.2. Obrona przed rozpoznaniem i zakłócaniem elektronicznym 57

4.3. Obrona przed niszczeniem ogniowym oraz bronią naprowadzającą się na źródła promieniowania energii elektromagnetycznej 62

4.4. Zabezpieczenie przed niekompatybilnością elektromagnetyczną 63

4.5. Kontrola elektroniczna 66

5. PRZYGOTOWANIE WALKI ELEKTRONICZNEJ W DZIAŁANIACH TAKTYCZNYCH ZWIĄZKU TAKTYCZNEGO 68

5.1. Założenia ogólne 68

5.2. Ustalenie położenia sił i środków elektronicznych 69

5.3. Planowanie walki elektronicznej w działaniach taktycznych 69

5.3.1. Ocena sytuacji elektronicznej w działaniach taktycznych 73

5.3.2. Ocena terenu 74

5.3.3. Analiza dróg podejścia 77

5.3.4. Prognoza pogody 79

5.3.5. Prognoza zagrożenia elektronicznego 81

5.3.6. Oleat zdarzeń elektronicznych 87

5.3.7. Oleat elektronicznego wzorca wsparcia decyzji 88

5.3.8. Opracowanie koncepcji walki elektronicznej w działaniach taktycznych 90

5.4. Stawianie zadań w zakresie walki elektronicznej w działaniach taktycznych 92

5.4.1. Aneks „Walka elektroniczna" 92

5.4.2. Zarządzenie przygotowawcze 97

6. PROWADZENIE WALKI ELEKTRONICZNEJ W DZIAŁANIACH TAKTYCZNYCH ZWIĄZKU TAKTYCZNEGO 98
6.1. Cel walki elektronicznej w działaniach taktycznych 98
6.2. Zadania walki elektronicznej w działaniach taktycznych 99
6.3. Ugrupowanie bojowe środków walki elektronicznej w działaniach taktycznych 102
6.3.1. Struktura pododdziału WE 103
6.3.2. Elementy ugrupowania bojowego 103
6.3.3. Ugrupowanie pododdziału WE w działaniach obronnych 105
6.3.4. Ugrupowanie bojowe pododdziału WE w natarciu 106
6.3.5. Ugrupowanie bojowe pododdziału WE w działaniach opóźniających 107
6.3.6. Wybór i zajmowanie pozycji bojowych 108
6.3.7. Zmiana ugrupowania 108
6.4. Prowadzenie działań bojowych przez pododdział walki elektronicznej 109
6.4.1. Praca bojowa elementów pododdziału walki elektronicznej 109
6.4.2. Opracowywanie danych z rozpoznania elektronicznego 113
6.4.3. Łączność w pododdziale WE 114
ZAKOŃCZENIE 116
LITERATURA 118
ZAŁĄCZNIKI 119

WSTĘP

We współczesnych działaniach taktycznych o sukcesie wojsk w coraz większym stopniu decyduje elektronika. Jej znaczenie nieustannie wzrasta, a dalszy jej rozwój będzie miał duży wpływ na unowocześnianie środków walki oraz na charakter, przebieg i rezultat prowadzonych działań wojennych.

Środki i urządzenia elektroniczne są powszechnie wykorzystywane w dowodzeniu wojskami, kierowaniu środkami walki oraz nawigacji powietrznej i morskiej. Są bowiem głównymi elementami systemów dowodzenia wojskami, rozpoznania oraz naprowadzania najnowszej generacji systemów i środków rażenia. Nasycenie nimi pola walki gwałtownie się zwiększa. W nowoczesnych armiach każdy środek walki lub pojedynczy żołnierz ma co najmniej jeden-dwa środki elektroniczne. Środki te stają się niezbędne na współczesnym polu walki, a ich umiejętne wykorzystanie może zdecydować o powodzeniu w działaniach.

Minione wojny i konflikty lokalne wykazały, że w przypadkach gdy urządzenia elektroniczne decydowały o efektywności użycia środków walki i działania wojsk, w sferze zainteresowania walczących stron znalazły się możliwości oddziaływania na nie w celu obniżenia ich sprawności.

Dezorganizowanie obiegu danych, opóźnianie lub uniemożliwianie stawiania zadań, zbierania meldunków, powiadamiania, paraliż systemu rozpoznania i dowodzenia mogą osiągnąć taki stopień, że użycie wojsk i środków walki może stać się nieskuteczne lub wręcz niemożliwe. Oddziałując bezpośrednio na urządzenia oraz systemy elektroniczne, każda z walczących stron stara się bowiem zmniejszyć zdolność bojową strony przeciwnej i efektywność wykorzystywanego przez nią uzbrojenia, a tym samym wpływać na obniżenie skuteczności działania. Z tego też powodu poszukuje się jak najlepszych rozwiązań organizacyjnych i technicznych, mających na celu zabezpieczenie własnych środków elektronicznych przed oddziaływaniem coraz doskonalszych środków walki elektronicznej strony przeciwnej. Jest to jedna z ważniejszych płaszczyzn trwającego we współczesnych armiach wyścigu technologicznego. Ten, kto go wygra, zapewni sobie przewagę na przyszłym polu walki.

Podczas organizowania i prowadzenia działań taktycznych wojsk lądowych, należy pamiętać o tym, że istnieje możliwość dezorganizowania normalnego funkcjonowania każdego czynnego systemu elektronicznego. Ze względu na masowość wykorzystania środków elektronicznych na tym szczeblu i ograniczoność obszaru elektromagnetycznego może mieć zasadniczy wpływ na przebieg i rezultaty prowadzonych działań. Zwłaszcza, że uderzenia ogniowe z reguły poprzedzane są masowym użyciem środków rozpoznania i zakłócania elektronicznego, które niekiedy przyjmuje formę *natarcia elektronicznego*. Uwarunkowania te charakteryzują współczesne działania taktyczne.

1. ISTOTA WALKI ELEKTRONICZNEJ W DZIAŁANIACH TAKTYCZNYCH ZWIĄZKU TAKTYCZNEGO

1.1. Rola i miejsce walki elektronicznej w działaniach taktycznych

Wstąpienie Polski w struktury NATO oraz podejmowanie przez Siły Zbrojne RP coraz liczniejszych międzynarodowych misji pokojowych ONZ obliguje do zapewnienia ich interoperacyjności w wielu dziedzinach. Analiza poglądów obowiązujących w Sojuszu oraz dotychczasowego dorobku naszych teoretyków wojskowych stała się podstawą zdefiniowania pojęcia „walka elektroniczna" (WE)[1].

Walka elektroniczna (WE) – to przedsięwzięcia i działania wojsk, które wykorzystując energię elektromagnetyczną (EM), rozpoznają i dezorganizują systemy elektroniczne przeciwnika oraz zapewniają warunki do stabilnej pracy analogicznym systemom własnych wojsk.

Walka elektroniczna jest więc zamierzonym działaniem wojskowym, polegającym na wykrywaniu i identyfikacji emisji elektromagnetycznych oraz zastosowaniu energii elektromagnetycznej do zmniejszenia skuteczności lub uniemożliwienia użycia przez przeciwnika widma elektromagnetycznego i zapewnienia efektywnego jego wykorzystania przez siły własne.

Działanie to prowadzone jest na specyficznym elektronicznym polu walki, które obejmuje środki elektroniczne promieniujące i odbierające energię elektromagnetyczną w odpowiednim środowisku elektromagnetycznym[2]. Główne obszary elektronicznego pola walki przedstawione zostały na rysunku 1.

Na elektroniczne pole walki ma wpływ *działalność organizacyjna, działalność ogniowa i przede wszystkim działalność elektromagnetyczna zamierzona i niezamierzona,* zarówno własnych sił jak i przeciwnika, wyposażonych w odpowiednie środki i systemy elektroniczne.

Drgania sejsmiczne	Fonia	Radio	Radar	Podczerwień	Światło widzialne	Ultra--fiolet	Promienie X	Promienie kosmiczne

Rys. 1. Główne obszary elektronicznego pola walki

[1] Po raz pierwszy pojęcia „walka elektroniczna" w odniesieniu do SZ RP użyto w *Regulaminie działań WL,* AON, Warszawa 1998.

[2] Środowisko elektromagnetyczne jest często określane w literaturze fachowej [9, 15, 22] jako „przestrzeń elektromagnetyczna", „spektrum EM" lub „eter". Korzystanie ze środowiska elektromagnetycznego jest możliwe dzięki urządzeniom promieniującym energię EM i urządzeniom odbierającym w różnych zakresach częstotliwości. Współdziałanie między tymi urządzeniami jest możliwe wówczas, gdy pracują one na tej samej częstotliwości i tym samym rodzajem modulacji, a warunki rozprzestrzeniania pozwalają urządzeniom odbiorczym na kontakt energetyczny z urządzeniami nadawczymi. Do środków elektronicznych, które odpowiadają tym kryteriom, można zaliczyć następujące: łączności radiowej, rozpoznania radiolokacyjnego i optoelektronicznego, radionawigacyjne, czujnikowe oraz sterowania uzbrojeniem, radiozapalniki, identyfikacji celów oraz rozpoznania i zakłócania elektronicznego (systemy WE), a także systemy niszczenia (lasery mocy, generatory impulsu elektromagnetycznego oraz środki wypromieniowujące spójną wiązkę mikrofalową, czyli masery).

Działalność organizacyjna decyduje o sposobach wykorzystania urządzeń elektronicznych, ich powiązaniach, sposobie rozmieszczenia w ugrupowaniu bojowym, czasie wykorzystania itp.

Działalność ogniowa z kolei pozwala na niszczenie urządzeń elektronicznych, tym samym zmniejszenie ich liczby u przeciwnika. Ponieważ za pomocą środków ogniowych likwiduje się najważniejsze ogniwa systemów elektronicznych, które często są trudne do odtworzenia, to działalność ta ma duży wpływ na obszar WE i skutecznie ją wspiera.

Działalność elektromagnetyczna jest związana z przechwytywaniem energii EM i zakłócaniem urządzeń odbiorczych przeciwnika. Intensywność oddziaływania w obszarze EM zależy od intensywności pracy urządzeń elektronicznych przeciwnika promieniujących i odbierających energię elektromagnetyczną, posiadanego własnego potencjału WE oraz przyjętej taktyki działania.

Na podstawie definicji walki elektronicznej można przyjąć, że *walka ta ma dwa charakterystyczne, niezależne od siebie nurty:*

1. Ofensywny – to aktywne oddziaływanie na środki elektroniczne przeciwnika przez rozpoznanie ich w obszarze elektromagnetycznym oraz ich zakłócanie elektroniczne.

2. Defensywny – to stworzenie warunków dla własnych środków elektronicznych, aby mogły pracować i w niezakłócony sposób spełniać wyznaczoną dla nich rolę na polu walki.

Istotą *pierwszego nurtu* jest uzyskanie danych o pracujących środkach elektronicznych przeciwnika przez przechwytywanie fal elektromagnetycznych emitowanych przez jego urządzenia nadawcze oraz ustalenie na podstawie kierunku przychodzenia i analizy sygnałów możliwości ich zakłócenia lub rażenia środkami ogniowymi. Uzyskane dane mogą być także wykorzystywane do kierowania walką ogólnowojskową.

Innym działaniem może być blokowanie możliwości zbierania danych przez urządzenia elektroniczne przeciwnika (zwłaszcza radiolokacyjne), blokowanie przepływu danych w środkach łączności bezprzewodowej, zakłócanie funkcjonowania urządzeń radionawigacyjnych i urządzeń sterowania środkami walki (w tym głównie ogniowymi), powodowanie przedwczesnego lub spóźnionego zadziałania zapalników radiowych oraz fizyczne uszkadzanie urządzeń elektronicznych.

Ponieważ prowadzenie WE odbywa się w środowisku elektromagnetycznym, więc realizowanie tych zadań będzie polegało na przechwytywaniu energii wypromieniowywanej przez nadawcze urządzenia elektroniczne przeciwnika oraz na oddziaływaniu energią zakłócającą na jego urządzenia odbiorcze. Oddziaływanie energią elektromagnetyczną może przyjmować formę zakłócania elektronicznego, polegającą na uniemożliwianiu odbioru sygnałów użytecznych, oraz formę niszczącą, polegającą na fizycznej destrukcji podzespołów elektronicznych silnymi impulsami EM, promieniowaniem mikrofalowym lub spójnym strumieniem energii EM z laserów i maserów.

Istotą *drugiego nurtu* jest zapewnienie własnym systemom elektronicznym warunków do niezakłóconej pracy i tym samym zabezpieczenie procesu zbierania i dystrybucji danych. Zadania z zakresu obrony elektronicznej są wielokierunkowe, realizowane z korzyścią dla wła-

snych środków elektronicznych i zespołów obsługujących te środki. Celowo jest dzielić je na organizacyjne (tj. takie, które umożliwiają optymalne wykorzystanie posiadanych środków elektronicznych) oraz techniczne (tj. konstruowanie urządzeń elektronicznych zdolnych do pracy w warunkach prowadzenia WE przez przeciwnika).

Przebieg lokalnych wojen i konfliktów zbrojnych dowodzi, że rola i znaczenie WE na współczesnym polu walki są bezdyskusyjne, a działania podejmowane w tym zakresie wpływają na realizację zadań przez inne rodzaje wojsk. Zaliczyć do nich można ograniczenie dopływu danych rozpoznawczych, przerwy lub ich opóźnienia w czasie realizacji zadań, pogorszenie dokładności oraz wprowadzenie fałszywych danych. Walka elektroniczna wpływa głównie na skuteczność wykorzystywanych środków ogniowych oraz na sposób i czas dokonywanego w walce manewru siłami i środkami.

Ograniczenie lub przerwa w przepływie danych w środkach łączności zwiększają czas lub powodują brak reakcji na zachodzące zmiany w walce, ograniczają lub wydłużają czas stawiania zadań przez środki łączności.

Zakłócenie urządzeń radionawigacyjnych i sterowania powoduje utrudnienia w dotarciu środka ogniowego do wyznaczonego celu, zwiększenie błędu trafienia, detonacje ładunków w nieprzewidzianym miejscu i czasie lub niezrealizowanie wyznaczonego zadania. Przy współczesnych środkach walki takie działanie znacząco zmniejsza efektywność wykorzystania ich walorów technicznych.

Podobne zależności obserwuje się między obroną elektroniczną a działaniem wojsk własnych. Przy braku skuteczności *systemów rozpoznania elektronicznego* i ogniowych środków obrony powietrznej zwiększają się możliwości działania środków napadu powietrznego przeciwnika. Zjawisko to potęguje straty w systemach OP i lotnictwa, co jeszcze bardziej obniża potencjał ogniowy i wpływa na wzrost zagrożenia wojsk lądowych uderzeniami z powietrza.

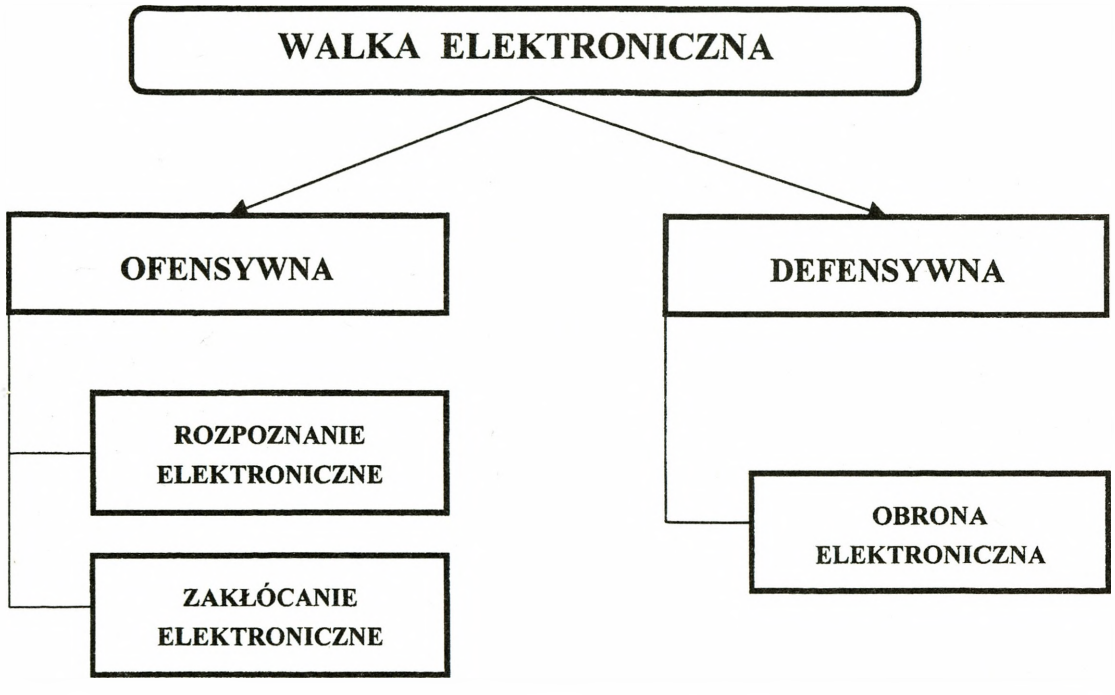
Utrudnienia transmisji danych w systemie łączności opóźniają zbieranie wiadomości rozpoznawczych, stawianie zadań, zbieranie meldunków, ostrzeganie i alarmowanie. W wyniku tych trudności wojska stają się mniej manewrowe, przeciwnik natomiast uprzedza je uderzeniami ogniowymi i manewrem.

Brak wystarczającej obrony elektronicznej systemów radionawigacyjnych i sterowania ogranicza możliwości lub czyni nieskutecznymi nowoczesne środki ogniowe. Prowadzi to z kolei do zwiększonego zużycia środków walki.

Należy dostrzegać również *zależności występujące między elementami WE*, które decydują o efektywności jej prowadzenia. Spośród nich za najważniejszą uznaje się zależność między *środkami rozpoznania elektronicznego a efektywnością środków zakłócania elektronicznego*. Aby w jakikolwiek sposób przeciwdziałać pracującym środkom elektronicznym przeciwnika, należy najpierw je wykryć, następnie określić charakter i wreszcie ustalić niektóre parametry. Względy te dyktują potrzebę ścisłego powiązania środków i systemów rozpoznania elektronicznego z siłami i środkami zakłócania elektronicznego oraz sprawnych systemów łączności, służących do transmisji danych między nimi.

Nie ulega wątpliwości, że walka elektroniczna jest częścią walki ogólnowojskowej. Wymaga ona zatem kompleksowego i systematycznego rozpatrywania, *ścisłego koordynowania i łączenia działalności elektronicznej z uderzeniami wojsk, uderzeniami wojsk rakietowych i artylerii oraz uderzeniami lotnictwa.* Wymaga także wyjątkowo wysokiej taktycznej i technicznej umiejętności określania newralgicznych miejsc w systemach dowodzenia wojskami, kierowania środkami walki, rozpoznania i walki elektronicznej przeciwnika przy równoczesnych niezawodnych i prostych sposobach działania oraz umiejętnym wykorzystaniu środków elektronicznych.

Walka elektroniczna jest w swej istocie przede wszystkim walką o informację, jest więc elementem składowym walki informacyjnej[3]. Polega na prowadzeniu rozpoznania elektronicznego, zakłócania systemów i środków elektronicznych przeciwnika w powiązaniu z ich rażeniem ogniowym oraz na obronie elektronicznej własnych systemów. Zasadnicze zadania, jakie we współczesnych działaniach taktycznych są podejmowane w zakresie zwalczania i obrony środków i systemów elektronicznych, sprawiają, że walka elektroniczna stanowi szeroko rozbudowany system. Ze względu na zakres działania jest podzielona na określone części składowe*: rozpoznanie elektroniczne, zakłócanie elektroniczne oraz obronę elektroniczną* (rysunek 2).



Rys. 2. Podział walki elektronicznej

[3] Walka informacyjna to kooperacja negatywna wzajemna, realizowana w sferach: zdobywania informacji (rozpoznania), zakłócania informacyjnego i obrony informacyjnej.

Rozpoznanie elektroniczne polega na zdobywaniu i przetwarzaniu danych o przeciwniku, których nośnikami są fale elektromagnetyczne oraz inne efekty towarzyszące działaniom bojowym. Współczesne rozpoznanie elektroniczne obejmuje: rozpoznanie radioelektroniczne, radiolokacyjne, optoelektroniczne, czujnikowe i informatyczne.

Rozpoznanie elektroniczne w działaniach wojsk lądowych jest prowadzone w celu wykrycia bezpośredniego zagrożenia elektronicznego i niezwłocznego przeciwdziałania mu w każdej sytuacji pola walki. Dane uzyskane w wyniku prowadzonego rozpoznania elektronicznego dotyczą parametrów technicznych emisji oraz położenia i działalności bojowej środków elektronicznych przeciwnika. Uzyskane tą drogą informacje o przeciwniku są wykorzystywane do realizacji przedsięwzięć zakłócania elektronicznego i obrony elektronicznej wojsk własnych, a także na potrzeby informacyjnego (rozpoznawczego) przygotowania pola walki.

Zakłócanie elektroniczne to zespół skoordynowanych przedsięwzięć i działań ukierunkowanych na dezorganizację procesów informacyjnych przeciwnika funkcjonujących w środowisku elektromagnetycznym. Zakłócanie elektroniczne obejmuje: zagłuszanie, pozorowanie i neutralizację. Przedsięwzięcia zakłócania elektronicznego powinny ograniczać efektywne wykorzystanie środowiska elektromagnetycznego przez przeciwnika i w ten sposób wykluczyć lub ograniczyć jego możliwości dowodzenia i użycia środków walki.

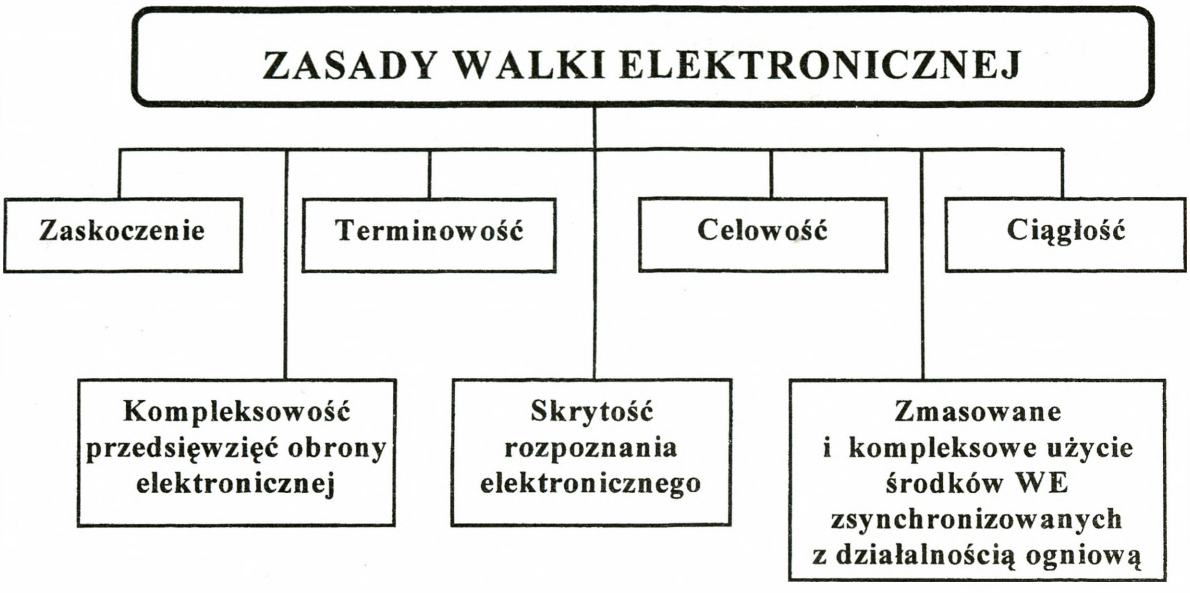
Zakłócanie elektroniczne może przyjmować formę rażenia lub uderzenia elektronicznego wyrażających zmasowane i kompleksowe użycie w określonym czasie i miejscu aktywnych środków WE w ścisłym powiązaniu z rażeniem ogniowym.

Obrona elektroniczna powinna stwarzać warunki do zachowania ciągłości dowodzenia własnymi siłami i środkami oraz żywotności wykorzystywanych środków i systemów elektronicznych. Obrona elektroniczna stanowi zespół przedsięwzięć organizacyjno-technicznych zapewniających stabilną pracę własnym systemom elektronicznym podczas prowadzonej przez przeciwnika WE oraz w warunkach wzajemnego oddziaływania środków elektronicznych wojsk własnych. Obejmuje ona obronę własnych systemów elektronicznych przed: rozpoznaniem i zakłócaniem elektronicznym przeciwnika, niszczeniem ogniowym bronią naprowadzającą się na źródła promieniowania elektromagnetycznego, a także zabezpieczenie przed niekompatybilnością elektromagnetyczną i kontrolę elektroniczną.

1.2. Podstawowe zasady WE

W walce elektronicznej obowiązują zasady i prawidłowości, które wynikają z praw i zasad walki zbrojnej. Określają one charakter tej walki na danym etapie rozwoju, jak również wymagania dotyczące racjonalnego i efektywnego wykorzystania posiadanego w wojskach potencjału elektronicznego, przeznaczonego do prowadzenia aktywnych i pasywnych działań elektronicznych.

Analiza literatury potwierdza, że zasady te modyfikowano w wyniku doświadczeń wojennych stosownie do zmian, jakie następowały w uzbrojeniu wojsk i w taktyce prowadzenia działań zbrojnych. Zasady współczesnej walki elektronicznej stanowią więc uogólnienie doświadczeń minionych wojen, przeprowadzonych ćwiczeń oraz doświadczeń poligonowych z wojskami. Najbardziej reprezentatywne zasady walki elektronicznej[4] przedstawione zostały na rysunku 3.



Rys. 3. Zasady walki elektronicznej

Walkę elektroniczną należy prowadzić we wszystkich rodzajach działań taktycznych wojsk lądowych. W określonym zakresie prowadzi się ją także w czasie pokoju. Pełną skuteczność WE można osiągnąć tylko pod warunkiem przygotowania już w okresie pokoju sztabów i wojsk oraz oddziałów i pododdziałów WE do jej prowadzenia. Podczas pokoju powinna być prowadzona obrona elektroniczna – mająca za zadanie przygotować technicznie i organizacyjnie własne środki elektroniczne, aby stały się odporne na oddziaływanie elektroniczne i ogniowe przeciwnika.

Przedsięwzięcia w zakresie walki elektronicznej powinny skutecznie wspierać działania taktyczne. Aby to osiągnąć, niezbędne jest przygotowanie planu walki elektronicznej, w pełni zintegrowanego z planem walki. Walka elektroniczna musi być koordynowana pomiędzy rodzajami wojsk na wszystkich szczeblach dowodzenia. W tym celu powinny być opracowywane odpowiednie procedury skutecznego jej koordynowania.

Odpowiedzialność za walkę elektroniczną ponosi – zgodnie z obowiązującymi dokumentami normatywnymi – dowódca. Natomiast za jej przygotowanie i prowadzenie – szef roz-

[4] Problematyka ta szerzej jest przedstawiona w pracy pt. *Walka elektroniczna w działaniach taktycznych wojsk lądowych*, AON, Warszawa 1999.

poznania (G2). Przedsięwzięcia rozpoznania oraz zakłócania elektronicznego powinny być realizowane przez etatowy (przydzielony) pododdział walki elektronicznej (pododdział elektroniczny) zgodnie z otrzymanym zadaniem, a przedsięwzięcia obrony elektronicznej – przez wszystkich użytkowników systemów i urządzeń elektronicznych.

Pomyślna realizacja przedsięwzięć walki elektronicznej uzależniona jest w dużej mierze od utworzenia w okresie pokoju bazy danych oraz systematycznego jej aktualizowania. Zgromadzone w niej dane o sprzęcie elektronicznym i taktyce jego wykorzystania są niezbędne dla prawidłowego funkcjonowania systemów rozpoznania i zakłócania elektronicznego. Są pomocne również podczas realizacji przedsięwzięć obrony elektronicznej.

2. ROZPOZNANIE ELEKTRONICZNE

2.1. Istota rozpoznania elektronicznego

Postęp naukowy, techniczny i technologiczny w wielu dziedzinach spowodował, że elektronika stała się niezbędna na współczesnym polu walki między innymi do pozyskiwania danych o przeciwniku. Lokalne konflikty zbrojne ostatniego ćwierćwiecza (zwłaszcza działania zbrojne w rejonie Zatoki Perskiej) potwierdzają, że o sukcesie walczących stron w znacznym stopniu zdecydowały elektroniczne środki walki wspomagające lotnictwo, siły morskie i wojska lądowe.

Zmiana orientacji nastąpiła w połowie latach 70., kiedy to w połączonych siłach zbrojnych NATO przyjęto program kompatybilnego rozwoju systemów działających w oparciu o elektronikę i określono go skrótem „C^3I"[5]. Było to rezultatem przeprowadzonych badań, które jednoznacznie wykazały, że eksploatowane systemy są przestarzałe i nie spełniają wymogów ówczesnego pola walki.

Po przebudowie, związanej z przyjęciem programu „C^4I^2"[6], nowoczesne systemy elektroniczne integrują szereg różnych funkcji w jedną całość i zapewniają między innymi:

– możliwość zdobywania danych o przeciwniku;

– kontrolę własnych wojsk;

– komputerowe wspomaganie procesów decyzyjnych;

– niezawodnie funkcjonującą łączność.

Skład, struktura organizacyjna, rozmieszczenie przestrzenne elementów takiego systemu oraz więzi informacyjne i funkcjonalne występujące między nimi pozwalają na realizację następujących zadań:

– usprawnienie przegrupowania i manewru wojsk;

– automatyzację kierowania środkami walki;

– kontrolę wykonania postawionych zadań i przebiegu walki.

Zdobywanie danych o siłach i środkach przeciwnika determinowane jest dążeniem do osiągnięcia stanu, który pozwoli na dostarczenie własnym wojskom wiernego i aktualnego obrazu pola walki oraz prawdopodobnych przyszłych zachowań przeciwnika w czasie zbliżonym do rzeczywistego, oczywiście bez jego wiedzy o inwigilacji. To ostatnie kryterium najlepiej spełniają systemy rozpoznania elektronicznego.

---

[5] C^3I – ang. Command, Control, Communication and Intelligence. Jest programem w znaczeniu rzeczowym i procedurą w znaczeniu czynnościowym (nie jest systemem).

[6] C^4I^2 – ang. Command, Control, Communications, Computers, Intelligence and Information.

Rozpoznanie elektroniczne, będące elementem składowym WE, jest również jednym z elementów składowych rozpoznania wojskowego, realizowanego w celu zdobywania i przetwarzania tych danych o przeciwniku, których nośnikami są fale elektromagnetyczne oraz inne efekty uboczne towarzyszące działaniom bojowym (zjawiska akustyczne, magnetyczne, chemiczne). Rozpoznanie elektroniczne można prowadzić bez względu na porę roku, doby i warunki atmosferyczne. Jest to najszybszy, najtańszy, najbardziej manewrowy i skryty rodzaj rozpoznania. Do jego mankamentów zalicza się podatność na zakłócenia i dezinformację.

Rozpoznanie elektroniczne dzieli się na:

– radioelektroniczne;

– radiolokacyjne;

– optoelektroniczne;

– czujnikowe;

– informatyczne.

Na szczeblu taktycznym nowoczesny system rozpoznania elektronicznego powinien więc zapewniać pozyskiwanie, weryfikację, gromadzenie i dystrybucję danych rozpoznawczych ze środowiska elektromagnetycznego i zjawisk ubocznych towarzyszących walce zbrojnej.

W systemie rozpoznania wojsk lądowych rozpoznanie elektroniczne jest istotną częścią rozpoznania taktycznego. Należy je prowadzić za pomocą urządzeń rozpoznawczych w podzakresach widma wykorzystywanych przez środki instalowane na pojazdach i aparatach latających.

Rozpoznanie taktyczne prowadzi się w strefie bezpośredniej styczności wojsk, w strefie walki obronnej lub zaczepnej oddziałów i związków taktycznych. Jego głównym celem jest wsparcie informacyjne dowódców podejmujących decyzje o użyciu wojsk i sposobie rozegrania walki (bitwy). Obejmuje ono rozpoznanie naziemne oraz powietrzne.

W taktycznym rozpoznaniu elektronicznym zazwyczaj wykorzystuje się:

– samoloty, śmigłowce i środki bezpilotowe wyposażone w rozpoznawcze urządzenia radiowe, zestawy czujnikowe, aparaturę fotograficzną, urządzenia noktowizyjne i techniki podczerwieni oraz kamery telewizyjne;

– polowe środki rozpoznania elektronicznego, takie jak: aparatownie odbioru i analizy emisji radiowych różnych zakresów częstotliwości, namierniki radiowe, stacje rozpoznania systemów radiolokacyjnych, stacje rozpoznania łączności radioliniowej i satelitarnej, stanowiące wyposażenie pododdziałów rozpoznania i walki elektronicznej;

– różnego rodzaju artyleryjskie środki rozpoznania radiolokacyjnego i dźwiękowego;

– polowe stacje radiolokacyjne obserwacji pola walki wojsk lądowych rozwijane w ugrupowaniu bojowym batalionów i brygad.

2.2. Rozpoznanie radioelektroniczne

Rozpoznanie radioelektroniczne ma na celu zdobywanie i przetwarzanie danych o systemach i środkach przeciwnika emitujących energię elektromagnetyczną w postaci sygnałów oraz informacji zawartych w tych sygnałach. Rozpoznanie wymienionych środków[7] dostarcza różnorodnych danych o przeciwniku i o jego systemach radioelektronicznych.

Metodami zdobywania danych w rozpoznaniu radioelektronicznym są: *poszukiwanie, przechwytywanie, śledzenie aktywności źródeł, namierzanie oraz analiza techniczno-operacyjna.*

Poszukiwanie, zdaniem zespołu badawczego, jest podstawowym procesem, który ma na celu wykrycie sygnałów wypromieniowanych przez źródła rozpoznania i wyselekcjonowanie tych, którymi prowadzący rozpoznanie jest zainteresowany.

Aby mogło nastąpić wykrycie źródła sygnału, muszą być spełnione następujące warunki:

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

2. energetyczny – tzn. moc sygnału na wejściu urządzenia rozpoznawczego Ps_{we} musi być nie mniejsza od jego realnej czułości Po_{we}:

$$Ps_{we} \geq Po_{we} \quad (2.2.1)$$

3. częstotliwościowy – tzn. odbiornik urządzenia rozpoznawczego musi być nastrojony na częstotliwość pracy (nośną) źródła sygnału *fs*, z odpowiednią dokładnością:

$$fo - \frac{\Delta f}{2} \leq fs \leq fo + \frac{\Delta f}{2} \quad (2.2.2)$$

gdzie:

fo – częstotliwość, na którą jest nastrojony odbiornik;

Δf – szerokość pasma przepuszczania odbiornika;

fs – częstotliwość nośna sygnału.

W trakcie poszukiwania realizowanego za pomocą odpowiednich urządzeń każdy wykryty sygnał zazwyczaj zostaje poddany wstępnej identyfikacji i klasyfikacji. Poszukiwanie sygnałów prowadzi się w częstotliwości, kierunku lub równocześnie w częstotliwości i kierunku.

Poszukiwanie w częstotliwości polega na przestrajaniu urządzenia odbiorczego w całym jego zakresie lub określonym podzakresie i ustaleniu tych częstotliwości, na których występują poszukiwane sygnały. Jedną z form poszukiwania w częstotliwości jest jednoczesny odbiór w kilku przedziałach częstotliwości przy użyciu odbiorników wielokanałowych.

[7] W teorii rozpoznania nazywa się je źródłami. Źródłami rozpoznania radioelektronicznego są wszystkie środki pracujące w zakresie widma elektromagnetycznego od dolnej granicy podzakresu radiowego do górnej granicy podzakresu optycznego.

Te ostatnie są szczególnie przydatne przy poszukiwaniu emisji rozproszonych typu FH[8]. Nowoczesne urządzenia rozpoznawcze realizujące poszukiwanie w częstotliwości są bardzo szybkie. Prędkość przestrajania osiąga wartości ok. 20 – 40 GHz/sek., dlatego wykrywanie sygnałów emisji FH nie stanowi dla nich problemu. Z reguły urządzenia te są wyposażone w anteny o charakterystyce dookólnej, sektorowej lub kierunkowej.

Poszukiwanie w kierunku (azymucie) jest realizowane przez zmianę położenia całego urządzenia rozpoznawczego lub samej anteny. Urządzenia rozpoznawcze do poszukiwania w azymucie mają anteny o charakterystyce kierunkowej, podobnie jak źródła rozpoznania, których poszukują. Jedną z form poszukiwania w azymucie jest jednoczesny odbiór przy pomocy kilku (kilkunastu) anten kierunkowych. Po wykryciu i identyfikacji sygnału następuje namierzanie jego źródła.

Przechwytywanie oznacza odbiór sygnałów nadawanych przez wykryte źródła rozpoznania i rejestrowanie bądź samych sygnałów, bądź zawartych w nich informacji. Polega na dostrojeniu urządzenia rozpoznawczego do częstotliwości pracy rozpoznawanego źródła i ciągłej rejestracji nadawanych informacji lub zmian parametrów nadawanego sygnału. Kryterium wyboru źródła do przechwytywania stanowi jego wartość informacyjna oraz ranga i miejsce obiektu, który to źródło obsługuje. Innymi słowy, przechwytuje się nadawanie tych źródeł, które w danej sytuacji przekazują ważne informacje bądź są ważnym elementem rozpoznawanego systemu.

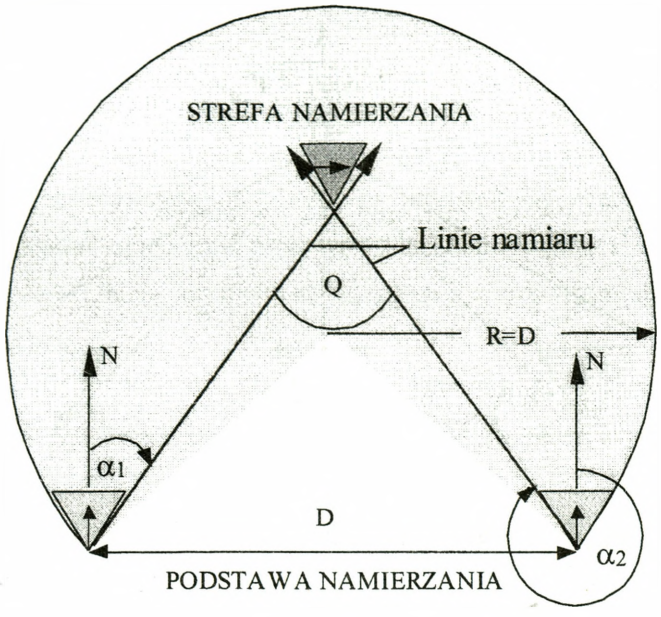
Śledzenie polega na okresowym sprawdzaniu pracy rozpoznawanych źródeł. Śledzi się te źródła, których sygnały nie wymagają przechwytywania, lub których wartość informacyjna w danej sytuacji jest drugorzędna. Śledzenie polega na okresowym dostrojeniu urządzenia rozpoznawczego do ustalonej wcześniej częstotliwości pracy źródła oraz krótkotrwałej rejestracji jego nadawania w celu sprawdzenia (potwierdzenia) danych posiadanych o tym źródle. Część źródeł, takich jak stacje radiolokacyjne czy radionawigacyjne, podlega śledzeniu ciągłemu. W konsekwencji można więc wyróżnić śledzenie:

– ciągłe;
– okresowe;
– kontrolne.

Namierzanie to proces lokalizacji źródła promieniowania elektromagnetycznego za pomocą namierników[9] (stacji namierzania). Prowadzi się je co najmniej dwoma namiernikami rozwiniętymi w określonej odległości od siebie (rys. 4). Ta odległość, zwana podstawą namierzania (D), jest uzależniona od głębokości i zakładanej dokładności lokalizacji.

[8] Emisja typu FH (od ang. Freqency Hopping) polega na permanentnej zmianie wykorzystywanych częstotliwości radiowych. Typowa szybkość to ok. 200–300 zmian w ciągu sekundy.

[9] W niektórych materiałach określenie „namiernik" jest używane zamiennie z nazwą „pelengator".



Rys. 4. Lokalizacja źródła dwoma namiernikami

Dokładność lokalizacji warunkuje między innymi wielkość kąta wcięcia (Q). Największą dokładność uzyskuje się przy kącie wcięcia 90°, zaś granicznymi wartościami są kąty 30° i 150°. Uwzględniając te ograniczenia, ustala się głębokość rozpoznania, którą określa strefa namierzania odpowiadająca okręgowi o promieniu (R) równym podstawie namierzania (D). Kierunki na pracujące źródło rozpoznania określa się przy pomocy namierników lub innych urządzeń posiadających anteny o charakterystyce kierunkowej, które pozwalają na dokonanie i odczytanie namiaru (azymutu).

Namiarem nazywamy dodatni kąt (α) zawarty pomiędzy kierunkiem północy magnetycznej (geograficznej, topograficznej) a kierunkiem na namierzane źródło. Kierunek ten wyznaczają linie namiaru.

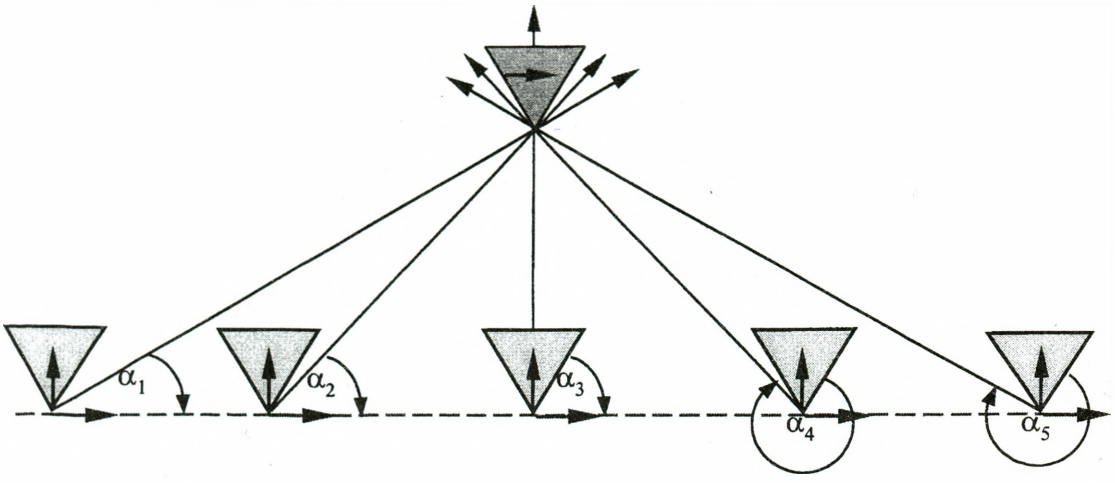
Lokalizacji źródła można też dokonać za pomocą tylko jednego namiernika. W takim przypadku dokonuje się kilkakrotnego namiaru na to samo źródło z kolejnych pozycji ruchomego namiernika. Ten sposób namierzania ilustruje rys. 5. Celowe jest zainstalowanie namiernika na samolocie, śmigłowcu lub innym aparacie latającym. Jednak przy tym sposobie namierzania muszą być spełnione dwa podstawowe warunki: dostatecznie długi czas pracy namierzanego źródła oraz precyzyjne określenie własnego położenia przez namiernik w trakcie namiaru.

Rozróżnia się trzy sposoby namierzania:

– automatycznie (synchronicznie);

– na komendę;

– według zadań stałych.



Rys. 5. Namierzanie pojedynczym namiernikiem zamontowanym na ruchomym środku

Namierzanie automatyczne (synchroniczne) polega na określeniu azymutów na źródło rozpoznania jednocześnie przez wszystkie namierniki, które przy pomocy specjalnej aparatury są dostrajane do częstotliwości pracującego źródła. Ten sposób jest wykorzystywany w nowoczesnych, zautomatyzowanych systemach namierzania.

Namierzanie na komendę polega na określaniu azymutów na źródło przez wszystkie namierniki, które dostraja się do częstotliwości źródła po otrzymaniu zadania ze stanowiska kierowania namierzaniem lub bezpośrednio ze stanowiska rozpoznawczego. Ten sposób był i nadal jest stosowany w tradycyjnych systemach namierzania.

Namierzanie według zadań stałych polega na określaniu azymutów na pracujące źródła zgodnie z wcześniej opracowanym harmonogramem (zadaniem). Ten sposób jest wykorzystywany w przypadku braku łączności z poszczególnymi posterunkami namierzania.

Analiza techniczno-operacyjna jest to proces zmierzający do określenia charakterystycznych cech sygnałów i ich źródeł, wyróżniających je spośród innych. Dotyczy to sygnałów i obiektów zarówno znanych, jak i nowo wykrytych. Pozwala to przy kolejnych przypadkach wykrycia na ich identyfikację z dokładnością do rodzaju obiektu, a nawet pojedynczego egzemplarza sprzętu.

W tym procesie dokonuje się również logicznego uporządkowania informacji o rozpoznawanych obiektach. Ocenia się ich skład i rozmieszczenie, stan ilościowo-jakościowy, rodzaj działalności i zamierzenia ich użytkowników.

Ze względu na rodzaje środków w rozpoznaniu radioelektronicznym szczebla taktycznego możemy wyróżnić:

– rozpoznanie radiowe;

– rozpoznanie systemów radiolokacyjnych;

– rozpoznanie systemów radionawigacyjnych.

2.2.1. Rozpoznanie radiowe

Rozpoznanie radiowe jest rodzajem rozpoznania radioelektronicznego, które obejmuje środki łączności radiowej i środki zakłócające tę łączność. Ma na celu zdobycie informacji o stanie ilościowym i jakościowym tych środków, miejscu ich rozmieszczenia i sposobach wykorzystania. Owe środki mogą pracować w systemach łączności radiowej krótkofalowej (KF) i ultrakrótkofalowej (UKF), łączności radioliniowej (horyzontowej i pozahoryzontowej) oraz łączności satelitarnej.

Łączność radiowa KF, traktowana obecnie jako rezerwowa, w dalszym ciągu nie straciła na znaczeniu w dowodzeniu wojskami. Mimo tendencji do pomniejszania jej roli stanowi nadal dla rozpoznania radioelektronicznego jedno z zasadniczych źródeł rozpoznania, co wynika głównie z propagacji fal krótkich, których zasięg jest w zasadzie nieograniczony.

Łączność radiowa UKF jest wykorzystywana przez wszystkie szczeble dowodzenia. Stanowi podstawowy rodzaj łączności do szczebla brygady włącznie. Natomiast od szczebla dywizji wzwyż służy do wewnętrznych połączeń na stanowiskach dowodzenia. Ponadto jest stosowana we współdziałaniu wojsk lądowych z lotnictwem taktycznym w relacjach ziemia-samolot. Łączność radiowa UKF wojsk lądowych (20 – 88 MHz) i sił powietrznych (220 – 400 MHz) jest jednym z podstawowych źródeł rozpoznania na szczeblu taktycznym.

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

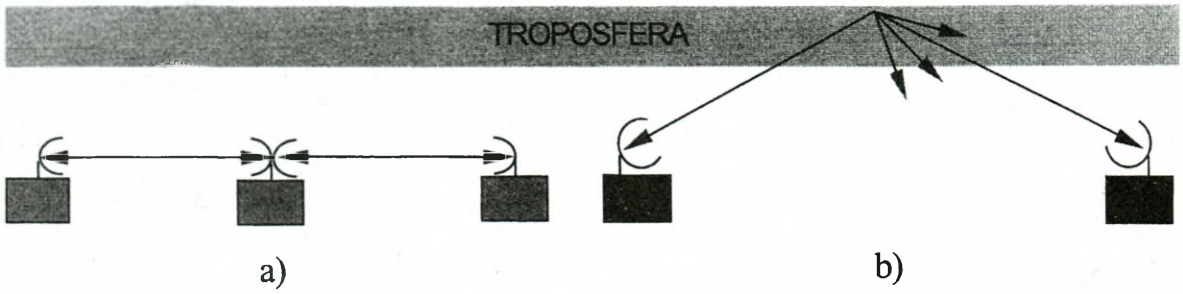
Rozpoznanie łączności radioliniowej obejmuje przedsięwzięcia prowadzące do zdobywania danych dotyczących tych środków i systemów łączności. Polega na wykrywaniu sygnałów przekazywanych w kierunkach radioliniowych oraz przechwytywaniu i analizowaniu danych przesyłanych w kanałach radioliniowych horyzontowych i pozahoryzontowych.

Środki rozpoznania łączności radioliniowej są instalowane w specjalnych aparatowniach, które poszukując sygnałów, poruszają się po drogach rokadowych, bądź na statkach powietrznych (pilotowych i bezpilotowych) latających w strefach dyżurowania nad własnym ugrupowaniem.

W przypadku rozpoznania łączności horyzontowej anteny stacji radioliniowych i urządzenia rozpoznawczego muszą być w zasięgu optycznym (muszą się „widzieć"), natomiast rozpoznanie łączności pozahoryzontowej wykorzystującej rozproszenie wiązki na niejednorodnościach troposfery (stąd potoczna nazywa łączności troposferycznej) nie wymaga warunku bezpośredniej widoczności, w tym przypadku anteny stacji radioliniowej i urządzenia rozpoznawczego mogą się znajdować w znacznej odległości od siebie (poza zasięgiem optycznym). Ideę łączności radioliniowej horyzontowej i pozahoryzontowej ilustruje rys.6.

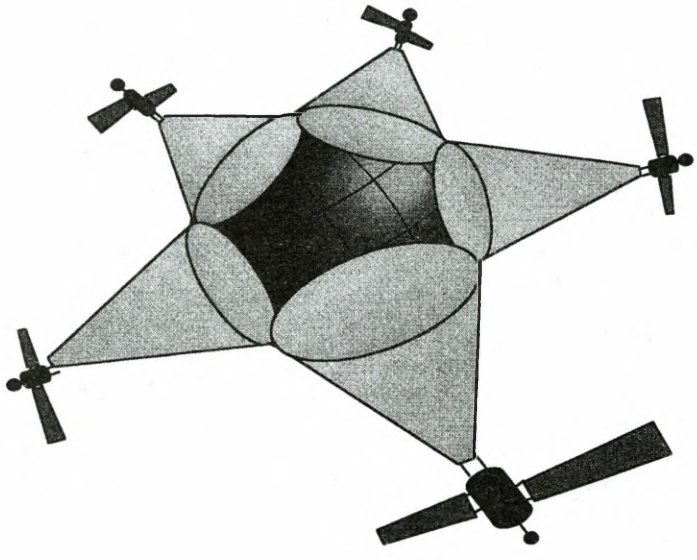
Wraz z rozwojem systemów łączności satelitarnej kształtował się nowy rodzaj rozpoznania elektronicznego – *rozpoznanie łączności satelitarnej*. Rozpoznanie łączności satelitarnej obejmuje przedsięwzięcia prowadzące do zdobywania danych o środkach i systemach łączno-

ści wykorzystujących sztuczne satelity Ziemi. Polega na wykrywaniu sygnałów przekazywanych z satelity, ich przechwytywaniu i analizowaniu.



Rys. 6. Łączność radioliniowa: a) horyzontowa, b) pozahoryzontowa

Działanie większości systemów łączności możliwe jest dzięki dużym satelitom telekomunikacyjnym rozmieszczonym na orbitach geostacjonarnych (rys. 7). Krążą one na wysokości około 36 tys. kilometrów, przy zachowaniu tych samych współrzędnych geograficznych, czyli unoszą się nad tym samym punktem na powierzchni Ziemi, w płaszczyźnie równika.



Rys. 7. Pięć satelitów geostacjonarnych tworzy konstelację systemu łączności

W zależności od systemu na orbicie rozmieszcza się od trzech do dziewięciu satelitów geostacjonarnych, które pokrywają swym zasięgiem niemalże cały glob ziemski (z wyjątkiem rejonów podbiegunowych).

Do rozpoznania łączności satelitarnej wykorzystuje się urządzenia odbiorcze, a ich anteny ustawia się w kierunku możliwego rozmieszczenia satelitów. Położenie orbit i satelitów geostacjonarnych jest zazwyczaj znane, co znacznie ułatwia proces poszukiwania w kierunku. Zasadniczym problemem w procesie wykrywania jest więc poszukiwanie w częstotliwości.

W zależności od generacji systemu łączności satelitarnej wykorzystywane przez nie pasma częstotliwości mieszczą się w przedziałach:

– starsze – w pasmie C (650 – 800 MHz);

– nowsze – w pasmie Ku (12 – 18 GHz) i pasmie Ka (26,5 – 40 GHz).

Sygnały przekazywane w tych pasmach, ze względu na efektywność wykorzystania widma częstotliwości są zazwyczaj poddane kompresji, co znacznie utrudnia proces rozpoznania.

Oprócz satelitów geostacjonarnych w globalnych systemach łączności wykorzystuje się również satelity na tzw. średnich orbitach (10 – 16 tys. km). Proces rozpoznania w tym przypadku jest o wiele bardziej złożony. Urządzenia rozpoznawcze muszą prowadzić poszukiwanie w azymucie, elewacji i częstotliwości, a po ich wykryciu ruchome anteny urządzeń rozpoznawczych muszą podążać za wykrytym obiektem do momentu jego zniknięcia za linią horyzontu.

Rozpoznanie łączności satelitarnej stoi przed koniecznością rozwiązywania problemów związanych z systemami działającymi na podstawie satelitów na niskich orbitach (poniżej 2 tys. km). Złożoność tych systemów, liczba wykorzystywanych satelitów (od 14 do 66), jak i bardzo duża prędkość kątowa wynosząca ok. 3,6°/min (czas obiegu jednego satelity wokół Ziemi wynosi około 100 minut) stanowią prawdziwe wyzwanie dla specjalistów rozpoznania łączności satelitarnej.

Omówione systemy łączności radiowej, radioliniowej i satelitarnej mogą być niewyczerpanymi źródłami danych, z których przy dobrze zorganizowanym rozpoznaniu radioelektronicznym można czerpać dane rozpoznawcze w interesującym nas zakresie.

Należy jednak pamiętać, że każde z tych źródeł charakteryzuje się indywidualnymi cechami rozpoznawczymi[10], co powinno być uwzględniane przy organizowaniu rozpoznania radioelektronicznego.

2.2.2. Rozpoznanie systemów radiolokacyjnych

Rozpoznanie systemów radiolokacyjnych polega na zdobywaniu danych dotyczących systemów i środków radiolokacyjnych rozpoznania pola walki, artylerii i środków napadu powietrznego przez poszukiwanie, przechwytywanie i analizę sygnałów wypromieniowanych przez te środki oraz ich namierzanie i śledzenie.

Analiza położenia wykrytych środków radiolokacyjnych przeciwnika stwarza możliwość ustalenia rozmieszczenia jego posterunków rozpoznania pola walki, pododdziałów i oddziałów artylerii z ich stanowiskami dowodzenia i kierowania oraz posterunków wykrywania środków napadu powietrznego.

---

[10] Problematyka ta szerzej jest przedstawiona w pracy pt. *Walka elektroniczna w działaniach taktycznych wojsk lądowych*, AON, Warszawa 1999.

Aby nastąpiło wykrycie pracującego źródła promieniowania radiolokacyjnego, muszą być spełnione podobne warunki jak w przypadku rozpoznania radiowego, tzn. energetyczny, częstotliwościowy, przestrzenny oraz czasowy.

Warunki te określają możliwości prowadzenia rozpoznania systemów radiolokacyjnych oraz mają zasadniczy wpływ na rozwiązania konstrukcyjne i sposoby działania urządzeń rozpoznawczych. Szczególne znaczenie dla możliwości poszukiwania i wykrywania stacji radiolokacyjnych mają warunki przestrzenny i częstotliwościowy, ponieważ wykrycie źródła emisji następuje w kierunku i w częstotliwości.

Pod względem ufności wyniki finalne dzielą się na pewne i prawdopodobne. Oznaczając przez:

N – zbiór poszukiwanych stacji radiolokacyjnych;

a – zdarzenie polegające na wykryciu stacji radiolokacyjnej „w kierunku";

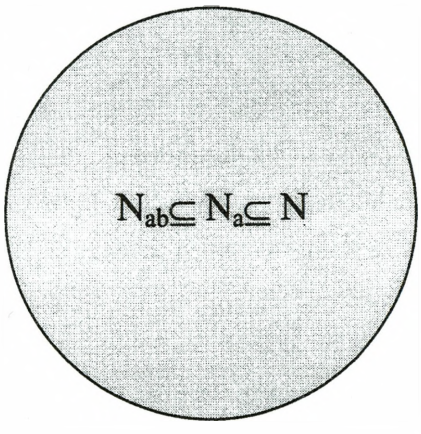
b – zdarzenie polegające na wykryciu stacji radiolokacyjnej „w częstotliwości";

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

a) przy poszukiwaniu i wykrywaniu pewnym

$$N = N_a = N_{ab} \qquad \text{bo: } N_{ab} \subseteq N_a \subseteq N$$

Co geometrycznie interpretuje się jak na rys. 8.



Rys. 8. Interpretacja geometryczna zbiorów wykrywanych stacji radiolokacyjnych przy wykrywaniu pewnym

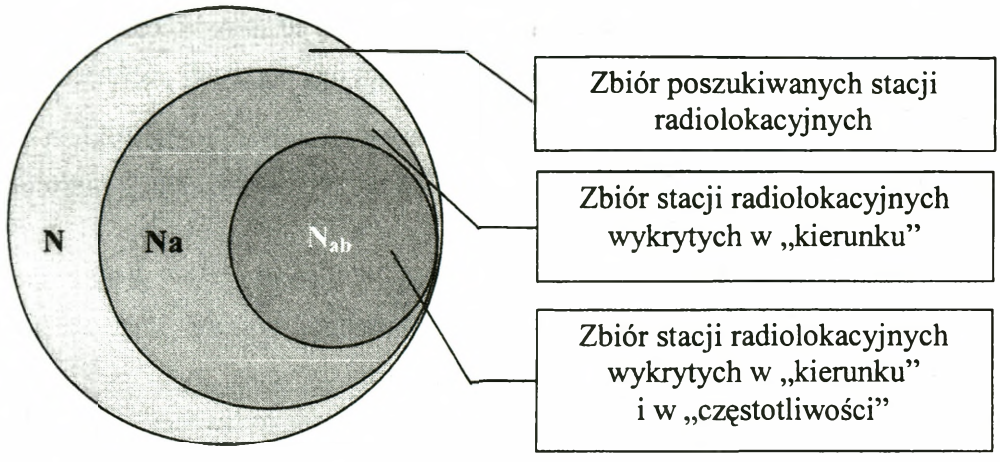
b) przy poszukiwaniu i wykrywaniu prawdopodobnym

$$N \geq N_a \geq N_{ab} \qquad \text{bo: } N_{ab} \subset N_a \subset N$$

Co geometrycznie interpretuje się jak na rys.9.

Z powyższego wynika, że finalnym wynikiem poszukiwania i wykrywania, tak w pierwszym jak i drugim wypadku, jest zbiór stacji radiolokacyjnych wykrytych w „częstotliwości" i w „kierunku", czyli zbiór „N_{ab}". W obydwu przypadkach zbiór stacji radiolokacyjnych wykrytych w kierunku i w częstotliwości jest podzbiorem zbioru stacji wykrytych w kierunku, co można zapisać:

$$N_{ab} \subset N_a$$



Rys. 9. Interpretacja geometryczna zbiorów wykrywanych stacji radiolokacyjnych przy wykrywaniu prawdopodobnym

Pierwszą czynnością w procesie poszukiwania i wykrywania jest więc poszukiwanie i wykrywanie stacji radiolokacyjnych „w kierunku", a następnie „w częstotliwości". Do prowadzenia w takiej kolejności procesu poszukiwania i wykrywania dostosowane są również w większości przypadków rozpoznawcze stacje radiolokacyjne.

W warunkach poszukiwania i wykrywania pewnego miernikiem możliwości jest czas przewidziany na pewne wykrycie, w kierunku i w częstotliwości, „N" zbioru stacji radiolokacyjnych. Czas ten jest sumą czasów potrzebnych między innymi na:

– pewne wykrycie określonego zbioru stacji „w kierunku";

– pewne wykrycie określonego zbioru stacji „w częstotliwości";

– analizę zbioru sygnałów stacji radiolokacyjnych wykrytych w „częstotliwości", co w zapisie wyraża się

$$T_p = T_a + T_b + T_c$$

gdzie:

T_p – sumaryczny czas pewnego wykrycia „N" zbioru stacji radiolokacyjnych „w kierunku" i „w częstotliwości";

T_a – czas pewnego wykrycia „N" zbioru stacji radiolokacyjnych „w kierunku";

T_b - czas pewnego wykrycia „N" zbioru stacji radiolokacyjnych „w częstotliwości";

T_c – czas analizy sygnałów „N" zbioru stacji radiolokacyjnych wykrytych „w częstotliwości".

W praktyce wygodniej jest jednak korzystać ze wzoru:

$$T_p = \overline{\overline{N}} \, (T_{a1} + T_{b1} + T_{c1})$$

gdzie:

$\overline{\overline{N}}$ – moc (liczność) zbioru poszukiwanych stacji radiolokacyjnych;

T_{a1} – czas pewnego wykrycia „w kierunku" jednej stacji radiolokacyjnej;

T_{b1} – czas pewnego wykrycia „w częstotliwości" jednej stacji radiolokacyjnej;

T_{c1} – czas analizy jednego sygnału stacji radiolokacyjnej wykrytej „w częstotliwości".

W warunkach poszukiwania i wykrywania prawdopodobnego miernikiem możliwości jest wartość prawdopodobieństwa określająca stopień wykrywalności stacji radiolokacyjnych, co symbolicznie oznacza się i odczytuje:

$P_{an}(N) = p_n$ prawdopodobieństwo wykrycia „w kierunku" „N" zbioru stacji radiolokacyjnych, przy „n" razy obróconej antenie stacji radiolokacyjnej w sektorze obserwacji (rozpoznania), wynosi „p_n";

$P_{bk}(N_a) = p_k$ prawdopodobieństwo wykrycia „w częstotliwości" „N_a" zbioru stacji radiolokacyjnych (zbioru wcześniej wykrytego w kierunku), przy „k" razy przeszukanym (przestrojonym) podzakresie odbiornika rozpoznawczego stacji radiolokacyjnej, wynosi „p_k";

$P_{ab}(N) = p$ prawdopodobieństwo finalne - określające, że „N" zbiór stacji radiolokacyjnych został wykryty i „w kierunku", i „w częstotliwości" - wynosi „p".

Miernikiem możliwości poszukiwania i wykrywania „prawdopodobnego" jest również moc zbioru wykrytych stacji radiolokacyjnych. Moc tego zbioru wyraża się następująco:

a) w odniesieniu do stacji radiolokacyjnych wykrytych tylko „w kierunku"

$$\overline{\overline{N}}_a = \overline{\overline{N}}\, P_{an}(N)$$

b) w odniesieniu do stacji radiolokacyjnych wykrytych „w kierunku"i „w częstotliwości":

$$\overline{\overline{N}}_{ab} = \overline{\overline{N}}\, P_{a(n-j)}(N)$$

Przy czym „n-j" oznacza, że liczba obrotów anteny rozpoznawczej stacji radiolokacyjnej pomniejszona została o „j" razy, to jest o ilość obrotów anteny w czasie niezbędnym do poszukiwania stacji radiolokacyjnej w częstotliwości, kiedy antena zatrzymana była na jednym kierunku (nie obracała się).

Wykrywanie sygnałów w dziedzinie kąta, zwane *wykrywaniem w kierunku* (azymucie), wiąże się z określeniem kierunku przyjścia sygnału od źródła emisji i może być prowadzone następującymi metodami:

– bez poszukiwania, tzw. wykrywanie natychmiastowe;

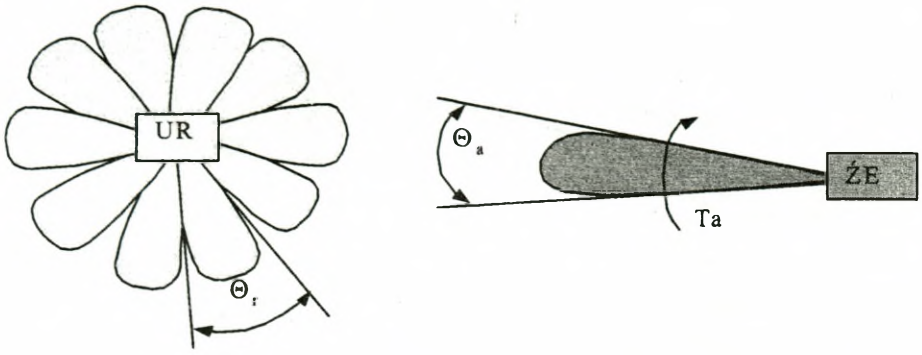
– z poszukiwaniem.

Do metod *wykrywania w kierunku bez poszukiwania* zalicza się:

– wykrywanie za pomocą dookólnego odbioru kierunkowego;

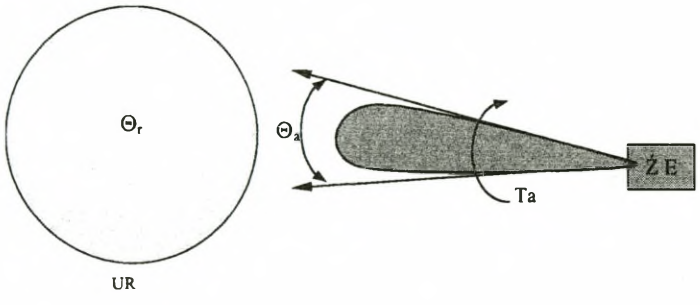
– wykrywanie za pomocą odbioru bezkierunkowego.

Charakterystyczną cechą tego sposobu wykrywania jest jednoczesny odbiór ze wszystkich kierunków, zazwyczaj za pomocą wielu anten kierunkowych (rys.10) lub anteny bezkierunkowej (rys.11).



Rys. 10. Wykrywanie źródeł emisji metodą dookólnego odbioru kierunkowego

System wielu anten kierunkowych daje natychmiastową informację o kierunku, z którego odebrany został sygnał. Jego zasadniczą wadą jest jednak mała dokładność określania kierunku – równa w przybliżeniu połowie szerokości charakterystyki kierunkowej anteny urządzenia rozpoznawczego.

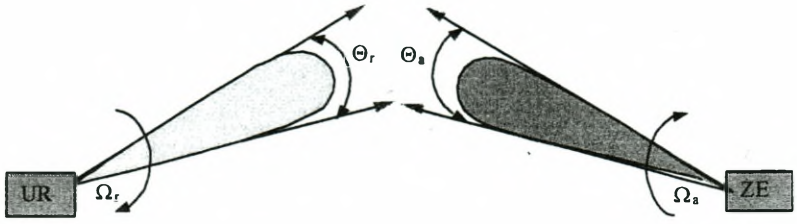


Rys. 11. Wykrywanie źródeł emisji metodą odbioru bezkierunkowego

Znacznie lepsze efekty uzyskuje się, stosując metodę interferometryczną z wykorzystaniem dyskryminatorów fazy. W metodzie tej określenia kierunku, z którego odbierany jest sygnał, dokonuje się, mierząc przesunięcia fazowe sygnałów z dwu lub więcej anten. Metoda ta pozwala na bardzo szybkie i dokładne określenie kierunku, nawet przy odbiorze niewielkiej ilości sygnałów czy wręcz tylko jednego.

Poszukiwanie i wykrywanie stacji radiolokacyjnych w kierunku (azymucie) prowadzi się przy ustawieniu rozpoznawczej stacji radiolokacyjnej na pracę detektorową, zapewniającą odbiór sygnałów radiolokacyjnych w szerokim paśmie częstotliwości.

Warunkiem wykrycia stacji radiolokacyjnej w azymucie jest zdarzenie polegające na tym, że charakterystyki anten stacji nadawczej (rozpoznawanej) i odbiorczej (rozpoznającej) znajdą się na jednej linii – „spotkają się" w przestrzeni (rys. 12).



- Ω_r – prędkość kątowa anteny urządzenia rozpoznawczego;
- Ω_a – prędkość kątowa anteny urządzenia rozpoznawanego;
- Θ_r – szerokość charakterystyki anteny urządzenia rozpoznawczego;
- Θ_a – szerokość charakterystyki anteny rozpoznawanego źródła emisji.

Rys. 12. Wykrywanie stacji radiolokacyjnych w kierunku z poszukiwaniem

Teoretycznie należałoby rozpatrywać możliwości spotkania w przestrzeni trójwymiarowej, ponieważ jednak większość urządzeń rozpoznawczych posiada stosunkowo szerokie charakterystyki w płaszczyźnie pionowej (elewacji) np. typu cosecans^2 i nie stosuje się przeszukiwania w tej płaszczyźnie, to w celu uproszczenia rozważań przyjmuje się jako warunek spotkanie charakterystyk w płaszczyźnie poziomej.

Czas trwania takiego „spotkania" oznacza jednocześnie czas trwania odbioru sygnału stacji radiolokacyjnej (ŹE) przez stację rozpoznania systemów radiolokacyjnych (UR) i zależy od szerokości charakterystyk poziomych tych stacji oraz szybkości kątowych obrotu ich anten. Oznaczając przez „t_o" czas trwania odbioru sygnału źródła przez urządzenie rozpoznawcze, zależności te wyrażają się następująco:

$$t_o = t_{os} = \frac{\Theta_s}{\Omega_s}$$

jeśli:

$$\frac{\Theta_r}{\Omega_r} \geq \frac{\Theta_s}{\Omega_s}$$

lub:

$$t_o = t_{or} = \frac{\Theta_r}{\Omega_r}$$

jeśli:

$$\frac{\Theta_r}{\Omega_r} < \frac{\Theta_s}{\Omega_s}$$

W tych metodach anteny urządzenia rozpoznawczego są ruchome (obrotowe) i w zależności od szybkości obrotów anten urządzenia rozpoznawczego i źródła emisji, wykrycie w kierunku może być:

– pewne ($P_w = 1$)

– prawdopodobne ($P_w < 1$)

Prawdopodobieństwo wykrycia sygnału (P_w) w kierunku można wyrazić wzorem:

$$P_w = P_{sp} \qquad P(t_s \geq t_z)$$

gdzie:

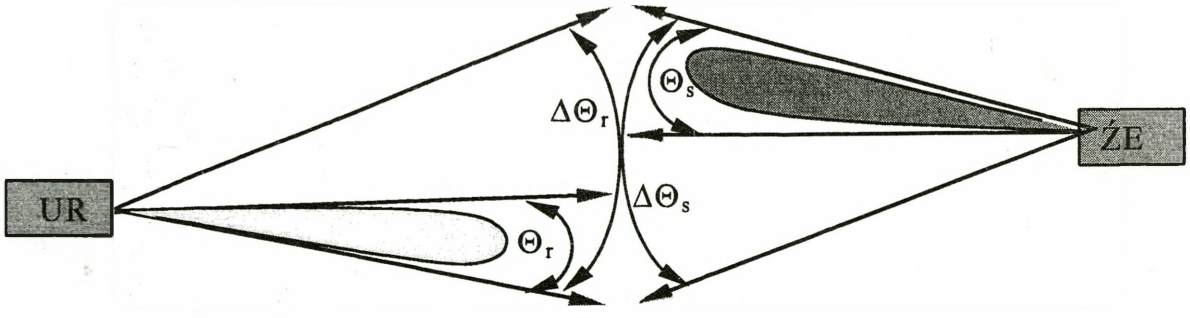
P_{sp} – prawdopodobieństwo spotkania charakterystyk kierunkowych anten UR i ZE w czasie największego z okresów obrotów tych anten;

$P(t_s \geq t_z)$ – prawdopodobieństwo odbioru sygnału o czasie przebywania w odbiorniku nie mniejszym od zadanego (w czasie spotkania charakterystyk kierunkowych anten).

Wartość P_{sp} zależy bezpośrednio od stosunku okresów obrotu anten urządzenia rozpoznawanego i rozpoznawczego ($\frac{Ta}{Tr}$).

W zależności od wartości tego stosunku w rozpoznaniu systemów radiolokacyjnych wyróżnia się poszukiwanie w kierunku: powolne, szybkie i z prędkością średnią[11].

W praktyce zarówno anteny urządzeń rozpoznawczych, jak i rozpoznawanych rzadko obracają się ze stałą prędkością w płaszczyźnie poziomej. Znacznie częściej jest stosowana praca sektorowa, przy której anteny szczególnie urządzeń rozpoznawczych poruszają się tylko w pewnym określonym zakresie. Z tego faktu wynika dodatkowy warunek wykrycia pracującej stacji radiolokacyjnej przez urządzenie rozpoznawcze: sektor obserwacji urządzenia rozpoznawanego musi się przynajmniej w części pokrywać (zazębiać) z sektorem obserwacji urządzenia rozpoznawczego (rys. 13). Tylko w części wspólnej tych sektorów mogą zaistnieć warunki do odbioru sygnału przez odbiornik urządzenia rozpoznawczego.



$\Delta\Theta_s$ - sektor obserwacji rozpoznawanej stacji radiolokacyjnej;
$\Delta\Theta_r$ - sektor obserwacji stacji rozpoznania systemów radiolokacyjnych.

Rys. 13. Ilustracja warunku „zazębiania się" sektorów obserwacji urządzenia rozpoznawczego i rozpoznawanego

[11] Problematyka ta szerzej jest przedstawiona w pracy pt. *Walka elektroniczna w działaniach taktycznych wojsk lądowych*, AON, Warszawa 1999.

We współczesnych urządzeniach stosowane są dwie metody określania częstotliwości *bez poszukiwania i z poszukiwaniem*, przy czym mogą być one wykorzystywane jednocześnie w tym samym urządzeniu w zależności od potrzeb i realizowanych zadań.

Metoda bez poszukiwania pozwala niemal na natychmiastowe określenie częstotliwości, podczas gdy metody wykorzystujące poszukiwanie wymagają pewnego czasu uwarunkowanego koniecznością przestrajania odbiornika. Metoda ta umożliwia znaczne skrócenie czasu rozpoznania, ale odbywa się to kosztem zmniejszenia dokładności i rozróżnialności pomiarów bądź też kosztem zwiększenia objętości aparatury.

Istota sposobu określania częstotliwości bez poszukiwania polega na tym, że rozpoznanie prowadzi się jednocześnie na wszystkich podzakresach roboczego zakresu częstotliwości. Aktualnie są znane następujące metody określania częstotliwości bez poszukiwania:

– rozpoznanie z zastosowaniem dyskryminatorów częstotliwościowych;

– metody interferencyjne;

– rozpoznanie za pomocą odbiorników wielokanałowych.

W rozpoznaniu prowadzonym przy użyciu dyskryminatorów częstotliwości wykorzystuje się możliwości przekształcania odchylenia częstotliwości od wartości zadanej w napięcie proporcjonalne do tego odchylenia.

Interferencyjne metody określania częstotliwości opierają się na zależności przesunięcia fazowego sygnału od długości drogi i częstotliwości. Porównując fazy rozpoznawanego sygnału przesłane przez odcinki falowodu o różnej długości, z dużą dokładnością możemy określić częstotliwość rozpoznawanego sygnału.

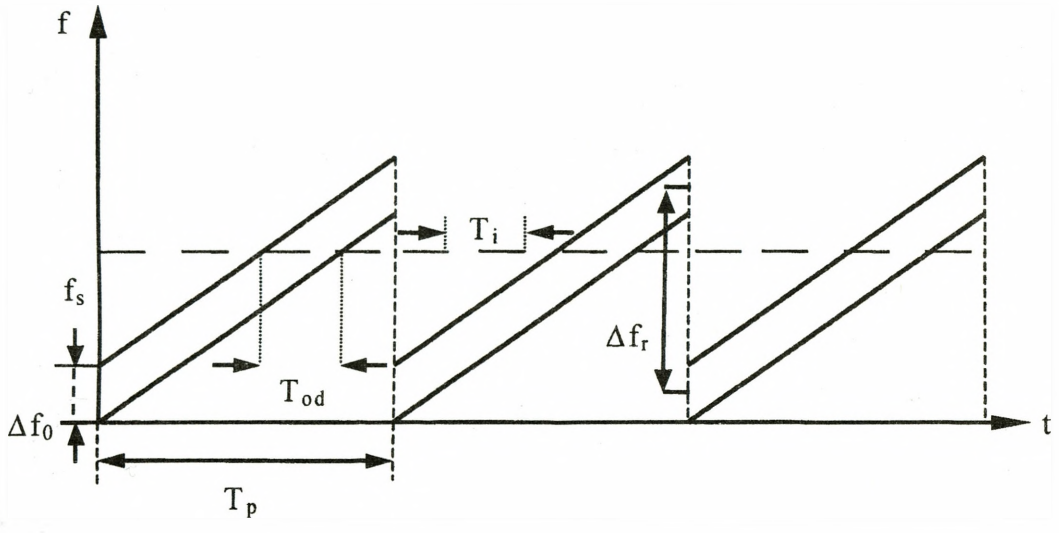
Rozpoznawanie z wykorzystaniem odbiorników wielokanałowych polega na podzieleniu całego zakresu rozpoznawanych częstotliwości na szereg podzakresów za pomocą zestawu filtrów o przylegających do siebie pasmach przepuszczania i odbiorze sygnałów z każdego podzakresu przez odpowiedni kanał odbiornika. Dokładność określania częstotliwości w tym przypadku jest uzależniona od wielkości wydzielonych podzakresów. W celu zredukowania ilości kanałów odbiornika przy zachowaniu dokładności określania częstotliwości w praktyce często jest używany tak zwany odbiornik macierzowy, w którym stosuje się metodę kilkustopniowego odbioru wielokanałowego z kilkukrotną przemianą częstotliwości.

Poszukiwanie i wykrywanie w częstotliwości ma na celu dokładne określenie częstotliwości nośnej (lub przedziału częstotliwości) sygnału stacji radiolokacyjnych wykrytych wcześniej w azymucie. Proces ten realizuje się po przełączeniu urządzenia rozpoznawczego na odbiór superheterodynowy (wąskopasmowy) i zatrzymaniu anteny na kierunku wykrytego sygnału. Podobnie jak w przypadku poszukiwania w kierunku, poszukiwanie w częstotliwości dzieli się na pewne i prawdopodobne. Do pewnych zalicza się poszukiwanie wolne i szybkie, do prawdopodobnych poszukiwanie z prędkością średnią. Kryterium podziału jest stosunek okresu przestrajania odbiornika urządzenia rozpoznawczego w pełnym zakresie częstotliwości i czasu trwania sygnału urządzenia rozpoznawanego.

Poszukiwanie wolne charakteryzuje się tym, że odbiornik urządzenia rozpoznawczego przestraja się o szerokość jego superheterodynowego pasma przepuszczania w czasie nie mniejszym niż okres powtarzania się cykli opromieniowania anteny urządzenia rozpoznawczego przez poszukiwaną stacje radiolokacyjną (rys. 14).

Jeżeli określenia częstotliwości można dokonać na podstawie jednego impulsu, to wolne poszukiwanie zapewnia prawdopodobieństwo wykrycia okresowego sygnału impulsowego P=1 w czasie przestrajania T_p. Istotną wadą wolnego poszukiwania jest duży czas obsługi, mała przepustowość i odpowiednio małe prawdopodobieństwo rozpoznania urządzeń radiolokacyjnych włączanych na krótki czas.

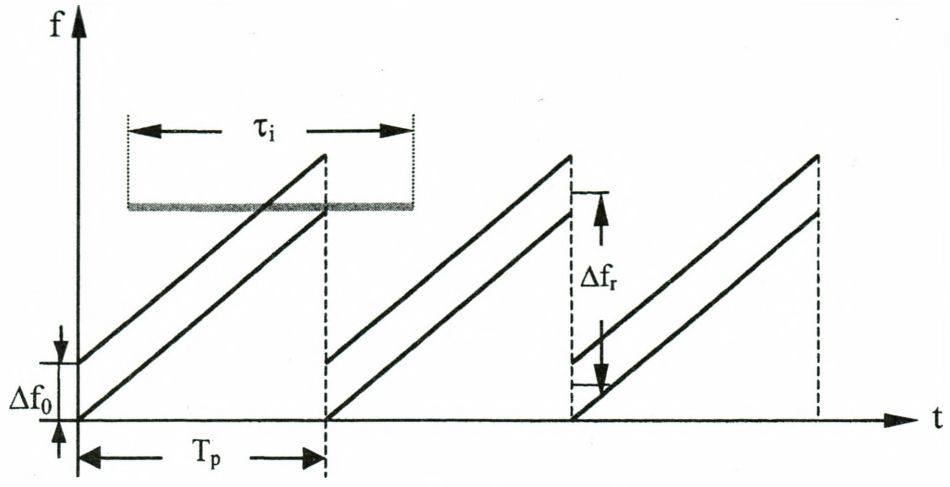
W celu zmniejszenia czasu rozpoznania przy zadanym zakresie przeszukiwania i danej prędkości przestrajania zachodzi konieczność rozszerzenia pasma przepuszczania odbiornika. W związku z powyższym dokładność określenia częstotliwości nośnej za pomocą tego typu odbiorników nie może być duża, ponieważ jest ona w przybliżeniu równa połowie szerokości pasma przepuszczania odbiornika. Z tych samych względów jest ograniczona również czułość tych odbiorników, często są to odbiorniki detektorowe z przestrajanymi obwodami wejściowymi.



Δf_0 – szerokość pasma odbiornika urządzenia rozpoznawczego;
Δf_r – zakres przestrajania odbiornika urządzenia rozpoznawczego (zakres rozpoznawanych częstotliwości);
T_p – czas przestrajania odbiornika w pełnym zakresie częstotliwości;
T_i – okres powtarzania impulsów rozpoznawanych;
T_{od} – czas przestrajania odbiornika o szerokość jego pasma przepuszczania.

Rys. 14. Wykres ilustrujący zasadę przeszukiwania wolnego w częstotliwości

Poszukiwanie szybkie charakteryzuje się tym, że odbiornik urządzenia rozpoznawczego przestraja się w całym roboczym zakresie w czasie nie przekraczającym czasu jednego opromieniowania anteny urządzenia rozpoznawczego przez poszukiwaną stację radiolokacyjną (czasu trwania odbieranego sygnału – rys. 15).



τ_i – czas trwania odbieranego sygnału;
Δf_0 – szerokość pasma odbiornika urządzenia rozpoznawczego;
Δf_r – zakres przestrajania odbiornika urządzenia rozpoznawczego (zakres rozpoznawanych częstotliwości);
T_p – czas przestrajania odbiornika w pełnym zakresie częstotliwości.

Rys. 15. Wykres ilustrujący zasadę przeszukiwania szybkiego w częstotliwości

Szybkość przestrajania odbiornika w tym przypadku musi być bardzo duża (setki i tysiące megaherców na sekundę). Jest ona ograniczana dopuszczalnymi granicami zmniejszania czułości, dokładności i rozróżnialności przy określaniu częstotliwości wprowadzanymi przez bezwładność układów rezonansowych odbiornika.

Ze względu na wzajemną zależność między pasmem przepuszczania układu rezonansowego i szybkością przestrajania zwiększenie szybkości przestrajania wywołuje pogorszenie dokładności pomiaru częstotliwości nośnej i zmniejszenie czułości. Każdej szybkości przestrajania odpowiada optymalna szerokość pasma przepuszczania odbiornika. Skracając czas poszukiwania, tracimy na dokładności określania częstotliwości i odwrotnie: zwiększając dokładność określania częstotliwości, musimy zwiększyć czas rozpoznawania.

Poszukiwanie z prędkością średnią jest to rodzaj poszukiwania w częstotliwości, w którym czas przestrajania odbiornika o szerokość jego pasma przepuszczania jest większy od czasu trwania rozpoznawanego sygnału i jednocześnie mniejszy od okresu powtarzania tych sygnałów. Jest to sposób najbardziej typowy dla rozpoznania systemów radiolokacyjnych. Charakterystyczną cechą tego rodzaju rozpoznania jest brak pewności wykrycia pracy impulsowej stacji radiolokacyjnej w ciągu jednego okresu przestrajania odbiornika rozpoznawczego. Innymi słowy, prawdopodobieństwo wykrycia rozpoznawanego sygnału jest dla tego przypadku w zasadzie zawsze mniejsze od jedności.

Proces poszukiwania i wykrywania prawdopodobnego (z prędkością średnią) realizuje się w ten sposób, że jeśli poszukiwanie i wykrywanie w kierunku jest prawdopodobne, to wykrywanie w częstotliwości musi być pewne. Może być też odwrotnie, a zależy to tylko od technicznych rozwiązań w budowie urządzenia rozpoznawczego. Powyższa zależność jest

konieczna, ponieważ połączenie dwu poszukiwań prawdopodobnych (iloczyn wartości prawdopodobieństw) daje w efekcie niedopuszczalnie niskie prawdopodobieństwo wykrycia.

Namierzanie w rozpoznaniu systemów radiolokacyjnych realizuje się w podobny sposób jak w przypadku rozpoznania radiowego. Pewna specyfika występuje w najczęściej stosowanych metodach namierzania, jak również problemach związanych z faktem, że anteny rozpoznawanych urządzeń zwykle obracają się (dookólnie lub sektorowo).

Metody namierzania w rozpoznaniu systemów radiolokacyjnych są ściśle powiązane z metodami wykrywania w kierunku. Jeżeli wykrywanie w kierunku realizowane jest metodą bez poszukiwania, to taką samą metodą realizuje się namierzanie. Przy wykrywaniu w kierunku metodą z poszukiwaniem namiary realizowane są zwykle metodą poszukiwania wolnego, a dokładny kąt ustalany metodą „na maksimum sygnału", „równosygnałową" lub połączeniem obu tych metod.

Metoda równosygnałowa polega na zrównywaniu ze sobą sygnałów odebranych równocześnie przez dwie kierunkowe i ustawione w stosunku do siebie pod pewnym kątem anteny urządzenia rozpoznawczego lub też dokonanie dwu namiarów przy pomocy jednej anteny odchylanej w dwie strony od kierunku maksymalnego sygnału. Dwusieczna otrzymanego w ten sposób kąta stanowi namiar na źródło emisji sygnału radiolokacyjnego.

W odniesieniu do stacji radiolokacyjnych prowadzących obserwacje sektorowo warunkiem namierzania jest dodatkowo szerokość sektora obserwacji tych stacji. W tym względzie może się tak zdarzyć, że sektor obserwacji będzie tak wąski, iż przemieszczająca się w nim antena stacji radiolokacyjnej opromieniowywać będzie tylko jedną stację rozpoznawczą z danej sieci. Kolejne stacje mogą już być nie opromieniowywane, a zatem wykluczone zostaną warunki namierzania.

Dodatkową trudność w namierzaniu stacji z obracającymi się antenami stanowi fakt, że sygnały od tych stacji odbierane są przez urządzenia rozpoznawcze systemu w różnym czasie, a różnica obioru przez kolejne stacje systemu jest uzależniona od szybkości obrotów anteny i może wynosić kilka sekund. Powoduje to oczywiście trudności w jednoznacznym określeniu położenia rozpoznawanej stacji, bowiem istnieje możliwość, że dwie stacje rozpoznawcze „widzą" dwa różne nadajniki pracujące na zbliżonych częstotliwościach i posiadające anteny o zbliżonej szybkości obrotowej. Warto zauważyć, że w odróżnieniu od środków łączności stacje radiolokacyjne mają zwykle niewielkie możliwości przestrajania w częstotliwości i w praktyce wiele stacji radiolokacyjnych może jednocześnie pracować na tej samej częstotliwości. Wyeliminowanie tych niejednoznaczności możliwe jest przez pomiar różnic czasu opromieniowania kolejnych stacji systemu rozpoznania lub też w nowoczesnych rozwiązaniach przez identyfikację konkretnego egzemplarza stacji radiolokacyjnej.

2.2.3. Rozpoznanie systemów radionawigacyjnych

Rozpoznanie systemów radionawigacyjnych polega na wykrywaniu systemów i środków radionawigacyjnych wykorzystywanych przez przeciwnika.

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

W klasyfikacji systemów radionawigacyjnych można wyróżnić kilka kryteriów podziału, m.in. ze względu na zasięg, dokładność i miejsce lokalizacji, zakresy wykorzystywanego widma częstotliwości czy cechy sygnałów.

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

Systemy bliskiej nawigacji obejmujące środki radiotechniczne rozmieszczone na lądzie (aparatach latających, okrętach) mają promień działania ograniczony do kilkuset kilometrów. Pracując w zakresie fal krótkich i ultrakrótkich, charakteryzują się stosunkowo dużą dokładnością.

Systemy nawigacji dalekiej obejmujące środki radiotechniczne rozmieszczone na lądzie (aparatach latających, okrętach) mają promień działania około kilku tysięcy kilometrów. W tych systemach są wykorzystywane podzakresy fal radiowych średnich, długich i bardzo długich, a za ich pomocą znacznie trudniej uzyskać dużą precyzję lokalizacji.

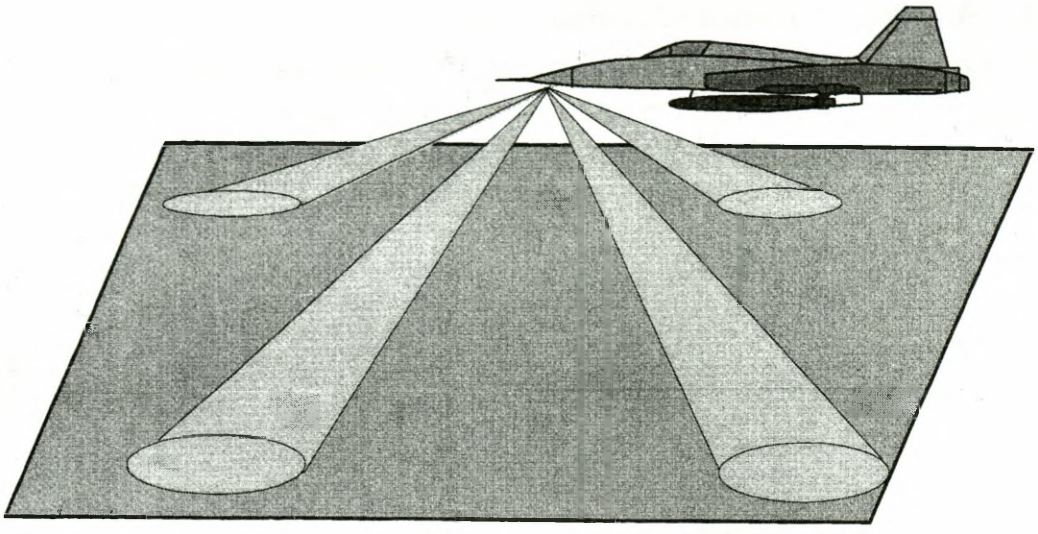
Możliwości prowadzenia rozpoznania systemów radionawigacji bliższej i dalszej są zdeterminowane przez zakresy częstotliwości, w których systemy te pracują oraz przez sposoby określania pozycji, a w szczególności przez wykorzystywanie pokładowych urządzeń zapytujących.

Ogólnie systemy radionawigacyjne podzielić możemy na:

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

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

W przypadku systemów autonomicznych, opartych o pokładowe stacje radiolokacyjne, możliwości i sposoby rozpoznania są identyczne jak w rozpoznaniu systemów radiolokacyjnych. Rozpoznanie jest jednak utrudnione ze względu na niewielki zasięg tych stacji oraz kierunek emisji promieniowania elektromagnetycznego, bowiem w urządzeniach pokładowych samolotów wiązki promieniowania są zwykle skierowane pod dużym kątem w dół (rys. 16).



Rys. 16. Rozkład wiązek pokładowego radiolokatora dopplerowskiego

Możliwości i zakres rozpoznania w przypadku systemów nieautonomicznych są zróżnicowane w zależności od zakresu wykorzystywanych częstotliwości i systemu uzyskiwania danych nawigacyjnych.

Bezkierunkowe radiolatarnie systemów hiperbolicznych (Loran, Decca, Omega) pracujące na falach średnich, długich i bardzo długich mogą być rozpoznawane za pomocą namierników radiowych pracujących w odpowiednich zakresach częstotliwości, podobnie jak kierunkowa radiolatarnia ultrakrótkofalowego systemu VOR.

W przypadku systemów odległościowych i kierunkowo–odległościowych, takich jak radiodalmierz DME czy systemy TACAN i RSBN, oprócz rozpoznawania radiolatarni istnieje również możliwość rozpoznawania pokładowych urządzeń zapytujących. Urządzenia te pracują w pasmie ok. 1000 MHz i mogą być rozpoznawane przy wykorzystaniu urządzeń rozpoznania systemów radiolokacyjnych.

2.3. Rozpoznanie radiolokacyjne

Rozpoznanie radiolokacyjne[12] jest prowadzone za pomocą stacji radiolokacyjnych, które służą do wykrywania powietrznych, naziemnych i nawodnych celów ruchomych i nieruchomych. Określają ich bieżące współrzędne, kierunek oraz prędkość ruchu na podstawie zdobytych i przetworzonych danych o obiektach, których nośnikami są fale elektromagnetyczne. Współczesne rozpoznanie radiolokacyjne obejmuje: systemy rozpoznania obszaru powietrznego, systemy nadzorowania pola walki, systemy kierowania ogniem, systemy obrony prze-

[12] Pasywne, jeżeli stacje radiolokacyjne przechwytują fale elektromagnetyczne, same zaś nie promieniują energii. Aktywne, jeżeli są dostosowane do zdobywania i przetwarzania tylko tych danych, których postacie stanowi odbita od różnych obiektów przeciwnika własna energia elektromagnetyczna.

ciwlotniczej, systemy rozpoznania powierzchni ziemi SLAR i inne. Prowadzone jest przez samoloty rozpoznawcze wyposażone w stacje radiolokacyjne oraz naziemne i okrętowe stacje radiolokacyjne pracujące w różnych zakresach częstotliwości. Dane pozyskiwane przez te urządzenia w kontekście budowy baz danych powinny dotyczyć:

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

– tras przelotu samolotów oraz obrazów radiolokacyjnych celów ruchomych (czołgów, transporterów opancerzonych, samochodów, pododdziałów oraz pojedynczych żołnierzy;

– współrzędnych tych celów.

W radiolokacji wykorzystywany jest głównie podzakres fal radiowych zwany zakresem mikrofalowym. Wszystkie obiekty, które mogą być wykryte za pomocą fal radiowych (samoloty, okręty, rakiety, infrastruktura naziemna, chmury itp.), nazywane są celami radiolokacyjnymi[13], a sygnał odbity od tych obiektów – echem radarowym lub echem radiolokacyjnym.

W siłach zbrojnych rozpoznanie radiolokacyjne zajmuje szczególne miejsce. Prowadzi się je we wszystkich rodzajach wojsk i niektórych rodzajach służb. Jest ono jednym z zasadniczych elementów składowych rozpoznania wojskowego.

Współczesne rozpoznanie radiolokacyjne szczebla taktycznego obejmuje m.in. systemy:

– rozpoznania obszaru powietrznego;

– nadzorowania pola walki;

– kierowania ogniem;

– obrony przeciwlotniczej;

– rozpoznania powierzchni ziemi.

Naziemne rozpoznanie radiolokacyjne szczebla taktycznego skupia się na obserwacji przestrzeni powietrznej, rozpoznaniu pola walki oraz kierowaniu ogniem artylerii – czyli dotyczy obiektów stałych i ruchomych przeciwnika oraz terenu z elementami infrastruktury.

Rozpoznanie radiolokacyjne może być prowadzone na małą (do 50 km) i dużą (do 500 km) głębokość, niezależnie od pory roku i doby oraz warunków meteorologicznych. Uzyskanie wymaganej głębokości rozpoznania zawsze zależy od prawidłowego doboru środków rozpoznania, ich możliwości technicznych oraz od rozmieszczenia tych środków w terenie stosownie do położenia wojsk przeciwnika, prawdopodobnych kierunków jego działania oraz rozpoznawanych obiektów i systemów radioelektronicznych.

Szczebel taktyczny może również korzystać z danych uzyskanych przez powietrzne rozpoznanie radiolokacyjne.

Powietrzne rozpoznanie radiolokacyjne ma na celu obserwację obiektów powietrznych oraz obserwację obiektów naziemnych stałych i ruchomych.

Najbardziej rozpowszechnione są stacje radiolokacyjne obserwacji przedniej półsfery (ostatnio również tylnej półsfery), lokalizujące zarówno obiekty powietrzne, jak i naziemne

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

(nawodne). Stacje te umożliwiają także kierowanie i naprowadzanie pocisków rakietowych typu „powietrze – ziemia" i „powietrze – powietrze".

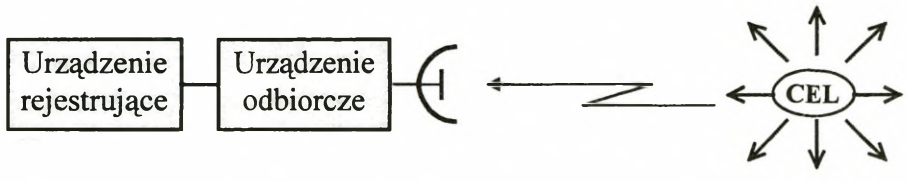
Występują również lotnicze SRL, które są wykorzystywane do nawigowania statkiem powietrznym, określania wysokości lotu lub identyfikacji „swój – obcy". Tendencją w konstrukcji nowoczesnych lotniczych stacji radiolokacyjnych jest ich wielozadaniowość, tzn. realizacja wielu funkcji przez jedną stację.

Powietrzne rozpoznanie radiolokacyjne jest prowadzone z dużych wysokości (od 5 do 12 tysięcy metrów) i obejmuje swoim zasięgiem znaczne obszary przestrzeni powietrznej, morskiej i lądowej.

Morskie rozpoznanie radiolokacyjne realizuje zadania związane ze zdobywaniem danych radiolokacyjnych o obiektach (siłach) morskich i wybrzeża morskiego, a także o obiektach lotnictwa morskiego przeciwnika i warunkach hydrometeorologicznych na morskim teatrze działań. Morskie rozpoznanie radiolokacyjne jest prowadzone przez autonomiczne urządzenia radiolokacyjne okrętów oraz SRL obserwacji brzegowej. Stacje te wykrywają i identyfikują obiekty nawodne, a także obiekty powietrzne nad akwenem morskim lub lądem w strefie wybrzeża morskiego. Oprócz wymienionych zadań służą też do kierowania środkami ogniowymi (rakietowymi).

Wyróżniamy dwa sposoby prowadzenia rozpoznania radiolokacyjnego: pasywne i aktywne.

Pasywne rozpoznanie radiolokacyjne polega na odbiorze energii elektromagnetycznej emitowanej przez obiekty w sposób niezamierzony i zamierzony (rys. 17).



Rys. 17. Idea radiolokacji pasywnej

Do sygnałów takich zalicza się:

– promieniowanie termiczne obiektów o temperaturze wyższej od zera bezwzględnego ($0^{O}K = -273{,}16^{O}C$);

– promieniowanie w zakresie fal radiowych, powstające przy pracy silników rakietowych, reakcjach jądrowych i wyładowaniach atmosferycznych;

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

Podstawową zaletą urządzeń radiolokacji pasywnej jest ich niewykrywalność. Nie mają żadnych urządzeń nadawczych, których sygnały mogłyby być odbierane przez urządzenia odbiorcze przeciwnika, więc w zasadzie są niewykrywalne.

Aktywne rozpoznanie radiolokacyjne jest oparte na własnych środkach emitujących w sposób zamierzony energię elektromagnetyczną. W radiolokacji aktywnej wykorzystuje się sygnały impulsowe i ciągłe.

Do zalet pracy w metodzie impulsowej należy zaliczyć możliwość generacji sygnału bardzo dużej mocy (rzędu megawatów) w postaci impulsu o czasie trwania rzędu milisekund przy stosunkowo małej mocy średniej nadajnika. Poza tym praca impulsowa pozwala na jednoczesne wykrywanie i pomiar współrzędnych dużej liczby obiektów oraz wykorzystywanie jednej anteny do nadawania i odbioru sygnałów.

Przy radiolokacji aktywnej w skład urządzenia radiolokacyjnego wchodzi nadajnik wytwarzający sygnały radiolokacyjne, odbiornik odbierający sygnały echa radiolokacyjnego oraz urządzenie zobrazowania.

Ze względu na sposób uzyskiwania sygnału echa wyróżnia się następujące rodzaje radiolokacji aktywnej:

– z pasywną odpowiedzią;

– z aktywną odpowiedzią;

– radiolokację półaktywną.

Radiolokacja aktywna z pasywną odpowiedzią polega na wykorzystaniu zjawiska odbijania fal radiowych od obiektu, a więc zdolności do pasywnej odpowiedzi. Odbity sygnał radiolokacyjny (echo) może zawierać dane o położeniu celu (współrzędne dwu- lub trójwymiarowe), parametrach ruchu (prędkości), a także o takich własnościach fizycznych, jak wymiary i kształt celu, jego przewodność itd.

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

$$R = \frac{ct}{2}$$

gdzie:

R – odległość od celu do urządzenia radiolokacyjnego (km);

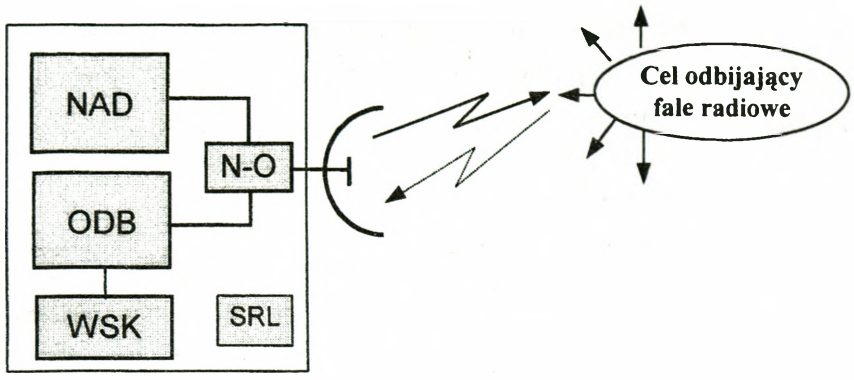
c – szybkość rozprzestrzeniania się fal radiowych (c ≈300 tys. km/s);

t – czas od wysłania do powrotu sygnału radiolokacyjnego (s).

Dane o współrzędnych kątowych celu uzyskuje się dzięki kierunkowym własnościom anten radiolokacyjnych oraz praktycznie prostoliniowemu rozprzestrzenianiu się fal.

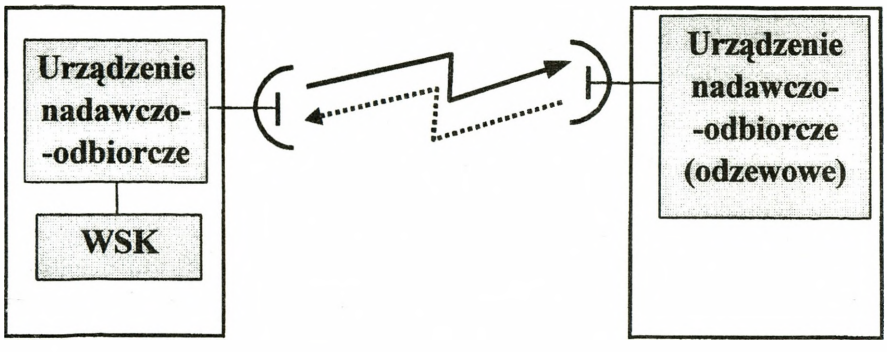
Uzyskanie danych o szybkości celu umożliwia zjawisko Dopplera, polegające na zmianie częstotliwości sygnału odbitego od ruchomego celu. Uzyskanie pozostałych danych umożliwia analiza odbitych sygnałów radiolokacyjnych.

Radiolokacja aktywna z pasywną odpowiedzią pozwala na wykrycie obiektu, który nie promieniuje energii elektromagnetycznej. Wykryty zostanie każdy obiekt, który odbija fale elektromagnetyczne, dlatego też ten rodzaj rozpoznania należy do najczęściej spotykanych w praktyce. Ideę radiolokacji aktywnej z pasywną odpowiedzią ilustruje rys. 18.



Rys. 18. Zasada pracy radiolokatora aktywnego z pasywną odpowiedzią

Radiolokacja aktywna z aktywną odpowiedzią polega na współpracy urządzenia radiolokacyjnego lub specjalnego urządzenia wywoławczego (zapytującego) z zainstalowanym na wykrywanym obiekcie urządzeniem odzewowym (odpowiadającym). Jest to urządzenie nadawczo-odbiorcze wraz z anteną, które po odebraniu słabych sygnałów wywoławczych powoduje automatyczne nadawanie sygnałów odzewowych o stosunkowo dużej mocy niekoniecznie na tej samej częstotliwości (rys. 19).



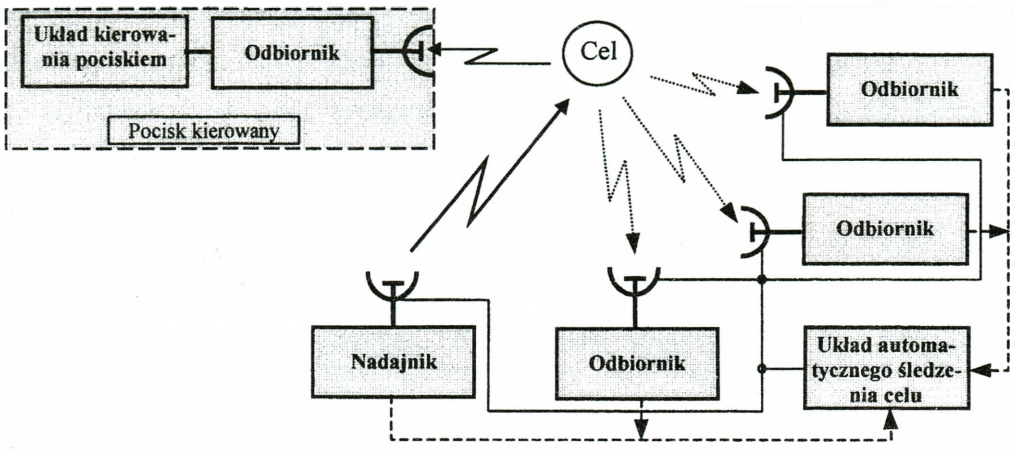
Rys. 19. Radiolokacja aktywna z aktywną odpowiedzią

Metodę tę wykorzystuje się do określenia przynależności państwowej samolotów, tzw. określenie „swój – obcy", lub też w systemach radionawigacyjnych. W przypadku gdy nosiciel urządzenia zapytującego wyśle sygnał zapytania, to urządzenie (radiolatarnia) odpowie na zapytanie, wysyłając sygnał zwrotny. Układy przeliczające określą wówczas miejsce położenia obiektu.

Radiolokacja półaktywna polega na stosowaniu dwu lub więcej stacji radiolokacyjnych, z których jedna jest przeznaczona do „oświetlania" celu, a druga do odbioru odbitych przezeń sygnałów (radiolokacja bistatyczna lub multistatyczna)[14]. Tego rodzaju urządzenia są wyko-

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

rzystywane do specjalnych zastosowań, jak np. dla ułatwienia naprowadzania pocisków kierowanych na cel lub wykrywania obiektów w technologii „stealth". Zasadę tego rodzaju radiolokacji przedstawia rys. 20.



Rys. 20. Radiolokacja półaktywna

Naziemna stacja radiolokacyjna może zawierać kilka urządzeń odbiorczych. Im większa ilość urządzeń odbiorczych, tym większe prawdopodobieństwo wykrycia obiektu o bardzo małej powierzchni skutecznej odbicia. Sygnały odbite od obiektu docierają do odbiorników radiolokacyjnych i po synchronizacji sygnałów można dokładne określić położenie obiektu, jego prędkość i kierunek poruszania. Podobnie jest przy kierowaniu pociskiem: sygnały odbite od obiektu są odbierane przez urządzenie odbiorcze w pocisku i wykorzystywane do naprowadzania go na obiekt (cel).

Cechą charakterystyczną urządzeń radiolokacyjnych jest wysyłanie przez nadajnik sygnału o stosunkowo dużej mocy oraz odbieranie odbitego od celu sygnału o znikomej mocy. Moc ta może być mniejsza od mocy sygnału nadawanego $10^{12} - 10^{11}$ i więcej razy. Oprócz opisanych powyżej urządzeń pracujących impulsowo wykorzystuje się również urządzenia pracujące na fali ciągłej, w których następuje jednoczesne wysyłanie sygnałów i odbiór echa. Wyodrębnienie odbitego sygnału następuje dzięki temu, że w punkcie odbioru ma on w danej chwili inną częstotliwość lub fazę od sygnału nadawanego.

Urządzenia pracujące na fali ciągłej można podzielić na:

a) urządzenia z falą ciągłą niemodulowaną:

– dopplerowskie;

– z przesunięciem fazowym;

– z kodowaniem fazowym.

b) urządzenia z falą ciągłą modulowaną:

– częstotliwościowo;

– szumem;

– ponadto z modulacją amplitudy i z modulacją fazy.

2.4. Rozpoznanie optoelektroniczne

Rozpoznanie optoelektroniczne ma na celu zdobywanie oraz przetwarzanie tych danych rozpoznawczych o przeciwniku, których nośnikami są fale elektromagnetyczne pasma optycznego[15].

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.

Do pracy w tym pasmie skonstruowano całą rodzinę urządzeń optoelektronicznych pozwalających na prowadzenie rozpoznania w ultrafiolecie, w zakresie promieniowania widzialnego oraz w zakresie bliskiej, średniej i dalekiej podczerwieni. Użytkowane są tutaj wszelkiego rodzaju urządzenia:

– telewizyjne;
– termowizyjne;
– noktowizyjne;
– oraz laserowe.

Telewizja - to dział telekomunikacji zajmujący się przekazywaniem na odległość, za pomocą elektrycznego kanału łączności, obrazów ruchomych wraz z towarzyszącym dźwiękiem. W celu przetworzenia obrazu optycznego na sygnał elektryczny wykorzystuje się zjawisko fotoelektryczne, natomiast dla odwrotnego przetworzenia wykorzystuje się zjawisko katodoluminescencji.

Termowizja – to postrzeganie obrazów w widmie promieniowania podczerwonego (aktualnie wykorzystywane są tylko dwa pasma tego widma: 3 – 5μm i 10 – 13 μm). Termowizja, w istocie wykorzystywanego zjawiska, podobna jest do noktowizji pasywnej. Różnica polega tylko na tym, że termowizja posiada jeszcze urządzenie skanujące zamieniające obraz widziany w podczerwieni na ciąg impulsów elektrycznych (noktowizor pasywny z urządzeniem skanującym można nazywać termowizorem).

Noktowizja - to dziedzina zastosowań techniki optoelektronicznej umożliwiającej widzenie w widmie promieniowania o długości 0,76 – 1000 μm. Zakres ten podzielono na podczerwień bliską 0,76 – 1,5 μm, średnią 1,5 – 5,6 μm i daleką 5,6 – 1000 μm (w dolnym pasmie podczerwieni dalekiej wyróżniany jest również zakres zwany podczerwienią skrajną). Obserwacja różnych obiektów w podczerwieni może być realizowana przez wykorzystywanie ich promieniowania własnego (wszystkie ciała, których temperatura jest wyższa od zera bezwzględnego, wysyłają własne niekoherentne promieniowanie podczerwone) lub odbitego. W związku z tym przyrządy noktowizyjne dzieli się na pasywne i aktywne.

---

[15] Pasmo optyczne (zakres optyczny) widma elektromagnetycznego stanowi promieniowanie: ultrafioletowe (długość fali: 0,01 – 0,38μm), widzialne (długość fali: 0,38 – 0,76μm) i podczerwone (długość fali: 0,76 – 1000μm).

Laser – to optyczny generator kwantowy lub generator światła spójnego, czy też źródło monochromatycznych fal elektromagnetycznych w zakresie optycznym (promieniowanie monochromatyczne to promieniowanie elektromagnetyczne o ustalonej długości fali). Nazwa „laser" została utworzona z początkowych liter angielskich słów: Light Amplification by Stimulated Emission of Radiation (wzmacniacz światła z wymuszoną emisją promieniowania).

2.5. Rozpoznanie czujnikowe

Rozpoznanie czujnikowe jest jednym z nowszych rodzajów rozpoznania elektronicznego. Ma na celu zdobywanie i przetwarzanie danych o przeciwniku, których nośnikami są fale sprężyste i inne zjawiska fizyczne i chemiczne. W zakresie fal sprężystych możemy wyróżnić:

– rozpoznanie akustyczne (z zakresem infradźwięków i ultradźwięków);

– rozpoznanie sejsmiczne.

Innym rodzajem rozpoznania czujnikowego jest rejestracja efektów zmian pola magnetycznego Ziemi oraz zjawisk chemicznych.

Informacje o przeciwniku i środowisku pola walki pozyskiwane z rozpoznania czujnikowego powinny dotyczyć:

– nadzorowania aktywności przeciwnika w wybranych rejonach zainteresowania;

– natężenia ruchu wzdłuż wybranych tras;

– nadzorowania planowanych rejonów zrzutu desantów taktycznych;

– rejestracji zmian w obrębie stanowisk i punktów dowodzenia;

– rejonów ogniowych artylerii i stanowisk startowych rakiet.

Rozpoznanie czujnikowe jest perspektywicznym rodzajem rozpoznania na szczeblu taktycznym, umożliwia bowiem pozyskiwanie danych z rejonów niedostępnych innym rodzajom rozpoznania w czasie zbliżonym do rzeczywistego.

2.6. Rozpoznanie informatyczne

Rozpoznanie informatyczne[16], z uwagi na masowy rozwój sieci informatycznych o zasięgu globalnym oraz lokalnym, powinno być prowadzone na wszystkich szczeblach dowodzenia. Sieci informatyczne mogą być bogatymi źródłami danych o siłach i środkach potencjalnego przeciwnika. Pozyskiwanie tych danych jest stosunkowo łatwe i w zasadzie nie wymaga specjalnych urządzeń ani też specjalistycznego przygotowania załóg. Potwierdzeniem tej tezy mogą być międzynarodowi piraci komputerowi (ang. *hackers*), którzy bez większych przeszkód włamują się do dobrze zabezpieczonych systemów komputerowych (m.in. Pentagonu). Nie trzeba zatem być bogatym państwem z rozbudowanym zapleczem nauko-

[16] W USA jest jednym z elementów walki informacyjnej.

wym, technicznym i technologicznym, aby skutecznie prowadzić rozpoznanie informatyczne. Bardzo bogatym i niezmiernie wartościowym źródłem danych rozpoznawczych jest samo promieniowanie niezabezpieczonego komputera. Przykładem możliwości rozpoznania informatycznego niech będą wspomniane systemy komputerowe Pentagonu. Hackerzy dokonują każdego roku 250 tysięcy włamań, z czego 65% kończy się powodzeniem. Departament Obrony Stanów Zjednoczonych przeprowadził badania, w ramach których przeprowadzono 8932 próby penetracji własnych systemów komputerowych. Powiodło się 88% prób penetracji, z tego tylko 320 włamań zostało wykrytych, a jedynie 22 zostały zgłoszone przez system zabezpieczający. Włamywacze dostają się do systemów komputerowych, ponieważ potrafią ominąć specjalne zabezpieczenia. Najczęściej włamanie jest zakończone powodzeniem, gdy wcześniej hackerzy monitorują wybraną sieć, a następnie podszywają się pod jeden z uprawnionych komputerów tej sieci i na podstawie przechwyconych informacji otwierają sobie „drzwi" do całego systemu. Włamywacze nie muszą korzystać wyłącznie z luk w systemach bezpieczeństwa. Mają możliwość „podglądania" interesującej ich sieci dzięki urządzeniom fabrycznie wbudowanym w sprzęt komputerowy. Mogą także przechwytywać emisję pola elektromagnetycznego generowanego przez monitor (np. głównego komputera w sieci) i na tej podstawie odtwarzać informacje wyświetlane na tym monitorze.

Doskonaląc systemy rozpoznania, należy obowiązkowo uwzględnić możliwość pozyskiwania różnorodnych danych, szczególnie w okresie pokoju, przez rozpoznanie informatyczne.

* *
*

Systemy elektroniczne przeciwnika mogą stanowić niewyczerpane źródła danych, z których przy dobrze zorganizowanym rozpoznaniu elektronicznym, można pozyskiwać dane rozpoznawcze w interesującym nas zakresie. Od informacji o przeciwniku nie mniej ważne są dane o położeniu i sytuacji własnych wojsk oraz skutkach ich działania. Ocenia się, że dopiero gruntowna i obiektywna analiza jednych i drugich grup danych oraz ich konfrontacja mogą zapewnić poprawne wnioskowanie i wypracowanie słusznych decyzji (komend).

System rozpoznania w działaniach taktycznych powinien terminowo zasilać procesy analityczne, decyzyjne i kontrolne wszechstronnymi danymi źródłowymi o sytuacji na polu walki, położeniu i działalności bojowej przeciwnika, stanie jego sił i środków, a także o terenie oraz warunkach atmosferycznych.

System rozpoznawczy związku taktycznego powinien:

– dostarczać dane w odpowiednim czasie i zakresie, zależnie od użytkownika, dla którego są przeznaczone;

– czerpać dane z innych podsystemów rozpoznania;

– określać przeznaczenie bojowe różnych obiektów i identyfikować cele;

– stanowić bazę dla prowadzenia WE przez gromadzenie danych niezbędnych do zakłócania i mylenia.

3. ZAKŁÓCANIE ELEKTRONICZNE

3.1. Istota zakłócania elektronicznego

Zakłócanie elektroniczne jest jednym z ważnych elementów składowych walki elektronicznej. Przedsięwzięcia zakłócania elektronicznego powinny ograniczać efektywne wykorzystanie przestrzeni elektromagnetycznej przez przeciwnika i w ten sposób wykluczyć lub ograniczyć jego możliwości dowodzenia i użycia środków walki.

Zakłócanie elektroniczne może też przyjmować formę *rażenia* lub *uderzenia elektronicznego* wyrażających zmasowane i kompleksowe użycie, w określonym czasie i miejscu, aktywnych środków WE w ścisłym powiązaniu z rażeniem ogniowym.

Na szczeblu taktycznym prowadzi się je w działaniach wszystkich wojsk, w różnych warunkach terenowych i meteorologicznych, w stosunku do środków elektronicznych, w które wyposażone są wojska przeciwnika.

Zasadniczymi obiektami zakłócania elektronicznego w działaniach taktycznych wojsk lądowych powinny być:

– w systemach łączności – urządzenia łączności radiowej KF i UKF;

– w systemach radionawigacyjnych – pokładowe i naziemne urządzenia odbiorczo-wskaźnikowe i odbiorcze danych nawigacyjnych;

– w systemach radiolokacyjnych – naziemne stacje radiolokacyjne rozpoznania pola walki, stacje naprowadzania rakiet i kierowania ogniem oraz pokładowe stacje radiolokacyjne lotnictwa i sił morskich;

– w systemach samonaprowadzania – urządzenia elektroniczne głowic samonaprowadzających się bomb, pocisków, rakiet, itp.;

– w systemach radiotelesterowania – różnego typu środki i urządzenia zapewniające zdalne sterowanie uzbrojeniem wojsk, samolotami bezpilotowymi oraz pociskami rakietowymi (przeciwpancernymi, przeciwlotniczymi itp.);

– w systemach optoelektronicznych – urządzenia elektroniczne prowadzące rozpoznanie w ultrafiolecie, w zakresie promieniowania widzialnego oraz bliskiej, średniej i dalekiej podczerwieni;

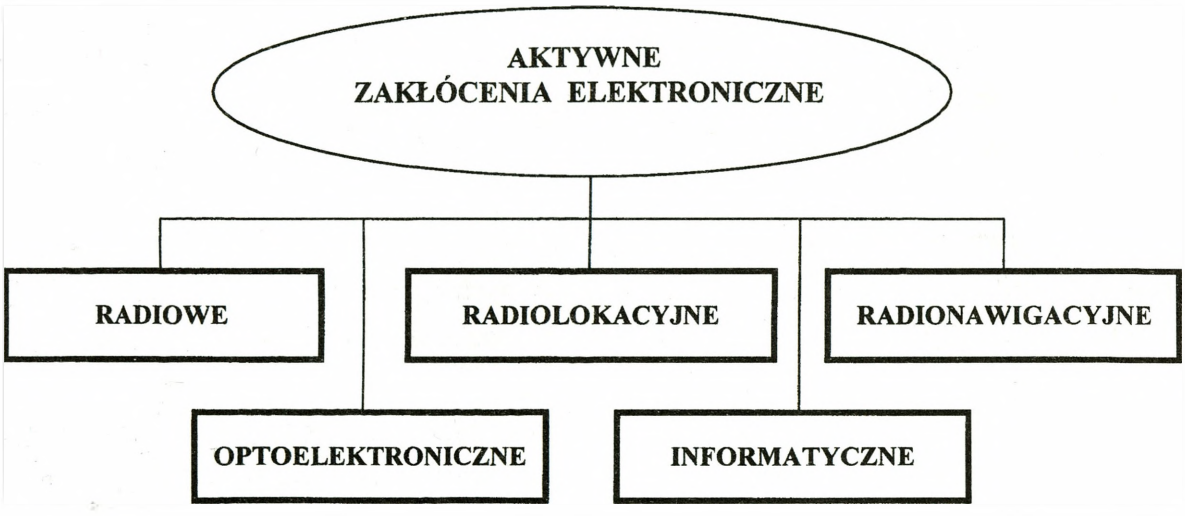
– w systemach informatycznych – sieci informatyczne rozległe i lokalne oraz zautomatyzowane miejsca pracy na stanowiskach dowodzenia przeciwnika.

Z uwagi na charakter powstawania wyróżnia się zakłócenia: przypadkowe[17] oraz celowe. Zakłócenia celowe są wytwarzane przez specjalne stacje (nadajniki) zakłócające lub pasywne retranslatory energii elektromagnetycznej. Wyodrębnia się zakłócenia celowe: aktywne, pasywne[18] i kombinowane (w przypadku jednoczesnego stosowania zakłóceń aktywnych i pasywnych).

3.2. Aktywne zakłócenia elektroniczne

Aktywne zakłócenia elektroniczne polegają na promieniowaniu przez urządzenie nadawcze zakłócającej energii elektromagnetycznej na częstotliwościach lub w pasmie pracy zakłócanych urządzeń odbiorczych.

Zakłóceniami aktywnymi oddziałuje się na urządzenia odbiorcze poszczególnych środków elektronicznych. Wyróżnia się zakłócenia (rysunek 21): radiowe, radiolokacyjne, radionawigacyjne, optoelektroniczne i informatyczne.



Rys. 21. Podział aktywnych zakłóceń elektronicznych

Zakłócenia radiowe polegają na celowym promieniowaniu zakłócającej energii EM powodującej utrudnienie w pracy środków radiowych przeciwnika. Zakłócenia radiowe użyte w sposób zmasowany mogą całkowicie zdezorganizować funkcjonowanie *systemów łączności*

[17] Zakłócenia przypadkowe powstają w wyniku oddziaływania zjawisk przyrodniczych (naturalne) oraz urządzeń technicznych na urządzenia elektroniczne, najczęściej podczas wyładowań atmosferycznych, oddziaływania zorzy polarnej lub wybuchów słonecznych, opadów atmosferycznych, pracy urządzeń przemysłowych, w tym: spawarek, urządzeń wyładowczych, źle zabezpieczonych silników elektrycznych. Powstają ponadto w rezultacie oddziaływania na środki elektroniczne polowych urządzeń elektrycznych lub w wyniku nieumiejętnego rozmieszczenia środków elektronicznych na stanowiskach dowodzenia. Zakłócenia przypadkowe mogą być również pochodzenia kosmicznego, powoduje je też, naturalne wewnętrzne szumy, powstające podczas pracy odbiorczych urządzeń elektronicznych. Zakłócenia przypadkowe mogą powstawać także wewnątrz aparatury.

[18] Zakłócenia pasywne są powszechnie wykorzystywane w pozorowaniu elektronicznym.

radiowej. Mogą bowiem uniemożliwić odbiór sygnałów, pogorszyć słyszalność, spowodować nieprawidłowe działanie urządzeń końcowych, wprowadzić w błąd operatorów lub zwiększyć błędy urządzeń automatycznych. Przy pomocy zakłóceń radiowych można utrudnić lub uniemożliwić pracę jednego urządzenia, kilku lub kilkunastu naraz, a nawet całego systemu łączności określonego szczebla dowodzenia. Zakłócenia radiowe są najbardziej ekonomicznym, a zarazem skutecznym sposobem dezorganizowania pracy systemów łączności przeciwnika.

Zakłócenia radiowe mogą być także wykorzystane do dezorganizacji pracy *urządzeń radiowych powodujących detonację bomb, rakiet i pocisków (radiozapalników)*. Mogą one spowodować przedwczesny wybuch lub niewybuch przez całkowite zablokowanie radiozapalnika. Zakłócenia radiowe należy zatem powszechnie stosować w działaniach taktycznych wojsk lądowych.

Zakłócenia radiolokacyjne[19] to niepożądane sygnały zniekształcające lub zakłócające sygnały użyteczne, stanowiące nośniki danych w systemach radiolokacyjnych. Mogą być prowadzone przeciwko wszystkim rodzajom radiolokacyjnych urządzeń rozpoznawczych oraz przeciwko środkom sterowania[20]. Zakłócenia radiolokacyjne powinno się szeroko wykorzystywać się w działaniach taktycznych wojsk lądowych z uwagi na pracę różnych stacji radiolokacyjnych przeciwnika w strefie taktycznej (do 20 km).

Zakłócenia radionawigacyjne obejmują środki i systemy radionawigacyjne (w tym bliskiej radionawigacji oraz systemy globalne). Zakłócenia radionawigacyjne systemów bliskiej radionawigacji z pewnością w przyszłości znajdą zastosowanie w działaniach taktycznych wojsk lądowych.

Zakłócenia optoelektroniczne[21] dotyczą środków rozpoznania i sterowania pracujących w podczerwieni, termolokatorów, urządzeń telewizyjnych oraz urządzeń laserowych. Z uwagi na coraz szersze wykorzystywanie tych środków w działaniach taktycznych wojsk lądowych należy przewidzieć stosowanie tego typu zakłóceń.

Zakłócenia czujnikowe[22] polegają na obezwładnianiu poszczególnych detektorów lub uniemożliwianiu ich pracy drogą dostarczania energii zakłócającej, odpowiadającej parametrami sygnałom bodźcowym charakterystycznym dla danego środowiska – akustycznego, magnetycznego, elektrycznego, chemicznego. Należy przewidzieć stosowanie tego typu zakłóceń w przyszłych działaniach taktycznych wojsk lądowych.

Zakłócenia informatyczne[23] stanowią perspektywiczny rodzaj oddziaływania elektronicznego (broni elektronicznej). Mogą być wykorzystywane przeciwko systemom informatycz-

---

[19] Etatowe siły i środki zakłóceń radiolokacyjnych występują na szczeblu operacyjnym.

[20] Środki sterowania obejmują urządzenia sterowania uzbrojeniem, samosterujące oraz urządzenia sterujące różnorodną techniką wojskową (rakietami, środkami bezpilotowymi, systemami rozpoznania itp.).

[21] Dotychczas brak jest sił i środków zakłóceń optoelektronicznych w SZ RP.

[22] Jest to perspektywiczny rodzaj zakłóceń elektronicznych.

[23] Zakłócenia informatyczne będą jednym z najważniejszych rodzajów zakłóceń prowadzonych w ramach walki informacyjnej w XXI wieku. Na przykład systemy komputerowe Departamentu Obrony USA stają się coraz częściej celem hackerów, którzy włamując się do komputerów Pentagonu, mają dostęp do informacji zastrzeżonych. Hackerzy dokonują każdego roku około 250 tysięcy włamań, z czego 65% kończy się powodzeniem.

nym w postaci tak zwanego zdalnie sterowanego wirusa. Ten komputerowy wirus ma kształt powtórzeń i zakłóceń programowych. Wprowadzany może być przez kanały radiowe i linie łączności światłowodowej łączące centralną jednostkę systemu z terminalami użytkowników. Może objawiać swoje działanie przez nieprawidłowe działanie niektórych programów, kasowanie pamięci, a także niezauważalne dla użytkownika dokonywanie zmian niektórych danych.

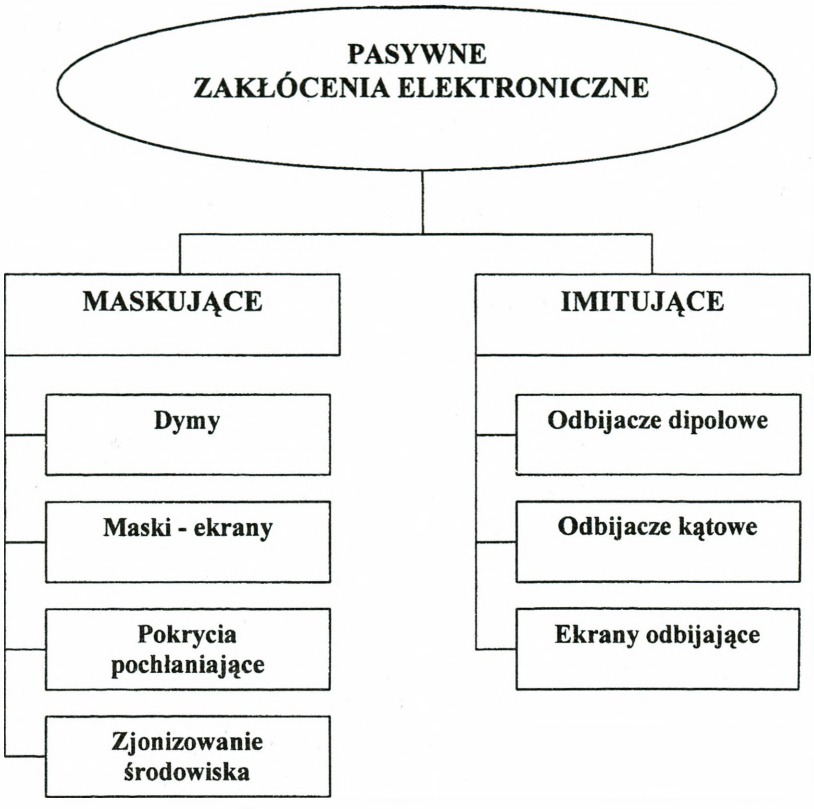
Jim Settle, konsultant ds. bezpieczeństwa FBI, jest przekonany, że przyszła wojna będzie polegać na blokowaniu dostępu do informacji i wprowadzaniu w błąd strony przeciwnej przez celowe ułatwienia w dostępie do fałszywych danych. W odróżnieniu od broni jądrowej środki walki informacyjnej są w zasięgu możliwości prawie każdego państwa. Celem tej walki będzie rozpoznanie a następnie obezwładnienie systemów komputerowych przeciwnika, tak aby nie był zdolny do podejmowania jakichkolwiek działań. Skoro systemy obrony większości państw są oparte na systemach komputerowych, aby przeprowadzić skuteczny atak, wystarczy zakłócić pracę takiego systemu.

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

3.3. Pasywne zakłócenia elektroniczne

Pasywne zakłócenia elektroniczne polegają na wtórnym promieniowaniu, odpromieniowaniu, odbijaniu, rozpraszaniu lub wchłanianiu energii elektromagnetycznej przez środki nie dysponujące generatorem energii EM. Prowadzone są w celu zmylenia systemów elektronicznych i odwrócenia uwagi przeciwnika. Zakłócenia pasywne dotyczą najczęściej środków radiolokacyjnych, środków pracujących w podczerwieni oraz urządzeń laserowych. Ze względu na sposób oddziaływania na urządzenia elektroniczne przeciwnika rozróżnia się zakłócenia *maskujące i imitujące* (rysunek 22).

Zakłócenia maskujące utrudniają lub uniemożliwiają przeciwnikowi wykrycie i obróbkę sygnału użytecznego. Przy ich zastosowaniu urządzenia rozpoznania elektronicznego przeciwnika rejestrują niepełny i niezgodny z rzeczywistością obraz pracy środków elektronicznych. Analiza oparta na tych danych może doprowadzić do wyciągnięcia fałszywych wniosków. Dla uzyskania efektu zakłóceń maskujących wykorzystuje się dymy metalizowane, ekrany maskujące, pokrycia przeciwradiacyjne, a także zjonizowanie środowiska. Zastosowanie środków wywołujących lokalną jonizację atmosfery powoduje zmianę jej właściwości elektromagnetycznych i stanowi barierę, podobnie jak różnego rodzaju przeciwradiacyjne ekrany. W przypadku ich użycia wyklucza się możliwość wykorzystania fal elektromagnetycznych do wszelkiego rodzaju pomiarów i przekazywania danych.



Rys. 22. Rodzaje zakłóceń pasywnych

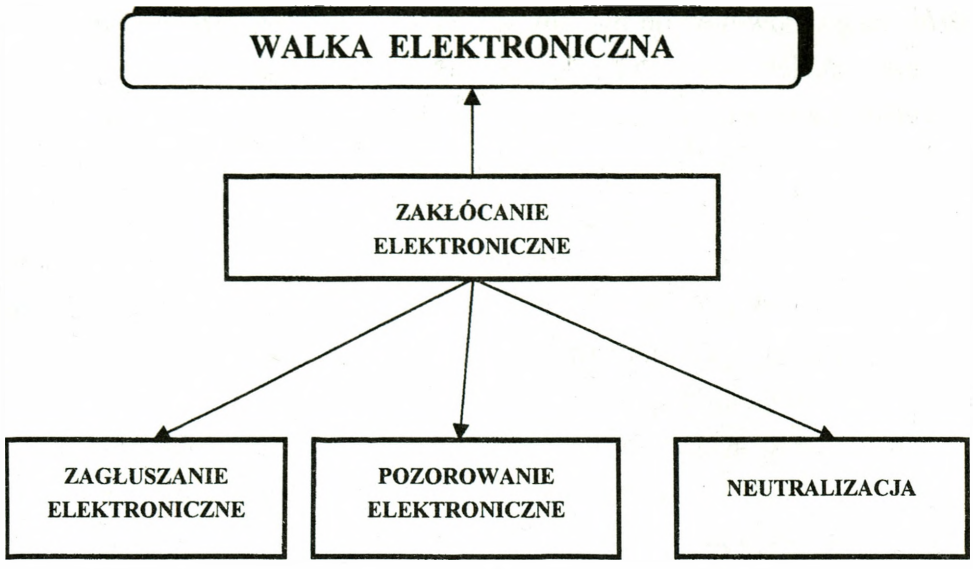
Zakłócenia imitujące wprowadzają do zakłócanego systemu fałszywe dane. Za ich pomocą można wytworzyć na ekranie wskaźnika stacji radiolokacyjnej zobrazowanie celu w takim azymucie i odległości, gdzie nie ma celów rzeczywistych. Zastosowanie tych zakłóceń dezorientuje przeciwnika oraz utrudnią mu podjęcie właściwej decyzji. Jako środki do wytwarzania imitujących zakłóceń pasywnych stosowane są odbijacze kątowe[24], odbijacze dipolowe[25], wszelkiego rodzaju pułapki i fałszywe cele radiolokacyjne.

Zakłócanie elektroniczne powinno być wykonywane przez: zagłuszanie elektroniczne, pozorowanie elektroniczne oraz neutralizację. Podział zakłócania elektronicznego przedstawiono na rysunku 23.

---

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

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



Rys. 23. Podział zakłócania elektronicznego

Największą efektywność zakłócania elektronicznego można osiągnąć w wyniku kompleksowego wykonywania różnego rodzaju oddziaływań elektronicznych w stosunku do najważniejszych środków i obiektów elektronicznych przeciwnika w sposób zmasowany, niespodziewanie, na głównych kierunkach i w decydujących etapach taktycznych.

Mając na uwadze potrzeby walki, należy wydzielić większość sił i środków zakłócania elektronicznego w rejon głównego wysiłku (na głównym kierunku) działania wojsk. Jest to niezbędne do wyeliminowania ważnych środków elektronicznych przeciwnika, a tym samym stworzenia dogodnych warunków do działań wojsk własnych.

3.4. Zagłuszanie elektroniczne

Zagłuszanie elektroniczne polega na celowym promieniowaniu energii elektromagnetycznej w celu osłabienia efektywności użycia odbiorczych urządzeń (systemów) elektronicznych wykorzystywanych przez przeciwnika.

Zagłuszanie elektroniczne powoduje dezorganizację pracy środków i systemów elektronicznych przeciwnika. W dużym stopniu może ograniczać zakres i możliwości ich wykorzystania przez poszczególne dowództwa, a ponadto – mimo, że nie powoduje bezpośrednich materialnych zniszczeń – w wielu sytuacjach jest przyczyną znacznych, często bezpowrotnych strat przeciwnika. Zagłuszanie elektroniczne należy prowadzić we wszystkich rodzajach wojsk, w każdych warunkach terenowych i meteorologicznych.

Realizowane jest przez stosowanie nadajników, emitujących aktywne sygnały zakłócające o strukturze zbliżonej do sygnałów użytecznych przeciwnika. Bardzo ważną rolę w procesie zagłuszania elektronicznego odgrywa *dobór odpowiedniego sygnału zakłócającego do*

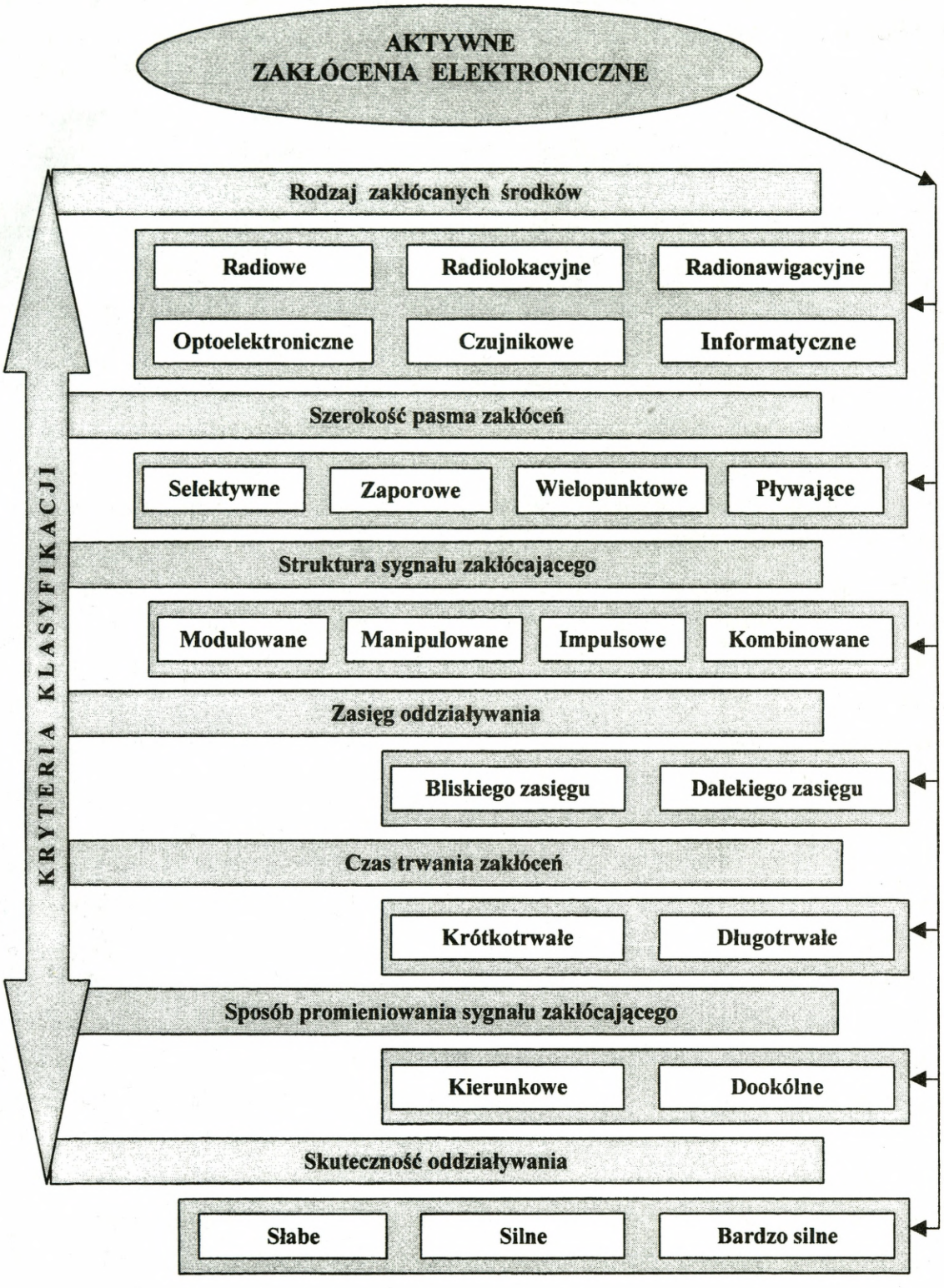
sygnału zakłócanego. Powinien on być dokonywany według poniższych kryteriów (sposoby klasyfikacji zakłóceń elektronicznych przedstawiono także na rysunku 24).

1. Ze względu na szerokość zakłócanego pasma:

- *Zakłócenia selektywne (wąskopasmowe, punktowe)* odznaczają się dużą dokładnością dostrojenia urządzeń stacji zakłócającej do częstotliwości roboczej zakłócanego środka elektronicznego. Przy stosowaniu tych zakłóceń nadajnik promieniuje sygnał zakłócający o szerokości pasma optymalnej do zakłócanego urządzenia. Zasadniczym zaś warunkiem, pozwalającym na realizację zakłóceń wąskopasmowych, jest dokładna znajomość częstotliwości roboczych poszczególnych środków elektronicznych przeciwnika. W działalności bojowej tego rodzaju zakłócenia stosuje się głównie w systemach wąskopasmowej łączności radiowej, radionawigacji oraz systemach telesterowania. Dokładność dostrojenia do częstotliwości nośnej emisji wąskopasmowych nie powinna być niższa niż 15-30 Hz.

Do podstawowych zalet zakłóceń wąskopasmowych można zaliczyć maksymalny zasięg zakłóceń (cała moc zakłóceń przypada na częstotliwość zakłócaną) oraz minimalny wpływ na pracę własnych stacji. Spośród wad najistotniejsze są: łatwość uniknięcia zakłóceń selektywnych, wymóg znajomości zakłócanej częstotliwości, mało efektywne wykorzystanie własnych środków zakłócających.

- *Zakłócenia zaporowe* (szerokopasmowe) są stosowane do obezwładniania jednocześnie kilku, kilkunastu lub jeszcze większej liczby środków elektronicznych. Za pomocą wielu nadajników lub nadajników zakłócających jednorazowego użycia można prowadzić zagłuszanie całych pasm częstotliwości wykorzystywanych przez przeciwnika. Zakłócenia takie stosuje się w przypadku słabego rozpoznania spektrum elektromagnetycznego przeciwnika. Zaporowe zakłócenia radiowe mogą być stosowane do zagłuszania środków łączności na szczeblu taktycznym. Celem zakłóceń zaporowych jest uniemożliwienie przeciwnikowi korzystania z częstotliwości roboczych w określonym pasmie (podzakresie). Zakłócenia zaporowe efektywnie oddziałują przeciwko szerokopasmowym źródłom emisji, wymagają minimalnego sterowania, mogą być wykorzystane do zakłócania wielu sygnałów, zmuszają do rekonfigurowania rozbudowanych sieci łączności – to ich podstawowe zalety. Do wad zaliczymy małą efektywność (wykorzystana moc nadajników rozkłada się proporcjonalnie na wszystkie częstotliwości zakłócanego pasma) i duże prawdopodobieństwo zakłócenia pracy własnych stacji.
- *Zakłócenia wielopunktowe* to zakłócanie pojedynczych częstotliwości. Ich główną zaletą jest zwiększona efektywność zakłócania w porównaniu z zakłócaniem selektywnym (punktowym).
- *Zakłócenia pływające* polegają na punktowo-zaporowym przemieszczaniu (przemiataniu) energii zakłócającej po zakłócanych częstotliwościach. Zasadniczymi zaletami zakłóceń pływających są: efektywne użycie zakłóceń przeciwko sieciom wieloczęstotliwościowym, skupienie (w danej chwili) całej mocy sygnału zakłócającego na jednej częstotliwości, duży zasięg zakłóceń, możliwość sterowania własnymi stacjami w celu uniknięcia zakłóceń wzajemnych. Skomplikowane technicznie urządzenia to główna wada tego rodzaju zakłóceń.



Rys. 24. Sposoby klasyfikacji aktywnych zakłóceń elektronicznych

2. Ze względu na strukturę sygnału zakłócającego:

- *Zakłócenia modulowane (szumowe)* to drgania wielkiej częstotliwości modulowane amplitudowo, częstotliwościowo lub fazowo. Najbardziej rozpowszechnionym rodzajem zakłóceń modulowanych są zakłócenia szumowe, charakteryzujące się przypadkowymi zmianami napięcia modulującego. Zakłócenia te są otrzymywane przez modulację drgań wielkiej częstotliwości sygnałem szumowym. Zakłócenia szumowe mogą być stosowane w celu zakłócenia wielu rodzajów pracy radiostacji, a przede wszystkim pracy fonicznej.
- *Zakłócenia manipulowane* to drgania wielkiej częstotliwości manipulowane ręcznie lub automatycznie amplitudowo, częstotliwościowo lub fazowo. Stosowane są najczęściej do zakłócania wąskopasmowych emisji telegraficznych z manipulacją amplitudy, częstotliwości lub fazy.
- *Zakłócenia impulsowe* to następujące po sobie krótkotrwałe impulsy modulowane w czasie trwania, amplitudzie, częstotliwości, fazie lub kilku parametrach jednocześnie. Zakłócenia te odznaczają się bardzo krótkim czasem promieniowania energii (rzędu mikrosekund). Są ciągami impulsów wielkiej częstotliwości, wytworzonymi przez nadajnik zakłócający na częstotliwościach zakłócanych środków radioelektronicznych. Jeśli częstotliwość powtarzania zakłóceń pokrywa się z częstotliwością powtarzania zakłócanej stacji, mamy do czynienia z zakłóceniami synchronicznymi. Jeżeli natomiast te częstotliwości się nie pokrywają, mówimy o zakłóceniach impulsowych niesynchronicznych. Zakłócenia te mogą być odzewowe (jednokrotne lub wielokrotne) albo niezależne (nieodzewowe). Zakłócenia impulsowe są wykorzystywane do zakłócania środków pracujących impulsowo, np. stacji radiolokacyjnych, stacji radioliniowych, urządzeń telesterowania itp.
- *Zakłócenia kombinowane* to drgania wielkiej częstotliwości modulowane i manipulowane równocześnie kilkoma sposobami, na przykład manipulacja impulsowa w połączeniu z modulacją szumami. Tego rodzaju zakłócenia stosowane są głównie do naruszania pracy środków radioliniowych oraz radiotelegrafii z przesuwem częstotliwości.

3. Ze względu na zasięg działania:

- *Zakłócenia bliskiego zasięgu* zapewniają skuteczne zagłuszanie i dezorganizację pracy środków elektronicznych przeciwnika na odległość do 10 km od miejsca pracy nadajnika lub stacji zakłócającej. Występują one podczas użycia nadajników zakłócających jednorazowego użycia, autonomicznych środków zakłócających oraz niektórych środków wykorzystywanych na szczeblach taktycznych.
- *Zakłócenia dalekiego zasięgu* zapewniają skuteczne zagłuszanie i dezorganizację pracy środków elektronicznych przeciwnika na odległość powyżej 10 km (nawet do kilkuset kilometrów). Taki zasięg zakłóceń uzyskuje się, wykorzystując naziemne i powietrzne stacje średniej (100–1000 W) i dużej mocy (powyżej 1000 W).

4. Ze względu na czas trwania:

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

• *Zakłócenia* długotrwałe polegają na zakłócaniu pracy środków elektronicznych w czasie od kilkunastu minut do kilku godzin. Stosowane są m.in. przy wykorzystaniu nadajników jednorazowego użytku.

5. Ze względu na sposób promieniowania:

• *Zakłócenia dookólne* występują wówczas, gdy promieniowanie anteny odbywa się we wszystkich kierunkach z jednakową mocą. Stosuje się je wtedy, gdy miejsca rozmieszczenia zakłócanych środków są nieznane, a ponadto w nadajnikach zakłócających jednorazowego użytku i często w stacjach pracujących w ruchu. Ujemną cechą zakłóceń dookólnych jest stosunkowo niski stopień efektywności wykorzystania energii wynikający ze znacznego jej rozproszenia.

• *Zakłócenia kierunkowe* występują wtedy, gdy energia EM jest promieniowana przez antenę stacji zakłócającej w kierunku zakłócanego środka elektronicznego przeciwnika. Osiąga się to przez stosowanie dobranych anten o charakterystyce kierunkowej. Dzięki kierunkowości anten istnieje możliwość uzyskania w punkcie odbioru większego natężenia pola energii zakłócającej. Zakłócenia kierunkowe zwiększają efektywność wykorzystania mocy nadajnika. Stosowanie takich zakłóceń jest konieczne w przypadku zagłuszania urządzeń o dużej kierunkowości anten oraz skomplikowanych strukturach sygnału.

6. Ze względu na skuteczność działania[26]:

• *Zakłócenia słabe,* przy których natężenie pola elektrycznego sygnału zakłócającego (Ez) w punkcie odbioru u przeciwnika jest większe od natężenia sygnału użytecznego (Es) i wynosi średnio 3-5% *(Ez>Es – średnio o 3-5%)*. Przy tego rodzaju zakłóceniach poziom zakłóceń w punkcie odbioru sygnału użytecznego powoduje obniżenie wiarygodności przesyłanych danych w granicach 5-15%. Oznacza to, że w rezultacie stosowania słabych zakłóceń występują tylko pewne zniekształcenia przekazywanych danych. W relacjach łączności jest utrudniony odbiór telegramów lub prowadzenie bezpośrednich rozmów. W zasadzie w większości wypadków odbiór jest możliwy przez doświadczonego operatora przygotowanego do pracy w warunkach zakłóceń. Istnieje potrzeba powtarzania transmisji w granicach 10-15%. W urządzeniach radiolokacyjnych występują utrudnienia w odróżnieniu celu.

• *Zakłócenia silne* to takie, przy których natężenie pola elektrycznego sygnału zakłócającego w punkcie odbioru po stronie przeciwnika jest większe o 5-15 % od natężenia pola elektrycznego sygnału użytecznego środka elektronicznego przeciwnika *(Ez>Es o 15-50%)*. Tego typu zakłócenia powodują utratę lub obniżenie wiarygodności danych od 15 do 50 %. Oznacza to, że w relacjach łączności będzie poważnie utrudniony odbiór, a nawet nastąpi utrata znacznej części danych. W najnowszych systemach może dojść do zerwania synchronizacji ich pracy. W systemach radiolokacyjnych na ekranach wskaźników w znacznym stopniu będzie ograniczona widzialność i rozróżnialność celów. Zamiast celów rzeczywistych mogą pojawiać się cele pozorne, nieczytelne sektory i pasy, obejmujące do 50% ekranu.

---

[26] Metodyka oceny skuteczności zakłóceń elektronicznych jest zamieszczona w pracy pt. *Walka elektroniczna w działaniach taktycznych wojsk lądowych,* AON, Warszawa 1999.

- *Zakłócenia bardzo silne* (tłumiące), przy których natężenie pola elektrycznego sygnału zakłócającego w punkcie odbioru jest ponad 50% wyższe od natężenia pola elektrycznego sygnału użytecznego *(Ez> Es ponad 50%).* Przy tego rodzaju zakłóceniach poziom zakłóceń w punkcie odbioru jest tak wysoki, że powoduje całkowitą utratę danych.

3.5. Pozorowanie elektroniczne

Pozorowanie elektroniczne to zespół przedsięwzięć i działań ukierunkowanych na ukrywanie rzeczywistych zamiarów własnych wojsk. Polega na użyciu energii elektromagnetycznej do emisji fałszywych danych i sygnałów elektromagnetycznych maskujących sygnały użyteczne oraz na odpowiednim odbijaniu lub tłumieniu sygnałów, w sposób mający na celu zmylenie przeciwnika w zakresie wykorzystania danych pozyskanych przez jego systemy elektroniczne. W pozorowaniu elektronicznym wykorzystuje się w szerokim zakresie pasywne zakłócenia elektroniczne.

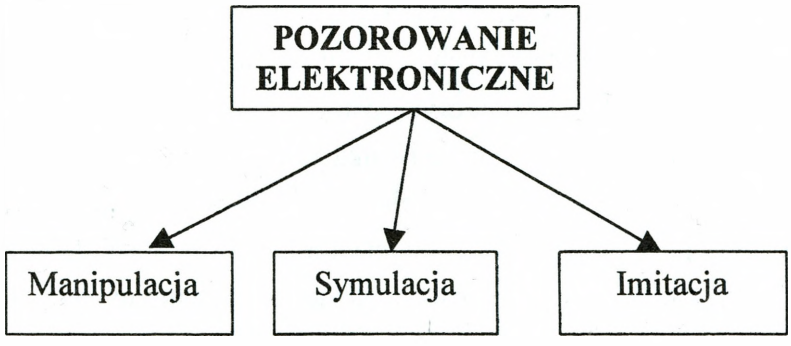
Pozorowanie elektroniczne stanowi część ogólnego planu wprowadzania przeciwnika w błąd. Wymaga zwykle scentralizowanej koordynacji i kierowania, dlatego w działaniach taktycznych wojsk lądowych działania pozorujące mają zastosowanie w ograniczonej skali i w określonych kluczowych okresach walki.

Wybrane elementy pozorowania elektronicznego w działaniach taktycznych WL (rys. 25) realizuje się poprzez:

– manipulację;

– symulację;

– imitację.



Rys. 25. Sposoby pozorowania elektronicznego

Manipulacja[27] polega na zmianie profili rozmieszczenia własnych środków elektronicznych w celu uniemożliwienia przeciwnikowi rozpoznania sygnałów, np. przez emisję fałszywych informacji we własnych relacjach łączności oraz tworzenie pozornych relacji łączności. Stosując manipulację, należy mieć na uwadze fałszywe poziomy promieniowania energii dotyczącej ruchu wojsk własnych, a także zmiany parametrów obiektów oraz kontrolowane zerwania i naruszenia zasad wymiany radiowej (wyłomy, przekroczenia, naruszenia, wyciek spreparowanych informacji związanych z działaniami bojowymi lub etapami walki).

Realizacja przedsięwzięć w zakresie manipulacji wymaga odpowiedniej zmiany własnego elektronicznego rozkazu bojowego. Powinna być ostrożnie planowana i realizowana tylko wtedy, kiedy przeciwnik będzie działał tradycyjnie przeciwko naszym wojskom[28].

Symulacja[29] to elektroniczna prezentacja własnych sił (całych lub części systemów elektronicznych) w innych miejscach niż znajdują się one w działaniach rzeczywistych (w trakcie trwania tzw. ciszy radiowej). Jej celem jest przeciwdziałanie rozpoznaniu elektronicznemu ugrupowania wojsk własnych, rozmieszczenia środków, możliwości oraz zamiarów. Do prowadzenia symulacji niezbędne są dodatkowe siły i środki elektroniczne. Główną cechą symulacji jest fałszywa lokalizacja obiektów (tzw. obiektów pozornych).

Imitowanie[30] polega na upodobnieniu sygnałów zakłócających do sygnałów użytecznych emitowanych przez przeciwnika. Za jego pomocą można wytworzyć na ekranie wskaźnika stacji radiolokacyjnej zobrazowanie celu w takim azymucie i odległości, gdzie nie ma celów rzeczywistych. Zastosowanie tych zakłóceń dezorientuje użytkownika oraz utrudnia podjęcie właściwych decyzji.

3.6. Neutralizacja

Neutralizacja polega na celowym użyciu energii elektromagnetycznej o dużej gęstości mocy do chwilowego uszkodzenia, jak i stałego zniszczenia urządzeń elektronicznych przeciwnika.

Badania nad wzbudzaniem silnych impulsów EM (niszczących) środkami klasycznymi wskazują, że należy zwrócić szczególną uwagę na ten problem. Impuls EM wywołuje krótkotrwałe wzbudzenie bardzo dużych napięć (prądów) w aparaturze elektronicznej, powodując uszkodzenie (przegrzewanie) wrażliwych elementów tej aparatury: układy scalone, tranzysto-

[27] Dotychczas w SZ RP w odniesieniu do systemów łączności i radionawigacyjnych używano pojęcia „dezinformacja radiowa".

[28] Potencjalny przeciwnik zawsze zbiera wiadomości o emisjach elektromagnetycznych w czasie pokoju i obserwuje każdą z nich oddzielnie podczas np. specjalistycznych ćwiczeń.

[29] Dotychczas w SZ RP wykorzystywano pojęcie „mylenie radioelektroniczne".

[30] W teorii walki elektronicznej w SZ RP imitowanie w odniesieniu do środków łączności i radionawigacji utożsamiane było z dywersją elektroniczną, którą uznawano za specyficzną formę obezwładniania elektronicznego, polegającą na przekazywaniu danych przeciwnikowi w taki sposób, aby odbierający nie zorientował się, że pochodzi ona ze stacji przeciwnika, a przekazaną treść przyjął jako prawdziwą.

ry, diody itp. Przyszłe bomby impulsowe charakteryzować się będą zatem dużymi mocami promieniowania, ponad tysiąc razy większymi niż klasyczne środki WE. W literaturze fachowej otrzymały już miano superśrodka zakłócającego. Napływające sygnały o badaniach tego zjawiska wykazują, że środkami tymi może być porażona aparatura elektroniczna na znacznym obszarze oraz urządzenia wykonane w technologii „stealth".

Środkami niszczącymi EM dużej gęstości mocy mogą być zarówno urządzenia mikrofalowe, jak i laserowe. Można je wykorzystywać do niszczenia środków elektronicznych, szczególnie czułych na to zjawisko systemów termowizyjnych i czujników laserowych, a także innej wrażliwej na takie oddziaływanie aparatury.

3.7. Znaczenie zakłócania elektronicznego

Zakłócanie elektroniczne stanowi bardzo skuteczny sposób dezorganizacji pracy i działania różnorakich środków i systemów elektronicznych wykorzystywanych w dowodzeniu wojskami i kierowaniu środkami walki przeciwnika. Ogranicza zakres i możliwości wykorzystania wyżej wymienionych systemów przez poszczególne dowództwa i sztaby, a ponadto w wielu sytuacjach jest przyczyną powstających u przeciwnika znacznych strat w sile żywej i sprzęcie bojowym.

W rezultacie zakłócania elektronicznego środków i systemów elektronicznych przeciwnika następują zmiany w ilości danych przesyłanych do poszczególnych dowództw i sztabów oraz do wojsk wykonujących określone zadania bojowe. Często, mimo sprawności technicznej środków elektronicznych, w wielu ogniwach dowodzenia wystąpić może całkowita lub częściowa utrata danych albo opóźnienie w przekazywaniu wiadomości bojowych. Poza tym przekazywane dane mogą być w znacznym stopniu zniekształcone, zamazywane i deformowane. Występować może zmniejszenie ich ilości lub też zwiększenie w drodze imitowania. Do dowództw i sztabów (na stanowiska dowodzenia), do wojsk i środków walki będą docierać dane niepełne, wątpliwe, odznaczające się niskim stopniem wiarygodności. Przekaz danych może być też na pewien czas całkowicie przerwany. Brak danych lub niski stopień ich wiarygodności uniemożliwia lub utrudnia realizację terminowego, skoordynowanego i operatywnego dowodzenia wojskami i kierowania środkami walki. Obniża to sprawność bojową wojsk, ich siłę uderzeniową i skuteczność działań, uniemożliwia terminowe wykonanie zadań bojowych oraz bardzo często prowadzi do znacznych strat w sile żywej i sprzęcie bojowym.

Należy mieć na uwadze, że efekty zakłócania elektronicznego wzrastają w przypadku ścisłej koordynacji działań elektronicznych z oddziaływaniem ogniowym na wybrane obiekty elektroniczne. Czas zakłócania elektronicznego powinien być podporządkowany potrzebom

wykonania zadań ogniowych i manewrowych. Szczególnie jest to widoczne w walce z systemami obrony powietrznej i systemami dowodzenia wojsk lądowych.

Zakłócanie elektroniczne może być prowadzone selektywnie na wybrane obiekty i środki elektroniczne lub w sposób zmasowany na środki elektroniczne w wybranych rejonach. W takim przypadku wszystkie środki elektroniczne przeciwnika w tych rejonach podlegają obezwładnieniu.

Decyzja dowódcy o zakłócaniu zależy od wielu czynników. Kluczowym czynnikiem jest czas. Rozpoznanie i zakłócanie nie mogą być prowadzone jednocześnie w stosunku do tych samych węzłów łączności przeciwnika. Dowódca ZT musi decydować o priorytetach czasowych zakłócania, rozpoznania, rażenia ogniowego i innych aspektach działań taktycznych.

4. OBRONA ELEKTRONICZNA

4.1. Istota obrony elektronicznej

Obrona elektroniczna obejmuje odpowiednio skoordynowane działania podejmowane w celu efektywnego wykorzystania widma elektromagnetycznego przez własne wojska.

W aspekcie ogólnowojskowym obrona elektroniczna stanowi ważny rodzaj zabezpieczenia bojowego. W działaniach taktycznych wojsk lądowych jest realizowana przez odpowiednie zadania (zasadnicze i cząstkowe) dla dowództw, sztabów i wojsk, będących dysponentami i użytkownikami środków elektronicznych. Większość środków elektronicznych stanowi materialną i funkcjonalną bazę systemu dowodzenia wojskami i kierowania środkami walki.

Celem obrony elektronicznej jest zachowanie ciągłości dowodzenia własnymi wojskami przez zachowanie żywotności środków i systemów elektronicznych w różnych warunkach pola walki.

Stanowi ona zespół przedsięwzięć organizacyjno-technicznych zapewniających stabilną pracę własnym systemom elektronicznym (rysunek 26).

Obrona elektroniczna obejmuje:

– obronę własnych systemów elektronicznych przed rozpoznaniem i zakłócaniem elektronicznym przeciwnika, niszczeniem ogniowym oraz bronią naprowadzającą się na źródła promieniowania elektromagnetycznego;

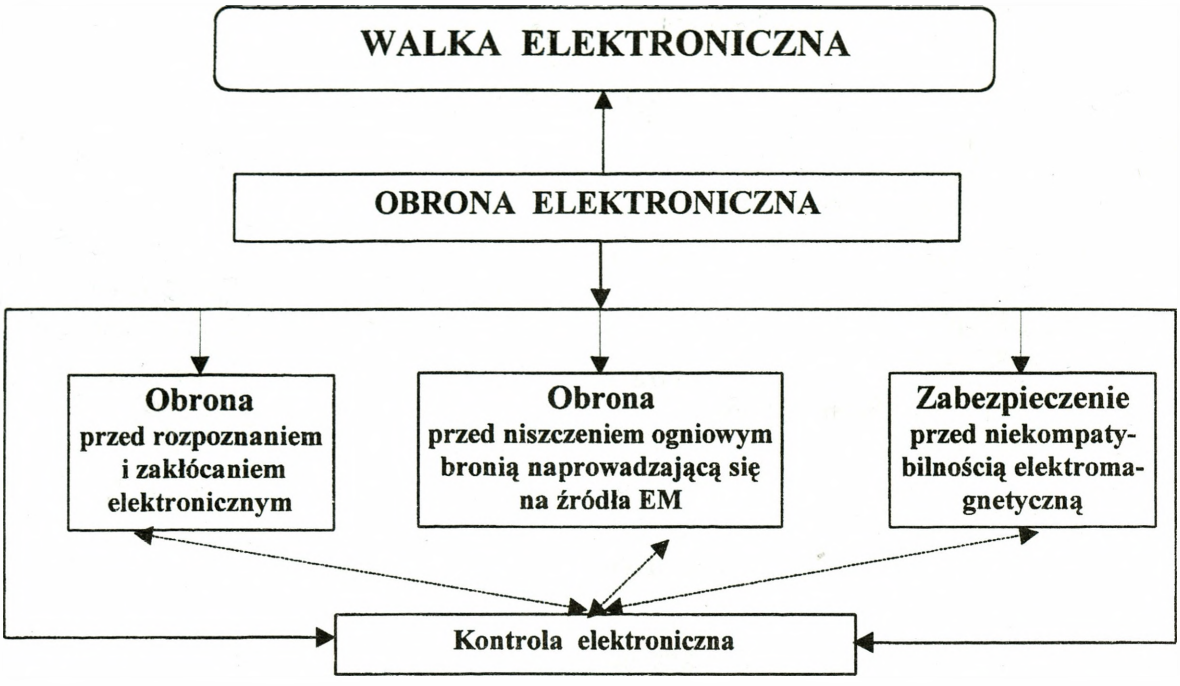
– zabezpieczenie przed niekompatybilnością elektromagnetyczną;

– kontrolę elektroniczną.

Możliwość realizacji przedsięwzięć obrony elektronicznej w działaniach taktycznych dywizji zależy m.in. od czasu przebywania elementów systemu elektronicznego w zasięgu oddziaływania środków przeciwnika. Realizacja zadań powinna się rozpocząć z takim wyprzedzeniem czasowym i przestrzennym, aby osiągnąć pełną efektywność działania, zanim wojska własne znajdą się w zasięgu określonego rodzaju elektronicznych środków walki przeciwnika[31].

Dokładne wyniki rozpoznania elektronicznego umożliwiają z dużym wyprzedzeniem czasowym przyjęcie odpowiedniego ugrupowania zaczepnego lub obronnego, wykonanie właściwego manewru ogniem i wojskami w celu stworzenia przewagi w określonych rejonach i na wybranych kierunkach prowadzenia działań bojowych.

[31] Należy nadmienić, że na użytek przyszłych działań zbrojnych zainteresowane strony z reguły prowadzą ciągłe rozpoznanie już w czasie pokoju oraz dokonują oceny zagrożenia elektronicznego. Wyniki rozpoznania określają potencjalnemu przeciwnikowi plan realizacji zadań walki elektronicznej, skierowanych na wykryte obiekty; mogą również służyć wypracowaniu danych do rażenia ogniem systemu dowodzenia strony przeciwnej.



Rys. 26. Zakres przedsięwzięć obrony elektronicznej

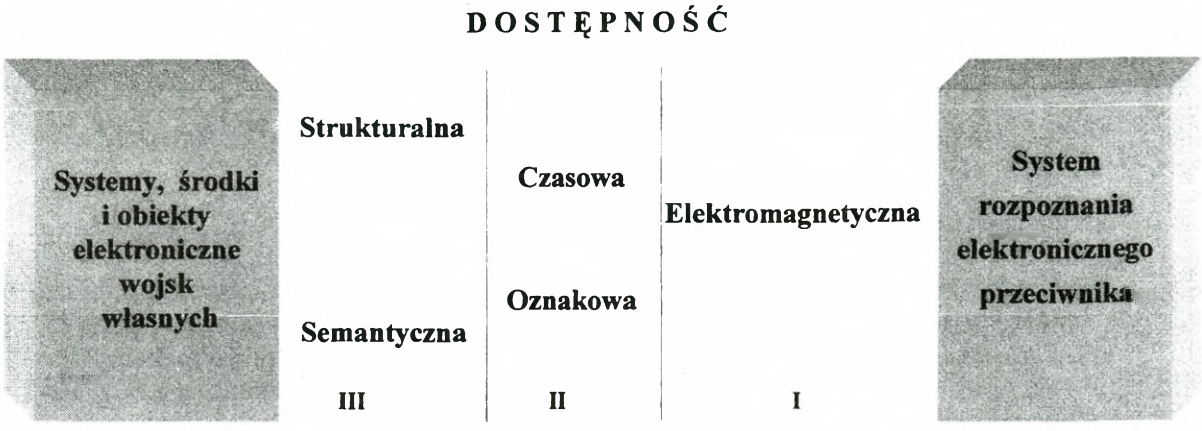
4.2. Obrona przed rozpoznaniem i zakłócaniem elektronicznym

W systemie dowodzenia wojsk lądowych w działaniach taktycznych można wyróżnić wiele różnorodnych i odrębnych elementów. Organizacja i funkcjonowanie tych elementów są uwarunkowane specyfiką techniki, spełnianej funkcji i przynależności do określonych dysponentów. Środki elektroniczne wykorzystywane w systemach dowodzenia można podzielić na:

- radiowe (KF, UKF, radioliniowe, satelitarne);
- radiolokacyjne;
- radionawigacyjne;
- optoelektroniczne;
- kablowe (przewodowe, światłowodowe);
- informatyczne.

Tak uszeregowane grupy środków elektronicznych wymagają odpowiedniej, specyficznej obrony i ochrony na polu walki, gdyż funkcjonują w warunkach zróżnicowanej dostępności. Dostępność środków i obiektów elektronicznych dla systemów rozpoznania elektronicznego przeciwnika przedstawiono na rysunku 27.

Dostępność elektromagnetyczna jest uzależniona od warunków energetycznych, tj. wymaganym stosunkiem poziomu sygnału do szumu na wejściu urządzenia rozpoznawczego. Środki elektroniczne są dostępne w ściśle określonym obszarze, który można określić jako strefę dostępności elektromagnetycznej.



Rys. 27. Dostępność środków i obiektów elektronicznych

Głębokość strefy dostępności elektromagnetycznej zależy od mocy nadajnika, rodzaju modulacji, wysokości wyniesienia (zawieszenia) anteny nadawczej i anteny odbiorczej urządzenia rozpoznawczego przeciwnika, a także od długości fali nośnej, jej polaryzacji oraz właściwości elektrycznych gruntu na trasie między źródłem a środkiem rozpoznania.

Dostępność czasową warunkują czasy trwania seansów radiowych oraz intensywność wymiany radiowej.

Dostępność oznakowa i strukturalna są uwarunkowane istnieniem cech (oznak, właściwości) demaskujących pracę środków i systemów elektronicznych. Cechy te umożliwiają organom rozpoznania elektronicznego zidentyfikowanie sygnałów emitowanych przez te środki, a przez to ich lokalizację, określenie składu sieci (linii) i węzłów łączności oraz ich przynależności do szczebla dowodzenia.

Dostępność semantyczna jest zależna od stopnia utajnienia wiadomości przekazywanych w systemach elektronicznych.

Z uogólnionej oceny wynika, że do obiektów elektronicznych szczególnie wrażliwych i najmniej odpornych na rozpoznanie, a następnie zakłócanie, należą systemy radiowe krótkofalowe (KF), systemy radiolokacyjne oraz radionawigacyjne. Stosunkowo większą odpornością charakteryzują się systemy radiowe ultrakrótkofalowe (UKF) małej mocy oraz systemy radioliniowe. Najwyższą odpornością cechują się systemy kablowe (przewodowe, światłowodowe) i informatyczne.

Zadania obrony elektronicznej powinny uwzględniać zróżnicowaną dostępność, aby zagwarantować ciągłą pracę poszczególnych systemów elektronicznych. Zakres i sposób ich realizacji należy rozpatrywać w dwóch okresach: przygotowania walki oraz w toku jej prowadzenia.

W okresie przygotowania walki obrona przed rozpoznaniem i zakłócaniem elektronicznym przeciwnika powinna być organizowana przez:

1. Opracowanie dokumentów bojowych dla poszczególnych systemów i środków elektronicznych.

2. Wypracowanie koncepcji prowadzenia obrony elektronicznej. Opracowanie apendyksu do planu walki elektronicznej.

3. Opracowanie wykazu częstotliwości roboczych, zabronionych i zastrzeżonych, czasu pracy środków elektronicznych, sposobów zmiany rodzajów pracy, sposobów wykorzystania rezerwowych środków i kanałów łączności.

4. Tworzenie elementów pozornej sytuacji elektronicznej w rejonie walki. Zadania i przedsięwzięcia należy skoordynować w ramach planu maskowania.

5. Określenie sygnałów ostrzegania i przedsięwzięć do natychmiastowego wykonania.

W toku prowadzenia walki obrona przed rozpoznaniem i zakłócaniem elektronicznym polega na wykonywaniu przedsięwzięć zawartych w uprzednio opracowanych planach.

Obrona przed rozpoznaniem i zakłócaniem elektronicznym dzieli się na: obronę radiową, radiolokacyjną, radionawigacyjną, optoelektroniczną, czujnikową, informatyczną i maskowanie techniczne.

Obrona radiowa polega głównie na ograniczeniu pracy środków radiowych, ograniczaniu cech demaskujących urządzeń nadawczych, przestrzeganiu reżimów pracy i obowiązujących przepisów korespondencji radiowej, utajnianiu danych przekazywanych w sieciach i kierunkach radiowych.

Obrona radiolokacyjna ma na celu osłonę własnych środków radiolokacyjnych przed rozpoznaniem i zakłócaniem przeciwnika. Może ona sprowadzać się do zmiany potencjału informacyjnego określonych postaci sygnałów.

Obrona optoelektroniczna skupia się na stosowaniu osłon i filtrów szerokopasmowych na urządzenia pracujące w tym zakresie promieniowania elektromagnetycznego. Polega to np. na malowaniu wozów bojowych specjalnymi farbami. W czasie obserwacji celu w podczerwieni powstaje złudzenie polegające na zlaniu się widma podczerwieni obserwowanego celu z widmem tła. Środki metamorficzne powodują zmianę koloru pod wpływem warunków zewnętrznych (temperatury, natężenia oświetlenia). Obrona przed generatorami promieniowania mikrofalowego dużej mocy polega na uodpornieniu i izolowaniu układów, aby nie powstawała w nich energia cieplna. Ponadto stosuje się flary emitujące promieniowanie cieplne, mają one na celu zmylenie pocisków naprowadzanych na źródło ciepła. Mogą być wystrzeliwane ze specjalnie skonstruowanych zasobników. Flary charakteryzują się zdolnością prawie natychmiastowego uzyskiwania szczytowego poziomu energii promieniowania podczerwonego, a czas ich palenia wynosi z reguły cztery sekundy.

Obrona czujnikowa polega na ochronie przed rozpoznaniem i zakłócaniem własnych detektorów, które wykorzystują energię odpowiadającą parametrami sygnałom bodźcowym, charakterystycznym dla środowiska – akustycznego, magnetycznego, elektrycznego, chemicznego. Na przykład obrona przed generatorami infradźwięków opiera się na budowaniu tzw. miękkich zasłon, w celu absorpcji energii fali dźwiękowej, oraz tworzeniu tzw. pól ak-

tywnego hałasu. Istota ich działania polega na wytworzeniu fali dźwiękowej tej samej długości co fala atakująca, lecz odwróconej w fazie (o 180°). Zasadniczym problemem w stosowaniu tej broni jest stworzenie odpowiedniego zestawu specjalistycznych głośników oraz wzmacniaczy, które wymagają m.in. bardzo wydajnych układów chłodzenia.

Obrona informatyczna obejmuje ochronę przed wirusami, koniem trojańskim, bombami logicznymi, robakami i bakteriami.

Ochrona przed „wirusami" to przede wszystkim niedopuszczanie do ładowania systemu z dyskietek niewiadomego pochodzenia. Należy pamiętać o tym, aby w stacji dysków podczas uruchamiania nie było żadnej dyskietki (wszystkie płyty główne mają obecnie funkcję umożliwiającą wybranie pierwszego dysku, włączającego system; dzięki tej funkcji nawet pozostawiona w stacji dyskietka z wirusem przestaje być groźna). Wirus zarażonego komputera można usunąć, uruchamiając system z czystej, niezawirusowanej dyskietki i zastępując zainfekowany sektor startowy czystym.

Najlepszą metodą unikania „konia trojańskiego" jest nieuruchamianie żadnego programu ani skryptu, dopóki się nie przeczyta dokładnie całego pliku. Do czytania pliku należy stosować program czy edytor, który wyświetla kody sterujące w widoczny sposób. Nie należy również uruchamiać programu, którego czytanie nie wyjaśnia wszystkich pojawiających się wątpliwości.

Ochrona przed „złośliwymi bombami" 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 „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 i królikami" polega na zachowaniu szczególnej ostrożności w stosunku do importowanych programów zarówno w postaci kodów źródłowych, jak i w postaci skompilowanej z nieznanych źródeł.

Maskowanie techniczne na współczesnym polu walki jest realizowane w szerokim zakresie widma promieniowania elektromagnetycznego, to jest od ultrafioletu do pasma mikrofalowego. Występuje ono w obronie radiowej, radiolokacyjnej i optoelektronicznej. Do najczęściej stosowanych środków maskujących należy zaliczyć:

– siatki (pokrycia) maskujące (zespołowe środki maskowania) wykonane z tworzyw sztucznych i tkanin bawełnianych;

– farby do malowania deformującego (farby na dyspersji alkidowej, poliuretanowej, farby rozpuszczalne w wodzie);

– zestawy do maskowania sprzętu bojowego (zestawy Barracuda, składające się z kilku dużych parasoli ustawionych bezpośrednio na sprzęcie lub obok niego oraz tzw. maski deformujące);

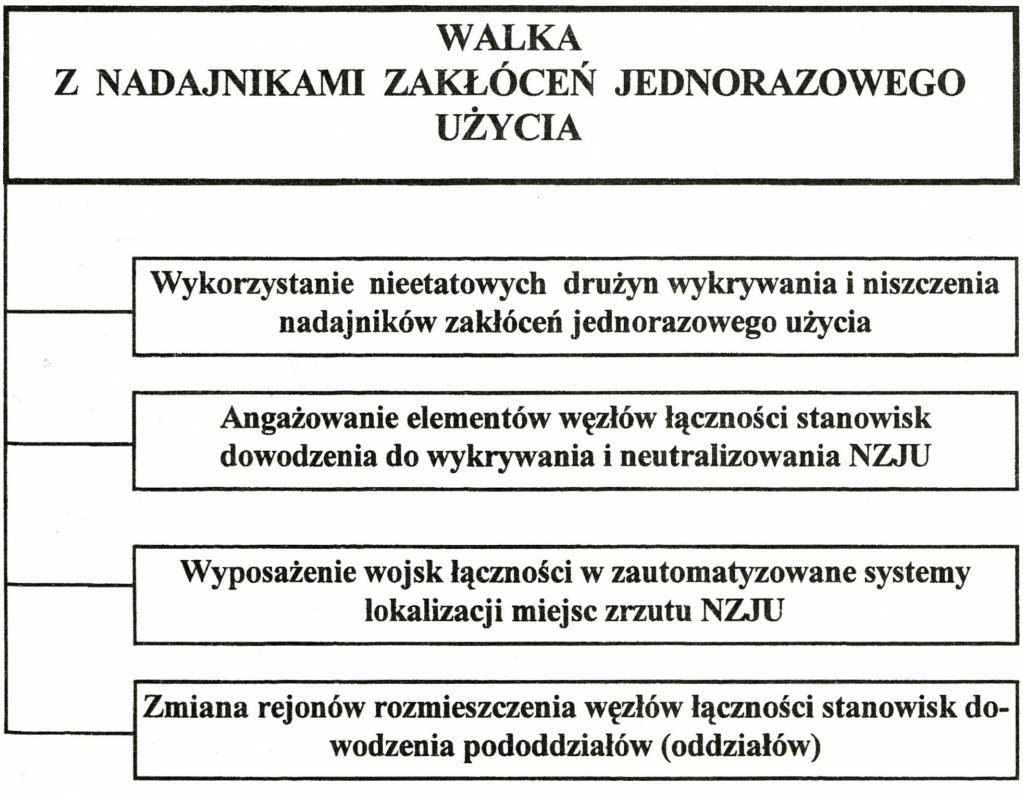
– środki maskowania przeciwradiolokacyjnego (pokrycia przeciwradiolokacyjne w postaci siatek oraz różnego rodzaju materiały radioabsorpcyjne, paski folii metalowej);

– środki do maskowania przed rozpoznaniem termalnym (osłony termiczne, maty tekturowe, ekrany termoizolacyjne);

– piany maskujące (krótkotrwałe, trwałe, emisyjne);

– środki systemu maskowania aktywnego (urządzenia ostrzegające o opromieniowaniu obiektu wiązką laserową lub radiolokacyjną, wyrzutnie środków dymnych, wyrzutnie substancji i ładunków emitujących energię cieplną, cele radiolokacyjne).

Szczególnie trudnym zadaniem, wymagającym rozwiązań zarówno organizacyjnych, jak i technicznych, jest *walka z nadajnikami zakłóceń jednorazowego użycia (NZJU)*. Zespoły węzłów łączności powinny umieć je wykrywać, niszczyć lub neutralizować, bądź też wychodzić poza strefy skutecznego ich oddziaływania. Zestaw działań w tym zakresie przedstawiono na rysunku 28.



Rys. 28. Walka z nadajnikami zakłóceń jednorazowego użycia

Neutralizowanie nadajników polega na ekranowaniu za pomocą, np. lekkich metalizowanych siatek, cienkich arkuszy folii aluminiowej lub kilku 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*. Należy mieć na uwadze fakt, że wyżej wymienione systemy pelengacyjne powinny mieć możliwość odróżniania sygnałów pochodzących z NZJU od sygnałów emitowanych przez własne nadajniki. Natomiast *na niższych szczeblach dowodzenia (kompania, batalion, a nawet brygada) należy przewidywać zmianę rejonów rozmieszczenia węzłów łączności z chwilą pojawienia się zakłóceń emitowanych przez te nadajniki.*

4.3. Obrona przed niszczeniem ogniowym oraz bronią naprowadzającą się na źródła promieniowania energii elektromagnetycznej

Do niszczenia ogniowego obiektów elektronicznych przeciwnik może użyć wszystkich rodzajów swojego lotnictwa, naziemnych sił rakietowych i artylerii polowej. Użycie poszczególnych rodzajów broni będzie ściśle uwarunkowane sytuacją taktyczną, a także zostanie dostosowane do różnych obiektów elektronicznych w celu uzyskania maksymalnych efektów. Należy mieć na uwadze, że obiektami rażenia ogniowego będą głównie środki elektroniczne rozmieszczone w strefie taktycznej, w szczególności stanowiska dowodzenia i węzły łączności oraz posterunki i stacje radiolokacyjne wykorzystywane do wykrywania i śledzenia celów powietrznych.

Obrona przed niszczeniem ogniowym i bronią naprowadzającą się na źródło promieniowania energii elektromagnetycznej powinna polegać w dużej mierze na:

– ograniczeniu czasu pracy stacji radiolokacyjnych i innych środków promieniujących energię elektromagnetyczną podczas promieniowania do celu – nosiciela rakiety (pocisku) samonaprowadzającej się;

– natychmiastowym wyłączeniu nadajników środków elektronicznych po zakończeniu strzelania do celów powietrznych i naziemnych;

– stosowaniu telewizyjno-optycznych metod wykrywania i śledzenia celów powietrznych i naziemnych;

– regularnym szkoleniu zespołów obsługujących środki elektroniczne w celu wyrobienia odporności psychicznej do działania w warunkach zagrożenia bronią samonaprowadzającymi się na źródło promieniowania;

– wszechstronnym wykorzystaniu ochronnych właściwości terenu;

– ciągłym maskowaniu i systematycznej rozbudowie fortyfikacyjnej.

4.4. Zabezpieczenie przed niekompatybilnością elektromagnetyczną

Zadanie to ma na celu zapewnienie kompatybilności elektromagnetycznej[32] w pracy własnych systemów i środków elektronicznych przez uniknięcie występowania szkodliwego i niepożądanego zjawiska interferencyjnych (wzajemnych) zakłóceń wewnętrznych lub zewnętrznych. Do głównych przyczyn powstawania zakłóceń interferencyjnych (wzajemnych) w pracy środków elektronicznych 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.

Obrona środków elektronicznych przed zakłóceniami interferencyjnymi powinna zmierzać do wyeliminowania lub maksymalnego zmniejszenia niepożądanego oddziaływania jednych środków na drugie. Zdolność tę można uzyskać przez wcześniejsze uzgodnienie wzajemnego działania środków elektronicznych. W tym celu należy podejmować odpowiednie działania organizacyjne i techniczne. Zestawienie przedsięwzięć z zakresu eliminacji zakłóceń interferencyjnych przedstawiono na rysunku 29.

Istotne znaczenie dla zapewnienia kompatybilności elektromagnetycznej ma rozśrodkowanie obiektów elektronicznych. Wybór miejsca pracy środków elektronicznych obejmuje wykorzystanie właściwości terenu (ukształtowanie, pokrycie i infrastrukturę) w celu zmniejszenia występowania wzajemnych zakłóceń z najbardziej zagrożonych kierunków. Warunki terenowe w rejonie rozwijania środków elektronicznych mogą wielokrotnie zmniejszać gęstość mocy energii elektromagnetycznej w przestrzeni, na której są przeszkody, np. las, zabudowa, konstrukcje metalowe. Umiejętne wykorzystanie terenu pozwoli obniżyć poziom wzajemnych zakłóceń lub całkowicie je wyeliminować. Rozwiązanie tego problemu powinno sprowadzać się do rygorystycznego przestrzegania przewidzianych dokumentami normatyw-

[32] Kompatybilność elektromagnetyczna pozwala na prawidłowe funkcjonowanie środków elektronicznych (z założoną jakością) w otaczającym je środowisku elektromagnetycznym, bez wywierania szkodliwego wpływu na to środowisko.

nymi odległości między środkami elektronicznymi, a zwłaszcza pomiędzy radiostacjami średniej mocy i stacjami radioliniowymi rozwijanymi w obrębie tego samego stanowiska dowodzenia (węzła łączności) lub w sąsiednich rejonach.

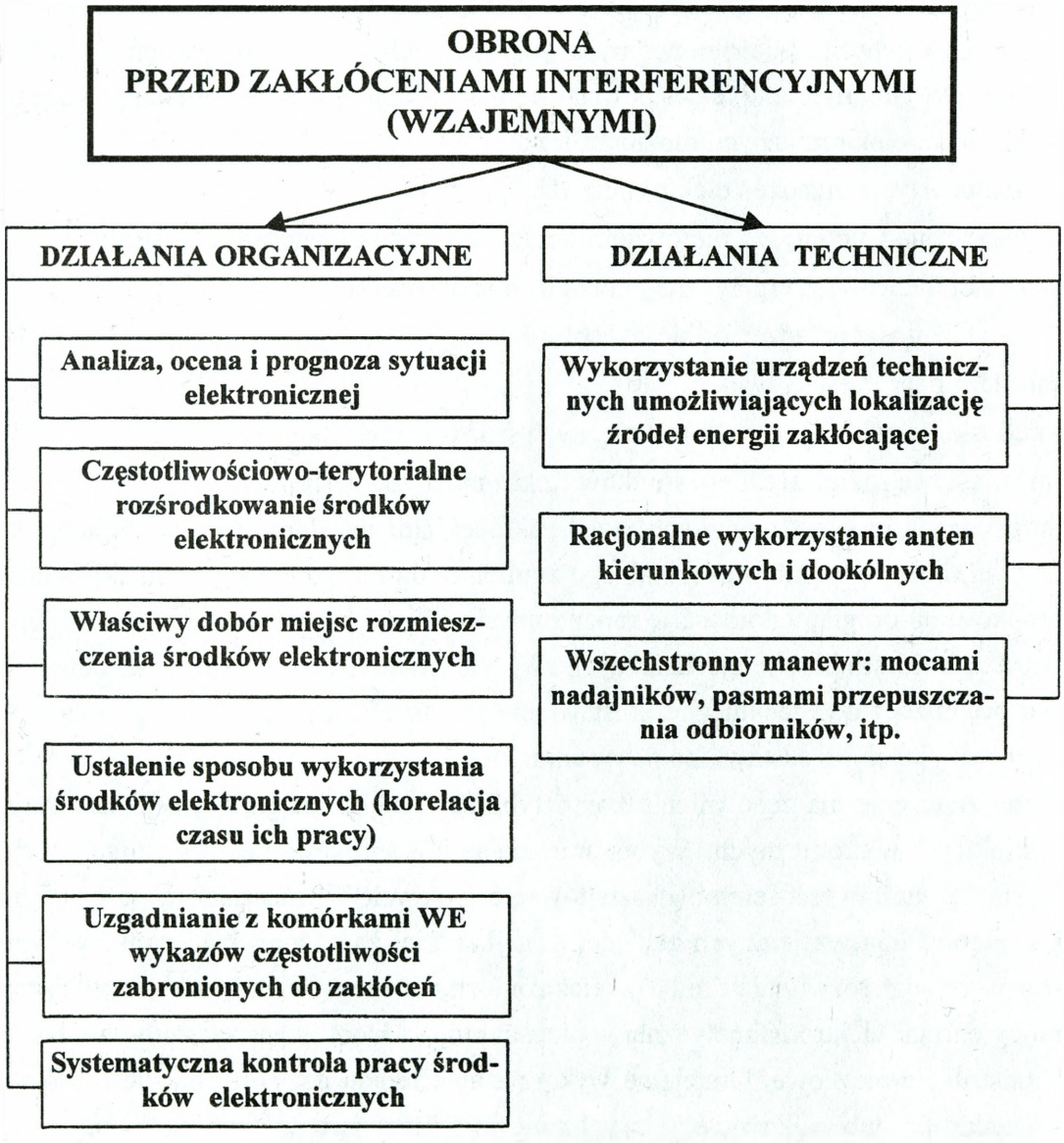
Odległości te powinny być nie mniejsze niż:

– między radiostacjami średniej mocy a stacjami radioliniowymi: 1500-2000 m;

– między stacjami radioliniowymi: 200-300 m;

– między radiostacjami średniej mocy KF i UKF: 300-400 m;

– w grupie powyżej 4 radiostacji średniej mocy: 800-1000 m.



Rys. 29. Działania wojsk w zakresie obrony przed zakłóceniami interferencyjnymi

Pozostałe elementy węzłów łączności powinny być rozśrodkowane z zachowaniem odstępów 50-70 m, natomiast grupy środków radiowych powinny być rozmieszczone w odległości: WŁ SD (ZSD) ZO 3-5 km i więcej; WŁ SD (ZSD) ZT 1-3 km; WŁ SD oddziału 1-1,5 km.

Wybór miejsca rozwijania środków elektronicznych powinien odgrywać również duże znaczenie dla eliminowania wzajemnych zakłóceń. Idealne – z punktu widzenia kompatybilności elektromagnetycznej – miejsce do rozwijania środków elektronicznych umożliwia ekranowanie anteny odbiorczo-nadawczej w obszarze promieniowania niepożądanego z wykorzystaniem ekranów naturalnych oraz stwarza korzystne warunki propagacji fal elektromagnetycznych w obszarze promieniowania pożądanego.

Ważnym przedsięwzięciem, eliminującym wpływ zakłóceń pochodzących od wojsk własnych, jest uzgodnienie z komórkami walki elektronicznej częstotliwości zabronionych do zakłóceń[33].

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 czasie pracy środków elektronicznych lub zakazie ich wykorzystania w określonym czasie. Należy uwzględniać zasadę, 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.

Kontrola pracy środków elektronicznych i warunków propagacji fal elektromagnetycznych powinna być realizowana przez specjalistyczne komórki WE. Należy mieć na uwadze, że prawdopodobieństwo naruszenia kompatybilności elektromagnetycznej, np. w działaniach taktycznych dywizji I rzutu wynosi około 0,9999997. Jeśli uwzględni się wpływ środków przeciwnika oraz zakłóceń atmosferycznych i przemysłowych, to łączne prawdopodobieństwo wystąpienia naruszeń kompatybilności elektromagnetycznej będzie jeszcze wyższe. W przypadku drastycznych naruszeń kompatybilności elektromagnetycznej należy przewidzieć wyłączanie mniej ważnych środków elektronicznych lub podejmowanie innych działań.

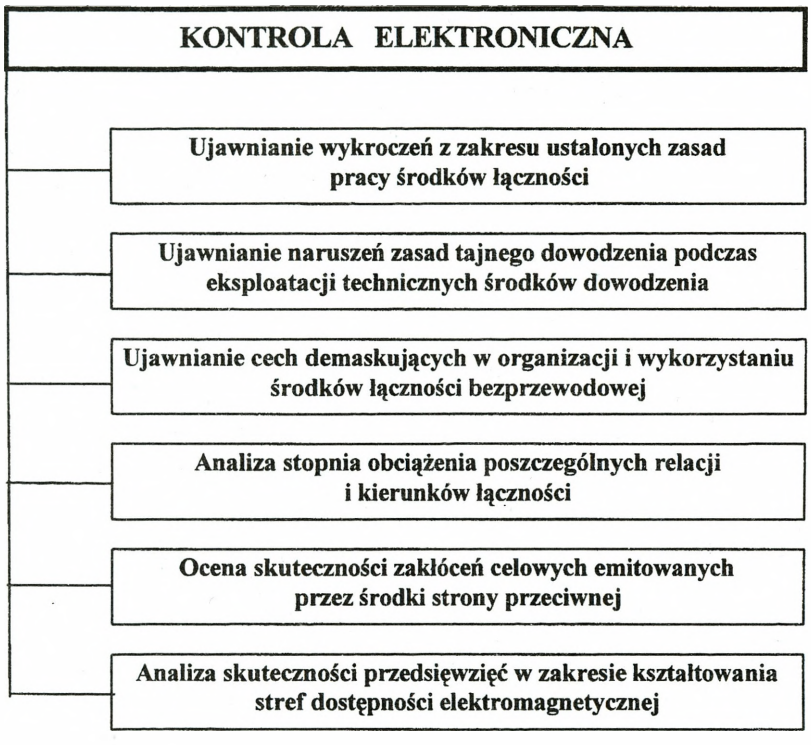
Przedsięwzięcia techniczne są realizowane przez zespoły obsługujące wszystkie środki elektroniczne. W ramach działań technicznych należy przede wszystkim wyposażyć wojska łączności w urządzenia *umożliwiające identyfikację i lokalizację źródeł energii zakłóceniowej, przez* ciągłe śledzenie źródeł emitujących energię elektromagnetyczną na częstotliwościach przydzielonych środkom elektronicznym danego SŁ, węzła łączności, itp. Pozostałe techniczne działania mające na celu eliminację zakłóceń interferencyjnych (wzajemnych) powinny być podejmowane analogicznie jak w przypadku obrony przed zakłócaniem elektronicznym.

[33] Wykazy takie powinny być zamieszczone w formie apendyksów do aneksu „Walka elektroniczna i łączność".

4.5. Kontrola elektroniczna

Kontrolę elektroniczną prowadzi się w celu wykrycia i eliminowania cech demaskujących pracę własnych środków elektronicznych oraz sprawdzenia przestrzegania regulaminu i ustalonych zasad pracy. Powinna ona umożliwiać ponadto określenie głębokości stref rozpoznania przeciwnika i sprawdzenie skuteczności przedsięwzięć maskowania elektronicznego.

Do jej prowadzenia powinny być angażowane na szczeblu taktycznym wyspecjalizowane siły i środki WE. Pod względem formy i treści kontrola ta powinna dzielić się na tym szczeblu dowodzenia na kontrolę radiową (rys. 30) i radiotechniczną.



Rys. 30. Zakres kontroli elektronicznej

Kontrolę radiową należy organizować również w wojskach dowodzenia i łączności (na własne potrzeby). W tym celu powinny być wyznaczane zespoły oficerskie oraz odpowiednie siły i środki wojsk łączności. W składzie węzła łączności związku taktycznego muszą znaleźć się (i funkcjonować) aparatownie kontroli radiowej. Takie aparatownie powinny być również wykorzystywane w miarę możliwości w oddziałach ogólnowojskowych.

Kontrola radiotechniczna powinna być organizowana i prowadzona na szczeblu operacyjnym, a w miarę możliwości również na szczeblu taktycznym. Jej zadanie to sprawdzenie technicznych norm pracy środków elektronicznych, takich jak: stabilność częstotliwości, szero-

kość pasma jednej emisji, wielkość mocy sygnałów informacji. Do tego jest niezbędny specjalistyczny sprzęt techniczny: aparatownie kontrolne i analizatory komputerowe oraz wyszkolone zespoły osób funkcyjnych.

* *
*

Uogólniając dotychczasowe rozważania warto podkreślić, że jest konieczne, aby *obrona elektroniczna* miała charakter powszechny, to znaczy była podejmowana w odpowiednim zakresie przez wszystkich użytkowników środków elektronicznych. Powinna być prowadzona kompleksowo i obejmować odpowiednie przedsięwzięcia organizacyjne i techniczne, uodporniające systemy elektroniczne na ich wielopłaszczyznowe zagrożenie wynikające z charakteru współczesnego pola walki.

Formy i sposoby obrony elektronicznej należy systematycznie doskonalić w celu zapewnienia stabilnej i niezawodnej pracy systemów elektronicznych.

5. PRZYGOTOWANIE WALKI ELEKTRONICZNEJ W DZIAŁANIACH TAKTYCZNYCH ZWIĄZKU TAKTYCZNEGO

5.1. Założenia ogólne

Przygotowanie walki elektronicznej jest nierozerwalnie związane z procesem przygotowania działań taktycznych ZT[34] i obejmuje:

1. Ustalenie położenia sił i środków elektronicznych przeciwnika.
2. Planowanie walki elektronicznej.
3. Stawianie zadań.
4. Utrzymanie zdolności bojowej sił i środków walki elektronicznej (własnych i przydzielonych pododdziałów elektronicznych).
5. Przygotowanie rejonów (rubieży) do rozwinięcia pododdziałów walki elektronicznej.
6. Kontrolę realizacji zadań.

Przygotowanie walki elektronicznej w działaniach taktycznych to całokształt przedsięwzięć realizowanych przez sztab dywizji, w którym najważniejsze zadania realizują: G 2 (wydział rozpoznawczy), dowództwo i sztab batalionu rozpoznawczego oraz pododdział walki elektronicznej. Celem przygotowania walki elektronicznej jest określenie kolejności, sposobów i terminów wykonania zadań walki elektronicznej (WE) przez ZT, oddziały oraz specjalistyczne pododdziały WE, rozwiązanie problemów współdziałania i zabezpieczenia walki oraz organizacji dowodzenia.

W etapie planowania walki elektronicznej oficerowie sekcji walki elektronicznej sztabu związku taktycznego wypracowują ogólną koncepcję prowadzenia walki elektronicznej oraz ustalają potrzeby niezbędne do jej realizacji. Koncepcja prowadzenia walki elektronicznej w każdym przypadku jest podporządkowana zadaniom, jakie otrzymał ZT oraz celowi i decyzji dowódcy. Jest ściśle skoordynowana z prowadzeniem rozpoznania wojskowego i rażeniem ogniowym.

Z punktu widzenia pododdziału walki elektronicznej zasadniczym zadaniem na tym etapie jest wypracowanie decyzji o jego użyciu. Po wypracowaniu decyzji następuje etap jej wdrażania.

---

[34] *Regulamin działań wojsk lądowych,* Wyd. DWL, Warszawa 1999.

5.2. Ustalenie położenia sił i środków elektronicznych

Podczas analizy zadania (rozkazu operacyjnego) dowódca wraz ze sztabem ZT przystępuje do ustalenia położenia sił przeciwnika i oceny wojsk własnych. W komórce G 2 ustala się szczegółowo położenie sił przeciwnika w chwili otrzymania zadania oraz na tej podstawie wyciąga wnioski co do prognozy rozwoju sytuacji. Podobne czynności wykonuje komórka WE, koncentrując się przede wszystkim na analizie środowiska elektromagnetycznego, w którym rozgrywana jest WE.

Celem ustalenia położenia - z punktu widzenia potrzeb procesu elektronicznego przygotowania pola walki (EPB)[35] - jest uporządkowanie, a następnie zobrazowanie danych o rozmieszczeniu i ukompletowaniu elementów elektronicznych przeciwnika w jego dotychczasowych działaniach, przedstawienie otoczenia pola walki (teren, pogoda, warunki demograficzne itp.), a także położenia i realizowanych zadaniach przez potencjał rozpoznania wojsk własnych. Dane są pozyskiwane przez systemy rozpoznawcze z obszaru *odpowiedzialności rozpoznawczej ZT*, a za dostarczanie ich z obszaru *zainteresowania rozpoznawczego* jest odpowiedzialny przełożony.

Podstawę do ustalenia położenia przeciwnika stanowią meldunki z rozpoznania, rozkazy operacyjne i komunikaty szczebla nadrzędnego, dane uzyskane od sąsiadów, wojsk obrony terytorialnej oraz układu pozamilitarnego.

Położenie własnych sił i środków rozpoznania jest z kolei ustalane na podstawie meldunków od podwładnych.

Zebrane dane są porządkowane i ewidencjonowane oraz poddawane wstępnej analizie, ocenie i uogólnieniu. Tak przetworzone stają się materiałem wyjściowym dla procesu EPB w etapie planowania, którego właściwością jest ciągłe weryfikowanie danych. Dzięki temu możliwa jest ich aktualizacja, uwiarygodnianie oraz poszerzanie obszaru wiedzy o przeciwniku.

Wnioski z procesu EPB w omawianej fazie mają swoje odzwierciedlenie w takich dokumentach, jak: mapa informacyjna lub sytuacyjna, meldunek okresowy, rozkaz operacyjny.

5.3. Planowanie walki elektronicznej w działaniach taktycznych

Proces wypracowania decyzji w zakresie użycia sił i środków walki elektronicznej jest realizowany w wydziale rozpoznawczym sztabu dywizji i nazywany etapem wypracowania koncepcji prowadzenia WE.

Wypracowanie decyzji rozpoczyna się po otrzymaniu rozkazu operacyjnego dowódcy korpusu (niekiedy jest on poprzedzony zarządzeniem przygotowawczym albo wstępnym za-

[35] EPB – elektroniczne przygotowanie pola walki. Szczegółową analizę zawiera opracowanie G. Nowackiego i W. Scheffsa; *Elektroniczne przygotowanie pola walki,* AON, Warszawa 1999.

rządzeniem operacyjnym). Po otrzymaniu takiego dokumentu oficerowie z sekcji walki elektronicznej (WE), którzy przeprowadzają analizę zadania pod kątem prowadzenia działań elektronicznych, przystępują do rozpoczęcia procesu elektronicznego przygotowania pola walki.

Ocena dotychczasowych działań elektronicznych przeciwnika i prognoza przyszłych działań w znaczeniu ogólnym dotyczy zbierania informacji ze strefy odpowiedzialności rozpoznawczej ZT (SOR) oraz spektrum elektromagnetycznego. Określenie wielkości strefy i zakresu wykorzystania spektrum elektromagnetycznego ma decydujący wpływ na skuteczność oraz trafność uzyskiwanych wyników, albowiem można zapobiec zdobywaniu danych ze zbyt dużego obszaru lub przedziału częstotliwości oraz wykluczyć pozyskiwanie danych ze zbyt małego obszaru i zakresu częstotliwości.

Wielkość SOR ZT jest określona przez przełożonego, a zakres częstotliwości pracy środków elektronicznych przeciwnika wiąże się z możliwościami taktyczno-technicznymi środków rozpoznawanych, z normami prowadzenia działań taktycznych oraz ich rodzajem. Przełożony, znając możliwości bojowo-rozpoznawcze podwładnego, nie powinien wyznaczać zbyt rozległego obszaru odpowiedzialności rozpoznawczej. Innym czynnikiem wpływającym na wielkość SOR ZT mogą być siły i środki przeciwnika oraz zakres zadań przez nie realizowanych.

Można więc stwierdzić, że uzyskiwanie właściwych wyników podczas oceny przeciwnika wiąże się z prowadzeniem tego procesu w takim obszarze i zakresie częstotliwości, aby obejmowała co najmniej pas działań taktycznych szczebla oceniającego oraz obszary na prawo i lewo o jeden szczebel niżej (w zależności od rodzaju działań ta szerokość będzie inna). Natomiast zakres częstotliwości powinien obejmować kanały wykorzystywane przez dany rodzaj wojsk przeciwnika[36].

W praktyce wyróżnia się następujące formy oceny sił i środków elektronicznych przeciwnika:

– indywidualna - dokonywana przez dowódcę, szefa sztabu lub szefa komórki G 2;

– kolektywna - prowadzona przez dowódcę oraz zespół oficerów z G 2 i G 3, w składzie tego zespołu powinien znajdować się oficer walki elektronicznej;

– prowadzona z wykorzystaniem środków automatyzacji procesu dowodzenia.

W zależności od stylu pracy dowódcy oraz sztabu, a także od posiadanych umiejętności, wiedzy i środków technicznych wspomagających proces decyzyjny oraz organizacyjny dowódca narzuca odpowiednią formę pracy. Forma ta będzie obowiązywała w całym sztabie. Wybór formy postępowania będzie miał wpływ na wnioski, jakie sekcja WE musi wypracować w procesie EPB. Wnioski te wspierają dowódcę i sztab w procesie decyzyjnym. Graficzna ocena sytuacji odzwierciedla prawdopodobne elektroniczne działanie przeciwnika, co pozwala dowódcy wpływać na przebieg bitwy. W trakcie działań taktycznych graficzna ocena

[36] Przykładowo zakres UKF wojsk lądowych obejmuje częstotliwości od 20 do 88 MHz.

sił elektronicznych przeciwnika oraz zadania bojowe mogą ulegać zmianie wraz z dynamicznie rozwijającą się sytuacją na polu walki. Prognoza elektronicznego przygotowania pola walki ma pomagać dowódcy kontrolować jej przebieg. Wskazanie najsłabszych punktów w ugrupowaniu przeciwnika oraz czasu i kierunku przemieszczania się jego wojsk ułatwia tę kontrolę, ponadto pokazuje dowódcom, kiedy, gdzie i jak przeciwnik użyje swoje pododdziały elektroniczne, jak najefektywniej może być związany ogniem, manewrem oraz w którym momencie może zostać przechwycona inicjatywa.

Przedstawiając graficznie proces EPB, można określić z dużym prawdopodobieństwem cele wysoko opłacalne (HPT)[37], między innymi cele elektroniczne, w obszarze walki. Na podstawie tych najważniejszych celów zbudowana jest koncepcja walki dowódcy. Cele te należy atakować tak, aby zmniejszyć efektywność oddziaływania sił przeciwnika, opóźniać jego działanie lub wymusić na przeciwniku użycie kolejnych sił (odwodów), które mogą stać się przedmiotem kolejnego ataku ogniowego, oddziaływania elektronicznego, dywersyjnego lub propagandowego.

Na podstawie EPB przedstawia się elektroniczne warianty zagrożenia, które wykonywane są, aby odzwierciedlić (graficznie i opisowo) siły i środki walki elektronicznej przeciwnika, węzły elektroniczne i łączności[38] oraz zakres ich oddziaływania. Analizie podlegają możliwości bojowo-rozpoznawcze sprzętu walki elektronicznej przeciwnika lądowego i powietrznego (urządzenia naziemne, samoloty wsparcia, śmigłowce i BŚR), sposoby jego działania oraz słabe punkty w ugrupowaniu, a także możliwości bojowe urządzeń łączności i technicznego rozpoznania, będące w obrębie węzłów elektronicznych i łączności.

Przebieg procesu elektronicznego przygotowania pola walki (rys. 31) jest następujący:

- ocena sytuacji elektronicznej w działaniach taktycznych;
- analiza terenu pod względem przeszkód terenowych utrudniających rozprzestrzenianie się fal EM, obszarów zakrytych dla fal EM;
- ocena dróg podejścia i wykonywania manewrów pododdziałami elektronicznymi przeciwnika (węzłami łączności, węzłami elektronicznymi, szczególnie pododdziałami WE);
- analiza pogody pod kątem rozprzestrzeniania się fal elektromagnetycznych;
- prognoza zagrożenia elektronicznego, a w niej:

– porównanie wzorców doktrynalnych działania przeciwnika z bieżącą sytuacją elektroniczną;

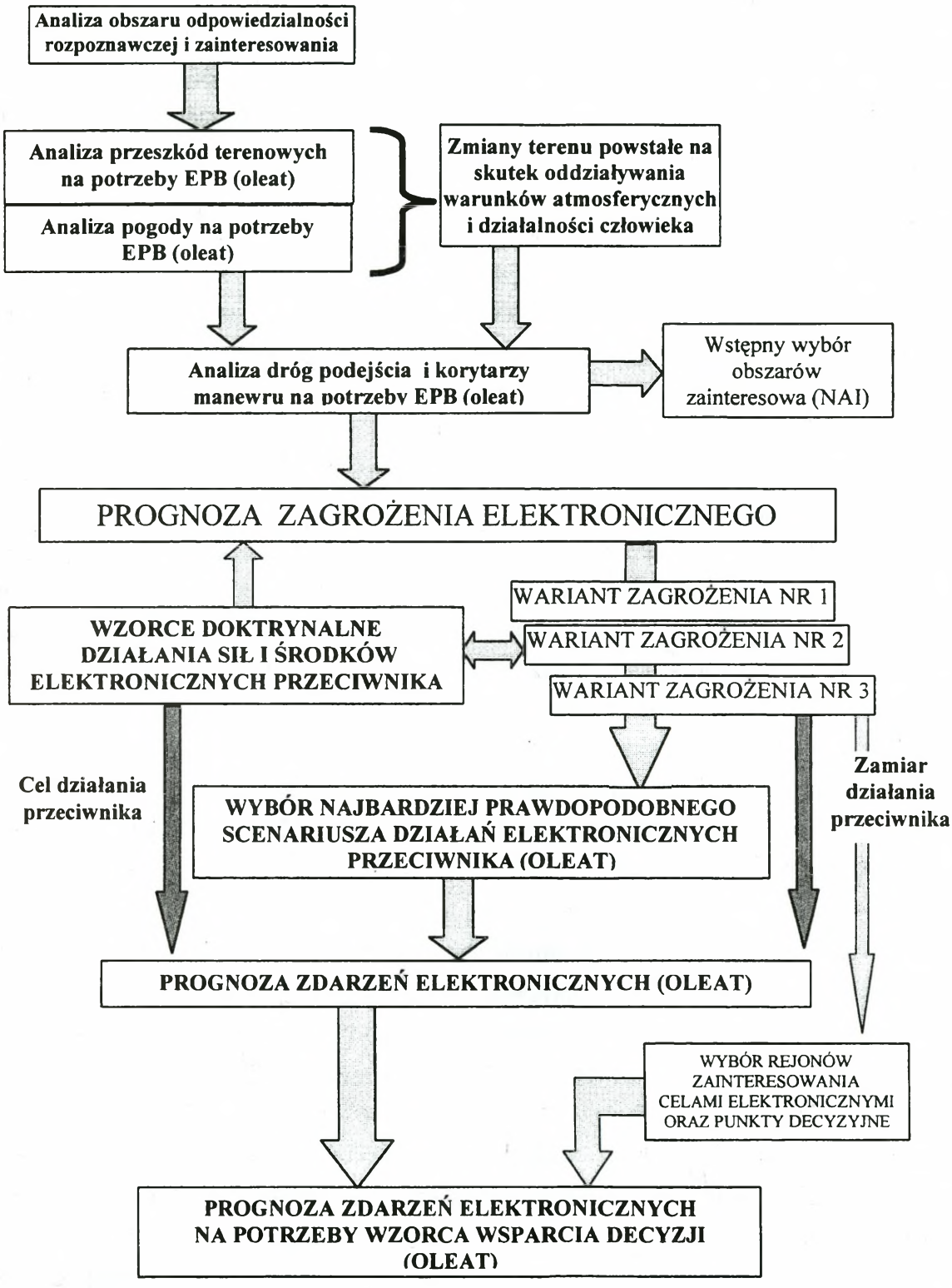
– prognoza działania sił i środków elektronicznych przeciwnika;

- uzgodnienie z oficerem rozpoznania wojskowego celu i zamiaru działania przeciwnika z jednoczesnym wariantowaniem użycia sił i środków elektronicznych;
- odprawa z udziałem G 2 i G 3 i podjęcie decyzji odnośnie wyboru wariantu działania przeciwnika, na tej podstawie następuje proces prognozowania zdarzeń elektronicznych;

---

[37] HPT (High payoff targets) - cele wysoko opłacalne; są to najbardziej istotne cele wynikające z sytuacji bojowej (elektronicznej).

[38] Zob. G. Nowacki i W. Scheffs; *Elektroniczne przygotowanie pola walki,* AON, Warszawa 1999.



Rys. 31. Przebieg procesu elektronicznego przygotowania pola walki

- precyzowanie wniosków w zakresie potrzeb rozpoznania i zakłócania elektronicznego;
- ocena posiadanych sił i środków, ich możliwości – w aspekcie zadania dywizji oraz warunków terenowych i pogodowych.

5.3.1. Ocena sytuacji elektronicznej w działaniach taktycznych

W tym etapie analizuje się możliwości prowadzenia rozpoznania elektronicznego w strefie odpowiedzialności rozpoznawczej i w strefie zainteresowania rozpoznawczego ZT.

Strefa odpowiedzialności rozpoznawczej ZT (rys. 32) obejmuje obszar, w którym dowodzenie i odpowiedzialność za prowadzenie działań taktycznych zostają powierzone dowódcy. Obszar ten jest określony granicami lub punktami rzeźby terenu i przekazany w formie załączników do rozkazu (planu działania) na folii lub kalce.

Strefa zainteresowania rozpoznawczego ZT jest częścią strefy odpowiedzialności rozpoznawczej przełożonego i jej cały rozmiar nie musi być znany dowódcy ZT. Wymiary strefy zainteresowania ZT są ograniczone możliwościami bojowymi elementów rozpoznawczych przełożonego w zakresie zdobywania danych o siłach i środkach przeciwnika.

Dowódca na podstawie ustaleń z oficerami G 2 musi uwzględnić w strefach wszystkie wymiary pola walki:

– szerokość;

– głębokość;

– wysokość (przestrzeń powietrzna);

– czas;

– spektrum elektromagnetyczne[39].

Przy określaniu i analizie obszaru działań dla wojsk lotniczych i obrony powietrznej określa się również dwie strefy:

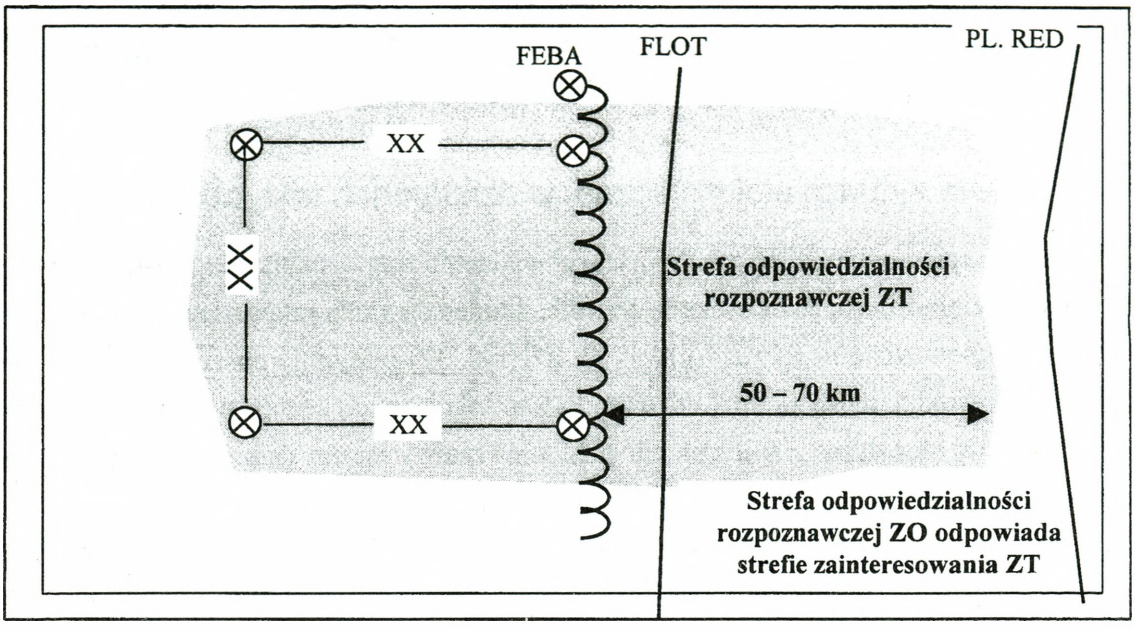
- powietrzną strefę odpowiedzialności rozpoznawczej;

- powietrzną strefę zainteresowania.

Powietrzna strefa odpowiedzialności rozpoznawczej ZT jest identyczna jak strefa odpowiedzialności rozpoznawczej ZT, wówczas gdy analizuje się naziemne systemy broni. Z tej strefy dostarczane są informacje o obiektach położonych w głębi SOR ZT.

Powietrzna strefa zainteresowania LWL ZT jest zwykle większa niż strefa zainteresowania ZT. Jej wymiary uwzględniają maksymalny pułap działania samolotów, śmigłowców i BŚR wojsk własnych i przeciwnika oraz maksymalny zasięg systemów broni obrony powietrznej. Strefa ta jest obszarem odpowiedzialności rozpoznawczej przełożonego i on dostarcza niezbędne dane o przeciwniku i o grożących mu niebezpieczeństwach.

[39] Spektrum elektromagnetyczne jest uwzględniane przede wszystkim przez oficerów WE podczas elektronicznego przygotowania pola walki.



– FEBA (forward edge of the battle area) – linia styczności wojsk;

– FLOT (forward line of own troops) – linia, która wskazuje najbardziej wysunięte pozycje sił własnych, prowadzących pewien rodzaj działań bojowych w określonym czasie. FLOT identyfikuje się z najbardziej wysuniętą pozycją sił ubezpieczenia i osłony bez elementów rozpoznawczych. Elementy rozpoznawcze rozwinięte za linią FEBA działają na całą głębokość strefy odpowiedzialności rozpoznawczej.

– PL. RED - linia strefy, np. w tym przypadku linia działania lotnictwa wojsk lądowych.

Rys. 32. Strefy odpowiedzialności rozpoznawczej ZT i ZO

Oba wymiary powietrzny i lądowy są przedmiotem analizy prowadzonej przez oficerów WE podczas oceny strefy odpowiedzialności rozpoznawczej ZT. Wnioski z tej analizy są pomocne dowódcy ZT w ustaleniu zadań dla pododdziałów rozpoznawczych. Wstępnie ustala się spodziewane kierunki działania i oddziaływania sił przeciwnika (ogniowego i elektronicznego).

5.3.2. Ocena terenu

Po zapoznaniu się z zadaniem bojowym i strefą odpowiedzialności rozpoznawczej ZT kolejnym krokiem w procesie elektronicznego przygotowania pola walki jest analiza terenu.

Na szczeblu związku taktycznego zajmuje się nią zespół oficerów z sekcji topograficznej odpowiednio przygotowanych do jej prowadzenia. Na niższych szczeblach problem rozpatrywany jest przez oficerów wojsk inżynieryjnych przy współudziale oficerów operacyjnych. Ocena powinna w pełnym (wymaganym do podjęcia decyzji) zakresie oddawać właściwości i specyfikę strefy odpowiedzialności rozpoznawczej. Z jednakową wnikliwością dokonuje się oceny terenu zarówno po stronie przeciwnika, jak i własnej[40].

[40] M. Wrzosek, *Praca taktycznej komórki rozpoznawczej G 2*. Dodatek do PWL nr 9/97, Warszawa 1997, s. 12.

Analitycy sekcji WE korzystają z oleat i opisów przeszkód terenowych wykonanych przez sekcję topograficzną G 2. Specjalistyczną ocenę terenu mogą prowadzić samodzielnie lub z udziałem oficerów sekcji topograficznej.

Analiza terenu na potrzeby EPB dokonywana przez oficerów sekcji WE wymaga specjalnych rozważań dotyczących działań sił i środków rozpoznania i zakłócania elektronicznego, stref zakrytych dla rozprzestrzeniania się energii EM oraz przeszkód terenowych, mających istotny wpływ na rozprzestrzenianie się energii elektromagnetycznej lub maskowanie elektroniczne. Celem analizy terenu jest redukowanie niepewności związanych z działaniem środków elektronicznych przeciwnika w czasie działań taktycznych w środowisku naturalnym lub wykorzystywanym przez człowieka środowisku elektromagnetycznym.

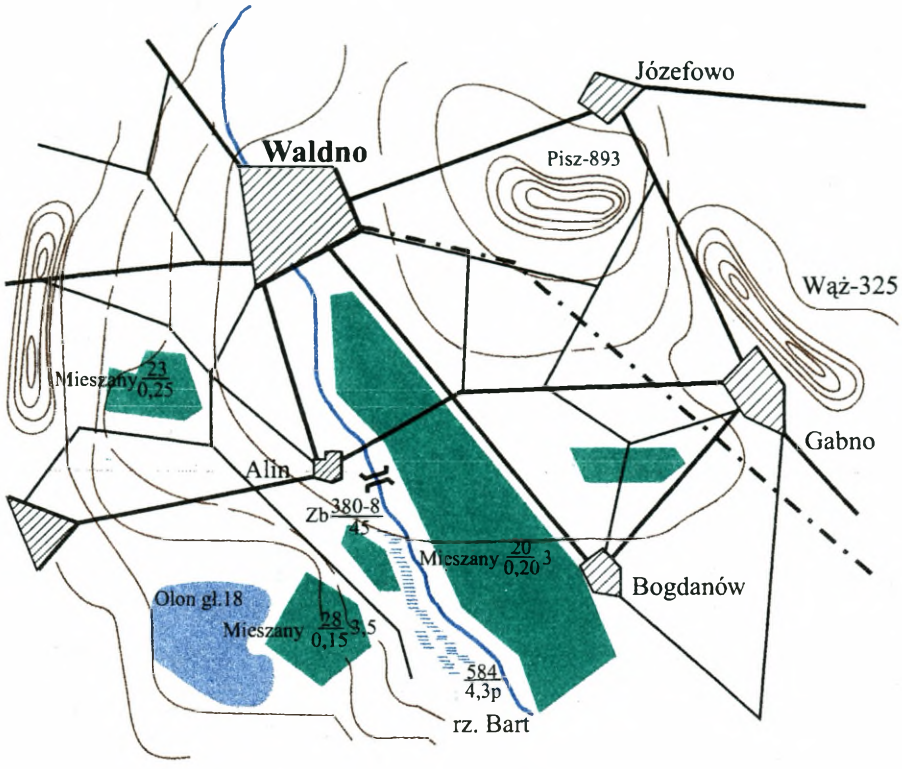
Analizując teren pod względem możliwości prowadzenia obserwacji optycznej (wzrokowej) i elektronicznej (horyzontu radiowego), analityk rozważa strefy widzialności – wzrokowej i horyzontów radiowych (LOS)[41]. Strefy te są niezbędne do określenia w rozpatrywanym obszarze charakterystycznych punktów i możliwości prowadzenia rozpoznania elektronicznego, ognia bezpośredniego oraz rozprzestrzeniania energii elektromagnetycznej. Bardzo często rozmieszczenie środków ogniowych, punktów obserwacyjnych i miejsc dyslokacji środków elektronicznych wymaga wielu uzgodnień i kompromisów.

Innym, koniecznym do uwzględnienia czynnikiem oceny terenu jest określenie zdolności manewrowych elementów i całych systemów elektronicznych przeciwnika i wojsk własnych.

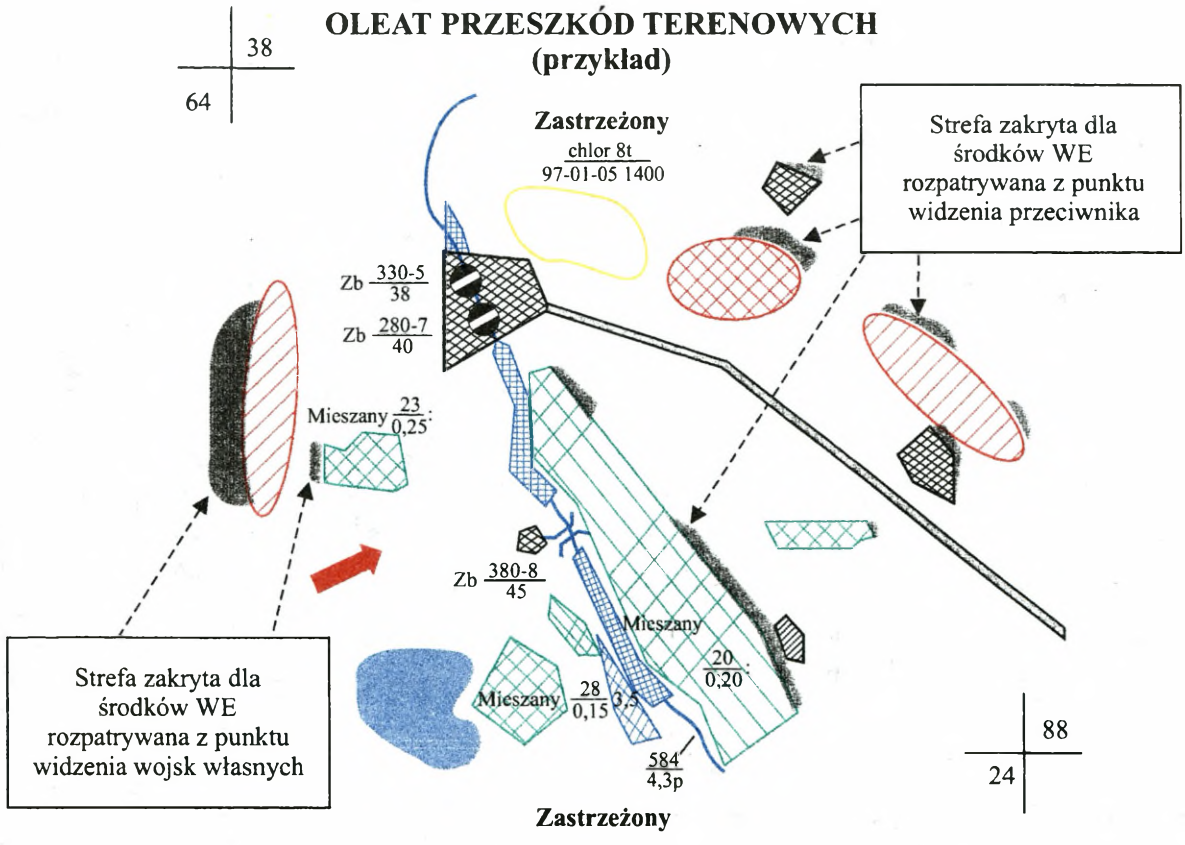
Przeszkody naturalne, takie jak lasy, jeziora, bagna, wzniesienia terenowe i góry, w istotny sposób wpływają na manewr siłami i środkami elektronicznymi, mają wpływ na czas jego wykonania i możliwości zapewnienia łączności pomiędzy elementami systemu. Infrastruktura terenu (urządzenia hydrotechniczne, elektrownie, linie energetyczne, sieć kolejowa, wysoka zabudowa) ma duży wpływ na rozprzestrzenianie się energii elektromagnetycznej, może powodować przerwy w łączności lub pojawienie się zakłóceń na ekranach SRL.

W celu utrudnienia obserwacji wzrokowej, radiolokacyjnej i termicznej stosuje się kolorowe, metalizowane, dymy, aerozole, mgły, zasłony termiczne, co w konsekwencji utrudnia ocenę terenu. Ten podstawowy sposób maskowania bezpośredniego może być uzupełniany przez całą gamę środków pozorujących obiekty realne. Dokładna analiza tych czynników wpływa na właściwą ocenę terenu oraz prognozę zagrożeń działaniami elektronicznymi ze strony przeciwnika. Przykładową mapę terenu otrzymaną z sekcji topograficznej i wykonaną na jej podstawie oleatę przeszkód terenowych pokazano na rysunkach 33 i 34.

[41] LOS (Line of sight) - Linia obserwacji (widzialności).



Rys. 33. Przykładowa mapa terenu z wyszczególnionymi przeszkodami terenowymi otrzymana z sekcji topograficznej



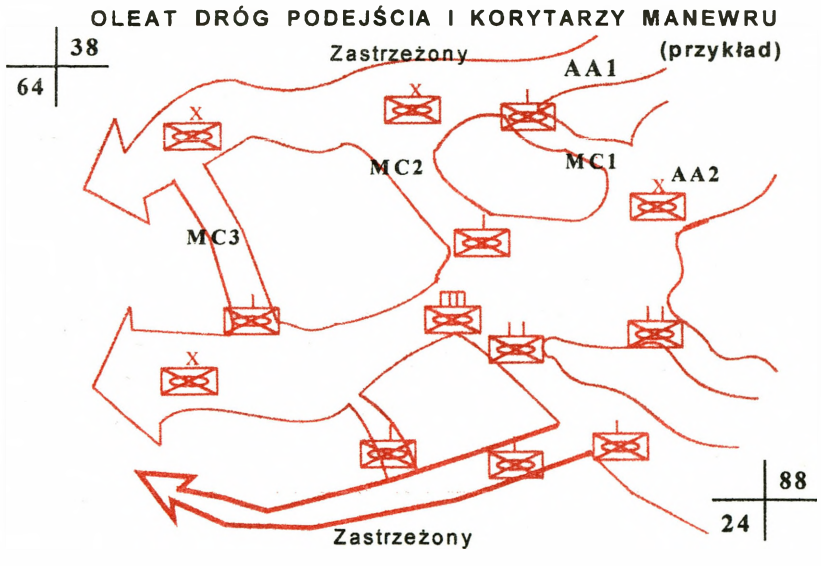
Rys. 34. Oleat przeszkód terenowych z rejonami zakrytymi i przeszkodami utrudniającymi manewr pododdziałom elektronicznym wykonywany przez sekcję WE

5.3.3. Analiza dróg podejścia

Jednym z dokumentów pomocniczych, wykorzystanym w trakcie oceny terenu jest oleat dróg podejścia i korytarzy manewru (rys. 35). Podstawą do przygotowania właściwego oleatu jest prawidłowa ocena i charakterystyka terenu. Dokument ten wykonują oficerowie z sekcji opracowania danych o terenie i pogodzie z G 2, natomiast analitycy z sekcji WE wykorzystują go dla własnych potrzeb oceny sytuacji elektronicznej.

Prowadzący analizę dróg podejścia główną uwagę skupiają na obszarach trudno przekraczalnych, o niskiej przejezdności, utrudniających manewr sprzętem elektronicznym. Pomimo dynamicznego rozwoju środków transportowych[42] (w tym i powietrznych) wydaje się mało prawdopodobne, aby wojska zrezygnowały z istniejącej sieci dróg. W tych warunkach jest konieczna stała obserwacja rejonów (punktów), które zapewniają swobodę manewru.

Graficzne przedstawienie oleatu dróg podejścia i korytarzy manewru wykonuje się na jednym oleacie dla całego G 2. Sekcja WE analizuje oleat dróg podejścia, interpretując i określając przeszkody terenowe, które utrudnią lub uniemożliwią manewr środkami elektronicznymi lub WE . Zwykle sporządza się ten dokument nakładając na siebie oleaty: dróg podejścia i przeszkód terenowych. Wnioski z tej analizy pozwalają wstępnie określić obszary zainteresowania.



Rys. 35. Oleat dróg podejścia i korytarzy manewru

[42] W wojnie powietrzno-lądowej może nastąpić ograniczenie wykorzystania dróg lądowych, ale powstaną wówczas korytarze powietrzne. Ich obserwacja będzie nastręczała pewnych trudności, ale też pozwoli na określenie kierunków przemieszczania się wojsk przeciwnika i słabych stron takich manewrów, np. lądowiska, lotniska polowe, drogowe odcinki lotnicze. Kontrola tych rejonów jest niezmiernie ważna.

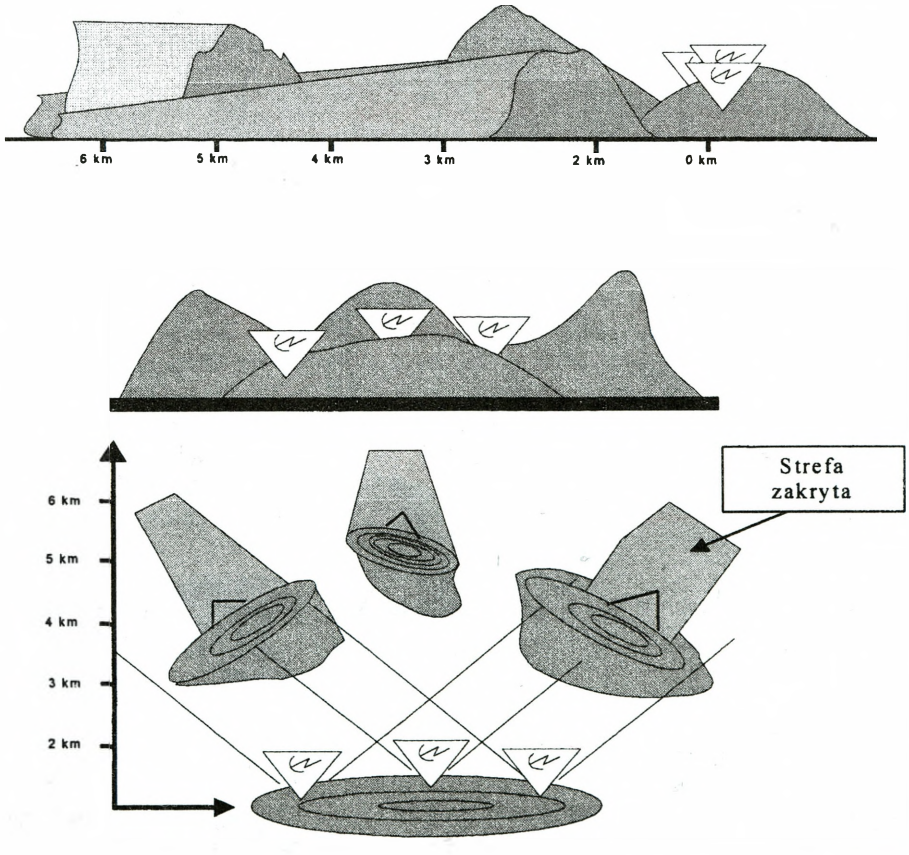
Obok lądowych dróg podejścia analizie poddaje się drogi podejścia w przestrzeni powietrznej. Analitycy sekcji WE korzystają z przygotowanych przez oficerów z zespołu planowania powietrznego, wchodzących w skład sekcji planowania i kierowania rozpoznaniem G 2, powietrznych dróg podejścia samolotów i śmigłowców.

Każda droga podejścia musi być analizowana pod kątem widzialności optycznej i horyzontu radiowego. W procesie tym uwzględnia się następujące czynniki:

- teren;
- wysokość i zwartość roślinności lub drzew;
- punkty wysokościowe w terenie zabudowanym;
- właściwości mikrorzeźby terenu (pola zakryte);
- wpływ pogody na możliwość obserwacji.

Analiza powyższych czynników pozwala określić, czy przeciwnik będzie mógł oddziaływać ogniem bezpośrednim, skąd będzie mógł prowadzić zakłócenia elektroniczne oraz gdzie znajdują się „pola zakryte" dla rozprzestrzeniania się energii elektromagnetycznej lub rozwinięcia sprzętu elektronicznego.

Rozpatrując wykorzystanie przez przeciwnika środków łączności UHF i VHF na drogach podejścia, połączony zespół oficerów WE i sił powietrznych dokonuje analizy przeszkód terenowych. Brak łączności bowiem może być spowodowany złą pogodą lub wysokimi przeszkodami terenowymi (rys. 36).



Rys. 36.Przeszkody terenowe i ich wpływ na obserwację

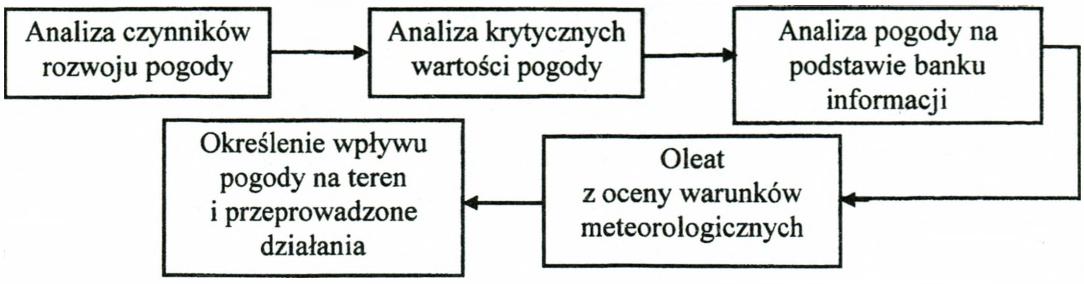
Warunki terenowe ograniczają zasięg fal elektromagnetycznych wysyłanych przez stacje radiolokacyjne nadzorujące pole walki lub wykrywające cele powietrzne. Pododdziały radiotechniczne zwykle rozmieszcza się na wzniesieniach w celu zwiększenia zasięgu obserwacji. Również urządzenia zakłócające i radiostacje wymagają takiego usytuowania w terenie, aby ich strefy horyzontów radiowych w stosunku do obiektów nie utrudniały pracy własnych środków elektronicznych. Jednocześnie wyżej wymienione urządzenia zakłócające umożliwią dezorganizację pracy środków łączności przeciwnika prowadzących wymianę radiową.

Oleat przeszkód terenowych z liniami widoczności optycznej i radiowej, stanowi podstawę do określania rejonów „zakrytych" oraz miejsc, gdzie przeciwnik może rozmieścić swoje środki elektroniczne.

5.3.4. Prognoza pogody

Warunki meteorologiczne w strefie odpowiedzialności rozpoznawczej ZT analizuje się w celu określenia ich wpływu na działanie zarówno własnych wojsk, jak i przeciwnika. Analiza pogody jest prowadzona równocześnie z analizą terenu, ponieważ działania taktyczne wymagają, aby informacje o pogodzie i terenie były analizowane równolegle, a wynik analizy zawarty był w jednym dokumencie. Podczas analizy pogody na potrzeby rozpoznania i zakłócania elektronicznego rozważa się wpływ pogody na rozmieszczenie oraz wykorzystanie systemów łączności, elementów rozpoznania i zakłóceń elektronicznych wojsk własnych i przeciwnika. Analizę tę wykonują oficerowie zespołu prognozy pogody. Oficerowie sekcji WE korzystają z opracowanej już prognozy i wyciągają wnioski dotyczące wpływu warunków atmosferycznych na pracę urządzeń elektronicznych. Jeżeli wystąpią obiektywne trudności w analizie czynników pogodowych wykonywanej przez sekcję WE, to oficerowie „meteo" wspomagają proces analizy. Proces analizy pogody (rys. 37) zarówno na potrzeby IPB, jak i EPB zawiera pięć elementów:

Analiza czynników rozwoju pogody. Tabele analizy czynników pogody są narzędziem pokazującym wykorzystanie i sposób przedstawiania pogody dla wsparcia działań taktycznych. Zespół prognozy pogody wykorzystuje odpowiednio opracowane tabele dla wsparcia IPB (EPB), w celu określenia zadań dla pododdziałów i środków walki. Każdy czynnik, który ma wpływ na wykonanie zadania przez jednostkę, posiada wyznaczoną wartość krytyczną. Jeśli warunki atmosferyczne przekroczą wyznaczoną wartość krytyczną lub spadną poniżej niej, działania taktyczne, zazwyczaj, nie mogą być kontynuowane.



Rys. 37. Proces analizy pogody

Analiza krytycznych wartości pogody. Są to dane o czynnikach pogody, które w głównej mierze wpływają na zdolność bojową sił własnych i przeciwnika. Zalicza się do nich: temperaturę, kierunek i szybkość wiatru, wilgotność powietrza, widzialność, ilość opadów. Ekstremalnie wysokie lub niskie temperatury wpływają na wydajność pracy załóg oraz na czuły sprzęt elektroniczny. Kurz i wilgotność mogą powodować uszkodzenia łączy oraz usterki komponentów elektronicznych. Wyładowania elektryczne w czasie burz powodują powstanie dużych przepięć i impulsów elektromagnetycznych, co z kolei może spowodować uszkodzenie obwodów wejściowych urządzeń (złączy tranzystorów i układów scalonych). Szczególnie podatne na zniszczenie przez te czynniki są nowoczesne mikroukłady. Na wszystkie typy środków łączności HF i VHF[43] może mieć ujemny wpływ aktywność słoneczna. Wiejący wiatr, a także kurz, deszcz, śnieg i mżawka powodują zmniejszenie efektywności wszystkich stacji radiolokacyjnych. Zasięg ich wykrywalności może być ograniczony do minimum widzialności przewidzianej normami technicznymi stacji.

Analiza pogody na podstawie banku informacji. Aby utworzyć bank informacji o pogodzie w danym rejonie, należy dokładnie przeanalizować dane pogodowe z poprzednich pięciu lat. Pozwoli to określić najważniejsze parametry pogody w tym rejonie. Takich kalkulacji powinno dokonywać się na wyższych szczeblach dowodzenia. Wykorzystuje się do tego bardzo szybkie komputery, a wnioski są przekazywane podwładnym do wykorzystania. Forma i treść *oleatu z oceny warunków meteorologicznych* przedstawiona została na rysunku 38.

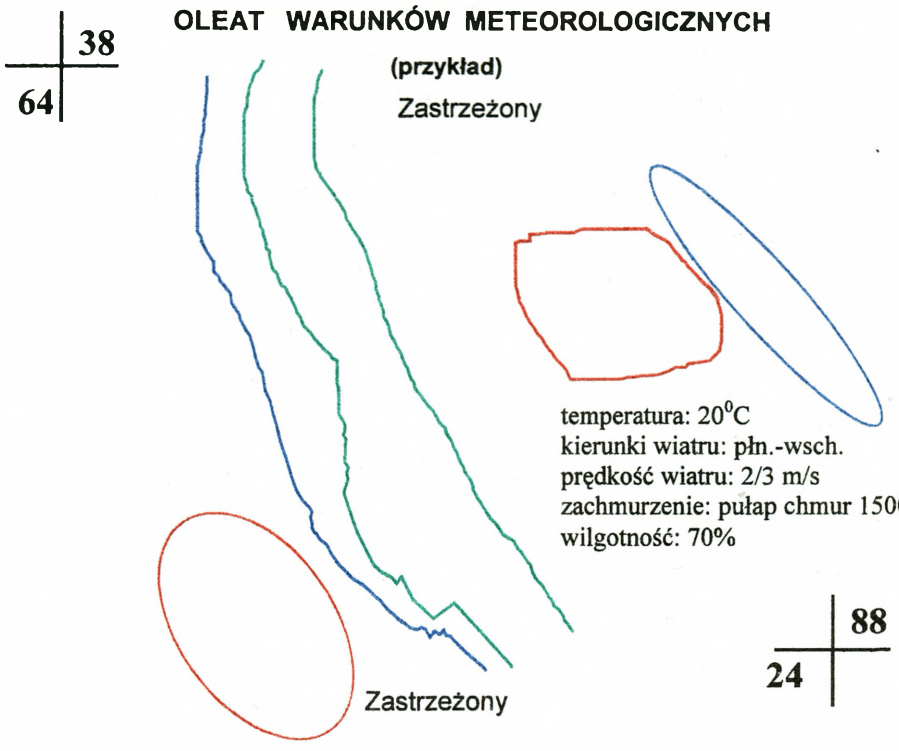
Prognozę pogody przedstawia się graficznie na oleacie. Obok prognozy w formie graficznej wykonuje się szereg tabel wpływu pogody na działania taktyczne lub połączoną prognozę wpływu pogody i terenu na przyszłe działania. Dane są analizowane na określoną godzinę lub z odpowiednim wyprzedzeniem czasowym, nie większym jednak na szczeblu taktycznym niż 24 godziny.

Opis wpływu terenu i pogody na rozprzestrzenianie się fal elektromagnetycznych ujmuje się w apendyksie do aneksu dotyczącego rozpoznania[44] rozkazu operacyjnego, natomiast graficzne zobrazowanie przedstawia się na oleatach.

---

[43] HF i VHF – High frequency i Very high frequency – wysoka częstotliwość i bardzo wysoka częstotliwość.

[44] Ponieważ komórka rozpoznawcza G 2 wykonuje apendyks pogodowy, celowe jest dołączenie do niego informacji dotyczących rozprzestrzeniania się fal elektromagnetycznych. Pamiętać należy tylko, żeby apendyks ten był rozsyłany do wszystkich jednostek, szczególnie jednostek walki elektronicznej.



Rys. 38. Oleat oceny warunków meteorologicznych

5.3.5. Prognoza zagrożenia elektronicznego

Prognoza zagrożenia elektronicznego stanowi część składową prognozy zagrożenia ogólnego, a w procesie wypracowania decyzji jest to jeden z filarów służący poprawnemu jej opracowaniu. Należy przy tym uwzględnić dwa aspekty. Pierwszym jest rozpatrywanie zagadnień związanych z położeniem, stanem i możliwościami oddziaływania elektronicznego oraz przewidywanym charakterem działań sił elektronicznych przeciwnika. Drugim – praktyczna wiedza o przygotowywaniu i prowadzeniu działań taktycznych przez pododdziały elektroniczne przeciwnika. Poziom tej wiedzy często decyduje o skutkach prowadzonej walki. W okresie pokoju przygotowaniem odpowiednich materiałów służących poszerzeniu wiedzy o siłach i środkach elektronicznych przeciwnika powinien zajmować się zespół rozpoznania w sekcji WE G 2. Dane te powinny być uzupełniane na bieżąco z własnych źródeł rozpoznawczych i otrzymywanych od przełożonego.

Do zasadniczych wymagań stawianych zespołowi prognozy zagrożenia elektronicznego należą:

– znajomość i świadomość celu działania;
– szczegółowa i wnikliwa znajomość sił i środków elektronicznych przeciwnika;
– ciągłość i systematyczność pracy;
– umiejętność prognozowania zagrożenia;
– bazowanie na danych wiarygodnych;

– uwzględnienie wszystkich zależności i czynników, mogących mieć wpływ na przyszłe działania elektroniczne przeciwnika;

– zachowanie w wynikach prognozy proporcji między szczegółowością i ogólnością;

– przestrzeganie terminowości podczas dokonywania prognozy;

– formułowanie wniosków z przeprowadzonej prognozy w sposób syntetyczny.

Prognoza zagrożeń elektronicznych polega na określeniu podstawowych danych dotyczących zagrożenia i możliwości bojowych (oddziaływania elektronicznego) przeciwnika. Dokumenty oceny zagrożeń elektronicznych wykonuje się w postaci tabel, schematów, wykresów oraz graficznie na oleatach (np. węzłów elektronicznych, łączności, ugrupowania sił i środków walki elektronicznej, działania lotnictwa i innych). Z punktu widzenia walki elektronicznej prognoza zagrożenia pociąga za sobą opracowanie danych w aneksie walki elektronicznej do rozkazu operacyjnego dotyczącego działań systemów i środków elektronicznych oraz oceny zagrożeń jednostek elektronicznych. Szczegółowo ocenia się możliwości przeciwnika w zakresie zapewnienia łączności, prowadzenia walki elektronicznej i innych środków wykorzystujących energię elektromagnetyczną (np. stacje radiolokacyjne, urządzenia optoelektroniczne, czujnikowe). Komputerowe bazy danych powinny zawierać informacje na temat stanu etatowego i rodzajów środków łączności, stanowisk dowodzenia poszczególnych szczebli, innych środków emitujących energię, ugrupowania środków rozpoznania i zakłóceń radiowych, a także środków elektronicznych, jakie mogą wystąpić na każdym szczeblu dowodzenia i w każdej jednostce organizacyjnej przeciwnika.

Doktrynalne wzorce działań środków elektronicznych zawierają wszystkie dane o sposobach działań taktycznych 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 zmian w metodach szkolenia jednostek potencjalnego przeciwnika. Każda baza danych o siłach i środkach przeciwnika musi podlegać modyfikacji, szczególnie, gdy stwierdza się wprowadzenie do jednostek elektronicznych nowego sprzętu.

Oprócz danych dotyczących systemów i sprzętu elektronicznego należy gromadzić charakterystyki osobowo-zawodowe dowódców poszczególnych szczebli dowodzenia (jednostek elektronicznych), co pozwoli na ustalenie, jakich decyzji należy spodziewać się po określonym dowódcy, i właściwe prognozowanie działań strony przeciwnej. Za przygotowanie doktrynalnych wzorców działań przeciwnika odpowiada przełożony. Technika ich tworzenia jest różna w czasie pokoju i wojny. W czasie pokoju informacje o przeciwniku powinny być dostarczane przez przełożonego, a w czasie wojny nowe dane oraz informacje, potwierdzające działanie przeciwnika, jako pierwsze uzyskują pododdziały prowadzące walkę. Jest to więc obieg danych odwrotny od pokojowego.

W obydwu sytuacjach sekcja WE jest zobowiązana do posiadania aktualnej bazy danych o przeciwniku. Obowiązek aktualizacji baz danych spoczywa na sekcji WE w G 2, zajmującej się wnikliwą analizą wszelkich konfliktów zbrojnych. Taktyka i sposoby wykorzystania

sprzętu stosowanego w różnych konfliktach zbrojnych powinny być analizowane i przesyłane do zainteresowanych jednostek jako załączniki do obowiązujących instrukcji i regulaminów. Wzorce doktrynalne są przechowywane w specjalnych bankach informacji. Po rozpoczęciu działań wojennych wzorce opisujące węzły elektroniczne są wykorzystywane do wskazywania ważnych obiektów, które należy rozpoznać lub zakłócić. Służą one także do wskazania celów, które powinny być niszczone środkami ogniowymi. Przykładowy wzorzec doktrynalny rozmieszczenia węzłów łączności ZT przeciwnika w natarciu przedstawia załącznik 1.

Dane zawarte we wzorcach działań elektronicznych potwierdza sekcja walki elektronicznej, do której 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. Z reguły tworzy się kilka oddzielnych wzorców elektronicznych przeciwnika. Pierwszy zawiera dane o węzłach łączności, drugi dotyczy pozostałych urządzeń emitujących energię elektromagnetyczną, a trzeci określa zasady użycia sił i środków WE. Przykładowy wzorzec rozmieszczenia środków WE przeciwnika przedstawia załącznik 2. Pomimo tego że dla jednego związku taktycznego powstaje kilka wzorców, to pomagają one uniknąć dwuznaczności obrazu sytuacji elektronicznej. Wzorce powinny też uwzględniać liczbę i typ urządzeń związanych z każdym węzłem elektronicznym przeciwnika. Poziom szczegółowości oraz klasyfikacja tych wzorców zależy od obowiązujących wymagań.

Do pełnego zobrazowania sytuacji elektronicznej jest również niezbędna analiza działań przeciwnika powietrznego i systemów przeciwlotniczych. Dlatego ze szczególną uwagą powinno się analizować wzorce doktrynalne działań samolotów (śmigłowców) i elementów OPL. Przykłady takich wzorców zawierają załączniki 3 i 4.

Wykonując wzorce doktrynalne węzłów łączności i węzłów elektronicznych na potrzeby oceny i prognozy zagrożenia ze strony przeciwnika (np. zakłócania radiowego), dokonuje się oceny tego zagrożenia o jeden szczebel w dół, gdy wojska własne są w obronie, a o dwa szczeble w dół, gdy prowadzi się natarcie.

Ocena aktualnej sytuacji elektronicznej. Na szczeblu związku taktycznego sekcja WE zbiera dane z rozpoznania elektronicznego i zakłócania elektronicznego, które wykorzystuje do opracowania sytuacji elektronicznej oraz sprecyzowania kierunku działania przeciwnika i celu, jaki chce osiągnąć. Podległe pododdziały (np. batalion rozpoznawczy) analizują opracowane przez sekcję WE warianty zagrożenia elektronicznego i zdarzeń elektronicznych i przekształcają je do takiego poziomu szczegółowości, jaki wymagany jest dla wsparcia jednostek wykonujących zadanie bojowe.

Oleat sytuacji elektronicznej sekcja WE wykonuje na podstawie:

– własnych danych o sytuacji bieżącej;

– wiadomości od przełożonego;

– danych od jednostek osłonowych, sąsiadów;

– innych źródeł (np. uchodźców, dezerterów, wojsk OT).

Treścią tego dokumentu jest graficzny obraz odzwierciedlający sytuację elektroniczną połączoną z koncepcją doktrynalną, zgodną z obowiązującymi zasadami rozmieszczenia techniki elektronicznej i prawdopodobnym zamiarem przeciwnika, bez odniesienia do terenu i warunków meteorologicznych. Tak przygotowany oleat jest podstawą do dalszych rozważań nad prawdopodobnym działaniem przeciwnika. Dokument ten sporządza się na co najmniej dwóch oleatach, w takiej skali jak wykorzystywane mapy[45]. Na jednym oleacie rysowane są węzły łączności, a na drugim inne emitery energii EM. Mogą być wytworzone kolejne wzorce, np. z rozmieszczeniem środków walki elektronicznej – będzie to tylko zależało od potrzeb i szczegółowości oceny.

Wiadomości z banków danych (wzorce węzłów łączności i węzłów elektronicznych) przerysowuje się na oleaty z zachowaniem norm ugrupowania, a następnie uaktualnia się je na podstawie sytuacji elektronicznej (załączniki 5 i 6). Dla przejrzystego zobrazowania sytuacji wszystkie potwierdzone wiadomości o przeciwniku uzyskane od przełożonego i podwładnych są traktowane jako pewne i nanosi się je linią ciągłą, natomiast położenie jednostek elektronicznych wynikające z zasad doktrynalnego działania przedstawia się liniami przerywanymi. W ten sposób powstaje przejrzysty, prawdopodobny obraz aktualnego położenia elementów elektronicznycho wojsk przeciwnika (fotografia sytuacji).

Oleaty sytuacji elektronicznej stanowią dla oficerów walki elektronicznej pomocnicze narzędzie, niezbędne do określenia potrzeb w zakresie uzupełnienia danych o elementach elektronicznych. Podczas oceny sytuacji elektronicznej analizuje się i ustala:

– ogólną ilość obiektów w pasie rozpoznania (w strefie odpowiedzialności rozpoznawczej dywizji);

– ilość źródeł rozpoznania obsługujących obiekty w pasie rozpoznania dywizji z podziałem na pasma częstotliwości;

– ilość i rodzaj obiektów oraz źródeł rozpoznania, które ze względu na promieniowaną energię, mogą się znaleźć w zasięgu rozpoznania elektronicznego w trakcie realizacji zadania przez dywizję;

– najbardziej prawdopodobne rodzaje emisji, ich ewentualną informatywność i cechy rozpoznawcze możliwe do identyfikacji w procesie rozpoznania;

– gęstość zajętości pasma częstotliwości.

W zakończeniu oceny sytuacji elektronicznej precyzuje się wnioski wynikające z potrzeb rozpoznawczych, to znaczy określa się liczbę obiektów i źródeł, których rozpoznanie jest konieczne (lub pożądane) z uwagi na zadania bojowe realizowane przez dywizję. Ponadto ustala się priorytety rozpoznawcze co do poszczególnych obiektów i źródeł.

Kolejnym etapem pracy oficerów walki elektronicznej będzie wypracowanie prawdopodobnych wariantów działania elektronicznego przeciwnika w walce. Wypracowane warianty

[45] L. Ciborowski; *Planowanie i organizowanie walki zbrojnej wg poglądów NATO*, cz. II: *Informacyjna preparacja pola walki*, AON, Warszawa 1996, s. 36.

są potrzebne między innymi oficerom komórki G 3 i wsparcia ogniowego do skoordynowania działań jednostek wykonujących zadanie bojowe.

Wariantowanie zagrożeń elektronicznych. Warianty zdarzeń elektronicznych powinny być opracowywane z uwzględnieniem oceny przygotowanej przez oficerów z sekcji planowania i kierowania rozpoznaniem. Na tej podstawie oficerowie sekcji walki elektronicznej określają prawdopodobny wariant działania przeciwnika oraz potrzeby w zakresie uzupełniania brakujących danych. W wypracowanym wariancie powinno się uwzględnić wpływ pogody i terenu na działania bojowe przeciwnika oraz w określonym czasie opisowo lub w sposób graficzny prognozować, jak jego siły i środki będą wykonywać manewr (np. wzdłuż jakich dróg podejścia i korytarzy manewru, z wykorzystaniem jakich środków łączności). Ponadto należy brać pod uwagę, w jakim zakresie działanie przeciwnika może odbiegać od wzorców doktrynalnych lub w jaki sposób przeciwnik może zmieniać szerokość i głębokość ugrupowania czy rozmieszczenie elementów ugrupowania bojowego, aby sprostać wymaganiom pogody i terenu.

Rozważając wpływ pogody i terenu na warunki rozprzestrzeniania się energii elektromagnetycznej oraz działań przeciwnika odbiegających od wzorców doktrynalnych, należy dokonać analizy jego możliwości w zakresie zapewnienia łączności, wykrywania celów, kierowania ogniem, rozpoznania i zakłócania elektronicznego. Analiza taka jest niezbędna w celu zapewnienia maksymalnej ochrony przed oddziaływaniem elektronicznym przeciwnika na systemy wojsk własnych. Opracowywany wariant zagrożenia elektronicznego powinien uwzględniać dane z rozpoznania elektronicznego, które pozwolą na ustalenie urządzeń elektronicznych przeciwnika oraz potencjalnych rejonów ich rozmieszczenia.

Praktyką jest, że analitycy sekcji WE nakładają wzorce doktrynalne na oleaty przeszkód terenowych i dróg podejścia – w celu określenia najlepszych pozycji rozwinięcia urządzeń emitujących energię elektromagnetyczną, które przeciwnik może wykorzystać do zakłócania potencjalnych obiektów. Trzeba rozważyć także działania przeciwnika mające na celu maskowanie stanowisk dowodzenia (punktów obserwacyjnych) przed rozpoznaniem i zakłóceniami stosowanymi przez stronę przeciwną. W obrębie danego segmentu korytarza manewru analizuje się przewidywane rozmieszczenie jednostek przeciwnika (węzłów łączności) oraz innych emiterów energii. W trakcie wariantowania zdarzeń elektronicznych (sytuacji) muszą zostać rozważone normy taktyczne, sposoby i możliwości działania przeciwnika, szczególnie te, które powodują uzyskanie korzystnego stosunku sił, tempa działań oraz zaskoczenia. Analiza danych z rozpoznania elektronicznego i wariantów zdarzeń elektronicznych koncentruje się na określeniu linii widzialności optycznej i radiowej. Ponadto ustala się 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 elektronicznych ujmuje się zarówno charakterystyki emisji elektromagnetycznych poszczególnych elementów, jak i ich umiejscowienie. Pogoda i teren mają wpływ na wykorzystanie systemów łączności i innych urządzeń emitujących energię oraz ograniczają rozmieszczenie poszczególnych elementów tych systemów. Charakterystyka wariantów użycia źródeł energii elektromagnetycznej zmienia się w zależności od czasu i miejsca na polu walki. Oficerowie grupy rozpoznania i zakłóceń elektronicznych, dokonując analiz systemów elektronicznych i węzłów doktrynalnych, muszą się z tym liczyć i reagować na zmiany z odpowiednim wyprzedzeniem.

Po rozpoczęciu zbierania danych przez własne systemy do sekcji WE przekazywane są aktualne dane o ugrupowaniu przeciwnika oraz jego działaniach elektronicznych. Analitycy WE wstępnie opracowują napływające dane i porównują je z danymi zawartymi (opisanymi) w wariantach sytuacji, we wzorcu zagrożeń i węzłów elektronicznych. Pozwala to na:

– przekazanie aktualnych danych przełożonemu i podległym jednostkom w celu wymiany wiadomości o przeciwniku;

– dokonanie korekty wariantów zagrożenia elektronicznego i zdarzeń elektronicznych;

– dokonanie identyfikacji emiterów energii elektromagnetycznej przez sekcję walki elektronicznej wraz ze współpracującymi oficerami z innych rodzajów służb;

– skorygowanie lokalizacji obiektów elektronicznych przeciwnika na podstawie ich cech identyfikacyjnych, ustalenie linii rozgraniczenia wojsk oraz wyselekcjonowanie ważnych celów (obiektów) elektronicznych.

Efektem pracy oficerów WE z G 2 jest opracowanie prawdopodobnego wariantu działania przeciwnika, po czym następuje jego ostateczna weryfikacja podczas spotkań roboczych komórek G 2 i G 3. Finałem tych spotkań jest wybór wariantu zagrożenia elektronicznego (wariant kompatybilny z wariantem działania przeciwnika wykonanym przez sekcję planowania G 2), na jego podstawie dokonuje się szczegółowego planowania użycia własnych pododdziałów elektronicznych. W przypadku gdy wariant wybrany przez G 2 nie zostaje zaakceptowany, wraca się do pozostałych wariantów, wcześniej odrzuconych.

Przy wariantowaniu działań przeciwnika powinien również powstać plan alternatywny (zapasowy), który znacząco odbiega od wzorców doktrynalnych. Taki wariant działania przeciwnika, zazwyczaj przeczy logice działania i czasami jest sprzeczny z zasadami walki znanymi dotychczas stronie przeciwnej. Planem alternatywnym może być także odrzucony wariant zagrożenia z niektórymi elementami działania przeciwnika sprzecznymi z obowiązującymi normami. Przykładowe warianty zagrożeń elektronicznych ilustrują załączniki 7, 8, 9.

5.3.6. Oleat zdarzeń elektronicznych

Na podstawie wariantu zagrożenia elektronicznego jest sporządzany (wspólnie z G 2) wariant zdarzeń elektronicznych. Swoją formą nie odbiega od oleatu zdarzeń wykonywanego prze oficerów z sekcji planowania i kierowania rozpoznaniem G 2. Różni się jednak położeniem rejonów zainteresowania (NAI)[46] i ich znaczeniem (chociaż w niektórych przypadkach mogą się one pokrywać). Jeżeli czas pozwala, opracowuje się kolejne oleaty zdarzeń elektronicznych do pozostałych wariantów oceny zagrożenia. Połączenie danych z rozpoznania elektronicznego przełożonego i własnych elementów rozpoznawczych pozwala na określenie ważnych zdarzeń na polu walki oraz wytypowanie urządzeń promieniujących fale elektromagnetyczne, które dostarczają danych na temat kierunków prowadzonych działań przez przeciwnika i celów, jakie pragnie osiągnąć. Oficer WE dokonujący analizy musi dostrzec różnicę pomiędzy zdarzeniami, które już zostały zaobserwowane, a tymi, które są tylko przewidywane. Ponadto kontroluje działania przeciwnika zmierzające do wprowadzania nas w błąd, aby nie dopuścić do skupienia wysiłku własnych jednostek rozpoznania na obiektach (obszarach) pozornych.

Po rozpoczęciu działań bojowych wiedza o tym, gdzie i kiedy może nastąpić istotne zdarzenie na polu walki, może zostać wzbogacona[47]. Gdy przeciwnik porusza się po drogach podejścia, wówczas rozpoznanie elektroniczne może ujawnić węzły łączności (elektroniczne) stanowisk dowodzenia i stacji kontroli w szczególnie ważnych (kluczowych) obszarach. Obszary te zostają oznaczone jako NAI.

Rejony zainteresowania celami nie zawsze będą się znajdować na drogach podejścia. Często występować będą poza nimi ze względu na specyfikę pracy oraz możliwości bojowe sprzętu elektronicznego. Rejony te są ważne, gdyż znajdują się w najbardziej prawdopodobnych miejscach decydujących zdarzeń czy też działań na polu walki oraz mogą w nich występować cele wysoko opłacalne[48].

Rejony zainteresowania stanowią podstawę do wariantowania zdarzeń, ponieważ wskazują kierunki działania przeciwnika, ogniskują zbieranie danych oraz są uwzględniane w opracowaniu wymagań wobec informacji pozyskiwanych przez rozpoznanie. Rejony zainteresowania celami są dla rozpoznania i zakłócania elektronicznego obszarami wzdłuż dróg podejścia oraz poza nimi, a występowanie źródeł emisji elektromagnetycznych przeciwnika może potwierdzić lub zaprzeczyć wypracowanej wersji przebiegu działań. Aby trafnie określić zamiary przeciwnika, aktywność urządzeń promieniujących energię elektromagnetyczną 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 urządzeń promieniujących energię może również stanowić dla rozpozna-

[46] NAI – Named Areas of Interest.

[47] Przeciwnik będzie dążyć do ograniczenia informacji o swoim działaniu i stan naszej wiedzy może nie zmienić się mimo rozpoczęcia działań.

[48] Cele o znaczeniu decydującym dla działania wojsk przeciwnika.

nia i zakłócania elektronicznego wskazówkę o istnieniu jakiegoś urządzenia w obrębie obszaru niekontrolowanego. Numeracja NAI ustalana jest w czasie spotkań koordynacyjnych wewnątrz G 2, pomiędzy oficerami sekcji planowania i WE. Ustalenia te są niezbędne dla wyeliminowania błędów i dwuznaczności w oznaczeniach lub oznaczeń dublujących, ponieważ niektóre obszary NAI mogą występować w tym samym miejscu.

Wariant zdarzeń opracowany przez analityków grupy rozpoznania elektronicznego z sekcji WE w procesie EPB dostarcza danych do ustalenia kolejności oddziaływania na przeciwnika oraz na podstawie rozpoznanych emisji EM – sposobu i rodzaju zakłócania. Wariant zdarzeń elektronicznych jest konkretyzowany w toku „gry wojennej" (pomiędzy G 2 i G 3) – dla każdego wariantu działań przeciwnika, od momentu ich rozpoczęcia do momentu osiągnięcia celów (obiektów) tych działań. Jeśli będą miały miejsce zdarzenia lub działania wojsk sygnalizowane pracą urządzeń promieniujących energię elektromagnetyczną, to do ich synchronizacji w obrębie każdej drogi podejścia będą wykorzystywane czasowe linie wyrównania (TPL)[49]. Oleat zdarzeń elektronicznych przedstawia załącznik 10[50].

5.3.7. Oleat elektronicznego wzorca wsparcia decyzji

Oleat elektronicznego wzorca wsparcia decyzji (EDST)[51] jest wykonywany na potrzeby śledzenia prognozowanej sytuacji elektronicznej przeciwnika i pomocy dowódcy w procesie podejmowania decyzji. Z elektronicznego wzorca wsparcia decyzji na wzorzec wsparcia decyzji wykonywany przez G 3 są nanoszone tylko informacje niezbędne w procesie podejmowania decyzji przez dowódcę ZT, wspierające jego zamiar rozegrania walki. Pozostałe informacje z elektronicznego wzorca wsparcia decyzji służą G 2 i sekcji walki elektronicznej do kontroli działania przeciwnika.

W wyniku analizy zdarzeń elektronicznych są wskazywane i opisywane kluczowe elektroniczne obiekty (cele) przeciwnika wraz z obszarami oddziaływania elektronicznego (TAI)[52]. Oficerowie sekcji WE prowadzący analizę danych otrzymanych z pododdziału WE określają obszary oddziaływania elektronicznego (ogniowego). Podstawą wyboru TAI jest analiza obszarów NAI w czasie odprawy koordynacyjnej wewnątrz G 2 oraz wiadomości z rozpoznania elektronicznego napływające w czasie przebiegu EPB. Podczas odprawy koordynacyjnej ustala się rejony TAI, które są najistotniejsze do rozpoznania i zakłócania, oraz te, które się tylko kontroluje, nie zapominając, iż przeciwnik może rozwinąć swoje środki elek-

[49] TPL – Timephase Line – czasowa linia wyrównania.

[50] Koncepcja rozwoju sytuacji elektronicznej po stronie przeciwnika ma odzwierciedlenie również w aneksie „Walka elektroniczna" (pkt 3b).

[51] EDST – Electronic Decision Support Templat – elektroniczny wzorzec wsparcia decyzji. Nazwa może kojarzyć się z dokumentem wykonywanym przez komputer, co wynika z przetłumaczenia oryginalnego dokumentu z języka angielskiego. Dokument ten może być wykonywany przy pomocy techniki komputerowej, ale nie jest dokumentem elektronicznym.

[52] TAI (Target Areas of Interest) – obszar oddziaływania ogniowego. W odniesieniu do walki elektronicznej jest to obszar oddziaływania energią elektromagnetyczną.

troniczne poza prognozowanymi rejonami zainteresowania. Obszary NAI i TAI służą do kontroli przemieszczania elementów elektronicznych przeciwnika, dając w ten sposób obraz jego działań.

Gdy wariant przebiegu walki elektronicznej i niszczenia obiektów przeciwnika jest już ustalony, sekcja WE G 2 opracowuje EDST, aby zapewnić dowódcy dywizji pełny obraz proponowanych rozwiązań. Dowódca, posiadając takie informacje o przeciwniku, jest w stanie określić, jak najefektywniej wykorzystać środki walki znajdujące się pod jego kontrolą.

Wzorzec wsparcia decyzji w zakresie elektroniki opisuje obszary oddziaływania elektronicznego (określone przez rozpoznanie elektroniczne), punkty decyzyjne (określone przez G 3) oraz czasowe linie wyrównania – wzdłuż każdej drogi podejścia (korytarza ruchu) i rejonów poza nimi, gdzie można zatrzymać siły przeciwnika lub ograniczyć jego możliwości: ogniowe, manewrowe, elektroniczne oraz uniemożliwić mu działania. Obszar oddziaływania elektronicznego obejmuje rejon, w którym przeciwnik może zostać pozbawiony zdolności bojowej, przyjąć narzucony sposób walki lub zaniechać planowanego wariantu działania.

Obszary oddziaływania ogniowego (elektronicznego), pierwotnie mogą być identyfikowane jako NAI. Ponieważ NAI wykorzystuje się w celu zbierania danych potwierdzających słuszność prognozowanego wariantu działania przeciwnika, mogą być one usytuowane w głębi ugrupowania przeciwnika. Z kolei TAI wyznacza się na głębokości oddziaływania środków ogniowych lub elektronicznych. Jeżeli NAI i TAI pokrywają się, to obszary zainteresowania nie muszą być uwzględniane na wzorcu wsparcia decyzji. Decyzje co do sposobu wykorzystania środków walki elektronicznej mogą być wypracowywane dla każdego punktu decyzyjnego i linii czasowej. Decyzje te mogą dotyczyć wspomagania działań obronnych, zaczepnych, opóźniających i pościgowych. Mogą mieć na celu wprowadzenie przeciwnika w błąd albo spowodowanie zmiany priorytetów w zbieraniu danych. Punkty decyzyjne dotyczące wykorzystania środków WE wskazują dowódcy te momenty walki, które wymagają podjęcia decyzji. Gdy EDST jest już przygotowany, dowódca zapoznaje się z jego treścią i opiniami innych specjalistów, aby upewnić się, że działania własnych wojsk będą efektywne. Przykład EDST z TAI i punktami decyzyjnymi – jest przedstawiony w załączniku 11.

Elektroniczny wzorzec wsparcia decyzji wraz z oleatem przeszkód terenowych (MCOO)[53] przesyła się również do batalionu rozpoznawczego w celu weryfikacji postawionego zadania. Zbieranie danych wymaga bowiem skoordynowanego wysiłku wszystkich zbierających i potwierdzających dane z rejonów zainteresowań celami elektronicznymi (NAI). Sztab batalionu rozpoznawczego na podstawie prognozy zdarzeń musi sprecyzować potrzeby informacyjne z wybranych obszarów zainteresowania.

Proces prognozowania działań elektronicznych przeciwnika kończy się z chwilą podjęcia decyzji przez dowódcę. Dla sekcji WE jest to sygnał do rozpoczęcia szczegółowego opracowania dokumentów do przyjętego wariantu działania wojsk własnych i przeciwnika.

---

[53] MCOO (Modified combined obstacie overlay) – zmodyfikowana oleata przeszkód terenowych.

5.3.8. Opracowanie koncepcji walki elektronicznej w działaniach taktycznych

Etap opracowania planu walki elektronicznej w działaniach taktycznych następuje po odprawie decyzyjnej, w czasie której dowódca zatwierdza wariant działania własnych sił w stosunku do przyjętego wariantu działania przeciwnika.

Opracowanie koncepcji (planu) walki elektronicznej w działaniach taktycznych dla jednostek WE rozpoczyna się od oceny posiadanych sił i środków rozpoznania i zakłócania elektronicznego, ich możliwości wsparcia w wykonaniu zadania bojowego dywizji, oceny terenu i warunków meteorologicznych. Przedsięwzięcia tego etapu częściowo są realizowane podczas wariantowania zagrożenia elektronicznego, ale wówczas większą uwagę zwraca się na systemy elektroniczne przeciwnika niż na własne elementy elektroniczne.

Korzystając z danych ustalonych podczas oceny sytuacji elektronicznej, oficerowie sekcji WE szacują liczbę źródeł możliwych do wykrycia w strefie odpowiedzialności rozpoznawczej ZT oraz precyzują możliwości zakłócania elektronicznego celów wysoko opłacalnych. Następnie wnikliwie analizują rzeźbę terenu i jego pokrycie, ustalając możliwe do uzyskania zasięgi (linie horyzontu radiowego) rozpoznania i zakłócania na planowanych rubieżach rozwinięcia oraz możliwości w zakresie lokalizacji źródeł promieniowania energii EM.

Kolejną czynnością jest ustalenie możliwych kierunków uderzeń samolotów, śmigłowców i BŚR, ich stref dyżurowania i prawdopodobnych obiektów przeznaczonych do niszczenia w ugrupowaniu ZT.

Dysponując danymi co do obiektów przeznaczonych do rozpoznania i zakłócania elektronicznego, ustala się głębokość rozpoznania i zakłócania, jak również dokładność w zakresie lokalizacji źródeł rozpoznania, a następnie przechodzi się do oceny aktualnego położenia sił i środków pododdziału elektronicznego. W tym względzie analizuje i ocenia się stopień, w jakim ich aktualne położenie odpowiada potrzebom wynikającym z zadania dywizji, ustala się przy tym ewentualne sposoby i czasy przemieszczeń na rubieże rozwinięcia systemu walki elektronicznej. W tym czasie kompania elektroniczna zazwyczaj przygotowuje się do działań na podstawie zadań wynikających z zarządzenia przygotowawczego.

W końcowym etapie oceny posiadanych sił i środków walki elektronicznej dokonuje się porównania potrzeb z istniejącymi możliwościami, konkretyzuje się rodzaj i liczbę obiektów oraz źródeł rozpoznania, które powinny i mogą być rozpoznawane. Wyznacza się obiekty do zakłócania. Wyniki tych kalkulacji przedstawia się w zestawieniach i tabelach. Formy pracy i sposoby przedstawiania wspomnianych zamierzeń muszą w efekcie udzielić odpowiedzi na pytanie: jakich celów poszukiwać (rozpoznawać), a jakie zakłócać elektronicznie.

Po otrzymaniu rozkazu operacyjnego od przełożonego sztab ZT wstępnie precyzuje możliwe sposoby użycia sił i środków WE, ze szczególnym uwzględnieniem możliwości ich użycia na pierwszej rubieży rozwinięcia. Te pierwsze decyzje są przekazywane już w trakcie planowania w zarządzeniach przygotowawczych. Jeżeli dywizja nie otrzymała jeszcze rozka-

zu operacyjnego od przełożonego, a tylko zarządzenie przygotowawcze, to również powinna wysłać do podwładnego zarządzenie przygotowawcze, aby mógł rozpocząć planowanie.

Koncepcję użycia pododdziału WE oficerowie sekcji WE ZT nanoszą na oleat „Plan walki elektronicznej[54]", przedstawiając uzasadnienie w postaci danych kalkulacyjno-uzupełniających zawartych w tabelach, schematach, itp. w oddzielnych opracowaniach. Mapa sytuacyjna jest jedna dla całej sekcji.

Przeprowadzone kalkulacje i obliczenia oraz zaplanowany scenariusz przebiegu WE jest ujmowany w aneksie „Walka elektroniczna" (pkt 3b). Stanowi on uzupełnienie scenariusza przebiegu działań elektronicznych i w całości tworzy koncepcję prowadzenia walki elektronicznej. Na podstawie tej koncepcji przygotowuje się także plan zakłóceń (będzie on przedmiotem rozważań w następnym podrozdziale).

Zaplanowane użycie pododdziału WE nanoszone jest na prowadzoną w komórce WE mapę sytuacyjną. Mapa sytuacyjna jest aktualizowana w miarę otrzymywania okresowych meldunków od podległych elementów WE. W czasie bezpośredniego kontaktu kierownika G 2 z oficerami pionu G 3 i wsparcia ogniowego dokonuje się uzgodnień, które mają zapobiec powstaniu sytuacji, w czasie których elementy WE byłyby narażone na wzajemne zakłócanie. Mapa sytuacyjna może zawierać także informacje o zasięgu własnego rozpoznania i zakłócania elektronicznego oraz technicznych możliwościach innych urządzeń elektronicznych. Praktyczny sposób prowadzenia mapy sytuacyjnej może być różny, np.:

1. Informacje od przełożonego nanosi się kolorem czarnym a własne zamierzenia kolorem niebieskim.
2. Każdy podsystem rozpoznania i zakłócania nanosi się innym kolorem.
3. Wykonuje się oddzielne oleaty, obrazujące działanie każdego podsystemu, po czym nakłada się jedne na drugie w celu zobrazowania całego systemu rozpoznania i zakłócania elektronicznego.

W trakcie organizowania walki elektronicznej w działaniach taktycznych najistotniejszymi dokumentami wykonywanymi przez sekcję WE są: *Aneks H „ Walka elektroniczna"* do rozkazu operacyjnego wraz z apendyksami. Plan walki elektronicznej jest jednym z apendyksów do aneksu i stanowi wraz z nim całość.

Obok wymienionych dokumentów prowadzi się również inne np.: mapę informacyjną, dziennik działań bojowych, zapotrzebowanie na wiadomości, komunikaty elektroniczne (dołącza się je do ogólnego komunikatu rozpoznawczego), okresowe meldunki elektroniczne.

[54] Oleat „Plan WE" traktowany jest jako jeden z apendyksów. Może być wykonany na oddzielnej folii lub w połączeniu z oleatem „Plan rozpoznania". W SZ RP nie podjęto dotychczas decyzji w tej sprawie. Przeważa opcja za połączeniem tych dwóch dokumentów.

5.4. Stawianie zadań w zakresie walki elektronicznej w działaniach taktycznych

5.4.1. Aneks „Walka elektroniczna"

Aneks H do rozkazu operacyjnego – „Walka Elektroniczna". Aneks może być przesyłany razem z rozkazem operacyjnym lub oddzielnie. W tytule aneksu występuje odpowiednia litera wynikająca z podziału dokumentów wykonanych przez oficerów G 3. Przydział odpowiedniej litery uzależniony jest od liczby wykonywanych aneksów. Dość często spotyka się litery „F' lub „H" odpowiadające walce elektronicznej, ale nie jest to regułą.

W aneksie „Walka elektroniczna" do rozkazu operacyjnego (załącznik 12) są zawarte szczegółowe zadania precyzujące, co rozpoznawać i zakłócać, gdzie i kiedy. Aneks składa się z następujących części:

– pierwsza – dotyczy elektroniki przeciwnika, w krótki i zwięzły sposób charakteryzuje jego siły i środki elektroniczne, a także siły i środki walki elektronicznej, które mogą oddziaływać na własne elementy ugrupowania; wyniki porównania obiektów, na które będzie oddziaływał przeciwnik swoimi środami WE, można przedstawić za pomocą liczb lub wskaźników procentowych;

– druga – zawiera zadanie dla związku taktycznego, czyli określa gdzie, kiedy i jak prowadzić walkę elektroniczną z przeciwnikiem;

– trzecia – dotyczy koncepcji prowadzenia WE, czyli koncepcji (zamiaru) działania, zadań dla wszystkich jednostek ZT (dotyczących obrony elektronicznej) i ich koordynacji;

– czwarta – dotyczy zabezpieczenia działań, czyli wsparcia logistycznego, bojowego i uzupełnień;

– piąta – ujmuje problemy dowodzenia i łączności.

Do aneksu są dołączane apendyksy określające te informacje, które nie zostały ujęte w aneksie. Liczba apendyksów jest uzależniona od ilości niezbędnych danych, jakie należy przekazywać jednostkom w celu ułatwienia realizacji zadania.

Apendyksy do aneksu „Walka elektroniczna". W apendyksach dotyczących walki elektronicznej są uwypuklone przede wszystkim informacje przeznaczone dla kompanii elektronicznej. Apendyksy mogą zawierać informacje dla pozostałych jednostek, ale dane te będą dotyczyły głównie obrony elektronicznej.

Ilość apendyksów nie jest ograniczona. Nie są to dokumenty normatywne. Powinny być wykonane i traktowane jako dokumenty pomocnicze, służące konkretyzowaniu warunków i zadań. Apendyksy dołączane do aneksu „Walka elektroniczna" mogą być następujące:

– oleat walki elektronicznej przeciwnika (powstaje w procesie EPB);

– plan obrony elektronicznej;

– oleat walki elektronicznej wojsk własnych;

– plan zakłóceń elektronicznych;

– lista celów elektronicznych;

– rejony i częstotliwości zastrzeżone;

– wykaz wykrytych środków elektronicznych przeciwnika;

– wykaz punktów i rejonów NAI i TAI;

– oleat z podziałem obszaru działania, z umowną siatką współrzędnych np. do prowadzenia wsparcia lotniczego i zakłócania elektronicznego;

– oleat z planem zapasowym;

– inne według potrzeb.

Apendyks „Oleat walki elektronicznej przeciwnika" (załącznik 13) jest wykonywany przez oficerów sekcji WE komórki G 2 na folii lub kalce technicznej. Dokument ten przedstawia ugrupowanie sił i środków walki elektronicznej przeciwnika działającego na kierunku ZT oraz potencjalne zasięgi jego oddziaływania elektronicznego na systemy elektroniczne ZT. Na oleacie ujmuje się:

– punkty odniesienia;

– linie rozgraniczenia;

– rubież styczności wojsk;

– wykryte elementy ugrupowania bojowego pododdziałów walki elektronicznej (linią ciągłą);

– prawdopodobne rejony rozwinięcia elementów ugrupowania bojowego pododdziałów walki elektronicznej (linią przerywaną);

– zasięgi rozpoznania (namierzania);

– zasięgi zakłóceń;

– zasięg użycia NZJU.

W przypadku braku wiadomości o rejonach rozwinięcia elementów WE przeciwnika zaznacza się schematycznie, jakie siły WE mogą występować w strukturze organizacyjnej przeciwnika.

Plan obrony elektronicznej wykonują oficerowie sekcji WE komórki G 2 w ścisłej współpracy z zespołem działań przeciwrozpoznawczych komórki G 2 oraz komórką do spraw operacyjnych G 3. Dokument ma formę tabeli, w której wymieniane są kolejne przedsięwzięcia przeciwdziałające rozpoznaniu elektronicznemu przeciwnika i zapewniające skuteczną pracę własnym środkom elektronicznym. W kolejnych rubrykach określa się czas realizacji danego przedsięwzięcia, wykonawcę, a także odpowiedzialnego za kontrolę wykonania tego przedsięwzięcia. Przykład apendyksu przedstawiony jest poniżej.

Tabela 1

APENDYKS DO ANEKSU „WALKA ELEKTRONICZNA"
PLAN OBRONY ELEKTRONICZNEJ

Lp.	Przedsięwzięcie	Czas wykonania	Wykonawca	Odpowiedzialny	Uwagi
1.	*Zabezpieczenie kontroli wykorzystywania aparatury utajniającej i przestrzegania zasad korespondencji radiowej*	*Od 08.00 do 17.05*	*Szef łączności 2 KZ*	*Szef łączności 2 KZ*	

Apendyks „Plan walki elektronicznej wojsk własnych" (załącznik 14)[55] opracowują oficerowie zespołu walki radioelektronicznej w ścisłym porozumieniu z zespołem kierowania rozpoznaniem i komórką do spraw operacyjnych. Dokument ten jest sporządzany na folii lub kalce technicznej. Ujmuje się w nim:

– punkty odniesienia (koordynaty);

– strefy odpowiedzialności rozpoznawczej ZT;

– rubież styczności wojsk(FEBA);

– linie rozgraniczenia;

– zasadnicze i zapasowe rubieże rozwinięcia pododdziałów WE (na rubieżach zaznacza się dozwolone rejony rozwinięcia środków WE);

– zadania pododdziałów WE;

– zasięgi rozpoznania (namierzania);

– zasięgi zakłóceń;

– zasięgi użycia lub planowane rejony użycia NZJU;

– stanowiska ogniowe pododdziałów artylerii strzelającej pociskami z NZJU;

– stanowiska dowodzenia sztabu własnego i nadrzędnego;

– jednostki współdziałające po prawej i lewej stronie;

– lądowiska śmigłowców WE;

– strefy dyżurowania aparatów latających przeciwnika;

– obszary zainteresowania (NAI) i oddziaływania elektronicznego (TAI).

Apendyks „Plan zakłóceń elektronicznych" (załącznik 15) jest sporządzany w G 3 przez oficerów zespołu walki elektronicznej we współdziałaniu z oficerami wsparcia lotniczego i artyleryjskiego. Dokument ten ma formę tabelaryczną. W dolnej części tabeli wymienia się zadania stawiane zakłóceniom oraz obszary zainteresowania, na które w pierwszej kolejności będą oddziaływać zakłócenia. Na osi czasu w górnej części tabeli dla każdej jednostki bojowej, która ma siły i środki zakłócające, nanosi się zadania z zakresu zakłóceń. Wskazuje się

[55] Patrz podrozdział 5.2.6.

także obszary, przeciw którym będą prowadzone zakłócenia, oraz obiekty objęte zakłóceniami. W wypadku planowania użycia nadajników zakłóceń jednorazowego użycia określa się w tym planie ilość kompletów oraz sposób ich użycia.

Apendyks „Wykaz celów elektronicznych" jest identyfikatorem celów elektronicznych przeciwnika. Do celów elektronicznych zaliczamy węzły łączności – stanowisk dowodzenia, pomocnicze, garnizonowe i inne; węzły elektroniczne – grupy stacji zakłóceń; posterunki namierzania radiowego; radiowe centra odbiorcze i nadawcze; posterunki radiolokacyjne i inne obiekty wyposażone w środki elektroniczne. Oficer zespołu walki elektronicznej, wykonując ten dokument, przyporządkowuje każdej jednostce (celowi elektronicznemu) kod identyfikacyjny. Przyporządkowanie celów następuje w porozumieniu z oficerami G 3 i wsparcia ogniowego. Jest to pierwszy etap w przygotowaniu dokumentu, jakim jest „Plan zakłóceń elektronicznych".

Apendyks „Rejony i częstotliwości zastrzeżone" (tabela 2) jest wykonywany przez oficerów zespołu walki elektronicznej komórki G 2 w ścisłym współdziałaniu z zespołem kierowania rozpoznaniem, zespołem działań specjalnych oraz komórką G 6. Pod pojęciem rejonu zastrzeżonego należy rozumieć wyznaczony przez przełożonego obszar terenu, w którym zabronione jest działanie elementów rozpoznawczych określonych szczebli dowodzenia. Rejony zastrzeżone określamy minimum trzema punktami charakterystycznymi z jednoczesnym podaniem ich współrzędnych. Częstotliwości zastrzeżone to częstotliwości używane przez przeciwnika i wykorzystywane przez organa WE jako źródło informacji rozpoznawczej. Częstotliwości zakazane to częstotliwości o takiej ważności, że nie mogą być nigdy zakłócane.

Apendyks „Wykaz wykrytych środków elektronicznych przeciwnika" (tabela 3) wykonują oficerowie zespołu walki elektronicznej na podstawie danych otrzymanych od szczebla nadrzędnego oraz jednostek aktualnie prowadzących rozpoznanie elektroniczne. Sporządzony w formie tabeli dokument stanowi dla podwładnych bank danych o wykrytych środkach elektronicznych pracujących w naszej strefie odpowiedzialności rozpoznawczej. Służy jednocześnie jako dokument pomocniczy do aktualizacji mapy informacyjnej i sytuacyjnej. W podanym czasie pracy pierwsze dwie cyfry określają dzień, a cztery następne godzinę i minutę (np. 10.17.30). Bardzo duże znaczenie dla identyfikacji źródła energii elektromagnetycznej mają parametry charakterystyczne: szybkość telegrafowania, głębokość modulacji, przesuw częstotliwości, szybkość obrotów anteny, częstotliwość powtarzania impulsów itd. Informacje te porównuje się ze wzorcami doktrynalnymi poszczególnych węzłów łączności lub elektronicznych.

Tabela 2

H-5-1
Klauzula tajności

APENDYKS DO ANEKSU „WALKA ELEKTRONICZNA"
REJONY I CZĘSTOTLIWOŚCI ZASTRZEŻONE

Rejony zastrzeżone			Częstotliwości zastrzeżone		Częstotliwości zakazane
1	Międzyleś	0432	2342	11634	1792
	Zapłocie	0440	1455	12354	1931
	Rządza	9836	2356	13546	5516
2	Myszadła	1648	3665	21456	36151
	Jaczew	1456	3790	23685	54006
	Sewerynów	1050	4133	35788	
3	Siodło	7248	5678	39000	
	Kamionka	7052	5789	42345	
	Żaków	7044	7890	43567	
4	Stawek	7254	8125	44550	
	Jeruzal	7058	8379	4797	
	Waliska	7072	8500	4900	
5	Jagoda	7140	8460	4932	
	Wiśnia	7334	8778	4689	

H-5-1
Klauzula tajności

Tabela 3

H-7-1
Klauzula tajności

APENDYKS DO ANEKSU „WALKA ELEKTRONICZNA"
WYKAZ WYKRYTYCH ŚRODKÓW ELEKTRONICZNYCH PRZECIWNIKA

Lp.	Częstotliwość pracy	Liczba stacji	Sygnały rozpoznawcze	Czas wykrycia	Rodzaj emisji	Obsługa obiektu	Miejsce pracy	Charakterystyczne parametry
1	3756	2	Vh7i	10.17.30	A1	1KZ	LUBLIN	
2	4451	1	DHJ-55	10.16.50	F1	2KZ	KRAŚNIK	

H-7-1
Klauzula tajności

5.4.2. Zarządzenie przygotowawcze

Zarządzenie przygotowawcze sporządza się i wysyła do podwładnych natychmiast po tym, jak dowódca przekaże wytyczne dla sztabu. Musi być ono krótkie, lecz zawierać taką ilość informacji, która wystarczy do rozpoczęcia procesu przygotowania walki przez podwładnych. Kolejne zarządzenia mogą być sukcesywnie wydawane dla zapewnienia podwładnym dopływu aktualnych informacji i umożliwienia jak najszybszego rozpoczęcia przez nich planowania i organizowania działań taktycznych.

Zarządzenie przygotowawcze nie ma ustalonego układu. Przyjmuje się jednak, że powinno zawierać:

1. **Tytuł** – słowa „Zarządzenie przygotowawcze".
2. **Położenie** – krótka informacja o położeniu wojsk własnych i przeciwnika.
3. **Zmiany w podporządkowaniu** – informacje o ewentualnych zmianach w podporządkowaniu powinny być przekazane podwładnym tak szybko, jak to możliwe, aby dać im jak najwięcej czasu na przejście w podporządkowanie nowych sił (lub na ich przekazanie).
4. **Czas podjęcia działań** – podanie podwładnym tego terminu pozwala im przeprowadzić realną kalkulację czasu.
5. **Charakter i czas przyszłych działań** – podwładny powinien otrzymać tyle informacji, aby mógł rozpocząć planowanie działań. Punkt ten może także zawierać sprecyzowane zadanie szczebla wydającego zarządzenie.
6. **Czas i miejsce wydania rozkazu operacyjnego** – określa się kto, gdzie i kiedy powinien stawić się w celu otrzymania rozkazu.
7. **Informacje na temat wsparcia logistycznego.**
8. **Wymagania dotyczące potwierdzenia otrzymania zarządzenia.**

6. PROWADZENIE WALKI ELEKTRONICZNEJ W DZIAŁANIACH TAKTYCZNYCH ZWIĄZKU TAKTYCZNEGO

6.1. Cel walki elektronicznej w działaniach taktycznych

Skuteczność działania związku taktycznego w dużej mierze jest uzależniona od sprawnie działającego systemu dowodzenia i nowoczesnych systemów kierowania uzbrojeniem. O sprawności działania tych systemów w coraz większym stopniu decyduje żywotność ich komponentów elektronicznych. Walka elektroniczna wpływa negatywnie na elektroniczne komponenty systemów dowodzenia i kierowania uzbrojeniem, przez co obniża ich możliwości techniczno-bojowe. Ma to z kolei wpływ na obniżenie potencjału bojowego wojsk oraz dynamikę prowadzenia walki.

Prowadzenie WE polega na zmniejszeniu efektywności lub pozbawieniu możliwości wykorzystania przez przeciwnika elektronicznych systemów dowodzenia i kierowania walk przy jednoczesnym zapewnieniu warunków niezakłóconej pracy analogicznym systemom własnych wojsk. Walka ta w ZT planowana jest przez sekcję WE komórki G 2, a prowadzona przez pododdział walki elektronicznej, w zakresie obrony elektronicznej także przez pozostałe jednostki ZT.

Ogólnym celem WE w działaniach taktycznych jest rozpoznawanie i zakłócanie środków i systemów elektronicznych przeciwnika przy jednoczesnym tworzeniu warunków do niezakłóconej pracy własnych środków.

Konkretny cel walki elektronicznej w działaniach taktycznych wynika każdorazowo z zadań, jakie otrzymał ZT, i może być różnie precyzowany. Dowódca, określając cel działania ZT, określa jednocześnie cele dla poszczególnych rodzajów wojsk i służb.

Ogólny cel WE, który chce osiągnąć dowódca ZT, powinien być precyzyjnie określany w stosunku do poszczególnych rodzajów środków, poszczególnych ogniw dowodzenia, kierunków i pasów działania. Podstawą do właściwego określenia celu jest rzetelnie przeprowadzona analiza i prognoza zagrożenia elektronicznego w ramach EPB oraz możliwości posiadanych sił i środków.

Ogólny cel WE może być realizowany przez cele pośrednie (cząstkowe). Cele pośrednie można realizować w różnych fazach działań taktycznych. Do takich celów można zaliczyć:

– zerwanie dowodzenia w jednym ogniwie na określony czas prowadzonych działań;

– zerwanie lub dezorganizowanie dowodzenia w jednym oddziale;

– zerwanie lub dezorganizowanie współdziałania w okresie wprowadzania nowych sił do walki;

– zerwanie lub dezorganizowanie współdziałania między środkami ogniowymi, a nacierającymi wojskami na określonym szczeblu;

– zakłócanie elektroniczne konkretnego systemu rozpoznania elektronicznego przeciwnika w określonym czasie;

– zakłócanie elektroniczne określonego systemu kierowania środkami ogniowymi;

– utrudnienie przeciwnikowi zakłócania systemów radiolokacyjnych lub kierowania środkami walki;

– utrudnienie dezorganizowania dowodzenia wojskami własnymi.

Cele pośrednie powinny być tak precyzowane, aby ich osiągnięcie dawało wymierne korzyści dla walczących wojsk, a zarazem wyzwalało możliwości realizacji kolejnego celu.

6.2. Zadania walki elektronicznej w działaniach taktycznych

Niezależnie od rodzaju działań taktycznych[56] zadania WE w ZT skupiają się wokół następujących problemów:

– rozpoznania systemów i środków elektronicznych (węzłów łączności i węzłów elektronicznych) elementów ugrupowania przeciwnika na szczeblu ZT (równorzędnym) zarówno wojsk lądowych, jak i lotnictwa wojsk lądowych, a w rejonach nadmorskich także sił morskich. Dokonywanie analiz rozpoznawanych emisji elektromagnetycznych, śledzenia dyslokacji środków elektronicznych i intensywności ich pracy;

– zakłócania systemów i środków elektronicznych (węzłów elektronicznych) przeciwnika będących w strefie odpowiedzialności rozpoznawczej ZT. Szczególną uwagę zwraca się na systemy dowodzenia i kierowania środkami walki pierwszorzutowych jednostek nacierających w pasie obrony ZT;

– obrony elektronicznej, ukierunkowanej na maskowanie i ukrywanie przed rozpoznaniem elektronicznym przeciwnika danych o własnych systemach i zamiarach, osłony pracy własnych urządzeń elektronicznych przed zakłócaniem elektronicznym i rażeniem środkami ogniowymi oraz naprowadzającymi się na źródła promieniowania elektromagnetycznego, a także eliminacji zakłóceń interferencyjnych (wzajemnych, współkanałowych) i kontroli elektronicznej.

Realizowane przez ZT zadania WE mają różne priorytety w poszczególnych etapach działań taktycznych.

W okresie przygotowania działań uwaga sekcji WE jest skupiona na:

– analizie pracy systemów i środków elektronicznych przeciwnika;

– drogach przemieszczania środków elektronicznych przeciwnika;

---

[56] Wyróżnia się trzy podstawowe rodzaje prowadzenia działań taktycznych: obronę, natarcie i działania opóźniające. Pozostałymi rodzajami walki są: działania desantowo-szturmowe, działania specjalne, wycofanie i działania nieregularne. We wszystkich wymienionych rodzajach działań taktycznych WE realizuje się zadania w trzech podstawowych obszarach: rozpoznania elektronicznego, zakłócania elektronicznego i obronie elektronicznej.

– porównaniu dotychczasowego ugrupowania z wzorcami działań środków elektronicznych w bankach danych;

– symptomach wskazujących na cel i zamiar prowadzonych przez przeciwnika działań elektronicznych;

– prognozowaniu rozwoju sytuacji elektronicznej;

– zaplanowaniu użycia pododdziału walki elektronicznej ZT.

W tym samym czasie pododdział WE (jeżeli jest w styczności z przeciwnikiem) kieruje uwagę na:

– rozpoznawanie nowo uruchamianych emiterów energii EM, ich charakter i intensywność pracy, używane kody, usytuowanie w ugrupowaniu bojowym;

– kontrolowanie wcześniej wykrytych źródeł energii EM (węzłów łączności i elektronicznych);

– kontrolowanie przestrzegania dyscypliny wykorzystywania urządzeń emitujących energię EM wojsk własnych (ZT) oraz maskowanie ich pracy;

– stosowanie w szerokim zakresie przedsięwzięć pozorowania elektronicznego (przede wszystkim przy wykorzystaniu środków pasywnego zakłócania elektronicznego).

Podczas przemieszczania lub zajmowania rejonu ześrodkowania główny wysiłek walki elektronicznej związku taktycznego koncentruje się na obronie elektronicznej. W znaczący sposób ogranicza się w tym okresie pracę środków emitujących energię elektromagnetyczną lub wprowadza całkowity zakaz ich pracy. Wzmacnia się kontrolę przestrzegania ustalonych zasad pracy środków elektronicznych. Można także wykonywać przedsięwzięcia o charakterze demonstracyjnym i dezinformacyjnym.

Z chwilą rozpoczęcia realizacji zadań bojowych przez ZT uwaga sekcji WE jest skupiona na:

– realizacji zadań wynikających z planu WE;

– ciągłej aktualizacji sytuacji elektronicznej w ugrupowaniu przeciwnika;

– reagowaniu na zmieniającą się sytuację elektroniczną;

– realizacji przedsięwzięć obrony elektronicznej, w tym szczególnie zapewnieniu kompatybilności elektromagnetycznej środków wojsk własnych w rejonach rozmieszczenia;

– koordynacji działań systemu WE z pododdziałami innych rodzajów wojsk;

– powiadamianiu o zachodzących zmianach w wykorzystywaniu urządzeń elektronicznych przez przeciwnika;

– planowaniu dalszej WE z chwilą otrzymania nowego zadania.

W tym samym czasie pododdział WE oraz użytkownicy systemów elektronicznych ZT realizują:

– proces poszukiwania nowych źródeł energii EM przeciwnika; szczególna uwaga powinna być skupiona na obszarach i punktach szczególnego zainteresowania określonych w elektronicznym przygotowaniu pola walki oraz środkach i systemach elektronicznych, których działalność będzie miała wpływ na przebieg walki (cele wysoko opłacalne);

– obserwację zmian w ugrupowaniu elementów elektronicznych przeciwnika;

– proces zakłócania źródeł energii EM ujętych w planie zakłóceń ;

– przedsięwzięcia obrony elektronicznej systemu łączności ZT, systemów radiolokacyjnych OPL, obserwacji pola walki, systemów sterowania uzbrojeniem i in.

W działaniach obronnych związku taktycznego podstawowym zadaniem walki elektronicznej jest wszechstronne rozpoznanie systemu dowodzenia przeciwnika w celu ustalenia możliwych wariantów rozwoju sytuacji taktycznej. Wykonanie tego zadania jest uzależnione od terminowego i dokładnego rozpoznania systemu dowodzenia wojskami pierwszego rzutu na głównym kierunku, jednostek rakietowych i artylerii, pododdziałów rozpoznania i walki elektronicznej oraz systemu dowodzenia (naprowadzania) lotnictwem taktycznym (lotnictwem szturmowym – wsparcia pola walki).

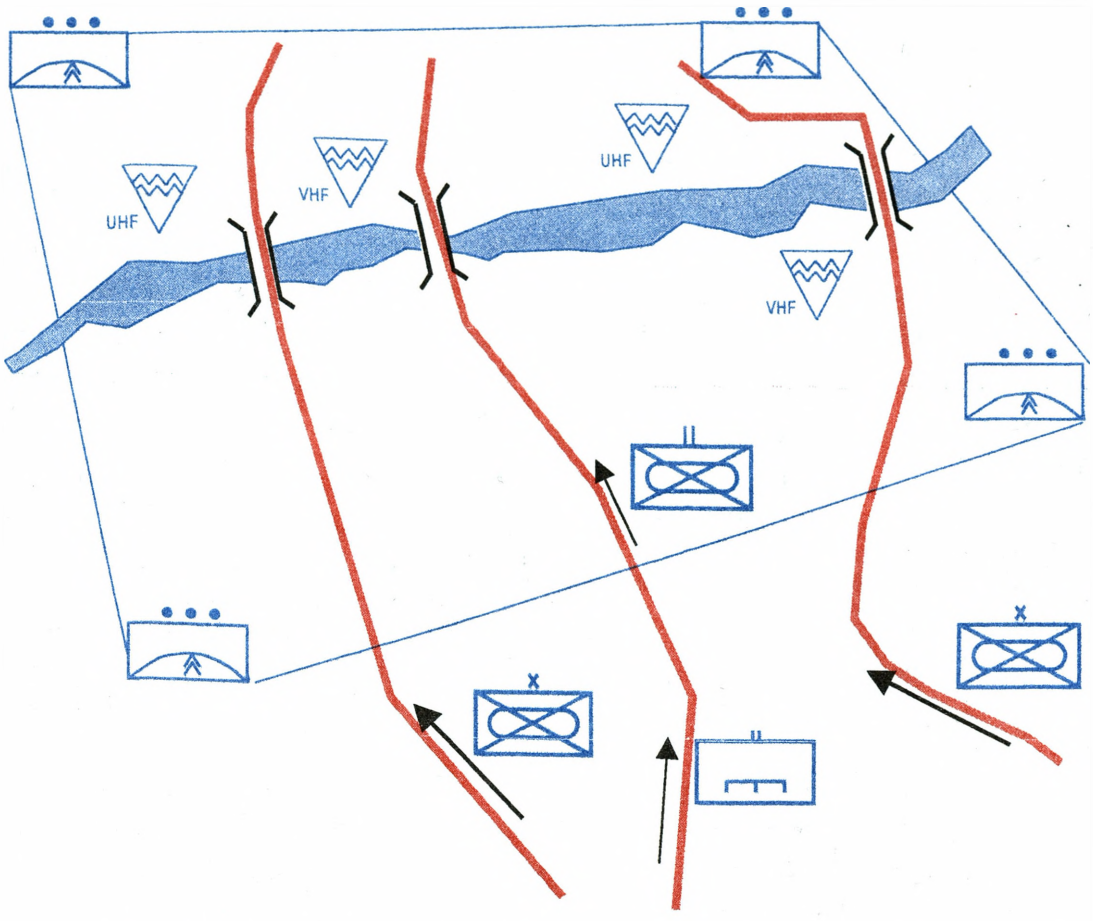
Podczas odpierania ataku przeciwnika przez wojska dywizji, broniące przedniego skraju głównego pasa obrony dywizji, wysiłek pododdziału elektronicznego skupia się na rozpoznaniu (potwierdzaniu) rozmieszczenia zasadniczych SD, ich węzłów łączności i węzłów elektronicznych, a także na zakłócaniu relacji łączności radiowych oddziałów i pododdziałów głównego zgrupowania uderzeniowego przeciwnika, jak również naprowadzania lotnictwa taktycznego.

W niektórych sytuacjach, np. podczas organizowania osłony przepraw wodnych związku taktycznego, wydziela się środki WE do zakłócania łączności radiowej naprowadzania lotnictwa taktycznego. W tym przypadku zadania zakłócania elektronicznego realizowane przez pluton zakłóceń są wykonywane we współdziałaniu z pododdziałami OPL osłaniającymi przeprawę (rysunek 39).

W przypadku udziału ZT w działaniach opóźniających wysiłek pododdziału WE skoncentruje się na zadaniach zmierzających do prowadzenia zakłócania elektronicznego w sieciach radiowych dowodzenia i współdziałania. Realizowane powinny być także przedsięwzięcia pozorowania radiowego.

Podstawowym zadaniem walki elektronicznej ZT w działaniach zaczepnych (kontrataku) jest zakłócanie elektroniczne systemu dowodzenia pierwszorzutowych wojsk oraz systemu rozpoznania i kierowania uzbrojeniem na kierunku działań. Zadanie to pododdział WE realizuje we współdziałaniu z pododdziałami artylerii.

We wszystkich rodzajach działań taktycznych (natarcie, obrona, działania opóźniające) wysiłek WE jest skupiony na obniżeniu efektywności działania systemów i środków elektronicznych dowodzenia, kierowania środkami walki i rozpoznania elektronicznego oraz zapewnieniu stabilnej pracy własnych systemów elektronicznych.



Rys. 39. Udział elementów zakłóceń elektronicznych w osłonie przepraw

6.3. Ugrupowanie bojowe środków walki elektronicznej w działaniach taktycznych

Ugrupowanie bojowe pododdziału elektronicznego ZT zależy głównie od warunków taktycznych i parametrów sprzętu. Wpływają na nie następujące czynniki:

– warunki terenowe i pogodowe;

– warunki rozprzestrzeniania się fal elektromagnetycznych w terenie działań;

– warunki i charakter działań taktycznych;

– sytuacja taktyczna i elektroniczna;

– struktura i wyposażenie kompanii elektronicznej w sprzęt rozpoznawczy i zakłócający;

– otrzymane zadanie w zakresie WE;

– ugrupowanie i sposoby działania środków elektronicznych przeciwnika.

Tworząc ugrupowanie bojowe, pododdział WE rozwija całość swoich sił i środków na pozycjach bojowych, nie pozostawiając żadnych środków w odwodzie (rezerwie).

6.3.1 Struktura pododdziału WE

Pododdział WE ZT składa się z:

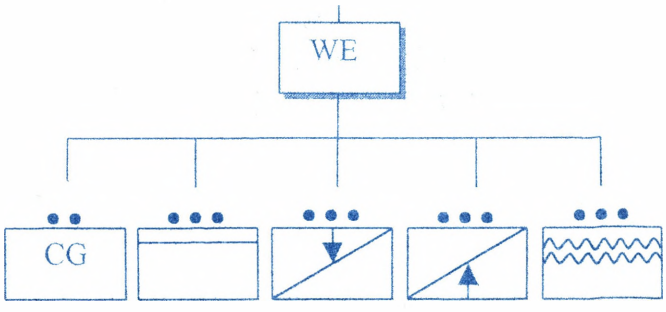
1. Grupy kierowania – przeznaczonej do sprawnego kierowania pracą bojowo-rozpoznawczą z punktu dowodzenia (PD) oraz realizacji wstępnej oceny sytuacji elektronicznej.

2. Plutonu dowodzenia – przeznaczonego do organizowania i utrzymania systemu łączności kierowania zakłóceniami i obiegu danych.

3. Plutonu rozpoznania elektronicznego – przeznaczonego do prowadzenia rozpoznania elektronicznego.

4. Plutonu namierzania elektronicznego – przeznaczonego do namierzania środków elektronicznych przeciwnika emitujących energię EM.

5. Plutonu zakłóceń elektronicznych – przeznaczonego do prowadzenia zakłóceń elektronicznych.



Rys. 40. Struktura organizacyjna pododdziału walki elektronicznej (wariant)

6.3.2. Elementy ugrupowania bojowego

Ugrupowanie bojowe pododdziału WE (rys. 41) zawiera następujące elementy składowe:

1. Punkt dowodzenia (PD) pododdziału.

2. Centrum rozpoznawcze (CR).

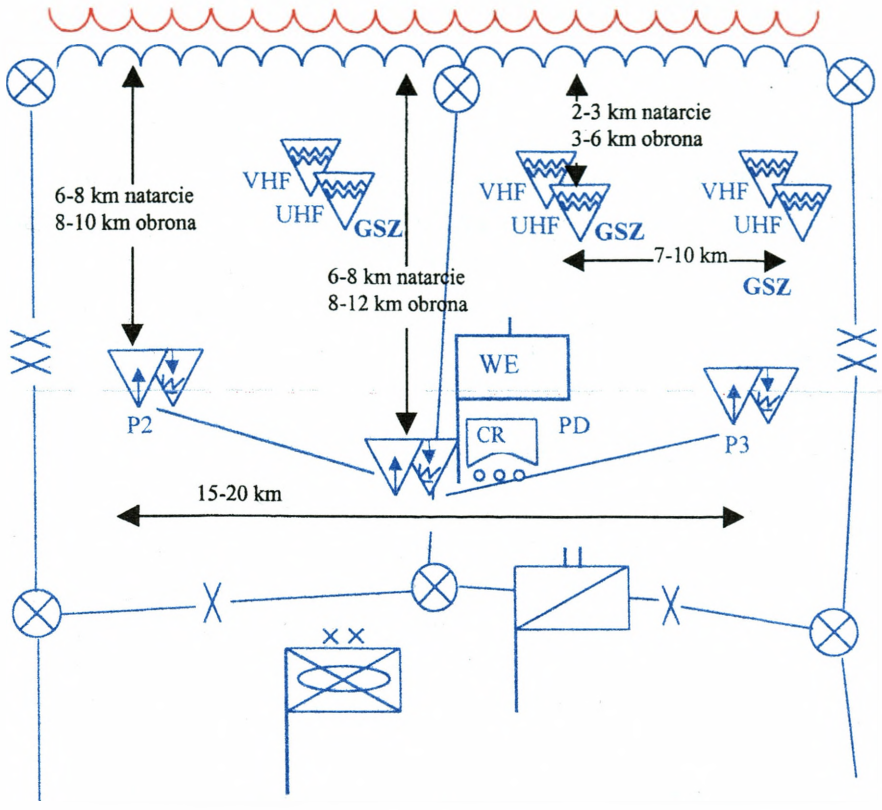
3. System (sieć) namierzania elektronicznego (SN) złożony z trzech posterunków namierzania (PN).

4. System rozpoznania i namierzania radiolokacyjnych środków i systemów pola walki (SNSRL) złożony z trzech posterunków.

5. Grupa środków zakłóceń (GSZ).

Punkt dowodzenia pododdziału elektronicznego rozmieszcza się z reguły w środku ugrupowania za pozycjami bojowymi grup stacji zakłóceń elektronicznych, w odległości 6-8 km od linii styczności wojsk w natarciu i od 8 do 12 km w obronie. Punkt dowodzenia kompanii składa się ze stanowiska dowódcy kompanii oraz stanowiska grupy kierowania.

Centrum rozpoznawcze rozmieszcza się z reguły w centrum ugrupowania pododdziału elektronicznego, w pobliżu środkowego posterunku namierzania lub punktu dowodzenia kompanii. Jako wariant można przyjąć rozwinięcie w pobliżu siebie wszystkich trzech wyżej wymienionych elementów, jeżeli analiza położenia wykaże, że będzie to wariant optymalny i uzasadniony.



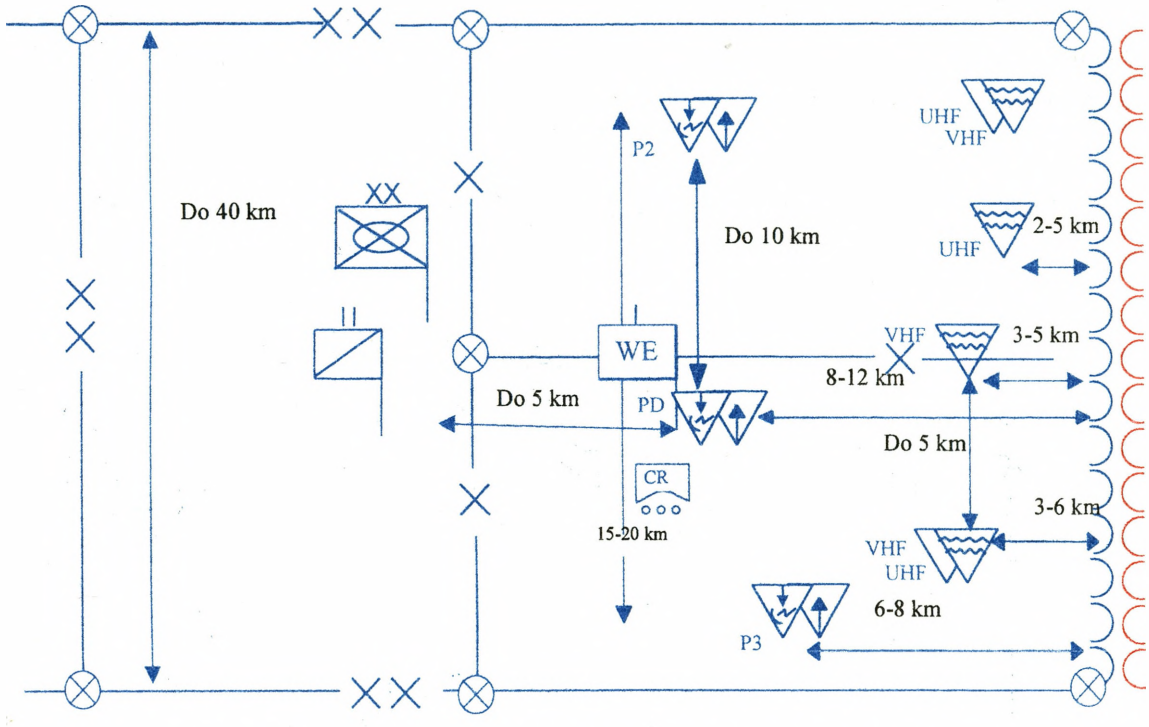
Rys. 41. Schemat ugrupowania bojowego pododdziału WE

Pluton zakłóceń elektronicznych (radiowych) rozmieszcza się w zasadzie grupami stacji zakłóceń (w każdej grupie po jednej stacji zakłóceń VHF i jednej UHF pasma lotniczego) w odległości od 2 do 3 km w natarciu i od 3 do 6 km w obronie od linii styczności wojsk, z zachowaniem odległości między grupami od 5 do 10 km. Jako wariant ugrupowania dopuszczalne jest rozmieszczanie pojedynczych stacji zakłóceń z większym lub mniejszym rozproszeniem. Należy jednak pamiętać o konieczności zachowania ciągłości sterowania stacjami. Zwracać trzeba również uwagę na zapewnienie kompatybilności elektromagnetycznej, tj. spełnienie warunków, by w pobliżu nie pracowały węzły łączności (WŁ) z rozbudowaną łącznością VHF i UHF oraz środkami rozpoznania elektronicznego HF, VHF i UHF.

Pluton namierzania elektronicznego rozwija się w ugrupowaniu bojowym pododdziału elektronicznego w dwa systemy (namierzania radiowego – po trzy posterunki każdy oraz rozpoznania i namiaru systemów radiolokacyjnych) w pasie od 4 do 6 km w natarciu i od 6 do 10 km w obronie od linii styczności wojsk, z zachowaniem odległości co najmniej od 7-10 km pomiędzy sąsiednimi posterunkami (baza namierzania systemu złożonego z trzech posterunków powinna wynosić od 15 do 20 km i więcej). Jako wariant optymalny można łączyć na pozycjach bojowych posterunki namierzania elektronicznego i radiolokacyjnego, tworząc zespoły namierzania elektronicznego. Odległość między stacjami może wynosić wówczas od 100 do 300 m.

6.3.3. Ugrupowanie pododdziału WE w działaniach obronnych

W działaniach obronnych pododdział WE rozmieszcza się całością sił na spodziewanym głównym kierunku natarcia przeciwnika z takim wyliczeniem, żeby pozostać poza zasięgiem ognia bezpośredniego przeciwnika. Wysiłek rozpoznania jest skierowany na rozpoznanie i potwierdzenie węzłów łączności i elektronicznych w pasie natarcia przeciwnika. Wysiłek zakłócania skupia się natomiast na zakłócaniu środków dowodzenia i kierowania walką pierwszorzutowych jednostek. Wariant ugrupowania pododdziału WE w obronie ZT przedstawia rys. 42.



Rys. 42. Wariant ugrupowania pododdziału WE w obronie ZT

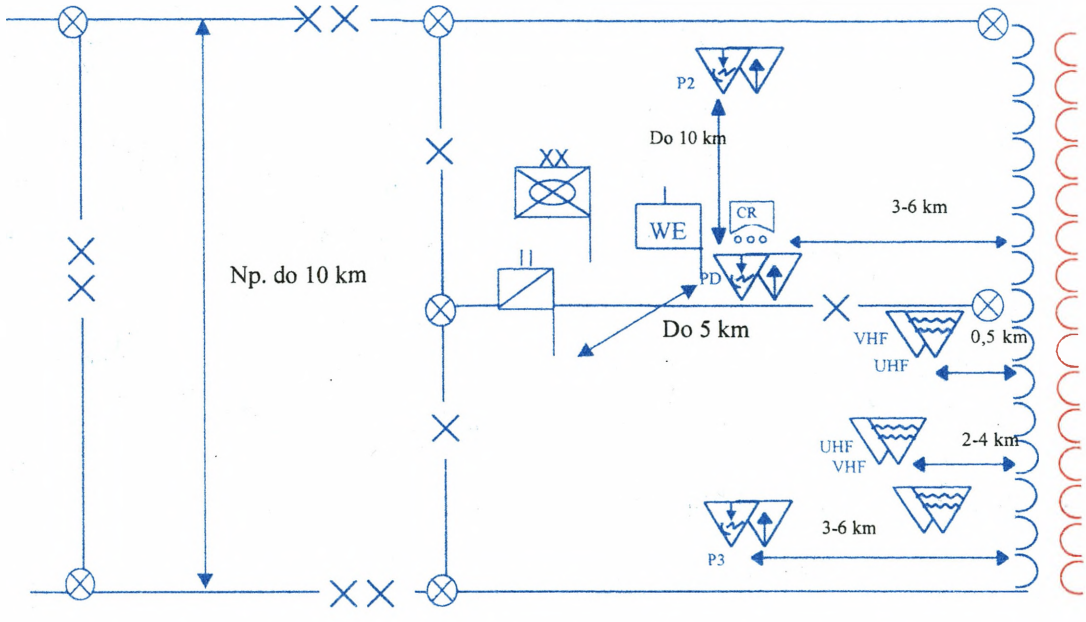
W walce obronnej w okrążeniu zgrupowania wojsk dywizji, siły i środki pododdziału elektronicznego są wykorzystywane do rozpoznania systemu dowodzenia przeciwnika, a następnie zakłócania relacji radiowych tych oddziałów wojsk lądowych i pododdziałów wojsk artylerii, które przygotowują manewr mający na celu rozcięcie ugrupowania okrążonych wojsk.

Podczas przygotowania i przełamywania pierścienia okrążenia przez okrążone wojska, pododdział elektroniczny rozwija się na odcinku przełamania w gotowości do prowadzenia zakłóceń łączności radiowej przeciwnika broniącego się na odcinku przełamania.

6.3.4. Ugrupowanie bojowe pododdziału WE w natarciu

Pododdział elektroniczny wykonujący zadanie w natarciu wysuwa się do przodu w celu zajęcia pozycji bojowych na kierunku uderzenia dywizji jeszcze przed rozpoczęciem przemieszczania pododdziałów artylerii. Wariant ugrupowania pododdziału WE w natarciu ZT przedstawia rys. 43.

Należy tak skalkulować gotowość pododdziału elektronicznej, aby czas realizacji pierwszej fazy zadań, tj. rozpoznania elektronicznego, był wystarczający do uszczegółowienia danych o sytuacji elektronicznej po stronie przeciwnika. Celowe jest stosowanie w tym okresie zakłóceń manewrowych, polegających na wyselekcjonowanym zakłócaniu rozpoznanych relacji radiowych i innych emisji. Może to powodować przechodzenie na częstotliwości zapasowe, które należy rozpoznać i zidentyfikować.



Rys. 43. Wariant ugrupowania pododdziału WE w natarciu ZT

Z chwilą rozpoczęcia przemieszczania wojsk dywizji na rubież ataku pododdział elektroniczny zakłóca łączność radiową systemów rozpoznania, dowodzenia i kierowania ogniem artylerii przeciwnika. Pozycje bojowe stacji zakłóceń i rozpoznania elektronicznego wybiera się na skrzydłach atakujących wojsk.

Podczas przełamywania obrony główny wysiłek walki elektronicznej skupia się na dezorganizacji łączności radiowej broniących się na przednim skraju pododdziałów oraz łączności współdziałania ze środkami ogniowymi i naprowadzania lotnictwa taktycznego.

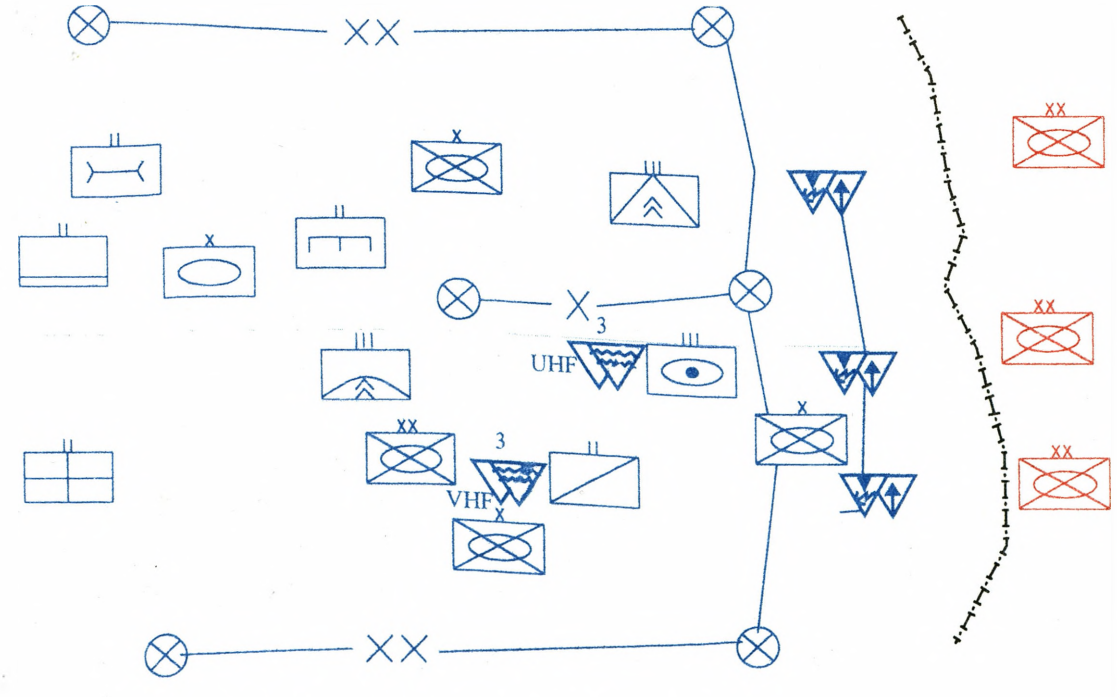
W miarę rozwijania się natarcia i przesuwania wojsk dywizji w głąb obrony przeciwnika pluton zakłóceń, po przełamaniu pierwszej linii obrony, przesuwa się do przodu, zajmując dogodne pozycje bojowe. Z pozycji tych prowadzi identyfikację, a następnie zakłócanie systemu łączności radiowej dowodzenia pododdziałami drugiego rzutu.

W czasie wprowadzania do walki odwodu dywizji pododdział WE zakłóca łączność radiową systemów rozpoznania oraz kierowania ogniem artylerii. Celowe jest wówczas wybieranie pozycji bojowych rozmieszczonych w pobliżu rubieży wejścia do walki drugiego rzutu.

6.3.5. Ugrupowanie bojowe pododdziału WE w działaniach opóźniających

W działaniach opóźniających wysiłek pododdziału WE koncentruje się na prowadzeniu zakłócania elektronicznego w sieciach radiowych dowodzenia i współdziałania. Organizuje się także przedsięwzięcia pozorowania radiowego. Środki zakłócania elektronicznego pododdziału WE rozmieszcza się w większym rozproszeniu w dwu rzutach lub prowadzi się pracę bojową w marszu. W celu zwiększenia skuteczności i efektywności rozpoznania i zakłócania elektronicznego pododdział WE rozwija się całością lub częścią sił w pasie przesłaniania, jeżeli taki jest organizowany.

W miarę odchodzenia oddziałów broniących pasa przesłaniania pododdział WE przemieszcza swoje elementy do rejonów obrony brygad pierwszego rzutu dywizji, zajmuje główne pozycje bojowe i osiąga gotowość do działań do czasu rozpoczęcia ogniowego wsparcia i rozwijania sił głównych przeciwnika. Główne pozycje posterunków rozpoznania i namierzania elektronicznego oraz stanowiska stacji zakłóceń wybiera się zarówno przed frontem, jak i na skrzydłach prawdopodobnego kierunku głównego uderzenia przeciwnika, natomiast stacje zakłócające są rozmieszczane na kierunkach prawdopodobnego użycia lotnictwa taktycznego przeciwnika. Na rysunku 44 pokazano wariant ugrupowania pododdziału WE w pasie przesłaniania.



Rys. 44. Wariant użycia pododdziału WE w pasie przesłaniania

6.3.6. Wybór i zajmowanie pozycji bojowych

Pozycje bojowe dla elementów ugrupowania pododdziału elektronicznego wybiera się według następujących kryteriów:

– zapewnienie maksymalnego horyzontu radiowego;

– możliwość realizacji celu i zadań elektronicznych w zasadniczym ugrupowaniu bojowym związku taktycznego;

– zachowanie bezpiecznej odległości od linii styczności wojsk;

– zapewnienie warunków kompatybilności elektromagnetycznej;

– zachowanie warunków do sprawnego funkcjonowania w systemie, w tym głównie utrzymanie bezpiecznej i pewnej łączności;

– zapewnienie ciągłości dowodzenia oraz możliwości manewru siłami i środkami.

Wyboru pozycji można dokonywać na podstawie mapy. Celowe jest wyznaczanie dwóch alternatywnych pozycji – głównej i zapasowej. Pozycję główną należy precyzować przez rekonesans lub na podstawie komputerowej bazy zobrazowania terenu.

6.3.7. Zmiana ugrupowania

W toku działań bojowych w wyniku zmian w sytuacji taktycznej siły i środki pododdziału elektronicznego przemieszcza się na kolejne rubieże bojowe. Zmiany położenia dotyczą zarówno całości sił pododdziału, poszczególnych systemów, jak też wybranych elementów (posterunków). Podyktowane jest to wieloma względami, w tym głównie koniecznością utrzymania tzw. kontaktu elektromagnetycznego z przeciwnikiem, utrzymania odpowiedniego poziomu maskowania przed rozpoznaniem oraz wyprowadzenia sił i środków pododdziału poza zasięg oddziaływania bezpośredniego ognia przeciwnika.

Częstotliwość przemieszczeń jest uzależniona od dynamiki zmian położenia linii styczności walczących wojsk. O czasie i sposobie przemieszczania decyduje przełożony pododdziału WE (dowódca batalionu rozpoznawczego), a w przypadku okresowego zerwania łączności i dostania się w zasięg ognia przeciwnika – także dowódca pododdziału.

Przemieszczenie pododdziału WE w nowy rejon całością sił będzie praktykowane w sytuacjach konieczności przemieszczenia sił na dużą odległość (powyżej 30-40 km) lub w przypadku nowych zadań dotyczących zmiany kierunku działania.

W przypadkach małej dynamiki zmian w pobliżu linii styczności wojsk oraz potrzeby utrzymania ciągłości rozpoznania i zakłócania elektronicznego siły i środki pododdziału przegrupowuje się na kolejne pozycje etapami – kolejnymi elementami ugrupowania, tj. posterunkami namierzania, grupami zakłóceń. Punkt dowodzenia kompanii i centrum radiowe przemieszcza się w dwóch rzutach w celu utrzymania ciągłości działania.

6.4. Prowadzenie działań bojowych przez pododdział walki elektronicznej

Zasadnicza działalność bojowa pododdziału WE dotycząca rozpoznania i zakłócania elektronicznego sprowadza się do realizacji zadań wg algorytmu (rys. 45) obejmującego:

– systematyczne dostarczanie do sztabu nadrzędnego (S 2 batalionu rozpoznawczego) wiarygodnych danych o sytuacji elektronicznej po stronie przeciwnika;

– zakłócanie pracujących środków elektronicznych przeciwnika w celu dezorganizowania ich pracy w określonych przedziałach czasowych.

Rozpoznanie elektroniczne jest realizowane od chwili przyjęcia ugrupowania bojowego i przygotowania środków do pracy. Po wstępnej analizie sytuacji panującej w przestrzeni EM należy przejść do kontroli najważniejszych obszarów ugrupowania przeciwnika (NAI), określonych obiektów elektronicznych (celów wysokoopłacalnych), pasm częstotliwości i relacji radiowych ważnych dla przebiegu działań.

Zakłócanie elektroniczne w działaniach taktycznych prowadzi się w określonych przedziałach czasowych, bardzo często koncentrując wysiłek na konkretnych obiektach lub źródłach (sieciach radiowych rozpoznania, węzłach łączności wybranej jednostki lub szczebla dowodzenia, sieciach naprowadzania lotnictwa, artylerii, kierowania ogniem).

Grupa kierowania jest elementem koordynującym pracę bojową elementów rozpoznania i zakłóceń, dokonuje wstępnej obróbki i analizy danych, a także odpowiada za przygotowanie okresowych sprawozdań dla sztabu nadrzędnego.

6.4.1. Praca bojowa elementów pododdziału walki elektronicznej

Centrum rozpoznawcze prowadzi poszukiwanie, przechwytywanie (rejestrację) oraz śledzenie pracy źródeł emisji elektromagnetycznych w pasmach HF, VHF, UHF.

Organizowanie pracy w centrum rozpoznawczym obejmuje:

– techniczne przygotowanie urządzeń do prowadzenia rozpoznania;

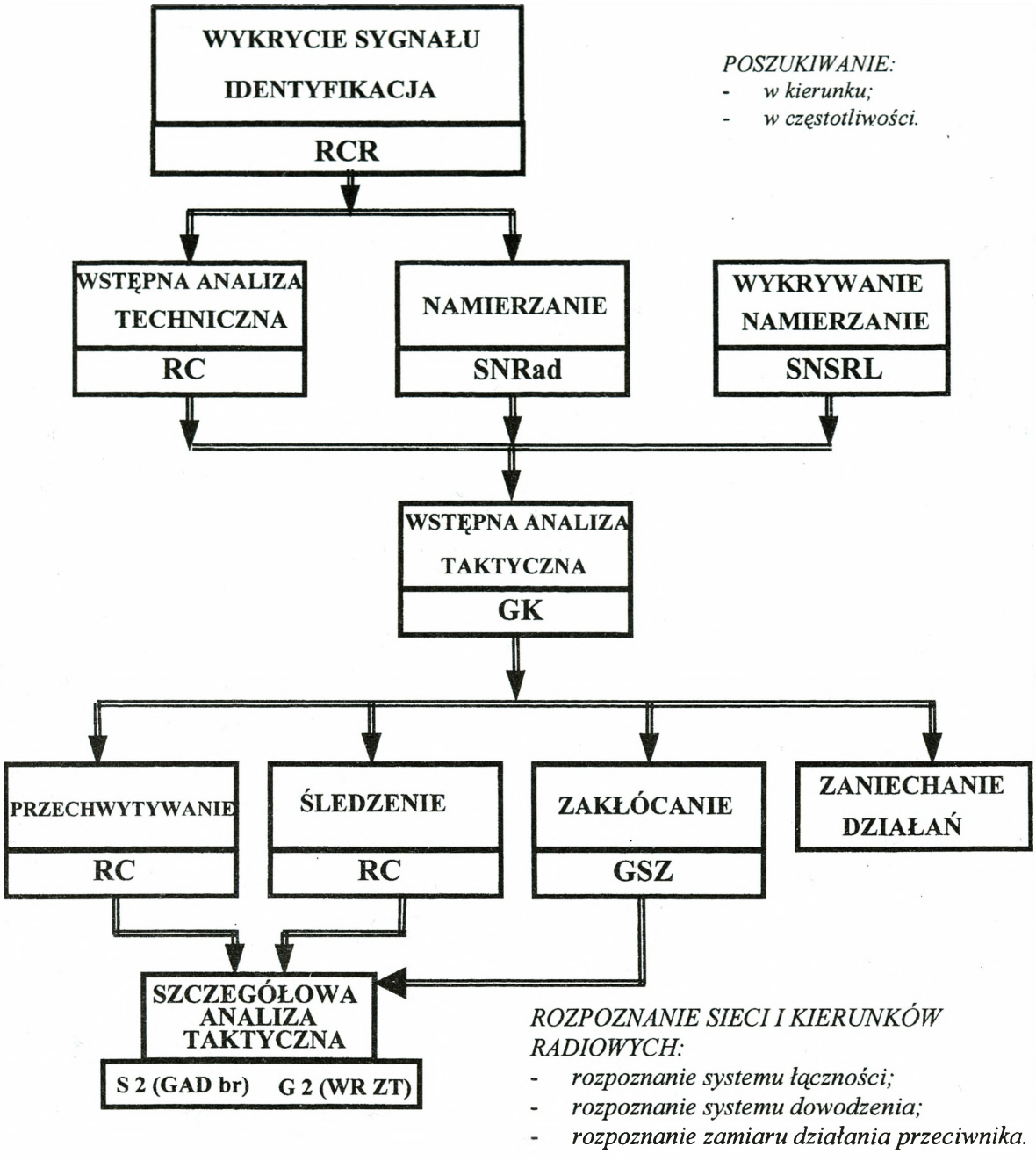
– dokonanie podziału sił i środków do prowadzenia pracy bojowo-rozpoznawczej;

– stawianie zadań dla obsług stanowisk rozpoznawczych.

Przygotowanie środków do pracy bojowo-rozpoznawczej polega na terminowym ich rozwinięciu, sprawdzeniu stanu technicznego oraz zorganizowaniu sieci łączności pomiędzy aparatowniami odbiorczymi, grupą kierowania oraz stanowiskiem dowódcy pododdziału.

Podział sił i środków do prowadzenia całodobowej pracy polega na wyznaczeniu dyżurnych zmian stanowisk rozpoznawczych i starszych zmian .

Po rozwinięciu i przygotowaniu urządzeń do pracy oraz wyznaczeniu zmian dyżurnych dowódca centrum rozpoznawczego (dowódca plutonu) stawia zadania dla wszystkich stanowisk, określając:



Rys. 45. Algorytm funkcjonowania WE na poziomie pododdziału WE

a) w zadaniu na poszukiwanie:

– zakres (pasmo) częstotliwości;

– cechy rozpoznawcze poszukiwanych źródeł rozpoznania;

– prawdopodobne rejony zainteresowań;

– sposób i zakres rejestracji przechwyconych emisji;

– sposób postępowania po wykryciu poszukiwanego źródła;

b) w zadaniu na przechwytywanie:

– częstotliwość;

– sygnał (kryptonim) rozpoznawczy;
– rodzaj nadawania (emisji);
– sposób przechwytu i rejestracji;
– rejony zainteresowań celami;
– czas i sposób meldowania danych;
– czas i sposób podawania komend do namierzania;
c) w zadaniu na śledzenie:
– źródła rozpoznania przewidziane do śledzenia;
– częstotliwości, rodzaj emisji i cechy rozpoznawcze;
– źródła (węzły łączności), na które należy zwracać największą uwagę;
– sposób i czas (termin) śledzenia;
– sposób rejestracji odbieranych emisji;
– czas i sposób meldowania danych rozpoznawczych;
– czas i sposób podawania komend do namierzania.

Wykryte przez stanowisko poszukiwania nowe źródło rozpoznania przekazuje się na stanowiska przechwytywania, na których ustala się ich wartość rozpoznawczą oraz określa sposób postępowania w dalszej działalności (czy należy je przechwytywać, śledzić, wskazać do namierzania lub zakłócania, czy też rezygnować z dalszego ich rozpoznawania).

W określonych warunkach sytuacji bojowej wartość rozpoznawcza źródeł może ulegać zmianie. Źródła o rosnącej wartości rozpoznawczej przekazuje się na stanowiska przechwytywania, a o malejącej – na stanowiska śledzenia. Umiejętny podział zadań rozpoznawczych pomiędzy stanowiska odbiorcze oraz stosowanie właściwego manewru nimi stanowią podstawę wykonania zadań w zakresie rozpoznania elektronicznego.

Posterunkami rozpoznania elektronicznego są *posterunki namierzania radiowego i posterunki rozpoznania systemów radiolokacyjnych.* W czasie pracy bojowej posterunki te tworzą odpowiednie systemy rozpoznania elektronicznego.

Organizowanie pracy rozpoznawczej każdego z systemów obejmuje:
– techniczne przygotowanie urządzeń do prowadzenia rozpoznania;
– nawiązanie łączności w systemie;
– podział sił i środków do prowadzenia całodobowej pracy bojowo-rozpoznawczej;
– postawienie zadań dla poszczególnych stanowisk rozpoznawczych (posterunków).

W warunkach pracy w systemie jeden z wyznaczonych posterunków (z reguły środkowy) powinien pełnić rolę stanowiska kierowania namiarem.

Posterunki namierzania elektronicznego dostarczają danych umożliwiających lokalizację źródeł rozpoznania. Namiarów dokonuje się na źródła nowo wykryte w celu ustalenia miejsca ich rozmieszczenia, a także na źródła przechwytywane i śledzone w celu potwierdzenia bądź uaktualnienia danych o ich lokalizacji.

Jeżeli pododdział elektroniczny jest wyposażony w system automatycznego namierzania, to całość procesu odbywa się na stanowisku kierowania. Jeżeli zaś namierzanie odbywa się sposobem ręcznym, to należy dostroić odbiornik na stanowisku namierzania do częstotliwości pracy, zidentyfikować źródła, dokonać namiaru i przekazać wynik na stanowisko kierowania namiarem.

Czas wykonania powyższych czynności nie jest stały i zależy głównie od:

– intensywności pracy namierzanych źródeł;

– właściwości namierników;

– przepustowości kanału łączności podawania zadań i zbierania wyników namierzania;

– intensywności oddziaływania elektronicznego przeciwnika na system rozpoznania;

– poziomu wyszkolenia obsług.

Średnio przyjmuje się, że obsada posterunku namierzania elektronicznego może wykonać w systemie ręcznym „na komendę" do 30-40 namiarów w ciągu godziny, a w systemie zautomatyzowanym około dziesięciu razy więcej, tj. 300-400 namiarów na godzinę.

P*osterunek rozpoznania systemów radiolokacyjnych* jest przeznaczony do zdobywania danych o stacjach i systemach radiolokacyjnych przeciwnika. Proces rozpoznania na tym posterunku obejmuje:

– poszukiwanie i wykrywanie pracujących stacji radiolokacyjnych przeciwnika;

– określanie azymutów na wykryte stacje radiolokacyjne;

– przechwytywanie sygnałów wykrytych stacji radiolokacyjnych, określanie ich parametrów technicznych oraz cech taktycznych;

– śledzenie rozpoznawanych źródeł w celu potwierdzenia lub uaktualnienia posiadanych danych;

– przekazywanie zdobytych danych do zespołu kierowania.

Grupy zakłóceń elektronicznych są elementami wykonawczymi zadań w zakresie zakłócania elektronicznego. Ze względów bezpieczeństwa ich ciągła praca „na nadawanie" nie powinna trwać dłużej niż jedną godzinę. Po tym czasie grupa powinna wykonać manewr na pozycję zapasową. Podstawą pracy jest realizacja zadań postawionych przez dowódcę pododdziału za pośrednictwem grupy kierowania. Może wystąpić wariant, w którym stacje zakłóceń samodzielnie prowadzą poszukiwanie źródeł energii EM i jednocześnie je zakłócają.

Grupa kierowania jako organ koordynujący pracę bojową pododdziału WE odpowiada za:

– przygotowanie zadań dla centrum rozpoznawczego, poszczególnych systemów namierzania oraz środków zakłóceń;

– opracowywanie danych z rozpoznania elektronicznego;

– kierowanie zadaniami rozpoznania i zakłócania elektronicznego w toku działań.

W grupie kierowania prowadzi się następujące dokumenty:

– dziennik działań bojowych pododdziału elektronicznego;

– mapę informacyjną;

– mapę sytuacyjną;

– książkę zadań do rozpoznania i zakłócania elektronicznego;

– mapę namierzania oraz arkusze zadań i wyników namierzania[57];

– blankiety zadań stanowisk odbiorczych.

Ponadto w grupie kierowania znajdują się najnowsze wydania wzorców doktrynalnych działań elektronicznych przeciwnika, mapy oraz inne pomocnicze materiały, tj. zestawienia, plansze i szablony obrazujące:

– podział zakresu częstotliwości do rozpoznania;

– organizację łączności rozpoznawanego przeciwnika;

– organizację i nasycenie systemów radiolokacyjnych rozpoznawanego przeciwnika;

– stosowane skróty, sygnały alarmowe i umowne formy radiogramów przeciwnika;

– cechy rozpoznawcze źródeł rozpoznania;

– zakres i zadania walki elektronicznej stosowane przez przeciwnika i inne.

6.4.2. Opracowywanie danych z rozpoznania elektronicznego

Opracowywanie danych z rozpoznania obejmuje:

– gromadzenie i klasyfikowanie elementarnych danych rozpoznawczych;

– analizowanie i porównywanie sklasyfikowanych danych;

– uogólnianie wniosków w postaci elektronicznej oceny przeciwnika;

– transponowanie sytuacji elektronicznej na ocenę sytuacji taktycznej przeciwnika.

Z danych rozpoznania elektronicznego tylko treść jawnej korespondencji przekazywanej w kanałach łączności może zawierać bezpośrednie dane charakteryzujące w większym lub mniejszym stopniu wojska przeciwnika. Pozostałe dane dotyczące pracy systemów elektronicznych wymagają szczegółowej analizy w celu uzyskania informacji rozpoznawczych. Analizy tej dokonuje się na podstawie zgromadzonych danych, takich jak:

– częstotliwości i czasy pracy, czasy trwania impulsów, okresy powtarzania impulsów i okresy obrotów anten źródeł rozpoznania;

– wiadomości o składzie sieci i kierunków radiowych;

– informacje o sposobach i częstotliwościach zmian danych radiowych;

– wiadomości o intensywności pracy źródeł;

– kryptonimy, znaki rozpoznawcze, skróty, znaki służbowe, umowne frazy i kody używane w korespondencji radiowej;

– indywidualne cechy rozpoznawcze radiotelegrafistów obsługujących radiostacje;

– indywidualne cechy sprzętu stanowiącego źródło rozpoznania;

– wiadomości o natężeniu ruchu w relacjach radiowych przeciwnika;

[57] W sytuacji gdy grupa kierowania przejmuje rolę stanowiska kierowania namiarem.

– azymuty (namiary) na pracujące źródła rozpoznania z posterunków rozpoznania elektronicznego.

Dane powyższe stanowią podstawę do identyfikacji źródeł z obiektami rozpoznania (w węzłach łączności lub elektronicznych), określenia ich położenia, składu i – głównie na tej podstawie – odtworzenia fragmentów sytuacji pola walki w rozpoznawanym obszarze. Uzyskanie takich efektów w procesie analizy jest możliwe do osiągnięcia tylko dzięki wcześniejszemu zgromadzeniu odpowiedniej ilości danych rozpoznawczych, ich sklasyfikowaniu, porównaniu z dotychczas posiadanymi, wyselekcjonowaniu i odrzuceniu dezinformacji oraz uogólnieniu.

Finalnym efektem procesu analizy są dane rozpoznawcze przedstawione w postaci meldunku dla przełożonego, zawierające opis odtworzonych fragmentów sytuacji pola walki w rozpoznawanym obszarze. Na podstawie tych danych zmiana dyżurna grupy kierowania uaktualnia mapę informacyjną, nanosząc na nią:

– stanowiska dowodzenia dywizji, brygad i batalionów;

– pododdziały artylerii;

– pododdziały przeciwlotniczych pocisków rakietowych;

– bataliony pierwszego rzutu brygad;

– wysunięte punkty naprowadzania lotnictwa wsparcia;

– punkty (stanowiska) kierowania rozpoznaniem i walką elektroniczną oraz inne według potrzeb.

6.4.3. Łączność w pododdziale WE

Dla potrzeb dowodzenia i kierowania pracą bojową rozwija się system łączności pododdziału WE oparty na łączności radiowej, radioliniowej i przewodowej (na PD może być rozwijana sieć komputerowa na światłowodach). Planistą i organizatorem w tym zakresie jest dowódca plutonu dowodzenia, a do jego obowiązków należy:

– planowanie i zgrywanie systemu łączności;

– dystrybucja danych radiowych;

– utrzymanie w sprawności sprzętu łączności (będącego na wyposażeniu plutonu dowodzenia oraz udzielanie fachowej pomocy w zakresie eksploatacji pozostałego w kompanii pokładowego sprzętu łączności);

– całościowe i terminowe rozwijanie systemu łączności;

– utrzymanie w drożności kanałów i łączy;

– współpraca z dowódcą kompanii w zakresie przeciwdziałania powstającym (przewidywanym) przypadkom niekompatybilności;

– obrona elektroniczna rozwiniętego systemu łączności.

Uogólniając należy stwierdzić, że prowadzenie walki elektronicznej we wszystkich etapach i rodzajach działań taktycznych jest ukierunkowane przede wszystkim na zmniejszenie lub pozbawienie sprawności działania elektronicznych systemów dowodzenia wojskami i kierowania środkami walki przeciwnika, lub co najmniej kontrolę ich pracy.

Struktura organizacyjna pododdziału WE uwzględnia prowadzenie walki elektronicznej w całym rejonie działania związku taktycznego.

Walka elektroniczna w działaniach taktycznych powinna być prowadzona przez wszystkie walczące wojska. Jej zakres jest zróżnicowany i zależy od wyposażenia walczących wojsk. Wszystkie pododdziały i oddziały powinny realizować przedsięwzięcia obrony elektronicznej.

Wybór rejonu rozwinięcia elementów walki elektronicznej należy poprzedzić rekonesansem przeprowadzonym przez ich dowódców. Dowódca problem ten może sprowadzić do oceny terenu na podstawie komputerowych baz danych o terenie. Wykorzystując odpowiednie oprogramowanie z aktualnymi bazami danych, może zaoszczędzić czas niezbędny do podjęcia właściwej decyzji i zajęcia dogodnych pozycji bojowych.

Praca elementów rozpoznawczych pododdziałów walki elektronicznej na szczeblu taktycznym jest skoncentrowana na poszukiwaniu i analizie przechwyconych danych. Jak wynika z analizy systemów łączności, często już na szczeblu plutonu dane przesyłane drogą radiową są kodowane z dużą mocą kryptograficzną. Wobec powyższego analiza treści takiej wymiany jest niemożliwa bądź zajmuje zbyt dużo czasu. Bardziej celowa jest lokalizacja miejsc promieniowania tych źródeł, określenie ich przynależności do danego szczebla dowodzenia i na tej podstawie sprecyzowanie prawdopodobnego zamiaru działania przeciwnika.

ZAKOŃCZENIE

Obecnie wydaje się, że postęp zachodzący w tworzeniu nowoczesnych systemów i środków elektronicznych, w dużym stopniu uodpornionych na rozpoznanie i zakłócanie przesyłanych za ich pomocą danych, przebiega szybciej niż w zakresie tworzenia systemów i środków walki elektronicznej zdolnych do ich zwalczania. Bierze się to stąd, że przy konstruowaniu wojskowych środków i systemów łączności, radiolokacji, radionawigacji itp. korzysta się z bogatych doświadczeń dynamicznie rozwijających się cywilnych systemów elektronicznych. Przykładem mogą być systemy łączności satelitarnej, telefonii komórkowej, czy też nawigacji satelitarnej GPS NAVSTAR.

W tej sytuacji niezbędne są zmiany w teorii prowadzenia WE, która powinna być dostosowana do zmieniającego się obszaru elektromagnetycznego oraz warunków prowadzenia walki zbrojnej. Doświadczenia minionych wojen i konfliktów lokalnych[58] dowodzą, że taka sytuacja będzie nadal istniała, a więc teoria powinna być rozwijana stosownie do warunków pola walki, wyposażenia w elektroniczne środki prowadzenia walki oraz celów i sposobów jej prowadzenia. W ostatnich latach walka elektroniczna jest postrzegana przez wielu teoretyków wojskowych jako część składowa walki informacyjnej rozgrywanej w wielu płaszczyznach.

W nadchodzącej przyszłości teoria walki zbrojnej będzie rozwijać się w kierunku kompleksowego ujmowania wszystkich jej głównych aspektów, tj. informacji, manewru oraz rażenia elektronicznego i ogniowego.

W obszarze rozpoznania elektronicznego konieczne będzie uzyskiwanie precyzyjnych, wiarygodnych i aktualnych danych o przeciwniku (o jego możliwościach, zamiarach i działaniach), terenie itd., gdyż bez posiadania tych informacji niemożliwe byłoby skuteczne kierowanie działalnością wojsk. Znaczenie rozpoznania stale wzrasta, zwłaszcza w warunkach potęgowania siły uderzeniowej i ruchliwości wojsk oraz zwiększania ich możliwości działania na dużych przestrzeniach. Efektywne wykorzystanie systemów konwencjonalnych o dużej precyzji rażenia, a także innych współczesnych środków walki, w pełni jest uzależnione od posiadania dokładnych danych o siłach przeciwnika.

Wzrastające znaczenie rozpoznania wymusza z kolei rozwój środków i konieczność doskonalenia sposobów jego prowadzenia. Dowodem na to może być fakt, że obecnie – dzięki osiągnięciom w dziedzinie elektroniki i informatyki – istnieją już realne możliwości rozpoznania dowolnego rejonu na kuli ziemskiej.

Współczesne pole walki stawia przed rozpoznaniem nowe zadania, do których można zaliczyć:

---

[58] Ogólne założenia (zasady) WE zostały wypracowane już w drugiej wojnie światowej, a każdy kolejny konflikt zbrojny „dokładał cegiełki" do jej rozwoju.

– rozszerzenie przechwytywanego pasma częstotliwości oraz zwiększenie dokładności namierzania, co pozwoli na efektywniejsze zwalczanie obiektów przeciwnika;

– szersze wykorzystanie zdalnie sterowanych aparatów latających;

– stosowanie bardziej złożonych układów „sztucznej inteligencji" w centralnych ogniwach systemu, w celu przyspieszenia konwersji danych do postaci pozwalającej na ocenę sytuacji;

– posiadanie mniejszych, szybko rozwijanych zestawów antenowych;

– integrację urządzeń rozpoznania radioelektronicznego z czujnikami różnych typów.

W obszarze zakłócania elektronicznego teoria powinna być rozszerzona o problemy masowego wykorzystania nadajników zakłócających jednorazowego użycia i autonomicznych środków WE, powietrznych, a w tym i bezpilotowych środków walki elektronicznej, oraz generatorów impulsów mikrofalowych, a także środków zakłóceń optoelektronicznych, czujnikowych i informatycznych. Pozostaje do rozwiązania problem koordynacji wysiłku elektronicznego i ogniowego. W związku z rozwojem broni samosterującej przed zakłócaniem elektronicznym jawi się problem kompleksowego zastosowania biernych środków WE w zakresie pozorowania i maskowania środków pola walki w szerokim obszarze spektrum elektromagnetycznego.

Ogólna teoria obrony elektronicznej powinna być uzupełniana o części składowe związane z pojawieniem się nowych rodzajów środków WE. Ze względu na olbrzymie nasycenie pola walki środkami elektronicznymi powinna zostać przygotowana teoria powszechnej obrony elektronicznej i teoria obrony elektronicznej realizowanej przez wyspecjalizowane siły i środki. W tej sytuacji problematykę powszechnej obrony elektronicznej trzeba ujmować ogólnie jako teorię obrony elektronicznej oraz indywidualnie w stosunku do każdego środka i systemu elektronicznego. Należy oczekiwać, że najpierw ukażą się opracowania dotyczące realizacji obrony elektronicznej w stosunku do konkretnych środków i systemów.

Wraz z rozwojem informatyzacji pola walki pojawia się nowy rodzaj broni elektronicznej, wykorzystywany przeciwko systemom informatycznym. Trudno obecnie ocenić, jakie szkody mogłaby poczynić tego typu broń w dzisiejszych systemach elektronicznych. Należy tylko przypuszczać, że przyszłe systemy dowodzenia wojskami i kierowania środkami rażenia, w dużym stopniu „uzależnione" od komputerowego wspomagania, mogą stać się bezużyteczne, jeżeli nie będą w porę podjęte odpowiednie ochronne środki zaradcze[59].

[59] Przedsięwzięcia te powinny mieć odzwierciedlenie w ramach obrony elektronicznej.

LITERATURA

1. *ATP-51 (STANAG 6010) Electronic Warfare in Land Battle.*

2. Ciborowski L.; *Rozpoznanie radioelektroniczne szczebla taktycznego wojsk lądowych*, wyd. ASG WP, Warszawa 1989.

3. Ciborowski L.; *Walka informacyjna*, wyd. ECE, Toruń 1999.

4. Grabau R.; *Sześć wymiarów wojny – walka o spektrum elektromagnetyczne*, [w:] „Wojskowy Przegląd Zagraniczny" nr 3/1987.

5. Grabau R.; *Nadzór radiowy i walka radioelektroniczna*, [w:] „Wojskowy Przegląd Zagraniczny" 1988.

6. Janczak J., Bezoń B., Scheffs W.; *Walka elektroniczna w działaniach taktycznych wojsk lądowych*, wyd. AON, Warszawa 1999.

7. Janczak J.; *Obrona radioelektroniczna mobilnych systemów łączności*, wyd. AON, 1998.

8. *Kompendium zasadniczego sprzętu WRE SZ RP*, wyd. Szt. Gen. WP, Warszawa 1998.

9. Kruszyński M., Magnucki Z.; *Walka radioelektroniczna w działaniach bojowych dywizji (DZ, DPanc)*, wyd. ASG WP, Warszawa 1986.

10. Magnucki Z., Korzecki K.; *Uwarunkowania operacyjno-taktyczne stosowania elementów dipolowych w wojskach lądowych*, wyd. AON, Warszawa 1990.

11. Magnucki Z., Scheffs W.; *Charakterystyka struktur organizacyjnych i środków WRE w wybranych państwach*, wyd. AON, Warszawa 1996.

12. Matuszewski J.; *Podstawy walki radioelektronicznej*, wyd. WAT, Warszawa 1996.

13. *M-34-130 „Inteligence Preparation of the Beattlefield"*, ed. Headqartes Departament of the Army 1989.

14. Nowacki G.; *Walka informacyjna – próba kategoryzacji*, AON, Warszawa 1999.

15. Nowacki G., Scheffs W.; *Elektroniczne przygotowanie pola walki*, wyd. AON, Warszawa 1998.

16. *Poradnik oficera rozpoznania radioelektronicznego*, wyd. OPK, Warszawa 1990.

17. *Regulamin działań wojsk lądowych*, wyd. DWL, Warszawa 1999.

18. Simon M., K. Omura J, K.; *Spread Spectrum Communications Handbook*, wyd. II poprawione, Mc Graw-Hill, 1994.

19. Strzoda M., Trembecki J.; *Ocena wariantów działań*, wyd. AON, Warszawa 1999.

20. *Tymczasowe wzory dokumentów bojowych (rozpoznanie, WRE i działania psychologiczne)*, wyd. DWL, Warszawa 1999.

21. *Walka radioelektroniczna w SZ RP*, wyd. AON, Warszawa 1997.

22. Wakin S. A., Szustow L.N.; *Zasady przeciwdziałania radioelektronicznego*, wyd. MON, Warszawa 1972.

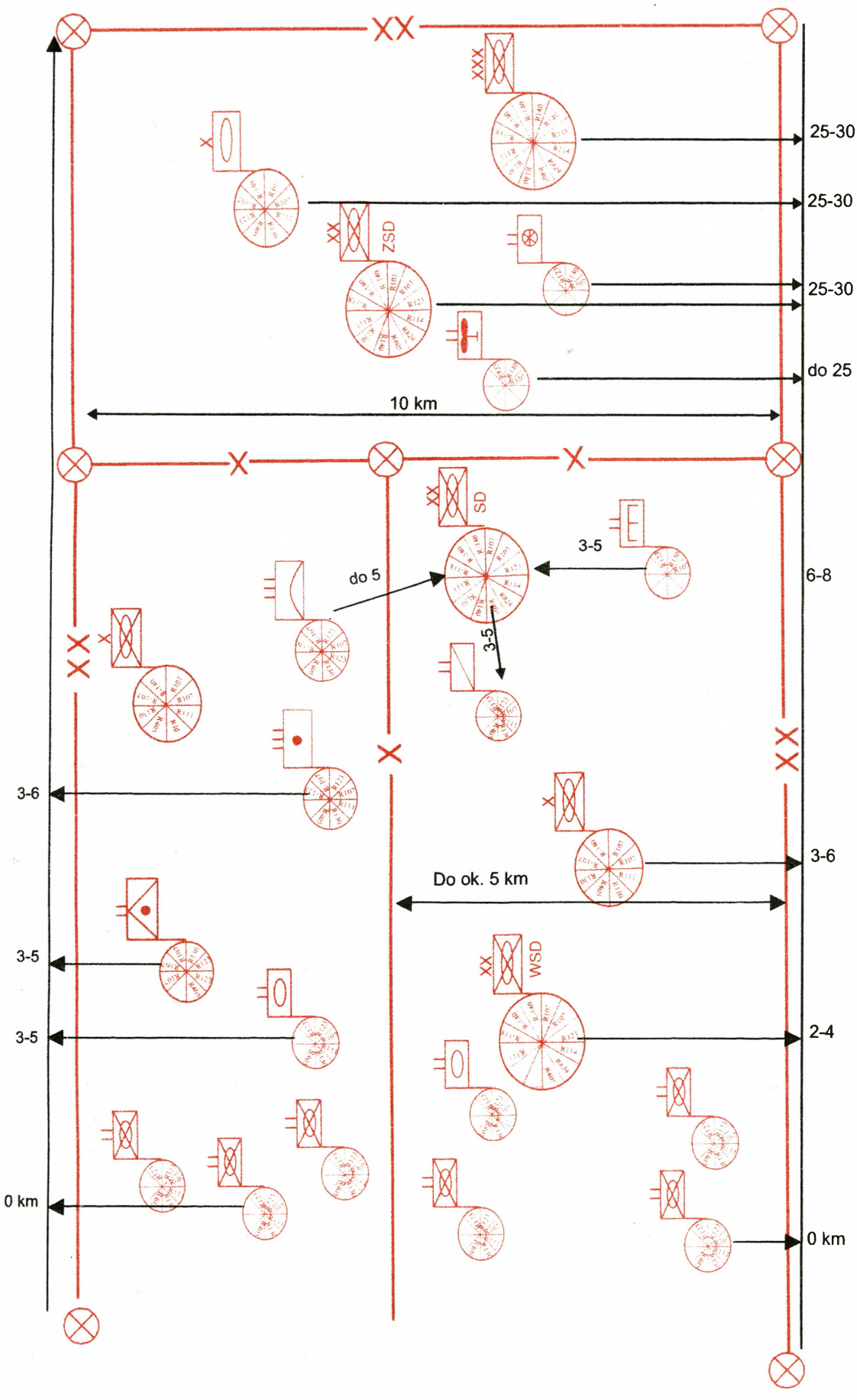
23. *Wojna elektroniczna według poglądów państw NATO*, wyd. Szt. Gen. WP, Warszawa 1989.

24. *Vademecum walki radioelektronicznej*, wyd. WLiOP, Warszawa 1994.

25. *Zasady przygotowania i prowadzenia walki radioelektronicznej przez Siły Zbrojne RP*, wyd. Szt. Gen. WP, Zarząd II, Warszawa 1995.

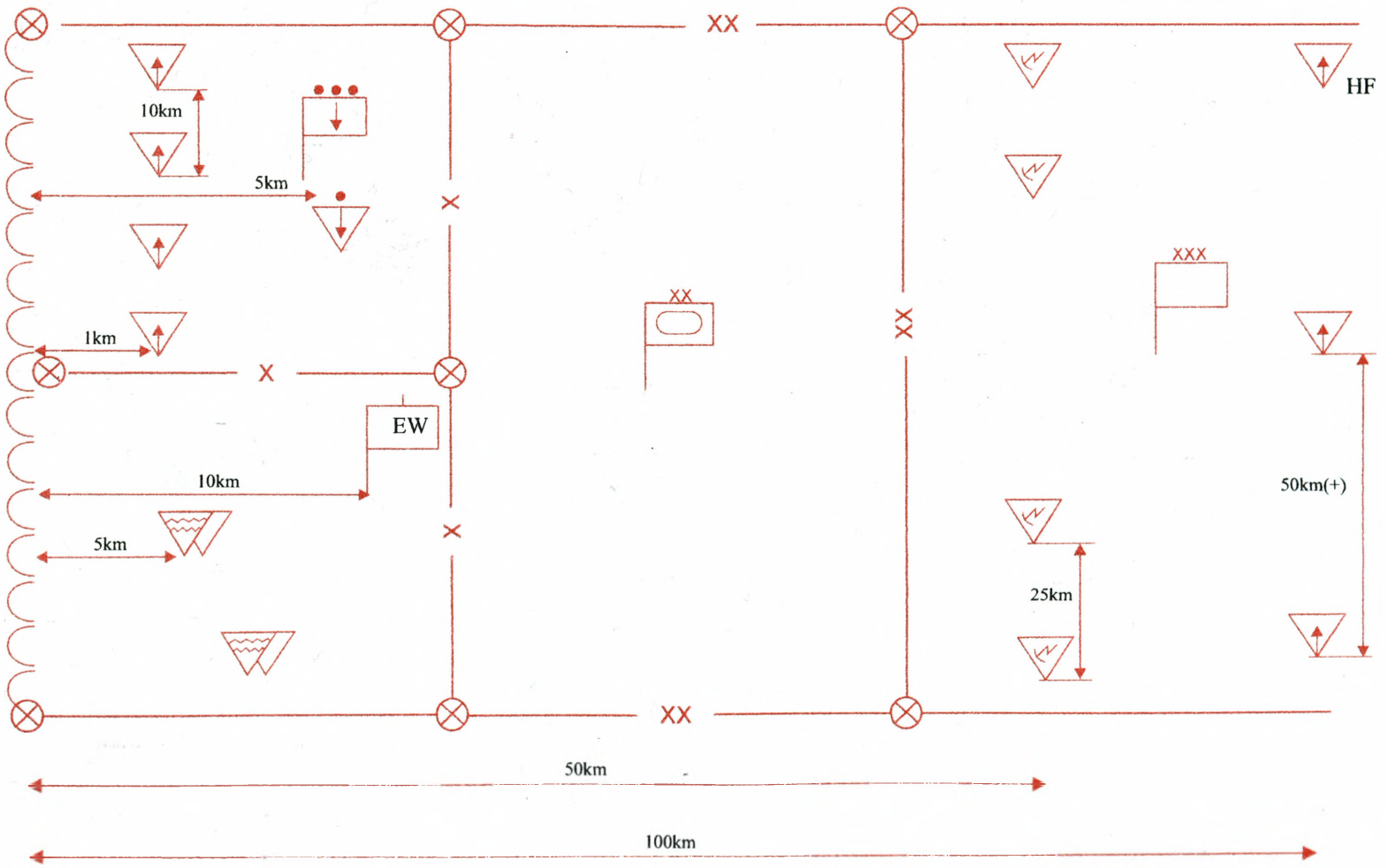
Załącznik 1

WZORZEC DOKTRYNALNY WĘZŁÓW ŁĄCZNOŚCI DZ W NATARCIU PRZECIWNIKA

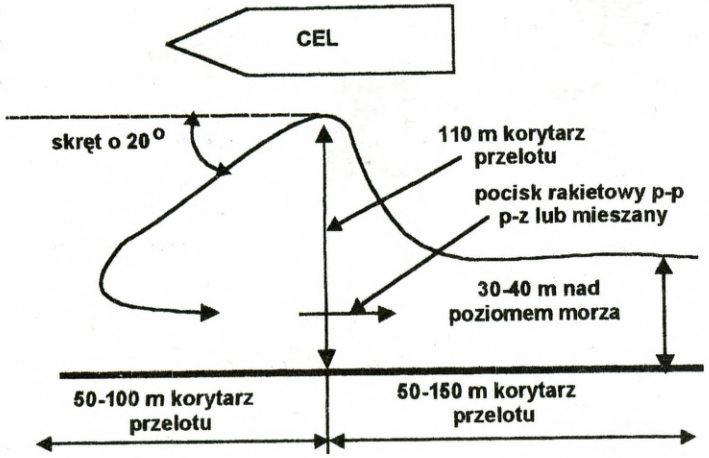


Załącznik 2

WZORZEC UGRUPOWANIA ELEMENTÓW WE DZ ZT I CZĘŚCIOWO ZO PRZECIWNIKA
(przykład)

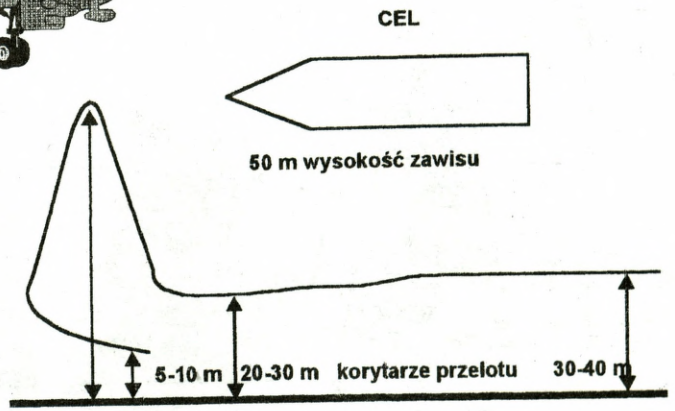


WZORZEC ŚNP Mi-24 (przykład)



PROWADZENIE OGNIA W RUCHU

PROFILE ATAKU ŚMIGŁOWCA Mi-24



PROWADZENIE OGNIA Z ZAWISU

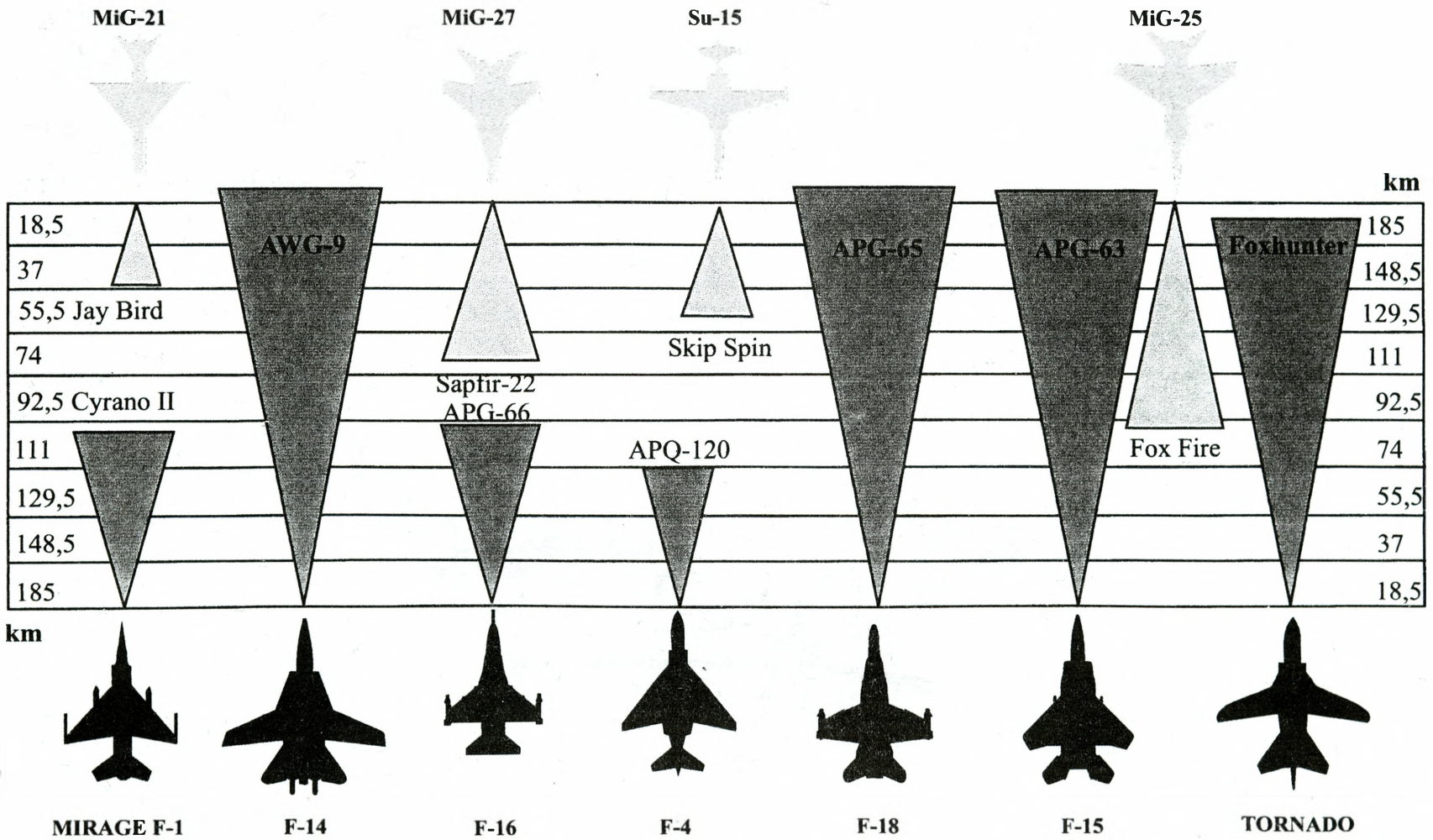
Prędkość 320 km/h
Promień działania 160 km
Liczba przewożonych żołnierzy 8-10

Uzbrojenie:
1x12,7 mm działko z lufą gwintowaną,
4x250 kg bomby
4x32 niekierowane pociski rakietowe 57 mm,
PODS zasobnik rakietowy
4xAT-2/3/6 ppk
1x30 mm działko szybkostrzelne (HIND F dwulufowe)

Uzbrojenie śmigłowca zależy od zadania, zasięgu i pogody. Minimalna wysokość operacyjna 10 m

Załącznik 4

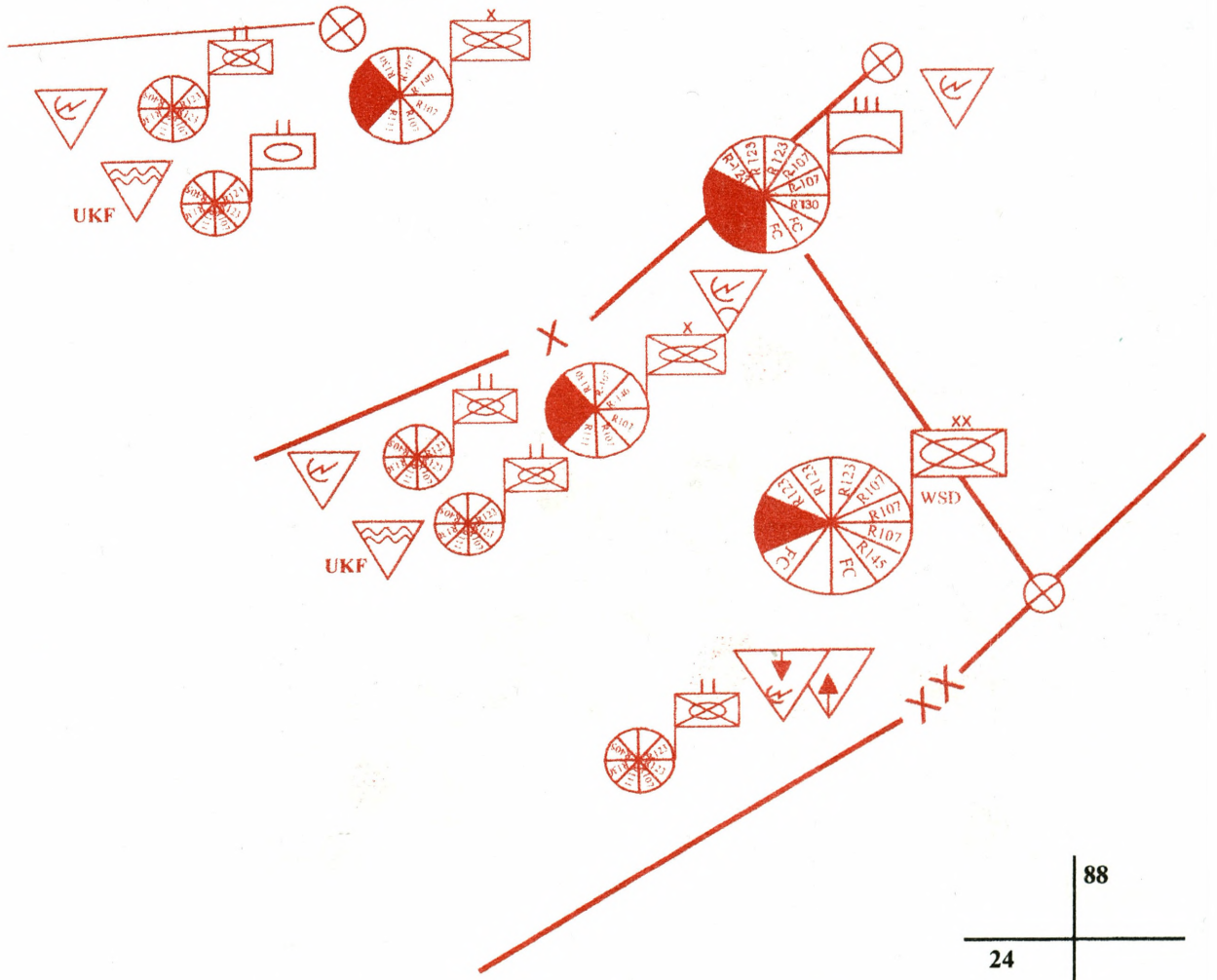
WZORZEC PORÓWNAWCZY ZASIĘGÓW SRL DLA ŚNP (przykład)



OLEAT SYTUACJI ELEKTRONICZNEJ (sytuacja bieżąca)
(przykład)

Zastrzeżony

38
64



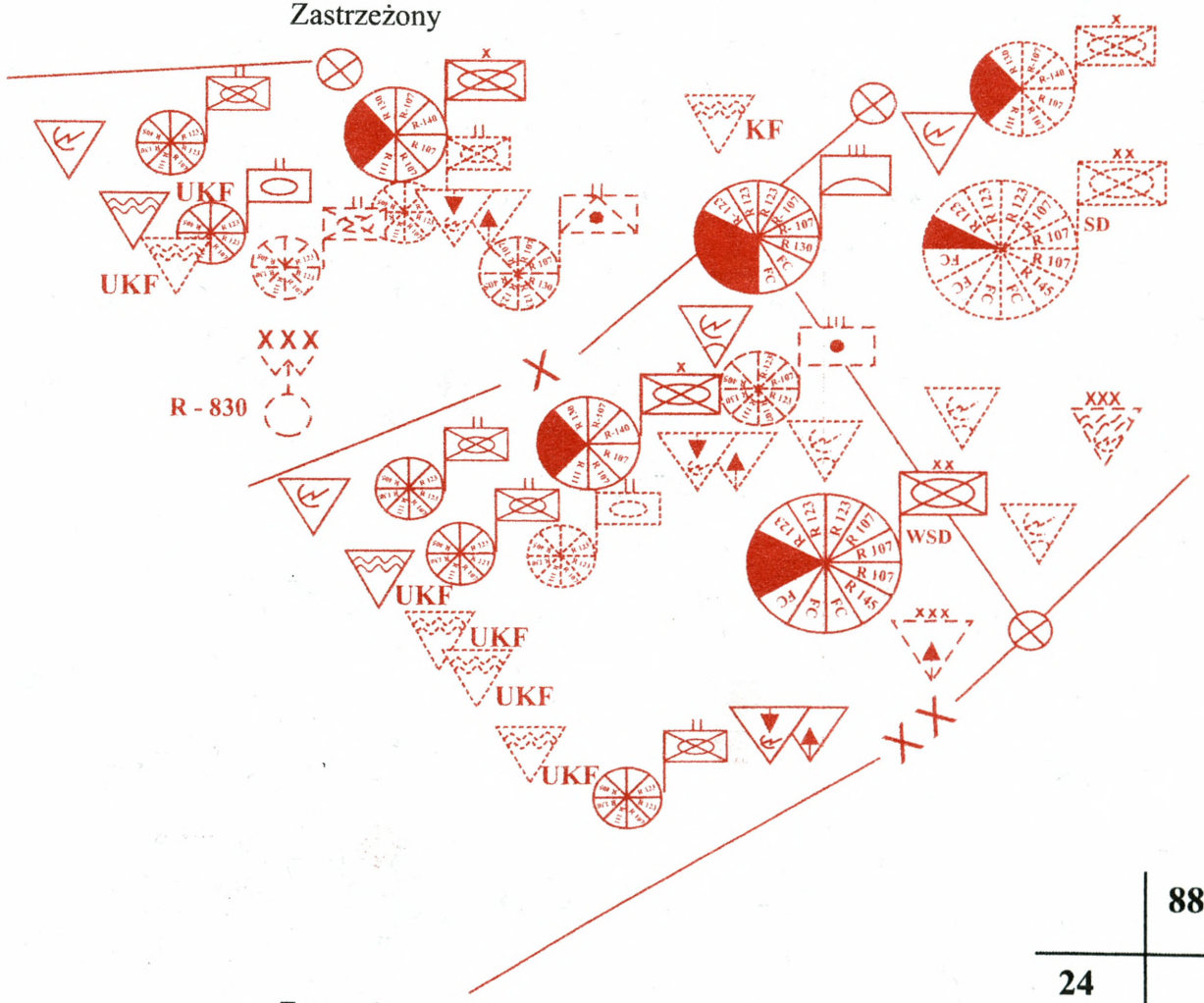
88
24

Zastrzeżony

OLEAT PORÓWNAWCZY SYTUACJI ELEKTRONICZNEJ WŁ I WĘZŁÓW ELEKTRONICZNYCH DZ W NATARCIU Z BIEŻĄCĄ SYTUACJĄ ELEKTRONICZNĄ
(przykład)

38
64

Zastrzeżony

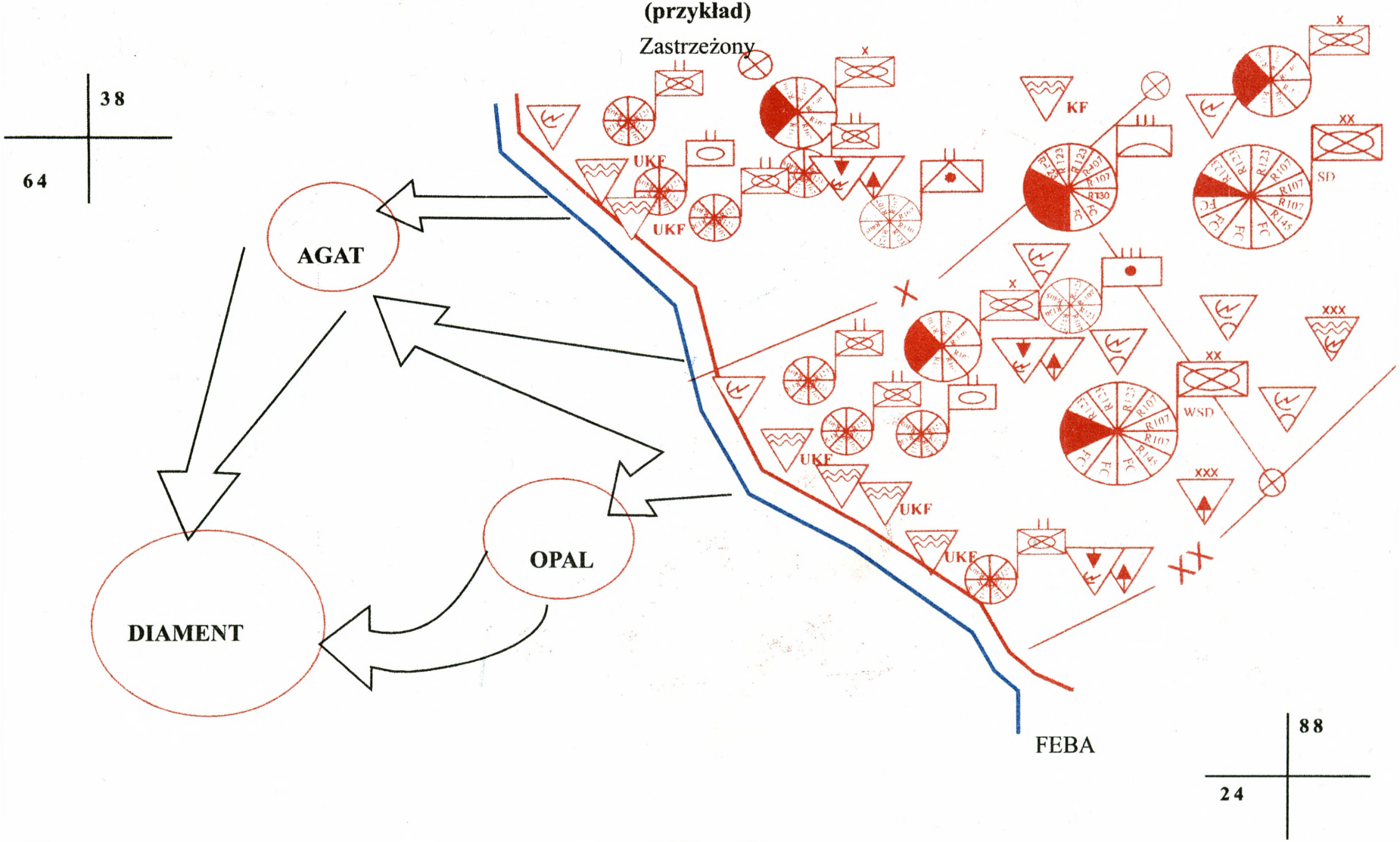


88
24

Zastrzeżony

OLEAT PROGNOZY ZAGROŻENIA ELEKTRONICZNEGO (wariant 1)
(przykład)

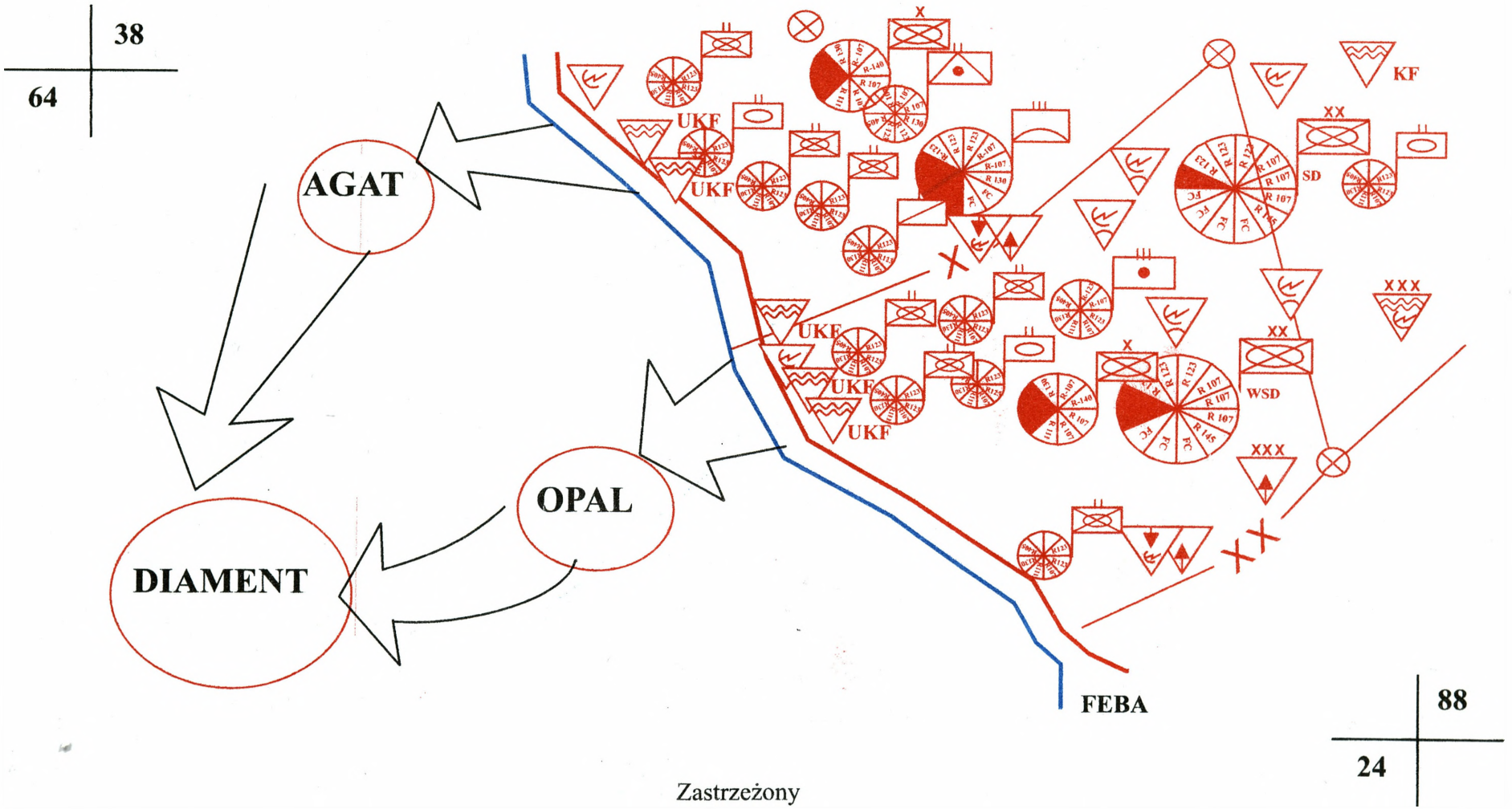
Zastrzeżony



Zastrzeżony

OLEAT PROGNOZY ZAGROŻENIA ELEKTRONICZNEGO (wariant 2)
(przykład)

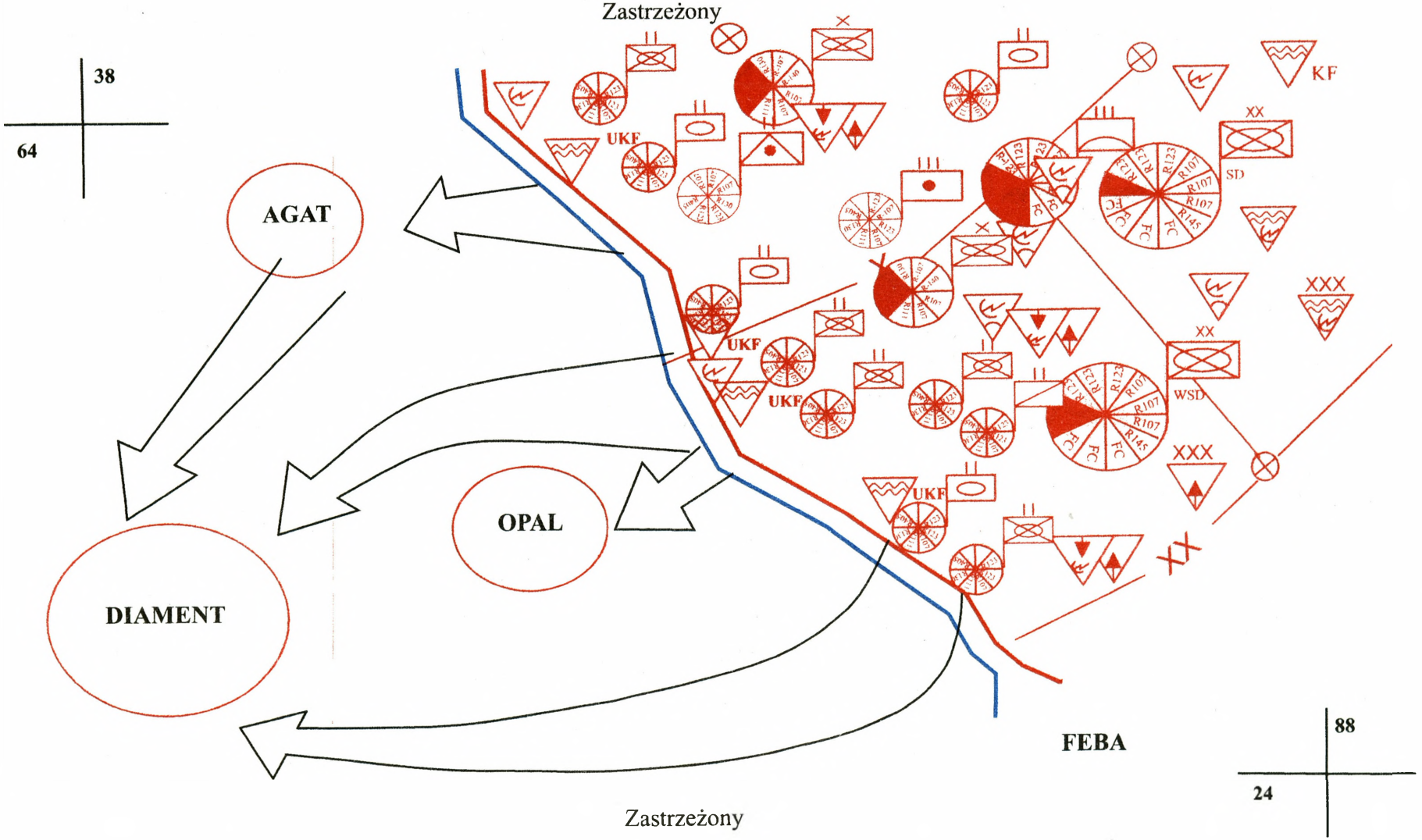
Zastrzeżony



Zastrzeżony

OLEAT PROGNOZY ZAGROŻENIA ELEKTRONICZNEGO (wariant 3)
(przykład)

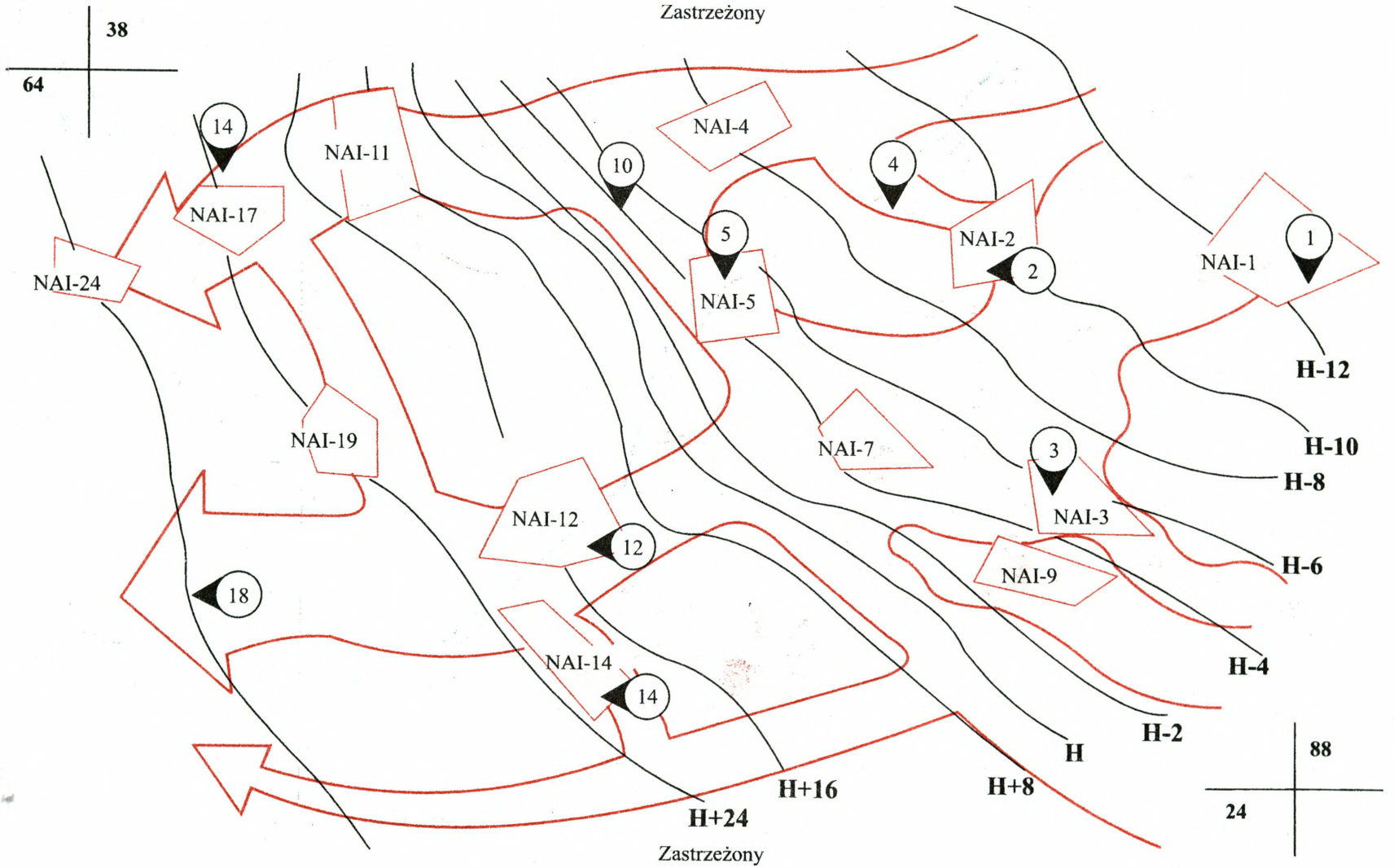
Zastrzeżony



Zastrzeżony

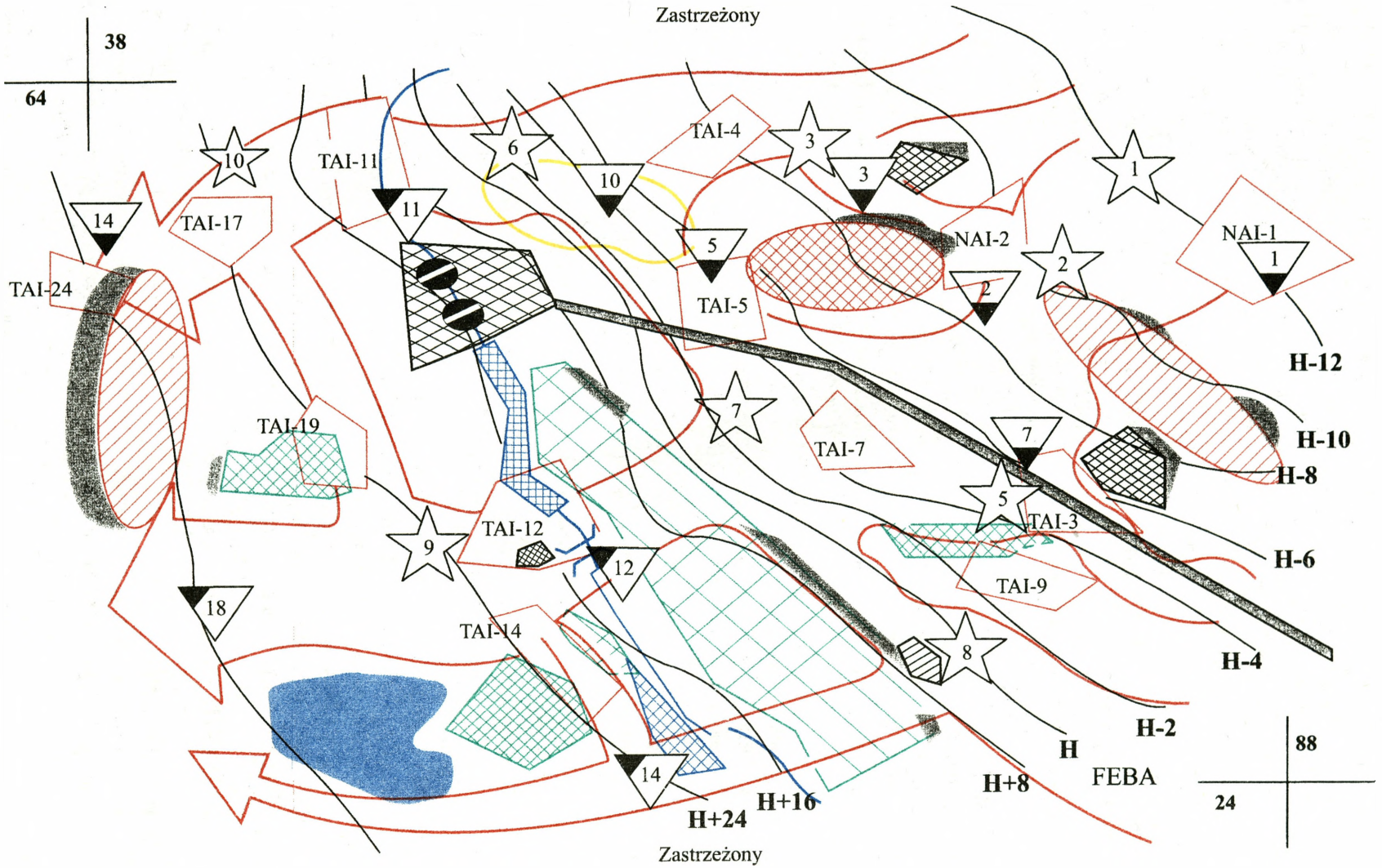
Załącznik 10

OLEAT ZDARZEŃ ELEKTRONICZNYCH
(przykład)



Załącznik 11

OLEAT WSPARCIA DECYZJI W ZAKRESIE ELEKTRONICZNYM
(przykład)



Załącznik 12

H-1

klauzula tajności

Kopia nr 4 z 25 kopii
2 DZ FRANKOWO (MA 7751),
NIEBIESCY
251700 A July 1995
XA 33

ANEKS H „WALKA ELEKTRONICZNA"
DO ROZKAZU OPERACYJNEGO 2 DZ nr 1

Dokumenty odniesienia:
Mapa, 1501 EUROPA; arkusze: NN 33-12, NM 33-3, NM 33-6, NN 34-10, NN 34-11, NM 34-1, NM 34-2, NM 34-4, NM 34-5; wydanie 1-OTSG; skala 1 : 250 000.
Strefa czasowa: ALFA – *może być ponownie powtórzona*

1. SYTUACJA

a. Siły przeciwnika

(1) Siły główne - o*desłanie do: Aneks B (rozpoznanie) do planu działania 2K.*
(2) Systemy elektroniczne przeciwnika - *krótka charakterystyka wykorzystywanych środków łączności, stacji radiolokacyjnych i innych środków elektronicznych.*
(3) Środki WE przeciwnika – u*ogólniona charakterystyka środków WE wykorzystywanych przez przeciwnika*

b. Wojska własne

(1) Przedsięwzięcia WE realizowane przez przełożonego - w*ymienia się, jakie przedsięwzięcia z zakresu WE realizował będzie przełożony na kierunku działania dywizji.*
(2) Wsparcie sił powietrznych w zakresie WE – w*ymienia się, jakie przedsięwzięcia z zakresu WE realizowane będą przez inne rodzaje sił zbrojnych – lotnictwo, siły morskie.*
(3) Przedsięwzięcia sąsiadów – *przedsięwzięcia w zakresie WE realizowane przez sąsiadów.*
(4) Przydział wzmocnienie – *wymienić, jakie siły WE zostały przydzielone, jakie podporządkowane czasowo, jakie się wydziela.*

c. Założenia

(1) Plan działania – *odnośnik do Aneksu C.*
(2) Przewidywane przedsięwzięcia przeciwnika - *jakie przedsięwzięcia WE może zastosować przeciwnik w operacji.*
(3) Spodziewane nowe systemy i środki WE - k*rótka charakterystyka użycia nowych systemów WE w toku prowadzonych działań.*
(4) Przewidywana taktyka użycia sprzętu WE przez przeciwnika.

2. ZADANIE – *jakie zadanie z zakresu WE realizować będzie szczebel wydający rozkaz.*

3. WYKONANIE

a. Koncepcja działania (zamiar). *Określenie głównego wysiłku WE. Wyjaśnienie sposobu wykorzystania elementów ugrupowania bojowego. Patrz: plan działania Aneks C.*

b. Zadania dla elementów ugrupowania bojowego. *W kolejnych podpunktach stawiane są zadania dla poszczególnych elementów ugrupowania bojowego. W większości zadania te dotyczyć będą obrony elektronicznej. Bardziej szczegółowo dla elementów WE. Nie powtarza się zadań postawionych w rozkazie operacyjnym i apendyksach.*

c. Koordynacja działań. *Wyszczególnienie informacji dotyczących dwóch i więcej elementów ugrupowania bojowego i podanie niezbędnych współrzędnych, linii koordynacyjnych. Czasy rozpoczęcia i zakończenia zakłócania elektronicznego. Ustalenia w zakresie zastrzeżonych i zabronionych częstotliwości. Czasy gotowości do działań mogą być powtórzone.*

4. ZABEZPIECZENIE LOGISTYCZNE

a. Zaopatrywanie w sprzęt WE – o*dwołanie do aneksu „Plan zabezpieczenia logistycznego".*

b. Zabezpieczenie techniczne przydzielonych środków walki elektronicznej – o*dwołanie do aneksu „Plan zabezpieczenia logistycznego".*

c. Uzupełnienie – o*dwołanie 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 L „Łączność - elektronika".*

[podpis dowódcy (dowolny)]
(.....nazwisko dowódcy...)
(.....stopień.....)

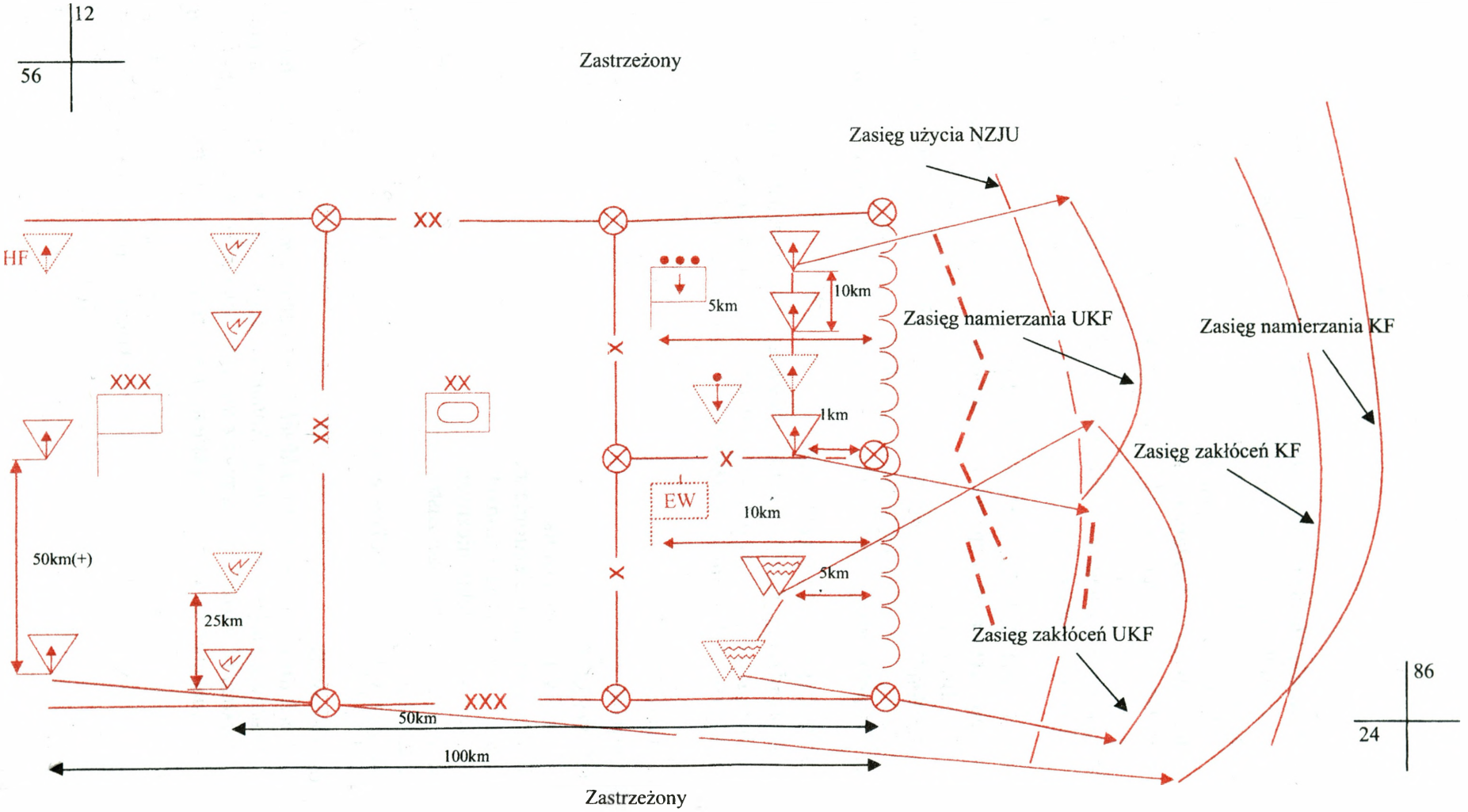
ZA ZGODNOŚĆ
(..poświadczenie G3..)

APENDYKSY:
1. Oleat – WRE przeciwnika
2. Plan obrony radioelektronicznej
3. Oleat – WRE wojsk własnych
4. Wykaz celów elektronicznych
5. Rejony i częstotliwości zastrzeżone
6. Plan zakłóceń
7. Wykaz wykrytych środków elektronicznych przeciwnika

Rozdzielnik: B

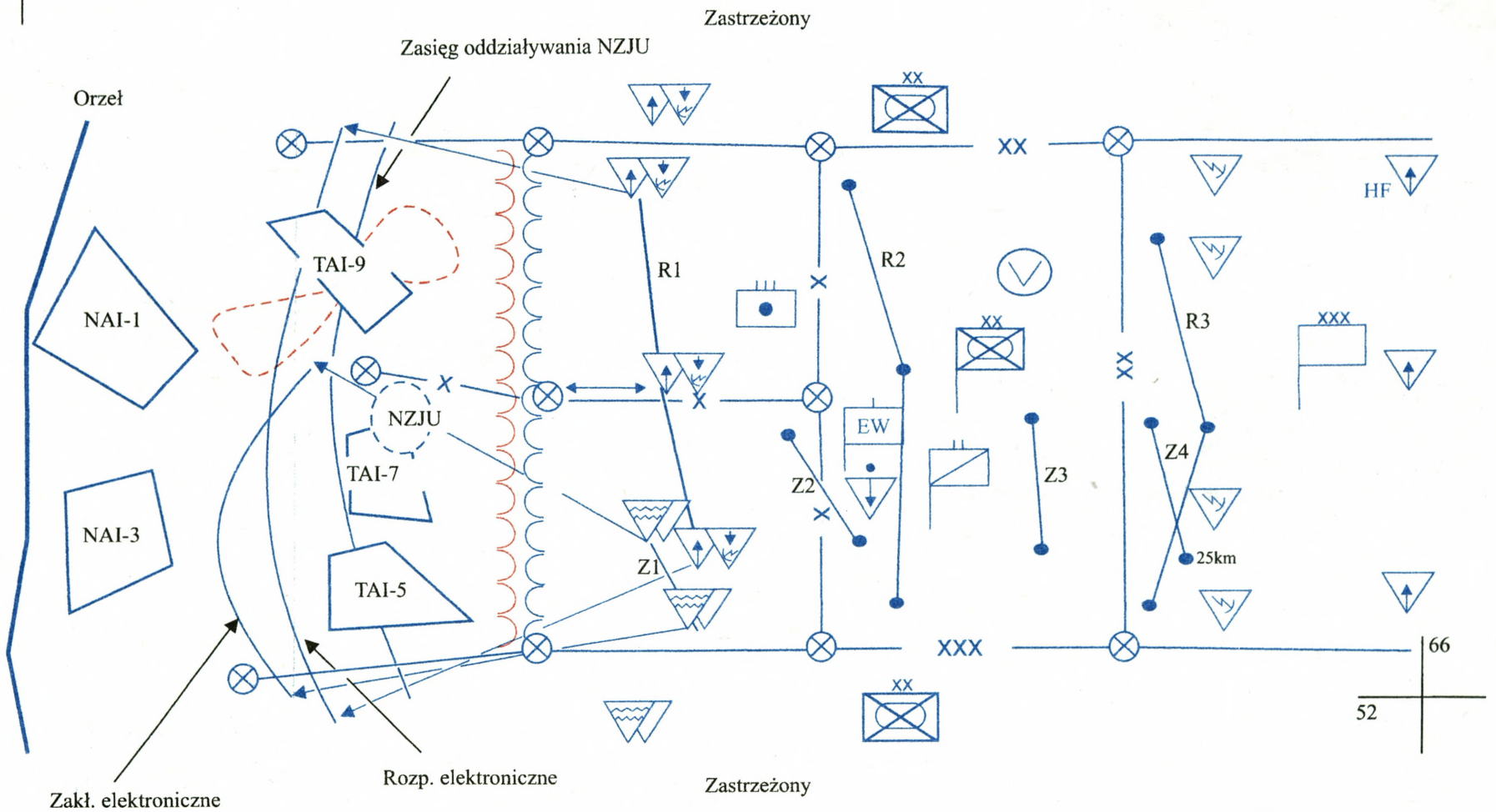
Jeżeli aneks jest wysyłany oddzielnie od rozkazu, musi być opisany tak jak rozkaz (strona tytułowa, podpis, rozdzielnik). Natomiast w sytuacji gdy jest on integralną częścią rozkazu i jest rozprowadzany według tego samego rozdzielnika, wystarczy sam tytuł dokumentu.- wówczas w aneksie nie umieszcza się tekstu zaznaczonego ramkami.

OLEAT - WALKA ELEKTRONICZNA PRZECIWNIKA - NATARCIE



96
48

OLEAT - PLAN WALKI ELEKTRONICZNEJ ZT - OBRONA



66
52

Akademii Obrony Narodowej
BIBLIOTEKA GŁÓWNA - ARCHIWUM
II
Nr Cimf 52596

Załącznik 15

H-6-1
Klauzula tajności

PLAN ZAKŁÓCEŃ ELEKTRONICZNYCH ZT

CZAS / WYKONAWCA	2 4 6 8 10 12 14 16 18 20 22	2 4 6 8 10 12 14 16 18 20
Plzr (grupa zakłóceń elektronicznych)	1 A — 2 C	
e. śm. WRE	3	
BAA	1 — 20 NZJU / A - 1500	

ZADANIE	Dezorganizacja systemu dowodzenia .... pa [1]	Dezorganizacja systemu kierowania ogniem ...DZ [2]	Dezorganizacja systemu dowodzenia . . .BPanc [3]	Dezorganizacja systemu dowodzenia . . .BZ [4]
Obszar zainteresowania i oddziaływania elektronicznego.	A – TAI – 8 NAI - 12 B – TAI – 9	C - TAI - 10 D - TAI - 7	E ..... F	
Zakłócane cele po wykryciu	A1500 A1560 A1590	A1540 A1565 A1575	A...	

H-6-1
Klauzula tajności