AKADEMIA
OBRONY NARODOWEJ

AON 5209/2000

Płk dr inż. Józef JANCZAK

MODELOWANIE SYMULACYJNE ZAGROŻENIA ELEKTRONICZNEGO MOBILNEGO SYSTEMU ŁĄCZNOŚCI ZWIĄZKU OPERACYJNEGO WOJSK LĄDOWYCH

WARSZAWA 2000

AKADEMIA OBRONY NARODOWEJ

AON 5209/2000

Płk dr inż. Józef JANCZAK

MODELOWANIE SYMULACYJNE ZAGROŻENIA ELEKTRONICZNEGO MOBILNEGO SYSTEMU ŁĄCZNOŚCI ZWIĄZKU OPERACYJNEGO WOJSK LĄDOWYCH

WARSZAWA 2000

Redaktor techniczny
Beata Klarowska

Korekta
Kazimiera Krześniak

Skład, druk i oprawa:
Akademia Obrony Narodowej – Wydział Wydawniczy
Zam. nr 776/99

SPIS TREŚCI

WSTĘP

Mobilny system łączności wojsk lądowych związku operacyjnego wojsk lądowych (MSŁ ZO WL) jest wielce złożonym i nieodzownym elementem systemu dowodzenia wojsk lądowych. O szczególnych właściwościach usługowych systemu stanowią przede wszystkim jego urządzenia telekomunikacyjne. Współczesne urządzenia telekomunikacyjne posiadają ogromne możliwości i dzięki temu usprawniają proces dowodzenia wojskami. Mają jednak szereg wad, wyeliminowanie których wymaga podejmowania skomplikowanych działań. Do najistotniejszych, niepożądanych cech mobilnego systemu łączności ZO WL można zaliczyć:

– brak pełnej gwarancji bezpieczeństwa danych przesyłanych pomiędzy użytkownikami systemu,

– promieniowanie na zewnątrz ubocznych produktów, które ujawniają strukturę systemu, a tym samym – pozwalają zlokalizować miejsca pracy jego użytkowników, a nawet przerwać (zakłócić) ich proces komunikowania się.

Powyższe niepożądane cechy powodują, że mobilny system łączności ZO WL jest obiektem szczególnego zainteresowania sił zbrojnych ewentualnych przeciwników RP, bowiem jest opłacalnym i dogodnym celem do rozpoznania, niszczenia środkami ogniowymi i zakłócenia środkami walki elektronicznej (WE). Zmasowane użycie środków rozpoznania i walki elektronicznej przez siły zbrojne tych państw, w ścisłym współdziałaniu ze środkami ogniowymi (głównie z bronią precyzyjnego rażenia) umożliwia skuteczne obniżenie zdolności do wykonania zadań stojących przed systemem łączności, a tym samym – przed systemem dowodzenia wojskami. Należy podkreślić, że wykonanie takiego zadania nie stwarza większych problemów współczesnym siłom i środkom WE tych państw, bowiem cały obszar naszego kraju znajduje się w zasięgu satelitarnych i powietrznych systemów rozpoznania elektronicznego oraz wielospektralnego rozpoznania obrazowego. Z obiektów satelitarnych i naziemnych (stacjonarnych i polowych) siły zbrojne innych państw mogą oddziaływać elektronicznie (prowadzić rozpoznanie i zakłócanie elektroniczne) na

podsystemy łączności bezprzewodowej w zakresie fal długich, średnich, krótkich i ultrakrótkich, obejmując zasięgiem niemal całe terytorium Polski. W takiej sytuacji wystąpią zjawiska *zagrożenia elektronicznego* mobilnego systemu łączności ZO WL, a w konsekwencji – dezorganizacja funkcjonowania systemu dowodzenia wojskami i kierowania środkami walki. Oznacza to, że zagadnienie określenia wielkości zagrożenia elektronicznego mobilnego systemu łączności ZO WL jest niezmiernie istotne zarówno dla jego projektantów jak i przyszłych jego eksploatatorów. Nie może być rozwiązywane w dalszym ciągu przy pomocy tradycyjnych metod.

Dostrzegając wagę tego problemu, autor podjął się przedstawienia projektu koncepcyjnego modelu symulacyjnego zagrożenia elektronicznego mobilnego systemu łączności ZO WL[1], jako skutecznego narzędzia, wykorzystującego możliwości środków informatycznych do modelowania ww. zjawisk w postaci komputerowych gier wojennych.

Praca studyjna składa się ze wstępu, 3 rozdziałów merytorycznych, zakończenia, wykazu bibliograficznego oraz załączników.

Wstęp obejmuje uzasadnienie opracowania pracy, jej cel oraz ogólną charakterystykę.

W rozdziale pierwszym uzasadniono możliwości zastosowania symulacji komputerowej do modelowania zagrożenia elektronicznego mobilnego systemu łączności związku operacyjnego wojsk lądowych.

W rozdziale drugim zawarto model matematyczny zagrożenia elektronicznego mobilnego systemu łączności związku operacyjnego wojsk lądowych.

W rozdziale trzecim przedstawiono projekt koncepcyjny modelu symulacyjnego zagrożenia elektronicznego mobilnego systemu łączności związku operacyjnego wojsk lądowych.

W zakończeniu wskazano na możliwości wykorzystania modelu w sztabach wojsk lądowych różnych szczebli dowodzenia oraz w działalności dydaktycznej uczelni wojskowych i placówek naukowych.

---

[1] Stwierdzenie to stanowi cel pracy studyjnej.

Wykonany na podstawie modelu projekt technologiczny oraz komputerowa egzemplifikacja modelu może być wykorzystana w Szefostwach Wojsk Łączności i Informatyki Okręgów Wojskowych (ZO) oraz w Oddziałach Rozpoznania i WE (G-2), a także w specjalistycznych placówkach dydaktycznych i naukowych. Stworzy bowiem możliwość prowadzenia wszechstronnych eksperymentów, uwzględniających dynamicznie zmieniającą się sytuację elektroniczną we współczesnych zbrojnych działaniach wojennych.

1. MOŻLIWOŚCI ZASTOSOWANIA SYMULACJI KOMPUTEROWEJ DO MODELOWANIA ZAGROŻENIA ELEKTRONICZNEGO MOBILNEGO SYSTEMU ŁĄCZNOŚCI ZWIĄZKU OPERACYJNEGO WOJSK LĄDOWYCH

1.1. Wprowadzenie

Symulacja jako metoda badawcza, aczkolwiek znana i stosowana od dawna, dopiero dzięki technice komputerowej uzyskała właściwe oblicze i nabrała tym samym szczególnego znaczenia. Właśnie dzięki symulacji komputerowej zwiększyły się znacznie możliwości budowy modeli złożonych systemów działania oraz prowadzenia badań w szerokim zakresie zmian warunków ich funkcjonowania.

Ważną cechą symulacji komputerowej jest jej naukowo-artystyczny charakter[2]. Oznacza to, że przy obecnym stanie wiedzy, mimo naukowego rozwiązania wielu zagadnień szczegółowych, nadal pozostawia się znaczne pole intuicji i doświadczeniu eksperymentatora[3]. Nie zostały jeszcze ostatecznie ukształtowane ogólne zasady tworzenia modeli symulacyjnych i badania ich adekwatności. Aktualnie jednak panuje ciągle jeszcze znaczna różnorodność podejść interpretacyjnych oraz ocen istoty i treści symulacji komputerowej jako metody oceny zagrożenia elektronicznego złożonych systemów działania, jakimi bez wątpienia są mobilne systemy łączności wojsk lądowych. Wyrazem tego jest znaczne zróżnicowanie proponowanych przez czołowych przedstawicieli badań symulacyjnych definicji i procedur badawczych[4].

---

[2] E.R. Shannon: *System simulation – the art and science*. Prince-Hall, Inc., Englewood Cliffs, New Jersey 1975.

[3] G. Beney: *Models and reality: some reflection on the art and science of simulation*. w: Simulation, 1977, 29/5.

[4] F. Ackoff – „Symulacja to sposób użycia modelu. Jest to eksperymentowanie nie tyle z samym zjawiskiem, co raczej z jego modelem. Modele są fotografiami, a symulacja – filmami zjawisk".

T. Naylor – „Symulacja – jest to technika numeryczna dokonywania eksperymentów na pewnych rodzajach modeli matematycznych, które opisują przy pomocy EMC zachowanie się złożonego systemu w ciągu długiego okresu czasu".

F. Barton – „Symulacja – jest to działanie modelu systemu przedmiotowego, realizowane w jakimś określonym celu".

Analiza zamieszczonych w przypisie i wielu innych, nie wymienionych definicji wskazuje na dużą różnorodność interpretacji pojęcia „symulacja" oraz na pewną cechę modeli i metod symulacyjnych, którą jest *imitacja zjawisk zachodzących w systemach rzeczywistych.*

Zasadniczą rolę w symulacyjnej metodzie badawczej odgrywa poprawne sformułowanie modelu badanego systemu, ukierunkowanego na odwzorowanie zdarzeń, zjawisk i procesów, a więc – dynamiki systemu.

Przez *model symulacyjny* należy rozumieć model symboliczno-formalny, w którym do opisu zachowania się systemu w wybranym przedziale czasu wykorzystuje się zarówno aparat opisu matematycznego, jak i niematematycznego, który umożliwia symulację na komputerach. Modele symulacyjne są z reguły prostsze w stosunku do modeli analitycznych. Dają się formułować w oparciu o logiczny opis działania poszczególnych elementów systemu i często nie wymagają analitycznego określenia złożonych relacji charakteryzujących funkcjonowanie całego systemu (np. funkcyjnych opisów zależności bodźców i reakcji systemu).

W dostępnej literaturze przedmiotu [1, 2, 6] funkcjonuje także dość złudny pogląd, którego wyznawcy uważają, że tworzenie modeli symulacyjnych jest stosunkowo proste i ułatwione w odniesieniu do procesów walki i operacji w wojskach lądowych. Uważają oni bowiem, że w nauce wojskowej funkcjonuje stosunkowo mało precyzyjny, opisowy język, określający możliwy przebieg działań bojowych, od którego łatwo jest przejść do logicznego opisu działania badanego systemu, czyli do sformułowania modelu symulacyjnego. Trudno podzielić ten pogląd, albowiem na stopień trudności w opracowaniu modelu ma wpływ nie tylko język opisu systemu, a przede wszystkim – sam system, jego charakter, stopień złożoności i warunki funkcjonowania. To projektant musi ocenić, czy stopień precyzji stosowanego aktualnie języka opisu systemu

---

R. Cruon – „Symulacja jest to eksperymentalne użycie abstrakcyjnego modelu".

G. Evans – „Symulacja – jest to zastosowanie modelu w celu chronologicznego wygenerowania historii stanów tegoż modelu, a która jest uważana za historię stanów modelowanego sytemu".

G. Gordon – „Symulację systemów definiujemy jako technikę rozwiązywania zagadnień polegającą na śledzeniu w czasie zmian zachodzących w dynamicznym modelu układu".

I. Maroński – „Metoda symulacji – jest to technika badania systemów przez obserwację modelu tego systemu".

umożliwia opracowanie jego modelu symulacyjnego. Jeśli jest inaczej, zwiększa się znacznie zakres prac badawczych i opisowych modelowego systemu. Wykorzystując symulację komputerową jako metodę modelowania procesów zagrożenia elektronicznego MSŁ ZO WL, należy mieć na uwadze tak ważne problemy, jak *historia stanów*[5] modelowanych zjawisk, obejmująca systemy i wojska walki elektronicznej potencjalnego przeciwnika oraz własne systemy i wojska łączności, znajdujące się w każdej chwili w określonym stanie (położenie, rodzaj działań, stan sił i środków, zakres oraz intensywność oddziaływania przeciwnika oraz intensywność ruchu we własnym SŁ itp.). Badając modelowane zagrożenie elektroniczne MSŁ ZO WL należy rozważyć jego stany w chronologicznym porządku kolejnych chwil należących do danego przedziału czasowego. Historia stanów składa się z szeregu chronologicznie uporządkowanych opisów, odpowiadających stanom systemu w każdej z rozpatrywanych w danym przedziale kolejnych chwil czasu. Wygenerowana historia stanów (informacje wynikowe z symulacyjnych programów komputerowych) jest jedną z najcenniejszych informacji podczas oceny zagrożenia elektronicznego MSŁ ZO WL.

Należy mieć na względzie, że w sensie ogólnym *model bezpośrednio nie przedstawia działania lub zachowania się badanego systemu.* Przedstawienie jego działania lub zachowania się umożliwia dopiero historia stanów modelu. Mając więc system i jego model należy przyjąć, że *symulacja jest to zastosowanie modelu w celu chronologicznego wygenerowania historii stanów tegoż modelu, a która jest uważana za historię stanów modelowanego systemu.*

Analiza wyników badań zamieszczonych w dostępnej literaturze przedmiotu wskazuje na znaczną przydatność symulacji komputerowej do modelowania procesów walki, a w tym i zagrożenia elektronicznego MSŁ ZO WL. Aktualnie jednak brak jest jednolitego *kryterium celowości stosowania symulacji komputerowej*. Mimo tego, można wskazać kilka cech decydujących o jej stosowaniu, do których należą przede wszystkim:

– możliwość badania oraz eksperymentowania w zakresie złożonych wewnętrznych interakcji występujących w badanym systemie;

[5] Historia stanów modelowanego systemu rzeczywistego (hipotetycznego) jest jedną z podstawowych kategorii symulacji komputerowej.

– możliwość badania „osobliwości" funkcjonowania systemu w szerokim zakresie zmian warunków jego funkcjonowania;

– możliwość badania wpływu zmian informacyjnych, organizacyjnych lub innych – występujących w otoczeniu na działanie systemu, przez wprowadzenie zmian w modelu systemu i obserwację oddziaływań tych zmian na zachowanie się systemu;

– szczegółowa informacja o symulowanym systemie może doprowadzić do lepszego zrozumienia sposobu jego funkcjonowania i do wypracowania propozycji jego usprawnienia, osiągnięcie czego innymi sposobami nie byłoby możliwe;

– symulacja może być użyta jako instrument pedagogiczny w nauczaniu (studentów i praktyków) podstawowych umiejętności w zakresie analizy teoretycznej, analizy statystycznej i teorii podejmowania decyzji;

– symulacja pozwala na badanie systemów dynamicznych zarówno w czasie skomprymowanym, jak i w dłuższym okresie;

– doświadczenia prowadzone przy pomocy symulacji nie mają bezpośredniego wpływu na badany system;

– symulacja znacznie skraca czas badania systemu.

Symulacja komputerowa, jako metoda badania złożonych systemów działania jest ciągle w fazie opracowywania. Dlatego odpowiedź na pytanie: kiedy poszukiwać rozwiązań analitycznych, a kiedy stosować symulację? – pozostaje nadal zagadnieniem otwartym. Nie wydaje się prawdopodobne, aby w bliskiej przyszłości można było sformułować ogólne wskazówki, które pozwoliłyby praktykowi na uzyskanie łatwej odpowiedzi na tak postawione pytania.

1.2. Ogólne zasady modelowania symulacyjnego zagrożenia elektronicznego mobilnego systemu łączności związku operacyjnego wojsk lądowych

Model symulacyjny zagrożenia elektronicznego mobilnego systemu łączności związku operacyjnego wojsk lądowych przedstawia sobą pewną symboliczną abstrakcję, skonstruowaną zgodnie z zachodzącymi w rzeczywistym systemie zjawiskami i procesami, lub – jak to ma miejsce dla systemów hipotetycznych – opartą na określonych założeniach teoretycznych. Powstaje on

w wyniku głębokiej analizy modelowanych zjawisk na drodze symbolicznego, matematycznego i niematematycznego opisu. Konstrukcja modelu symulacyjnego zagrożenia elektronicznego MSŁ ZO WL powinna przewidywać odwzorowanie takiego obszaru zjawisk i procesów oraz zastosowania w szczególności takiego aparatu matematycznego, a także wykorzystania takiego zbioru informacji (wejściowych i tych, które do modelu wkomponowano na stałe), które – ze względu na otrzymane wyniki – pozwolą z dostatecznym przybliżeniem sądzić o przebiegu procesów rzeczywistych. Przyjęte ponadto w procesie symulacyjnego modelowania zagrożenia elektronicznego MSŁ ZO WL założenia i podstawy teoretyczne odpowiadać powinny założeniom nauki wojskowej, zasadom taktyki i sztuki operacyjnej oraz teorii i metodom dowodzenia. Uwzględniać powinny także obowiązujące zarządzenia i regulaminy, perspektywy rozwoju metod i środków WE przeciwnika oraz łączności wojsk własnych, a także powinny bazować – co jest równie ważne – na całym dotychczasowym doświadczeniu i głębokiej znajomości przeciwnika.

Modelowanie symulacyjne zagrożenia elektronicznego MSŁ ZO WL – podobnie jak modelowanie walki należy do najbardziej złożonych i czasochłonnych. Wymaga on od projektanta doskonałej znajomości modelowanych systemów, zjawisk i procesów w nich zachodzących oraz rozległej wiedzy teoretycznej oraz praktycznych umiejętności w zakresie modelowania (nie tylko symulacyjnego) złożonych systemów działania. Powstanie i rozwój symulacji komputerowej, która współcześnie znajduje coraz szersze zastosowanie w wielu dziedzinach praktycznej i twórczej działalności człowieka znacznie ułatwia pracę projektanta. Coraz szersze jej wykorzystanie wpływa na ilościowy i jakościowy rozwój komputerowych gier wojennych (KGW). Doświadczenia wskazują, że opracowując dowolny symulacyjny model działań bojowych, szczególną uwagę należy zwrócić na takie zagadnienia jak:

– zakres i stopień szczegółowości odwzorowania elementów, zjawisk i procesów systemu rzeczywistego;
– procedura realizacji i sposobu opisu modelu;
– wymagania jakie powinien spełniać model;
– ocena adekwatności modelu;
– kryteria oceny modelowanego systemu.

Podstawę (bazę informacyjną) do rozpoczęcia prac nad modelowaniem symulacyjnym zagrożenia elektronicznego MSŁ ZO WL powinny stanowić przede wszystkim:

– wyniki badań rzeczywistych systemów WE przeciwnika oraz MSŁ ZO WL;

– sformułowane ogólne i szczegółowe cele modelu symulacyjnego jako komputerowej gry wojennej (KGW);

– sprecyzowane wymagania dotyczące struktury, treści i sposobu wykorzystania KGW.

Uogólniona analiza wszystkich z wymienionych elementów oraz występujących między nimi zależności i uwarunkowań powinna umożliwić określenie taktycznych granic i treści modelowanego zagrożenia elektronicznego MSŁ ZO WL, związki matematyczno-logiczne, które odwzorowują zjawiska i procesy rzeczywistych systemów WE przeciwnika oraz MSŁ ZO WL, oraz treść i strukturę informacji wejściowych niezbędnych do funkcjonowania modelu symulacyjnego zagrożenia elektronicznego MSŁ ZO WL.

Efektem tak przeprowadzonej analizy, w zakresie modelowania symulacyjnego zagrożenia elektronicznego MSŁ ZO WL powinno być:

– sporządzenie zbioru możliwych, szczegółowych scenariuszy przebiegu działań rzeczywistych systemów WE przeciwnika oraz MSŁ ZO WL, z uwzględnieniem etapów tych działań, czasu i przestrzeni oraz biorących udział w działaniach sił i środków;

– wypracowanie uogólnionego obrazu sytuacji elektronicznej (w oparciu o sporządzone scenariusze), który powinien stanowić tło taktyczne modelu symulacyjnego;

– ustalenie rodzaju i zakresu działań – prowadzonych przez obie walczące strony i odwzorowywanych w modelu symulacyjnym;

– ustalenie elementów uczestniczących w walce po obu stronach, które zamierza się odwzorować w modelu symulacyjnym;

– opisanie środowiska operacji (walki) i jego wpływu na funkcjonowanie obu walczących stron;

– określenie dla systemów WE przeciwnika oraz MSŁ ZO WL zbiorów możliwych stanów i związanych z nimi zdarzeń oraz czynniki określające czasy

ich funkcjonowania w poszczególnych stanach i warunki wymuszające zmiany stanów;

– określenie tych decyzji obu walczących stron, w wyniku podjęcia których powstające informacje stanowią dane wejściowe do modelu symulacyjnego zagrożenia elektronicznego MSŁ ZO WL;

– ustalenie rodzaju i zakresu parametrów opisujących pododdziały i oddziały WE przeciwnika oraz wojsk łączności ZO WL oraz sprzętu i środków walki, które powinny być uwzględnione w modelu symulacyjnym zagrożenia elektronicznego MSŁ ZO WL;

– określenie sposobów i wskaźników identyfikacji sił i środków wojsk własnych i przeciwnika, znajdujących się w rejonach, z których istnieje możliwość wzajemnego oddziaływania elektronicznego.

Podczas modelowania symulacyjnego zagrożenia elektronicznego MSŁ ZO WL najwięcej wątpliwości budzi zwykle problem *stopnia szczegółowości odwzorowania elementów modelu*. Wydaje się, potwierdzają to zresztą wyniki prac projektowych nad KGW, że w tym zakresie jako wiodące powinno być przyjęte dążenie do szczegółowego uwzględnienia w modelu symulacyjnym tylko tych elementów rzeczywistych systemów WE przeciwnika oraz MSŁ ZO WL, bez odwzorowania których opracowanie modelu nie jest możliwe. Te elementy, których nie odwzorowuje się w modelu wprost, powinny być uwzględnione w tzw. *modułach funkcjonalnych*. Na pierwszym planie powinno znajdować się również przestrzeganie zasady jedności charakterystyk czasowo-przestrzennych zadań bojowych, do wykonania których przeznacza się posiadane obiekty, siły i środki.

Nie bez znaczenia jest również rola jaką spełnia elementarny środek WE przeciwnika oraz środek łączności w całokształcie działań bojowych. Dlatego też oceniając stopień szczegółowości odwzorowania elementów, zjawisk i procesów w modelowanym systemie WE przeciwnika oraz MSŁ ZO WL, należy uwzględnić między innymi:

– zakres zadań i funkcji jakie powinny realizować pododdziały, oddziały i funkcjonalne podsystemy WE przeciwnika oraz elementów MSŁ ZO WL od-

wzorowane w modelu symulacyjnym, uwzględnienie których determinuje ich użyteczność;

– zakres i stopień zgodności parametrów opisujących zadania bojowe, planowane dla pododdziałów i oddziałów WE przeciwnika oraz wojsk łączności ZO, ZT i oddziałów WL;

– możliwość realizacji samodzielnego zadania bojowego przez elementarny środek walki (WE przeciwnika oraz wojsk łączności ZO, ZT i oddziałów WL).

Uwzględnienie ww. zaleceń powinno ułatwić projektantowi – najczęściej w kilku cyklach iteracyjnych – opracowanie takiego modelu symulacyjnego zagrożenia elektronicznego MSŁ ZO WL, w którym zakres i stopień szczegółowości odwzorowania zjawisk i procesów systemów rzeczywistych odpowiada sformułowanym celom i wymaganiom KGW.

Po opracowaniu pierwszej, w pewnym sensie – przybliżonej wersji modelu symulacyjnego, należy przystąpić do szczegółowego precyzowania jego treści i struktury. Wydaje się celowe, aby po zakończeniu związanych z tym czynności i procedur, udzielić wyczerpującej odpowiedzi na następujące pytania:

– czy nie włączono do modelu żadnych niewłaściwych zmiennych, to znaczy takich, które mało przyczyniają się do możliwości prawidłowego przewidywania zachowań się wyjściowych zmiennych modelu?

– czy nie pominięto którejkolwiek ze zmiennych wejściowych, które prawdopodobnie oddziaływają na zachowanie się zmiennych wyjściowych modelu?

– czy nie popełniono nieścisłości w opisie jakichkolwiek zależności funkcyjnych między zmiennymi wyjściowymi i wejściowymi?

– czy prawidłowo aproksymowano oceny parametrów podstawowych cech modelu lub równań obrazujących zachowanie się w systemie rzeczywistym?

– czy estymacje parametrów użytych w modelu symulacyjnym są istotne pod względem statystycznym?

– jak na podstawie odrębnych obliczeń (jeśli jeszcze nie powstał program komputerowy) porównać teoretyczne wartości uzyskiwanych w modelu informacji wyjściowych z historycznymi wartościami zmiennych?

Gdy uzyska się pozytywną odpowiedź *na każde* z wymienionych pytań, można przejść do kolejnych faz projektowania modelu symulacyjnego zagroże-

nia elektronicznego MSŁ ZO WL związanych z oceną jego adekwatności i opracowaniem kryteriów oceny modelowanych procesów.

W toku szczegółowego precyzowania treści i struktury modelu, należy uwzględnić także *wymagania* jakie powinien spełnić model symulacyjny zagrożenia elektronicznego MSŁ ZO WL. Należy podkreślić, że wymagania ogólne, precyzowane dla symulacyjnych modeli walki mają charakter operacyjno-systemowy i odpowiednio obejmują:

1) w zakresie wymagań operacyjnych:

– obiektywizm rezultatów modelowania, który uzyskuje się poprzez szczegółowe odwzorowania czynników i warunków istotnych dla modelowania działań bojowych, a także poprzez zastosowanie takiego aparatu matematycznego, który modelowane procesy opisuje z wymaganą precyzją;

– szybkość uzyskiwania wyników z komputerowej realizacji modelu (odpowiednią do szczebla dowodzenia, odwzorowywanego w ramach KGW), którą uzyskuje się poprzez wykorzystanie szybkiego komputera, jednorazowe założenie i bieżącą aktualizację bazy danych, racjonalną konstrukcją algorytmów i programów, prosty sposób przygotowania danych wejściowych, czytelne wydruki z komputera oraz poprzez wyrabianie w użytkownikach przekonania do wykorzystania KGW;

– unifikację wykorzystywanych kryteriów i normatywów – poprzez opracowanie dla każdego modelu (kompleksu modeli) systemu spójnych i niesprzecznych kryteriów – głównych i cząstkowych;

– czułość modelu na zmiany wartości parametrów i wskaźników opisujących odwzorowywane w modelu działań bojowych zjawiska, procesy i elementy systemu rzeczywistego, którą uzyskuje się poprzez taką konstrukcję zależności funkcyjnych i odwzorowanie takiego zbioru zdarzeń i stanów zagrożenia elektronicznego MSŁ ZO WL, przy których istotna zmiana wartości parametrów lub (i) wskaźników wywołuje widoczne zmiany w modelowanym systemie;

– ochronę informacji przetwarzanych w komputerze – głównie poprzez działania o charakterze organizacyjno-technicznym.

2) w zakresie wymagań systemowych:

– modularność opracowywanych modeli (submodeli), którą uzyskuje się poprzez dopasowanie poszczególnych modeli (submodeli) do poziomu dowodzenia, dla którego zostały opracowane oraz do celu i przeznaczenia, wymagań operacyjnych i uwzględnianego w procesie ich modelowania zbiorów innych czynników: struktury i treści informacji wejściowej/wyjściowej, kryteriów i normatywów, systemu klasyfikacji i kodowania, zawartości banku danych, wykorzystywanych środków informatyki itd.;

– efektywne wykorzystanie bazy danych przez wszystkie opracowane modele walki, co uzyskuje się poprzez uniezależnienie jej struktury od programów komputerowych i struktury danych wejściowych oraz poprzez centralne jej tworzenie i traktowanie, systematyczną aktualizację, przestrzeganie wymagań trybu wykorzystania i zasad dostępu do przechowywanych zbiorów informacji;

– unifikację form matematycznego opisu projektowanego modelu zagrożenia elektronicznego MSŁ ZO WL, co uzyskuje się poprzez ujednolicenie symboliki i form przedstawiania oraz jednakową ich interpretację.

Odwzorowanie wszystkich z wymienionych wymagań, w każdym konkretnym przypadku modelowania symulacyjnego zagrożenia elektronicznego MSŁ ZO WL jest mało prawdopodobne, jednak pełna wiedza o zakresie problematyki jakiej dotyczą, dyscyplinuje proces projektowania modelu symulacyjnego, a często i całej KGW. W ten sposób może przyczynić się do większej efektywności działań projektanta.

Podczas modelowania symulacyjnego zagrożenia elektronicznego MSŁ ZO WL istotną rolę spełniają poprawnie sformułowane *założenia i ograniczenia*. Tę część z nich, która określa w pewnym stopniu granice modelowania, należy sprecyzować już w początkowej fazie projektowania modelu. Udokładnia się zaś i formułuje dalsze – po całkowitym jego opracowaniu. Założenia i ograniczenia modelu symulacyjnego odnoszą się także do całej KGW, w której model będzie funkcjonował i powinny obejmować m.in.:

– zakres i stopień szczegółowości odwzorowania pododdziałów (oddziałów) WE przeciwnika oraz łączności wojsk własnych;

– graniczne wartości przyjętych normatywów i wskaźników;

– postać zależności funkcyjnych i generatorów liczb losowych;

– ilość i charakter ról spełnianych w grze;
– charakter i przebieg gry;
– ilość uczestników gry i reguły oceny graczy.

Szczegółowy opis założeń i ograniczeń powinien być przedstawiony przy opisie poszczególnych modułów modelu symulacyjnego zagrożenia elektronicznego MSŁ ZO WL.

1.3. Sposoby oceny adekwatności modelu symulacyjnego zagrożenia elektronicznego MSŁ ZO WL

W modelowaniu symulacyjnym szczególnie wiele problemów sprawia *ocena adekwatności* opracowanych modeli, czyli zgodności opisu systemu z jego stanem rzeczywistym[6]. Wynika to głównie z ograniczonej przewidywalności zachowań systemów działania, która stanowi ich immanentną cechę. Istotna jest także konieczność takiego wyboru języka i narzędzi modelowania symulacyjnego, aby na tę cechę systemów działania nie „nakładały się" ograniczenia będące własnościami samego modelu.

Ocena adekwatności modeli symulacyjnych polega na opracowaniu reguły, która w oparciu o wyniki eksperymentów na badanym systemie rzeczywistym lub sprawdzonych modelach oraz wyniki uzyskane na podstawie modelu symulacyjnego, pozwala na wypowiedź wartościującą: wyrażającą aprobatę lub dezaprobatę dla modelu, z punktu widzenia adekwatności modelu i badanej rzeczywistości[7]. Zwykle jest ona realizowana w oparciu o *predykcję retrospektywną* procesów zachodzących w systemie rzeczywistym. W zależności od charakteru i celu badań symulacyjnych oraz od zakresu i stopnia szczegółowości posiadanych informacji o rzeczywistym systemie, ocena adekwatności modelu symulacyjnego ma charakter *jakościowy* lub *ilościowy*.

Jakościowa ocena adekwatności powinna polegać przede wszystkim na poprawności wyznaczania historii stanów modelu symulacyjnego. Dla wskaźni-

[6] P. Sienkiewicz: *Inżynieria systemów – wybrane zastosowania wojskowe*. Wyd. MON, Warszawa 1983.

[7] E. Kołodziński, T. Pietkiewicz: *Adekwatność modeli symulacyjnych*. Postępy Cybernetyki, nr 2/1978.

ków jakościowych, będących zwykle zmiennymi losowymi, jako oceny przyjmuje się najczęściej miarę *niezgodności rozkładów prawdopodobieństw* opisujących zmienne losowe systemu rzeczywistego i jego modelu symulacyjnego. Ocena polega w głównej mierze na wyznaczeniu stopnia niezgodności pomiędzy ciągami wyników obserwacji procesów systemu rzeczywistego i jego modelu symulacyjnego.

Ocena ilościowa powinna dotyczyć zgodności wartości określonych wielkości uzyskanych z eksperymentu symulacyjnego oraz eksperymentu przeprowadzonego na systemie rzeczywistym i obejmuje zgodność wskaźników jakościowych badanego procesu i jego modelu oraz zgodność historii stanów badanego procesu z historią stanów modelu symulacyjnego.

Ocena adekwatności modelu symulacyjnego zagrożenia elektronicznego MSŁ ZO WL, ze względu na specyfikę tego typu systemu, polegającą głównie na ograniczonych możliwościach uzyskania pełnych, aktualnych i niezawodnych informacji o systemie rzeczywistym (w warunkach pokojowych nie istnieje przecież możliwość „uruchomienia" systemu i przeprowadzenia jego badań z zachowaniem pełnych realiów pola walki), z konieczności musi mieć charakter przede wszystkim jakościowy. Oznacza to, że w wyniku oceny adekwatności modeli można stwierdzić, że *model jest dobry lub zły*. Nie można natomiast nic powiedzieć o stopniu zgodności modelu z rzeczywistym zagrożeniem elektronicznym MSŁ ZO WL. Brak informacji o warunkach funkcjonowania rzeczywistego zagrożenia nie wyklucza jednak całkowicie możliwości przeprowadzenia ilościowej oceny adekwatności modelu symulacyjnego. Powinna jednak ona być ograniczona i dotyczyć tylko wybranych fragmentów modelu (obszarów funkcjonowania rzeczywistego zagrożenia), a opierać się głównie na informacjach historycznych oraz uzyskanych na podstawie innych, sprawdzonych już modeli. Jak wskazują doświadczenia, ocena adekwatności modelu symulacyjnego zagrożenia elektronicznego MSŁ ZO WL powinna przebiegać niejako w trzech płaszczyznach, obejmujących odpowiednio[8]:

[8] E.R. Shannon w: *System simulation – the art and science.* Prince-Hall, Inc., Englewood Cliffs, New Jersey, 1975.

– ocenę zgodności informacji wejściowych rzeczywistego systemu WE przeciwnika oraz MSŁ WŁ i informacji wejściowych wykorzystywanych w modelu symulacyjnym;

– ocenę „wewnętrznej" zgodności modelu z przebiegiem procesów, zjawisk i funkcjonowania rzeczywistego systemu WE przeciwnika oraz MSŁ ZO WL wojsk własnych;

– ocenę zgodności informacji wyjściowych modelu symulacyjnego z informacjami uzyskiwanymi w rzeczywistym systemie WE przeciwnika oraz MSŁ ZO WL wojsk własnych (ocena problemowa o charakterze taktyczno-operacyjnym).

Ocena adekwatności modelu symulacyjnego zagrożenia elektronicznego MSŁ ZO WL nie powinna sprowadzać się tylko do obserwacji określonych wartości systemu rzeczywistego i modelu symulacyjnego, konstrukcji właściwych kryteriów oceny, czy też prowadzenia niezbędnych w tym celu eksperymentów symulacyjnych. Stanowi bowiem złożony kompleks przedsięwzięć realizowanych we wszystkich etapach projektowania modelu symulacyjnego. Szczegółową analizę przedsięwzięć i zabiegów zmierzających do uzyskania maksymalnej zgodności modelu symulacyjnego z systemem rzeczywistym, realizowanych w każdym etapie, wydaje się celowe przedstawić na tle współzależności poszczególnych etapów badań symulacyjnych. Wzrost zgodności modelu symulacyjnego i rzeczywistego zagrożenia elektronicznego MSŁ ZO WL uzyskać można:

1) na etapie badań rzeczywistego zagrożenia elektronicznego MSŁ ZO WL poprzez:

– dobór takich metod i procedur badawczych oraz taką organizację procesu badań, które umożliwiają uzyskanie pełnych, aktualnych i wiarygodnych informacji o tych zjawiskach, procesach, elementach i warunkach funkcjonowania rzeczywistego zagrożenia elektronicznego MSŁ ZO WL, których znajomość jest istotna z punktu widzenia projektowania modeli symulacyjnych. Najczęściej będą to informacje dotyczące czasowych i strukturalnych charakterystyk strat ponoszonych przez wojska, przebiegu zmian w funkcji wszystkich ważnych czynników, wartości parametrów opisujących poszczególne rodzaje i typy

środków WE przeciwnika i łączności, np. moce nadajników, rodzaje pracy, zyski energetyczne anten itp.;

2) na etapie modelowania zagrożenia elektronicznego MSŁ ZO WL poprzez:

a) sprawdzenie, na ile logiczne sieci działań[9] i wykorzystywane zależności matematyczne wyrażają koncepcję modelu, co w szczególności obejmuje:

– odwzorowanie wszystkich istotnych zjawisk, procesów i elementów rzeczywistego systemu WE przeciwnika oraz MSŁ ZO WL;

– porównanie każdej funkcji modelu z jej realizacją w sieci działań;

– sprawdzenie poprawności rozwiązań i przejść w sieci działań;

– zbadanie stopnia czytelności i dokładności opisu poszczególnych bloków i modułów modelu;

– sprawdzenie kompletności opisu poszczególnych bloków i modułów modelu;

– zbadanie prawidłowości przyjętego sposobu numeracji bloków;

– sprawdzenie prawidłowości modyfikacji, korekt i uzupełnień we wszystkich blokach i modułach modelu;

b) sprawdzenie czy sieć działań jest pełna i realizuje funkcje we właściwej kolejności, co w szczególności obejmuje:

– sprawdzenie wszystkich logicznych cykli oraz wejść i wyjść;

– zbadanie wielkości wejściowych i wyjściowych łączących poszczególne bloki i moduły modelu;

– sprawdzenie hierarchicznego rozdziału elementów w sieci działań modelu;

– sprawdzenie istnienia w poszczególnych blokach i modelach określonych wejść i wyjść niezbędnych do poprawnego funkcjonowania logicznej sieci działań;

c) sprawdzenie prawidłowości wykorzystania wszystkich wyrażeń matematycznych, co w szczególności obejmuje:

– sprawdzenie prawidłowości wszystkich równań, w tym także – kryteriów oceny;

---

[9] Model symulacyjny w początkowej swojej formie jest przedstawiony w postaci logicznej sieci działań, zwanej także algorytmem ogólnym [9].

– zbadanie wiarygodności źródła informacji wejściowych dla wszystkich równań;

– zbadanie jednostek miary dla zmiennych we wszystkich wyrażeniach matematycznych;

– sprawdzenie prawidłowości przyjęcia wszystkich stałych w równaniach;

– sprawdzenie prawidłowości otrzymywania wszystkich stałych, parametrów i zmiennych;

– sprawdzenie prawidłowości używania wszystkich symboli matematycznych i symulacyjnych;

– zbadanie poprawności użycia indeksów, wielkości skalarnych i wektorów;

– sprawdzenie poprawności przyjęcia i funkcjonowania generatorów liczb losowych;

– zbadanie prawidłowości przyjęcia rozkładów opisujących odwzorowywane w modelu zmienne losowe;

– sprawdzenie prawidłowości zadanych wartości początkowych wszystkich parametrów i zmiennych;

– sprawdzenia kompletności tablic parametrów;

3) na etapie oprogramowania modelu zagrożenia elektronicznego MSŁ ZO WL poprzez:

– sprawdzenie pierwotnej programowej sieci działań z siecią działań otrzymaną w wyniku analizy programu;

– sprawdzenie poprawności poszczególnych podprogramów (modułów) poprzez wykonanie obliczeń na komputerze dla różnych wariantów danych testujących;

– sprawdzenie poprawności całego „symulatora", który łączy w sobie wszystkie sprawdzone podprogramy funkcjonujące, pod kontrolą specjalnego programu zarządzającego;

– analizę generowanych tzw. wydruków pośrednich, pozwalających śledzić poprawność zmian historii stanów modelu symulacyjnego;

4) na etapie projektowania przebiegu eksperymentu symulacyjnego poprzez:

– zaprojektowanie takiego układu eksperymentu symulacyjnego, w którym

właściwie rozwiązano problem zbieżności stochastycznej, rozmiaru i motywu projektowanego eksperymentu oraz tzw. reakcji wielokrotnych[10];

– wielokrotne rozgrywanie różnych wariantów modelu zagrożenia elektronicznego MSŁ ZO WL, przez doświadczonych oficerów sztabu przy udziale ekspertów;

– przygotowanie takiego wariantu danych wejściowych, a także wybór takich rozkładów zmiennych losowych, które *a priori* stwarzają ekstremalnie trudne warunki funkcjonowania modelowanego zagrożenia elektronicznego MSŁ ZO WL (jeśli wyniki z tak przeprowadzonego eksperymentu będą wg oceny ekspertów pozytywne, to istnieje duże prawdopodobieństwo tego, że model zostanie uznany za adekwatny do systemu rzeczywistego);

– rozgrywanie modelu symulacyjnego dla diametralnie różnych wariantów danych wejściowych i porównywanie otrzymanych rezultatów z ocenami ekspertów, wynikami ćwiczeń i badań poligonowych oraz z wynikami wcześniej opracowanych i sprawdzonych modeli zagrożenia elektronicznego MSŁ ZO WL;

– określenie granic problemowych, w których model symulacyjny wskazuje duży stopień zgodności z systemem rzeczywistym.

Przedstawione rozważania nie wyczerpują całej złożonej i bogatej problematyki oceny adekwatności modeli symulacyjnych. Mając na uwadze fakt, że absolutna adekwatność modelu symulacyjnego zagrożenia elektronicznego MSŁ ZO WL nie jest możliwa (chociażby ze względu na ograniczoną *przewidywalność*[11] systemów działania), celowe jest prowadzenie w tym zakresie dalszych prac, których wyniki służyć powinny zapewnieniu maksymalnej zgodności symulacyjnego modelu i systemu rzeczywistego.

[10] T.H. Naylor: *Modelowanie cyfrowe systemów ekonomicznych*. PWN, Warszawa 1975.

[11] Cecha ta jest traktowana często jako jeden z najistotniejszych czynników warunkujących uznanie gry jako paradygmat systemu działania.

1.4. Wybrane kryteria oceny zagrożenia elektronicznego mobilnego systemu łączności związku operacyjnego wojsk lądowych

Ważnym przedsięwzięciem, pojawiających się podczas projektowania symulacyjnych modeli walki, jest opracowanie merytoryczne poprawnych i praktycznie użytecznych *kryteriów*[12]*oceny* modelowanych działań bojowych. Zagadnienie to nabiera szczególnego znaczenia właśnie w komputerowych grach wojennych, bowiem wykorzystywane w nich modele mają przede wszystkim charakter ocenowy. Oznacza to, że kryteria oceny modelowanego systemu stanowić powinny ich integralny element. Jako naczelne kryterium oceny modelowanych działań bojowych przyjmuje się najczęściej ***efektywność***[13], rozumianą bardzo szeroko i obejmującą np. efekty organizacyjne, efekty informacyjne i wiele innych rezultatów realizacji działań i spełnianych funkcji. Punktem wyjścia do rozpoczęcia prac nad formułowaniem kryteriów efektywności modelowanych działań bojowych jest szczegółowa i wszechstronna analiza celów funkcjonowania modelowanego zagrożenia elektronicznego MSŁ ZO WL oraz celów dotyczących KGW. W wyniku tej analizy rozstrzygnąć należy następujące zagadnienia:

– jakiego rodzaju cele mają być uwzględnione w modelu symulacyjnym zagrożenia elektronicznego MSŁ ZO WL (kwantyfikowalne, mierzalne, złożone, wielorakie, stopniowalne itp.);

– jaki jest charakter związków występujących między celami modelowanych działań bojowych (zależność, niezgodność itp.);

– w jakiej formie wyrażone zostaną cele modelowanych działań bojowych;

– jaki należy wziąć pod uwagę zespół warunków ograniczających swobodę wyboru stosownych decyzji uczestników KGW.

Przy konkretyzacji empirycznej tych zagadnień należy uwzględnić w jakim stopniu fragment rzeczywistego zagrożenia elektronicznego MSŁ ZO WL od-

[12] Z formalnego punktu widzenia kryterium jest to funkcja przyporządkowująca poszczególnym stopniom realizacji celu liczby rzeczywiste, tworzące skalę z określoną jednostką miary.

[13] Przez ***kryterium efektywności*** modelowanego zagrożenia elektronicznego MSŁ ZO WL rozumieć należy wskaźnik liczbowy, po wartości którego sądzić można o stopniu realizacji celu modelowanych funkcji i wykonywanych zadań.

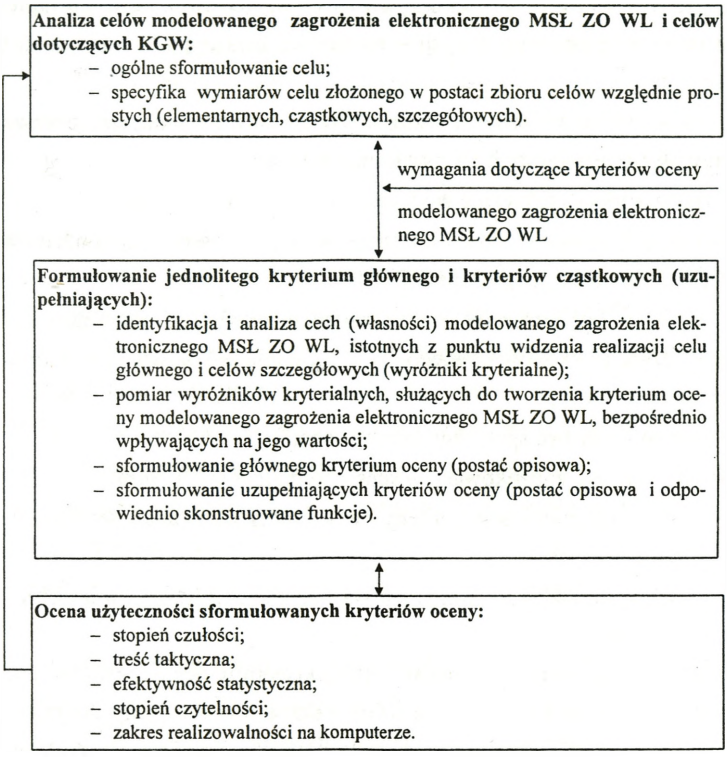
wzorowany zostanie w modelu symulacyjnym. Systemy WE przeciwnika oraz MSŁ ZO WL należą do tej klasy systemów działania, które charakteryzują się wielością i różnorodnością celów. Oznacza to, że ocena efektywności ich funkcjonowania powinna przebiegać w wielu płaszczyznach, tzn. na podstawie *wielu kryteriów*. Ze względu na dużą złożoność tych systemów oraz zróżnicowane pole recepcji poszczególnych funkcji – kryteriów mierzących w istocie realizację odrębnych celów modelowanego systemu, a co za tym idzie – nierzadko sprzeczne kierunki dokonywanych wyborów, trudno jest sformułować (często bywa to praktycznie niemożliwe) *globalne kryterium efektywności,* obejmujące wszystkie z ocenianych problemów funkcjonowania systemu. Zaznaczyć przy tym należy, że trudności sprawia głównie opracowanie merytorycznie i formalnie poprawnej takiej globalnej funkcji kryterium, która zapewniałaby wzajemną zgodność ekstremalnych wartości rozpatrywanych poszczególnych funkcji kryteriów. Z tych względów ocena efektywności funkcjonowania modelowanego zagrożenia elektronicznego MSŁ ZO WL dokonywana może być przy pomocy wielu *kryteriów cząstkowych*, zwanych także uzupełniającymi, których postać funkcyjna jest znacznie prostsza niż jednolitego kryterium głównego. Podkreślić jednak należy, że uwzględnienie w modelu zagrożenia elektronicznego MSŁ ZO WL więcej niż jednej funkcji kryterium, nie zawsze prowadzi do rozwiązania najlepszego tj. takiego, które zapewniałoby *optimum* ze względu na wszystkie kryteria jednocześnie.

Kryterium główne związane powinno być z oceną stopnia realizacji celu głównego. Kryteria cząstkowe powinny uzupełniać i w pewnym sensie wyjaśniać, a w razie potrzeby uzupełniać kryterium główne, odnosząc się do wybranych obszarów funkcjonowania modelowanego zagrożenia elektronicznego MSŁ ZO WL. Przykładowy zbiór możliwych kryteriów uzupełniających i odpowiadającego im kryterium głównego oceny efektywności modelowanego zagrożenia elektronicznego MSŁ ZO WL przedstawiono w tabeli 1.4.1.

Mając na względzie założenie o skończoności zbioru celów modelowanego zagrożenia elektronicznego MSŁ ZO WL, a także o ich kwantyfikalności i mierzalności procedura formułowania kryteriów jego oceny powinna obejmować problemy przedstawione na rys. 1.4.1.

Tabela 1.4.1. Zbiór cząstkowych (uzupełniających) kryteriów efektywności modelowanego zagrożenia elektronicznego MSŁ ZO WL (wariant)

Lp.	Podstawowe przedsięwzięcia (obszary funkcjonowania modelowanego zagrożenia elektronicznego MSŁ ZO WL) wymagające oceny	Kryteria cząstkowe (uzupełniające)
KRYTERIUM GŁÓWNE: Stopień zagrożenia elektronicznego MSŁ ZO WL w zadanym czasie		
1	Określenie możliwości bojowych sił i środków WE przeciwnika	– całkowity potencjał bojowy wojsk WE przeciwnika, – możliwości taktyczno-bojowe sił i środków WE przeciwnika.
2	Określenie możliwości bojowych sił i środków własnych wojsk łączności	– całkowity potencjał bojowy wojsk łączności. – możliwości taktyczno-bojowe sił i środków łączności wojsk własnych.
3	Ocena funkcjonowania MSŁ ZO WL w warunkach oddziaływania elektronicznego przeciwnika	– czas realizacji cyklu (poszczególnych etapów, faz) dowodzenia; – prawdopodobieństwo realizacji cyklu w określonym czasie; – prawdopodobieństwo przekazania w zadanym czasie komend, rozkazów, zarządzeń, meldunków, przy określonej stopie błędów, – czas pracy i nie pracy poszczególnych relacji łączności.
4	Zestawienie wskaźników oddziaływania elektronicznego środków WE na MSŁ ZO WL	– liczba wykryć, namierzeń zakłóceń poszczególnych relacji łączności tzw. *pomyślnych oraz nie pomyślnych według kryterium ilościowego (ze względu na posiadany przez przeciwnika potencjał WE),* – liczba wykryć, namierzeń zakłóceń poszczególnych relacji łączności tzw. *pomyślnych oraz nie pomyślnych według kryterium energetycznego,* – liczba wykryć, namierzeń zakłóceń poszczególnych relacji łączności tzw. *pomyślnych oraz nie pomyślnych według kryterium czasowego,* – liczba oraz zajętość środków WE przeciwnika, – czasy pracy i nie pracy poszczególnych środków WE przeciwnika, – efektywny czas pracy poszczególnych środków WE przeciwnika.



Rys. 1.4.1. Procedura formułowania kryteriów oceny modelowanego zagrożenia elektronicznego MSŁ ZO WL

Sformułowane kryteria oceny – zarówno główne, jak i cząstkowe – aby miały charakter użytkowy, powinny spełniać następujące wymagania:

– nie powinno być ich zbyt wiele;

– powinny uwzględniać istotne cechy modelowanego zagrożenia elektronicznego MSŁ ZO WL i jego otoczenia;

– powinny rzeczywiście wyrażać stan modelowanego zagrożenia elektronicznego MSŁ ZO WL, a w szczególności obiektywnie charakteryzować realizowane zadania bojowe odpowiednio do celu walki;

– powinny krytycznie reagować (być czułe) na zmiany podstawowych parametrów modelowanego zagrożenia elektronicznego MSŁ ZO WL i jego oto-

czenia (np. umożliwiać ocenę wpływu określonych czynników – uwzględnianych przy podejmowaniu decyzji – na stopień osiągnięcia celu działań bojowych;

– powinny być czytelne w sensie taktyczno-operacyjnym, tzn. sformułowane przy użyciu terminologii taktyczno-operacyjnej;

– powinny być efektywne w sensie statystycznym;

– powinny nadawać się do konstruowania globalnej oceny modelowanego zagrożenia elektronicznego MSŁ ZO WL;

– powinny być zrelatywizowane względem przyjętego otoczenia i systemu wartości czasu (wykorzystywanego np. w działaniach bojowych), w którym dokonywana jest ocena;

– nie powinny być sprzeczne między sobą;

– powinny być zunifikowane w sensie formalnego ich opisu;

– kryteria uzupełniające powinny być podporządkowane i wynikać niejako z kryteriów głównych;

– powinny umożliwiać komputerową realizację obliczeń związanych z ich wykorzystaniem.

Spełniający powyższe wymagania zbiór kryteriów oceny powinien być wykorzystywany przez kierownictwo KGW i ekspertów do oceny decyzji podejmowanych przez uczestników gry oraz do oceny funkcjonowania modelowanego zagrożenia elektronicznego MSŁ ZO WL. Zakres i sposób wykorzystania kryteriów oceny zależy w każdym przypadku od przyjętego regulaminu gry. W wielu KGW kryteria oceny wykorzystywane są także bezpośrednio przez uczestników gry do oceny trafności podejmowanych przez siebie decyzji.

Kalkulacje i obliczenia, związane z wykorzystywaniem kryteriów oceny w różnych fazach KGW, stanowiące integralny element regulaminu gry, powinny być wykonywane tradycyjnie lub komputerowo, w oparciu o określone procedury programowe. Zaznaczyć jednak należy, że zakres komputerowej realizacji kryteriów oceny modelowanego zagrożenia elektronicznego MSŁ ZO WL, w większości komputerowych gier wojennych jest znacznie ograniczony.

Pierwszą przyczyną tego jest potrzeba pozostawienia kierownictwu i ekspertom gry znacznej swobody doboru zestawu kryteriów oceny, adekwat-

nych do celu KGW oraz odpowiadających charakterowi i treści symulacyjnego modelu działań bojowych. Rozwiązanie takie, jak wykazują doświadczenia, znacznie zwiększa efektywność gry. Druga przyczyna związana jest z trudnościami w algorytmizacji i programowaniu procedur wykorzystania sformułowanych kryteriów oceny. Wynikają one głównie z konieczności przechowywania niezbędnych do tego celu dużych zbiorów informacji o zjawiskach i elementach systemu oraz ich charakterystycznych cechach, które nie zawsze są wykorzystywane w symulacyjnym modelu działań bojowych, a często także nie należą do zbioru parametrów opisujących podejmowane przez uczestników gry decyzje.

Ważną funkcję powinny spełniać także, oprócz kryteriów oceny modelowanych działań bojowych różnego rodzaju *normatywy* w sprawnym przebiegu KGW. Powinny być one interpretowane jako *krytyczne* lub *graniczne wartości parametrów* opisujących stany modelowanego zagrożenia elektronicznego MSŁ ZO WL lub jego poszczególnych elementów. Wykorzystywane w KGW normatywy powinny obejmować przede wszystkim:

– poziom strat ponoszonych przez mobilne pododdziały i oddziały łączności WL;

– wielkości czasów niezbędnych do podjęcia stosownej decyzji – związanej z zaistniałą krytyczną sytuacją na polu walki;

– wielkości czasów przebywania elementarnych pododdziałów w tzw. stanach technologicznych (np. rozwijanie i zwijanie sprzętu, czas odtwarzania gotowości bojowej, itp.);

– intensywność realizacji poszczególnych rodzajów działań bojowych,

– maksymalne prędkości przegrupowania dla poszczególnych rodzajów pododdziałów i ugrupowania marszowego;

– inne.

Wartości większości z wymienionych normatywów powinny być obliczane na podstawie analiz minionych i współczesnych konfliktów zbrojnych oraz prowadzonych ćwiczeń, eksperymentów i badań poligonowych, a także w oparciu o wyniki modelowania matematycznego i symulacyjnego. Podkreślić jednak należy, że prowadzenie ćwiczeń w celu określenia wartości wspomnia-

nych normatywów jest nie tylko drogie i pracochłonne, ale bardzo często samo w sobie stanowi złożony problem badawczy.

Ważną rolę powinny spełniać w komputerowych grach wojennych wszystkie z wymienionych normatywów. Rolę szczególną do spełnienia mają jednak normatywy określające poziom załamania poszczególnych rodzajów działań bojowych, czy też – jak się to często określa – *strat krytycznych*. Wykorzystanie ich, przy poprawnym oszacowaniu wartości, powinno umożliwiać odtworzenie złożoności rzeczywistego pola walki poprzez odwzorowanie krytycznych stanów (sytuacji) modelowanych działań bojowych, związanych z stratami ponoszonymi przez symulowane pododdziały, co w konsekwencji powinno stwarzać warunki „stawiające" uczestników gry w złożonych sytuacjach taktyczno-operacyjnych i zmuszania ich do podejmowania decyzji trudnych, adekwatnych do zaistniałej sytuacji.

Możliwości wykorzystania normatywów powinno pozwalać także, niezależnie od subiektywnych wyobrażeń uczestników gry o przebiegu modelowanych działań bojowych, nadawać komputerowej grze wojennej charakter bardziej dynamiczny, a co z tym związane – czynić ją bardziej atrakcyjną, zarówno w sensie treści, jak i sposobu jej przebiegu.

2. MODEL MATEMATYCZNY ZAGROŻENIA ELEKTRONICZNEGO MOBILNEGO SYSTEMU ŁĄCZNOŚCI ZWIĄZKU OPERACYJNEGO WOJSK LĄDOWYCH

2.1. Wprowadzenie

Podczas oceny zagrożenia elektronicznego MSŁ ZO WL istotną rolę odgrywają modele matematyczne zjawisk zachodzących w tym procesie. Uwzględniając możliwości zastosowania symulacji komputerowej do modelowania procesów walki zbrojnej[14] w rozdziale tym został przedstawiony model matematyczny zagrożenia elektronicznego mobilnego systemu łączności związku operacyjnego wojsk lądowych, który obejmuje następujące moduły:

– submodel matematyczny mobilnego systemu łączności związku operacyjnego wojsk lądowych;

– submodel matematyczny oddziaływania elektronicznego na niego środków WE potencjalnego przeciwnika.

2.2. Submodel matematyczny mobilnego systemu łączności ZO WL

Duża złożoność mobilnego systemu łączności ZO WL stwarza określone trudności w opracowaniu dla niego uniwersalnego modelu matematycznego. Według dostępnej literatury przedmiotu [2, 7, 15] każdy model opisuje rzeczywistość w pewnym uproszczeniu, względnie tylko ujmuje się pewne zjawiska (ważniejsze) oddziałujące na system. Zatem tak rozumiany model można potraktować jako pewien zbiór informacji o systemie łączności, zebranych np. w celu dokonania analizy i oceny jego funkcjonowania.

Analiza zadań, istoty i właściwości MSŁ ZO WL, jak również zasad i warunków jego funkcjonowania wskazuje, że może on być rozpatrywany jako zbiór urządzeń technicznych wraz z ich właściwościami, tworzącymi fizyczną strukturę sieci łączności między elementami, w których zachodzą określone relacje wynikające z przyjętych zasad funkcjonowania systemu. Uwzględniając

[14] Zawarte w poprzednim rozdziale.

ponadto relacje, jakie zachodzą między systemem łączności a jego otoczeniem, ogólny model mobilnego systemu łączności może być przedstawiony [5], [6], w postaci:

$$\mathbf{M_{SŁ}} = \langle \mathbf{S, O, W} \rangle \tag{2.2.1}$$

gdzie:

$\mathbf{M_{SŁ}}$ – model systemu łączności;

S – model sieci łączności;

O – model otoczenia;

W – model funkcjonowania.

Tak więc dla odwzorowania mobilnego systemu łączności ZO WL uwzględnia się znajomość struktury i parametrów sieci łączności (modelu otoczenia), algorytmów funkcjonowania systemu oraz współzależności zachodzących pomiędzy jego elementami.

Model sieci łączności można opisać w postaci:

$$\mathbf{S} = \langle \mathbf{G, F, f} \rangle \tag{2.2.2}$$

gdzie:

G – graf opisujący liczbę i sposób połączeń między sobą węzłów łączności:

$\mathbf{G} = \langle \mathbf{Q, U} \rangle = \left\{ q_i ; \quad \mathbf{i} = \overline{\mathbf{1, n}} \right\}$ – zbiór wierzchołków grafu (węzłów łączności);

$\mathbf{U} \subset \mathbf{Q} \times \mathbf{Q}$ – zbiór łuków grafu (linii łączności).

F i f określają stałe i zmienne parametry sieci i dotyczą odpowiednio węzłów łączności i rozwiniętych między nimi linii. W modelu odnoszą się do takich charakterystyk jak przepustowość linii i węzłów, liczebność kanałów w relacji, ilość relacji, prawdopodobieństwo zakłóceń kanału, relacji lub węzła łączności itp.

W danej chwili czasu t stan sieci łączności $s\tau_s \in \mathbf{S_s}^t$ określany jest przez chwilowe stany wszystkich jej elementów. Zmiany stanu sieci wynikają z warunków normalnego funkcjonowania systemu łączności (np. zajmowanie czy zwalnianie kanałów), z destrukcyjnego oddziaływania otoczenia (np. zakłócenia linii, relacji, węzła łączności) i z przyjętych zasad eksploatacji (np. okre-

sowe zmiany pojemności linii telekomunikacyjnych związanych przede wszystkim z intensywnością ruchu).

Model otoczenia stanowi zbiór czynników zewnętrznych (np. środków WE przeciwnika) oddziałujących na pracę systemu łączności. Można zapisać go przy pomocy zależności:

$$\mathbf{O} = \left\{\mathbf{O_i} : \mathbf{i} = \overline{\mathbf{1, x}}\right\} = \mathbf{O'} \cap \mathbf{O''} \qquad (2.2.3)$$

– przy czym $\mathbf{O'} \cap \mathbf{O''} = \Phi$

Zbiór powyższy składa się z dwóch rozłącznych podzbiorów. Elementy podzbioru **O'** stanowią procesy stochastyczne reprezentujące wejściowe strumienie zgłoszeń wraz ze wszystkimi jego parametrami (źródło, numer i ilość kanałów, ujście, priorytet itp.).

Podzbiór **O''** stanowią elementy procesów stochastycznych, reprezentujących czynniki zakłócające normalną pracę systemu (zakłócenia celowe teletransmisyjnych linii bezprzewodowych); niszczenie (porażenie ogniowe) węzłów, linii i kanałów, uszkodzenia (awarie sprzętu), błędy w eksploatacji i in. wraz z ich charakterystykami (rodzaj, czas, zakres, sposób oddziaływania).

W dowolnej chwili czasu t otoczenie systemu będzie znajdować się w stanie $s^t_0 \in S^t_0$. Stan ten jest chwilową realizacją procesów stochastycznych występujących w opisie otoczenia. Zmiany stanu otoczenia wynikają przede wszystkim z charakteru procesów zachodzących w otoczeniu związanym z pojawieniem się i zwiększeniem zapotrzebowań na realizację określonych usług, pojawieniem się i zanikaniem zakłóceń i uszkodzeń w kanałach.

Model funkcjonowania systemu łączności uzależniony jest od zadań realizowanych przez mobilny system łączności ZO WL. Wszelkie zadania realizowane przez system łączności są najczęściej rozpatrywane jako potrzeba przekazania określonego rodzaju informacji o określonej kategorii ważności (priorytetu usługi). Są one realizowane w systemie przy wykorzystaniu określonych reguł sterowania rozdziałem strumieni wiadomości, uwzględniających stan jego poszczególnych elementów, jak również zakres, stopień pilności (priorytet) i aktualnych potrzeb informacyjnych użytkowników. Funkcjonowanie systemu jest związane z realizacją określonych działań A w ramach przyjętych reguł ste-

rowania P, obejmujących badanie i zmianę stanu elementów systemu R, analizę parametrów chwilowych charakterystyk działań Φ^t.

Zatem model funkcjonowania systemu łączności można przedstawić w postaci następującej zależności:

$$\mathbf{W} = \left\langle \mathbf{A}, \mathbf{P}, \mathbf{R}, \phi^t = t \in \mathbf{T} \right\rangle \tag{2.2.4}$$

gdzie:

T – zbiór chwil czasu działania systemu.

Wykorzystując sformalizowany język, zwany schematem logicznym algorytmu [6], funkcjonowanie mobilnego systemu łączności związku operacyjnego WL można odwzorować w postaci układu formuł przejścia typu:

$$\mathbf{A}_j \rightarrow \mathbf{B}_j \tag{2.2.5}$$

Stosując zasady przekształceń tożsamościowych można przejść do schematu logicznego algorytmu funkcjonowania systemu łączności. Schemat ten odwzorowuje warunki oraz kolejność wykonywania działań od chwili pojawienia się np. zapotrzebowania na wymianę informacji, aż do chwili zaspokojenia potrzeb informacyjnych użytkowników systemu łączności.

Przedstawiony ogólny model systemu łączności ujmuje parametry strukturalne i funkcjonalne mobilnego systemu łączności ZO WL oraz ich reakcje z otoczeniem[15]. Zastosowany aparat formalny umożliwia odtworzenie działania mobilnego systemu łączności ZO WL przy pomocy symulacji komputerowej. Przydatny jest zwłaszcza w przypadkach, gdy celem prowadzonych badań jest ocena aktualnych i proponowanych rozwiązań systemów łączności z punktu widzenia zaspokojenia potrzeb informacyjnych użytkownikom systemów w określonym czasie i z odpowiednim priorytetem, przy uwzględnieniu destrukcyjnego oddziaływania otoczenia, np. oddziaływania radioelektronicznego przeciwnika. Pozwala on również na prowadzenie badań poszczególnych wariantów systemu łączności, np. w celu określenia wpływu zmian zachodzących w strukturze sieci, w algorytmie funkcjonowania czy w otoczeniu systemu na

[15] Szczegółowy opis sieci łączności MSŁ ZO WL znajduje się w dokumentach normatywnych Zarządu Wojsk Łączności i Informatyki Szt. Gen. WP.

skuteczność realizacji zadań stawianych przed danymi systemami łączności przez odpowiednie systemy dowodzenia. Powyższy model matematyczny systemu łączności można wykorzystać do budowy modelu symulacyjnego zagrożenia elektronicznego mobilnego systemu łączności ZO WL.

2.3. Submodel matematyczny oddziaływania elektronicznego środków WE przeciwnika na mobilny system łączności ZO WL

Budowa modelu symulacyjnego zagrożenia elektronicznego mobilnego systemu łączności związku operacyjnego wojsk lądowych powinna być poprzedzona parametryzacją oddziaływania na niego otoczenia, tj. środków WE przeciwnika. Jak wiadomo, wynika ono z ogólnych możliwości taktyczno-bojowych sił i środków rozpoznania elektronicznego i WE potencjalnego przeciwnika. W tym celu należy wykorzystać odpowiednie narzędzia, tj. model matematyczny. Analiza dostępnej literatury [8, 11] pozwala postawić tezę, że submodel matematyczny oddziaływania elektronicznego sił i środków WE przeciwnika na MSŁ ZO WL należy opracować z uwzględnieniem: *intensywności oddziaływania elektronicznego, dostępności elektromagnetycznej oraz dostępności czasowej* w odniesieniu do określonych jego parametrów systemu.

2.3.1. Intensywność oddziaływania elektronicznego środków WE przeciwnika na mobilny system łączności ZO WL

Do budowy submodelu matematycznego intensywności oddziaływania elektronicznego środków WE przeciwnika na mobilny system łączności związku operacyjnego wojsk lądowych można wykorzystać *metodę ilościową*, która polega na:

1. Ocenie realnej bazy materialnej sił i środków rozpoznania i WE przyjętych do badań oraz wyspecyfikowaniu jej możliwości[16] np.: w zakresie wykrywania [M_w], namierzania [M_n] oraz obezwładnienia zakłóceniami [M_z]. W ocenie tej należy uwzględnić wszystkie siły i środki rozpoznania i WE potencjalnego przeciwnika mogące oddziaływać elektronicznie na MSŁ ZO WL,

[16] Przedstawionej w specjalistycznej literaturze przedmiotu, np. [8].

tj. określoną część tych sił szczebla nadrzędnego, siły i środki szczebla równorzędnego oraz szczebli podległych.

2. Porównaniu możliwości ww. bazy w poszczególnych rodzajach zagrożenia z ilością[17] bezprzewodowych linii łączności przy uwzględnieniu relacji łączności różnych zakresów częstotliwości, np. KF [I_{KF}], UKF [I_{UKF}], Rln [I_{RLN}] organizowanych w ocenianym mobilnym systemie łączności,

3. Określeniu prawdopodobieństwa zagrożenia elektronicznego bezprzewodowych linii łączności z podziałem na różne zakresy częstotliwości z zakresie:

– wykrywania [P(w)] z jednej z zależności:

$$P(w_{KF}) = \frac{Mw_{KF}}{I_{KF}};\quad P(w_{UKF}) = \frac{Mw_{UKF}}{I_{UKF}};\quad P(w_{RLN}) = \frac{Mw_{RLN}}{I_{RLN}}; \quad (2.3.1.1)$$

– namierzania [P(n)] z jednej z zależności:

$$P(n_{KF}) = \frac{Mn_{KF}}{I_{KF}};\quad P(n_{UKF}) = \frac{Mn_{UKF}}{I_{UKF}}; \quad (2.3.1.2)$$

– obezwładnienia zakłóceniami [P(z)] z jednej z zależności:

$$P(z_{KF}) = \frac{Mz_{KF}}{I_{KF}};\quad P(z_{UKF}) = \frac{Mz_{UKF}}{I_{UKF}};\quad P(z_{RLN}) = \frac{Mz_{RLN}}{I_{RLN}}; \quad (2.3.1.3)$$

Wykorzystując matematyczne metody analityczne określa się prawdopodobieństwo oddziaływania elektronicznego w odniesieniu do bezprzewodowych linii łączności, które mogą być wykryte, namierzone oraz obezwładnione zakłóceniami w określonym czasie. Przy tym terytorialny zasięg zagrożenia elektronicznego określa się na podstawie instrukcyjnych wielkości.[18]

---

[17] Dane te zawarte są normatywach łączności oraz w specjalistycznej literaturze przedmiotu, np. [10, 12, 17].

[18] 1. Głębokość rozpoznania elektronicznego (wykrywania i namierzania) przyjmuje się:

– dla linii łączności KF na falach przestrzennych: 600-2000 km i więcej, a na falach przyziemnych 50-120 km w zależności od pory doby,

– dla linii łączności UKF: na głębokość do 50 km.

Powyższe wielkości mogą ulec znacznemu zwiększeniu w wyniku prowadzenia rozpoznania elektronicznego przy pomocy urządzeń instalowanych na samolotach (śmigłowcach), tzn. ponad 2000 km dla linii radiowych KF oraz do 500 km dla linii radiowych UKF.

2. Głębokość skutecznych zakłóceń radiowych przyjmuje się:

– dla naziemnych stacji zakłóceń 50-80 km w zakresie KF na falach przyziemnych oraz do 30 km w zakresie fal UKF,

– dla stacji zakłóceń instalowanych w samolotach (śmigłowcach) 200-400 km w zakresie KF na falach przyziemnych i 50-200 km w zakresie fal UKF.

W przedstawionej metodzie ilościowej przyjmuje się za podstawę oceny zagrożenia elektronicznego mobilnego systemu łączności związku operacyjnego wojsk lądowych potencjał środków rozpoznania i zakłóceń radiowych, który może być użyty do dezorganizacji pracy bezprzewodowych linii łączności, co w konsekwencji pozwala określić wielkość zagrożenia elektronicznego jedynie szacunkowo. Stąd też metoda ta obarczona jest pewnymi błędami, a mianowicie:

– upraszcza się problem skuteczności oddziaływania elektronicznego, zakładając jedynie ich wartości instrukcyjne,

– nie uwzględnia się dużych możliwości dokonywania manewru środkami rozpoznania i WE oraz uwarunkowań dynamicznych ocenianego systemu łączności, a w tym – szczególnie zróżnicowanej intensywności ruchu.

Przedstawiony submodel umożliwia bowiem określenie intensywności oddziaływania elektronicznego na planowany mobilny system łączności WL. Wyraża się ją w formie prawdopodobieństwa dezorganizacji poszczególnych bezprzewodowych linii łączności w przedziale (0 ÷ 1) lub procentowo (0 ÷ 100%), a więc w sposób sugestywny, a zarazem komunikatywny dla pozostałych komórek organizacyjnych sztabu danego szczebla dowodzenia.

Intensywność oddziaływania elektronicznego – zawężając problem jedynie do zakłócania elektronicznego – można wyrazić również w postaci:

– średniego czasu odstępu między zakłóceniami ($\bar{t}_{omz}$), który może być równy lub nieznacznie większy od średnich czasów odstępów między wiadomościami (danymi) przekazywanymi w MSŁ WL ($\bar{t}_{ompi}$) i wyraża się zależnością:

$$\bar{t}_{omz} \geq \bar{t}_{ompi} \qquad (2.3.1.4)$$

– liczby stacji zakłóceń wykorzystywanych na danym kierunku zagrożenia:

$$I_{sz} = 1...n \qquad (2.3.1.5)$$

Zaprezentowany submodel stanowi *podstawę do budowy modelu symulacyjnego* w części dotyczącej intensywności oddziaływania elektronicznego środków WE przeciwnika na system łączności MSŁ WL.

2.3.2. Dostępność elektromagnetyczna mobilnego systemu łączności ZO WL dla środków walki elektronicznej przeciwnika

Analityczne metody matematyczne stanowią podstawę prowadzenia badań oceny zagrożenia elektronicznego według kryterium energetycznego. Umożliwiają określenie dostępności elektromagnetycznej, a zatem – głębokości rozpoznania elektronicznego poszczególnych bezprzewodowych linii łączności MSŁ ZO WL dla środków rozpoznania i WE przeciwnika oraz skuteczności ich zakłóceń.

Dostępność elektromagnetyczna poszczególnych bezprzewodowych linii łączności MSŁ ZO WL dla środków rozpoznania elektronicznego potencjalnego przeciwnika uzależniona jest od ich przestrzennego rozmieszczenia w obszarze funkcjonowania ZO, ZT i oddziałów WL. Z analizy tego obszaru funkcjonowania wynika, że większość linii łączności organizowanych przy pomocy środków radiowych KF, UKF, radiotelefonicznych oraz radioliniowych są dostępne elektromagnetycznie dla środków rozpoznania elektronicznego potencjalnego przeciwnika rozwiniętego w tym obszarze.

Głębokość rozpoznania w zakresie fal przyziemnych uwarunkowana jest *horyzontem radiowym*, który dla częstotliwości poniżej 30 MHz (wykorzystywanych w środkach radiowych KF) określa się z zależności:

$$d_r = \frac{80}{\sqrt[3]{f}} \qquad (2.3.2.1)$$

gdzie:

d_r – horyzont radiowy [km],

f – częstotliwość [MHz].

Przykładowe wielkości liczbowe horyzontu radiowego dla pasma 1-30 MHz zamieszczono w tabeli 2.3.2.1.

Tabela 2.3.2.1. Horyzont radiowy dla pasma 1-30 MHz

f [MHz]	1	5	10	15	20	25	30
d_r [km]	80	46	37	32	29	27	25

Przy częstotliwościach powyżej 30 MHz (wykorzystywanych w środkach radiowych UKF oraz w stacjach radioliniowych zakresu megahercowego) horyzont radiowy oblicza się z zależności [15]:

$$d_r = 4{,}12\left(\sqrt{h_n} + \sqrt{h_o}\right) \qquad (2.3.2.2)$$

gdzie:

h_n – wysokość anteny nadawczej [m],

h_o – wysokość anteny odbiorczej [m].

Przykładowe wielkości liczbowe horyzontu radiowego [d_r] pasma powyżej 30 MHz zamieszczono w tabeli 2.3.2.2.

Tabela 2.3.2.2. Horyzont radiowy dla pasma powyżej 30 MHz

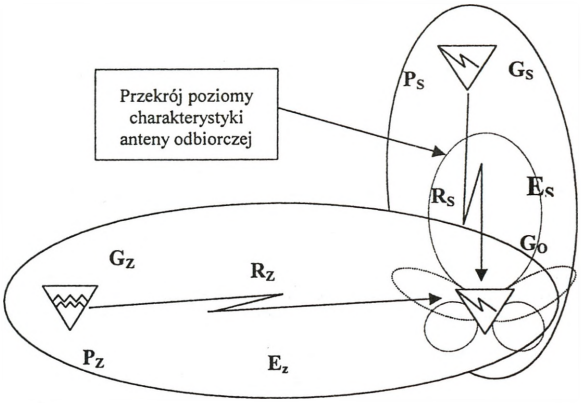
h_n [m]	4	4	4	4	4	4	4	4
h_o [m]	4	7	10	16	28	31	37	40
d_r [km]	16	19	21	25	30	31	33	34

Przy częstotliwościach powyżej 1 GHz (wykorzystywanych w stacjach radioliniowych zakresu gigahercowego), gdzie występuje zjawisko refrakcji oblicza się horyzont optyczny {**d**}z zależności [15]:

$$d_r = 3{,}57\left(\sqrt{h_n} + \sqrt{h_o}\right) \qquad (2.3.2.3)$$

Analiza zależności 2.3.2.1 (zakres KF) pozwala sądzić, że wykorzystywane na tym szczeblu środki radiowe KF będą znajdować się w strefie dostępności elektromagnetycznej dla rozpoznania elektronicznego przeciwnika bez względu na miejsce w ugrupowaniu operacyjnym ZO WL. Środki wykorzystujące częstotliwości powyżej 30 MHz będą również podlegać skutecznemu rozpoznaniu elektronicznemu. Na podstawie zależności (2.3.2.2) można wnioskować, że ww. środki odwodu ZO, które mogą być poza zasięgiem radiowym, będą poza strefą dostępności elektromagnetycznej dla naziemnych urządzeń rozpoznania elektronicznego przeciwnika.

Dla określenia *zagrożenia elektronicznego w zakresie obezwładnienia zakłóceniami* MSŁ ZO WL można wykorzystać analityczne metody matematyczne, które sprowadzają się do oceny skuteczności zakłóceń konkretnych bezprzewodowych linii łączności organizowanych w tym systemie. *Skuteczność zakłóceń* łączności radiowej, realizowanych w zakresie ultrakrótkofalowym i krótkofalowym na fali przyziemnej, zależy od czynników przedstawionych na rysunku 2.3.2.1.



Rys. 2.3.2.1. Schemat oceny skuteczności zakłóceń radiowych

Wszystkie wymienione czynniki decydujące o skuteczności obezwładniania zakłóceniami są z sobą ściśle współzależne. Podczas oceny skuteczności obezwładniania zakłóceniami należy wziąć pod uwagę, że urządzenie odbiorcze może być zakłócone przy odpowiednim poziomie sygnału zakłócającego w stosunku do sygnału użytecznego w miejscu jego rozwinięcia. Stosunek ten przyjęto nazywać współczynnikiem zakłóceń.

Współczynnik zakłóceń (K_z) jest wyrażany stosunkiem natężenia pola elektrycznego, pochodzącego ze stacji zakłócającej (E_z) do natężenia pola elektrycznego, pochodzącego z nadajnika pracującej radiostacji (E_s), mierzony na wejściu antenowym zakłócanego odbiornika.

W teorii zakłócania elektronicznego wyróżnia się dwa rodzaje współczynników zakłóceń: *według napięcia* (natężenia pola elektrycznego) i *według mocy*

sygnału zakłócającego oraz użytecznego, które można przedstawić w postaci zależności:

$$Kz^E = \frac{Ez}{Es} \quad \text{lub} \quad Kz^P = \frac{Pz}{Ps} \tag{2.3.2.4}$$

Zakłada się, że obezwładnienie zakłóceniami jest skuteczne, gdy spełniona jest nierówność:

$$E_z \rangle K^E_{Z_w} \quad \text{lub} \quad P_z \rangle P^E_{Z_w} \tag{2.3.2.5}$$

gdzie:

Kz_W – wymagany współczynnik zakłóceń, którego wartość jest wyznaczana doświadczalnie i zależy od rodzaju sprzętu, jego parametrów technicznych a przede wszystkim – rodzaju sygnału (emisji) bezpośrednio związanego z rodzajem pracy.

Wartości wymaganych współczynników zakłóceń (Kz_w) dla konwencjonalnego odbiornika superheterodynowego przedstawiono w tabeli 2.3.2.3. Na wyznaczenie współczynników zakłóceń oczekują takie emisje, jak: rozproszone (emisje szumopodobne), cyfrowe, modulowane fazowo oraz inne, pojawiające się w środowisku elektromagnetycznym.

Tabela 2.3.2.3. Wartość wymaganego współczynnika zakłóceń (Kz_w)

Lp.	Rodzaj emisji	Wymagana wartość współczynnika zakłóceń	
		wg natężenia pola (Kz^E_W)	wg mocy (Kz^P_W)
1	Manipulacja amplitudy	0,8	0,64
2	Manipulacja częstotliwości	1 - 1,1	1 - 1,21
3	Modulacja amplitudy	1,5 - 2	2,25 - 4
4	Modulacja jednowstęgowa	4 - 5	16 - 25
5	Modulacja częstotliwości	1,5	2,25
6	Modulacja FH[19]	5	25

[19] Wartości dla emisji FH przyjęto na podstawie analizy materiałów źródłowych [8, 13].

Dla określenia *zagrożenia elektronicznego w zakresie obezwładnienia zakłóceniami* MSŁ ZO WL należy zatem wyznaczyć rzeczywiste wartości współczynników zakłóceń (Kz_{rz}) charakteryzujące poszczególne bezprzewodowe linie łączności i porównać je z wartościami wymaganymi (Kz_w). W tym celu należy uwzględnić następujące czynniki:

– moc nadajnika stacji zakłócającej wykorzystywanej do obezwładnienia zakłóceniami łączności radiowej przeciwnika (Pz),

– moc radiostacji korespondenta przekazującej informacje w zorganizowanych relacjach łączności (Ps),

– odległość między nadajnikiem a odbiornikiem w zakłócanych relacjach łączności (Rs),

– odległość między urządzeniem odbiorczym (zakłócanym) a stacją (nadajnikiem) zakłócającym (Rz),

– współczynnik zysku kierunkowości anteny radiostacji (Gs) i stacji zakłócającej (Gz),

– wymagany współczynnik zakłóceń określany dla danego rodzaju pracy i typu środka łączności (Kz_w),

– współczynnik tłumienności anteny odbiornika z kierunku na stację zakłócającą (Go).

Podczas ocen bardziej szczegółowych należy również uwzględnić warunki rozprzestrzeniania się fal elektromagnetycznych – przyziemnych i przestrzennych. Na te warunki może mieć wpływ wiele czynników, jak: pokrycie terenu, wilgotność gleby, jonizacja powietrza (zwłaszcza po wybuchach jądrowych) i in.

Ocenę skuteczności zakłóceń łączności KF na falach przyziemnych, łączności UKF wojsk lądowych oraz łączności radiotelefonicznej (radiowej radiokomunikacji ruchomej) można przeprowadzić po odpowiednim przekształceniu zależności (2.3.2.4), rozwiązując następujące typy zadań:

1. Ocena skuteczności zakłóceń:

$$K_{z_{rz}}^{E} = \left(\frac{R_s}{R_z}\right)^2 * \sqrt{\frac{P_z * G_z * G_o}{P_s * G_s}} \qquad (2.3.2.6)$$

Jeżeli $K^{E}_{z_{rz}} \rangle K_{z_w}$ (uwzględnianego dla danego rodzaju pracy radiostacji), to oceniana linia będzie skutecznie zakłócona, w przeciwnym wypadku ww. linia jest odporna na zakłócenia.

2. Ocena głębokości skutecznych zakłóceń ($Rz_{sk.}$):

$$R_{zsk} = R_s * \sqrt[4]{\frac{P_z * G_z * G_o}{Ps * K^2_{z_w} * G_s}} \quad [km] \qquad (2.3.2.7)$$

3. Ocena skutecznej mocy zakłóceń ($Pz_{sk.}$):

$$P_{zsk} = \frac{Ps * R_z^4 * G_s * K^2_{z_w}}{R_s^4 * G_z * G_o} \quad [W] \qquad (2.3.2.8)$$

Do oceny skuteczności zakłóceń łączności KF na falach przestrzennych i UKF w relacjach samolot-samolot i ziemia-samolot, gdzie nie występuje zjawisko tłumienia fal elektromagnetycznych przez pokrycie Ziemi, celowe jest wykorzystanie przedstawionych niżej zależności:

1. Ocena skuteczności zakłóceń (K^{E}_{Zrz}):

$$K^{E}_{z_{rz}} = \frac{R_s}{R_z} * \sqrt{\frac{P_z * G_z * G_o}{P_s * G_s}} \qquad (2.3.2.9)$$

Jeżeli $K^{E}_{z_{rz}} \rangle K_{z_w}$ (uwzględnianego dla danego rodzaju pracy radiostacji), to oceniana linia będzie skutecznie zakłócona, w przeciwnym wypadku ww. linia jest odporna na zakłócenia.

2. Ocena głębokości skutecznych zakłóceń ($Rz_{sk.}$):

$$R_{zsk} = R_s * \sqrt{\frac{P_z * G_z * G_o}{Ps * K^2_{z_w} * G_s}} \quad [km] \qquad (2.3.2.10)$$

3. Ocena skutecznej mocy zakłóceń ($Pz_{sk.}$):

$$P_{zsk} = \frac{Ps * R_z^2 * G_s * K^2_{z_w}}{R_s^2 * G_z * G_o} \quad [W] \qquad (2.3.2.11)$$

Bardziej wszechstronna ***ocena skuteczności zakłóceń łączności radiowej KF na fali przestrzennej*** (odbitej) odbywa się przy pomocy specjalnych nomogramów [13]. Dotyczy to przede wszystkim przypadków wyboru miejsc rozmieszczenia stacji zakłóceń.

Dla emisji FH (ang. *frequency hopping*) istotnym czynnikiem zapewniającym skuteczność zakłóceń jest czas zakłócania sygnału na jednej częstotliwości. Wynosi on nie mniej niż 50%. W niektórych wypadkach przez zakłócanie końcowych sekwencji sygnału (synchronizujących) można doprowadzić do zerwania współpracy w pracujących sieciach, co prowadzi do braku możliwości przekazywania informacji.

Stosowanie ***zakłóceń łączności radioliniowej, troposferycznej i satelitarnej*** związane jest z koniecznością uwzględniania ostrych charakterystyk kierunkowych anten stacji radioliniowych. Jeżeli antena odbiorcza stacji radioliniowej skierowana jest w stronę przeciwległą do stacji zakłócającej, to skuteczne naruszenie jej pracy może być zapewnione tylko przy pomocy nadajników zakłócających o dużej mocy. Najwyższą skuteczność zakłóceń łączności radioliniowej osiąga się przy pomocy stacji zakłócających zainstalowanych na środkach latających (śmigłowcach, samolotach). Stacje takie o mocy 50-200 W są w stanie skutecznie zdezorganizować pracę środków radioliniowych na głębokość do 200 km, w zależności od wysokości i kierunku lotu samolotu (śmigłowca). *Głębokość skutecznych zakłóceń łączności radioliniowej, troposferycznej i satelitarnej emitowanych z powietrznych środków WE* oblicza się z zależności:

$$\mathbf{Rz^{*} = 0{,}67 * Rs^{2}} \text{ lub } \mathbf{Rz^{**} = 0{,}3 * Rs} \qquad (2.3.2.12)$$

Ocenę skuteczności zakłóceń emitowanych przez naziemne środki WE przeprowadza się zgodnie z zależnościami 2.2.3.6 - 2.2.3.8. Należy wówczas starannie dobrać współczynniki anten nadawczych i odbiorczych stacji radioliniowej (G_s i G_o).

---

* Przy zakłócaniu główną wiązką energii elektromagnetycznej.

** Przy zakłócaniu bocznymi (tylnymi) wiązkami energii elektromagnetycznej.

Przedstawione uwarunkowania energetyczne na bazie matematycznych metod analitycznych, wyrażone zależnościami (2.3.2.6-2.3.2.12) należy uwzględnić podczas projektowania modelu symulacyjnego oceny zagrożenia elektronicznego MSŁ ZO WL.

2.3.3. Dostępność czasowa mobilnego systemu łączności związku operacyjnego wojsk lądowych dla środków WE przeciwnika

Na dostępność czasową mają wpływ zarówno możliwości techniczno-bojowe środków łączności ocenianego SŁ jak i możliwości techniczne środków oraz zestawów rozpoznania i WE potencjalnego przeciwnika. Znajdujące się w oddziałach i pododdziałach rozpoznania i WE innych państw, z którymi RP nie posiada sojuszu obronnego środki i zestawy WE umożliwiają rozpoznanie i zakłócanie wszystkich rodzajów pracy (emisji radiowych) bezprzewodowych środków łączności MSŁ ZO WL. Kierowanie procesami rozpoznania, namierzania i zakłócania odbywa się na ogół w sposób zautomatyzowany. Posterunki namierzania sterowane są najczęściej przez komputery, które na podstawie danych wysyłanych ze stanowiska dowodzenia zapewniają namierzanie synchroniczne (zautomatyzowane), co umożliwia lokalizację źródeł promieniowania w bardzo krótkim czasie – poniżej 1 sekundy. Również stacje zakłócające umożliwiają prowadzenie zautomatyzowanego procesu zakłócania sterowanego centralnie przez SD. Proces ten jest zorganizowany w taki sposób, że w jednym cyklu są kolejno zakłócane częstotliwości pracy 4 nadajników, którym przypisano najwyższy priorytet (ze względu na znaczenie), a jednocześnie w krótkich przerwach między zakłóceniami jest prowadzone automatyczne śledzenie wszystkich z góry ustalonych relacji radiowych.

Istotną cechą charakteryzującą urządzenia rozpoznania i zakłócania elektronicznego, obok możliwości ilościowych, jest *czas reakcji systemu* rozumiany jako średnia wartość przedziału czasu pomiędzy wystąpieniem seansu wymiany danych w linii łączności strony przeciwnej a rozpoczęciem emisji sygnału zakłócającego ten seans.

Analiza funkcjonowania systemu rozpoznania i WE innych państw, uwzględniająca możliwości destrukcyjne ich bazy materialnej wskazuje, że czas

reakcji może być różny w zależności od typu stacji zakłócającej i sposobu jej wykorzystania. Stacje sterowane przez komputer pokładowy mają czas reakcji poniżej 1sekundy. Przy sterowaniu stacjami przez ośrodek kierowania czas reakcji wynosi do kilku do kilkunastu sekund. Natomiast gdy sytuacja jest nieznana oraz zachodzi potrzeba dokonania analizy i postawienia zadań do zakłócania, czas reakcji wzrasta do kilku minut. Oznacza to, że czas reakcji systemu rozpoznania i walki elektronicznej potencjalnego przeciwnika powinien być krótszy od występujących w poddawanym ocenie systemie łączności czasów trwania seansów wymiany danych ($\bar{t}_{swi}$), co można przedstawić w postaci zależności:

$$\bar{t}_{rsz} \leq \bar{t}_{swi} \qquad (2.3.3.1)$$

Należy mieć na uwadze, że w przyszłości środki WE będą pracowały w całym zakresie częstotliwości promieniowania elektromagnetycznego – od fal radiowych, poprzez mikrofale i podczerwień, aż do promieniowania widzialnego i nadfioletu. Dominującą tendencją w przyszłościowych systemach rozpoznania i WE będzie ich szeroka automatyzacja. Zastosowane będą systemy eksperckie. Głównym zadaniem tych systemów będzie tworzenie baz danych dla podsystemów rozpoznawczych i zakłócających, wybór optymalnego działania i zapewnienie kierowania tymi systemami w czasie rzeczywistym. Systemy eksperckie będą dokonywać również oceny strategii działania i jej realizacji w zależności od zaistniałej sytuacji. Zastosowanie systemów eksperckich pozwoli na skonstruowanie tzw. *uniwersalnych rozproszonych urządzeń zakłócających* z wydzielonymi stacjami nadawczymi, obejmującymi zakres UKF i KF. Przewiduje się zastosowanie na szeroką skalę robotyzacji, w celu wyeliminowania obsługi urządzeń zakłócających, które będą szczególnie narażone na polu walki. Poza tym należy oczekiwać zwiększenia mocy generowanych zakłóceń przy jednocześnie zwiększonej szerokości pasma zakłócanych częstotliwości, szczególnie przydatnych przy zakłócaniu emisji ze skokową zmianą częstotliwości i czasu (*ang.* frequency and time hopping). Urządzenia rozpoznawcze z kolei zapewnią wykrywanie sygnałów przeciwnika w szerokim paśmie częstotliwości nawet w warunkach silnych zakłóceń.

Perspektywiczne systemy rozpoznania i zakłócania elektronicznego będą obejmowały:

– uniwersalne naziemne oraz powietrzne (samolotowe) zestawy rozpoznawczo-zakłócające, wykorzystywane przede wszystkim na szczeblu operacyjnym,

– uniwersalne powietrzne (śmigłowcowe) oraz naziemne zestawy rozpoznawczo-zakłócające, które powinny obejmować również rozpoznanie i zakłócanie urządzeń radiolokacyjnych, wykorzystywane na szczeblu taktycznym.

Szeroko zautomatyzowane zestawy, o których mowa wyżej, będą posiadały odpowiednie urządzenia do automatycznego przetwarzania danych z rozpoznania, dodatkowe moduły zdolne do wykrywania nadajników radiowych z nowymi maskującymi sygnałami. Podobne urządzenia będą wykorzystane do zautomatyzowanego przetwarzania danych z zakłóceń elektronicznych. Dla zwiększenia żywotności wykorzystywanych systemów eksperckich przewiduje się możliwość wyboru każdej stacji systemu jako głównej, zdolnej do kierowania pozostałymi.

Poza tym prowadzone są intensywne badania w zakresie wykorzystania mikrofal w perspektywicznych środkach WE, które zamierza się wykorzystać się do:

– zakłócania systemów elektronicznych (radiolokacyjnych i łączności), co wymaga gęstości mocy rzędu 10^{-8}-10^{-6} W/cm^2,

– zablokowania działania elementów czujnikowych i układów elektronicznych w wyniku zaindukowania przez mikrofale prądu i wchłonięcia sygnału użytkowego, co pozwala również na zdalną inplantację wirusów komputerowych (wymaga gęstości mocy rzędu 10-100 W/cm^2),

– niszczenia elementów układów elektronicznych na skutek zaindukowania nadmiernego prądu, spowodowanego np. przez silny niejądrowy impuls elektromagnetyczny o dużej gęstości mocy (zjawisko dotychczas znane jako czynnik wybuchu jądrowego),

– szybkiego indukcyjnego wytworzenia wysokiej temperatury w atakowanym obiekcie, co wymaga gęstości mocy rzędu 1000-10 000 W /cm.^{2}

Przeprowadzone rozważania pozwalają na sformułowanie następujących uogólnień:

1. Siły i środki rozpoznania i WE innych państw, z którymi RP nie posiada sojuszu obronnego mają możliwość prowadzenia rozpoznania, namiaru i obezwładnienia zakłóceniami zarówno w strefie taktycznej jak i w pozostałych strefach zbrojnych działań wojennych. Dlatego należy liczyć się z ciągłym oddziaływaniem elektronicznym na MSŁ ZO WL.

2. MSŁ ZO WL może być obiektem ich oddziaływania z różnym nasileniem we wszystkich okresach walki. Oddziaływanie to będzie znaczniejsze w strefie taktycznej, a zdecydowanie mniejsze (w stosunku do środków radiowych UKF i radioliniowych) – w strefie operacyjnej.

3. Spośród elementów MSŁ ZO WL narażone będą głównie bezprzewodowe środki teletransmisyjne i organizowane za ich pomocą linie łączności. Wynika stąd, że w trakcie projektowania MSŁ WL należy uwzględnić bardzo duże możliwości oddziaływania elektronicznego potencjalnego przeciwnika. Budując model symulacyjny oceny zagrożenia elektronicznego MSŁ WL należy uwzględnić:

- intensywność oddziaływania elektronicznego (przedstawioną w podrozdziale 2.3.1), a wyrażoną w formie prawdopodobieństwa zdezorganizowania poszczególnych bezprzewodowych linii łączności w przedziale (0 ÷ 1) lub procentowo (0 ÷ 100%). Wskaźniki te są zarazem sugestywne i komunikatywne dla pozostałych agend sztabu różnych szczebli dowodzenia WL.
- uwarunkowania energetyczne. Przy czym najbardziej wymierne dane w zakresie oceny zagrożenia elektronicznego dotyczą skuteczności obezwładniania zakłóceniami bezprzewodowych linii łączności MSŁ ZO WL wyrażone zależnościami (2.3.2.6 ÷ 2.3.2.12), bowiem dane z rozpoznania elektronicznego wykorzystywane są z reguły kompleksowo przez różne agendy sztabów.
- uwarunkowania czasowe, które obejmują czas reakcji systemu zakłóceń potencjalnego przeciwnika oraz intensywność wymiany danych i czas reakcji systemu (linii) łączności na zakłócenia elektroniczne wyrażone zależnością 2.3.3.1. Uwarunkowania te umożliwiają oceny zagrożenia elektronicznego MSŁ ZO WL w wyniku symulacji procesów zachodzących w określonych przedziałach czasowych.

3. PROJEKT KONCEPCYJNY MODELU SYMULACYJNEGO ZAGROŻENIA ELEKTRONICZNEGO MOBILNEGO SYSTEMU ŁĄCZNOŚCI ZWIĄZKU OPERACYJNEGO WOJSK LĄDOWYCH

3.1. Założenia i ograniczenia modelu

Przedmiotem modelu powinno być opracowanie dwustronnej komputerowej gry wojennej, ze zmiennymi danymi wejściowymi wprowadzanymi na bieżąco. Oznacza to, że jest możliwe odwzorowanie w nim działań bojowych wojsk własnych i przeciwnika. Zatem integralnym elementem modelu symulacyjnego zagrożenia elektronicznego mobilnego systemu łączności związku operacyjnego wojsk lądowych (MS ZE MSŁ ZO WL) powinien być model funkcjonowania systemu łączności oraz jego otoczenia w formie komputerowej gry wojennej (KGW). Na jego treść i strukturę powinno składać się wiele wzajemnie powiązanych elementów zapewniających z jednej strony funkcjonowanie MSŁ ZO WL, z drugiej zaś elementów tworzących system walki elektronicznej przeciwnika destrukcyjnie oddziaływujący na stronę pierwszą. Ze względu na strukturę informacyjną systemu gry, zakres i stopień szczegółowości odwzorowywanych w modelu symulacyjnym zjawisk, procesów oraz elementów pola walki MS ZE MSŁ ZO WL powinien nadawać się do wielokrotnego rozgrywania – praktycznie nieograniczonego, licznego zbioru różnych złożonych sytuacji, scenariuszy użycia środków WE przez przeciwnika, oraz sposobów obrony MSŁ ZO WL przed ich oddziaływaniem[20].

Ze względu na złożoność modelowanych zjawisk, model symulacyjny celowo jest opracować w postaci wyodrębnionych funkcjonalnie modułów (submodeli) obejmujących działania bojowe oddziałów, pododdziałów i pojedynczych środków łączności MSŁ ZO WL (funkcjonowanie MSŁ ZO WL) oraz WE przeciwnika (funkcjonowanie jego systemu WE), procedury wprowadzania danych wejściowych, aktualizacji bazy danych, redagowania i zobrazowania informacji wynikowych, oraz procedury pomocnicze niezbędne do efektywnego

[20] Różnorodność sytuacji może wynikać np. z różnorodności warunków terenowych, struktur organizacyjnych wojsk, rodzajów i typów środków walki obu walczących stron itp.

funkcjonowania MS ZE MSŁ ZO WL. Na podstawie wyodrębnionych modułów zasadne jest opracowanie algorytmów ogólnych i szczegółowych, stanowiących bazę wyjściową do oprogramowania modelu symulacyjnego, które powinno być zawarte w projekcie technologicznym.

Wszystkie z wymienionych programów komputerowych powinny funkcjonować pod kontrolą specjalnego programu sterującego, symulującego m.in. fizyczne zjawisko upływu czasu rzeczywistych działań bojowych.

MS ZE MSŁ ZO WL powinien mieć wysoce ***interaktywny*** charakter. Wyrażać się to będzie możliwościami bieżącego wpływania uczestników gry na przebieg symulowanych działań bojowych oraz informowaniem ich o wszystkich istotnych sytuacjach modelowanych działań bojowych. Interaktywny charakter MS ZE ZOWL powinien stymulować wysoką aktywność uczestników gry zarówno w działalności „growej", jak i prowadzonej w związku z grą. Prezentowana komputerowa gra wojenna, powinna, umożliwiać modyfikowanie zakresu, treści i czasu dostarczanych uczestnikom gry informacji o wojskach przeciwnika. Rozwiązanie takie powinno umożliwiać jednak rozegranie wielu wariantów (scenariuszy) gry.

MS ZE MSŁ ZO WL powinien być w pełni ***autonomicznym*** modelem w tym zakresie. Nie wyklucza to jednak możliwości wykorzystania jej w ramach innych symulacyjnych modeli walki ZO i ZT WL. Możliwość taka powinna powstać dzięki funkcjonowaniu informacyjnego sytemu gry niezależnego od treści symulacyjnych programów komputerowych oraz poprzez wprowadzenie tzw. decydentów uogólnionych. Ci ostatni będą mogli spełniać role pierwotnie przypisane decydentom wszystkich niższych szczebli dowodzenia, dzięki czemu MS ZE MSŁ ZO WL stanowić może również element serii gier, od taktycznych – do operacyjnych włącznie. Ze względu na możliwość przerwania gry w dowolnym momencie oraz ponownego zasymulowania przebiegu działań bojowych dla innych wariantów decyzyjnych, MS ZE MSŁ ZO WL powinien umożliwiać uczestnikom gry porównanie – często diametralnie różnych – wyników modelowanych zagrożenia elektronicznego MSŁ ZO WL i wybór wariantu decyzyjnego najlepszego w danej sytuacji operacyjnej bądź taktycznej. Oznacza to równocześnie, że funkcjonujący w grze system przetwarzania danych powinien odpowiadać współczesnym tendencjom w zakresie projektowania kompu-

terowych systemów wspomagania dowodzenia DSS (ang. *Decision Support System*) i ES (ang. *Expert System*)[21] w obszarze dotyczącym wysokiej aktywności przetwarzanych na komputerze zadań. Istotą tych systemów jest wspomaganie decydenta (uczestnika gry) w procesie identyfikacji i oceny możliwych wariantów decyzji[22].

W komputerowych grach wojennych obok możliwości wariantowania decyzji podejmowanych przez uczestników gry, istotną rolę spełnia struktura i sposób odwzorowania fizycznego zjawiska upływu czasu, z którym związana jest tak ważna cecha modelowanego systemu, jak wysoka dynamika współczesnych zbrojnych działań wojennych. W MS ZE MSŁ ZO WL sposób odwzorowania upływu czasu powinien wynikać z przyjętej techniki modelowania symulacyjnego (metoda kolejnych zdarzeń, gdzie czas zegarowy ustawiany jest na chwilę, w której ma wystąpić następne zdarzenie)[23], a przydział czasu w którym symuluje się funkcjonowanie MSŁ ZO WL i jego otoczenia ograniczony powinien być tylko i wyłącznie celami gry. Oznacza to, że w MS ZE MSŁ ZO WL symulacja działań bojowych obejmować może dowolny przedział czasu, ale najczęściej jednak jego długość odpowiada czasowi realizacji zadania ZO, ZT i oddziałów WL.

Obok długości przedziału czasu, w którym symuluje się funkcjonowanie modelowanego systemu działań bojowych, ważna wydaje się skala jego odwzorowania. W MS ZE MSŁ ZO WL powinna być możliwość odwzorowania czasu w trzech różnych skalach. Pierwsza – powinna dotyczyć sytuacji, w której kilku jednostkom czasu rzeczywistego odpowiada jedna jednostka czasu funkcjonowania modelowanego systemu (symulacja w czasie skomprymowanym). Druga – powinna obejmować te sytuacje, w których jednej jednostce czasu funkcjonowania systemu rzeczywistego, odpowiada jedna jednostka czasu funkcjonowania modelowanego systemu (symulacja w czasie rzeczywistym). Trzecia skala odwzorowania powinna dotyczyć sytuacji, w których jednej jednostce

[21] W. Radzikowski: *Komputerowe systemy wspomagania decyzji.* PWE, Warszawa 1990.

[22] Realizowane w tym zakresie wspomaganie dotyczy przede wszystkim procesów przeddecyzyjnych, których szczegółową charakterystykę przedstawiono w: A. Kozielecki: *Psychologiczna teoria decyzji.* PWN, Warszawa 1975.

[23] G. Gordon: *Symulacja systemów.* WNT, Warszawa 1974.

czasu funkcjonowania rzeczywistego odpowiada kilka jednostek czasu funkcjonowania systemu modelowanego (symulacja w czasie rozciągniętym). Możliwości realizacyjne dwóch pierwszych sposobów odwzorowania czasu uzależnione są przede wszystkim od mocy obliczeniowych komputera, trzeciego zaś – wynikają z przyjętej organizacji gry.

Szczegółowy pogląd na złożoność MS ZE MSŁ ZO WL dać może pełny i wyczerpujący opis zarówno każdego z istotnych elementów gry, jak i działań związanych z efektywnym jej wykorzystaniem. Dlatego, mając na względzie celowość takiego opisu, ułatwiającego czytelność i zwiększającego poglądowość procesu projektowania i dokumentowania komputerowej gry wojennej.

Wymagania nakładane na model należy podzielić na dwie grupy:

– wymagania informacyjne,

– wymagania implementacyjne.

Wymagania informacyjne reprezentują potrzeby użytkownika, natomiast wymagania implementacyjne są odwzorowaniem wymagań informacyjnych na warunki techniczne rozumiane jako sprzęt i oprogramowanie.

Wymagania informacyjne powinny obejmować:

– zdolność do gromadzenia, przechowywania i użytkowania wiedzy w postaci danych elementarnych i informacji,

– zdolność do prezentacji informacji w sposób jasny i umożliwiający szybkie ich zrozumienie,

– łatwość użytkowania w postaci operacji i poleceń umożliwiających dostęp do informacji i ich prezentację,

– możliwość objaśnienia otrzymanych wyników i sposobu ich otrzymania.

Wymagania implementacyjne modelu powinny obejmować:

– zdolność do przetwarzania danych w środowisku sieci komputerowej umożliwiającym współbieżne ocenianie zagrożenia elektronicznego i planowanie systemu łączności,

– systemem liczącym powinien być jeden z modeli lokalnych sieci komputerowych lub systemów wielodostępnych,

– w przypadkach szczególnych (awarie, małe zasoby sprzętowe) implementacja powinna być możliwa na autonomicznym stanowisku komputerowym,

– zdolność do współpracy z komputerowym modelem planowania mobilnego systemu łączności WL,

– zapewnienie integralności danych w powyższych modelach,

– zapewnienie poufności przetwarzanych danych,

– zdolność do współpracy z oprogramowaniem narzędziowym, standardami programowymi oraz programami specjalistycznymi znajdującymi zastosowanie w obszarze dziedzinowym modelu (współpraca ta powinna opierać się o procedury eksportujące i importujące bazy danych oraz tekstowe zbiory danych),

– posiadanie lub asymilacja mechanizmów przekazywania danych na duże odległości przy pomocy transmisji szeregowej.

W modelu powinny wystąpić następujące *ograniczenia*:

– rezygnacja z implementacji tych wskaźników ocenowych zagrożenia elektronicznego, których modele matematyczne są wyjątkowo złożone, wymagające wprowadzania dużej ilości danych wejściowych, bądź dużego czasu przetwarzania informacji,

– uwzględnienie jedynie wybranych przedsięwzięć obrony elektronicznych MSŁ ZO WL[24].

Komputerowa egzemplifikacja modelu może być wykonana i wykorzystania w szefostwach wojsk łączności i informatyki sztabów różnych szczebli dowodzenia WL do wspomagania pracy planistycznej w organizacji mobilnych systemów łączności. Może być wykorzystana również przez odpowiednie komórki rozpoznania i WE WL podczas oceny sytuacji elektronicznej w części dotyczącej wojsk własnych lub przeciwnika. Warunkiem prawidłowego funkcjonowania MS ZE MSŁ ZO WL jest utworzenie odpowiedniej bazy danych o jego o siłach i środkach potencjalnego przeciwnika oraz o własnych systemach łączności i ich otoczeniu.

MS ZE MSŁ ZO WL powinien mieć możliwość wykorzystywania także jako elementu *mutimedialnego systemu dydaktycznego*[25] tzn. takiego, w którym obok tradycyjnych metod, środków i technik nauczania, w celu zwiększenia efektywności procesu dydaktycznego wykorzystuje się w sposób skoordynowa-

[24] Przedsięwzięcia obrony elektronicznej MSŁ ZO WL zawarte są w [7, 8].

[25] S. Jarmark: *Komputery w dydaktyce szkoły wyższej.* PWN, Warszawa 1979.

ny także film, telewizję, gry komputerowe i modele symulacyjne oraz efekty dźwiękowe pochodzące z rzeczywistego pola walki. Systemy takie, angażując najszerzej technikę komputerową i inteligentne sieci telekomunikacyjne, ewoluują najwyraźniej – podobnie jak gry wojenne, lecz nieco wolniej – w kierunku szerokiego wykorzystania systemów rozproszonych i rzeczywistości wirtualnej[26].

W dalszej części opracowania zostaną przedstawione wszystkie istotne zagadnienia obejmujące strukturę, treść, zakres i sposób wykorzystania MS ZE MSŁ ZO WL – w postaci wyodrębnionych bloków problemowych.

3.2. Ogólna struktura organizacyjna modelu

Jednym z podstawowych wymagań (założeń) modelu powinno być zapewnienie jego zdolności do prowadzenia oceny zagrożenia elektronicznego mobilnego systemu łączności WL we współbieżnym jego planowaniu przez poszczególnych planistów z wykorzystaniem komputerowego wspomagania tego procesu w środowisku sieci komputerowej. Podejście to powoduje przyjęcie *struktury organizacyjnej modelu* złożonej z następujących elementów:

- bazy danych,
- bazy metod, modeli i procedur,
- interfejsu użytkownika.

Baza danych powinna stanowić zbiór tablic zdefiniowanych w celu zgromadzenia przechowywania i przetwarzania danych dla potrzeb modelu. Baza danych występująca w modelu, powinna przechowywać informacje niezbędne na wszystkich etapach procesu oceny zagrożenia elektronicznego. Zgromadzone informacje tworzą *strukturę informacyjną modelu*. Architektura bazy danych w prezentowanym modelu, jak każdej nowoczesnej bazy danych, powinna być trójpoziomowa i obejmować:

- poziom fizyczny,
- poziom pojęciowy,
- poziom prezentacji.

[26] B. Steibrink: *Multimedia u progu technologii XXI wieku.* Wyd. Mark&Technik, Warszawa 1994.

Poziom fizyczny powinien określać sposób przechowywania danych w pamięci zewnętrznej komputera. Na poziomie fizycznym dane gromadzone są w plikach (zbiorach) danych o określonych strukturach. Zarówno z punktu widzenia projektanta, jak też użytkownika systemu, poziom ten nie ma wpływu na sposób pracy, ma jednak wpływ na ostateczne działanie aplikacji.

Poziom pojęciowy powinien być odwzorowaniem poziomu fizycznego przy pomocy języka definicji danych (ang. *data defnition language – DDL*). Reprezentacjami fizycznie istniejących danych stają się abstrakcyjne pojęcia oraz relacje między nimi. Zapewnienie użytkownikowi możliwości operowania danymi właśnie za pomocą pojęć abstrakcyjnych, pomijając całkowicie – jeśli to możliwe – fizyczny sposób przechowywania danych przez komputer, należy do zadań systemu zarządzania bazą danych.

Na poziomie prezentacji zawartość bazy danych powinna być odwzorowywana w sposób czytelny dla użytkownika, np. w postaci tabel, schematów, wydruków itp.

Projektując bazę danych na potrzeby modelu, należy przyjąć następujące założenia i ograniczenia:

– struktura organizacji danych w każdej tablicy bazy danych powinna być uniwersalna, tzn. mieć możliwość zdefiniowania jej na poziomie dowolnego systemu zarządzania bazą danych w dowolnym środowisku operacyjnym,

– struktura organizacji danych w tablicach powinna być pozbawiona redundancji[27],

– struktura organizacji danych w tablicach bazy danych powinna zapewniać integralność danych,

– baza danych powinna funkcjonować w środowisku sieci komputerowej,

– dane przechowywane na poziomie fizycznym bazy danych muszą być utajniane.

W celu zrealizowania pierwszego z założeń można przyjąć standardowe typy danych dla definiowanych pól tablic tak, aby ich strukturę organizacyjną

[27] Terminem *redundancji danych* określa się taki sposób ich organizacji, w którym dane są niepotrzebnie powielane. Redundancje można i należy eliminować na etapie projektowania tablic bazy danych. Jednym ze sposobów unikania redundancji jest odpowiednie wiązanie tablic relacjami [2, 11].

można było wprowadzić przy pomocy dowolnego systemu zarządzania bazą danych. Integralność bazy danych złożonej z tablic powiązanych relacjami jest kolejnym założeniem modelu. Zapewnienie integralności powinno polegać na takim zarządzaniu danymi, aby po wykonaniu dowolnej operacji na bazie danych, została zachowana pełna odpowiedniość pomiędzy jej elementami i obiektami świata rzeczywistego, których atrybuty te elementy reprezentują. Odpowiedniość ta powinna być zapewniana przez wewnętrzne mechanizmy systemu zarządzania bazą danych. System zarządzania bazą danych powinien zapewnić niejawność danych na poziomie fizycznym. Niejawność ta może być zapewniona przez wewnętrzne mechanizmy systemu zarządzania lub też przez specjalnie zaprojektowane procedury np. szyfracji i deszyfracji.

Komputerowa egzemplifikacja modelu symulacyjny zagrożenia elektronicznego MSŁ ZO WL powinna działać w środowisku sieci komputerowej, w związku z tym do jego budowy należy przyjąć taki system zarządzania bazą danych, który na poziomie fizycznym bazy zapewni udostępnianie i aktualizację danych zawartych w plikach o wspólnym dostępie wszystkich użytkowników bez utraty integralności danych. Tablice bazy danych powinny być dostępne w sieci komputerowej dla wszystkich interfejsów użytkownika.

Baza metod modeli i procedur powinna stanowić zbiór takich metod, modeli oraz procedur, które w przypadku rozpatrywanego modelu, zapewniają wspomaganie procesu oceny zagrożenia elektronicznego oraz planowania mobilnego systemu łączności WL. Baza metod, modeli i procedur powinna tworzyć zatem strukturę algorytmiczną modelu. Obejmuje procedury realizujące algorytmy czynności planistycznych w procesie oceny zagrożenia elektronicznego mobilnego systemu łączności WL. W procedurach zawarte powinny być metody rozwiązywania problemów decyzyjnych oraz modele matematyczne użyte w celu rozwiązywania tych problemów. Prowadzą one do wypracowania decyzji o organizacji mobilnego systemu łączności WL w warunkach oddziaływania elektronicznego.

Dzięki użyciu bazy metod, modeli i procedur powinna istnieć możliwość dostarczenia planistom szczegółowej analizy sytuacji decyzyjnej, symulowania zdarzeń oraz jej interpretacji w systemie oceny zagrożenia elektronicznego i wspomagania podejmowania decyzji. Charakterystyczne dla bazy metod, mo-

deli i procedur jest rozpoznanie sytuacji decyzyjnej przez wykorzystanie bazy danych przy pomocy procedur i ich algorytmów oraz powiązań między bazą danych, a procedurami na poziomie zarządzania bazą metod, modeli i procedur. Procedury oraz powiązania między nimi i bazą danych tworzy się przy pomocy wyrażeń języka programowania i pakietów oprogramowania wywoływanych przez funkcje zarządzania, np. pakietów matematycznych, pakietów komunikacyjnych itp.

Podstawowym celem działania bazy metod, modeli i procedur powinna być transformacja danych zawartych w bazie danych na informacje użyteczne dla decydenta do podjęcia decyzji. Cel ten można osiągnąć przez dostarczenie modeli użytecznych dla procesu oceny zagrożenia elektronicznego oraz planowania mobilnego systemu łączności WL. Modele te wspomagają wszystkie fazy procesu podejmowania decyzji o organizacji łączności, stanowią również pewną logiczną całość, zapewniającą jednolitość procesu planowania mobilnego systemu łączności z punktu widzenia integralności i aktualności informacyjnej, spójności i bezpieczeństwa.

Strukturę organizacyjną modelu symulacyjnego, opracowaną na podstawie identyfkacji procesu oceny zagrożenia elektronicznego, z uwzględnieniem zasad planowania mobilnego systemu łączności WL i ujęcia go jako procesu informacyjno-decyzyjnego na szczeblu związku operacyjnego WL przedstawiono na rysunku 3.2.1.

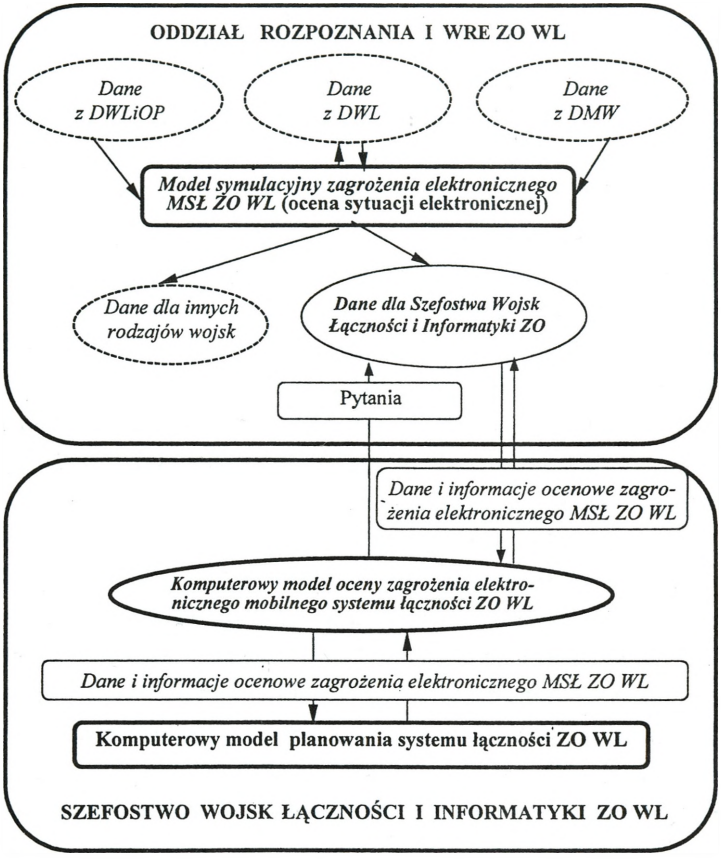
Oceniając *systemy i środki elektroniczne przeciwnika* należy rozpatrywać:

– sposób ich użycia, przynależność organizacyjną, wpływ tych środków na realizację zadań przez wojska łączności, a także ich możliwości taktyczno-techniczne oraz inne niezbędne dane;

– wnioski z oceny winny określać elementy tych systemów najbardziej wrażliwe na zakłócanie elektroniczne, a także optymalne sposoby ich obezwładniania zakłóceniami w różnych etapach operacji;

Oceniając *własne siły i środki WE* należy uwzględnić:

– aktualne ich położenie w obszarze odpowiedzialności WL, wielkość sił i środków WE (w tym – podległych ZO, ZT i oddziałów), elementów WE przełożonego, sąsiadów oraz ogniw pozamilitarnych;



Rys. 3.2.1. Struktura organizacyjna modelu symulacyjnego oceny zagrożenia elektronicznego systemu łączności ZO WL

– możliwości rozpoznawczo-zakłócające operacyjnych jednostek elektronicznych;

– najkorzystniejsze sposoby manewru bezpośrednio podległych jednostek elektronicznych w funkcji czasu lub zadań;

– organizację współdziałania w ramach operacyjnego systemu WE z jednostkami wojsk łączności i innymi elementami ugrupowania operacyjnego, a ponadto – z jednostkami elektronicznymi sąsiednich ZO;

– zadania obrony elektronicznej dla wszystkich dysponentów i użytkowników środków elektronicznych w WL (ZO, ZT, oddziałów) oraz czas i sposób ich wykonania;

– możliwości wykorzystania do realizacji zadań WE sił układu pozamilitarnego, znajdujących się w obszarze odpowiedzialności WL (ZO, ZT, oddziałów).

Dodatkowo *uzgodnieniu* powinny podlegać:

– problemy związane rozmieszczaniem środków łączności radiowej, radioliniowej i środków WE wojsk własnych względem siebie w obszarze odpowiedzialności WL (ZO, ZT, oddziałów);

– częstotliwości i rejony zastrzeżone do rozwijania środków elektronicznych;

– sposoby informowania o zakłóceniach w operacyjnych systemach łączności oraz ustalanie ich przyczyn;

– wspólne przedsięwzięcia obrony elektronicznej (pozorne sieci, kierunki radiowe, węzły łączności itp.).

W pełnej ocenie obszaru obrony WL (ZO, ZT, oddziałów) należy rozpatrywać także wpływ pokrycia terenu oraz zjawisk meteorologicznych na rozmieszczenie i działanie środków WE.

Wnioski z tak przeprowadzonej oceny sytuacji elektronicznej powinny być wykorzystane w odpowiednich szefostwach wojsk łączności i informatyki w procesie planowania mobilnych systemów łączności.

Interfejs użytkownika powinien stanowić warstwę pośrednią i odpowiada za dialog użytkownika z bazą danych i bazą metod modeli oraz procedur (dialog planistów z modelem). Podstawową formą przeglądania danych powinny być: tablice prezentacji danych (umożliwiające wyświetlanie dowolnych schematów danych – tzw. *perspektywy* – z różnych plików, pola do wprowadzania (wyświetlania) danych z informacjami opisowymi, pola do wprowadzania szablonów w celu wyszukiwania danych oraz okna graficznej informacji wynikowej. Każda tablica zawiera pola, które pozostają ze sobą w ścisłych zależnościach informacyjnych i tworzą zamknięte tematycznie grupy.

W interfejsie użytkownika należy wykorzystywać znormalizowane schematy obrazowania działania procedur. W praktyce oznacza to, że każda proce-

dura, która przetwarza dane w podobny sposób, będzie posługiwać się tymi samymi obiektami na ekranie w celu obrazowania jej działania.

Z punktu widzenia użytkownika na ekranie monitora powinny pojawiać się następujące obiekty do prezentacji danych:

- okna prezentacji tablic;
- pola do wprowadzania danych z informacjami opisowymi;
- pola do wyświetlania danych z informacjami opisowymi;
- pola do wprowadzania szablonów w celu wyszukiwania danych;
- okna graficznej informacji wynikowej.

Podstawową formą przeglądania danych powinny być tabele prezentacji danych. Mogą one wyświetlać dowolne schematy danych (tzw. *perspektywy*) z różnych plików, o ile powiązane są one relacjami. Znaczenia prezentowanych danych powinny być opisane nad tablicą tworząc nagłówki kolumn.

3.3. System informacyjny modelu

System informacyjny modelu powinien przedstawiać sobą odpowiednią strukturę, umożliwiającą zbieranie, przetwarzanie, przechowywanie, udostępnianie i aktualizację informacji o elementach, zjawiskach i procesach modelowanego systemu i jego otoczenia.

Ważną rolę w systemie informacyjnym modelu mają do spełnienia *informacje wejściowe* niezbędne do oceny zagrożenia elektronicznego oraz *informacje wynikowe*, niezbędne do zaplanowania systemu łączności w warunkach oddziaływania elektronicznego przeciwnika.

Informacje wejściowe, ze względu na źródło ich pochodzenia, należy podzielić na trzy główne grupy: zewnętrzne, wewnętrzne i pozostałe. Podział dotyczy zarówno informacji o przeciwniku, jak i o wojskach własnych. Ostatnia z grup może być utożsamiana z informacjami mało istotnymi dla oceny ZE lub tzw. szumem informacyjnym. Dlatego przedmiotem dalszego zainteresowania będą dwie pierwsze grupy.

Zewnętrzne źródła informacji powinny obejmować:

- informacje napływające od przełożonych;

– informacje napływające od podwładnych;

– informacje napływające od innych elementów ugrupowania operacyjnego.

Nadawcy tych informacji powinni stanowić bliższe i dalsze otoczenie systemu łączności związku operacyjnego WL.

Źródła wewnętrzne – to odzwierciedlenie wiedzy i doświadczeń oficerów Szefostwa Wojsk Łączności i Informatyki ZO WL nabytych w wyniku szkolenia, doskonalenia oraz pracy sztabowej. Stanowią one swoisty bank wiedzy, metod oraz procedur. Informacje wewnętrzne mogą być wprowadzone zawczasu jako *dane wejściowe* w ramach przygotowania systemu do pracy. Powinny być jednym z ważniejszych elementów systemu informacyjnego modelu. W MS ZE MSŁ ZO WL system informacyjny powinien obejmować między innymi następujące zbiory informacji o wojskach własnych i przeciwniku:

a) zbiory informacji wejściowych – względnie stałych:

– dane o strukturze organizacyjnej i wybranych elementach ugrupowania operacyjnego ZO WL (ugrupowania bojowego ZT lub oddziału);

– dane o elementach WE przeciwnika;

– parametry i normy taktyczno-techniczne środków łączności wojsk własnych;

– parametry i normy taktyczno-techniczne środków WE przeciwnika;

– słowniki nazw elementów ugrupowania bojowego, oddziałów i pododdziałów oraz środków walki;

– inne dane wprowadzane doraźnie.

b) zbiory informacji wejściowych – zmiennych:

– dane decyzyjne przygotowane przez uczestników tuż przed rozpoczęciem i w trakcie gry, opisujące scenariusze oddziaływania elektronicznego środków WE przeciwnika z założonego kierunku zagrożenia na poszczególne elementy systemu łączności ZO (ZT, oddziału) WL;

– dane decyzyjne przygotowane przez uczestników tuż przed rozpoczęciem i w trakcie gry, opisujące strukturę badanego mobilnego systemu łączności ZO (ZT, oddziału) WL oraz poszczególne jej elementy podatne na oddziaływanie elektroniczne środków WE przeciwnika z założonego kierunku zagrożenia.

Zbiory informacji wejściowych względnie stałych oraz zmiennych powinny mieć taką strukturę, aby nie ograniczały uniwersalnego charakteru MS ZE MSŁ ZO WL. Powinny zatem pozwalać na wielokrotne symulowanie działań bojowych dla różnych struktur organizacyjnych i wariantów ugrupowania bojowego oraz dla pododdziałów wyposażonych w dowolny rodzaj i typ środków walki. Struktura tych zbiorów powinna także zapewnić minimalny czas przygotowania i aktualizacji danych.

Informacje względnie stałe powinny być przygotowywane *przed rozpoczęciem gry*. Zakres ich ewentualnej aktualizacji ze zrozumiałych względów powinien być znacznie ograniczony. *Informacje wejściowe – zmienne*, przygotowywane przez uczestników gry *w trakcie jej przebiegu* i – w zależności od sytuacji zaistniałej w symulowanych działaniach bojowych powinny być poddawane bieżącej aktualizacji.

Zbiory informacji wejściowych względnie stałych oraz zmiennych powinny być ściśle ze sobą powiązane i tworzyć bank danych o hierarchicznej strukturze.

Obok informacji wejściowych, które opisują symulowane w MS ZE MSŁ ZO WL wojska własne i przeciwnika, szczególną rolę powinny mieć do spełnienia ***informacje wynikowe***. Są one przeznaczone do informowania uczestników gry o sytuacji zaistniałej na polu walki – niejako odwzorowując tym samym dynamikę w modelowanym zagrożeniu elektronicznym MSŁ ZO WL. Informacje wynikowe powinny być przekazywane uczestnikom gry w postaci doraźnych komunikatów o zaistniałych krytycznych w toku symulacji oraz (a przede wszystkim) po jej zakończeniu. Powinny obejmować:

– dane stanowiące treść meldunków okresowych o stanie, położeniu i działaniu pododdziałów odwzorowanych w MS ZE MSŁ ZO WL;

– dane stanowiące treść doraźnych komunikatów informujących uczestników gry o zaistniałych sytuacjach (zwłaszcza krytycznych) w modelowanym zagrożeniu elektronicznym MSŁ ZO WL;

– dane dotyczące intensywności oddziaływania elektronicznego środków WE przeciwnika;

– dane dotyczące możliwości obrony elektronicznej MSŁ ZO WL;

– graficzny obraz sytuacji elektronicznej (przedstawienie na tle struktury MSŁ ZO WL oraz obezwładnionych zakłóceniami linii łączności).

Komunikaty doraźne powinny być przekazywane w tych momentach czasu, które odpowiadają powstaniu krytycznej sytuacji w symulowanym zagrożeniu elektronicznym MSŁ ZO WL. Oznacza to, że przeznaczone powinny być one do bieżącego informowania uczestników gry, a co z tym związane – wspomagania proces operatywnego kierowania przebiegiem działań bojowych. W MS ZE MSŁ ZO WL powinno być zawarte wiele typów komunikatów doraźnych. Ich treści powinny dotyczyć tych wszystkich istotnych stanów rzeczy mogących zaistnieć w symulowanych działaniach bojowych, których odwzorowanie pozwala nadać grze wysoką dynamikę i realizm oraz osiągnąć wysoką aktywność jej uczestników. Należy podkreślić, że możliwość informowania uczestników gry i bieżącego ich reagowania na zaistniałe na symulowanym polu walki sytuacje, stanowi istotę interaktywnego charakteru MS ZE MSŁ ZO WL. Ilość, treść i struktura komunikatów jest pochodną zakresu i stopnia szczegółowości odwzorowania zjawisk i elementów pola walki w symulowanym modelu.

Informacje wynikowe wygenerowane po zakończeniu komputerowej gry wojennej powinny być zagregowane w dwóch wzajemnie uzupełniających się modułach:

1. Moduł danych statystycznych, obejmujący:

– liczbę wykryć, namierzeń zakłóceń poszczególnych relacji łączności tzw. *pomyślnych oraz nie pomyślnych według kryterium ilościowego (ze względu na posiadany przez przeciwnika potencjał WE);*

– liczbę wykryć, namierzeń zakłóceń poszczególnych relacji łączności tzw. *pomyślnych oraz nie pomyślnych według kryterium energetycznego;*

– liczbę wykryć, namierzeń zakłóceń poszczególnych relacji łączności tzw. *pomyślnych oraz nie pomyślnych według kryterium czasowego;*

– liczbę oraz zajętość środków WE przeciwnika;

– czasy pracy i nie pracy poszczególnych relacji łączności;

– czasy pracy i nie pracy poszczególnych środków WE przeciwnika;

– efektywny czas pracy poszczególnych środków WE przeciwnika.

2. Graficzny obraz oddziaływania elektronicznego naziemnych i powietrznych środków WE przeciwnika na mobilny system łączności WL, z podziałem na:

– relacje łączności radiowej KF (tylko naziemne);

– relacje łączności radiowej UKF;

– horyzontowe linie radiowe zakresu tzw. megahercowego oraz gigahercowego.

Szczegółowy opis struktury informacyjnej powinien być zawarty w projekcie technologicznym modelu.

3.4. Struktura algorytmiczna modelu

Struktura algorytmiczna modelu powinna być zbiorem procedur realizujących określone algorytmy. Dla uproszczenia prezentacji procedur należy wyróżnić ich typy i opisać ich cechy charakterystyczne. Procedury należy podzielić na cztery główne grupy:

– fazy przygotowania modelu do pracy;

– fazy weryfikacji i symulacji;

– fazy oceny przebiegu symulacji;

– pomocnicze.

Procedury fazy przygotowania modelu do pracy dotyczą głównie możliwości wprowadzenia obiektów, ich atrybutów oraz parametrów symulacji. Faza ta ma istotne znaczenia dla przebiegu symulacji, gdyż definiuje wszystkie najważniejsze elementy modelu. Procedury tej fazy podzielone są na 3 grupy: dotyczące modelu mobilnego systemu łączności ZO, wojsk WE przeciwnika oraz procedury pomocnicze, niezależne od wymienionych stron.

Procedury zawarte w MS ZE MSŁ ZO WL celowo jest podzielić na grupy, z których każda powinna charakteryzować się określonym podejściem do przetwarzania danych. Do zaprojektowanych w modelu procedur należą następujące typy:

– *TABLICA* – typ procedury, który powinien być przeznaczony do prezentacji danych w postaci tablicy. W kolumnach pionowych powinny być prezentowane pola danych, a w rzędach powinny być wyświetlane kolejne rekordy wprowadzone przez użytkownika. Procedura tego typu powinna być skojarzona z procedurą typu „formularz". Zadaniem procedury tablica powinna być prezentacja danych oraz umożliwienie ich przetwarzania poprzez wybór rekordu.

– *FORMULARZ* – typ procedury przeznaczony do wprowadzania rekordów danych, ich modyfikacji oraz usuwania z tablic. Powinien być skojarzony z procedurą typu „tablica" w ten sposób, że działał na rekordzie wybranym w procedurze „tablica". Powinien odpowiadać za poprawność wprowadzanych danych, a więc obiektów, ich atrybutów i parametrów symulacji.

– *RAPORT* – typ procedury przeznaczony do prezentacji danych w postaci tablic z zamiarem wyprowadzania danych na drukarkę. Dzięki procedurom tego typu użytkownik powinien mieć możliwość osiągania odpowiednią perspektywę tablicy danych w postaci różnych dokumentów.

– *OKNO* – typ procedury przeznaczony do prezentacji pojedynczych parametrów raczej, aniżeli tablic bazy danych. Parametry, których wartości powinny być widoczne na ekranie monitora, mogą być modyfikowane, ale nie mogą być usuwane.

– *MENU* – typ procedury, którego celem jest stworzenie możliwości wyboru ścieżki programu przez użytkownika. Procedury typu menu powinny zawierać zwykle nazwy opcji, których wybór powoduje uruchomienie odpowiedniej procedury innego typu.

– *KOD* – typ procedury, który nie powinien zawierać szablonu. Powinien być zbiorem instrukcji w określonym języku programowania tworzących kod źródłowy transponujący algorytm rozwiązania dowolnego problemu.

Działanie ***modelu mobilnego systemu łączności ZO WL*** powinno być oparte o funkcjonowanie następujących procedur i algorytmów działania:

– *OBSZAR ODPOWIEDZIALNOŚCI ZO WL* (typ – tablica). Obszar ten powinien być zdefiniowany przez wprowadzenie współrzędnych prostokątnych dwóch punktów na linii styczności z przeciwnikiem oraz poprzez sprecyzowanie głębokości obszaru. Wielkości te – jak wiadomo – opisują prostokąt. Do zbioru danych tej procedury powinny być zapisywane także inne dane np. szerokość obszaru, która jest odległością między dwoma zdefiniowanymi punktami oraz obliczone współrzędne prostokątne pozostałych dwóch wierzchołków prostokąta. Wszystkie wierzchołki powinny znaleźć się w tej samej strefie.

– *MIASTA* (typ – tablica). Celem działania procedury powinna być prezentacja miejscowości i ich współrzędnych prostokątnych w celu ułatwienia wprowadzania węzłów łączności i obiektów WE przeciwnika.

– *MIASTA* (typ – formularz). Celem działania procedury powinno być udostępnienie możliwości wprowadzania, modyfikacji oraz usuwania danych o miejscowościach.

– *WĘZŁY* (typ – tablica). Celem działania procedury powinna być prezentacja danych dotyczących węzłów łączności ZO WL.

– *WĘZŁY* (typ – formularz). Celem działania procedury powinno być udostępnienie możliwości wprowadzania, modyfikacji oraz usuwania danych o pomocniczych węzłach łączności (PWS) ZO WL. Oprócz nazwy węzła należy wprowadzić współrzędne prostokątne węzła. Wybór miejscowości powinien być przyczyną automatycznego uznania współrzędnych prostokątnych miejscowości jako współrzędnych węzła.

– *ROZMIESZCZENIE POMOCNICZYCH WĘZŁÓW ŁĄCZNOŚCI* (typ – kod). Celem działania procedury powinno być automatyczne rozmieszczenie podstawowych węzłów sieciowych w obszarze odpowiedzialności ZO WL. Procedura powinna mieć na celu przyspieszenie wprowadzania danych o zadanej liczbie PWS. Rozmieszczenie węzłów powinno odbywać się w określonej przez użytkownika strukturze składającej się z pewnej liczby rokad i osi. Siatka takiej sieci powinna być regularna, jednak użytkownik powinien mieć możliwość korygowania położenia PWS przy pomocy procedur WĘZŁY (typ – tablica) i WĘZŁY (typ – formularz). Po wygenerowaniu węzłów siatki i zapisaniu ich do tablicy WĘZŁY, powinny być generowane linie łączące węzły siatkowe i zapisywane do tablicy KIERUNKI według następującego algorytmu:

A) sprawdzenie parametrów rozmieszczenia PWS;

B) usunięcie dotychczas określonych PWS i linii je łączących;

C) rozmieszczenie PWS przy uwzględnieniu parametrów wprowadzanych przy pomocy procedury *ROZMIESZCZENIE PWS* (typ – parametry):

- obliczenie odległości między PWS na podstawie podanych parametrów:
  - odległość w linii rokady z zależności: $d_{rok} = (d_{sz} - 2*d_{rzg}) / (n-1)$,

gdzie:

d_{rok} – odległość międzywęzłowa w linii rokady,

d_{rzg} – odległość lewej osi PWS od linii rozgraniczenia,

d_{sz} – szerokość obszaru odpowiedzialności,

n – liczba osi w siatce.

- odległość międzywęzłowa w linii osi z zależności: $d_{os} = (d_{gł} - d_{st}) / m$, gdzie:

d_{os} – odległość międzywęzłowa w linii osi,

d_{st} – odległość pierwszej linii rokadowej PWS od linii styczności z przeciwnikiem,

$d_{gł}$ – głębokość obszaru odpowiedzialności,

m – liczba rokad w siatce.

- dla każdej rokady obliczenie współrzędnej pierwszego PWS na podstawie podanej odległości od linii styczności i odległości od lewej linii rozgraniczenia,
- obliczenie współrzędnych kolejnych PWS w rokadzie przez dodanie odległości międzywęzłowej;

D) zapis węzłów do tablicy WĘZŁY;

E) zapis linii łączących PWS do tablicy KIERUNKI.

– *ROZMIESZCZENIE (PARAMETRY) PWS* (typ – okno). Procedura powinna umożliwiać wyświetlanie i modyfikowanie parametry rozmieszczenia podstawowych węzłów sieciowych w mobilnym systemie łączności ZO WL. Do parametrów tych należą liczba rokad i liczba osi tworzących siatkę. Pozostałe parametry: odległość pierwszej linii PWS od linii styczności z przeciwnikiem oraz odległość lewej osi PWS od linii rozgraniczenia z sąsiednim ZO WL.

– *DOWIĄZANIE* (typ – kod). Celem działania procedury powinno być automatyczne dowiązanie węzła dostępowego do sieci podstawowej. Procedura ma na celu przyspieszenie wprowadzania danych o liniach radiowych. Dowiązanie węzłów powinno zachodzić w określonej przez użytkownika strukturze sieci składającej się z pewnej liczby rokad i osi. Kryterium dowiązania powinna stanowić najmniejsza odległość od węzła dowiązywanego do PWS. Wprowadzone dowiązanie może zostać skorygowane przy pomocy procedur

KIERUNKI (typ – tablica) i KIERUNKI (typ – formularz) według następującego algorytmu:

A) wybór węzła dostępowego w celu dowiązania;

B) sprawdzenie, czy istnieją węzły siatki; jeśli nie istnieją należy rozmieścić je przy pomocy procedury *ROZMIESZCZENIE PWS* lub wprowadzić każdy węzeł i linie je łączące;

C) usunięcie dotychczas istniejących dowiązań wybranego węzła;

D) obliczenie odległości od węzła dowiązywanego do wszystkich PWS w sieci;

E) wybranie dwóch PWS, do których odległość od węzła dostępowego jest najmniejsza;

F) zapis dowiązań do tablicy KIERUNKI.

– *KIERUNKI* (typ – tablica). Celem działania procedury powinna być prezentacja danych dotyczących istniejących linii radiowych w sieci łączności ZO WL.

– *KIERUNKI* (typ – formularz). Celem działania procedury powinno być udostępnienie możliwości wprowadzania, modyfikacji oraz usuwania danych o liniach łączności ZO WL. Linia powinna być wprowadzana przez wybranie dwóch węzłów, które ma połączyć. PWS powinny być wybierane z tablicy WĘZŁY. Zanim algorytm zatwierdzi poprawność linii powinien obliczyć jej długość (wg procedury DŁUGOŚĆ).

– *GRAFIKA SIECI RADIOLINIOWEJ* (typ – okno). Celem działania procedury powinno być graficzne przedstawienie schematu sieci radioliniowej ZO WL. Prostokąt reprezentujący obszar odpowiedzialności ZO powinien być kreślony na podstawie parametrów obszaru znajdujących się w tablicy PARAMETRY ZO WL. Współrzędne prostokątne wierzchołków prostokąta oraz położonych w nim węzłów łączności powinny być transponowane na współrzędne ekranowe i obrazowane w postaci punktów na ekranie. Linie powinny być kreślone między tymi punktami, które tworzą linie łączności w sieci podstawowej i linie dowiązań do niej.

– *RODZAJE SIECI* (typ – tablica). Celem działania procedury powinna być prezentacja danych dotyczących istniejących rodzajów sieci radiowych w sys-

temie łączności ZO WL. Rodzaje sieci należy wyróżnić ze względu możliwości łatwiejszego ich wprowadzania, modyfikowania i wyszukiwania. Dzięki tej procedurze użytkownik może podzielić wszystkie sieci radiowe ZO WL na grupy np. sieci dowodzenia, sieci powiadamiania, ostrzegania i alarmowania itp.

– *RODZAJE SIECI* (typ – formularz). Celem działania procedury powinno być udostępnienie możliwości wprowadzania, modyfikacji oraz usuwania danych o rodzajach sieci radiowych w łączności ZO WL.

– *SIECI RADIOWE* (typ – tablica). Celem działania procedury powinna być prezentacja danych dotyczących istniejących sieci radiowych w systemie łączności ZO WL. Ponieważ dane o sieciach celowo jest podzielić na grupy, to przed prezentacją danych powinien nastąpić wybór rodzaju sieci.

– *SIECI RADIOWE* (typ – formularz). Celem działania procedury powinno być udostępnienie możliwości wprowadzania, modyfikacji oraz usuwania danych o sieciach radiowych.

– *KORESPONDENCI* (typ – tablica). Celem działania procedury powinna być prezentacja danych dotyczących korespondentów w sieciach radiowych w systemie łączności ZO WL. Ponieważ dane o sieciach celowo jest podzielić na grupy, to przed prezentacją danych powinien nastąpić wybór rodzaju sieci. Dla każdego korespondenta powinien być precyzowany węzeł łączności, na którym pracuje. Pozwala to na umiejscowienie jego radiostacji w obszarze odpowiedzialności ZO WL.

– *KORESPONDENCI* (typ – formularz). Celem działania procedury powinno być udostępnienie możliwości wprowadzania, modyfikacji oraz usuwania danych o korespondentach w sieciach radiowych.

– *TYPY RADIOSTACJI* (typ – tablica). Celem działania procedury powinna być prezentacja danych dotyczących typów radiostacji stosowanych w systemie łączności ZO WL. Każda radiostacja powinna być opisana parametrami, które są niezbędne do obliczeń dotyczących oddziaływania elektronicznego przeciwnika.

– *TYPY RADIOSTACJI* (typ – formularz). Celem działania procedury powinno być udostępnienie możliwości wprowadzania, modyfikacji oraz usuwania danych o radiostacjach i ich parametrach.

– *TYPY STACJI RADIOLINIOWYCH* (typ – tablica). Celem działania procedury powinna być prezentacja danych dotyczących typów stacji radioliniowych stosowanych w systemie łączności ZO WL. Każda stacja radioliniowa powinna być opisana parametrami, które są niezbędne do obliczeń dotyczących oddziaływania elektronicznego przeciwnika.

– *TYPY STACJI RADIOLINIOWYCH* (typ – formularz). Celem działania procedury powinno być udostępnienie możliwości wprowadzania, modyfikacji oraz usuwania danych o stacjach radioliniowych i ich parametrach.

– *RODZAJE ANTEN* (typ – tablica). Celem działania procedury powinna być prezentacja danych dotyczących typów anten stosowanych w systemie łączności ZO WL i przez przeciwnika. Każda antena powinna być opisana parametrami, które są niezbędne do obliczeń dotyczących oddziaływania elektronicznego przeciwnika.

– *RODZAJE ANTEN* (typ – formularz). Celem działania procedury powinno być udostępnienie możliwości wprowadzania, modyfikacji oraz usuwania danych o antenach i ich parametrach.

– *EMISJE* (typ – tablica). Celem działania procedury powinna być prezentacja danych dotyczących rodzajów pracy (emisji) wykorzystywanych w środkach łączności. Każdy rodzaj emisji powinien być opisany wymaganym współczynnikiem zakłóceń, który jest niezbędny do obliczeń dotyczących oddziaływania elektronicznego przeciwnika.

– *EMISJE* (typ – formularz). Celem działania procedury powinno być udostępnienie możliwości wprowadzania, modyfikacji oraz usuwania danych o rodzajach emisji.

Model oddziaływania elektronicznego sił i środków WE przeciwnika powinien być zbudowany w oparciu o następujące procedury i algorytmy działania:

– *ŚRODKI WALKI ELEKTRONICZNEJ* (typ – tablica). Celem działania procedury powinna być prezentacja danych dotyczących typów środków WE stosowanych przez przeciwnika. W tablicy powinny być gromadzone dane, które nie muszą bezpośrednio uczestniczyć w symulacji. Dane o faktycznych środkach WE biorących udział w symulacji powinny być wprowadzane do tablicy POŁOŻENIE ŚRODKÓW przez wybieranie odpowiednich typów sprzętu WE

przy pomocy tej procedury. Środki WE powinny być wprowadzane z podziałem na następujące grupy:

- naziemne lub powietrzne,
- środki wykrywania, namierzania lub obezwładniania zakłóceniami.

– *ŚRODKI WALKI ELEKTRONICZNEJ* (typ – formularz). Celem działania procedury powinno być udostępnienie możliwości wprowadzania, modyfikacji oraz usuwania danych o typach sprzętu WE potencjalnego przeciwnika.

– *OBIEKTY WE* (typ – tablica). Celem działania procedury powinna być prezentacja danych dotyczących środków WE stosowanych przez potencjalnego przeciwnika, które będą bezpośrednio uczestniczyć w symulacji. Dane o faktycznym sprzęcie biorącym udział w symulacji powinny być wprowadzane do tablicy *POŁOŻENIE ŚRODKÓW* przez wybieranie odpowiednich typów sprzętu WE. Środki WE powinny być wprowadzane w następujących grupach:

- naziemne lub powietrzne,
- środki wykrywania, namierzania lub obezwładniania zakłóceniami.

– *OBIEKTY WE* (typ – formularz). Celem działania procedury powinno być udostępnienie możliwości wprowadzania, modyfikacji oraz usuwania danych o środkach WE przeciwnika użytych w symulacji.

Ważną rolę w modelowaniu zagrożenia elektronicznego MSŁ ZO WL powinny spełniać ***procedury pomocnicze***, a mianowicie:

– *WINETA* (typ – menu). Celem działania procedury powinien być wybór jednej z czterech podstawowych opcji w modelu:

- *MODEL MOBILNEGO SYSTEMU ŁĄCZNOŚCI ZO WL,*
- *MODEL ODDZIAŁYWANIA ELEKTRONICZNEGO PRZECIWNIKA,*
- *WERYFIKACJA I SYMULACJA,*
- *ANALIZA WYNIKÓW SYMULACJI.*

– *MODEL MOBILNEGO SYSTEMU ŁĄCZNOŚCI ZO WL* (typ – menu). Celem działania procedury powinien być wybór jednej z opcji dotyczących tworzenia opisu modelu mobilnego systemu łączności ZO WL.

– *MODEL ODDZIAŁYWANIA ELEKTRONICZNEGO PRZECIWNIKA.* Celem działania procedury powinien być wybór jednej z opcji dotyczących tworzenia opisu obiektów WE przeciwnika.

– *SYMULACJA* (typ – menu). Celem działania procedury powinien być wybór jednej z trzech opcji dotyczących weryfikacji modelu symulacyjnego, wprowadzenia parametrów czasowych symulacji oraz przebiegu i przeprowadzenia symulacji.

– *WYNIKI SYMULACJI* (typ – menu). Celem działania procedury powinien być wybór jednej z opcji dotyczących przeglądania i analizy wyników symulacji.

– *DŁUGOŚĆ* (typ – kod). Celem działania procedury powinno być obliczenie długości linii radiowej między dwoma węzłami opisanymi współrzędnymi prostokątnymi, które są parametrami procedury. Procedura powinna umożliwiać zwrot liczby rzeczywistej (REAL), która powinna stanowić długość linii w kilometrach, lecz z dokładnością do 1 metra. Oba węzły powinny znajdować się w jednej strefie geograficznej. Procedura powinna służyć także do obliczania odległości między obiektami systemu łączności ZO WL i obiektami WE przeciwnika.

Spośród ***procedur fazy weryfikacji modelu i symulacji*** w projekcie technologicznym należy uwzględnić:

– *PARAMETRY SYMULACJI* (typ – okno). Celem działania procedury powinno być wyświetlenie aktualnych parametrów symulacji oraz udostępnienie możliwości wprowadzania nowych parametrów. Do parametrów symulacji przyjętych w modelu powinny należeć:

- czas symulacji wyrażany w minutach, ograniczony do zadanej ilości dni operacji ZO WL,
- współczynnik szybkości symulacji zawierający się w przedziale 1÷100, który powinien opisywać szybkość realizacji zdarzeń i procesów (wartość 1 powinna oznaczać najszybsze ich wykonywanie).

– *PĘTLA GRAFICZNA* (typ – kod). Celem działania procedury powinna być realizacja pętli symulacyjnej. Procedura powinna skupiać wszystkie działania i algorytmy dotyczące weryfikacji parametrów i przebiegu symulacji.

Procedury fazy oceny przebiegu symulacji powinny obejmować:

– *WYNIKI – KIERUNKI* (typ –tablica). Celem działania procedury powinno być wyświetlenie wyników symulacji dla linii łączności. Dla każdej linii powinny być dostępne następujące wyniki symulacji:

- liczba skutecznych wykryć przez stacje wykrywania przeciwnika,

- liczba skutecznych namierzeń przez stacje namierzania przeciwnika,
- liczba skutecznych zdarzeń obezwładnienia zakłóceniami przez stacje zakłóceń przeciwnika,
- łączny czas obezwładniania zakłóceniami obliczany jako suma czasów od momentu rozpoczęcia zakłócania danej linii do momentu zakończenia reakcji systemu łączności na zakłócenie np. poprzez zmianę częstotliwości pracy,
- współczynnik zakłócania w [%] obliczany jako łączny czas zakłócania danej linii do czasu symulacji.

– *WYNIKI – SIECI* (typ – tablica). Celem działania procedury powinno być wyświetlenie wyników symulacji dla sieci łączności. Dla każdej sieci powinny być dostępne następujące wyniki symulacji:

- liczba skutecznych wykryć przez stacje wykrywania przeciwnika,
- liczba skutecznych namierzeń przez stacje namierzania przeciwnika,
- liczba skutecznych zdarzeń obezwładnienia zakłóceniami przez stacje zakłóceń przeciwnika,
- łączny czas obezwładniania zakłóceniami, obliczany jako suma czasów od momentu rozpoczęcia zakłócania danej sieci do momentu zakończenia reakcji systemu łączności na zakłócenie np. poprzez zmianę częstotliwości pracy.
- współczynnik zakłócania w [%], obliczany jako łączny czas zakłócania danej sieci do czasu symulacji.

– *WYNIKI-PRZECIWNIK* (typ – tablica). Celem działania procedury powinno być wyświetlenie wyników symulacji dla środków WE przeciwnika użytych w symulacji. Dla każdego środka należy zaprezentować następujące wyniki symulacji:

- liczba skutecznych wykryć, namierzeń i obezwładnień zakłóceniami zależnie od rodzaju pracy środka WE,
- liczba nieskutecznych wykryć, namierzeń i obezwładnień zakłóceniami zależnie od rodzaju pracy środka WE,
- skuteczność działania stacji wykrywania i namierzania obliczana jako iloraz liczby skutecznych wykryć lub namierzeń do łącznej ich liczby,
- czas efektywnej pracy stacji zakłóceń, obliczany jako suma czasów od momentu rozpoczęcia obezwładnienia zakłóceniami obiektu w sieci łączności

ZO WL do momentu zakończenia reakcji systemu łączności na zakłócanie np. poprzez zmianę częstotliwości pracy.

- wykorzystanie stacji zakłóceń w [%], obliczane jako łączny czas prowadzenia obezwładnienia zakłóceniami do czasu symulacji.

3.5. Funkcjonowanie modelu

Model powinien być funkcjonalnie podporządkowany cyklowi pracy zgodnemu z fazami procesu oceny zagrożenia elektronicznego oraz z fazami wyodrębnianymi w modelach symulacyjnych. Mając na uwadze powyższe założenia, należy wyodrębnić następujące fazy funkcjonowania MS ZE MSŁ ZO WL (rysunek 3.5.1):

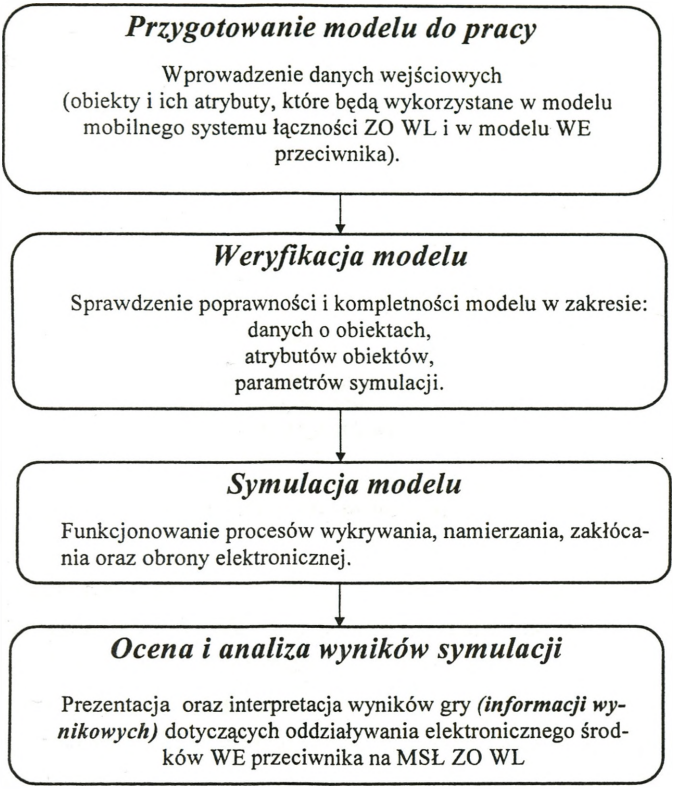
1. ***Przygotowanie modelu do pracy*** – faza, której celem jest wprowadzenie danych dotyczących obiektów uczestniczących w symulacji. Obiekty powinny zostać opisane przy pomocy atrybutów. Dla przejrzystości modelu obiekty powinny być podzielone na dwie główne grupy: obiekty modelu mobilnego systemu łączności WL oraz obiekty modelu przeciwnika. W tej fazie powinny być także wprowadzone wszystkie parametry symulacji.

2. ***Faza weryfikacji modelu*** – zadaniem tej fazy jest sprawdzenie poprawności i kompletności modelu systemu łączności ZO WL oraz modelu przeciwnika.

3. ***Faza symulacji*** – faza, której celem jest naśladowanie rzeczywistych procesów zachodzących w sytuacji walki elektronicznej dwóch stron.

Uczestnik gry po stronie przeciwnika powinien realizować następujące procesy:

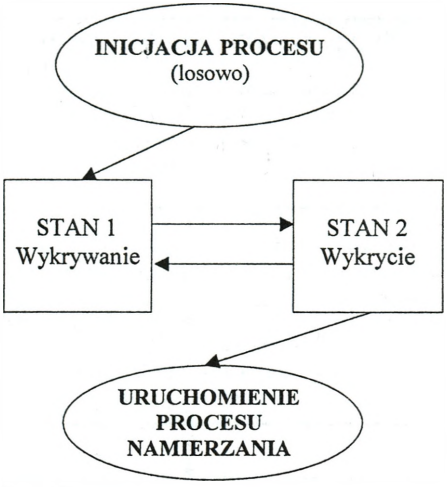
A.*Proces wykrywania środków łączności*. Podczas wykrywania należy generować *zasięg wykrywania środków łączności* z podziałem na: radiowe KF, radiowe UKF, radioliniowe – zakresu megahercowego, radioliniowe – zakresu gigahercowego, zgodnie z zależnościami 2.3.2.1÷2.3.2.3, przedstawionymi w podrozdziale 2.3.2. Podczas symulacji procesu wykrywania należy uwzględnić ponadto: *czas niezbędny do wykrycia środka łączności* – w postaci wprowadzanego parametru oraz *liczbę urządzeń rozpoznawczych pracujących w jednej aparatowni odbiorczej (na podstawie listy danych* technicznych środków WE przeciwnika).



Rys. 3.5.1. Struktura funkcjonalna modelu symulacyjnego zagrożenia elektronicznego mobilnego systemu łączności WL

Schemat procesu wykrywania realizowanego przez obiekt WE przeciwnika przedstawiony został na rysunku 3.5.2.

Jeśli w czasie wykrywania jeden ze środków łączności znajdzie się w zasięgu oddziaływania środka wykrywającego, obiekt WE przechodzi do stanu 2. W tym stanie przekazuje sygnał do obiektu WE, którym jest obiekt namierzania. Po przekazaniu sygnału obiekt wykrywania powinien być uwolniony i przystąpić do dalszej pracy, czyli przejść w stan 1. W tym momencie powinno być generowane kolejne zdarzenie, które sygnalizuje rozpoczęcie kolejnego procesu wykrywania przez dany obiekt WE.



Rys. 3.5.2. Schemat procesu wykrywania realizowanego przez obiekt WE przeciwnika

B. *Proces namierzania środków łączności oraz określania miejsca ich położenia*, z podziałem na radiowe KF, radiowe UKF. Należy przyjąć założenie, że środek łączności może być namierzony jeżeli został wcześniej wykryty. Poza tym należy *generować system namierzania przeciwnika* składający się co najmniej z trzech namierników charakteryzujący się określonym czasem namierzania.

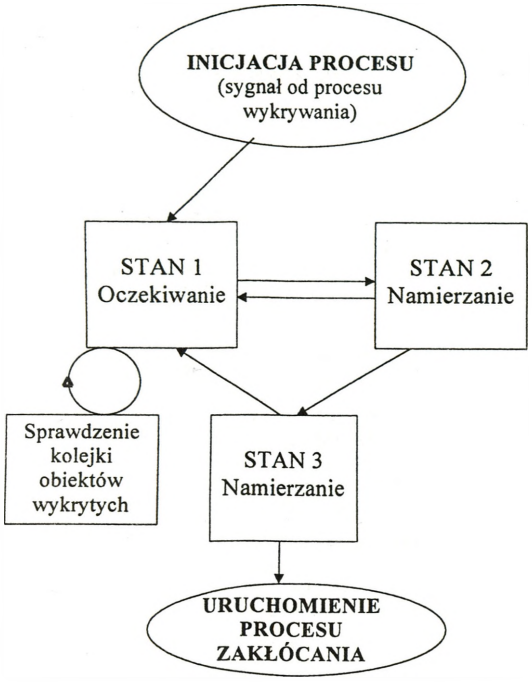
Czas ten należy zadawać w postaci parametru. Schemat procesu namierzania realizowanego przez obiekt WE przeciwnika przedstawiony został na rysunku 3.5.3.

C. Proces zakłócania. W cyklu tym uczestnik gry po stronie przeciwnika powinien mieć możliwość *wyboru dalszego wykrywania i namierzania pracujących środków łączności oraz obezwładnienia ich zakłóceniami po spełnieniu poprzednich cykli lub tylko pierwszego (tj. wykrywania).* Realizacja procesu zakłóceń powinna polegać na:

– generowaniu wolnej stacji zakłóceń (z listy środków WE przeciwnika),

– sprawdzeniu spełnienia uwarunkowań energetycznych, zgodnie z zależnościami 2.3.2.6 ÷ 2.3.2.12, przedstawionymi w podrozdziale 2.3.2,

– generowaniu czasu reakcji systemu zakłóceń na podstawie zależności 2.3.3.1, przedstawionej w podrozdziale 2.3.3,



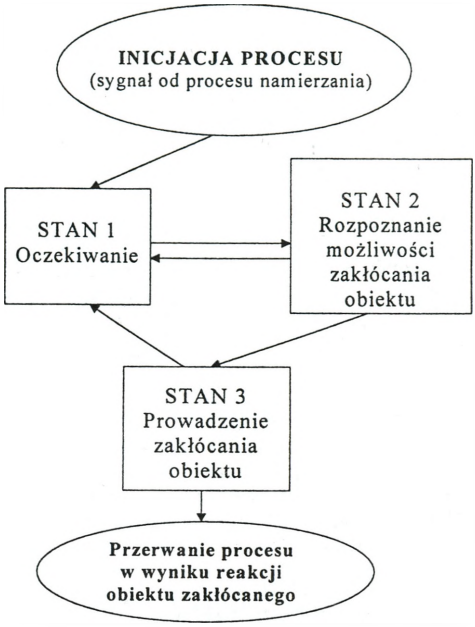
Rys. 3.5.3. Schemat procesu namierzania realizowanego przez obiekt WE przeciwnika

– generowaniu czasu rozpoczęcia lub trwania zakłóceń (możliwość wyboru z listy z generatorów liczb losowych),

– generowaniu czasu zakończenia zakłóceń (możliwość wyboru z listy z generatorów liczb losowych) – jeżeli generowano czas rozpoczęcia zakłóceń.

Proces zakłócania powinien być realizowany również z podziałem na środki naziemne KF, naziemne i powietrzne UKF, naziemne i powietrzne radioliniowe – uczestnicy gry po stronie przeciwnika. Schemat procesu zakłócania realizowanego przez obiekt WE przeciwnika przedstawiony został na rysunku 3.5.4.

Uczestnik gry po stronie wojsk własnych powinien inicjować proces wymiany informacji w poszczególnych relacjach łączności, który rozpoczyna się wraz z uruchomieniem pętli symulacyjnej. Z chwilą pojawienia się zakłóceń



Rys. 3.5.4. Schemat procesu zakłócania realizowanego przez obiekt WE przeciwnika

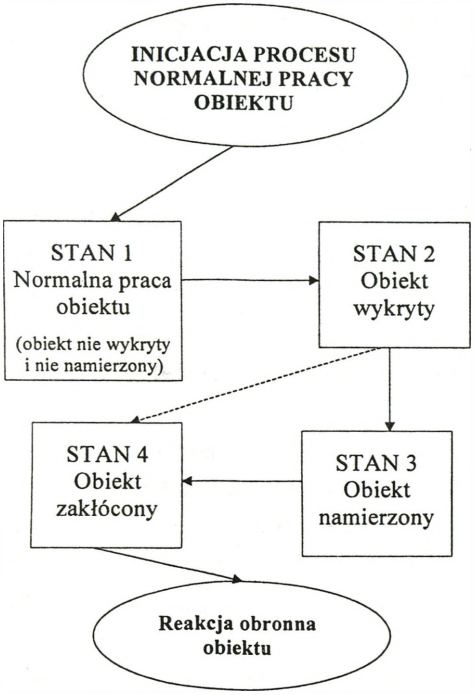
powinien mieć możliwość realizacji wybranych przedsięwzięć obrony elektronicznej (rysunek 3.5.5.), m.in.:

– generowania zmiany częstotliwości roboczej po upływie czasu zgodnie z zależnością 2.3.3.1 (podrozdział 2.3.3),

– zmiany wybranych parametrów technicznych sprzętu łączności, tj. mocy nadajnika, rodzaju pracy, rodzaju anteny, itd. z listy parametrów technicznych środków łączności.

W procesie inicjacji należy założyć, że wszystkie linie radiowe i sieci radiowe pracują nieprzerwanie przez cały czas symulacji. W czasie normalnej pracy obiektów łączności mogą one znajdować się w czterech stanach:

1. Obiekt jest nie wykryty i nie namierzony,
2. Obiekt jest wykryty,



Rys. 3.5.5. Schemat procesu reakcji obiektu MSŁ ZO WL na oddziaływanie elektroniczne

3. Obiekt jest wykryty i namierzony,

4. Obiekt jest obezwładniony zakłóceniami.

W pierwszych trzech stanach nie powinny być podejmowane próby reakcji, gdyż żaden z tych stanów nie ogranicza pracy obiektów mobilnego systemu łączności ZO WL. W czasie symulacji zliczane powinny być jedynie próby wykrywania i namierzania przeprowadzone przez obiekty WE przeciwnika.

Przejście od stanu 1 do stanu 4 nie powinno być niemożliwe. Jeśli obiekt zostanie wykryty i nie są podejmowane dalsze działania wobec niego, pozostaje on w tym stanie do końca symulacji. Podobna sytuacja zachodzi, gdy obiekt jest namierzony. Przejście do stanu 4 jest możliwe tylko po wystąpieniu reakcji

obronnej na obezwładnienie zakłóceniami. Przy czym nie zawsze obiekt musi być namierzony (stan 3).

W momencie obezwładnienia zakłóceniami obiekt mobilnego systemu łączności ZO WL powinien przejść w stan nieaktywny tzn. nie powinien pracować normalnie. Stan ten powinien trwać tak długo, ile wynosi wartość oczekiwana czasu reakcji obiektu na prowadzenie zakłóceń przez przeciwnika. W tym czasie powinny wystąpić działania obronne, które mają na celu skuteczną obronę przed zakłóceniem obiektu. Takimi działaniami w modelu powinny być:

- zmiana częstotliwości pracy zakłócanego obiektu,
- zmiana emisji, a co za tym idzie współczynnika zakłóceń skutecznych,
- inne.

Po upływie tego czasu obiekt powinien przejść w stan normalnej pracy, a obiekt WE przeciwnika powinien zaprzestać prowadzenia działań zakłócających i przejść w stan oczekiwania na kolejne sygnały o namierzeniu innego, bądź tego samego obiektu mobilnego systemu łączności ZO WL. Obiekt, który obroni się przed obezwładnieniem zakłóceniami powinien przejść w stan, gdy nie jest ani wykryty ani namierzony. Obezwładnienie go zakłóceniami po raz wtóry powinno być związane z pozytywnym zakończeniem się procesów wykrywania i namierzania oraz spełnieniem warunków skutecznego zakłócania.

Zachodzące w modelu procesy powinny pozostawać ze sobą w pewnych związkach przyczynowo-skutkowych. O ile proces wykrywania zachodzi całkowicie losowo i zależy od przyjętych parametrów rozkładu prawdopodobieństwa, o tyle inne procesy powinny wykazywać zależności deterministyczne.

Proces namierzania obiektu jest skutkiem jego wykrycia i może rozpocząć się albo bezpośrednio po wykryciu obiektu albo po upływie pewnego czasu w przypadku, gdy obiekty namierzania były akurat zajęte namierzaniem innego obiektu. Wynika stąd, że proces namierzania obiektu nie zajdzie, jeśli proces wykrywania nie zakończył się pomyślnie.

Proces obezwładnienia zakłóceniami powinien być skutkiem jego wykrycia i namierzenia (nie dotyczy relacji radioliniowych). Proces ten nie powinien zajść, jeśli proces wykrywania nie zajdzie pomyślnie.

Założenia te są w modelu bardzo istotne, gdyż mają znaczenie przy interpretacji wyników symulacji. W przypadkach, gdy w procesie symulacji nie występują pewne zdarzenia, znaczy to, że nie spełnione są pewne warunki zainicjowania procesów zależnych. Przykładowo, brak zdarzeń wynikających bezpośrednio z warunków przebiegu procesu zakłócania skłania do wniosku, że albo mobilny system łączności ZO WL jest odporny na takie działania albo rozmieszczenie i atrybuty obiektów zakłócających są nieadekwatne do badanej sytuacji.

Szczególnym przypadkiem symulacji może więc być taki, w którym zachodzą tylko nieskuteczne procesy wykrywania. Znaczy to, że żaden z obiektów wykrywania nie leży w odległości mniejszej niż horyzont radiowy każdego z obiektów mobilnego systemu łączności ZO WL.

Ważną rolę w procesie symulacji powinny odgrywać *zdarzenia generowane przez procesy wyszczególnione na listach zdarzeń*. Listy zdarzeń powinny rejestrować przejścia obiektów z jednego stanu do drugiego. Zdarzenie należy opisać w modelu następującymi atrybutami:

- nazwa zdarzenia;
- czas wystąpienia zdarzenia;
- nazwa i adres obiektu, który zainicjował zdarzenie;
- rodzaj pracy obiektu, jeśli jest to obiekt WE przeciwnika (wykrywanie, namierzanie, obezwładnianie zakłóceniami);
- nazwa i adres obiektu, który uczestniczy w skutkach zdarzenia np. jest namierzony lub zakłócony;
- stan tego obiektu.

Po każdym wygenerowaniu zdarzenia w modelu, powinno ono być umieszczane na końcu listy zdarzeń, po czym listę należy sortować według czasu wystąpienia zdarzenia. W ten sposób na czele listy powinno znajdować się zawsze zdarzenie, które ma wystąpić w najbliższej przyszłości. W modelu należy uwzględnić następujące zdarzenia:

- skuteczne wykrycie obiektu;
- brak efektu wykrywania;
- skuteczne namierzenie obiektu;
- brak możliwości namierzenia obiektu;

– rozpoczęcie obezwładnienia obiektu zakłóceniami;
– zakończenie obezwładnienia obiektu zakłóceniami;
– brak możliwości obezwładnienia obiektu zakłóceniami.

Skuteczne wykrycie obiektu powinno nastąpić wtedy, gdy obiekt pracuje normalnie, a więc nie jest właśnie zakłócany, namierzany lub wykryty. Jeśli wykrywanie nie przyniesie efektu, oznacza to, że wszystkie obiekty, które mogą być wykryte są już wykryte. Jeśli z przebiegu symulacji wynika, że są linie radiowe lub sieci radiowe, które nie są wykryte, a wykrywanie jest nieskuteczne, znaczy to, że obiekty te nie mogą być wykryte, gdyż obiekt wykrywania znajduje się od nich w odległości większe niż horyzont radiowy.

Skuteczne namierzenie obiektu powinno nastąpić wtedy, gdy obiekt jest wykryty oraz istnieją 3 wolne obiekty namierzania. Jeśli namierzanie nie przyniesie efektu, znaczy to, że obiekty namierzania będą zajęte namierzaniem innego obiektu.

Rozpoczęcie obezwładnienia zakłóceniami konkretnego obiektu mobilnego systemu łączności ZO WL powinno nastąpić wtedy, gdy obiekt ten zostanie wykryty i z reguły namierzony (nie dotyczy relacji radioliniowych), a obiekt WE przeciwnika jest wolny i nie będzie prowadził w danym momencie zakłóceń. Spełnienie tego warunku implikuje sprawdzenie, czy współczynnik zakłóceń rzeczywistych jest mniejszy od wymaganego. Dopiero wtedy może zajść powyższe zdarzenie. Brak możliwości obezwładnienia zakłóceniami danego obiektu powinno wynikać z niemożności spełnienia powyższych warunków.

Zdarzenie, które powoduje zakończenie obezwładniania zakłóceniami obiektu mobilnego systemu łączności ZO WL powinno zachodzić wtedy, gdy obiekt zakłócany podejmie skuteczne działania obronne. Jeśli obiekt ten nie podejmie takich działań, będzie w stanie obezwładnienia zakłóceniami do końca przebiegu symulacji.

W czasie symulacji użytkownik powinien być informowany o zachodzących zdarzeniach i czasie ich wystąpienia. Zastosowany mechanizm to skojarzenie zachodzących zdarzeń z systemem komunikatów, z których każdy składa się z opisu zdarzenia, obiektu generującego zdarzenia oraz obiektu, na którym skupiły się skutki zdarzenia.

Głównym realizatorem przebiegu symulacji w modelu powinna być *pętla symulacyjna*. Przed rozpoczęciem pętli należy zrealizować następujące działania:

- zainicjowanie zmiennych i kolejek dla procesu symulacji;
- wylosowanie miejsc alokacji obiektów WE przeciwnika;
- zainicjowanie licznika bieżącego czasu symulacji;
- zainicjowanie licznika czasu rzeczywistego;
- wprowadzenie na listę zdarzeń inicjujących cykl wykrywania dla wszystkich obiektów wykrywania przeciwnika (zdarzenia te zachodzą cyklicznie podczas całego przebiegu symulacji i muszą zostać zainicjowane);
- wykreślenie graficznego obrazu systemu łączności radioliniowej ZO WL.

Przebieg symulacji powinien charakteryzować się następującymi działaniami:

- odświeżanie licznika czasu rzeczywistego;
- generowanie zdarzeń;
- realizacja zdarzeń;
- nanoszenie zmian na graficzny obraz systemu radioliniowego ZO WL;
- opóźnianie przebiegu symulacji zgodnie ze współczynnikiem szybkości symulacji wprowadzanym jako parametr symulacji;
- sprawdzanie spełnienia warunków zakończenia symulacji.

Generowanie zdarzeń powinno zachodzić w każdym przebiegu pętli zgodnie z determinantami wynikającymi z rozkładów prawdopodobieństwa i następstw zdarzeń. Realizacja zdarzeń powinna obejmować pobranie pierwszego zdarzenia z uporządkowanej listy zdarzeń i zrealizowaniu skutków, jakie zdarzenie pociąga za sobą.

Nanoszenie zmian na schemacie łączności radioliniowej powinno zachodzić po realizacji każdego zdarzenia. Linie radiowe powinny być oznaczane następująco:

- linią ciągłą w kolorze czarnym – linia pracuje normalnie;
- linią przerywaną w kolorze zielonym – linia wykryta;
- linią punktową w kolorze niebieskim – wykryta i linia namierzona;
- linią ciągła w kolorze czerwonym – linia obezwładniona zakłóceniami.

Oznaczenia te pozwolą na śledzenie stanu sieci łączności radioliniowej i obserwowanie zmian zachodzących w czasie symulacji.

W modelu należy uwzględnić dwa warunki zakończenia pętli symulacyjnej:

– przekroczenie założonego czasu symulacji;

– przerwanie symulacji przez użytkownika.

Po zakończeniu symulacji powinny być zapisywane jej wyniki do odpowiednich zbiorów danych.

D. Zakończenie symulacji – powinno odbywać się powinno po upływie zadanego czasu lub gdy pojawi się komunikat o braku środków przeciwnika do prowadzenia WE.

4. ***Ocena i analiza wyników symulacji*** – faza mająca na celu interpretację wariantów organizacji systemu łączności w zależności od założonego zagrożenia, przede wszystkim poprzez prezentację oraz interpretację wyników gry (*informacji wynikowych)* dotyczących oddziaływania elektronicznego środków WE przeciwnika na MSŁ ZO WL. Wyniki symulacji powinny być zbierane w trzech tabelach reprezentowanych w modelu przez zbiory danych.

W tabeli wyników symulacji dla obiektów WE przeciwnika (załącznik 1) powinny być prezentowane dane statystyczne uzyskane wprost na podstawie przeprowadzonej symulacji oraz wskaźniki, które zostały obliczone. Do wskaźników tych powinny być zaliczone:

– skuteczność pracy obiektu wykrywania, namierzania i obezwładniania zakłóceniami;

– sposoby wykorzystania obiektu.

W tabeli wyników symulacji dla obiektów systemu łączności ZO WL, którymi są linie radiowe (załącznik 2) należy uwzględnić dane statystyczne dotyczące zliczanych zdarzeń oraz odpowiednie wskaźniki, np.:

– skuteczność pracy obiektu wykrywania, namierzania i obezwładniania zakłóceniami;

– współczynnik obezwładniania zakłóceniami.

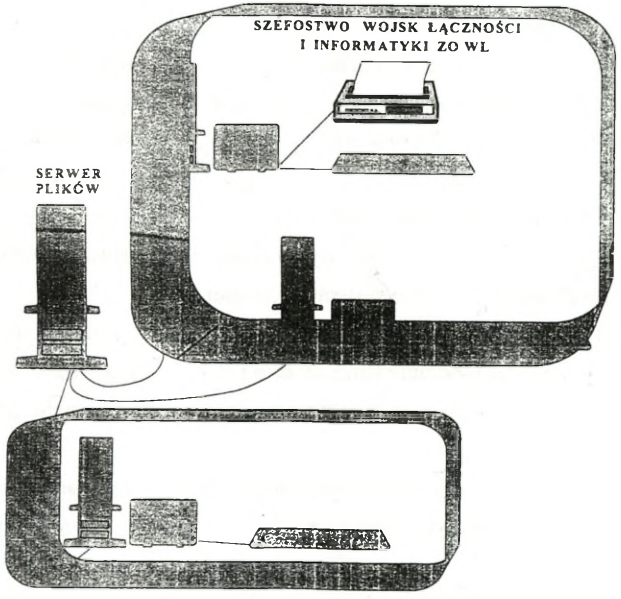
Podobne rezultaty wyników symulacji powinny dotyczyć dla sieci radiowych, których ilustrację należy przedstawić w odpowiedniej tabeli (załącznik 3).

3.6. Struktura techniczna modelu

Implementacja modelu symulacyjnego zagrożenia elektronicznego mobilnego systemu łączności związku operacyjnego WL powinna być wykonywana przy pomocy jednego z generatorów aplikacji relacyjnych baz danych.

Komputerowa egzemplifikacja modelu powinna być opracowana dla środowiska systemu operacyjnego Netware-Novell, natomiast sam model powinien być zdolny do przeniesionia w dowolne środowisko sieciowe. Konieczność pracy modelu w środowisku sieciowym podyktowana jest potrzebą równoległego wykonania czynności związanych z oceną zagrożenia elektronicznego przez różne osoby korzystające z tej samej bazy danych.

Strukturę techniczną modelu powinien stanowić komputer główny (serwer), co najmniej dwie stacje robocze oraz niezbędne urządzenia zewnętrzne (drukarka sieciowa, scaner). Topologia rozmieszczenia stacji roboczych powinna być magistralna lub gwiaździsta (rysunek 3.6.1).



Rys. 3.6.1. Struktura techniczna modelu symulacyjnego zagrożenia elektronicznego mobilnego systemu łączności ZO WL

Oprogramowanie zarządzające wymagane dla proponowanej struktury technicznej powinno obejmować:

– sieciowy system operacyjny, który powinien zostać zainstalowany na serwerze;

– środowisko Windows;

– programy usługowe dla potrzeb obsługi urządzeń peryferyjnych.

Dane na poziomie fizycznym powinny być ***szyfrowane***. Oznacza to, że teoretycznie nie będzie mogła odczytać ich osoba niepowołana przy pomocy programów narzędziowych.

Mechanizm szyfrowania należy zastosować następujący: każda tablica danych powinna otrzymać klucz szyfrowy, który szyfrowałby wprowadzane do niej dane. Klucz ten powinien być jednocześnie hasłem, dzięki któremu możliwy byłby dostęp do plików danych przy pomocy np. menadżera plików bazy danych systemu operacyjnego. Dane przekazywane między serwerem a stacjami roboczymi powinny być również zaszyfrowane, co zwiększałoby ich bezpieczeństwo i minimalizowałoby możliwość przechwytu danych podczas ich transmisji. Przedstawiony mechanizm ogranicza nie tylko możliwość przechwytu danych, ale praktycznie pozbawia sensu celowe kopiowanie ich na dyskietkę w celu odczytu na komputerze zewnętrznym. Odszyfrowanie danych z ponad 100 plików, z których każdy wykorzystuje inny klucz szyfrowy, jest wyjątkowo trudnym i czasochłonnym zadaniem. Z kolei odczytanie danych z kilku plików nie da jakiegokolwiek wyobrażenia o elementach strukturalnych i funkcjonalnych zaplanowanego systemu łączności.

Instalacja ***modelu*** w Szefostwie Wojsk Łączności i Informatyki Okręgu Wojskowego (ZO) oraz Oddziale Rozpoznania i WE (G-2) powinna przynieść – niemal natychmiast po jego oprogramowaniu i uruchomieniu – następujące korzyści:

1. Poprawę organizacji pracy planistycznej w zakresie wypracowywania decyzji do organizacji mobilnych systemów łączności o ocenę zagrożenia elektronicznego.

2. Umożliwienie obsługi dużych baz danych.

3. Wprowadzenie nowoczesnych procedur komunikacji między uczestnikami procesu: przesyłanie informacji między użytkownikami w trakcie pracy oraz wykorzystanie poczty elektronicznej.

4. Znaczne oszczędności w kosztach zakupu sprzętu i oprogramowania, które do tej pory należało zakupić dla każdego stanowiska mikrokomputerowego, a dzięki możliwości dzieleniu zasobów sieciowych można stosować tylko pojedyncze egzemplarze sprzętu lub programu.

5. Oszczędności w rozbudowie bazy mikrokomputerowej (np. do powiększenia bazy o kilka stanowisk potrzebny jest już tylko zakup stacji roboczych, a nie oprogramowania sieciowego i urządzeń peryferyjnych).

ZAKOŃCZENIE

Przedstawiana do służbowego wykorzystania praca studyjna jest kolejnym znaczącym krokiem podczas badania wpływu celowego, destrukcyjnego oddziaływania środków WE przeciwnika na funkcjonowanie mobilnego systemu łączności szczebla operacyjnego we współczesnych zbrojnych działaniach wojennych wojsk lądowych, gdyż:

1. *Dokonywana ocena zagrożenia elektronicznego mobilnego systemu łączności związku operacyjnego wojsk lądowych jest złożonym procesem decyzyjnym*, w którym ocena sytuacji prowadzi do podjęcia decyzji zapewniającej możliwość jego funkcjonowania w warunkach rosnącego oddziaływania elektronicznego środków walki elektronicznej potencjalnego przeciwnika.

2. Dokonywana ocena zagrożenia elektronicznego systemu łączności związku operacyjnego wojsk lądowych jest *procesem informacyjnym*, obejmującym gromadzenie, przetwarzanie i wymianę informacji z innymi komórkami sztabu ZO WL (np. Oddziałem Rozpoznania i WE).

3. Dokonywana ocena zagrożenia elektronicznego systemu łączności związku operacyjnego wojsk lądowych jako proces podlega ***optymalizacji*** (zysk czasowy), w wyniku wykorzystania możliwości środków informatycznych.

4. Symulacja komputerowa zagrożenia elektronicznego mobilnego systemu łączności związku operacyjnego wojsk lądowych umożliwia prowadzenie wszechstronnych jego badań w warunkach dynamicznie zmieniającej się sytuacji radioelektronicznej na współczesnym polu walki.

5. Opracowany projekt koncepcyjny stanowi podstawę do wykonania oprogramowania informatycznego modelu symulacyjnego zagrożenia elektronicznego mobilnego systemu łączności związku operacyjnego wojsk lądowych umożliwiającego realizację następujących zadań:

– prowadzenie komputerowej gry wojennej w zakresie modelowania zagrożenia elektronicznego mobilnego systemu łączności związku operacyjnego wojsk lądowych;

– ocenę zagrożenia elektronicznego planowanego systemu łączności z wykorzystaniem metody symulacji komputerowej;

– wspomaganie Szefa Wojsk Łączności i Informatyki ZO WL w podejmowaniu decyzji o organizacji łączności na szczeblu operacyjnym;

– wspomaganie czynności planistycznych zachodzących w procesie planowania systemu łączności;

– rozwiązywanie niektórych problemów współdziałania Oddziału Rozpoznania i WE z Szefostwem Wojsk Łączności i Informatyki w zakresie oceny sytuacji elektronicznej.

BIBLIOGRAFIA

1. Barczak A. i in.: *Inteligentne sieci telekomunikacyjne – aspekty metodologiczne i techniczno-projektowe.* WSOWŁ, Zegrze 1994.

2. Barczak A.: *Komputerowe gry wojenne.* Wyd. Bellona, Warszawa 1996.

3. Chwastek R., Filipiak J., Gajda M., Potempa J.: *Architektury i standardy systemów zarządzania.* Przegląd Telekomunikacyjny nr 10/1994.

4. Danecki J.: *TMN jako system zarządzania sieciami telekomunikacyjnymi.* Przegląd Telekomunikacyjny nr 10/1994.

5. Dąbrowski M., Zajdel A.: *Nowe podejście do zarządzania siecią telekomunikacyjną TPSA.* Przegląd Telekomunikacyjny nr 10/1994.

6. Gordon G.: *Symulacja systemów.* WNT, Warszawa 1974.

7. Gryciuk P.: *Doskonalenie metod oceny zagrożenia radioelektronicznego i uodpornienia systemu łączności dywizji z wykorzystaniem symulacji komputerowej.* ASG WP, Warszawa 1987.

8. Janczak J.: *Walka radioelektroniczna w działaniach operacyjnych wojsk lądowych.* AON, Warszawa 1998.

9. Koleśniak K., Huzar Z., Fryźlewicz Z.: *Symulacja komputerowa.* Wyd. Polit. Wrocław, 1976.

10. Händel M.: *Evolution of networks with ATM.* Telecom Report International nr 2/1994.

11. *Komputerowy model planowania systemu łączności związku operacyjnego wojsk lądowych.* Sprawozdanie z pracy naukowo-badawczej pod kier. prof. A. Barczaka, WSOWŁ, Zegrze 1993.

12. *Komputerowy model oceny zagrożenia radioelektronicznego systemu łączności związku operacyjnego wojsk lądowych.* Sprawozdanie z pracy naukowo-badawczej pod kier. prof. A. Barczaka, WSOWŁ, Zegrze 1996.

13. Leszczyński A., Mamcarz K.: *Komputerowe wspomaganie procesu planowania systemu łączności związku operacyjnego wojsk lądowych.* Rozprawa doktorska, AON, Warszawa 1995.

14. *Metodyki obliczeń operacyjno-taktycznych obezwładniania radioelektronicznego*, Szt. Gen. WP, Warszawa 1979.

15. Mezhvinsky A., Karneńska A.: *Radiowe systemy trankingowe.* Przegląd Telekomunikacyjny nr 5-6/1995.

16. *Modelowanie systemu łączności Sił Zbrojnych RP – metodologiczne i organizacyjne podstawy wykonania pracy naukowo badawczej.* Praca zespołowa pod kier. prof. A. Barczaka, WSOWŁ, Zegrze 1993.

17. *Mobile Subscriber Equipment Commander's Brief.* Wyd. GTEMSED, Taunton, 1991.

18. *Perspektywiczny system łączności związku operacyjnego wojsk lądowych.* Sprawozdanie z pracy naukowo-badawczej pod kier. prof. A. Barczaka. WSOWŁ, Zegrze 1995.

19. Rotkiewicz W. i inni: *Kompatybilność elektromagnetyczna w radiotechnice*, WKiŁ, Warszawa 1978.

20. Wojnar A.: *Systemy radiokomunikacji ruchomej lądowej.* Wyd. KiŁ, Warszawa 1989.

Załącznik 1

Wzór tabeli wyników symulacji dla obiektów WE przeciwnika

Typ obiektu	Rodzaj pracy	Liczba wykryć pomyślnych		Liczba wykryć niepomyślnych		Skuteczność wykrywania	Liczba namierzeń pomyślnych		Liczba namierzeń niepomyślnych		Skuteczność namierzania	Liczba pomyślnych zakłóceń		Liczba niepomyślnych zakłóceń		Skuteczność zakłócania	Czas zakłócania	Wykorzystanie obiektu [%]
-	-	sieci	linie	sieci	linie	-	sieci	linie	sieci	linie	-	sieci	linie	sieci	linie	-	-	-

Załącznik 2

Wzór tabeli wyników symulacji dla obiektów mobilnego systemu łączności ZO WL – linie radiowe

Linia radiowa		Długość linii [km]	Zakres	Liczba wykryć	Liczba namierzeń	Liczba zakłóceń	Skuteczność wykrywania	Skuteczność namierzania	Skuteczność obezwładniania zakłóceniami	Czas obezwładniania zakłóceniami	Współczynnik zakłóceń
Węzeł 1	Węzeł 2	-	-	-	-	-	-	-	-	-	-

Załącznik 3

Wzór tabeli wyników symulacji dla obiektów mobilnego systemu łączności ZO WL – sieci radiowe

Sieć radiowa	Zakres	Liczba wykryć	Liczba namierzeń	Liczba zakłóceń	Skuteczność wykrywania	Skuteczność namierzania	Skuteczność obezwładniania zakłóceniami	Czas obezwładniania zakłóceniami	Współczynnik zakłóceń