CENTRUM INFORMATYKI

Nr 2

Sztabu Generalnego Wojska Polskiego

1994 - 1999

Biuletyn Jubileuszowy

NR 2

CENTRUM INFORMATYKI

Sztabu Generalnego Wojska Polskiego

1994 - 1999

Biuletyn Jubileuszowy

CENTRUM INFORMATYKI SZTABU GENERALNEGO WP

Biuletyn Jubileuszowy (nr 2)

ZESPÓŁ REDAKCYJNY
Płk Andrzej Grochalski
Ppłk Stanisław Dąbrowski
Pan Jerzy Dominiak
Ppor. Jarosław Kopczyński

Centrum Informatyki
Sztabu Generalnego Wojska Polskiego
00-911 Warszawa 62 skr. poczt. 25 • ul. Nowowiejska 28a
Tel. 825.66.55 • Fax 825.66.55

Październik 1999

Drogi Czytelniku

Oddajemy do Twoich rąk drugi numer biuletynu Centrum Informatyki Sztabu Generalnego WP. Wydanie to jest dedykowane dla Wszystkich Sympatyków Informatyki i przypada na okres naszego skromnego Jubileuszu V-lecia Centrum.

Dziękuję za wszystkie słowa otuchy i uznania dla działalności Centrum. Dziękuję również za słowa konstruktywnej krytyki i wskazania do dalszych działań. Zarówno jedne, jak i drugie są motywacją do stanowienia lepszego jutra informatyki wojskowej.

Zapraszam do publikowania w naszym biuletynie wszystkich kontrowersyjnych ocen i propozycji. Proszę, aby biuletyn stał się forum dyskusyjnym dawców i BIORCÓW rozwiązań informatycznych.

Pozdrawiam Wszystkich Naszych Czytelników.

Komendant
Centrum Informatyki
Sztabu Generalnego WP

płk dr inż. Piotr Zaskórski

Warszawa, 09.09.1999 r.

MINISTER OBRONY NARODOWEJ

CENTRUM INFORMATYKI
SZTABU GENERALNEGO WP

Dynamiczny rozwój technologii elektronicznej spowodował powstanie przemysłu komputerowego jako nowoczesnej i rewolucyjnej gałęzi. Jej rozwój, a szczególnie miniaturyzacja urządzeń komputerowych, stworzyła nową dziedzinę działalności ludzkiej, jaką jest informatyka. Automatyzacja systemów informacyjnych poprzez programowanie urządzeń komputerowych, wykorzystywanych do przetwarzania, przechowywania, przesyłania i udostępniania informacji w formie oczekiwanej przez użytkowników -zmieniła obraz współczesnego świata. Postęp w tej dziedzinie spowodował zmiany kulturowe mające istotny wpływ na codzienną działalność poszczególnych osób w ramach instytucji, instytucji w państwie i państwa w skali globalnej. Przykładem tych zmian może być Internet, który w ostatnich kilku latach stał się dominującym środkiem komunikacji miedzy ludźmi na całym świecie oraz medium do powszechnego przekazywania i pozyskiwania informacji.

Analiza dorobku informatyki wojskowej uzmysławia, że Wojsko Polskie dotrzymuje kroku armiom innych państw należących do NATO. Rozwiązania techniczne i stan przygotowania kadr w dziedzinie zastosowań informatyki mogą zapewnić odpowiedni poziom interoperacyjności we współdziałaniu z siłami zbrojnymi naszych partnerów z NATO.

Z okazji Jubileuszu Centrum Informatyki Sztabu Generalnego WP składam serdeczne podziękowania i gratulacje za znaczące osiągnięcia w dziedzinie mającej duże znaczenie dla obronności oraz życzę wielu dalszych sukcesów.

Janusz ONYSZKIEWICZ

KOMENDANT
CENTRUM INFORMATYKI
SZTABU GENERALNEGO WP
Pan płk Piotr ZASKÓRSKI
00-911 Warszawa

Efektywne zarządzanie logistyką wojskową wymaga sprawnego systemu informacyjnego, dostarczającego decydentom informacji o potrzebach użytkowników, stanie zapasów, źródeł zaopatrzenia oraz o normach zużycia wykorzystywanych dla czynności planistycznych i prognostycznych logistyki produkcyjnej i konsumpcyjnej. Wymogom tym może jedynie sprostać komputerowo wspomagany system logistyki, dostosowany do potrzeb ogniw wykonawczych i zarządzających wszystkich szczebli logistyki tworzących system zintegrowany.

Z okazji jubileuszu informatyki wojskowej należy podkreślić, że w dziedzinie informatyzacji logistyki zrobiono najwięcej, ale jest to jednak za mało w stosunku do zmieniających się potrzeb w tej dziedzinie. Informatyzacja tej problematyki może przynieść wymierne korzyści ekonomiczne w okresie pokojowym, a w okresie zagrożenia i wojny może decydować o powodzeniu działań operacyjnych. Do najważniejszych zadań, które należy wykonać w pierwszej kolejności zalicza się;

- indeksację materiałów, uzbrojenia i usług, standaryzację procedur obsługi logistycznej zgodnej ze standardami NATO;
- opracowania koncepcji zintegrowanego systemu informatycznego logistyki;
- ewidencję zasobów logistycznych sił zbrojnych i gospodarki narodowej przydatnych do wykorzystania dla potrzeb obronnych.

Dla wszystkich informatyków wojskowych doskonalących systemy szeroko rozumianej logistyki, pragnę złożyć podziękowanie i przekazuję życzenia intensyfikacji procesu informatyzacji tej dziedziny działalności obronnej.

SEKRETARZ STANU I ZASTĘPCA
MINISTERA OBRONY NARODOWEJ

R. Szeremietiew

Dr Romuald SZEREMIETIEW

Komendant
Centrum Informatyki
Sztabu Generalnego WP

Pan płk Piotr Zaskórski

Szanowny Panie Pułkowniku

Z okazji piątej rocznicy utworzenia Centrum Informatyki Sztabu Generalnego WP pragnę przekazać na ręce Pana Pułkownika serdeczne gratulacje i pozdrowienia dla wszystkich żołnierzy i pracowników podległej Panu instytucji.

Zwłaszcza dzisiaj, gdy Polska jest członkiem NATO, działalność centrum na rzecz projektowania i wdrażania nowoczesnych technologii informatycznych w systemach dowodzenia i kierowania w Sitach Zbrojnych Rzeczypospolitej Polskiej stanowi o sprawności systemu informacyjnego w wojsku.

W tak wyjątkowym i uroczystym Dniu życzę Panu Pułkownikowi, żołnierzom i pracownikom Centrum Informatyki Sztabu Generalnego WP dalszych sukcesów i satysfakcji w służbie oraz pełnej realizacji osobistych zamierzeń i aspiracji życiowych.

SZEF
SZTABU GENERALNEGO WP

gen. bron Henryk SZUMSKI

Warszawa, 19 października 1999 r

KOMENDANT
CENTRUM INFORMATYKI
SZTABU GENERALNEGO WP
Pan płk Piotr ZASKÓRSKI
00-911 Warszawa

Utrwala się przekonanie, że istnieje konieczność nadania najwyższego priorytetu dla zadań związanych z zastosowaniem informatyki w resorcie obrony narodowej, a przede wszystkim dla:

- *koncepcji organizacji planowania, funkcjonowania rozwoju wojskowych systemów informatycznych i teleinformatcznych;*
- *przedsięwziąć związanych z osiągnięciem polskich celów interoperacyjności z NATO i państwami biorącymi udział w programie „Partnerstwo dla Pokoju" w zakresie systemów łączności i informatyki oraz procedur wymiany informacji;*
- *rozwoju bazy technicznej, technologicznej systemów informatycznych i teleinformatycznych oraz bezpieczeństwa informatycznego, a w tym inicjowania, organizowania, koordynowania przedsięwzięć związanych z normowaniem, standaryzacją i wdrażaniem informatycznych rozwiązań technicznych, programowych i proceduralnych.*

Z okazji jubileuszu Centrum Informatyki Sztabu Generalnego WP należy z satysfakcją stwierdzić, że wszystkie organa informatyki wojskowej dobrze wypełniły swoją misję, o czym w szczególności może świadczyć dobre przygotowanie użytkowników do korzystania z rozwiązań komputerowych i ich przygotowanie do działania w ramach struktur NATO. W okresie restrukturyzacji Sił Zbrojnych RP - informatyka, będąca wiodącą dziedziną doskonalenia procesów informacyjnych, musi dostosować się do zmian i rozwiązać problemy:

- *opracowania procedur planowania i finansowania przedsięwzięć w dziedzinie informatyki;*
- *dostosowania cyklu życia systemów informatycznych w resorcie obrony narodowej do rekomendacji i standardów NATO;*
- *przekształcenia strukturalnego organów informatyki wojskowej związanego ze zmianami strukturalnymi sił zbrojnych;*
- *projektowania i wdrażania rozwiązań informatycznych we współpracy z partnerami z NATO i komercyjnymi instytucjami krajowymi i zagranicznymi.*

Kadrze i pracownikom wojska Centrum Informatyki Sztabu Generalnego WP przekazuję podziękowania za dobrze wypełnione zadania oraz życzę utrwalenia pozycji pełnowartościowego partnera w ramach struktur NATO.

SZEF ZARZĄDU
ŁĄCZNOŚCI I INFORMATYKI SG WP

Gen. bryg. Wojciech WOJCIECHOWSKI

SZEF ZARZĄDU GENERALNEGO
DOWODZENIA ŁĄCZNOŚCI SG WP

Gen. bryg. Wojciech KUBIAK

Szanowni Państwo

Minęło pięć lat od przekształcenia Wojskowego Instytutu Informatyki w Centrum Informatyki SG WP. Sądzę, że jest to doskonała okazja aby podjąć próbę oceny dorobku tej zasłużonej dla Sił Zbrojnych RP Instytucji. Mniemam, że najwłaściwszą merytorycznie ku temu perspektywę wyznaczają trzy szczególne wydarzenia, które miały miejsce właśnie w ostatnim pięcioleciu.

Pierwsze z nich, to przygotowanie w 1994 r. przez Grupę na Wysokim Szczeblu do Spraw Społeczeństwa Informacyjnego Rekomendacji dla Rady Europy, zwanych raportem Bangemana. Stwierdza się w nim między innymi:

„Informacja i technologie komunikacyjne są źródłem nowej rewolucji. Jest to rewolucja oparta na informacji będącej wyrazem ludzkiej wiedzy. Postęp technologiczny pozwala nam dziś przetwarzać, wyszukiwać i przesyłać informacje niezależnie od sposobu jej zapisu – słownego, pisemnego czy obrazkowego, bez przeszkód stawianych przez czas, odległość i objętość. Rewolucja ta udostępnia nowe, wielkie możliwości ludzkiej inteligencji i tworzy zasoby, które zmienią sposoby naszej wspólnej pracy i życia"

Wyniesienie informacji do roli nośnika nowej rewolucji na miarę rewolucji przemysłowej stanowi więc szczególne wyzwanie dla wszystkich instytucji kreujących rozwój i zastosowanie technologii informacyjnych, a więc i także dla obchodzącego dzisiaj swoje święto Centrum Informatyki.

Kolejnym nie mniej ważnym wydarzeniem, chociaż tylko o zasięgu krajowym, był II Kongres Informatyki Polskiej, który obradował w grudniu ubiegłego roku w Poznaniu. Wynikiem jego prac było opublikowanie raportu pt. „Strategia Rozwoju Informatyki w Polsce – stan, zadania, perspektywy". W raporcie tym podkreśla się, że:

- *Szybki rozwój informatyki w Polsce jest zgodny z polską racją stanu;*
- *Powstanie globalnego społeczeństwa informacyjnego jest nieuniknione. Dominującym symbolem przyszłego społeczeństwa informacyjnego będzie nie maszyna lecz informacja;*
- *Polska należy do nielicznej grupy krajów, w której rozwój społeczeństwa informacyjnego traktowany jest marginesowo.*

Konstatując powyższe, nie może być wątpliwości, że społeczność informatyków wojskowych powinna włączyć się do budowy społeczeństwa informacyjnego, a więc także infomacyjnej armii, przygotowując do tego aktualnego i potencjalnego użytkownika, jak też stosowne rozwiązania techniczno-programowe.

Ostatnim wydarzeniem, znaczenie którego trudno dzisiaj przecenić, było przystąpienie Rzeczypospolitej Polskiej do Traktatu Północno-Atlantyckiego. Poza wszelkimi innymi aspektami, oznacza ono ukierunkowany i zdynamizowany rozwój

systemów łączności i informatyki, niezbędnych do efektywnego funkcjonowania SZ RP w strukturach NATO. Wymusza ono ponadto, konieczność spełnienia nowych wymagań i standardów oraz szerszy dostęp do nowych technologii, a także co należy podkreślić, przeniesienie na wyższy poziom konkurencyjności proponowane przez nas rozwiązania organizacyjne, programowo-techniczne, koncepcyjno-projektowe i wdrożeniowe. Istotnego znaczenia nabierze również skuteczne współdziałanie w dziedzinie militarnych zastosowań technologii informacyjnych.

Jestem przekonany, że wszystkie ze wspomnianych wydarzeń wyznaczały, chociaż z pewnością w różnym stopniu, istotę, treść i charakter realizowanych przez Centrum Informatyki prac projektowo-wdrożeniowych i badawczo-naukowych. Kształtowały one niejako profesjonalne i formalne otoczenie tej działalności. Najważniejszym jednak i zasadniczym, niejako strukturalnym komponentem wspomnianej działalności były i są Siły Zbrojne. Nie miejsce i okoliczność uzasadniające szczegółową analizę wszystkiego tego co istotnie wyróżniało ich charakter w ostatnim pięcioleciu. Uważam jednak, że przy okazji tak doniosłego Jubileuszu należy zasygnalizować tylko te problemy funkcjonowania SZ RP, które w istotny sposób determinowały skalę i charakter realizowanych przedsięwzięć informatycznych, warunkowały efektywność rozwoju i wdrożeń technologii informacyjnych. Sądzę, że w ostatnich latach charakteryzowała je znaczna dynamika zmian organizacyjno-funkcjonalnych i strategiczno-doktrynalnych. Posiadały więc one cechy typowe dla armii okresu przejściowego. Wyróżniały się ponadto znacznym niedoinwestowaniem i opóźnieniem w rozwoju i wykorzystaniu globalnej infrastruktury teleinformatycznej z wszystkimi wynikającymi z tego konsekwencjami. A więc autonomicznością i jednoszczeblowością zastosowań większości aplikacji informatycznych oraz brakiem efektywnego dostępu do poza militarnych zasobów informacyjnych. W tym czasie dały z całą siłą znać o sobie również prawa rynku, który wchłonął znaczącą ilość doskonale przygotowanej kadry wojskowych informatyków. Nie bez znaczenia było także często niedostrzeganie potrzeby pełnej korelacji strategicznych programów rozwoju poszczególnych komponentów i obszarów funkcjonalnych Sił Zbrojnych ze strategią ich kompleksowej informatyzacji. Wszystko to nie zawsze sprzyjało efektywnej eksploatacji, wdrażaniu i projektowaniu systemów informatycznych.

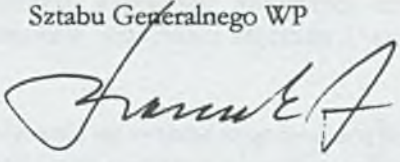
Taki stan rzeczy jak sądzę jest już za nami. Podjęte w ostatnich latach strategiczne decyzje w zakresie rozwoju infrastruktury teleinformatycznej (m.in. budowa globalnych rozległych sieci komputerowych) a także postępująca stabilizacja w sferze organizacyjno-funkcjonalnej, stwarzają warunki do efektywniejszego wykorzystania posiadanych systemów oraz zintensyfikowania prac projektowych nad hierarchicznymi, zintegrowanymi, strategicznie ważnymi systemami informatycznymi Sił Zbrojnych. Realizacja tak złożonego przedsięwzięcia będzie oczywiście możliwa tylko i wyłącznie przy pełnej koncentracji potencjału wykonawczego Centrum Informatyki na strategicznie ważnych i wysoce specjalistycznych informatycznych systemach wspomagania dowodzenia i kierowania SZ RP. Towarzyszyć temu powinny również intensywne prace nad integracją i modyfikacją wszystkich aktualnie eksploatowanych aplikacji i systemów

informatycznych, które w nowych uwarunkowaniach organizacyjnych i funkcjonalnych, a nade wszystko technicznych wymagały będą nowych, kompleksowych rozwiązań. Trudno nie zauważyć także potrzeby intensywnego i ciągłego rozpoznawania rynku i osiągnięć naukowych w dziedzinie technologii informatycznych, a także lepszego niż dotychczas dostosowania ich do wymagań i uwarunkowań SZ RP. Dużego znaczenia nabierać będzie także współudział w realizacji doktryny bezpieczeństwa informacyjnego oraz w rozwoju, utrzymywaniu i zarządzaniu zasobami teleinformatycznymi.

Dokonana przeze mnie, z okazji jubileuszu V-lecia Centrum Informatyki SG WP, próba przybliżenia uwarunkowań, problemów i specyfiki realizowanych oraz planowanych zadań jakie stoją przed Centrum Informatyki miała w istocie jeden cel – a mianowicie, zaakcentować, jak ważną funkcję w strukturze Sił Zbrojnych spełnia efektywnie funkcjonujący, Centralny Organ Wykonawczy Informatyki.

Przekonaniu, że wyjawiony przed Państwem zamiar udało mi się chociaż częściowo zrealizować, towarzyszą najlepsze życzenia, pełnej satysfakcji z wszystkich podejmowanych „informatycznych" działań, dla Komendanta i pracowników Centrum Informatyki SG WP.

Zastępca Szefa
Zarządu Łączności i Informatyki
Sztabu Generalnego WP



płk prof. dr hab. inż. Andrzej BARCZAK

1

1. Historia powstania informatyki wojskowej i jej zrębów instytucjonalnych

gen. dyw. w st. spocz. dr inż. Marian Pasternak

Na przełomie lat 50-tych i 60-tych, kierownictwo MON uznało za celowe i konieczne podjęcie prac nad doskonaleniem struktur organizacyjnych i wyposażeniem technicznym Sił Zbrojnych w celu poprawy efektywności dowodzenia wojskami na polu walki a także (a może w tym czasie przede wszystkim) usprawnienie efektywności zarządzania we wszystkich dziedzinach pokojowej działalności Sil Zbrojnych, szczególnie w gospodarce materiałowo-technicznej, w problematyce etatowo-mobilizacyjnej, kadrowej, finansowej itp.

Był to okres kiedy z jednej strony rozwój środków bojowych pod koniec II wojny światowej i po jej zakończeniu znacznie wyprzedzał możliwości efektywnego ich wykorzystania ze względu na ograniczone możliwości zbierania i szybkiej obróbki niezbędnych do tego celu informacji.

Z drugiej strony podobnie ukształtowała się sytuacja w gospodarce pokojowej, gdyż przy dużym postępie w mechanizacji i automatyzacji procesów roboczych systemy zarządzania podległy znacznie wolniejszym udoskonaleniom.

Decyzji o podjęciu prac nad doskonaleniem dowodzenia i zarządzania Siłami Zbrojnymi sprzyjał fakt, że w drugiej połowie lat 50-tych zostały stworzone większe możliwości dostępu do fachowej zachodniej literatury z dziedziny techniki obliczeniowej oraz zastosowania metod matematycznych w rozwiązywaniu problemów decyzyjnych, optymalizujących efekty działalności (skrócenie czasu reakcji, oszczędniejsze wykorzystanie środków materiałowych i finansowych, lepsze wykorzystanie kadr, usprawnienie struktur organizacyjnych itp.).

Przykładem takich działań były utworzone w czasie II wojny światowej naukowe zespoły specjalistów dla opracowania metod efektywnego wykorzystania sprzętu bojowego, tzw. grupy badań operacyjnych.

Realizacja celu określonego przez MON wymagała podjęcia odpowiednich przygotowań organizacyjnych, rozpoczęcia prac naukowo-badawczych, a przede

wszystkim rozpoczęcia szkolenia kadr specjalistów informatyki, a także przyszłych potencjalnych użytkowników, będących jednocześnie współtwórcami informatyzowanych systemów dowodzenia i zarządzania. W dalszej kolejności realizacja wymagała również rozpoczęcia prac inwestycyjnych.

Pierwszy krok uczyniono w sferze naukowo-badawczej. W 1959 r. Pion Techniczny Sztabu Generalnego WP podpisał umowę z Instytutem Maszyn Matematycznych na pracę naukowo-badawczą o kryptonimie "ŻÓŁW" nt. "Koncepcji zastosowania środków automatyzacji i mechanizacji w Siłach Zbrojnych". Praktycznie w realizacji ograniczono się do sfery materiałowo-technicznego zabezpieczenia - ogólnie do gospodarki materiałowej. Praca ta dała jednak początek współpracy wojska z krajowymi placówkami naukowo-badawczymi, a w perspektywie, współpracy z tworzonymi w WP instytucjami naukowo-badawczymi i projektowo-wdrożeniowymi.

Pierwszą taką instytucją, współpracującą z Instytutem Maszyn Matematycznych, był **Oddział ds. Automatyzacji Sztabu Generalnego WP** utworzony w 1961 r. w składzie 28 osób, który tworzyły:

- Wydział zastosowań elektronicznych maszyn cyfrowych (EMC);
- Wydział zastosowań maszyn licząco-analitycznych (ML-A);
- Wydział metod matematycznych.

Oddział ten w oparciu o pracę "ŻÓŁW" przystąpił do praktycznej realizacji systemu przetwarzania informacji w dziedzinie gospodarki częściami zamiennymi w jednej ze służb.

Dla kompleksowego przeanalizowania całości problemu doskonalenia struktur organizacyjnych w 1961 r. została powołana rozkazem (MON 0113/Org.) specjalna Komisja. Zaproponowała ona m.in. utworzenie Pionu Zabezpieczenia Dowodzenia, uzasadniając to tym, "że obecna struktura organizacyjna nie zapewnia kompleksowych zmian, jakie będą sukcesywnie wprowadzane pod naporem postępu ogólnego i unowocześniania systemu dowodzenia i zarządzania. Istnieje zatem obiektywna konieczność rozwinięcia stałej, wszechstronnej i planowej pracy badawczej nad sposobem i metodami doskonalenia całego systemu dowodzenia i zarządzania, przy czym działalność ta będzie wymagać specjalistycznych dociekań o charakterze operacyjno-organizacyjnym".

Komisja proponowała aby działalność tą koordynował nowo powołany Zastępca Szefa Sztabu Generalnego ds. Systemów Dowodzenia, któremu przewidywano powierzyć kierownictwo pracami badawczymi nad usprawnieniem systemu dowodzenia i zarządzania, stosownie do potrzeb operacyjnych, ogólny nadzór nad rozwojem automatyzacji i mechanizacji oraz koordynacji prowadzonych w wojsku prac naukowo-badawczych o charakterze operacyjno-organizacyjnym.

W Pionie Zabezpieczenia Dowodzenia zaproponowano utworzenie:

- Zespołu do spraw Systemów Dowodzenia
- Biura Automatyzacji i Mechanizacji
- Zarządu Administracyjno-Normatywnego

Zespół do spraw Systemów Dowodzenia miał być przeznaczony do realizacji zadań związanych z opracowywaniem perspektywicznego modelu kierowania siłami zbrojnymi, prowadzenia prac badawczych, a także koordynacji ogólnowojskowych badań, prowadzonych w zakładach naukowych, dowództwach i instytucjach, związanych z dowodzeniem i zarządzaniem.

Biuro do spraw Automatyzacji i Mechanizacji miało kierować rozwojem i wdrażaniem automatyzacji i mechanizacji do procesów dowodzenia i zarządzania siłami zbrojnymi, koordynować działalność centralnych organów zaopatrzenia w zakupie i dystrybucji urządzeń automatyzacji i mechanizacji, sprawować ogólny nadzór nad wdrażaniem i użytkowym zastosowaniem opracowań w tej dziedzinie, organizować szkolenie kadr dla potrzeb automatyzacji i mechanizacji.

Komisja widziała na tym etapie celowość utworzenia organu doradczego przy szefie Sztabu Generalnego WP - **Komitetu do spraw Usprawnień Dowodzenia**, w skład którego mieli wejść zastępcy szefa Sztabu Generalnego WP, zastępcy Głównego Inspektora Techniki i Planowania, szefowie zarządów : operacyjnego, wywiadowczego, organizacyjnego, szefowie: Zespołu Planowania Operacyjno-Obronnego Działów Komitetu Obrony Kraju, Inspektoratu Szkolenia, Inspektoratu Obrony Terytorialnej, Wojsk Łączności, Sztabu Głównego Kwatermistrzostwa WP oraz szefowie sztabów rodzajów sił zbrojnych.

Ponadto w ramach reorganizacji Zarządu VII Sztabu Generalnego proponowano utworzyć Zespół ds. Koordynacji Wojskowych Badań Ekonomicznych z wyłączonego z tego zarządu Wydziału Badań Wojskowo-Ekonomicznych oraz Oddziału ds. Automatyzacji.

Komisja uznała za niewłaściwe dokonanie w krótkim okresie czasu radykalnej przebudowy modelu kierowania siłami zbrojnymi i zaproponowała sukcesywne realizowanie przedstawionych propozycji w procesie permanentnej działalności usprawnieniowej prowadzonej na szczeblu centralnym, okręgowym, a w pewnych dziedzinach i taktycznym.

Wnioski wynikające z prac Komisji, a dotyczące zastosowania elektronicznej techniki obliczeniowej w doskonaleniu procesów dowodzenia i zarządzania w Wojsku Polskim, zostały zapoczątkowane rozkazem MON nr 02/MON z dnia 29.01.1962 r. oraz zarządzeniem wykonawczym szefa Sztabu Generalnego WP nr 017/Sztab z 2 marca 1962 r.

Zadania nakreślone w tych dokumentach obejmowały głównie przedsięwzięcia mające doprowadzić do stworzenia w latach 1962-1965 właściwych warunków organizacji dwuszczeblowego stacjonarnego systemu automatycznego przetwarzania danych dla potrzeb dowodzenia wojskami i zarządzania gospodarką wojskową. Szczególny nacisk położono na przygotowanie kadr technicznych oraz zabezpieczenie sieci łączności i transmisji danych dla potrzeb systemu automatyzacji i mechanizacji.

W wyniku realizacji ustaleń powyższych dokumentów, stworzone zostały w siłach zbrojnych podstawowe elementy bazy organizacyjno-technicznej i szkoleniowej rozwoju automatyzacji i mechanizacji. Pod koniec 1965 r. istniało:

- 7 organów sztabowych szczebla centralnego;
- Instytut Organizacji i Techniki Dowodzenia Akademii Sztabu Generalnego (powołany zarządzeniem MON nr 021 z 27 lipca 1964 r.);
- 6 ośrodków obliczeniowych, wyposażonych w 6 komputerów;
- 3 stacje maszyn licząco-analitycznych eksploatujących 6 zestawów ML-A.

Zabezpieczona została też baza szkoleniowo-kadrowa.

Niestety, mimo tak ogromnego wysiłku organizacyjnego, efekty działalności były niewspółmierne do oczekiwań. Wynikało to ze słabej koordynacji i jednolitej myśli przewodniej. Wynikała stąd konieczność dalszych zmian organizacyjnych, technicznych i szkoleniowych.

Najistotniejsze zmiany zostały wprowadzone w Sztabie Generalnym WP w latach 1966-1970. Utworzono stanowisko **Zastępcy Szefa Sztabu Generalnego WP ds. Systemów Kierowania**, któremu podporządkowano dwie jednostki organizacyjne:

- **Zarząd Normatywno-Administracyjny** sformowany w styczniu 1967 r. o stanie osobowym 62 wojskowych i 24 pracowników cywilnych. Skupione zostały w nim zadania planowania zasadniczych przedsięwzięć MON i Sztabu Generalnego WP, usprawnienia organizacji pracy i bieżącego zarządzania oraz systemu sprawozdawczości. Miał on także realizować przedsięwzięcia obejmujące strukturalno-funkcjonalne doskonalenie systemu kierowania siłami zbrojnymi;
- **Biuro ds. Automatyzacji i Mechanizacji** (BAiM) zostało utworzone w sierpniu 1966 r. (zarządzeniem Szefa Sztabu Generalnego WP nr 0110/Org. z 5.08.1966 r.). Powstało na bazie Oddziału Automatyzacji Zarządu Technicznego Sztabu Generalnego WP i w 1967 r. zostało podporządkowane Zastępcy Szefa Sztabu Generalnego WP do spraw Systemów Kierowania. Stan osobowy biura liczył 35 wojskowych i 6 pracowników cywilnych. Jego celem było stworzenie lepszych warunków do kompleksowego planowania, koordynowania, nadzorowania przedsięwzięć organizacyjnych, technicznych, inwestycyjnych i szkoleniowych w zakresie zastosowań informatyki.

W 1974 r. Biuro ds. Automatyzacji i Mechanizacji zostało podniesione do rangi **Zarządu XIV (Informatyki) Sztabu Generalnego WP**, co zwiększyło jego możliwości oddziaływania na realizację całokształtu przedsięwzięć związanych z wdrożeniem techniki obliczeniowej do praktyki w dowodzeniu i zarządzaniu.

W tym okresie poprzez utworzenie etatowej struktury hierarchicznej stworzono lepsze warunki organizacyjne rozwoju automatyzacji i mechanizacji procesów kierowania. W zarządach Sztabu Generalnego WP i większości instytucji centralnych (IC) MON sformowano oddziały lub wydziały automatyzacji i mechanizacji. W niektórych instytucjach centralnych - m.in. w departamentach i szefostwach Głównego Kwatermistrzostwa WP - utworzono stanowiska starszych inspektorów do spraw automatyzacji i mechanizacji.

W drugiej połowie lat sześćdziesiątych automatyzacją i mechanizacją procesów dowodzenia i zarządzania objęto okręgi wojskowe i rodzaje sił zbrojnych. W sztabach OW utworzono wydziały, a w sztabach rodzajów sił zbrojnych oddziały systemów kierowania. Do końca 1970 r. sformowano łącznie w IC MON, dowództwach OW i rodzajach sił zbrojnych 34 sztabowe komórki automatyzacji i mechanizacji liczące ogółem 172 stanowiska etatowe.

Pod kierownictwem BAiM WP, a później Zarządu XIV Informatyki Sztabu Generalnego, wymienione sztabowe organy informatyki kierowały rozwojem automatyzacji i mechanizacji w siłach zbrojnych, a jednocześnie były swoistym łącznikiem pomiędzy organami wykonawczymi a użytkownikami, czyli dowództwami, sztabami i instytucjami korzystającymi w procesie kierowania z elektronicznej techniki obliczeniowej (ETO). Organy wykonawcze świadczyły użytkownikom dwa podstawowe rodzaje usług, tj. projektowanie i wdrażanie rozwiązań informatycznych oraz bieżące, na ogół cykliczne, przetwarzanie danych dla potrzeb kierowania.

Zasadniczą rolę w dalszym rozwoju informatyki odgrywały organy wykonawcze szczebla centralnego ukierunkowane na działalność projektową i naukowo-badawczą dla potrzeb całych sił zbrojnych.

W tym czasie były nimi:

- **Instytut Dowodzenia Akademii Sztabu Generalnego (ID ASG)** przemianowany z Instytutu Organizacji i Techniki Dowodzenia ASG na podstawie zarządzenia Szefa Sztabu Generalnego WP nr 153 z dnia 10 grudnia 1966 r. Zadaniem jego było rozwiązywania zadań z zakresu automatyzacji i mechanizacji informacyjnych procesów dowodzenia w problematyce operacyjnej systemu terytorialnego i polowego. W końcu 1970 r. liczył 172 etaty;
- **Instytut Automatyzacji Systemów Zarządzania Wojskowej Akademii Technicznej (IASZ)** powołany zarządzeniem Ministra Obrony Narodowej nr 08/MON z 25 marca 1967 r. (zarządzenie wykonawcze Szefa Sztabu

Generalnego WP nr 099/Org. z 21 lipca 1967 r.). Powstał on na bazie Biura Maszyn Matematycznych WAT oraz niektórych organów wykonawczych informatyki Sztabu Generalnego WP. Instytut był przeznaczony do rozwiązywania zadań z zakresu automatyzacji systemów zarządzania, głównie obejmujących problematykę organizacyjną, mobilizacyjną, kadrową, kwatermistrzowską oraz zaopatrzenia materiałowo-technicznego. W końcu 1970 r. liczył 228 etatów.

Powołane instytuty zostały podporządkowane komendantom akademii, a ogólny nadzór nad ich działalnością merytoryczną został powierzony Szefowi Sztabu Generalnego WP poprzez Biuro do spraw Automatyzacji i Mechanizacji, a następnie od 1974 r. przez Zarząd Informatyki Sztabu Generalnego WP.

Zarządzeniem Szefa Sztabu Generalnego WP nr 064/Sztab z dnia 29 lipca 1967 r. dotychczasowy Ośrodek Maszynowego Przetwarzania Danych Sztabu Generalnego WP przemianowano na **Centralny Ośrodek Przetwarzania Informacji (COPI) MON**, a w roku 1971 na podstawie zarządzenia Szefa Sztabu Generalnego WP nr 056/Org. z 18 września 1971 r. utworzono **Ośrodek Przetwarzania Informacji Głównego Kwatermistrzostwa WP** (10 stanowisk wojskowych i 69 cywilnych) na bazie dotychczasowej Stacji Maszyn Licząco-Analitycznych Głównego Kwatermistrzostwa WP.

Ponadto w latach 1966-1975 utworzono 13 organów wykonawczych w OW, RSZ, niektórych IC MON oraz w instytutach wojskowych i wyższych szkołach oficerskich. Ogółem w końcu 1970 r. istniało w siłach zbrojnych 21 Ośrodków Przetwarzania Informacji (OPI) i Ośrodków Obliczeniowych (OObl.), w których zainstalowano 23 komputery i 12 zestawów maszyn licząco-analitycznych. Moc obliczeniowa zainstalowanej techniki cyfrowej w porównaniu z 1965 r. wzrosła 4-krotnie, a organy wykonawcze informatyki (instytuty, OPI i OObl.) posiadały w tym czasie **łącznie 1043 stanowisk etatowych**.

Dla realizacji zadań związanych z tworzeniem struktur organizacyjnych (sztabowych i wykonawczych) w dziedzinie informatyzacji Sił Zbrojnych zachodziła pilna potrzeba wykształcenia wyspecjalizowanych kadr analityków, projektantów, programistów i personelu technicznego, a także w niezbędnym zakresie przyszłych użytkowników wdrażanych systemów i urządzeń.

Problem ten rozwiązywano dwukierunkowo. W pierwszym rzędzie należało przygotować (przekwalifikować) kadrę wykładowczą, a także kadrę kierowniczą, przygotowującą instytucje MON do wdrażania nowych metod i technik zarządzania. W tym celu Instytut Matematyki PAN w porozumieniu z MON zorganizował dwukrotnie w latach 1960-64 dwuletnie podyplomowe studia z zakresu badań operacyjnych. Wykładowcami tego studium byli najwybitniejsi specjaliści z ośrodka warszawskiego i wrocławskiego. Podobne kursy kilkumiesięczne były następnie organizowane przez

WAT i ASG dla inżynierów i oficerów ogólnowojskowych. Dla pracowników Sztabu Generalnego został zorganizowany kilkumiesięczny kurs przez pracowników SGPiS.

Najważniejszym problemem było rozpoczęcie systematycznego kształcenia specjalistów wojskowych z zakresu informatyki. W 1963 r. wyodrębniono z Katedry Automatyki i Telesterowania Wydziału Elektroradiotechnicznego WAT Katedrę Maszyn Matematycznych. Pierwsi absolwenci ze specjalnością maszyny matematyczne opuścili WAT w 1965 r. Jednocześnie w tym samym roku na Wydziale Uzbrojenia Rakietowego została utworzona Katedra Bojowego Wykorzystania Sprzętu Wojskowego. Katedra ta w 1964 r. rozpoczęła kształcenie specjalistów z zakresu cybernetyki wojskowej. Grupę tej specjalności stanowiło 14 studentów wybranych po trzecim semestrze ze wszystkich wydziałów WAT. Absolwenci tego kierunku ukończyli studia w 1967 r. Jeden z tych absolwentów został w 1987 r. Komendantem WII.

W związku ze zwiększonymi potrzebami kadrowymi i wymaganiami specjalistycznymi postanowiono utworzyć w WAT nowy wydział - **Wydział Cybernetyki WAT**. Stworzono go na bazie komórek organizacyjnych Wydziału Elektroradiotechnicznego (maszyny matematyczne) i Wydziału Uzbrojenia (cybernetyka wojskowa - dawna katedra Bojowego Wykorzystania Sprzętu Bojowego).

W skład struktury Wydziału Cybernetyki wchodziły:

- Katedra Cybernetyki Technicznej;
- Katedra Badań Operacyjnych;
- Katedra Maszyn Matematycznych;
- Analogowy Ośrodek Obliczeniowy.

Wydział rozpoczął swą działalność od początku roku akademickiego 1968/1969.

Po 1975 r. główny wysiłek inwestycyjny i organizacyjny w dziedzinie informatyki ukierunkowany został na dalszą rozbudowę, modernizację i ujednolicenie bazy technicznej ośrodków przetwarzania informacji systemu terytorialnego oraz rozwój techniki dla potrzeb polowego systemu dowodzenia. W ramach rozbudowy i modernizacji bazy technicznej wyposażono systemowe ośrodki przetwarzania informacji jednolicie w komputery typu ODRA-1305. Rozwiązano pomyślnie trudny problem przygotowania maszynowych nośników informacji i przesyłania danych przez rozpoczętą w 1979 r. instalację w OPI wielostanowiskowych rejestratorów danych na taśmie magnetycznej typu MERA 9150 oraz wyposażenie ośrodków systemowych w urządzenia transmisji danych typu UTD-211 (zarządzenie szefa Sztabu Generalnego WP nr 044/Sztab z 18 września 1978 r.).

W końcu 1980 r. eksploatowano w wojsku komputery stacjonarne o łącznej mocy obliczeniowej około 8 mln operacji na sekundę.

Dużo uwagi poświęcono wdrażaniu rozwiązań bazujących na technice minikomputerowej powszechnie dostępnej na krajowym rynku tj. minikomputery serii MERA-300 i MERA-400. Pierwsze minikomputery - głównie typu MERA-302 i MERA-303 - zainstalowano w systemie abonenckim WAT (SAWAT). Kolejno w minikomputery zaczęto wyposażać dołowe ogniwa kierowania, a w tym: składnice służby czołgowo-samochodowej, służby uzbrojenia i elektroniki, bazy amunicji, rejonowe składnice kwatermistrzowskie, DKP WAM oraz niektóre instytucje centralne MON i wojskowe instytuty naukowo-badawcze.

W omawianym okresie szczególnie wyraźny postęp odnotowano w rozwoju bazy technicznej dla potrzeb informatycznego zabezpieczenia polowego systemu dowodzenia. Dużym osiągnięciem było zaprojektowanie, zbudowanie i eksperymentalne wdrożenie do sztabów szczebla operacyjnego (front, armia) 3 ruchomych ośrodków obliczeniowych (ROO). Ośrodki te zbudowano na bazie komputera RODAN-10 (wojskowy odpowiednik komputera ODRA-1325 zainstalowanego w klimatyzowanym kontenerze typu 1CC). ROO wyposażono w końcówki abonenckie, umożliwiające wykorzystanie zasobów informatycznych w systemie wielodostępu bezpośredniego z miejsc pracy poszczególnych użytkowników polowego systemu informatycznego.

Przedsięwzięcia organizacyjne, techniczne, naukowo-badawcze realizowane od 1960 r. do końca lat siedemdziesiątych wymagały wiele wysiłku merytorycznego i znacznych nakładów finansowych. Główną jednak przeszkodą była bariera psychologiczna wśród znacznej części kadry, wynikająca z nieuzasadnionego niepokoju, że technika obliczeniowa zagraża człowiekowi. Dużo wysiłku kosztowało, aby przełamać tę barierę i uświadomić, że komputer jest wspaniałym narzędziem w rękach rozumnego człowieka - chodzi tylko o to, by to narzędzie umiejętnie wykorzystać. Takiemu celowi służyły różne przedsięwzięcia popularyzujące możliwości techniki obliczeniowej (niestety w tym czasie były one nie w pełni zadowalające) oraz pokazy konkretnych rozwiązań.

Trzykrotnie problem zastosowań informatyki był tematem obrad Rady Wojskowej MON i demonstracji zastosowań na Stanowisku Dowodzenia OPK, w składnicach sprzętu wojskowego, na stanowiskach dowodzenia w czasie dużych ćwiczeń itp. Celowi popularyzacji i doradztwa służyło również powołanie, przy Szefie Sztabu Generalnego WP, Rady MON ds. Informatyki, w skład w której weszli ludzie o największych autorytetach w kraju.

W drugiej połowie lat 70-tych nastąpiły dalsze doskonalenia struktur organizacyjnych i wykonawczych organów informatyki.

Ważnym etapem kształtowania organów wykonawczych informatyki było utworzenie w 1979 r. **Wojskowego Instytutu Informatyki (WII)**, który w 1979 r. został sformowany na bazie ID ASG, IASZ WAT, COPI MON i OPI GK WP. Ze względów lokalowych komórki te pozostały w swoich dotychczasowych siedzibach otrzymując odpowiednio nazwy filii nr 1, 2, 3 i 4.

Do 1983 r. Zarząd Informatyki podlegał Zastępcy Szefa Sztabu Generalnego WP ds. Systemów Kierowania, zaś Szefostwo Wojsk Łączności - Zastępcy Szefa Sztabu Generalnego WP ds. Operacyjnych. Nie sprzyjało to dobrej współpracy tych dwóch instytucji Sztabu Generalnego WP, która w tym czasie była już niezbędna.

Podporządkowanie w 1983 r. obu tych instytucji jednemu zastępcy - Zastępcy Szefa Sztabu Generalnego WP do spraw Systemów Kierowania poprawiło sytuację.

Niestety dalsze zmiany w organizacji i podporządkowaniu, a przede wszystkim obniżenie rangi Wojskowego Instytutu Informatyki do **Centrum Informatyki Sztabu Generalnego WP**, pozbawiające m.in. prawa prowadzenia prac naukowo-badawczych, nie poprawiły sytuacji informatyki w WP.

2

2. Historia Wojskowego Instytutu Informatyki

płk rez. dr Mieczysław Ciechanowicz

Upłynęły już 22 lata od czasu, jak zostały podjęte starania o utworzenie w Wojsku Polskim organu informatycznego w randze instytutu, któremu nadano nazwę **Wojskowy Instytut Informatyki** powszechnie określanego WII. Motywem utworzenia Wojskowego Instytutu Informatyki były następujące przesłanki:

- Stworzenie możliwości skupienia wysiłku informatyki na najważniejszych dziedzinach,
- Konieczność zwiększania efektów operacyjnych i ekonomicznych poprzez wdrożenia systemów informatycznych w podstawowych dziedzinach działalności sił zbrojnych,
- Zapewnienie koncentracji, a także optymalnego wykorzystania potencjału kadrowego i technicznego informatyki,
- Potrzeba stworzenia zwartego zaplecza naukowo badawczego informatyki wojskowej.

Wojskowy Instytut Informatyki został utworzony na podstawie następujących aktów prawnych:

Zarządzenia nr 51 Prezesa Rady Ministrów z dn. 15 września 1977 r.,
Zarządzenia Ministra Obrony Narodowej nr 07/MON z dn. 25 sierpnia 1978 r.,
Zarządzenia Szefa Sztabu Generalnego WP nr 020/Org. z dn. 2 maja 1979 r.

Za datę sformowania Wojskowego Instytutu Informatyki przyjmuje się 9 września 1979 r. Nastąpiło to poprzez połączenie pod jednym kierownictwem następujących instytucji:

- **Instytutu Dowodzenia Akademii Sztabu Generalnego WP** (utworzonego w 1966 r.),
- **Instytutu Automatyzacji Systemów Zarządzania Wojskowej Akademii Technicznej** (utworzonego w 1967 r.),
- **Centralnego Ośrodka Przetwarzania Informacji Ministerstwa Obrony Narodowej** (utworzonego w 1969 r.),
- **Ośrodka Przetwarzania Informacji Głównego Kwatermistrzostwa WP** (utworzonego w 1971 r.).

Rozkazem Ministra Obrony Narodowej nr 0160 z dnia 6 września 1979 r. na stanowisko komendanta Wojskowego Instytutu Informatyki został wyznaczony płk doc. dr Mieczysław Ciechanowicz.

Zastępcami komendanta Wojskowego Instytutu Informatyki zostali wyznaczeni:

płk dr Jan Ławski (do spraw politycznych),
płk dr inż. Bernard Buśko (do spraw naukowych),
ppłk mgr inż. Zbigniew Kaliński (do spraw technicznych).

Kierownictwo instytutu zostało rozlokowane przy ul. Nowowiejskiej 26.

Z Instytutu Dowodzenia Akademii Sztabu Generalnego WP została utworzona **Filia nr 1** Wojskowego Instytutu Informatyki. Na komendanta Filii nr 1 WII – jednocześnie w randze zastępcy komendanta WII – został wyznaczony płk prof. dr hab. Władysław Filar. Etat Filii określał następujący stan osobowy żołnierzy i pracowników cywilnych wojska: 101 oficerów, 2 chorążych, 1 podoficer zawodowy, 46 pracowników cywilnych. Filia nr 1 pozostała na terenie Akademia Sztabu Generalnego WP w Rembertowie.

Z Instytutu Automatyzacji Systemów Zarządzania Wojskowej Akademii Technicznej została utworzona **Filia nr 2** Wojskowego Instytutu Informatyki. Na komendanta Filii nr 2 - jednocześnie w randze zastępcy Komendanta WII – został wyznaczony płk dr inż. Władysław Boratyn. Stan osobowy kadry i pracowników cywilnych Filii obejmował: 104 oficerów, 8 chorążych, 4 podoficerów zawodowych, 88 pracowników cywilnych. Filia nr 2 pozostała w dotychczas zajmowanym obiekcie WAT.

Z Centralnego Ośrodka Przetwarzania Informacji Ministerstwa Obrony Narodowej utworzono **Filię nr 3** Wojskowego Instytutu Informatyki. Na komendanta Filii nr 3 WII został wyznaczony ppłk mgr inż. Henryk Biniewski. Stan ewidencyjny Filii był następujący: 46 oficerów, 6 chorążych, 1 podoficer zawodowy, 57 pracowników cywilnych. Filia nr 3 pozostała w budynku Sztabu Generalnego WP przy ul. Rakowieckiej.

Z Ośrodka Przetwarzania Informacji Głównego Kwatermistrzostwa WP utworzono **Filię nr 4** Wojskowego Instytutu Informatyki. Na komendanta Filii nr 4 został wyznaczony płk mgr inż. Lucjan Woźniczka. Etat Filii przewidywał następujący stan osobowy: 22 oficerów, 3 chorążych, 1 podoficer zawodowy, 53 pracowników cywilnych. Filia Nr 4 pozostała w budynku mieszczącym ośrodek obliczeniowy Głównego Kwatermistrzostwa WP.

Ogółem po sformowaniu stan osobowy Wojskowego Instytutu Informatyki wynosi: 273 oficerów, 19 chorążych, 7 podoficerów zawodowych, 244 pracowników cywilnych. **Łącznie 543 osoby**. Opracowany przez Sztab Generalny WP etat Wojskowego

Instytutu Informatyki w kolejnych latach był kilkakrotnie zmniejszany aż do jednej trzeciej stanu początkowego.

W początkowej fazie funkcjonowania Wojskowego Instytutu Informatyki poszczególne Filie zostały ukierunkowane na informatyzację określonych rodzajów wojsk i służb.

Filia nr 1 prowadziła prace naukowo-badawcze i projektowo-wdrożeniowe dla potrzeb wojsk operacyjnych oraz wspomagała proces dydaktyczny Akademii Sztabu Generalnego WP.

Filia nr 2 prowadziła prace naukowo-badawcze i projektowo-wdrożeniowe dla potrzeb służb pionu technicznego oraz administracji wojskowej. Zajmowała się też badaniami dostępnego sprzętu informatycznego w aspekcie zastosowań wojskowych.

Filia nr 3 zajmowała się wyłącznie wdrażaniem i eksploatacją systemów informatycznych oraz wykonywaniem zadań bieżących na rzecz poszczególnych zarządów Sztabu Generalnego WP.

Filia nr 4 wykonywała prace projektowo-wdrożeniowe i eksploatacyjne dla potrzeb służb kwatermistrzowskich, głównie kierowania zaopatrywaniem i obsługą wojsk z elementami rozwiązań informatycznych dla potrzeb tyłowego stanowiska dowodzenia frontu.

Kolejnymi komendantami WII byli:

płk dr inż. Władysław BORATYN (1987 – 1991),
płk dr hab. Andrzej STOKALSKI-DZIERŻYKRAJ (1991 – 1994).

Należy podkreślić, że WII nie zajmował się problematyką Wojsk Lotniczych, Wojsk Obrony Powietrznej Kraju i Marynarki Wojennej, gdyż te rodzaje sił zbrojnych miały swoje dość liczne zespoły informatyki. Instytut z tymi zespołami utrzymywał ścisłą współpracę, udostępniając przede wszystkim swoje rozwiązania standardowe w obszarze projektowo-programowym i techniki komputerowej.

Organem doradczym i opiniodawczym komendanta instytutu była Rada Naukowa powoływana przez Ministra Obrony Narodowej. Członkami Rady Naukowej byli: zastępca Szefa Sztabu Generalnego WP do spraw Systemów Kierowania, prorektor ds. naukowych WAT, Szef Zarządu Informatyki Sztabu Generalnego WP, zastępcy komendanta WII, komendanci filii, komendant Wojskowego Instytutu Łączności oraz profesorowie z instytucji cywilnych, m.in.: K. Badźmirowski, J. Kulikowski, S. Paszkowski, W.M. Turski, A. Straszak. Rada Naukowa opiniowała plany prac naukowo-badawczych i projektowo-wdrożeniowych instytutu, zapoznawała się i oceniała ważniejsze opracowania przed ich wdrożeniem oraz inspirowała rozwój naukowy kadry instytutu.

Mimo ograniczonych możliwości obliczeniowych sprzętu informatycznego (głównie były to komputery typu Odra i Mera), w instytucie zaprojektowano i wdrożono dla potrzeb wojsk operacyjnych system informatyczny eksploatowany na komputerze „ODRA-1325" zainstalowanym w kontenerze (Ruchomy Ośrodek Obliczeniowy). System ten był powszechnie wykorzystywany (do 1992 r.) na wszystkich ćwiczeniach szczebla centralnego i w niektórych okręgach wojskowych.

Za kompleksowe opracowanie zasad wykorzystania polowego zautomatyzowanego systemu dowodzenia została przyznana nagroda Ministra Obrony Narodowej zespołowi w składzie: płk Czesław Flanek, płk Stanisław Chomenko, ppłk Jerzy Matela.

Opracowano i wdrożono szereg systemów informatycznych dla potrzeb codziennej działalności sił zbrojnych, głównie w charakterze ewidencyjno – sprawozdawczym statystycznym, z którego korzystały głównie służby kwatermistrzowskie i techniczne.

Na uwagę zasługuje – opracowany przez zespół pod kierownictwem płk Andrzeja Stokalskiego – mikrokomputerowy system wspomagania zespołów autorskich opracowujących ćwiczenia, treningi i gry wojenne. Umożliwiał miedzy innymi skrócenie czasu przygotowania tła operacyjnego i ćwiczebnych danych wojskach własnych i przeciwnika z około trzech miesięcy do około jednego tygodnia.

Rozpoczęto też projektowanie Terytorialnego Systemu Informatycznego Sił Zbrojnych. Opracowano koncepcję budowy systemu materiałowego służb technicznych. W trzech składnicach technicznych wdrożono do eksploatacji na minikomputerach systemy informatyczne będące elementami składowymi TSI SZ.

Unikatową pracą było wykonanie modelu kompleksowego trenażera do wstępnego szkolenia działonowych bojowego wozu piechoty. Dokumentacje techniczne do produkcji trenażera przekazano do Wojskowego Centralnego Biura Konstrukcyjno-Technologicznego.

Wdrożono też powielalne mikrokomputerowe systemy informatyczne w 15 składnicach kwatermistrzowskich.

Ciekawym opracowaniem było opracowanie oprogramowania dydaktycznego do nauki matematyki, fizyki i informatyki w szkołach średnich. Pakiet takich programów przekazano do Wojskowych Liceów Ogólnokształcących.

Podczas gry wojennej „MAJ–89" eksperymentalnie rozwinięto graficzne stanowisko pracy do zobrazowania sytuacji operacyjno-taktycznej oraz przetestowano bazową konfigurację mikrokomputerowego systemu wspomagania dowodzenia.

Spośród innych opracowań wykonywanych w instytucie należy wymienić:

- Koncepcję informatyzacji sił zbrojnych,
- Mikrokomputerowy system wspomagania dowodzenia operacyjnego,
- Zautomatyzowany system dowodzenia i kierowania uderzeniami rakiet,
- Polowy zautomatyzowany system dowodzenia tyłami,
- System rachunkowości finansowej działalności budżetowej,
- Mikrokomputerowy system wspomagania dyżurnych służb operacyjnych,
- System informatyczny rejonowych składnic kwatermistrzowskich,
- System prowadzenia i dystrybucji jednolitego kodu adresowego jednostek wojskowych,
- System ewidencji etatowych stanów osobowych wojsk,
- System wspomagania kierowania zaopatrzenia wojsk,
- Mikrokomputerowy system wspomagania działalności bieżącej wojskowej komendy uzupełnień,
- System gospodarowania zasobami rezerw osobowych WKU,
- System zaopatrzenia emerytalne żołnierzy zawodowych.

Wszystkie osiągnięcia jakie ma zapisane na swoim koncie Wojskowy Instytut Informatyki są dziełem pracy jego żołnierzy zawodowych i pracowników cywilnych.

Pragnę podkreślić, że WII miał bardzo zdolnych, wręcz wybijających się oficerów i pracowników cywilnych. Wielu z nich aktualnie tworzy oryginalne systemy informatyczne w ramach Centrum Informatyki Sztabu Generalnego WP. Wymownym dowodem talentu informatyków jest zajmowanie przez nich wysokich stanowisk w instytucjach centralnych wojska, a ci którzy pożegnali się z mundurem kierują informatyką w najwyższych urzędach państwowych.

Nie wymieniam tu nazwisk, gdyż lista utalentowanych pracowników instytutu jest zbyt długa. Poczytuje sobie za wielki zaszczyt, że ostatnie lata zawodowej służby wojskowej dane mi było kierowanie tak wspaniałymi ludźmi. Warto jednak przypomnieć, że działalnością Instytutu i jego filii kierowali:

Komendanci WII

płk dr inż. Władysław Boratyn
płk doc. dr hab. Andrzej Stokalski – Dzierżykraj

Zastępcy komendanta WII

płk mgr Jan Terepka	– do spraw politycznych
płk mgr inż. Wojciech Skurzak	– do spraw naukowych
płk dr inż. Jerzy Flakowski	– do spraw technicznych

Komendanci Filii nr 1 WII

płk mgr inż. Lucjan Woźniczka
płk doc. dr hab. Andrzej Stokalski – Dzierżykraj

Komendanci Filii Nr 2

płk dr inż. Odylon Gawęda

Komendanci Filii Nr 3

płk mgr inż. Henryk Biniewski

Komendanci CPI

płk mgr inż. Zygmunt Wroński
płk mgr inż. Zbigniew Świderski

Zastępcy komendantów Filii

płk mgr Jan Man	– do spraw politycznych Filii Nr 1
płk mgr Zenon Grelka	– do spraw politycznych Filii Nr 2
płk dr inż. Piotr Zaskórski	– do spraw naukowych Filii Nr 2
płk mgr Jan Gawin	– do spraw politycznych Filii Nr 3
płk mgr inż. Mieczysław Kempka	– Filii Nr 3

Na mocy Zarządzania Nr 86/MON Ministra obrony Narodowej z dnia 12 lipca 1994 roku rozformowano Wojskowy Instytut Informatyki i utworzono Centrum Informatyki Sztabu Generalnego WP.

3

3. Przesłanki transformacji centralnego organu wykonawczego informatyki wojskowej i jej rozwój na przełomie lat 1980/1990

płk. rez. dr hab. inż. prof. WAT. Andrzej Stokalski

płk. rez. dr inż. Władysław Boratyn

Wprowadzenie

Dla informatyki wojskowej **przełom lat 1980/1990** był okresem ambitnych zamierzeń, nieoczekiwanych okoliczności i dramatycznych zmian. Z formalnego punktu widzenia ich najbardziej spektakularnym wynikiem było rozwiązanie Wojskowego Instytutu Informatyki, ustawowo podporządkowanego Zastępcy Szefa Sztabu Generalnego WP ds. Systemów Kierowania, i utworzenie Centrum Informatyki Sztabu Generalnego WP w podporządkowaniu Szefa Wojsk Łączności i Informatyki. Okres pięciu lat, które upłynęły od tego wydarzenia jest wystarczającą perspektywą do obiektywnej oceny przesłanek takiego rozwoju sytuacji oraz skutków podjętych wówczas decyzji.

Przesłanki i efekty zmian przełomu lat 1980/1990

Zmiany przełomu lat 1980/1990 w informatyce wojskowej były kształtowane głównie wydarzeniami przebiegającymi w dwóch zasadniczych płaszczyznach:

- Reorganizacji Wojskowego Instytutu Informatyki (WII), a w szczególności jego podporządkowania, zadań i struktury organizacyjno-etatowej,
- Reorganizacji systemu kierowania siłami zbrojnymi, a w tym restrukturyzacji Sztabu Generalnego WP i zmiany statusu finansowo-prawnego wojskowych jednostek badawczo-rozwojowych.

Wojskowy Instytut Informatyki został powołany, jako centralny organ wykonawczy informatyki wojskowej Zarządzeniem Prezesa Rady Ministrów nr 51/77 z dn. 15.09.1977 r. i sformowany na podstawie Zarządzenia Ministra Obrony Narodowej nr 07/MON z dn. 25.08.1978 r. na bazie:

Instytutu Dowodzenia Akademii Sztabu Generalnego

Instytutu Automatyzacji Systemów Zarządzania Wojskowej Akademii Technicznej

Centralnego Ośrodka Przetwarzania Informacji Sztabu Generalnego WP

Ośrodka Przetwarzania Informacji Głównego Kwatermistrzostwa WP.

Dokumenty założycielskie, jako misję Instytutu stanowiły realizację zadań badawczo - rozwojowych, projektowo - wdrożeniowych i eksploatacyjnych w dziedzinie obronnych zastosowań technologii informacyjnych.

Powołanie Instytutu i równoległe działania zmierzające do szybkiego rozwoju szeroko rozumianej infrastruktury informatycznej (organizacja zespołów informatyki RSZ i OW, stworzenie zaplecza naukowo - szkoleniowego w postaci Wydziału Cybernetyki WAT, organizacja bazy informatycznej w ASG i Szkołach Oficerskich itp.) były potwierdzeniem wysokiego priorytetu dla tego obszaru działania, a w szczególności dla zaawansowanych technologii informacyjnych jako czynnika potęgowania potencjału obronnego. Instytut uzyskał w etacie ponad 500 stanowisk i miał przejściowo funkcjonować w strukturze czterech filii (Filia 1 przy ASG, Filia 2 przy WAT, Filia 4 przy Głównym Kwatermistrzostwie) i Filia 3 ulokowanej przy Sztabie Generalnym. Wspomniane dokumenty **nakazywały dokonanie integracji Instytutu w jednym miejscu w okresie 1979 - 1981**. Stan wojenny i problemy gospodarcze kraju spowodowały zaniechanie działań integracyjnych aż do końca lat 80.

Warunki do rozpoczęcia procedury integracyjnej pojawiły się na początku lat 90, wraz z przydzieleniem Instytutowi części budynku przy ul. Nowowiejskiej 28A, gdzie znajduje się jego obecna siedziba. Do nowej siedziby przenoszono kolejno filie zachowując jednocześnie filialną strukturę organizacyjną.

W roku 1993 przystąpiono do planowania przekształceń organizacyjno - etatowych Instytutu w radykalnie zmienionych zewnętrznych uwarunkowaniach organizacyjnych:

- Zlikwidowany został pion funkcjonalny Zastępcy Szefa SG WP ds. Systemów Kierowania. Rozformowano Zarząd XIV, odpowiedzialny za informatykę, a na jego bazie utworzono w Szefostwie Wojsk Łączności pion informatyki, przekształcając je w Szefostwo Wojsk Łączności i Informatyki.
- Utworzono pion funkcjonalny Szefa Planowania Strategicznego, któremu podporządkowano m.in. „tradycyjne" Zarządy I, II, IV i nowo utworzony Zarząd III (Dowodzenia) oraz Wojskowy Instytut Informatyki.

Szef Planowania Strategicznego SG WP, gen. Marian Robełek w meldunku do Szefa Sztabu Generalnego WP Nr PF37/1994 przedstawił nową koncepcję systemu kierowania rozwojem informatyki w SZ RP i restrukturyzacji Wojskowego Instytutu Informatyki, która przewidywała:

- Rozformowanie WII;
- Utworzenie Centrum Informatyki SG WP (4 zakłady naukowo-badawcze, 8 zakładów projektowo - produkcyjnych, 2 zakłady techniczne), jako informatycznej budżetowej jednostki badawczo - produkcyjnej, podporządkowanej Szefowi Planowania Strategicznego.

Proponowana struktura uwzględniała następujące założenia:

- Rola zaawansowanych technologii informacyjnych będzie systematycznie wzrastać w miarę ścisłego współdziałania SZ RP z NATO;
- Skala niezbędnych przedsięwzięć badawczo rozwojowych w dziedzinie automatyzacji dowodzenia wojskami i kierowania środkami walki będzie narastać;
- W interesie bezpieczeństwa narodowego jest utrzymanie „masy krytycznej" zespołów naukowo-badawczych zdolnych do rozwijania narodowych rozwiązań oraz formalno-prawne **zagwarantowanie bezpośredniego współdziałania** między komendą CI SG a głównymi użytkownikami na odpowiednim szczeblu dowodzenia.

Strategicznym celem restrukturyzacji WII było utrzymanie „masy krytycznej" potencjału badawczego wówczas obejmującego ponad 20 doktorów, w tym 11 informatyków - doktorów nauk wojskowych, których specjalistyczna wiedza wojskowa była potwierdzona przygotowaniem operacyjnym. Profil specjalistyczny kadry naukowej WII pokrywał zarówno obszary problemowe komórek organizacyjno - funkcjonalnych stanowisk dowodzenia od szczebla frontu do związku taktycznego, jak i istotne w tamtym czasie obszary problemowe cyklu rozwojowego infrastruktury informacyjnej systemów dowodzenia.

Włączenie Polski do programu „Partnerstwa dla pokoju" spowodowało konieczność przyspieszenia procesów automatyzacji dowodzenia. Brak silnego własnego potencjału wykonawczego w dziedzinie systemów dowodzenia dawałaby argumenty na rzecz zakupu gotowych rozwiązań na Zachodzie. Skutkiem byłby odpływ części budżetu obronnego do obcej gospodarki i osłabienie suwerenności w dziedzinie narodowej doktryny dowodzenia i rozwoju potencjału obronnego.

Koncepcja przedstawiona przez Szefa Planowania Strategicznego uzyskała po niewielkich zmianach aprobatę Szefa Sztabu Generalnego z zastrzeżeniem, iż liczba stanowisk etatowych powinna być ustalona na poziomie 300, przy czym podstawą do formalnego rozpoczęcia restrukturyzacji WII stało się Zarządzenie MON Nr 86/MON z dnia 12.07.1994r. w sprawie rozformowania Wojskowego Instytutu Informatyki i utworzenia Centrum Informatyki Sztabu Generalnego WP.

Dokument etatowy opracowany przez Zarząd VI SG WP znacznie odbiegał od pierwotnej, zaakceptowanej przez Szefa Sztabu Generalnego, koncepcji organizacyjno - funkcjonalnej Centrum, a mianowicie podporządkowywał Centrum Szefostwu Wojsk

Łączności i Informatyki, a struktura zawierała 7 zakładów projektowo - wdrożeniowych, dwa usługowe ośrodki przetwarzania informacji oraz pion logistyczny, ale w etacie nie przewidziano ***ani jednego*** stanowiska naukowego.

Komenda WII nie uzyskała żadnego formalnego wyjaśnienia tak dramatycznego odstępstwa od zaakceptowanej przez Szefa Sztabu Generalnego WP koncepcji, ani też powodów zignorowania przedstawionych wyżej strategicznych przesłanek restrukturyzacji.

Tworząc ***model funkcjonowania*** przyszłego hipotetycznego centralnego organu informatyki SZ RP poszukiwano analogii w strukturach NATO. Jako stosunkowo adekwatny wzorzec przyjęto Shape Technical Center (STC), który był organem budżetowym o profilu badawczym, podporządkowanym dowódcy NATO w Europie, o statutowej misji zbliżonej do dawnego Wojskowego Instytutu Informatyki, z wyłączeniem zadań eksploatacyjnych. Uwzględniając hipotetyczną możliwość (wydawała się wówczas wysoce prawdopodobna) kolejnych etapów transformacji w kierunku utworzenia pionu C4 w strukturze MON (np. poprzez powołanie urzędu pełnomocnika MON ds. Infrastruktury Informacyjnej) i w konsekwencji wyłączenia Centrum Informatyki ze struktury Sztabu Generalnego (np. w połączeniu z utworzeniem na jego bazie Agencji C4 - co miało ostatnio miejsce w przypadku STC), w propozycji etatowej rozbudowano pion logistyczny, a w szczególności służbę finansową.

Wstępnie rozpatrywano także wariant rozbicia WII na część eksploatacyjną (ośrodki obliczeniowe) pozostawioną w podporządkowaniu SG WP i część wykonawczą, podporządkowaną, jako jednostka badawczo-rozwojowa, Departamentowi Badań i Rozwoju. Ocena możliwości finansowania działalności Instytutu w tym czasie prowadziła do wniosku, iż przy dobrym rozwoju sytuacji byłoby konieczne zredukowanie jego stanu osobowego do 70 - 80 osób. Taka utrata potencjału praktycznie oznaczała radykalne zahamowanie procesu informatyzacji Sił Zbrojnych na wiele lat. Ponadto wariant ten nie został poparty przez Szefostwo Wojsk Łączności i Informatyki i nie był przedstawiany do rozpatrzenia na szczeblu kierownictwa SG WP.

Nie sposób przy tym pominąć faktu, że działalność badawczo - rozwojowa będzie nadal najważniejszym zadaniem Centrum. Słuszność takiego założenia potwierdza dziś z jednej strony skala jego zaangażowania w tematy finansowane przez Departament Rozwoju i Wdrożeń, z drugiej natomiast - skala problemów badawczo rozwojowych oczekujących na podjęcie, bo wymuszanych przez obiektywne tendencje rozwojowe. Jest swoistym paradoksem, iż pomimo powszechnego uznawania roli zaawansowanych technologii informacyjnych, jako czynnika potencjału obronnego, dziś SZ RP formalnie nie posiadają ani ***centralnego organu badawczo-rozwojowego o informatycznym profilu***, ani organu przeznaczonego do scentralizowanego ***zarządzania strategicznymi programami w dziedzinie automatyzacji dowodzenia wojskami i kierowania środkami walki***.

Transformacji Instytutu w Centrum towarzyszyło pogorszenie zaszeregowania stanowisk (w wielu przypadkach nawet o 4 grupy), na co nałożyła się narastająca dysproporcja między uposażeniami kadry oficerskiej a ofertą cywilnego rynku informatycznego. W efekcie, wraz z rozpoczęciem funkcjonowania Centrum Informatyki rozpoczął się odpływ znacznej części kadry o wysokich kwalifikacjach. Straty w grupie kadry naukowej były największe i trudne do odrobienia.

W tym miejscu wypada przy rocznicowej okazji złożyć gratulacje urzędującemu Komendantowi i wyrazić podziw, iż pomimo wymienionych problemów potrafił wypracować efektywną formułę funkcjonowania Centrum na polskiej scenie informatycznej, nie tylko w skali Sił Zbrojnych.

Rozwój informatyki wojskowej na przełomie lat 1980/1990

Rozwój informatyki wojskowej na przełomie lat 1980/1990 należy rozpatrywać w kontekście obszaru działania centralnego organu wykonawczego, jakim był Woskowy Instytut Informatyki. Warto przy tym pamiętać o inicjatywach informatyzacji, podejmowanych równolegle przez ówczesne Dowództwo Wojsk Obrony Powietrznej Kraju i Dowództwo Wojsk Lotniczych, później Dowództwo Wojsk Lotniczych i Obrony Powietrznej oraz Dowództwo Marynarki Wojennej i dowództwa okręgów wojskowych.

W rozwoju informatyki wojskowej od jej początków do połowy lat 90 można umownie wydzielić dwa okresy:

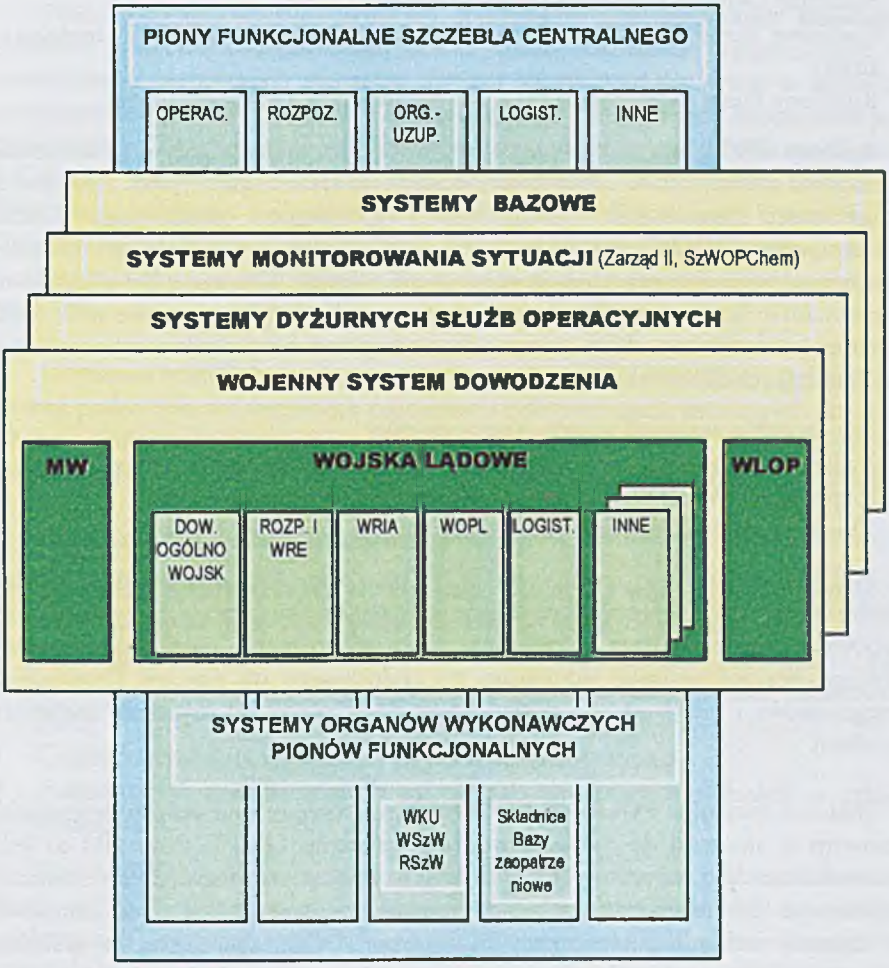
- Okres informatyzacji procesów zarządzania działalnością Sił Zbrojnych na szczeblu centralnym i okręgowym w oparciu o ośrodki obliczeniowe do połowy lat 80,
- Okres automatyzacji procesów dowodzenia wojskami i powszechnej informatyzacji działalności biurowo-sztabowej, zaopatrzeniowej (składnice, bazy zaopatrzenia) i mobilizacyjno-uzupełnieniowej (WKU, WSzW, RSzW) od połowy lat 80.

Połowę lat 80 przyjęto za punkt odniesienia, ponieważ faktycznie wiązała się z istotnym przełomem w kierunkach rozwoju informatyki wojskowej i stosowanych technologiach, a do najważniejszych czynników tego przełomu należy zaliczyć:

1. Przekroczenie zarówno przez wojskowe organa informatyki jak i zaplecze badawczo rozwojowe elektronicznego przemysłu obronnego pewnego „krytycznego poziomu dojrzałości", stwarzającego przesłanki do podejmowania kompleksowych przedsięwzięć z dziedziny obronnych zastosowań zaawansowanych technologii informacyjnych;
2. Świadomość potrzeby posiadania narodowych, zintegrowanych rozwiązań w dziedzinie automatyzacji dowodzenia wojskami i kierowania środkami walki narastająca w dowództwach RSZ i Głównym Zarządzie Szkolenia Bojowego, wspierana przez Zastępcę Szefa Sztabu generalnego ds. Systemów Kierowania i Szefa Zarządu XIV SG WP.

3. Dostępność sprzętu minikomputerowego oraz zapowiedź powszechnego dostępu do technologii mikrokomputerowych i zachodniej literatury naukowej.

Nowa sytuacja wymagała precyzyjnego zdefiniowania nowych obszarów działania w celu racjonalnego przeorganizowania potencjałów wykonawczych, a w szczególności określenia kierunków wymagających wyprzedzającego zainteresowań przyszłych użytkowników oraz przygotowania teoretycznego i technologicznego zespołów. Skala zaangażowania WII, a później CI SG WP w proces informatyzacji obszarów (Rys. 1) był różny z uwagi na różne priorytety i ograniczone możliwości.



Rys. 1 Ogólny model obszarów informatyzacji na przełom lat 80/90

Znaczenie tej dziedziny zastosowań technologii informacyjnych i jej rozwój zasługują na bardziej szczegółowe potraktowanie.

SYSTEMY DOWODZENIA WOJSKAMI OPERACYJNYMI

Przedsięwzięcia badawczo - rozwojowe w dziedzinie automatyzacji dowodzenia zostały zainicjowane przez Zarząd XIV SG WP. W połowie lat 80 zaprojektowano trzy systemy przeznaczone dla stanowisk dowodzenia szczebli operacyjnych:

- Ruchomy Ośrodek Obliczeniowy dla SD frontu i armii;
- Ruchomy Punkt Dowodzenia dla służb kwatermistrzowskich TSD frontu i armii ;
- Ruchomy Punkt Dowodzenia dla służb technicznych TSD fontu i armii.

System GROT bazował na przystosowanym do warunków polowych komputerze centralnym z rodziny ODRA 1300 z wielodostępnym system operacyjnym z możliwością obsługi stacji abonenckich. Integralnym wyposażeniem Ruchomego Ośrodka Obliczeniowego (ROO) były urządzenia transmisji danych, a opcjonalnym - urządzenia szyfrujące udostępniane przez resort spraw wewnętrznych. Komputer był zainstalowany w przewoźnym kontenerze. Wynośne stacje abonenckie były wyposażone w drukarki z klawiaturą i umożliwiały zdalne korzystanie z komputera bezpośrednio w miejscu pracy osób funkcyjnych SD w zakresie:

- Baz danych o wojskach własnych i przeciwnika;
- Zadań kalkulacyjnych według potrzeb Grupy Planowania Operacyjnego, rozpoznania, WRE, WRiA, Wojsk Opchem, Wojsk Inżynieryjnych,
- Zbierania meldunków i dystrybucji dokumentów dyrektywnych.

Pod koniec lat 80 w aparatownie ROO było wyposażone wszystkie dowództwa szczebli operacyjnych System był regularnie wykorzystywany w czasie ćwiczeń, treningów sztabowych i gier wojennych, a największą zaletą użytkową była możliwość stosunkowo szybkiego przygotowywania jednolitego tła operacyjnego do ćwiczeń i treningów o szczegółowości i merytorycznej poprawności nie możliwej do uzyskania tradycyjnymi metodami.

Budowę systemów **POLAR-K i POLAR-T** rozpoczęto z niewielkim przesunięciem czasowym w stosunku do cyklu rozwojowego systemu GROT. Pozwoliło to jednak zastosować bardziej zaawansowane, wcześniej nie dostępne rozwiązania techniczne i programowe. Zachowano wprawdzie architekturę abonencką systemu, ale zastosowano już krajową wersję minikomputera PDP firmy DEC, zbudowaną w technologii wielkoskalowej integracji, z bardzo sprawnym wielodostępnym systemem operacyjnym. Wykorzystywano terminale elektroniczne. Mniejsze gabaryty i większa odporność mechanoklimatyczna pozwoliła na zastosowanie podwozia samochodu ciężarowo–terenowego, a sam system zapewniał:

- Prowadzenie baz danych dla służb kwatermistrzowskich i technicznych;
- Usługi w zakresie zadań informacyjnych i kalkulacyjno-planistycznych z zakresu posiadanych środków materiałowo-technicznych oraz możliwości jednostek tyłowych;
- Usługi w zakresie zbierania meldunków i dystrybucji dokumentów dyrektywnych z wykorzystaniem transmisji danych.

Oba systemy uzyskały generalnie wysoką ocenę użytkownika ale narastające trudności finansowe resortu ograniczyły inwestycje do dwóch aparatowni, wykorzystywanych w czasie ćwiczeń na szczeblach operacyjnych.

Prace nad **Mikrokomputerowym Systemem Wspomagania Dowodzenia** (MSWD) rozpoczęto praktycznie jeszcze przed formalnym zakończeniem cyklu rozwojowego poprzednich systemów. System został zaprojektowany w architekturze określanej jako *„klaster lokalnych sieci komputerowych"*, z których każda obejmowała jeden z podsystemów funkcjonalnych SD: Centrum Dowodzenia Bojowego z Grupą Kierunków i Centrum Informacyjnym, Planowania Operacyjnego, Rozpoznania, WRE, Grupy Planowania Jądrowego i Ogniowego Porażenia, Wojsk Rakietowych i Artylerii, Wojsk Inżynieryjnych, Wojsk Chemicznych, Wojsk Obrony Przeciwlotniczej, zespołów autorskich opracowujących jednolite tło operacyjne i bazy danych na ćwiczenia i treningi sztabowe.

Użytkowo MSWD był wykorzystywany na szczeblach operacyjnych (głównie na SD frontu) praktycznie we wszystkich ćwiczeniach oraz treningach sztabowych przez blisko 10 lat i jednocześnie systematycznie rozbudowywany m.in. o grafikę operacyjną i symulacyjny model działań. Na początku lat 90 został uzupełniony o podsystem logistyki.

Do ważniejszych usług systemu należy zaliczyć:

- Prowadzenie baz danych o wojskach własnych, wojskach przeciwnika i obiektach operacyjnego przygotowania terenu z aktualizacją meldunkami,
- Zbieranie meldunków oraz opracowywanie dokumentów bojowych i ich dystrybucja w lokalnej sieci komputerowej (w ramach SD) i w sieci pakietowej X.25,
- Grafikę operacyjną i symulacyjny model działań bojowych ,
- Pakiety zadań specjalistycznych wg potrzeb wynikających z funkcji w cyklu dowodzenia.

Idea MSWD została faktycznie zainicjowana wspólnie przez ówczesne dowództwo frontu (GZSB) i komendę WII jako narodowa alternatywa dla zapowiadanego „układowego" systemu PASUW szczebla operacyjnego. Kadra kierownicza GZSB odważnie potwierdziła ambicje narodowe, i konsekwentnie promowała innowacyjne rozwiązania w dziedzinie automatyzacji dowodzenia wojskami operacyjnymi (gen. Saczonek, gen. Cepak, gen. Obroniecki i gen. Jauer).

Pierwszą edycję systemu opracowano na mikrokomputerach Zarządu II GZSB, które wypożyczono na dwa lata w celu stworzenia odpowiedniej bazy technologicznej. Na początku lat 90 MSWD powinien zakończyć cykl życia z uwagi na technologiczne zestarzenie oraz zmiany organizacyjne i doktrynalne w Siłach Zbrojnych. Instytut przystąpił do przeprojektowania wybranych podsystemów MSWD na komercyjne platformy UNIX w ramach innych zadań projektowych. Równolegle na polecenie Szefa Sztabu Generalnego opracowano. „Założenia operacyjno - funkcjonalne na zautomatyzowany system dowodzenia SZ RP". W wyniku realizacji tego zadania w 1995r powstał dokument, zatwierdzony przez Szefa Sztabu Generalnego WP. Stał się on podstawą dla realizowanych programów badawczo - rozwojowych w dziedzinie automatyzacji dowodzenia wojskami operacyjnymi.

INNE SYSTEMY DOWODZENIA

Ważne doświadczenia technologiczne dla informatyki wojskowej były związane z dwoma innymi przedsięwzięciami badawczo rozwojowymi zainicjowanymi w pierwszej połowie lat 90: systemem dowodzenia lotniczym związkiem taktycznym (oddziałem) i systemem powietrznego punktu dowodzenia wojsk operacyjnych.

W **systemie dowodzenia lotniczym związkiem taktycznym** po raz pierwszy zastosowano architekturę lokalnej sieci komputerowej jako infrastrukturę integrującą wielostanowiskowe, mobilne kabiny dowodzenia oraz Solarisową platformę aplikacyjną osadzoną na zmilitaryzowanych platformach sprzętowych Sun/Sparc (Super, Ultra itp.). Taki standard architektoniczny stanowi podstawę amerykańskiego systemu dowodzenia wojsk lądowych ATCCIS.

System powietrznego punktu dowodzenia pod względem funkcjonalnym stanowił w istocie odpowiednią syntezę funkcji podsystemów MSWD, docelowo przeniesioną na platformę aplikacyjną Solaris. Był jednak wielkim wyzwaniem technologicznym z uwagi na szczególne wymagania mechanoklimatyczne na sprzęt komputerowy i ograniczenia gabarytowe. W szczególności przewidziano w projekcie zastosowanie unikatowej, podwójnej stacji roboczej typu „face to face". Wydaje się, że wdrożenie tych systemów jest możliwe i potrzebne.

Systemy kierowania środkami walki i polowy sprzęt komputerowy Zgodnie z doktrynalnymi założeniami lat 80, *automatyzacja systemów kierowania działaniami WRE oraz wsparciem ogniowym i obroną przeciwlotniczą wojsk operacyjnych* stanowiła priorytetowy kierunek wzmacniania potencjału bojowego. Wychodząc na przeciw wyzwaniom, w połowie lat 80 Instytut podjął prace badawcze w czterech tematach z tego obszaru zastosowań zaawansowanych technologii informacyjnych:

- Analiza i identyfikacja sygnałów,
- Kierowanie uderzeniami rakiet wojsk operacyjnych,
- Kierowanie ogniem obrony przeciwlotniczej,

- Trenażery załóg pojazdów bojowych.

Analiza i identyfikacja sygnałów. Badania w tej dziedzinie realizowano na zlecenie poza resortowe. Uzyskane wyniki (w tym produkt w postaci analizatora) stwarzały realne szanse szybkiego rozwinięcia jego funkcji pod kątem potrzeb wojskowego rozpoznania elektronicznego, ale resort MON nie finansował dalszych badań.

System kierowania uderzeniami rakiet wojsk operacyjnych. Celem badań było zbudowanie dywizjonowego systemu (platforma komputerowa, oprogramowanie, peryferyjne urządzenia operatorskie i telekomunikacyjne) kierowania uderzeniami rakiet operacyjno - taktycznych i taktycznych. Opracowano model użytkowy systemu, który w zasadzie spełniał wszystkie wymagania funkcjonalne uzgodnione z potencjalnym głównym użytkownikiem (DWRiA). Po badaniach dalsze prace rozwojowe zostały wstrzymane ze względu brak zabezpieczenia finansowego. Wynikiem badań było potwierdzenie, że skala operacji manualnych przy wyrzutniach praktycznie niweczyła korzyści wynikające z automatyzacji procesów kalkulacyjnych i transmisji danych.

System kierowania ogniem obrony przeciwlotniczej wojsk lądowych. W drugiej połowie lat 80 Dowództwo WOPL rozpoczęło wdrażanie zautomatyzowanego systemu dowodzenia operacyjnego obroną powietrzną wojsk lądowych. Był to system wówczas bardzo nowoczesny, przeznaczony do pracy na połączonych stanowiskach dowodzenia WL/WOPL frontu i armii. Na początku lat 90 został uzupełniony systemem sieciowym. Do pełnego „domknięcia" cyklu C3I należało opracować systemy dowodzenia obroną przeciwlotniczą ogólnowojskowych związków taktycznych (dywizje, brygady) oraz systemy kierowania ogniem oddziałów i pododdziałów WOPL.

W ramach przedsięwzięć badawczo-rozwojowych związanych z automatyzacją procesów obrony przeciwlotniczej na szczeblach taktycznych Instytut (CI SG) był wykonawcą oprogramowania dla istniejących polowych systemów WOPL. Przeciąganie cyklu rozwojowego przy braku interwencyjnych środków finansowych doprowadziło do technologicznego zestarzenia prototypu jeszcze przed wdrożeniem do produkcji. W efekcie niezbędne są modyfikacje przedwdrożeniowe.

Trenażery załóg pojazdów bojowych. Celem pracy było zbudowanie rodziny „inteligentnych" trenażerów, umożliwiających szkolenie członków załóg pojazdów bojowych. Zbudowano prototyp trenażera dla załogi BWP, który przeszedł badania funkcjonalne. Zastosowane w nim rozwiązania technologiczne, oparte na technice mikroprocesorowej, graficznym zobrazowaniu pola walki oraz symulacji ruchu i ognia należały w tamtym czasie do najbardziej nowoczesnych. Dalsze prace rozwojowe nie były kontynuowane ze względu na zaniechanie finansowania.

Ponadto realizowano przedsięwzięcia związane z *polowym sprzętem komputerowym i metodami ochrony informacji.* W połowie lat 80 pojawił się problem: skali i sposobu realizacji

systemów polowych, spełniających rygorystyczne wymagania mechanoklimatyczne wynikające z Wojskowej Polskiej Normy (WPN 84) w oparciu o technikę mikrokomputerową. Wątpliwości wynikały z faktu, iż w przeciwieństwie do komputerów rodziny ODRA i MERA, mikrokomputerów w kraju nie produkowano. Proponowany wówczas przez IKSAIP przemysłowy mikrokomputer ELWRO 800 nie odpowiadał długofalowym tendencjom rozwojowym w dziedzinie automatyzacji dowodzenia i kierowania środkami walki. Sprzęt mikrokomputerowy odpowiadający prognozowanym potrzebom był wówczas praktycznie nieosiągalny (ograniczenia importowe, koszt, zagrożenia w zakresie bezpieczeństwa informacyjnego). Szczegółowe analizy wykazały, iż:

- Stosując odpowiednią selekcję i obróbkę (utwardzanie) komercyjnych pakietów mikrokomputerowych można zbudować mikrokomputer polowy spełniający co najmniej 8 grupę wymagań mechanoklimatycznych WPN 84 i gwarantujący praktycznie pełną szczelność elektromagnetyczną
- W komputerach polowych tego typu nawet do 70% kosztów stanowi obudowa, utwardzanie, wygłuszanie itp. zabiegi związane z przystosowaniem do specjalnych wymagań
- Kupując odpowiednie pakiety na otwartym rynku można uruchomić małoseryjną produkcję mikrokomputerów polowych stanowiących repliki sprzętu komercyjnego po kosztach nie przekraczających 50% ceny na rynkach zachodnich.

Dla potwierdzenia tej ostatniej tezy podjęto w WII pracę badawczo - rozwojową i jej efektem było zbudowanie prototypu polowego mikrokomputera klasy „zaawansowanego PC", a co ważniejsze, opracowanie technologii wytwarzania mikrokomputerów militarnych, spełniających międzynarodowe standardy szynowe. Do połowy lat 90 zbudowano w WII i CI SG dla różnych zastosowań wojskowych kilkanaście egzemplarzy tego komputera w różnych konfiguracjach architektonicznych.

Na początku lat 90 podjęto także problem integralnych urządzeń do szyfrowania informacji na nośnikach komputerowych i w mediach komunikacyjnych. Efektem prowadzonych prac było wtykowe (instalowane w standardowym gnieździe) urządzenie szyfrujące znane jako Indywidualny Moduł Szyfrujący (IMS). Urządzenie pracowało w oparciu o metodę klucza publicznego, zapewniając zależny tylko od długości kluczy poziom bezpieczeństwa informacyjnego.

Systemy MSWD czy POLAR były powodem dumy zawodowej. System grafiki operacyjnej wnosił nową jakość. W tym kontekście, rozwiązania opracowane w ramach tych programów mogły stanowić podstawę modyfikacji rozwojowych systemu na lata 2000 typu HEROS, WAVELL czy SICF.

Systemy informowania bieżącego, systemy bazowe

Jest to ważna grupa systemów informatycznych, funkcjonujących w obszarze Dyżurnych Służb Operacyjnych (segment Control w modelu C3I), Monitorowania

Sytuacji (segment Intelligence w modelu C3I) i systemy bazowe, których funkcją jest utrzymywanie referencyjnych baz danych, zasilających bazy systemów dziedzinowych (specjalistyczne) jednolitą informacją zewnętrzną.

Systemy Dyżurnych Służb Operacyjnych. Kompleksowe podejście do budowy informatycznego systemu DSO na początku lat 90 dało podstawę do:

- Bieżącego monitorowanie sytuacji w SZ RP i udostępnianie informacji osobom funkcyjnym sztabów,
- Integrację „kanałów meldunkowych" (Control) DSO z systemami monitorowania sytuacji powietrznej, morskiej i radioelektronicznej,
- Przejmowanie funkcji Stanowiska Dowodzenia Naczelnego Dowódcy w okresie narastania zagrożenia wojennego - do czasu rozwinięcia stanowisk dowodzenia.

Do połowy lat 90 zbudowano model demonstracyjny (użytkowy), wykorzystywany w codziennej pracy służby. Bazował on na komercyjnych pakietach i modułach programowych, opracowanych w ramach innych tematów (bazy danych, grafika operacyjna). Zastosowane wówczas rozwiązania zapewniały (przynajmniej teoretycznie) dyżurnej służbie operacyjnej funkcjonalność porównywalną z zachodnimi sojusznikami.

Systemy monitorowania sytuacji. Systemy operacyjnego monitorowania *sytuacji powietrznej* i *morskiej* były opracowywane przez organa informatyki podległe odpowiednio dowództwom WLOP i MW lub przez jednostki badawczo-rozwojowe pracujące na ich korzyść. System operacyjnego monitorowania *sytuacji radioelektronicznej*, ewidentnie przestarzały już w drugiej połowie lat 80, mógł być przydatny w latach 90 i być może dalszych pod warunkiem radykalnej modernizacji podsystemu zbierania informacji protokolarnej i jej uogólniania oraz osadzenia systemu na innej infrastrukturze telekomunikacyjnej. Jakkolwiek problem był postrzegany jako ważny i różne koncepcje modernizacji systemu były wielokrotnie rozpatrywane, to poważniejsze prace w tej dziedzinie nie były podjęte ze względów finansowych. Praktycznie duże znaczenie zachował do dziś opracowywany pod koniec lat 80 system monitorowania *sytuacji chemicznej, radiologicznej i bakteriologicznej* Szefostwa Wojsk Chemicznych (obecnie Wojsk Obrony Przeciwchemicznej), funkcjonujący w oparciu o strukturę Ośrodków Analizy Skażeń. Wojskowy Instytut Informatyki był współtwórcą oprogramowania systemu.

Systemy bazowe. Znaczenie systemów bazowych rośnie wraz ze skalą informatyzacji wielkich struktur organizacyjnych. W koncepcji rozwoju infrastruktury informacyjnej Sił Zbrojnych RP, opracowanej w WII na przełomie 1988/1989 głównie dla potrzeb planowania tzw. prac własnych, eksploatacja systemów bazowych miało być zasadnicza funkcją ośrodków obliczeniowych, których wyposażenie było też kompletowane głównie pod tym kątem (komputery IBM AS 400). Do połowy lat 1990 głównie przygotowywano bazę technologiczną do produkcji oprogramowania. Zaprojektowano także pewną liczbę systemów aplikacyjnych, w tym bazę cech adresowych jednostek wojskowych, etaty i należności.

Systemy pionów funkcjonalnych Sztabu Generalnego

Systemy sztabowe. W omawianym okresie w Wojskowym Instytucie Informatyki, a później Centrum Informatyki Sztabu Generalnego WP wdrażano corocznie kilka systemów informatycznych zabezpieczających potrzeby informacyjne instytucji szczebla centralnego: służb kwatermistrzowskich i technicznych, organów organizacyjno-etatowych i mobilizacyjno-uzupełnieniowych, organów kadrowych, finansowych itp. Generalnie były to systemy przeznaczone do okresowej eksploatacji w ośrodkach obliczeniowych, w cyklu odpowiadającym cyklowi ewidencyjno-sprawozdawczemu, kontrolnemu itp. - według specyfiki procesów realizowanych przez użytkownika.

W miarę upowszechniania się mikrokomputerów personalnych dojrzewała świadomość dramatycznej rozbieżności między możliwościami współczesnej technologii informacyjnej a ofertą usług tradycyjnej „informatyki ośrodkowej". W odpowiedzi na ewidentną potrzebę radykalnej zmiany technologii pracy komórek funkcjonalnych Sztabu Generalnego, dowództw RSZ i OW oraz szefostw RWiS, na początku lat 90 opracowano koncepcję **jednolitej infrastruktury informacyjnej** dowództw i sztabów. Dla zminimalizowania ewentualnych problemów interoperacyjność w relacjach międzynarodowych i zapewnienia odpowiedniego poziomu bezpieczeństwa informacyjnego systemów, koncepcję oparto na zaleceniach Departamentu Obrony USA *Technical Architecture Framework for Information Management.* Za podstawę przyjęto trzywarstwową architekturę, w której bazie lokalnej sieci komputerowej instytucji występuje warstwa serwerowa na platformie UNIX/INFORMIX, warstwa stacji roboczych na platformie Windows NT oraz warstwa routerowa jako sprzęg lokalnych sieci między sobą oraz z rozległą siecią telekomunikacyjną.

Zaawansowane aplikacje, szczególnie związane z komputerowym wspomaganiem specjalistycznych zadań komórek sztabowych, przewidziano na drugą połowę lat 90.

Systemy ogniw wykonawczych. Zarówno Zarząd XIV jak i WII co najmniej od połowy lat 80 dostrzegały kluczowa rolę organów wykonawczych pionu kwatermistrzowskiego i technicznego oraz pionu mobilizacyjno-uzupełnieniowego dla odtwarzania potencjału bojowego wojsk operacyjnych w czasie wojny. Efektem było znaczne zaangażowanie w informatyzację składnic i baz zaopatrzenia oraz Wojskowych Komend Uzupełnień a także Wojewódzkich (i eksperymentalnie) Regionalnych Sztabów Wojskowych. Pod względem skali wdrożeń, informatyzacja ogniw wykonawczych była do dziś przedsięwzięciem bezprecedensowym. O ile pierwsze instalacje składnicowe były realizowane na platformach komputerów MERA, to już systemy WKU i WSzW (RSzW) budowano na platformach UNIX/INFORMIX. Reprezentują one poziom informatyczny nie ustępujący standardom ogólnie akceptowanym w armiach NATO.

Niezależnie od sztandarowych przedsięwzięć badawczo-rozwojowych i projektowo-wdrożeniowych, o których wspomniano powyżej, w dorobku Wojskowego Instytutu

Informatyki, a później Centrum Informatyki Sztabu Generalnego WP znalazły się także prace o charakterze unikatowym. Można do nich zaliczyć zarówno systemy informatyczne (np.: systemy szpitalne, systemy komputerowej archiwacji dokumentów, systemy ewidencji i zobrazowania zasobów budowlanych) jak i opracowania analityczne (np. ekspertyza stanu bezpieczeństwa informacyjnego jednego z czołowych polskich banków). Szczególne miejsce w profilu WII/CI SG zajmowała zawsze problematyka telekomunikacyjna w segmencie związanym z tworzeniem sieci komputerowych.

Zakończenie

Przełom lat 80/90 był dla centralnego organu wykonawczego informatyki wojskowej, jakim był Wojskowy Instytut Informatyki, a później Centrum Informatyki Sztabu Generalnego WP, okresem wielkich wyzwań i odpowiedzialności za utrzymanie narodowej suwerenności w dziedzinie automatyzacji dowodzenia wojskami i kierowania środkami walki. Wyzwania te stanęły także, jakkolwiek w innej płaszczyźnie, przed instytucjami decydującymi o faktycznym miejscu i roli organów informatyki w strukturze Sił Zbrojnych RP. Jeśli czas potwierdzi znaczenie informatyki dla potencjału obronnego współczesnego państwa, jakie dziś skłonni jesteśmy jej przypisywać, to zapewne historia zechce też ocenić, w jakim stopniu wyzwaniom tym sprostaliśmy.

4

4. Koncepcja systemu Informatycznego SZ RP

płk dr inż. Piotr Zaskórski

Wprowadzenie

Informatyzacja sił zbrojnych jest wielodziedzinowym kompleksem przedsięwzięć organizacyjnych, badawczych, projektowych, produkcyjnych, wdrożeniowych, szkoleniowych oraz eksploatacyjnych. Obejmuje komputerowe wspomaganie dowodzenia i automatyzację procesu kierowania środkami walki oraz informatyzację zarządzania działalnością sił zbrojnych w czasie pokoju, zagrożeń i wojny. System Informatyczny Sił Zbrojnych RP (SI SZ RP) jest zbiorem systemów funkcjonujących na wszystkich szczeblach struktury organizacyjnej SZ RP, powiązanych technicznie, organizacyjnie, zadaniowo i informacyjnie (Rys. 2).

Rys. 2 Model współdziałania systemów informatycznych SZ RP

SI SZ RP jest strukturą hierarchiczną, która oznacza wzajemne uwarunkowania budowy i funkcjonowania składowych kompleksowego systemu. Poszczególne systemy przewidziane są do działania we wszystkich stanach, w których może się znaleźć państwo

lub część jego terytorium. Współdziałanie tych systemów jest głównym warunkiem użyteczności całego SI SZ RP.

Wszystkie obszary funkcjonalne powinny tworzyć spójną, komplementarną strukturę informacyjną dla:

- Procesu dowodzenia SZ RP w warunkach pokoju, zagrożeń i wojny,
- Procesu zarządzania i administrowania SZ RP,
- Procesu monitorowania wojsk własnych i sytuacji militarnej innych państw.

Komplementarność systemów oznacza potrzebę jednoznacznego identyfikowania gestorów i źródeł informacji.

Ocena stanu aktualnego

Charakterystyka ogólna

Funkcjonujące systemy informatyczne SZ RP zostały zaprojektowane dla pionów funkcjonalnych (dziedzinowych) lub jednostek organizacyjnych resortu obrony narodowej. Wiele z nich ma strukturę wieloszczeblową z powiązaniami funkcjonalnymi i technicznymi. Systemy te powstawały w długim okresie czasu, w którym nie zawsze istniały możliwości techniczne i organizacyjne do ich integracji. Eksploatacja tych systemów była organizowana w oparciu o stacjonarne ośrodki obliczeniowe, lokalne sieci obiektowe lub instytucjonalne, a także autonomicznie na bazie komputerów osobistych. Tylko część z nich ma możliwość korzystania z funkcjonujących sieci wymiany danych.

Eksploatowane systemy nie są w pełni adekwatne do zmian strukturalnych resortu oraz zmieniających się dynamicznie wymagań wynikających z członkostwa Polski w NATO. Zmiany strukturalne i funkcjonalne wymuszają konieczność ponownego zaprojektowania tej grupy systemów w postaci zintegrowanego kompleksowego systemu zapewniającego:

- Prowadzenie ewidencji i udostępnianie informacji,
- Planowanie i prognozowanie,
- Kierowanie i administrowanie,
- Kontrolę zadań i prowadzenie ocen.

Systemy organizacyjno-etatowe

W obszarze organizacyjno-etatowym funkcjonują systemy informatyczne wspomagające procesy:

- Ewidencji etatowych stanów osobowych i sprzętu wojska,
- Przygotowania i aktualizacji etatów - elementy struktur organizacyjnych SZ RP,
- Ewidencji cech adresowych jednostek wojskowych,
- Udostępniania danych.

Zmiany struktur organizacyjnych i zakresu kompetencji poszczególnych instytucji implikować będą potrzebę modernizacji wspólnych rozwiązań.

Systemy kadrowe

Działalność kadrowa jest wspierana przez system ewidencji osobowej żołnierzy zawodowych i system ewidencji osobowej pracowników wojska. System ewidencji osobowej wspomaga procesy:

- Utrzymywania danych osobowych i prowadzenia ewidencji stanów osobowych jednostek,
- Realizacji sprawozdawczości oraz dystrybucji danych i dokumentów między pionami kadrowymi instytucji.

System ewidencji osobowej pracowników wojska wspomaga działalność bieżącą komórek kadrowych instytucji na szczeblu centralnym (Biuro ds. Pracowników Wojska) oraz na szczeblu OW.

Systemy finansowe

Obszar finansowy jest w dużym stopniu zinformatyzowany i obejmuje:

- Ewidencję ilościowo-wartościową mienia wojskowego,
- Informowanie kierownictwa,
- Rachunkowość finansową działalności budżetowej i pozabudżetowej,
- Planowanie budżetowe i pozabudżetowe,
- Obrachunek uposażeń żołnierzy zawodowych, niezawodowych, wynagrodzeń pracowników wojska oraz wojskowych zaopatrzeń emerytalno-rentowych,
- Ewidencję i rozliczanie podatku dochodowego.

Zmiany systemu kierowania, unormowań prawnych oraz konieczność wymiany informacji między systemami powodują modyfikację istniejących rozwiązań i wymuszają ich zgodność z innymi rozwiązaniami resortowymi.

Systemy mobilizacyjno-uzupełnieniowe

W obszarze mobilizacyjno-uzupełnieniowym funkcjonuje kilka systemów. Do szczególnie ważnych należy system wspomagający działalność WKU w zakresie gospodarki zasobami osobowymi i środkami transportowymi. System ten wspomaga:

- Ewidencję poborowych,
- Ewidencję podoficerów i szeregowych rezerwy,
- Ewidencję środków transportowych,
- Procesy mobilizacji podoficerów i szeregowych rezerwy,
- Ewidencję oficerów i chorążych rezerwy,
- Procesy nadawania przydziałów mobilizacyjnych.

System logistyczny

System ten jest zbiorem systemów informatycznych występujących na wszystkich szczeblach struktury organizacyjnej SZ, spełniających funkcje komputerowego wspomagania zbierania, przechowywania i dystrybucji informacji logistycznych dla potrzeb zarządzania, dowodzenia i kierowania logistyką w okresie pokoju, sytuacji nadzwyczajnych i wojny. Wyróżnia się przy tym następujące grupy systemów informatycznych:

Logistyczne systemy bazowe (baza indeksowo-kodowa, normatywy, struktura zaopatrywania, zabezpieczenie materiałowe),

Terytorialne systemy logistyczne (gospodarka środkami materiałowymi, kierowanie zaopatrywaniem wojsk, kierowanie eksploatacją i remontami),

Systemy autonomiczne (wspomaganie osób funkcyjnych i specjalistycznych jednostek logistycznych),

Systemy dowodzenia (zautomatyzowany system kierowania zabezpieczeniem logistycznym).

Jednym z najważniejszych realizowanych przedsięwzięć w obszarze logistyki jest wdrożenie wieloszczeblowego systemu informatycznego kierowania eksploatacją oraz remontami uzbrojenia i sprzętu wojskowego.

Systemy bieżącego monitorowania SZ RP

Dostarczenie dowódcom i sztabom niezbędnych informacji operacyjnych do podejmowania decyzji i bieżącej pracy komórek organizacyjnych w siłach zbrojnych odpowiedzialnych za zbieranie i udostępnianie danych o aktualnej sytuacji jest bardzo ważnym obszarem. System monitoringu bieżącego SZ RP posiada strukturę wielostanowiskową, rozproszoną przestrzennie, wyposażoną w zautomatyzowane stanowiska pracy zainstalowane w ogniwach struktury organizacyjnej systemu i połączone ze sobą systemem telekomunikacyjnym, a do jego głównych zadań należy:

- Zbieranie i analiza informacji na temat sił, środków i dyslokacji wydzielonych wojsk do zadań specjalnych,
- Zbieranie danych o sytuacji operacyjnej w SZ RP,
- Zbieranie informacji o wojskach innych państw,
- Prezentowanie i archiwizowanie przetwarzanych informacji.

Systemy te umożliwią przyspieszenie obiegu informacji poprzez formalizację dokumentów oraz będą wspomagać osoby funkcyjne w zakresie wyszukiwania i analizy informacji.

Systemy informowania kierownictwa i wspomagania prac sztabowo-biurowych

Podstawowym zadaniem systemu informowania kierownictwa jest udostępnianie kierownictwu każdego szczebla wszechstronnej, przejrzystej i aktualnej informacji ułatwiającej podejmowanie decyzji i umożliwiającej skuteczne wykonywanie funkcji planistycznych, kontrolnych i operacyjnych. Celem informatyzacji instytucji wojskowej jest zastąpienie tradycyjnego systemu wytwarzania i obiegu dokumentów komputerowym wspomaganiem prac sztabowo–biurowych. Wprowadzenie systemu w pełnym wymiarze zapewni:

- Uporządkowany obieg i ochronę informacji wewnątrz instytucji,
- Gromadzenie, opracowywanie, wykorzystanie i udostępnianie informacji wewnętrznych i zewnętrznych,
- Opracowywanie dokumentów decyzyjnych, a w tym planów, prognoz i sprawozdań.

Zautomatyzowane systemy dowodzenia

Zautomatyzowane Systemy Dowodzenia (ZSyD) stwarzają warunki do wyprzedzania potencjalnego przeciwnika w realizacji cyklu dowodzenia i stanowią ważny czynnik wzmocnienia potencjału obronnego poprzez:

- Szybkie zbieranie informacji i utrzymywanie wiarygodnych danych o wojskach i terenie,
- Wieloaspektową analizę i ocenę sytuacji oraz wariantowe planowanie działań,
- Szybkie kalkulacje operacyjno-taktyczne i modelowanie oraz symulację wybranych działań bojowych,
- Sporządzanie i automatyczny obieg dokumentów bojowych w relacjach wewnętrznych i zewnętrznych oraz usprawnienie działalności sztabowej,
- Wymianę informacji graficznych z wykorzystaniem systemów GIS.

Aktualnie zbudowany jest demonstrator ZSyD dla potrzeb Naczelnego Dowódcy i Dowódcy Wojsk Lądowych, który powstał na bazie infrastruktury stacjonarnej z wykorzystaniem komercyjnego sprzętu i oprogramowania. Pod względem architektonicznym system posiada strukturę dwuwarstwową, obejmującą warstwę usług lokalnych i sieciowych. Poszczególni użytkownicy mogą pracować w oparciu o zautomatyzowane stanowiska pracy będące elementami sieci komputerowych poszczególnych stanowisk dowodzenia, które mogą zapewnić graficzną interakcję z mapą numeryczną. Elementy tego systemu mogą funkcjonować dla potrzeb różnych szczebli dowodzenia i wspomagać działalność szkoleniową, a także przygotowywać ćwiczenia oraz wspomagać kierowanie procesami rozwijania.

Trwają prace nad systemem taktycznym z rozwinięciem ZSyD do szczebla pododdziału poprzez zbudowanie rodziny zautomatyzowanych wozów dowodzenia oraz systemu wymiany danych na tych szczeblach.

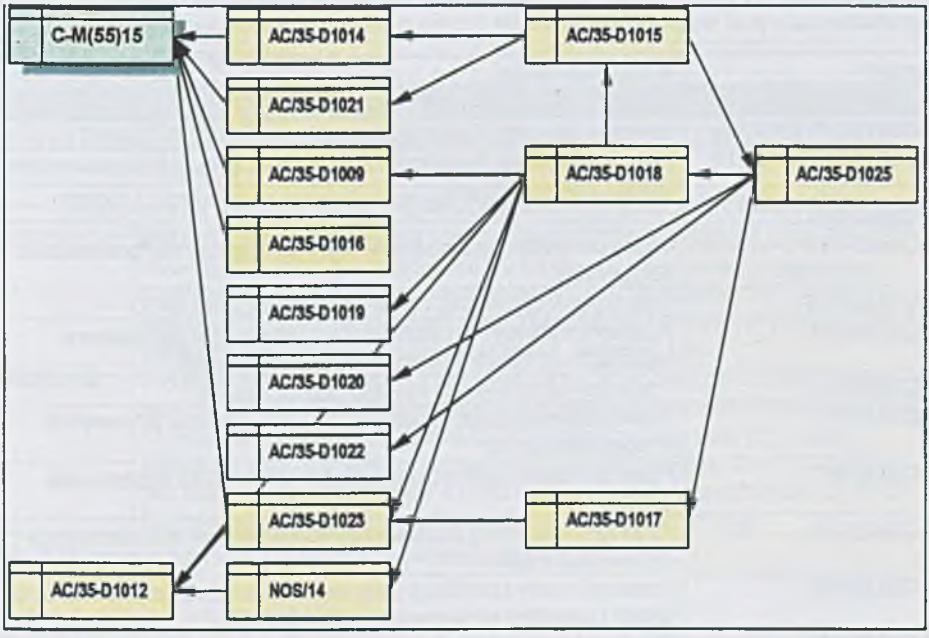
Wymagania NATO w zakresie współdziałania z systemem narodowym

Polska jest zobowiązana przez NATO do zapewnienia możliwości wymiany informacji niezbędnych w procesach informowania wzajemnego, planowania i realizowania wspólnych przedsięwzięć, a w tym wykonywania wielonarodowych operacji militarnych. Zadania te są realizowane poprzez wykorzystanie poczty elektronicznej oraz udostępnianie określonych kanałów informacyjnych i terminali systemów NATO. W perspektywie wieloletniej, wymagane będzie zwiększenie ilości i jakości powiązań między systemami łączności i informatyki. Stąd też projektowane rozwiązania muszą spełniać wiele szczegółowych wymagań w zakresie bezpieczeństwa, standardów wymiany informacji oraz w zakresie technologiczno-technicznym.

Bezpieczeństwo

Systemy narodowe muszą zapewniać wymianę informacji o różnych klauzulach poufności, aż do klauzuli NATO SECRET, co oznacza potrzebę:

- Zapewnienia właściwego poziomu tajności przechowywania i przesyłania informacji,
- Weryfikacji tożsamości i kontroli dostępu użytkowników,
- Zapewnienia bezpieczeństwa infrastruktury i urządzeń,
- Wdrożenia obligatoryjnych procedur postępowania.



Rys. 3 Struktura odwołań dokumentów NATO w zakresie bezpieczeństwa.

W zakresie bezpieczeństwa systemów informatycznych następuje dostosowanie polskiego prawodawstwa do standardów Unii Europejskiej i NATO (Rys. 3). Zmiany te mają wpływ na politykę bezpieczeństwa informacyjnego w resorcie Obrony Narodowej. Dokumenty związane z wojskowymi systemami teleinformatycznymi muszą przejść proces weryfikacji i nostryfikacji. Konieczna będzie weryfikacja i certyfikacja istniejących systemów. Kryteria oceny bezpieczeństwa obowiązujące w NATO zastosowane do polskich systemów wskazują, że tylko część z nich jest spełniona.

Wdrażanie wymagań NATO w zakresie bezpieczeństwa następuje poprzez odwoływanie się do „ACE Security Directive" (AD-70) z pominięciem polskiego prawodawstwa (Tab. 1).

Dokument AC/35-D/1012 będzie zastąpiony dokumentem określającym jednolite kryteria ocen produktów technologii informatycznych (**Common Criteria for Information Technology Security Evaluation - CCITSE**). Przyjęcie rygorystycznych wymagań pod względem bezpieczeństwa będzie powodować, że w systemach informatycznych należy zastosować bezpieczne produkty (Tab. 2).

Należy jednak zauważyć, że świadectwo bezpieczeństwa przy istotnych ograniczeniach uzyskały poprzednie wersje wyrobów funkcjonujące w określonym środowisku systemowym oraz sprzętowym. Lista produktów bezpiecznych zawiera tylko kilka produktów sieciowych i przykładowo brak jest poczty elektronicznej. System Windows NT otrzymał świadectwo bezpieczeństwa C2 przy bardzo silnych ograniczeniach pod względem sieciowym (poziom systemu autonomicznego).

Symbol	Nazwa dokumentu
C-M(55)15 (Final)	Bezpieczeństwo w NATO
AC/35 (WG/1) WP(94)4/x	(wytyczne dotyczące Wymagań Bezpieczeństwa Połączeń Systemu)
AC/35 (WG/1) WP(96)1/1	(wytyczne dotyczące Specyficznych dla Systemu Wymagań Bezpieczeństwa Informacji Elektronicznych)
AC/35-D/1000	
AC/35-D/1009	Ogólny przewodnik bezpieczeństwa systemów automatyzacji przetwarzania danych i sieci
AC/35-D/1012	Kryteria oceny bezpiecznych systemów komputerowych NATO
AC/35-D/1014	Przewodnik struktury i treści procedur wykonywania bezpieczeństwa w systemach automatyzacji przetwarzania danych i sieciach
AC/35-D/1015	Przewodnik opracowywania wymagań bezpieczeństwa
AC/35-D/1016	Przewodnik prowadzenia inspekcji i przeglądów systemów automatyzacji przetwarzania danych
AC/35-D/1017	Przewodnik analizy ryzyka bezpieczeństwa automatyzacji przetwarzania danych
AC/35-D/1018	Przewodnik specyfikacji charakterystyk bezpieczeństwa komputerowego w dokumentach dostawy
AC/35-D/1019	Przewodnik oceny i certyfikacji systemów i sieci automatyzacji przetwarzania danych i produktów bezpieczeństwa komputerowego
AC/35-D/1020	Przegląd charakteru i rozmiaru zagrożeń oraz podatności systemów i sieci automatyzacji przetwarzania danych

Symbol	Nazwa dokumentu
AC/35-D/1021	Przewodnik legalizacji systemów automatyzacji przetwarzania danych i sieci
AC/35-D/1022	Profesjonalny przewodnik polityki bezpieczeństwa dla połączeń sieci
AC/35-D/1023	Przewodnik oceny klas funkcjonalności i poziomów zabezpieczeń bezpieczeństwa komputerowego w określonych środowiskach
AC/35-D/1024	
AC/35-D/1025	Przewodnik organizacji i zarządzania bezpieczeństwem automatyzacji przetwarzania danych
NOS/14	Lista bezpiecznych produktów komputerowych NATO
	Lista bezpiecznych produktów komputerowych NATO podlegająca ocenie
	Lista zalecanych produktów NATO
AMSG	Allied Military Security Guideline (sojusznicze zalecenia bezpieczeństwa wojskowego)
MC	Military Communications (dokumenty łączności, w szczególności MC- 74/3: Bezpieczeństwo łączności NATO - COMSEC)

Tab. 1 Zasadnicze dokumenty NATO w zakresie bezpieczeństwa systemów informatycznych.

SYSTEMY OPERACYJNE OGÓLNEGO PRZEZNACZENIA	
POZIOM C2:	**AIX** v4.2, **AS/400** z **OS/400** v3r0m5, **HP-UX** v10.10, **Open VMS VAX** v6.1, **VAX/VMS** v 4.3, **SINIX** v5.42, **SOLARIS** v 2.4SE, **Windows NT** Workstation z NT Server v **3.51**, **Windows NT** Workstation z NT Server v**3.5** z SP3, Windows NT Serwer i Workstation v.4 z SP3
POZIOM B1:	**HP-UX BLS** v9.09+, **Trusted IRIX/B** v4.0.5EPL, **SEVMS VAX** v6.1, **Trusted SOLARIS** v1.2 ITSEC(E), **ULTRIX MLS+. Stacje robocze trybu ograniczonego: ARGUS B1/CMW** v1.2 (rozszerzenia dla Solaris 2.4, X-Windows), **DEC MLS+ CMW** v3.1A, **IBM E3/CMW** dla AIX
POZIOM B2:	**TRUSTED XENIX** v4.0
POZIOM B3:	**XTS-300** v STP 4.1 (system STOP 4.1 z Intel 80486 PC/AT i magistralą EISA, wiele interfejsów UNIX)
POZIOM A1:	**SCOMP** Secure Communications Processor v STOP r2.1 (dla 16-bitowych mikrokomp. Honeywell)
PRODUKTY SYSTEMÓW ZARZĄDZANIA BAZAMI DANYCH	
POZIOM C2:	**INFORMIX OnLine/Secure v5.0** (platforma Harris CX/SX, baza danych pojedynczego serwera), **INFORMIX OnLine/Secure-C2 v 5.0** (baza autonomiczna lub rozproszona z STAR/Secure na Sun Solaris; dostępna na unixy klasy C2), **ORACLE 7 v 7.0.13.6** (wymaga SO F-C2 ITSEC, na Sun Solaris), **ORACLE 7 v 7.0.13** (na HP-UX BLS, planowano inne platformy), **Sybase Secure SQL Server v 11.0.6**
POZIOM B1:	**INFORMIX OnLine/Secure v 5.0** (platforma Harris CX/SX; baza danych pojedynczego serwera), **INFORMIX OnLine/Secure-B1 v 5.0** (baza autonomiczna lub rozproszona z STAR/Secure na Sun Trusted Solaris CMW; dostępna na unixy klasy B1), **Trusted ORACLE 7 v 7.0.13.6** (wielopoziomowe bezpieczeństwo; wymaga SO F-B1 ITSEC; na Sun Solaris), **Trusted ORACLE 7 v 7.0.13** (wielopoziomowe bezpieczeństwo; na HP-UX BLS; planowano inne platformy), **Sybase Secure SQL Server v 11.0.6**

Tab. 2 Wybrane certyfikaty produktów programowych.

Infrastruktura

Zasadniczymi elementami infrastruktury niezbędnymi do współdziałania z NATO są jawne i utajnione sieci transmisji danych o pożądanej szybkości i jakości przesyłania. Do sieci wymiany danych NATO dołączony będzie szkielet jawnej poczty elektronicznej, szkielet sieci utajnionej poczty elektronicznej z wymianą wiadomości sformatowanych (ADatP-3) oraz wybrane systemy przetwarzania danych wraz z taktycznymi łączami transmisji danych NATO (LINK). Wymagać to będzie zakupu i alokacji sprzętu, oprogramowania, przeszkolenia personelu oraz specjalnego dostosowania pomieszczeń. Integracja naszych systemów z systemami NATO nastąpi poprzez dołączenie stacjonarnych elementów infrastruktury Sztabu Generalnego i Dowództw Rodzajów Sił Zbrojnych oraz jednostek wydzielonych.

Technologia

Spójność bazy technicznej i technologicznej oznacza potrzebę standaryzacji przyjętych rozwiązań. Problem ten staje się tym istotniejszy im bardziej zaawansowane są prace zmierzające do integracji ze strukturami NATO. Interoperacyjność w sferze technicznej wiąże się przede wszystkim z zabezpieczeniem wymiany danych pomiędzy systemami narodowymi. Proces ten wymaga określenia interfejsów, standardów protokołów oraz procedur zarządzania siecią. Złożoność tego problemu wymusza etapową realizację. W pierwszej fazie integracja obejmie wydzielone segmenty lokalnych sieci komputerowych oraz autonomiczne stanowiska pracy osób funkcyjnych.

Narodowe rozwiązania technologiczne powinny być **zgodne ze standardami państw NATO** (Rys. 4), określonymi w dokumentach standaryzacyjnych NATO (STANAG) i w normach organizacji międzynarodowych oraz państwowych (ISO, ANSI, NIST, X/Open, OSF itp.). Zasadnicze standardy w układzie warstwowym, od warstwy fizycznej odpowiedzialnej za nośniki informacji, poprzez warstwę połączeń, sieciową, transportową, sesji, prezentacji, aż po warstwę aplikacji są podstawą działania.

Na jakość systemów informatycznych, które obejmują różne dziedziny działania wpływają także normy z innych działów. Ze względu na wielonarodowy i wielojęzyczny charakter Sojuszu, jest w nim bardzo silnie rozwinięta sfera normalizacji. Należy więc uwzględniać wiele uwarunkowań standaryzacyjnych, które wpływają na przesyłanie, przetwarzanie i przechowywanie informacji.

Interfejsy poczty i przesyłania wiadomości

Do najistotniejszych standardów należeć będą standardy z zakresu wymiany informacji: wojskowej poczty elektronicznej X.400 (STANAG 4406 - MMHS), wymiany wiadomości (STANAG 5500 – ADatP-3), specyfikacje formatów wiadomości ACP, Compendium of Allied Land Force Messages (STANAG 2434 - APP-9, łącz danych taktycznych (STANAG 5501 dla Link 1, STANAG 5511 dla Link 11A i 11B oraz STANAG 5516 dla Link 16).

W ciągu najbliższych lat zostanie wdrożona nowa technologia wymiany informacji i protokoły przesyłania danych między bazami danych. W ramach budowy systemu taktycznego ATCCIS, systemu strategiczno-operacyjnego ACE CCIS oraz wysiłków stworzenia systemu ogólnonatowskiego, projektuje się szkieletową bazę danych (tzw. *General Hub*) wraz z protokołem wymiany danych. Prace te mają umożliwić osiągnięcie jednolitości i zgodności między dotychczas istniejącymi standardami, które posiadają wiele niespójności i redundancji. Dotychczasowe doświadczenia i eksperymenty wskazują, że jest to perspektywiczna droga rozwoju również dla naszych systemów narodowych.

Interoperacyjność

Podstawą interoperacyjności między systemami Polski i NATO będzie zapewnienie zgodności procedur wymiany danych między Zautomatyzowanymi Systemami Dowodzenia i bieżącego monitoringu.

Ze względu na problemy z interpretacją przekazów jest wymagane stosowanie jednolitych i otwartych formatów danych, protokołów, baz danych. Będzie to realizowane poprzez stosowanie standardów NATO. Zasadniczymi i perspektywicznymi kierunkami rozwoju informatyki są szeroko pojęte multimedia i ikonologia. W celu złagodzenia problemów językowych niezbędne będzie tworzenie aplikacji wielojęzycznych, dostarczanie aktywnych pomocy językowych i graficzne zobrazowanie treści.

BAZA TECHNOLOGICZNA					
BAZA PROGRAMISTYCZNA	INTRFEJS UŻYTKOWNIKA	ZARZĄDZANIE DANYMI	WYMIANA DANYCH	USŁUGI GRAFICZNE	USŁUGI KOMUNIKACYJNE
ADA COBOL (RPG) C/C++ PL 1 Narzędzia CASE ⇒ SNAP ⇒ PackBase ⇒ VisualAge ⇒ System Architect	X- Windows (MS –Windows) Motif	SQL 2 ISO RDA ODBC 2.0 IRDS Oracle DB2 Informix Sybase	Lotus-globalnie Exchange-lokalnie FORMETS CGM JPG LINK-16 HTML IGES RTF	PIGS CGM GKS MicroStation AUTOCAD Mapnik	NOSIP TCP/IP SMTP FTAM DMS X.400 X.500 ISDN
BEZPIECZEŃSTWO INFORMATYCZNE: GUARD, FIREWALL					
USŁUGI OCHRONY: OSI secr arch X.509			USŁUGI ZARZĄDZANIA SYSTEMEM: TIVOLI, DME, XMP, SNMP		
INTERFEJSY SYSTEMU OPERACYJNEGO: WINDOWS-NT, UNIX, POSIX, WIN-32					
INFRASTRUKTURA TECHNICZNA					

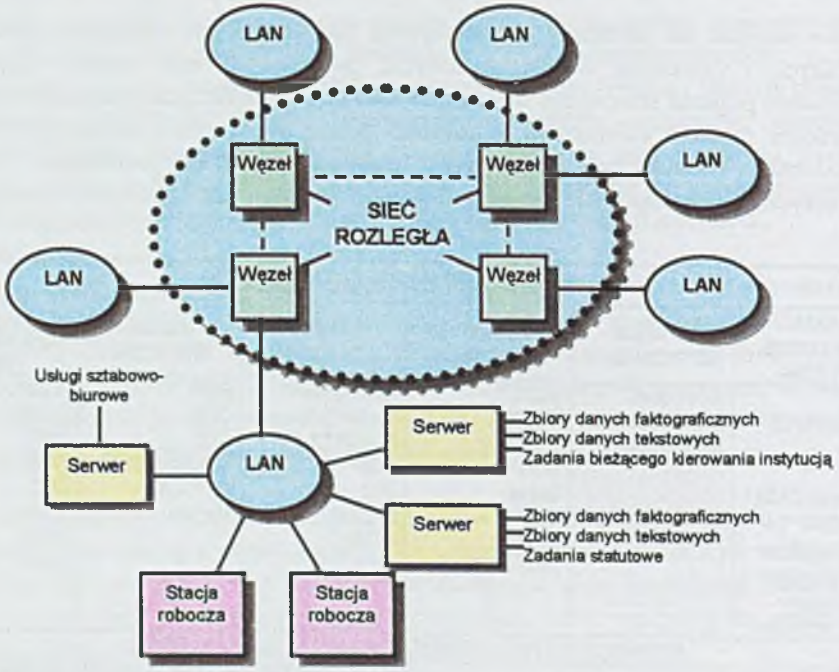
**) - prognozowane do włączenia*

Rys. 4 Zalecana baza technologiczna.

Koncepcja Systemu Informatycznego SZ RP

Docelowy System Informatyczny SZ RP będzie bazował na kompleksowej infrastrukturze teleinformatycznej integralnie związanej z systemami informatycznymi poszczególnych grup użytkowników. System informatyczny konkretnego użytkownika jest produktem sprzętowo-programowym wykonanym zgodnie z wymaganiami określonej struktury organizacyjnej i przeznaczony do wspomagania procesów informacyjno-decyzyjnych.

SI SZ RP powinien mieć charakter systemu narodowego, spełniającego wymagania formalno-prawne naszego Państwa. Powinien wspomagać instytucje, dowództwa, jednostki wojskowe występujące na wszystkich szczeblach struktury organizacyjnej dowodzenia i kierowania siłami zbrojnymi, a także współpracować z organami administracji państwowej oraz spełniać wymagania szeroko rozumianej interoperacyjności zapewniając współdziałanie z systemami NATO.



Rys. 5 Ogólna architektura SI SZ RP

Infrastrukturę SI SZ RP będą stanowić elementy stacjonarne, rozmieszczone na terytorium całego kraju i mobilne przeznaczone do działań operacyjnych. Ponadto muszą być zachowane wymagania bezpieczeństwa według standardów NATO, zapewniające przetwarzanie, przesyłanie, przechowywanie i udostępnianie danych niejawnych określonych kategorii. W ramach infrastruktury rozległej sieci komputerowej należy

określić relacje powiązań pomiędzy systemami informatycznymi z zastosowaniem kryterium zależności organizacyjnej i funkcjonalnej. Powiązania te muszą implikować interfejsy informacyjne wraz z zakresem informacyjnym i wymaganiami czasowymi meldunków i sprawozdań. Struktura systemu docelowego bazować będzie na standardzie modelu otwartego ISO.

System Informatyczny SZ RP w ujęciu modelowym obejmuje strukturę telekomunikacyjną i informatyczną. Sieć telekomunikacyjna zawiera w sobie rozległą sieć komputerową wraz z systemem zarządzania. Do węzłów tej sieci dołączane będą sieci lokalne, stanowiące strukturę telekomunikacyjną poszczególnych grup użytkowników. Stacje robocze będą końcowymi urządzeniami abonenckimi (Rys. 5).

Przyjęto, że dla systemu informatycznego użytkownika dostępny będzie: serwer realizacji zadań statutowych a także serwer realizacji zadań bieżących instytucji i serwer usług biurowo-sztabowych.

W każdym systemie informatycznym instytucji lub jednostki wojskowej przechowywane będą zbiory danych faktograficznych, określające stany obiektów informacyjnych i procesów realizowanych na tych obiektach oraz zbiory danych bieżących o stanie prawnym, normatywach i zadaniach.

Użytkownikami systemu informatycznego będą:

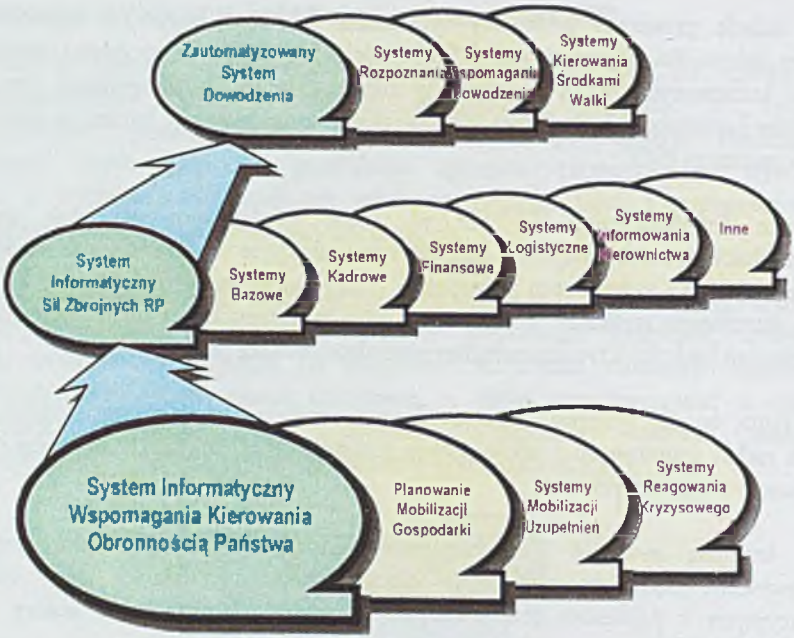
- Dowództwo wykorzystujące zbiory danych faktograficznych do procesów decyzyjnych,
- Specjaliści branżowi wykorzystujący zbiory danych faktograficznych i tekstowych w zakresie niezbędnym do realizacji procesów informacyjnych,
- Pracownicy instytucji wykorzystujący funkcje poczty elektronicznej w systemie sztabowo-biurowym.

Kompleksowy, docelowy SI SZ RP będzie strukturą hierarchiczną zapewniającą spójność informacyjną poprzez bazowanie na jednolicie opisanych strukturach organizacyjno-etatowych i systemach normatywnych.

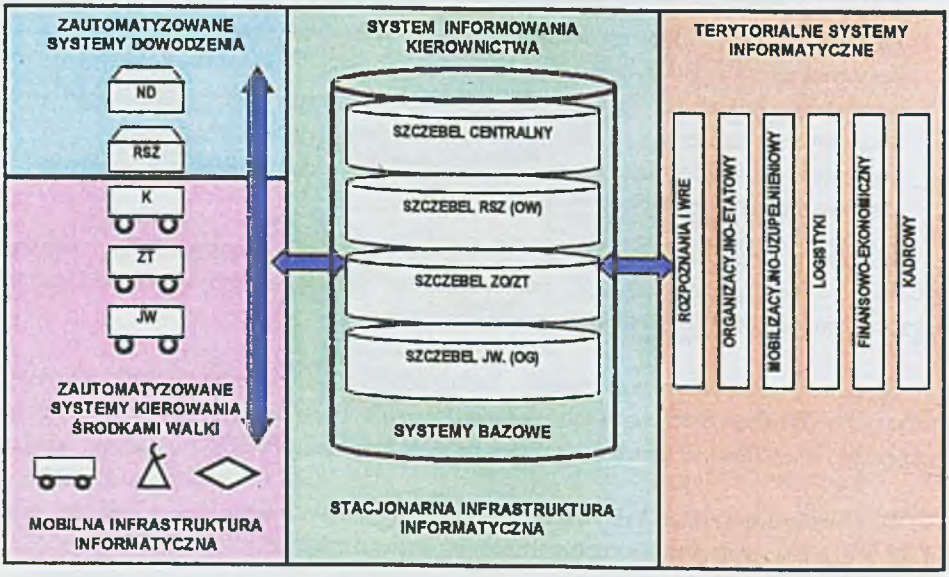
Systemy terytorialne wspomagać będą procesy zarządzania siłami zbrojnymi zarówno w układzie dziedzinowym jak i obiektowym. Będą one sprzężone z systemami gospodarki narodowej w aspekcie realizacji procesów mobilizacyjno-uzupełnieniowych.

W obszarze systemów kierowania obronnością państwa ważnym składnikiem będzie SI SZ RP, a jego najlepszą formą organizacyjną stanowić będzie ZSyD SZ RP (Rys. 6).

Budowane będą więc systemy informatyczne związków taktycznych i operacyjnych oraz systemy monitorowania (DSO) i rozpoznania (Rys. 7).



Rys. 6 Hierarchiczny model funkcjonalny SI SZ RP



Rys. 7 Struktura organizacyjno-funkcjonalna SI SZ RP

Pełna realizacja koncepcji docelowego SI SZ RP uwarunkowana jest budową stacjonarnej i mobilnej infrastruktury telekomunikacyjnej oraz funkcjonowaniem na

wszystkich szczeblach organizacyjnych lokalnych sieci komputerowych (serwery baz danych, dokumentów multimedialnych, poczty elektronicznej, zarządzania, ochrony systemu) z oprogramowaniem systemowym oraz użytkowym serwerów i stacji roboczych.

Systemy powinny być budowane zgodnie z dostępnymi standardami i zaleceniami NATO w zakresie technicznym, proceduralnym i operacyjnym. W pierwszym etapie należy zweryfikować oprogramowanie niezbędne do analizy koncepcji systemu, ukompletowania i funkcjonalności obiektów wraz z ich wyposażeniem, a w szczególności:

- Spójna platforma aplikacyjna (system operacyjny z oprogramowaniem usług użytkowych),
- Oprogramowanie baz danych z oprogramowaniem użytkowym i narzędziowym,
- Oprogramowanie w zakresie wytwarzania i obiegu sformalizowanych oraz niesformalizowanych dokumentów,
- Oprogramowanie zarządzania zasobami informacyjnymi i aplikacjami,
- Oprogramowanie bezpieczeństwa informacyjnego systemu.

W kolejnych etapach należy współbieżnie projektować specjalistyczne oprogramowanie użytkowe. Pełne wdrożenie rozwiązań informatycznych jest uwarunkowane możliwościami finansowymi w obszarze telekomunikacji i informatyki. Proces wdrażania złożonych systemów jest przedsięwzięciem wymagającym przygotowania organizacyjnego i technicznego.

Globalna informatyzacja SZ RP wymusi integrację systemów bazowych, dziedzinowych, obiektowych i autonomicznych. Docelowy zintegrowany system SZ RP składać się będzie z systemów dziedzinowych powiązanych ze sobą. Systemy te będą stanowić podstawę do działania stałych elementów ZSyD w czasie sytuacji nadzwyczajnych.

Kierunki dalszych prac

W najbliższej perspektywie planuje się przede wszystkim integrację usług i środowisk eksploatacji systemów SZ RP poprzez:

- Rozległą sieć wymiany danych gwarantującą bezpieczeństwo i odpowiedni poziom usług,
- Określenie i stosowanie jednolitych standardów i norm technicznych, technologicznych i informacyjnych,
- Tworzenie jednolitej bazy indeksowo-kodowej, słownikowej, struktur danych i zunifikowanych usług,
- Określenie i wdrożenie spójnych zasad bezpieczeństwa informacyjnego,
- Uodpornienie systemów na zmianę struktur organizacyjnych i funkcjonalnych SZ RP.

Do głównych kierunków rozwoju SI SZ RP w najbliższej perspektywie należeć będzie projektowanie, doskonalenie i wdrażanie:

- Bazowego systemu indeksowo-kodowego i ewidencji zasobów obronnych,
- Kompleksowego systemu wspomagania działalności resortu ON i informowania kierownictwa,
- Zintegrowanego, zautomatyzowanego systemu dowodzenia i kierowania wojskami.

Realizacja powyższych przedsięwzięć jest uwarunkowana:

- Zmianą statusu Centralnego Organu Informatycznego resortu ON upoważniającego do prowadzenia prac naukowo-badawczych we współpracy z firmami cywilnymi zapewniającymi możliwość kompleksowego wykonania systemu "pod klucz" dla dowództw, sztabów i instytucji,
- Klarowną oraz spójną politykę finansowania prac rozwojowych i wdrożeniowych w zakresie systemów informatycznych;
- Nowoczesną bazą techniczno-technologiczną do projektowania i wdrażania systemów nowej generacji,
- Drożnością procedur udostępniania danych oraz stabilnością struktur organizacyjnych i funkcjonalnych SZ RP;
- Aktywną polityką standaryzacyjną i szkoleniową użytkowników systemów.

Procesy informatyzacji SZ RP muszą uzyskać najwyższy priorytet wykonawczy, ponieważ zapewniają wymierny efekt wzmocnienia sprawności i potencjału obronnego państwa. Przekonują o tym wielorakie ekspertyzy specjalistów NATO.

Źródła informacji

Biuletyn nr 1 Centrum Informatyki Sztabu Generalnego WP, 1998 r.

Plany przedsięwzięć w dziedzinie informatyki w resorcie Obrony Narodowej.

Dokumenty projektowe systemów informatycznych opracowywanych przez CI SG WP.

Materiały Wojskowych Konferencji Teletransmisji i Informatyki, Zegrze.

Materiały Konferencji Naukowych Automatyzacji Dowodzenia, Jelenia Góra.

Materiały grup standaryzacyjnych NATO.

Technical Standards for Command and Control Information Systems (CCISs) and Information Technology, NATO.

Studium interoperacyjności systemów C4 dla Polski.

5

5. Projektowanie zintegrowanych systemów informatycznych

płk prof. dr hab. inż. Andrzej Barczak

Uwarunkowania realizacyjne

Zintegrowane Systemy Informatyczne (ZSI) są najbardziej zaawansowaną formą rozwiązań informatycznych wspomagających procesy zarządzania, a więc wymagają od przyszłych użytkowników spełnienia bardzo wielu warunków, determinujących efektywne wdrożenie i eksploatację.

Projekty informatyczne są z wielu powodów trudne w planowaniu i realizacji. Brakuje im tzw. efektu skali, charakterystycznego dla produktów materialnych. Efekt ten powoduje, że jednostkowe koszty produkcji maleją przy wzroście jej rozmiarów. W przedsięwzięciach informatycznych jest na ogół odwrotnie. Przy wzroście złożoności systemu koszt jego wytworzenia wzrasta nieproporcjonalnie. W projektach informatycznych mamy także do czynienia z paradoksalną, zdawałoby się, sytuacją. Częstokroć rozpoczynając projekt informatyczny, nie wiemy dokładnie, w jakiej technologii i za pomocą jakich narzędzi będzie on zrealizowany. Dzieje się tak w wyniku naturalnego dążenia twórców systemu do unowocześnienia rozwiązań oddawanych do użytku.

Projekty informatyczne są zwykle źle uwarunkowane. Nie stoją za nimi setki i tysiące lat doświadczeń ludzkości lub też duże, zbiorowe doświadczenie i dobrze sprecyzowane wyniki. Projektowanie ZSI w wielu przypadkach kończy się więc, niestety, tylko połowicznym sukcesem. Znaczna bowiem część przedsięwzięć informatycznych tego rodzaju jest opóźniona, przekracza przewidziany budżet i często nie spełnia zasadniczych oczekiwań użytkowników. Zdecydowana większość przyczyn tego stanu rzeczy jest spowodowana przede wszystkim złą organizacją prac przygotowawczych i projektowo-wdrożeniowych.

Proces projektowania ZSI należy rozpatrywać w kategoriach złożonego przedsięwzięcia informatycznego. Dokonuje się on przy zaangażowaniu dużych zasobów finansowych informatyzowanej instytucji oraz przy następujących założeniach:

- Proces obejmuje cały cykl życia systemu informatycznego, od studium wykonalności i analizy problemu, poprzez zadanie projektowe, projekt koncepcyjny i technologiczny, aż po wdrożenie, eksploatację użytkową i rozwój;
- Z uwagi na złożoność procesu i jego interdyscyplinarny charakter wymaga on udziału specjalistów z wielu dziedzin: informatyki, zarządzania, finansów, a niekiedy także zastosowań matematyki;
- Kierownictwo instytucji aktywnie uczestniczy w procesie informatyzacji, przykładając dużą wagę do eksploatacji wdrożonego ZSI, traktując to jako realizację perspektywicznych celów;
- Postrzegalny jest kompleksowy zakres proponowanego rozwiązania informatycznego, tak w ramach struktury funkcjonalnej, jak i realizacyjnej.

Niezależnie od przyjętego modelu rozwoju zastosowań informatyki w instytucji (niezależny, relatywny, współzależny) trzeba stwierdzić, że powodzenie pełnego wykorzystania technologii informatycznych wspomagających procesy zarządzania jest skutkiem integracji długofalowych planów strategicznych rozwoju z planami zastosowań rozwiązań informatycznych. Przedsięwzięcia, w których nie występują rzeczywiste powiązania między strategią instytucji i strategią rozwoju infrastruktury informatycznej, są nieefektywne i charakteryzuje je wiele negatywnych zjawisk. Do zasadniczych z nich należy zaliczyć m.in. to, że:

- Nie zmieniają w sposób istotny organizacji pracy instytucji;
- Nie umożliwiają integrację funkcji zarządzania wewnątrz instytucji i jej otoczenia;
- Nie powodują istotnych zmian w pozycji instytucji na rynku;
- Nie stwarzają nowych strategicznych szans dla informatyzowanej instytucji;
- Nie doprowadzają do istotnych zmian w praktyce zarządzania oraz w strukturach organizacyjnych instytucji.

Współcześnie zarysowuje się pozytywna tendencja w zakresie poszukiwania efektywnych strategii informatyzacji, a jej przykładem jest wykorzystywanie światowych standardów systemów informatycznych, takich np. jak R/3 (SAP), System 21 (JBA), Baan IV (Baan).

Należy jednak zwrócić uwagę, że istotą efektywnego podejścia w tym zakresie są przede wszystkim problemy związane z określaniem celów informatyzacji instytucji. Problematyka formułowania celów działania instytucji w połączeniu ze strategią informatyzacji jest zdeterminowana między innymi tym, że:

- Nie wszystkie instytucje mają jasno sformułowaną strategię rozwoju, a jej definiowanie i wdrażanie często wymaga długiego czasu;
- Transformacja wypracowanej strategii na bieżące działania jest procesem bardzo trudnym;
- Określenie efektów informatyzacji *a priori* ma w zasadzie charakter jakościowy, a rzetelne ilościowe analizy ex post są trudne do realizacji.

Problematyka ta oczywiście nie ma zbyt długiej tradycji. Zaczęła upowszechniać się na początku lat 90, a jej istotą jest łączenie na poziomie strategicznym instytucji takich elementów jak:

- Cele, produkty, rynki i grupy klientów;
- Analiza potencjału wewnętrznego ze szczególnym uwzględnieniem wsparcia informatycznego;
- Analiza otoczenia zewnętrznego i czynników związanych z technologią informatyczną;
- Analiza technologii informatycznej.

Efektem tej metody, która w literaturze przedmiotu znana jest jako metoda ITSGA (ang. *Information Technology Strategic Generic Actions)*, jest określenie działań strategicznych, w tym także z zakresu technologii informatycznych, które mają być realizowane jako składowe ogólnej strategii funkcjonowania przedsiębiorstwa.

Zakres i struktura

Zintegrowany system informatyczny charakteryzuje się przede wszystkim:

- Kompleksowością funkcjonalną- obejmuje wszystkie sfery działalności instytucji;
- Integracją danych i procesów wewnątrz instytucji oraz jej otoczenia - realizowaną w ramach struktury informatycznej;
- Elastycznością strukturalną i funkcjonalną, zapewniającą maksymalne dostosowanie rozwiązań sprzętowo-programowych do potrzeb instytucji w chwili instalowania i uruchamiania systemu oraz umożliwiającą dynamiczne jego dopasowanie przy zmiennych wymaganiach i potrzebach generowanych przez otoczenie;
- Otwartością - gwarantującą zdolność rozszerzania systemu o nowe moduły, skalowalną architekturą;
- Zaawansowaniem merytorycznym, zapewniającym pełne informatyczne wsparcie procesów informacyjno-decyzyjnych z wykorzystaniem mechanizmów ekstrakcji i agregacji danych, wariantowania, optymalizacji i programowania;
- Zaawansowaniem technologicznym gwarantującym zgodność z aktualnymi standardami sprzętowo-programowymi, możliwością przenoszenia na nowe platformy sprzętowe, systemów operacyjnych oraz mediów i protokołów komunikacyjnych;
- Zgodnością z aktualnie obowiązującymi przepisami normującymi działalność informatyzowanego instytucji.

Zintegrowany system informatyczny obejmuje w istocie rzeczy zwykle takie moduły i podsystemy jak:

- Gospodarczy system informacyjny;
- Komputerowe wspomaganie procesów inżynierskich;
- Komputerowe wspomaganie zarządzania jakością;
- Komputerowe wspomaganie zarządzania produkcją;

- Komputerowe wspomaganie projektowania;
- Komputerowe wspomaganie wytwarzania;
- Komputerowo wspomagane projektowanie procesu produkcyjnego;
- Komputerowo wspomagane planowanie procesu produkcyjnego;
- Komputerowo wspomagane sterowanie procesu produkcyjnego;
- System planowania i zarządzania zdolnościami produkcyjnymi;
- System planowania, kontroli oraz sterowania produkcją.

Szacowanie zasobów

Tendencje rozwojowe systemów informatycznych wykazują jednoznacznie na wzrost udziału kosztów analizy, projektowania, kodowania, testowania, wdrożenia, utrzymania i rozwoju w ogólnych kosztach systemów.

Nacisk kierownictwa i użytkownika na bardzo szczegółowe oceny na początkowych etapach prac nad systemem informatycznym jest zjawiskiem powszechnym i naturalnym. Wiąże się on z chęcią zaplanowania globalnych nakładów i zasobów potrzebnych do budowy systemu. Niestety, często te szacunki są potem wpisane do umów i, w konsekwencji, bardzo ściśle przestrzegane. Tymczasem na wstępnych etapach projektu duży błąd szacowania jest z natury rzeczy bardzo prawdopodobny, maleje natomiast w miarę postępu prac (pod warunkiem dokonywania kolejnych estymacji).

Szacowanie zasobów w projektach informatycznych jest kombinacją dobrych danych historycznych (doświadczeń) i metod ich wykorzystania w nowych przypadkach. Metody są różne i zwykle wykorzystywane łącznie, tj. do oszacowania zasobów projektu wykorzystuje się równocześnie dwie metody lub więcej. Można wyróżnić następujące możliwe sposoby szacowania zasobów projektów informatycznych:

- Opóźnianie oszacowań;
- Analogia;
- Metody dekompozycyjne;
- Ekstrapolacja przy pomocy różnych empirycznych modeli parametrycznych.

Opóźnianie procesu oszacowania pracochłonności i przenoszenie go na późniejsze etapy projektu ma swoje uzasadnienie w prostej zasadzie - im później oceniasz, tym więcej wiesz. W praktyce jednak, z wielu oczywistych względów, nie udaje się skutecznie stosować tej "metody".

Szacowanie przez analogię wymaga posiadania dużego doświadczenia w realizacji podobnych projektów. Można w tej metodzie opierać się także na doświadczeniach innych projektów informatycznych. Doświadczenia te, ujęte w wykresy i tabele pracochłonności poszczególnych etapów projektów umożliwiają, po oszacowaniu nakładów na jeden etap, wyznaczenie nakładów na cały projekt.

Idea **metod dekompozycyjnych** zakłada podział projektu informatycznego na wiele szczegółowych zadań, oszacowanie pracochłonności każdego z nich i wyznaczenie na tej podstawie pracochłonności całego projektu.

Metody ekstrapolacyjne polegają na budowie empirycznych modeli, pozwalających oszacować wielkości zasobów w projektach informatycznych na podstawie atrybutów produktywności. Modele te są opracowywane na podstawie danych empirycznych.

Do najbardziej znanych modeli parametrycznych należą:

- Model "linii kodu";
- Metoda punktów funkcyjnych;
- Model COCOMO (ang. *COnstructive COst Model).*

W **metodzie "linii kodu"** poważny problem stanowi samo pojęcie linii kodu. Czy komentarz w kodzie programu jest potrzebny i zliczany czy też nie? Linia linii nie jest równa. Co z poleceniami zajmującymi szereg linii? Czy deklaracje są liniami kodu?

Niska skuteczność modeli "linii kodu" wynika także z innego faktu. Mianowicie zużycie zasobów (w tym i pracochłonność) na kodowanie i testowanie nie przekracza na ogół 40-50% całkowitego zużycia w całym projekcie. Zwiększenie efektywności prac w wyniku zastosowania np. dwukrotnie "wydajniejszego" języka oprogramowania nie doprowadza do dwukrotnego zmniejszenia zasobochłonności projektu, głównie dlatego, że złożoność i, w konsekwencji, koszt prac analityczno-projektowych mało zależą od języka programowania. Uzależnione są one przede wszystkim od tego, co i w jaki sposób ma realizować aplikacja.

Metoda punktów funkcyjnych wydziela parametry przetwarzania w systemie informatycznym jako atrybuty produktywności dla nieistniejącego systemu. Szacuje wpływ każdego z nich na produktywność i nakłada na tę ocenę szacunek wpływu warunków realizacji projektu informatycznego. Wyznaczone w ten sposób punkty funkcyjne są traktowane jako miara produktywności, a więc i złożoności, a co za tym idzie - pracochłonności projektu informatycznego.

Metoda punktów funkcyjnych umożliwia oszacowanie złożoności projektu informatycznego z uwzględnieniem dwóch różnych grup czynników:

- Elementów przetwarzania informacji w systemie (w aspekcie funkcjonalnym i informacyjnym). Elementy te, to: wejścia i wyjścia z systemu, zbiory danych wewnętrznych i zewnętrznych i zapytania do bazy danych.
- Całościowej oceny stopnia złożoności systemu i warunków jego realizacji w postaci różnorodnych czynników korygujących składających się na kompleksowy współczynnik korygujący.

Nie skorygowane punkty funkcyjne wyznacza się jako ważoną sumę liczby elementów przetwarzania, występujących w systemie informatycznym, w pięciu następujących grupach, z uwzględnieniem wag o trzech poziomach wartości oceniających poziom złożoności elementu:

- Wejście użytkownika;
- Wyjście użytkownika;
- Zbiory danych wewnętrzne;
- Zbiory danych zewnętrzne;
- Zapytania zewnętrzne.

Wyznaczone w powyższy sposób nie skorygowane punkty funkcyjne podlegają modyfikacjom, uwzględniającym wpływ innych parametrów projektu.

Metoda punktów funkcyjnych wyróżnia następujące czynniki korygujące:

- Występowanie urządzeń komunikacyjnych;
- Rozproszenie przetwarzania;
- Czas oczekiwania na odpowiedź systemu;
- Stopień obciążenia systemu;
- Częstotliwość wykonywania transakcji;
- Wprowadzanie danych w trybie bezpośrednim;
- Wydajność użytkownika końcowego;
- Aktualizacja danych w trybie bezpośrednim;
- Złożoność przetwarzania danych;
- Możliwość ponownego użycia programów w innych zastosowaniach;
- Łatwość instalacji;
- Łatwość obsługi systemu;
- Rozproszenie terytorialne;
- Łatwość wprowadzania zmian - pielęgnowania systemu.

Wpływ każdego z powyższych czternastu czynników może być różny w danym projekcie. Jest on szacowany w skali sześciostopniowej (0, 1, 2, 3, 4, 5). Im większy, bardziej znaczący wpływ danego czynnika, tym wyższa jego ocena punktowa.

Metoda punktów funkcyjnych jest uniwersalną metodą pomiaru złożoności projektów informatycznych i umożliwia również:

- *Auditing* projektów;
- Wybór systemów informatycznych funkcjonujących w przedsiębiorstwie do *reengineeringu;*
- Szacowanie liczby testów;
- Ocenę jakości pracy i wydajności zespołów ludzkich;
- Ocenę stopnia zmian wprowadzanych przez użytkownika na poszczególnych etapach budowy systemu informatycznego (wymaga to ciągłego przeliczania punktów funkcyjnych, ale odwzorowuje zakres i koszt modyfikacji);

- Prognozowanie kosztów pielęgnacji i rozwoju systemów;
- Porównanie i ocenę różnych ofert dostawców oprogramowania pod kątem merytorycznym i kosztownym (np. Koszt jednego punktu).

Projektowanie

Zakres prac projektowych obejmujący realizację ZSI dzieli się zwykle na następujące etapy:

- Definiowanie zadania projektowego;
- Analizę funkcjonalną i specyfikację wymagań;
- Analizę otoczenia systemu;
- Projektowanie koncepcyjne;
- Projektowanie technologiczne;
- Testowanie;
- Wdrażanie, eksploatację i rozwój systemu.

W praktyce ZSI projektuje się wg różnych modeli cyklu życia systemu. W większości przypadków wykorzystuje się tradycyjny, **liniowy model** cyklu życia systemu. Model ten odpowiada w sposób naturalny działaniom projektowo-wdrożeniowym. Zazwyczaj jednak prace projektowe nie przebiegają nigdy w sposób sekwencyjny i z każdej fazy cyklu następuje powrót do poprzednich, a także część prac związanych z daną fazą może być wykonywana jednocześnie z częścią prac innej fazy.

Innym podejściem do realizacji ZSI jest tzw. **model prototypowania**. Jego istota sprowadza się do tego, że zamiast przygotowywać model nowego systemu, prezentowany jest przyszłym użytkownikom system prototypowy, a następnie dokonuje się jego iteracyjnej modyfikacji. Celem takiego działania jest między innymi:

- Skrócenie czasu oczekiwania na rezultaty prac projektowych;
- Zapewnienie efektywnego współdziałania użytkowników i projektantów ZSI;
- Skuteczniejszy opis potrzeb i ograniczenie liczby błędów dzięki lepszemu zrozumieniu potrzeb użytkownika;
- Istotne zwiększenie zaangażowania użytkownika w proces analizy potrzeb i projektowania systemu.

W ramach modelu prototypowania wyróżnić można dwa generalne podejścia:

- **Prototypowanie specyfikacji wymagań** - służy tylko do zdefiniowania wymagań użytkownika;
- **Prototypowanie rozwoju** - przygotowany system zostaje przekształcony w docelowy ZSI, spełniający wszystkie wymagania użytkownika.

Zainteresowanie projektantów zdobywa także **model spiralny**, stanowiący pewną odmianę modelu prototypowania. Pojawia się w nim dodatkowa faza, a mianowicie analiza ryzyka systemu. Cykl spiralny rozpoczyna się od planowania, obejmującego

analizę wstępnych wymagań użytkownika, a następnie wchodzi w fazę analizy ryzyka. Tu następuje ocena stopnia zagrożenia dla realizacji oczekiwań użytkownika w odniesieniu do proponowanego wariantu ZSI. W fazie wstępnej przygotowywana jest wersja prototypowa systemu, która w kolejnej fazie jest poddawana weryfikacji.

Przyjęta metodyka projektowania ZSI w praktyce rzadko odpowiada jednoznacznie jednemu z trzech omówionych modeli. Zwykle stanowi ona wariant mieszany, w którym akcenty rozkładają się różnie w zależności od założeń metodologicznych przyjmowanych przez zespół autorski.

Złożoność procesu projektowania ZSI jest przyczyną wielu błędów, które na różnych poziomach realizacyjnych można ująć następująco:

1) Na poziomie definiowania przedsięwzięcia informatycznego:
   a) Brak jasno sformułowanych celów przedsięwzięcia,
   b) Niezgodność działań projektowych ze strategią funkcjonowania i rozwoju przedsiębiorstwa,
   c) Brak należytego poparcia kierownictwa strategicznego,
   d) Nieadekwatność stosowanej technologii informatycznej do rzeczywistych potrzeb i możliwości instytucji,
   e) Niedocenianie barier we wprowadzaniu zmian;
2) Na poziomie planowania prac projektowych:
   a) Stosowanie nieefektywnych metod i narzędzi planowania,
   b) Zbyt optymistyczne oszacowania czasu trwania i kosztów projektu,
   c) Brak wszechstronnej analizy różnych scenariuszy realizacyjnych;
3) Na poziomie organizowania i koordynowania prac projektowych:
   a) Brak właściwych procedur organizacyjnych,
   b) Brak właściwej organizacji zespołów realizacyjnych, wynikającej ze specyfiki przedsięwzięcia,
   c) Niesprawności organizacyjne w zakresie monitorowania postępu prac i mechanizmów kontrolnych,
   d) Wadliwe mechanizmy motywowania realizatorów systemu;
4) Na poziomie realizacji projektu:
   a) Niekontrolowane zmiany w planie przedsięwzięcia,
   b) Rozpoczynanie prac w niewłaściwej kolejności,
   c) Niedocenianie trudności w kierowaniu ludźmi,
5) Na poziomie kontroli prac projektowych:
   a) Nieefektywny system komunikacji w zespołach wykonawczych, uniemożliwiający bieżącą kontrolę działań,
   b) Brak identyfikacji przyczyn odstępstw od planu (usuwanie skutków, a nie przyczyn),
   c) Brak działań korygujących;
6) Na poziomie organizacji pracy zespołów wykonawczych:
   a) Niedocenianie trudności w organizowaniu pracy zespołowej,

b) Brak właściwego systemu motywowania zespołu wykonawczego,
c) Nieprecyzyjne delegowanie zakresu obowiązków i odpowiedzialności oraz uprawnień i możliwości ich egzekwowania,
d) Niedocenianie roli kierownika przedsięwzięcia.

Wśród różnych scenariuszy realizacji ZSI instytucji możliwe są trzy następujące warianty postępowania:

1) Tworzenie ZSI od podstaw przez służby informatyczne przedsiębiorstwa:
   a) Zamiar mało realny dla przedsięwzięć średnich i dużych z uwagi na długi okres prac projektowo-wdrożeniowych i konieczność dysponowania rozbudowanym zespołem wysoko kwalifikowanych wykonawców, brak przekonywającego uzasadnienia ekonomicznego ze względu na bardzo duże nakłady czasowo-finansowe;
2) Zlecenie wykonania ZSI od podstaw zewnętrznej firmie informatycznej:
   a) Wynika z konieczności przygotowania indywidualnego systemu dla potrzeb konkretnego przedsiębiorstwa,
   b) Wymaga zazwyczaj zapytania ofertowego w celu wyłonienia potencjalnych wykonawców i dokonanie wyboru najlepszej z ofert,
   c) Oznacza całkowite uzależnienie się od zewnętrznych wykonawców, co może grozić utratą koniecznej kontroli w zakresie prowadzenia przyszłościowych prac rozwojowych planowanego systemu,
   d) W przypadku braku należytej organizacji prac projektowo-wdrożeniowych efekt końcowy może być daleki od oczekiwanych - powstanie system nie odpowiadający kierownictwu informatyzowanego przedsiębiorstwa,
   e) Konieczny jest zazwyczaj długi czas realizacji, a z uwagi na nie kończące się testowanie poszczególnych modułów systemu i ich integracji, efekt pełnego wdrożenia będzie permanentnie odraczany,
   f) Trudne są do oszacowania dokładniejsze nakłady czasowo-finansowe (przyjęte w kontrakcie odpowiednie wyliczenia z reguły są przekraczane w 200-300 %.),
   g) Bardzo niebezpieczne mogą być wszelkie wewnętrzne perturbacje w zespołach wykonawców (np. Rotacje projektantów, analityków, programistów, zmiany statusu funkcjonowania poszczególnych wykonawców, „zniknięcia" z rynku kooperantów),
   h) Wariant zalecany dla przedsiębiorstw o wyraźnej specyfice organizacyjno-technicznej;
3) Wybór, zakup i wdrożenie gotowego ZSI:
   a) Zakładana jest możliwość zaspokojenia potrzeb informatycznego wsparcia zarządzania w przedsiębiorstwie poprzez wybór jednego z dostępnych i sprawdzonych systemów zintegrowanych.

Wdrażanie

Jak wskazuje praktyka, najtrudniejsze jest zwykle wdrażanie systemów. Na przeszkodzie w skutecznej realizacji pełnego wdrożenia ZSI stoją:

1) W wymiarze czasowym:
   a) Błędy szacowania czasu trwania poszczególnych faz (czynności) wdrożenia,
   b) Przekraczanie deklarowanych terminów całego przedsięwzięcia i poszczególnych etapów, obejmujących wdrażanie kolejnych modułów,
   c) Zbyt długi czas usuwania błędów,
   d) Przecenianie technicznych aspektów przedsięwzięcia,
   e) Źle zaplanowane i skoordynowane terminy szkolenia i testowania systemu;
2) W wymiarze kosztów:
   a) Błędy w metodach planowania,
   b) Zbyt wysokie koszty przedsięwzięcia,
   c) Przekraczanie zaplanowanego budżetu,
   d) Brak należytej kontroli kosztów,
3) W wymiarze jakości:
   a) Niewystarczająca specyfikacja wymagań użytkownika,
   b) Ograniczona funkcjonalność systemu,
   c) Zawodność proponowanych rozwiązań,
   d) Niedostateczna wydajność systemu,
   e) Ograniczone możliwości rozwojowe rozwiązania,
   f) Złe praktyki testowania i odbioru etapów prac oraz całego systemu,
   g) Bagatelizowanie problematyki zarządzania jakością
   h) Brak kompletnej dokumentacji;
4) W wymiarze akceptacji działań przez użytkownika:
   a) Brak wystarczającej aktywności użytkownika w specyfikacji swoich wymagań względem realizowanego ZSI,
   b) Pomijanie użytkownika w pracach zespołu projektowo-wdrożeniowego,
   c) Brak udziału użytkownika w testowaniu i odbiorze systemu,
   d) Niedostateczne angażowanie użytkownika, a zwłaszcza - naczelnego kierownictwa przedsiębiorstwa, w procesy decyzyjne zarządzania przedsięwzięciem (dotyczy to zwłaszcza ewentualnych zmian w odniesieniu do zakresu prowadzonych prac, harmonogramu i budżetu).

W świetle powyższych rozważań wyróżniki udanej realizacji ZSI, jako określonej kategorii SI, można określić następująco:

- Wdrażając system nie ograniczono zakresu funkcjonalnego w stosunku do przyjętych założeń;
- Parametry eksploatacyjne ZSI są zgodne z zakładanymi;
- Rozwiązanie akceptują bezpośredni użytkownicy, wykorzystując go w pełni oraz zgodnie ze wcześniejszymi założeniami;
- Wdrożenie ZSI przyniosło zakładane korzyści;

- Utrzymano się w przyjętym harmonogramie działań i budżecie przy dotrzymaniu zakładanego poziomu jakości wdrożonego systemu.

Wyróżniki te stanowią pewien wzorzec, pozwalający ocenić stopień realizacji ZSI względem przyjętych założeń definiowanych na etapie zadania projektowego i koncepcji rozwiązania. Zarówno praktyka wdrożeń zagranicznych, jak i krajowych, wskazują na poważne rozbieżności w tym zakresie. Szczególnie trudne w warunkach polskich jest utrzymanie całości prac realizacyjnych w zakładanym harmonogramie i budżecie przy zachowaniu poziomu jakości prowadzonych prac. Obiektywnie trzeba stwierdzić, że w ostatnich kilku latach dostrzega się wyraźny postęp w tym zakresie.

Literatura:

Adamczewski P.: Zintegrowane systemy informatyczne. MIKOM, Warszawa 1998

Barczak A.: Problemy informatyzacji w siłach zbrojnych RP. Materiały konferencji

z okazji XXX lecia Wydziału Cybernetyki WAT nt. " Zagadnienia projektowania systemów informatycznych dla potrzeb SZ RP ", Warszawa 1999, str. 1 1-29

Flasiński M.: Wstęp do analitycznych metod projektowania systemów informatycznych. WNT, Warszawa 1997

Miłosz M.: Szacowanie zasobów w projektach informatycznych. Informatyka 11/97

Ochman J.: Integracja w systemach informatycznych zarządzania. Podstawy teorii i metodologii. PWE, Warszawa 1992

Sage A. P.: Systems management for Information Technology and Software Engineering. John Wiley & Sons, New York 1995

6

6. Ewolucja informatyki i jej wojskowych zastosowań

płk prof. dr hab. inż. Piotr Sienkiewicz

Wprowadzenie

Charakter tekstów pomieszczonych w „Biuletynie Jubileuszowym" skłania do refleksji nad ewolucją informatyki jako dyscypliny naukowej oraz jej zastosowań w Siłach Zbrojnych RP. Jednym z ważnych obszarów jej zastosowania jest proces automatyzacji systemów dowodzenia i kierowania środkami walki. W książce, cokolwiek archaicznej, bo powstałej w zupełnie innej epoce, zarówno ze względu na odmienną sytuację polityczną, jak i warunki technologiczne, lecz zamykającej jakby pewien etap informatyzacji w wojsku, napisano:

> „Istota automatyzacji polega na tym, że w systemach dowodzenia człowiek powinien czynić to, do czego jest najbardziej predysponowany, a więc twórczo myśleć, opracowując oryginalne koncepcje działania. Komputer natomiast powinien robić to, co robi lepiej od człowieka, a więc szybciej i dokładniej wykonywać operacje na złożonych zbiorach różnorodnych danych. Tak jak za czasów Miltiadesa, zwycięzcy spod Maratonu, Aleksandra Macedońskiego, Hannibala, Napoleona i wielu ich następców – do człowieka należy wybór czasu, miejsca i sposobu rozegrania bitwy. Człowiek bowiem ze swą wiedzą, doświadczeniem, intuicją, zdolnością myślenia produktywnego jest niezastąpiony. Jednak, aby te jego wyjątkowe cechy mogły być wykorzystane na polu walki, musi być wspomagany przez komputery. Należy sądzić, że w tym właśnie kryje się właściwy sens automatyzacji jako formy instrumentalizacji procesów informacyjno-decyzyjnych i jednocześnie jako formy intelektualizacji pola walki. Niekiedy mówi się, że współczesne kierowanie założonymi

procesami musi być realizowane z wiedzą systemową, także matematyczną, w głowie i z komputerem pod ręką". *(Sienkiewicz P. et al.)*

Należy sądzić, że dopiero rozwój teleinformatyki, Internetu i intranetów, systemy wspomagania decyzji (DSS), nowe efektywne metody projektowania systemów informatycznych i zarządzania złożonymi projektami, a więc osiągnięcia ostatniej dekady XX wieku, pozwolą skutecznie urzeczywistnić dość oczywiste postulaty wyżej sformułowane.

Informatyka jako dyscyplina

Zespół powołany przez **The Association for Computing Machinery** podaje następującą definicję informatyki:

„Informatyka to systematyczne badanie systemów algorytmicznych, które opisują i przetwarzają informacje: ich teoria, projektowanie, efektywność, implementacja i zastosowanie. Fundamentalne pytanie brzmi: co można (efektywnie) zautomatyzować?"

Powyższe ujęcie istoty informatyki jest, oczywiście, jedynym z możliwych i zapewne nie wyczerpuje pełnego kanonu informatyki. Warto zauważyć, że angielski termin *computer science*, utożsamiany często z informatyką, budzi także wątpliwości, bowiem porównano niegdyś nazwanie informatyki *nauką o komputerach* z określeniem chirurgii jako *nauki o nożu*. Autorzy przytoczonej wyżej definicji proponują następujące główne obszary zastosowań (?) informatyki:

Algorytmy i struktury danych (jakie algorytmy są najlepsze dla poszczególnych klas problemów);
Języki programowania (jakie są możliwe organizacje maszyny reprezentowanej przez język, jak są one implementowane i jaką składnię zastosować, by efektywnie określić, co komputer ma robić);
Architektura komputerów (jakimi metodami połączyć sprzęt i oprogramowanie w efektywny i niezawodny system);
Obliczenia numeryczne i symboliczne (jak efektywnie i dokładnie rozwiązywać określone zadania);
Systemy operacyjne (jak efektywnie sterować przydziałem zasobów do wykonywania programów);
Inżynieria oprogramowania (jak projektować bezpieczne i niezawodne oprogramowanie spełniające specyfikację);
Bazy danych i systemy wyszukiwania informacji (jak organizować duże zbiory danych, by były efektywnie dostępne i uaktualniane);

Sztuczna inteligencja (jaka powinna być symboliczna reprezentacja wiedzy i wnioskowanie z jej wykorzystaniem przez komputer);
Komunikacja człowiek - komputer (jak efektywnie wymieniać informację w dowolnej postaci pomiędzy człowiekiem i komputerem).

Zapewne powyższy wykaz obszarów (dziedzin) trudno uznać za zupełny i rozłączny, lecz zgodzić się należy z tym, że stanowią one fundamentalny kanon informatyki tworzący jej istotę jako dyscypliny.

Z kolei Zdzisław Bubnicki wyróżnia następujące dziedziny rozpatrując funkcje komputera jako środka „automatyzacji pracy umysłowej":

Inżynieria obliczeń (komputer jako środek do obliczeń);
Inżynieria rozwiązywania problemów (komputer jako środek do rozwiązywania problemów);
Inżynieria informacji (komputer jako środek do gromadzenia i przetwarzania danych);
Inżynieria wiedzy (komputer jako ekspert, tj. środek do rozwiązywania problemów z reprezentacją wiedzy i rozumowaniem).

Jeżeli przeniesiemy propozycje Z. Bubnickiego dotyczące komputeryzacji zarządzania na sferę dowodzenia, to możemy powiedzieć, że podstawowa funkcja dowodzenia polega na podjęciu decyzji na podstawie odpowiednich informacji. Dowodzenie na pewno zaś wprowadza pewną specyfikę do ogólnej problematyki algorytmizacji i komputeryzacji podejmowania decyzji. A zatem ogólny problem podstawowy można sformułować następująco:

Wyznaczenie algorytmów podejmowania decyzji z uwzględnieniem ich komputerowej realizacji oraz z uwzględnieniem specyfiki problemu i obiektu dowodzenia.

Ewolucja informatyzacji dowodzenia

Wszelkie próby periodyzacji rozwoju złożonych procesów o licznych uwarunkowaniach: organizacyjnych, metodologicznych, technicznych, technologicznych itp. trzeba uznać za umowne i ryzykowne. Stosunkowo łatwy jest podział na dekady, co w przypadku rozwoju zastosowań informatyki w polskich siłach zbrojnych może znaleźć uzasadnienie zmianami technicznymi, jakie w tych okresach zachodziły.

- Modele walki W.L. Lanchestera;
- Wojskowe zastosowania metod optymalizacji (programowanie liniowe, nieliniowe, dynamiczne);
- Modele grafów i sieci, modele kolejek...;
- Pierwsze oryginalne prace nt. Modelowania sytuacji konfliktowych (J. Skibiński, S. Piasecki);
- Utworzenie Wydziału Cybernetyki WAT (pierwszy w kraju, 1969 r.).

- Automatyzacja systemów dowodzenia i kierowania ogniem;
- Algorytmizacja procesów decyzyjnych;
- Symulacja komputerowa;
- Inżynieria systemów;
- Utworzenie Wojskowego Instytutu Informatyki.

- „Boom pc - towy";
- Symulacja komputerowa procesów walki;
- Komputerowe gry wojenne;
- Analiza systemowa.

- Program informatyzacji systemów dowodzenia i kierowania ogniem;
- Sieci komputerowe – Internet/Intranet;
- Systemy wspomagania decyzji w sytuacjach kryzysowych i konfliktowych;
- Wspomaganie kierowania obronnością państwa;
- Systemy ekspertowe, systemy grafiki;
- Rozwój modelowania i symulacji komputerowej;
- Komputerowe gry wojenne;
- Utworzenie Centrum Informatyki Sztabu Generalnego WP.

Wojny informatyczne

Gdy podsumowano wpływ technologii na rezultat wojny w Zatoce Perskiej, posłużono się skrótem „4S", co miało oznaczać: niewidzialne samoloty (*Stealth*), manewrujące rakiety wystrzeliwujące z okrętów (*Sea-Launched Cruise Missiles*), defensywę zorganizowaną zgodnie z założeniami Strategicznej Inicjatywy Obronnej (*SDI-Like*

Defense) oraz systemy rozpoznawania kosmicznego (*Space System-Spy Satelites*). Następnie dodano piąte S – *Semiconductors*, czyli po prostu półprzewodniki, podstawę technologii informatycznych, od których rozwoju zależały pozostałe cztery. Znany publicysta Alvin Toffler napisał, nie bez pewnej przesady, że wojnę w Zatoce Perskiej wygrała inteligencja ukryta w mikroprocesorach systemów uzbrojenia oraz systemach dowodzenia, łączności i rozpoznania.

Wśród głównych przyczyn klęski armii irackiej, której potencjał był oceniany jako czwarty na świecie, uznaje się przestarzałą elektronikę. Była mało wydajna, oparta na łatwo zakłócanej technice analogowej, uniemożliwiającej efektywną, kompleksową automatyzację systemów dowodzenia, łączności i kierowania środkami walki. Na przegranej Irakijczyków zaważył również zbyt mały i przestarzały potencjał systemów, które nie były w stanie dostarczyć danych niezbędnych do planowania i wykonania uderzeń na obiekty alianckie. Obrazu klęski dopełnił mało elastyczny i zhierarchizowany system dowodzenia i kierowania środkami walki. W tych obszarach wyraziła się druzgocąca wprost przewaga aliantów, co można wyrazić jako starcie systemów należących do dwóch różnych generacji technologicznych. Wojna w Zatoce, zwana „Pierwszą wojną informacyjną" i lata 90, uświadomiły znaczącą rolę technologii i systemów informacyjnych w rozwoju systemów obrony oraz stanowiły swoistą antycypację charakteru przyszłych wojen, który informatyka i telekomunikacja będą kształtować w dominującym stopniu. I dlatego u schyłku XX wieku pojawiły się nowe pojęcia „**Infowar**" i „**Cyberwar**" wyróżniające swoistą „**walkę na bity**".

Wspomniany wcześniej A.Toffler pisze, że „wojna cybernetyczna" narzuca:

> „**próbę dowiedzenia się wszystkiego o przeciwniku i równocześnie zapobieganie temu**, by wiele dowiedział się on o nas samych. Powoduje to przesunięcie „równowagi informacji i wiedzy" na naszą korzyść, pomimo że równowaga sił przesunięciu takiemu nie podlega".

Toffler postuluje sformułowanie „strategii opartej na wiedzy".

Intranet antykryzysowy

Kryzys jest zawsze stanem ewoluującym, pojmowanym jako przejściowy. Stan kryzysu następuje po stanie rozumianym jako (względnie) normalny. Kryzys albo przeradza się w katastrofę, albo zostaje wchłonięty, pociągając następstwa różnorodnej natury i wagi.

Dotychczasowe badania nad kryzysami (sytuacjami kryzysowymi) charakteryzuje: brak spójnej logicznie konceptualizacji (jasnych podstaw analizy związków przyczynowo-skutkowych), brak danych empirycznych, nie zweryfikowane empiryczne sądy o naturze

zależności między cechami tworzącymi kryteria oceny kryzysów, wpływ sentymentów i resentymentów, sądów obiegowych i tzw. zdrowo rozsądkowych na opisy kryzysów itp. Dopiero pojawienie się koncepcji typu Crisis Management, będącej w istocie pragmatycznym wariantem analizy systemowej w dziedzinie zarządzania strategicznego, sprawiło, że problem sytuacji kryzysowych i sterowania kryzysami (wyboru racjonalnych strategii przeciwdziałania kryzysom) stał się interesującym przedmiotem analizy systemowej.

Sytuacją kryzysową, nazywać będziemy zjawisko takiej kumulacji zjawisk (procesów, zdarzeń) negatywnych, które prowadzą do zagrożenia zdolności autonomicznego rozwoju systemu (realizacji jego podstawowych funkcji). Kryzysem określać będziemy stan zagrożenia utraty zdolności pożądanego rozwoju systemu. Przyczyny kryzysu systemu dzielimy na:

- Zewnętrzne, czyli skumulowane zjawiska negatywne, których źródłem jest otoczenie systemu;
- Wewnętrzne, czyli skumulowane zjawiska negatywne, których źródła znajdują się wewnątrz systemu.

Na podstawie analizy realnych sytuacji kryzysowych można przyjąć następujące hipotezy:

- Kryzys jest zjawiskiem o ograniczonej sterowności;
- Należy przyjąć za możliwe i prawdopodobne, że system za pomocą swojego potencjału jest w stanie rozwiązać sytuacje kryzysową.

Prawdopodobieństwo pomyślnego rozwiązania przez system sytuacji kryzysowej jest tym wyższe, im system:

- Jest dojrzalszy (kierownictwo dysponuje dostatecznym doświadczeniem w rozwiązywaniu sytuacji trudnych, nowych i niepewnych);
- Dysponuje silnymi związkami koopercyjnymi z otoczeniem;
- Zmiany w otoczeniu są obserwowalne i w pożądanym stopniu przewidywalne;
- Dysponuje odpowiednim „potencjałem antykryzysowym" (system wczesnego ostrzegania o zagrożeniach, komórka ds. „zarządzania w kryzysie", „sztab antykryzysowy")
- Kierownictwo posiada zdolność zarządzania strategicznego itp.

W związku z powyższym przyjęto następujące założenia metodologiczne:

- Kryzys jest zjawiskiem systemowych (intrasystemowym),
- Kryzys jest zjawiskiem obiektywnym, czyli istniejącym niezależnie od woli ludzi działających w systemie;

- Kryzys jest zjawiskiem o ograniczonej (czyli niepełnej) obserwowalności, predykcyjności (przewidywalności) i sterowalności;
- Sterowalność kryzysu (sytuacji kryzysowej) zależy od fazy obserwacji kryzysu oraz wielkości użytego do jego rozwiązania potencjału systemu;
- Kryzys zawsze stanowi punkt zwrotny w życiu systemu, co oznacza, że zmusza on system do głębokich zmian systemowych (strategicznych, strukturalnych, funkcjonalnych oraz celów i funkcji).

Infrastruktura systemu rozwiązywania sytuacji kryzysowych

Cechami charakterystycznymi podejmowania decyzji w sytuacji kryzysowej są:

- Wysoki stopień niepewności i ryzyka;
- Nowość sytuacji dla decydentów (ryzykowność);
- Duża złożoność struktury sytuacji (złożoność);
- Przewidywane wystąpienie konfliktów w rozwiązywaniu sytuacji (konfliktowość);
- Dużą pilność rozwiązywania (presja czasu);
- Kluczowe znaczenie dla organizacji (presja wagi sytuacji);
- Przewidywana trudność akceptacji rozwiązań (presja „niepopularności" decyzji);
- Zagrożenie decydenta formalnymi sankcjami za złą decyzję (presja kary).

Oznacza to, że system informatycznego wspomagania rozwiązywania sytuacji kryzysowych powinien:

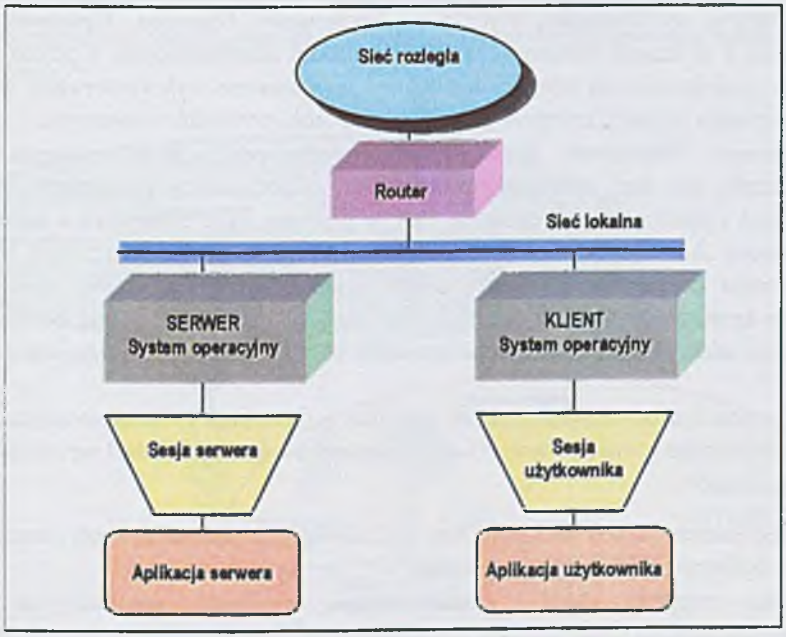
- Umożliwiać dostęp do wiarygodnych i aktualnych danych związanych z sytuacją kryzysową;
- Pozwalać na współdziałanie centrów antykryzysowych różnych szczebli i specjalności;
- Dostarczać narzędzi wspomagających analizę i ocenę sytuacji kryzysowej, pozwalające na symulacje efektów podjętych decyzji i prognozujące dalsze losy kryzysu;
- Narzędzia wspomagające muszą być bardzo proste w obsłudze, znane i sprawdzone w codziennej eksploatacji, aby koniecznością swej obsługi nie zwiększać stresogennej sytuacji kryzysowej.

Wszystkie te funkcje muszą być spełnione wraz z zapewnieniem funkcjonowania sytemu w warunkach kryzysu (odpomość systemu na skutki sytuacji kryzysowej) oraz w warunkach wysokiej odpomości na penetrację systemu (wykradanie, fałszowanie, usuwanie danych, podszywanie się pod inne osoby i źródła informacji...). Są to cechy występujące w eksploatowanych obecnie systemach zamkniętych, specjalnego przeznaczenia, bazujących na wydzielonej infrastrukturze teletechnicznej, ze ściśle zdefiniowaną liczbą abonentów i powiązań, wspomaganych urządzeniami utajniającymi,

jednak o przestarzałej strukturze technicznej (łączność telegraficzna) i niewydolnej przepustowości informacyjnej. Ponadto specyfika sytuacji kryzysowych powoduje, że trudno jest przewidzieć *a priori* wszystkich uczestników działań antykryzysowych, zakres tych działań oraz źródła pozyskiwania informacji. Skłania to do budowania systemu o strukturze otwartej i ściśle powiązanego z Internetem, jednakże z zachowaniem wysokiego poziomu bezpieczeństwa. Rozwiązaniem jest więc **INTRANET ANTYKRYZYSOWY**.

Intranet, czyli prywatna sieć komputerowa oparta o standardy, sprzęt i oprogramowanie wykorzystywane w sieci Internet, charakteryzuje się niskimi kosztami budowy i utrzymania oraz krótkim czasem wdrażania. Jest to wynikiem następujących czynników:

- Stosowana jest typowa aparatura i oprogramowanie;
- Istnieje szeroki rynek producentów i specjalistów, co obniża koszty i gwarantuje ciągłość dostaw i rozwoju technologicznego;
- Możliwe jest wykorzystanie już zainstalowanego sprzętu i oprogramowania;
- Użytkownicy intranetu posługują się tymi samymi narzędziami, które znają z CODZIENNYCH kontaktów z Internetem;
- Nie ma potrzeby budowania zdublowanej infrastruktury teleinformatycznej (system otwarty i zamknięty).



Rys. 8 Elementy podlegające ochronie w systemie teleinformatycznym rozwiązywania sytuacji antykryzysowych.

Kluczowym elementem jest tu jednak konieczność zapewnienia możliwie najwyższego poziomu bezpieczeństwa obejmującego wszystkie poziomy działania systemu (Rys. 8). Z uwagi na konieczność wykorzystywania urządzeń i oprogramowania pochodzących od producentów zagranicznych, posiadanie możliwości posługiwania się metodami szyfrowania o gwarantowanej (certyfikowanej przez upoważnione instytucje) mocy kryptograficznej jest warunkiem decydującym o użytkowym wdrożeniu takiego systemu.

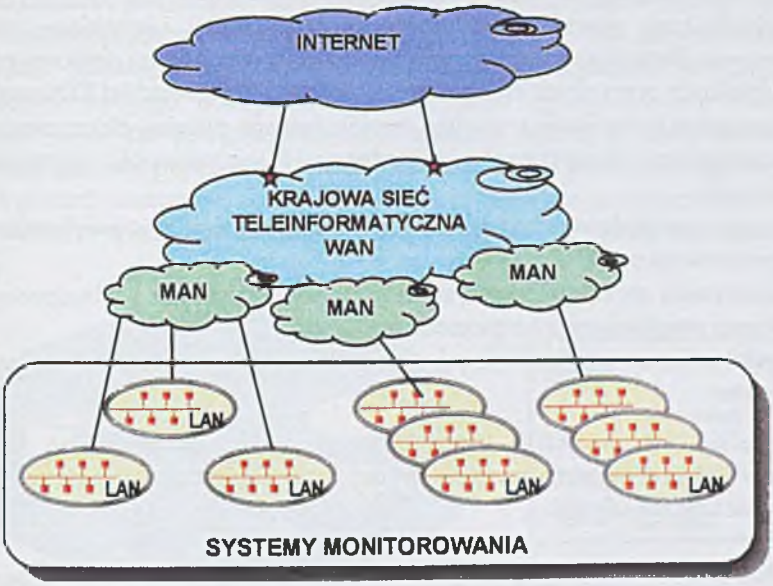
Projektowana infrastruktura musi zapewnić możliwość współdziałania instytucji odpowiedzialnych za bezpieczeństwo kraju, zarówno na szczeblu centralnym, jak i w układzie terytorialnym. Oznacza to, że należy przewidywać możliwość współdziałania następujących instytucji: Ministerstwo Obrony Narodowej, (w tym Sztab Generalny WP, dowództwa WLąd, MW, WLOP), Ministerstwo Spraw Wewnętrznych i Administracji (w tym Policja, Straż Graniczna, Straż Pożarna, UOP itd.), Ministerstwo Spraw Zagranicznych, Urząd Prezydenta, Premiera, Senat, Sejm.

Te instytucje muszą być powiązane wysokowydajną siecią teleinformatyczną pozwalającą na jednoczesne przesyłanie dużych ilości informacji multimedialnych (dane komputerowe, telefonia, telewizja). Wydaje się celowe, zbudowanie rządowej sieci łączności o zasięgu krajowym z wykorzystaniem i rozbudową istniejących sieci miejskich (MAN) w głównych ośrodkach administracyjnych. W pierwszym etapie powinna ona objąć MANy w Warszawie, Wrocławiu, Bydgoszczy, Poznaniu, Krakowie, Gdyni i Gdańsku, a w dalszej kolejności pozostałe ośrodki administracyjne i przemysłowe, w których rozlokowane są ośrodki decyzyjne i wykonawcze wykorzystywane w procesie rozwiązywania sytuacji kryzysowych. W ten sposób powstanie inwestycja o znaczeniu strategicznym **"Krajowa Sieć Teleinformatyczna"**, która powinna zastąpić przestarzałą już sieć łączności specjalnej, z jednoczesnym przejęciem jej funkcji, uprawnień i poziomu bezpieczeństwa. Sieć ta powinna mieć połączenie z siecią Internet za pomocą 2-3 łączy. Mała ilość połączeń sieci krajowej z Internetem ma służyć zwiększeniu bezpieczeństwa przez zainstalowanie aparatury specjalnej, monitorującej ruch na łączu i sygnalizującej próby naruszenia obowiązującego planu bezpieczeństwa. Umożliwi także rejestrowanie i archiwizowanie ruchu między określonymi abonentami.

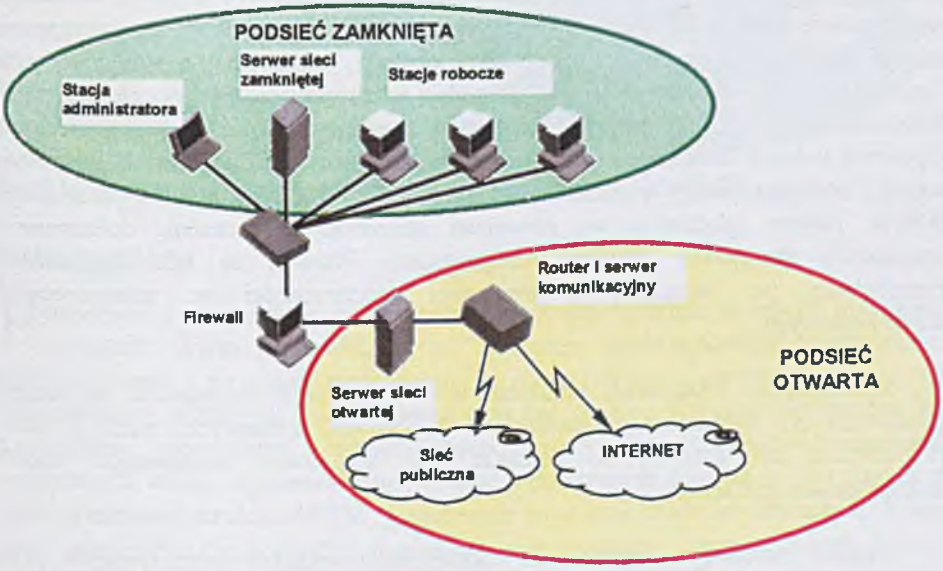
Zgodnie z omówionymi powyżej zasadami infrastruktura teleinformatyczna systemu wspomagającego rozwiązywanie sytuacji kryzysowych będzie składała się z następujących warstw (Rys. 9):

- Sieci lokalne (LAN) instytucji (Rys. 10), zawierające podsieć otwartą i zamkniętą (o podwyższonym bezpieczeństwie);
- Sieci miejskie (MAN) zrealizowane na bazie wydzielonych łącz telekomunikacyjnych, o dużej prędkości przesyłania danych i pozwalających na transmisję multimedialną (wymagane są właściwości izochroniczne, np. ATM, FR);

- Sieć krajowa (WAN) zapewniająca łączność między sieciami miejskimi i posiadająca także właściwości izochroniczne pozwalające na transmisję głosu i obrazu.



Rys. 9 Infrastruktura teleinformatyczna krajowego systemu rozwiązywania sytuacji kryzysowych



Rys. 10 Struktura sieci lokalnej (LAN) o podwyższonym bezpieczeństwie

Tak zbudowana sieć zapewniać będzie bezpieczeństwo przechowywania i przesyłania informacji dzięki:

- Stosowaniu urządzeń utajniających transmisję w łączu fizycznym;
- Przeciwdziałanie zjawiskom elektromagnetycznej emisji ujawniającej przez stosowanie ekranowania oraz zapobieganie rozgłoszeniowemu trybowi pracy sieci lokalnych przez użycie sieci przełączających (np. typu switched Ethernet);
- Wykorzystaniu weryfikacji z użyciem certyfikowanego podpisu elektronicznego gwarantującego niezaprzeczalność nadawcy i niezmienność przesyłanej informacji;
- Używaniu standardowych, pochodzących z Internetu, środków zwiększających bezpieczeństwo (np. SSL);
- Wykorzystaniu systemów operacyjnych i urządzeń sieciowych z wbudowanymi funkcjami zwiększającymi bezpieczeństwo;
- Ukryciu struktury sieci zamkniętych przez stosowanie rozwiązań typu *firewall* i *proxy server*.

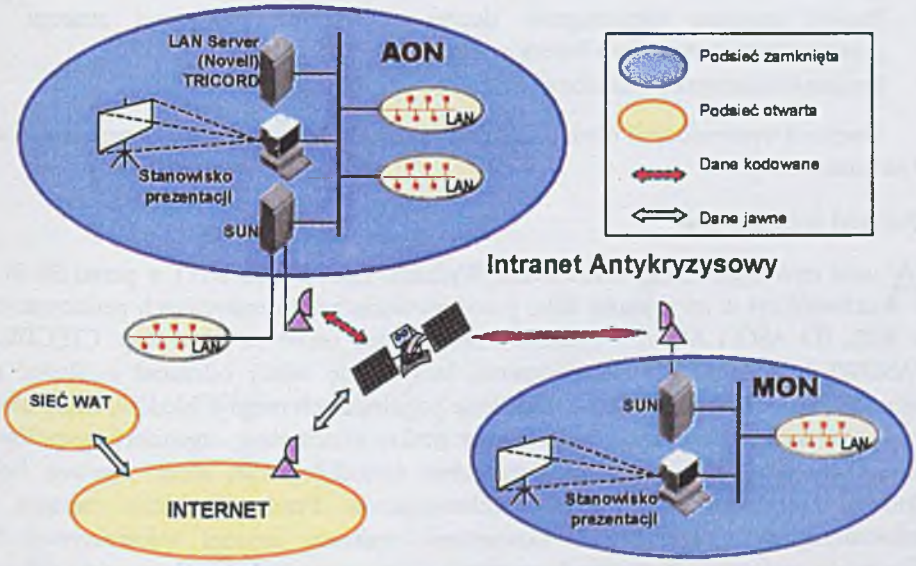
Niezbędne jest tu jednak wytworzenie procedury certyfikowania wszystkich składników systemu (sprzęt, oprogramowanie) pod względem bezpieczeństwa przez odpowiednie krajowe ośrodki.

W **Intranecie antykryzysowym** w warstwie oprogramowania wykorzystane zostaną serwery WWW i przeglądarki internetowe (tzw. "*Web Servery*" i "*Web browsery*"). Istniejące obecnie serwery WWW pozwalają na gromadzenie i udostępnianie praktycznie każdego typu informacji (tekst, hipertekst, grafika, wykresy, dźwięk, obraz video), pozwalają na dostęp, aktualizację i przeszukiwanie baz danych, a nawet na zdalne wykonywanie aplikacji dowolnego typu. Przeglądarki WWW umożliwiają prezentowanie danych zgromadzonych w serwerach. Ich obsługa jest prosta, a wbudowywanie "inteligencji" do dokumentów WWW pozwalają na zwiększenie funkcjonalności takich dokumentów przy jednoczesnym ułatwieniu posługiwania się techniką sieciową. Ogromne nakłady finansowe i intelektualne wielkich firm informatycznych gwarantują szybki i znaczący postęp w zakresie zwiększania możliwości serwerów i przeglądarek WWW. Należy spodziewać się rozwiązań ułatwiających tworzenie dokumentów opisujących rzeczywiste obiekty trójwymiarowe. Pozwoli to na "wędrowanie" przeglądarką po wirtualnej 3-wymiarowej rzeczywistości w zastosowaniach antykryzysowych.

Multimedialne właściwości standardu WWW, ogromna elastyczność w zakresie możliwych do wykorzystania standardów graficznych, tekstowych, audio i video, predestynują ten standard do pełnienia roli "wspólnego mianownika" między różnorodnymi aplikacjami.

Główny problem to umożliwienie udostępniania wyników wypracowanych przez różnorodne aplikacje ściśle określonej grupie osób uczestniczących w procesie antykryzysowym (w większości bez możliwości interakcyjnych). Koncepcja, sprawdzona

w trakcie warsztatów towarzyszących I Międzynarodowej Konferencji Naukowej nt. Modelowania i Symulacji Komputerowej Sytuacji Konfliktowych CONSIM'96 (AON Rembertów 19-21.09.1996) oparta była o gromadzenie na serwerach kopii ekranów z wynikami działania programów "antykryzysowych" w postaci plików GIF z "oprawą" w postaci zbiorów opisujących w standardzie HTML. Dostęp do tych danych zrealizowano przy użyciu polskojęzycznych przeglądarek (Internet Explorer). W przypadkach wymagających zdalnego dostępu do aplikacji użyto oprogramowanie NetMeeting pozwalające także na przejęcie sterowania aplikacją zdalną, a także umożliwiające komunikację głosową poprzez sieć komputerową, nawet na powolnych łączach (14.400 b/s). Dla potrzeb warsztatów zbudowana została rozległa sieć komputerowa - "Intranet antykryzysowy" - między AON, MON i WAT przy wykorzystaniu łącz satelitarnych. (Rys. 11).



Rys. 11 "Intranet Antykryzysowy" warsztatów konferencji CONSIM'96

Zakończenie

Przeprowadzona symulacja działań antykryzysowych wykazała słuszność przyjętych rozwiązań. Warto podkreślić, że w "Intranecie antykryzysowym" zastosowano oprogramowanie i procedury pochodzące "ze starego systemu", w żadnej mierze nie wykorzystujące możliwości pracy grupowej jakie daje intranet. Wzbogacenie systemu np. o możliwość gromadzenia i przeszukiwania dokumentów, meldunków, opracowań analitycznych, norm, regulaminów itp., a także wykorzystanie dostępu do baz danych z wykorzystaniem formularzy WWW, generowania na żądanie raportów i zestawień, dodaje nowe właściwości funkcjonalne, ułatwiające proces analizy i podejmowania decyzji antykryzysowych. Proces rozwoju "Intranetu Antykryzysowego" będzie przebiegał w

kierunku wykorzystania nowych możliwości pracy grupowej jakie dają współczesne narzędzia internetowe.

Prace, podjęte w połowie lat 90, nad systemami informatycznego wspomagania decyzji w sytuacjach kryzysowych i konfliktowych, wymagały zbiorowego wysiłku zespołów badawczych i projektowo-wdrożeniowych. W ich skład wchodzili przedstawiciele MON i uczelni wojskowych (AON, WAT), BBN oraz MSWiA. Stanowiły dobry przykład współpracy cywilno-wojskowej w procesie rozwiązywania problemów interdyscyplinarnych ukierunkowanych na osiągnięcie pragmatycznych celów. Do nich należy zaliczyć następujące:

- Projekt systemu wczesnego ostrzegania o zagrożeniach dla bezpieczeństwa państwa;
- Projekt systemu wspomagania decyzji - wyboru efektywnej strategii przeciwdziałania sytuacjom kryzysowym;
- Projekt infrastruktury teleinformatycznej.

Ostatni z wymienionych obejmował tzw. „Intranet Antykryzysowy" - przedstawiony w niniejszym artykule.

Uwagi końcowe

Autor niniejszych uwag – absolwent Wydziału Cybernetyki WAT z przed 30 lat – uczestniczył w co najmniej kilku przedsięwzięciach informatycznych realizowanych w WIŁ, ID ASG i AON. Większość z nich trudno uznać za udane (np. CIĘCIWA, PASUW), lecz przyniosły doświadczenia, których nie należy odrzucać i „skazać na zapomnienie". Chodzi nie tylko o uniknięcie popełnionych niegdyś błędów. Choć miały miejsce w innych warunkach, to problemy analizy systemowej, organizacji zespołów i zarządzania projektami zawierają zagadnienia metodologiczne, które zapewne będą aktualne bez względu na zmiany technologiczne. Przełom wieków oznacza w informatyce także konieczność powierzenia realizacji strategii informatyzacji Sił Zbrojnych profesjonalistom oraz zapewnienia efektywnego współdziałania wielu różnych zespołów i ośrodków zarówno wojskowych, jak i cywilnych. I tu należy dostrzegać różnice między okresem „teleinformatyzacji" w ostatniej dekadzie XX wieku, a okresami wcześniejszymi, charakteryzującymi się występowaniem dotkliwych luk organizacyjnych i technologicznych, skazujących niejako wiele podejmowanych przedsięwzięć na niepowodzenie.

Literatura

Bubnicki Z., Podstawy informatycznych systemów zarządzania. Wrocław 1993.

Campen A.(ed), The First Information War. AFCEA 1992.

Campen A., Dearth D., Goodden R. (ed), Cyberwar: Security, Strategy and Conflict in the Information Age. AFCEA 1996.

Denning P. J. (et al.), Computing as a Discipline. Communications of ACM, 32 (1989).

Goban – Klas T., Sienkiewicz P., Społeczeństwo informacyjne-szanse, zagrożenia, wyzwania. Kraków 1999.

Sienkiewicz P., Analiza systemowa. Bellona, Warszawa 1995.

Sienkiewicz P., Wojna informatyczna. Computerworld, 31 (1997).

Sienkiewicz P., Wiśniewski J., Intranet antykryzysowy. „Firma i Rynek" nr 7, Szczecin 1997.

Sienkiewicz P., Szczepaniak M., Więckowski W., Dowodzenie z komputerem. MON, Warszawa 1984.

Toffler A. i H., Wojna i anty wojna., Muza S.A., Warszawa 1997.

Węglarz J., Informatyka jako dyscyplina a wizja społeczeństwa informacyjnego. Pro Dialog 7 (1998).

7

7. Infrastruktura teleinformatyczna w układzie stacjonarnym i mobilnym

płk mgr inż. Kazimierz Kaczmarczyk

Wprowadzenie

Siły Zbrojne bazują na informacjach pozyskiwanych z wielu rozproszonych źródeł z możliwością sprawnego i bezpiecznego ich przekazywania.

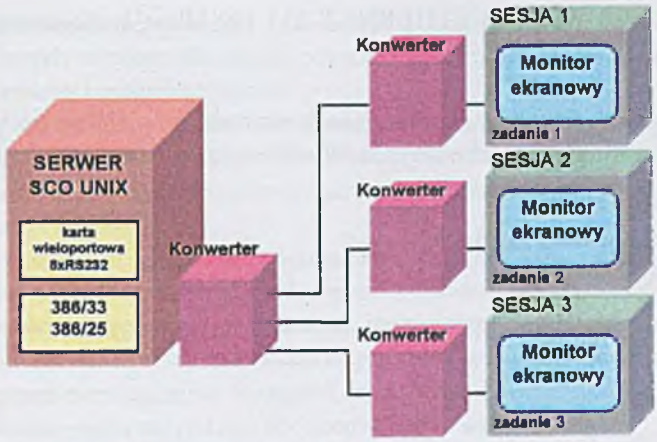
Potrzeby informatyczne współczesnych Sił Zbrojnych wymagają odpowiednio szybkich infostrad opartych o nowoczesny stacjonarny i mobilny system telekomunikacyjny. Nałożenie na ten system warstwy lokalnych sieci komputerowych, metropolitalnych (MAN) i rozległych (WAN), stworzy nowoczesny system teleinformatyczny.

Pozwoli to na efektywne pozyskiwanie, gromadzenie, opracowywanie, przetwarzanie, zobrazowanie i dystrybucję informacji, co jest istotnym elementem efektywnego procesu dowodzenia.

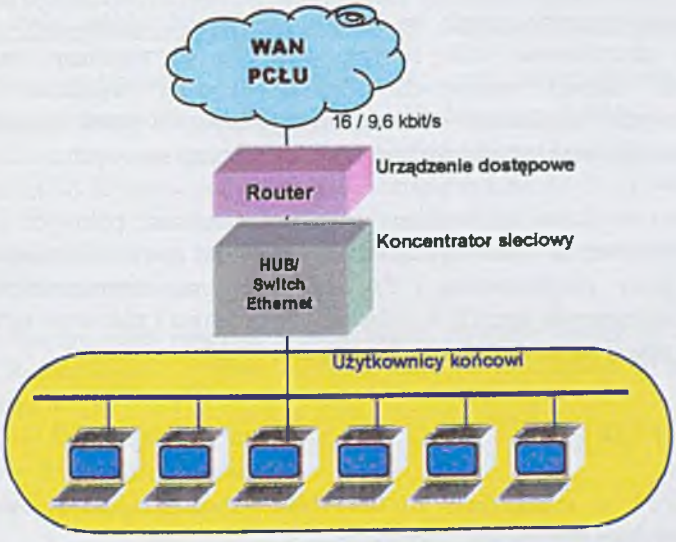
Ocena stanu aktualnego

Ocena jakościowa funkcjonującej w resorcie Obrony Narodowej infrastruktury technicznej może być dokonywana w różnych aspektach. Najbardziej istotne wydaje się przedstawienie jej charakterystyki pod kątem zastosowanych technologii, jak i zastosowań poszczególnych struktur, głównie ze względu na bezpieczeństwo przetwarzanych informacji.

Jedną z pierwszych technologii „sieciowych" wdrażanych do eksploatacji w resorcie ON były systemy umożliwiające wielostanowiskowy tryb pracy. Centralnym punktem każdej z nich był serwer - komputer klasy PC pracujący pod kontrolą SCO UNIX. Użytkownicy uzyskują dostęp do zgromadzonych na serwerze danych poprzez wykorzystywanie terminali znakowych. Połączenia pomiędzy terminalami użytkowników a centralnym komputerem były budowane w oparciu o linie telefoniczne i konwertery prądowe (Rys. 12). Omówione systemy funkcjonują jeszcze w ponad stu lokalizacjach.



Rys. 12 Model struktury sieci terminali



Rys. 13 Struktura aktualna WAN

Z początkiem lat 90-tych dominujące znaczenie w budowie infrastruktury wymiany danych uzyskały lokalne sieci komputerowych na bazie okablowania strukturalnego. Sieci LAN wykorzystywane są na każdym szczeblu. Największy stopień nasycenia występuje na szczeblu centralnym, przy czym w organach wykonawczych na poziomie oddziału, jednostki wojskowej instalacje sieciowe są również często użytkowane.

Dotychczas wykonano okablowanie strukturalne oparte w przeważającej mierze na skrętce ekranowanej (STP, FTP) kategorii 5 oraz światłowodach wielomodowych. Duża dynamika wprowadzania nowych technologii skutkuje znacznym zróżnicowaniem.

Generalnie przeważa standard ETHERNET 10 i 100 Mbps, wzbogacony urządzeniami przełączającymi (SwitchEthernet).

Na szczeblach niższych oraz w organach terytorialnych lokalne sieci komputerowe zrealizowane są w różnych technologiach. W zależności od okresu instalacji dominuje:

- Kabel koncentryczny;
- Skrętka ekranowana kat. 3 ÷ 5;
- Światłowód.

W zakresie zainstalowanego sprzętu aktywnego i pasywnego charakteryzują się dużą różnorodnością, zarówno w zakresie bezpieczeństwa struktury sieci, standardów mediów jak i platform sprzętowych.

Odrębną kategorię stanowią lokalne sieci komputerowe, na których realizowane są systemy informatyczne wspomagające dowodzenie i kierowanie wojskami.

W okresie ostatnich trzech lat zaczęły powstawać lokalne sieci komputerowe posiadające zdecydowanie inne przeznaczenie. Są to struktury dedykowane do przetwarzania danych niejawnych. Oparte są one wyłącznie na mediach światłowodowych i elementach ochrony zabezpieczających przed ulotem informacji – kabinach ekranujących i bezpiecznych stanowiskach komputerowych.

Utajniona wojskowa sieć wymiany danych w warunkach polowych i stacjonarnych bazuje na Podsystemie Cyfrowej Łączności Utajnionej z wykorzystaniem kanałów 16 kbit/s dla pracy synchronicznej i 9,6 kbit/s dla pracy asynchronicznej. Struktury techniczne budowanych sieci (5) w układzie stacjonarnym i polowym są podobne a ich architektura opiera się na następujących podstawowych elementach:

- Router
- SITCH, HUB
- Modem
- oraz LAN w standardach 10/100 BaseT zbudowanych w obiekcie lub rozwijanych na stanowiskach dowodzenia SD.

Sieć podkładowa

Głównym przeznaczeniem sieci podkładowej jest stworzenie możliwości realizacji zintegrowanej sieci teleinformatycznej obejmującej swoim zasięgiem cały kraj. Budowane obecnie, jawne i utajnione struktury telekomunikacyjne, wymagają integracji w struktury metropolitalne a te z kolei w ogólnokrajową sieć rozległą WAN.

W związku z powyższym sieć podkładowa powinna zapewnić:

- Wysoką niezawodność wymiany informacji tj. zapewnienie ciągłości ruchu wymiany danych w przypadku awarii poszczególnych elementów sieci (węzłów, głównych traków komunikacyjnych);
- Wzajemną komunikację między użytkownikami w ramach danej instytucji lub jednostki organizacyjnej, na wszystkich szczeblach dowodzenia;
- Komunikowanie się użytkowników między sobą (w ramach określonych przez usługobiorców reguł);
- Dostęp, poprzez infrastrukturę telekomunikacyjną do usług rozproszonych terytorialnie serwerów, niezależnie od miejsca lokalizacji abonenta (sieć powinna być podatna na modyfikacje i zmiany organizacyjne w resorcie obrony narodowej);
- Ochronę przed niepożądanym dostępem do zasobów informacyjnych;
- Priorytetowanie ruchu wg rodzaju abonentów i typu wiadomości;
- Użytkownikom wykorzystania w sytuacjach kryzysowych infrastruktury telekomunikacyjnej innych operatorów;
- Stworzenie technicznej możliwości komunikacji z grupami specjalnymi;
- Możliwość dowiązywania mobilnych struktur nie sieciowych do stacjonarnych.

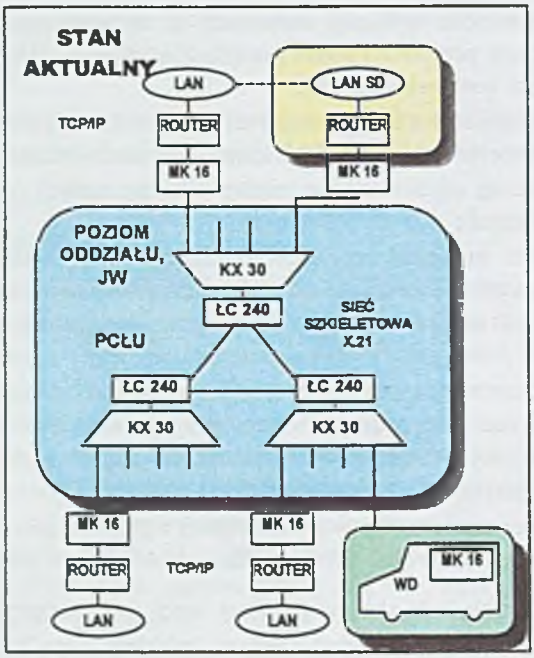
Zasadniczym problemem budowy takiej sieci jest zabezpieczenie mediów o odpowiednich przepustowości między węzłami szkieletu sieci ≥ 2 Mb/s i sieci LAN ≥ 128 kb/s w dostępie do węzła szkieletu sieci. Dotychczasowa baza telekomunikacyjna systemu łączności SZ RP nie w pełni stwarzała warunki techniczne do jej budowy.

Rozwój sieci podkładowej związany jest z obecnym procesem przebudowy systemu łączności SZ RP w zakresie:

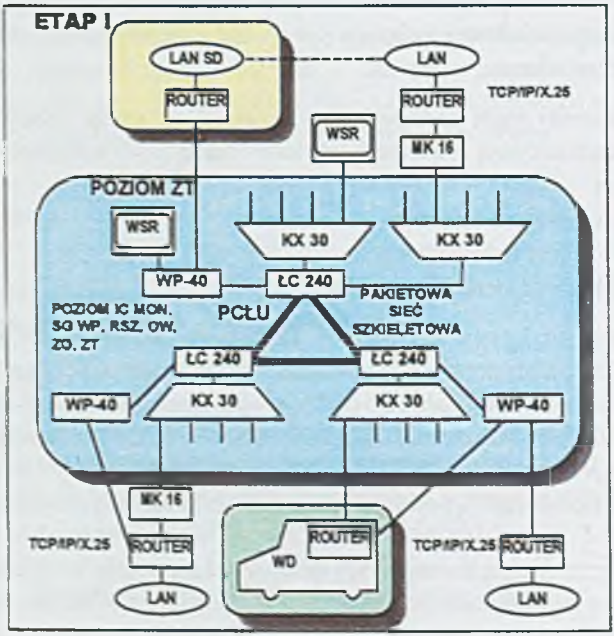
- Wymiany sprzętu starej generacji (analogowego) na sprzęt oparty na cyfrowej technice komutacyjnej (cyfrowe centrale tranzytowo-końcowe i terminale abonenckie);
- Ucyfrowienia kabli miedzianych;
- Rozbudowy linii światłowodowych;
- Budowy cyfrowych kierunków radioliniowych.

Modernizacja Podsystemu Cyfrowej Łączności utajnionej (PCŁU) w systemie stacjonarnym i polowym poprzez doposażenie ich w węzły pakietowe (WP-40) stworzy warunki techniczno – funkcjonalne do budowy utajnionej stacjonarnej oraz mobilnej sieci WAN. Węzeł pakietowy umożliwia dołączenie struktur LAN obiektowych stacjonarnych i mobilnych poprzez styk V-35, V-24, i Ethernet do utajnionego systemu łączności i stanowi główny element dostępowy do szkieletu sieci WAN (Rys. 14, Rys. 15).

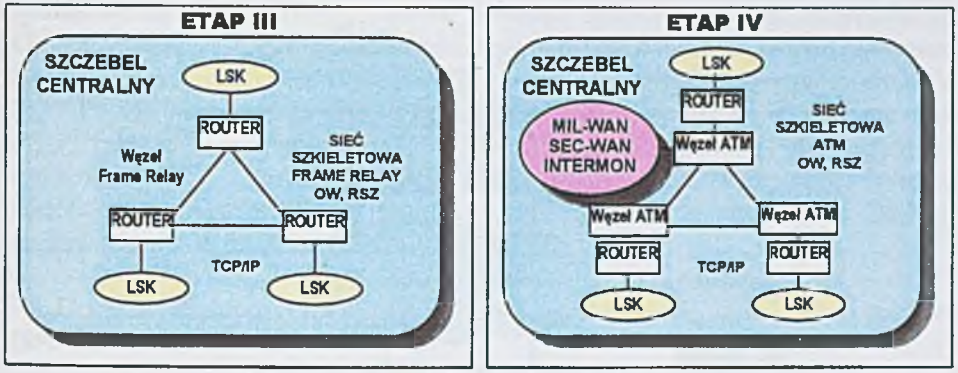
Natomiast rozwój sieci jawnej WAN dokonywał się będzie w oparciu o nowoczesne cyfrowe centrale wyposażone w styki ISDN (2B+D), G-703 ze skalowalnością w kierunku interfejsów ATM (Rys. 16).



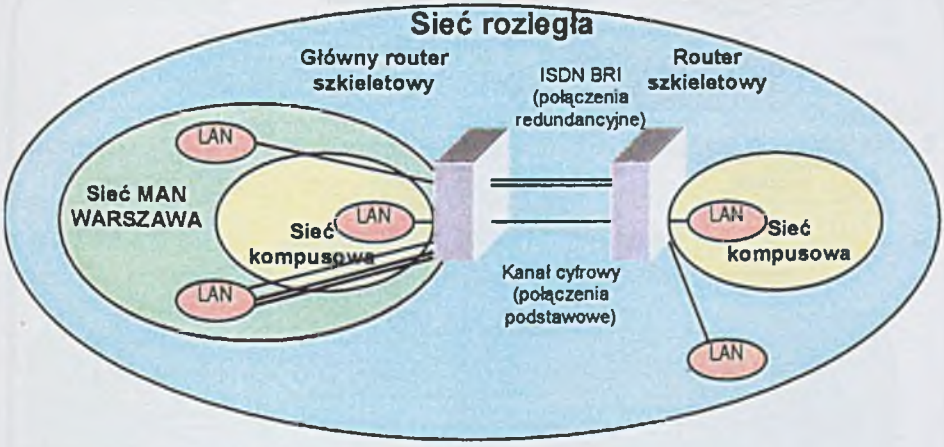
Rys. 14 Etapy rozwoju sieci podkładowej



Rys. 15 Etap I rozwoju sieci podkładowej

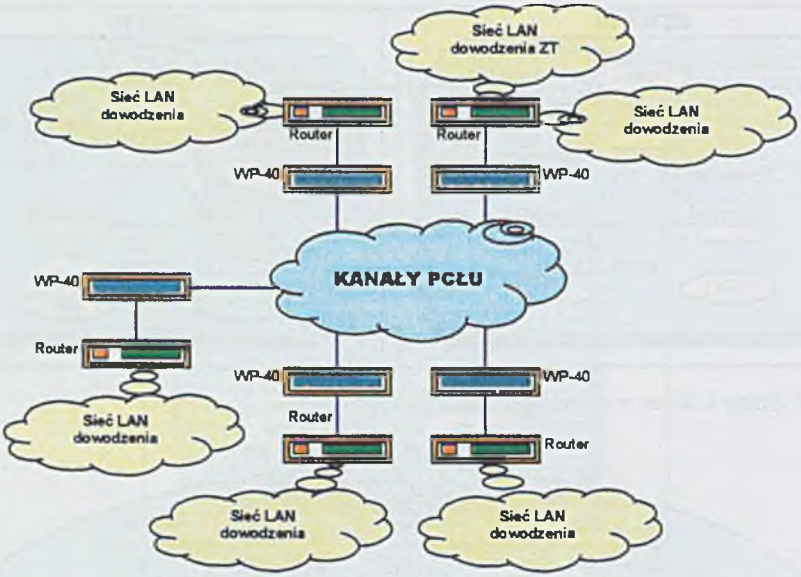


Rys. 16 Etapy kolejne rozwoju sieci podkładowej

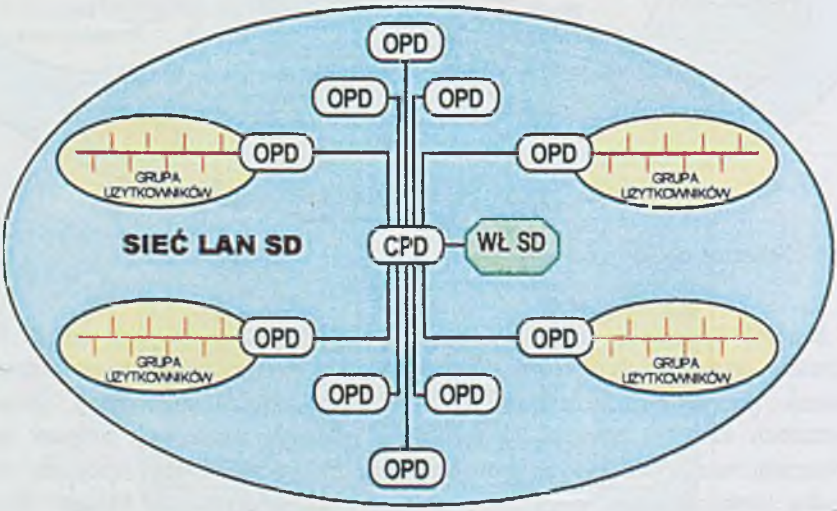


Rys. 17 Schemat ogólny sieci rozległej

Rozwój bazowych struktur sieciowych LAN (kampusowych), MAN i WAN sprowadza się do dwóch rodzajów działań (Rys. 17). Pierwszy z nich to zwiększenie ilości instalacji pasywnych (obiektowej infrastruktury telekomunikacyjnej) głównie w instytucjach szczebla związku taktycznego i jednostki wojskowej. Stopień nasycenia strukturami sieciowymi na tych poziomach jest zdecydowanie zbyt mały, aby zapewnić globalne funkcjonowanie wdrażanych systemów informatycznych. Drugim kierunkiem będzie modernizacja dotychczas funkcjonujących struktur. Sieci lokalne ewoluować będą w stronę technologii przełączalnych, poprzez switche warstwy trzeciej dają jakościowo nowe możliwości tworzenia V-Lanów co wpłynie na zdecydowany przyrost możliwości funkcjonalnych. W kolejnych etapach należy spodziewać się migracji lokalnych węzłów oraz sieci węzłów metropolitalnych i WAN w kierunku technologii ATM.



Rys. 18 Schemat o poglądowy modelu sieci rozległej przetwarzania danych niejawnych

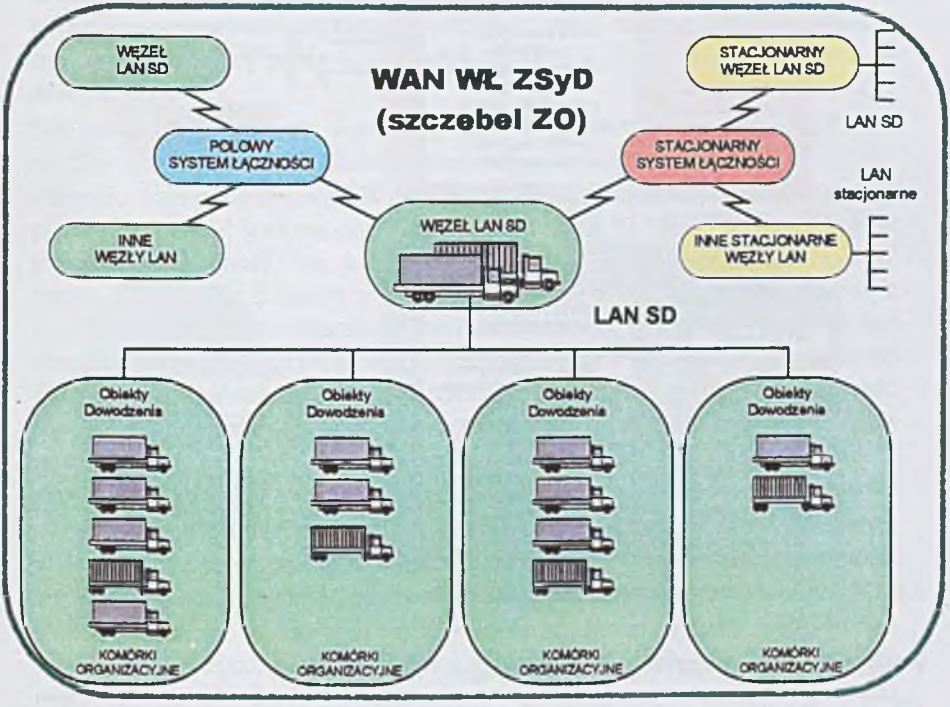


Rys. 19 Ogólny schemat struktury sieci LAN SD

Mobilna infrastruktura teleinformatyczna (Rys. 19) jest realizowana na bazie wyspecjalizowanego sprzętu łączności i informatyki SZ RP z elementami pasywnymi i aktywnymi niezbędnymi do budowy sieci WAN i LAN w warunkach polowych. Infrastruktura dla sieci WAN jest budowana w oparciu o modernizowany Podsystem Cyfrowej Łączności Utajnionej wyposażony w węzeł pakietowy WP-40. System ten

spełnia wymagania na STANAG'u 4206 dotyczące cyfrowego systemu transmisyjnego. Ostatnie ćwiczenia CE'99 potwierdziły jego kompatybilność z innymi systemami łączności, takich państw jak: USA, Francja, Niemcy i Czechy. Interfejsy użytkownika V-35, V-24, G-703 pozwalają na dołączenie sieci LAN lub pojedynczych abonentów do PCŁU. LAN na stanowisku dowodzenia SD (11) budowany powinien być w oparciu o obiektowe (OPD) i centralne (CPD) punkty dystrybucyjne wyposażone w sprzęt sieciowy. Rozmiary tych sieci zależne będą od szczebla dowodzenia. Medium transmisyjnym sieci powinien być światłowód (FO).

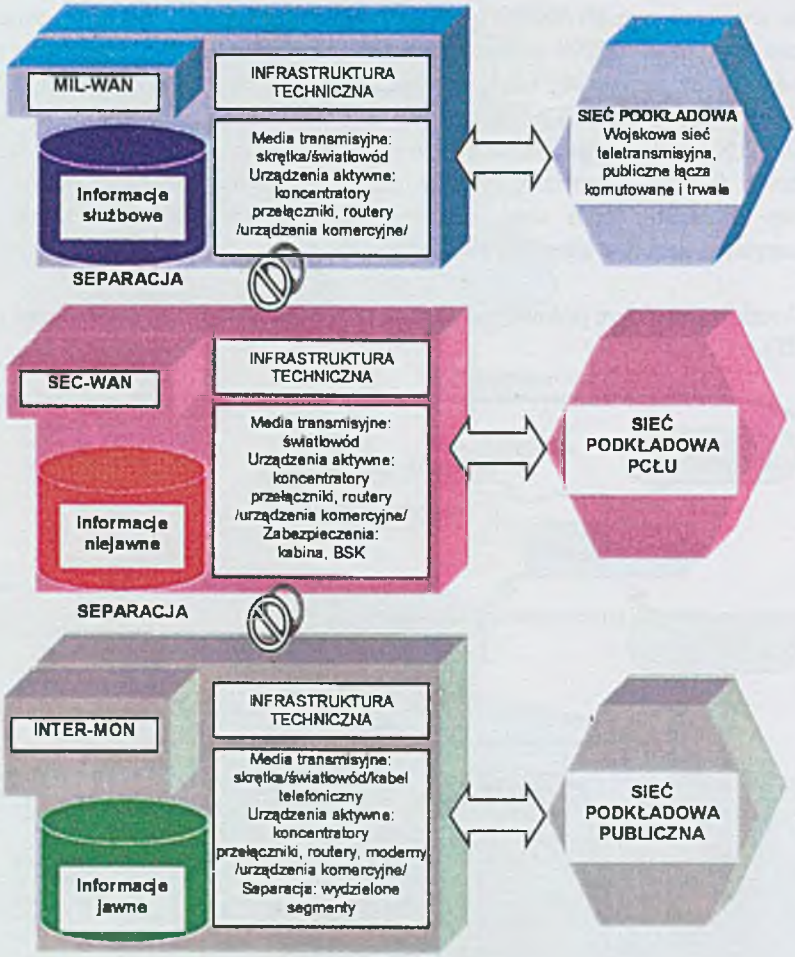
Docelową strukturę polowej sieci LAN będą stanowiły wozy dowodzenia i sztabowe (Rys. 20).



Rys. 20 Polowa struktura sieci LAN

Obecnie infrastruktura techniczna (Rys. 21) ewoluuje w kierunku budowy w Siłach Zbrojnych RP trzech odrębnych struktur sieciowych.

- Sieci jawnej – MIL-WAN - rozległej sieci wymiany danych przeznaczonej do przetwarzania informacji służbowych;
- Sieci specjalnej – SEC-WAN - sieci dedykowanej do przetwarzania danych o wyższych klauzulach poufności;
- Sieci internetowej – INTER-MON - sieci umożliwiającej dostęp do Internetu.



Rys. 21 Model funkcjonalno – techniczny struktur sieciowych

Podstawowe kategorie usług.

Sieć podkładowa powinna zabezpieczyć obecne potrzeby użytkowników resortu ON, jak również być w stanie sprostać nowym wymaganiom, jakie powstaną w trakcie jej budowy, wdrażania i eksploatacji nowych systemów informatycznych oraz rosnących potrzeb użytkowników.

Budowana sieć podkładowa powinien zapewnić poniższe kategorie usług (w przyszłości ich integrację):

- Poczta elektroniczna i system wymiany wiadomości;
- Transmisja danych (komputerowych, głosu, obrazów wideo);
- Praca grupowa i wielodostęp do zasobów;

- Wideo konferencja z wybranymi abonentami systemu: dynamiczne zarządzanie wideokonferencjami, połączenia w trybie rozgłoszeniowym 'multicasting';
- Monitoring poligonów (w przyszłości pola walki), newralgicznych obiektów;
- Integracja systemów sygnalizacji zagrożeń (teleakcja): telealarm, telealert, telemetria;
- Scentralizowane zarządzanie siecią podkładową i funkcjonowaniem sytemu.

Kryteria jakościowe infrastruktury.

Budowana infrastruktura teleinformatyczna powinna spełniać następujące kryteria:

- Zarówno w jawnej i utajnionej sieci WAN w układzie stacjonarnym i polowym, podstawowym stykiem współpracy węzłów z siecią teletransmisyjną powinien być znormalizowany przez CCITT styk G.703 i V 35 w transmisji danych w dostępie do węzła.
- Sieć podkładowa powinna zapewnić przepływność w szkielecie sieci ≥ 2Mb/s z możliwością skalowania w kierunku transmisji szerokopasmowej.
- Aktywne komponenty sieci WAN, MAN i LAN (rouetry, huby, switche) powinny zapewnić budowę sieci LAN w standardzie 10 BaseT, 10 BaseFL, Fast Ethernet 100 BaseT na kablu miedzianym i światłowodowym oraz w przyszłości Gigabit Ethernet z dostępem do węzłów MAN i WAN przez styk G.703 i V35 w infrastrukturze stacjonarnej i polowej. Ponadto powinny m. in.: charakteryzować się prostotą instalacji, eksploatacji i zarządzania, umożliwiać łatwą i tanią rozbudowę, posiadać modularną konstrukcję dającą możliwość modyfikacji sprzętowych, pozwalać na tworzenie segmentów o zmiennej ilości portów, mieć możliwość diagnozowania w warstwie fizycznej i zgodnej z protokołem SNMP, posiadać wysoką niezawodność (średni czas między uszkodzeniami ≥ 10000 godzin), posiadać wsparcie techniczne przedsiębiorstwa w Polsce, być serwisowane w sposób zapewniający przywrócenie sprawności technicznej sieci w ciągu 24 godzin od chwili zgłoszenia uszkodzenia.
- Budowę struktur sieciowych należy opierać się o system okablowania strukturalnego, zgodne ze standardami instalacyjnymi: ISO/IEC 11801 (norma amerykańska), EN 50173 (norma europejska) oraz projektowaną polską normą PrPn-EN50173.
- W zakresie bezpieczeństwa danych: zapewnienie poufności przechowywanych danych i przesyłanych informacji, weryfikacja tożsamości uprawnionego użytkownika, uniemożliwienie nieuprawnionym użytkownikom zmian konfiguracji urządzeń sieciowych. Ponadto w sieciach niejawnych: w budowie sieci wymiany danych kierować się zaleceniami zawartymi w tymczasowych wytycznych Szefa Zarządu Łączności i Informatyki nr Pf16/Łączn. z dnia 9.12.1998 r. (okablowanie strukturalne oraz ustawa z dnia 22. 01 1999r. Dz. U. nr 11 poz. 95 w zakresie ochrony informacji niejawnych), komponenty węzła sieci nie spełniające wymagań TEMPEST należy instalować w kabinach ekranowych lub szafach dystrybucyjnych antyemisyjnych. Gdy pomieszczenie

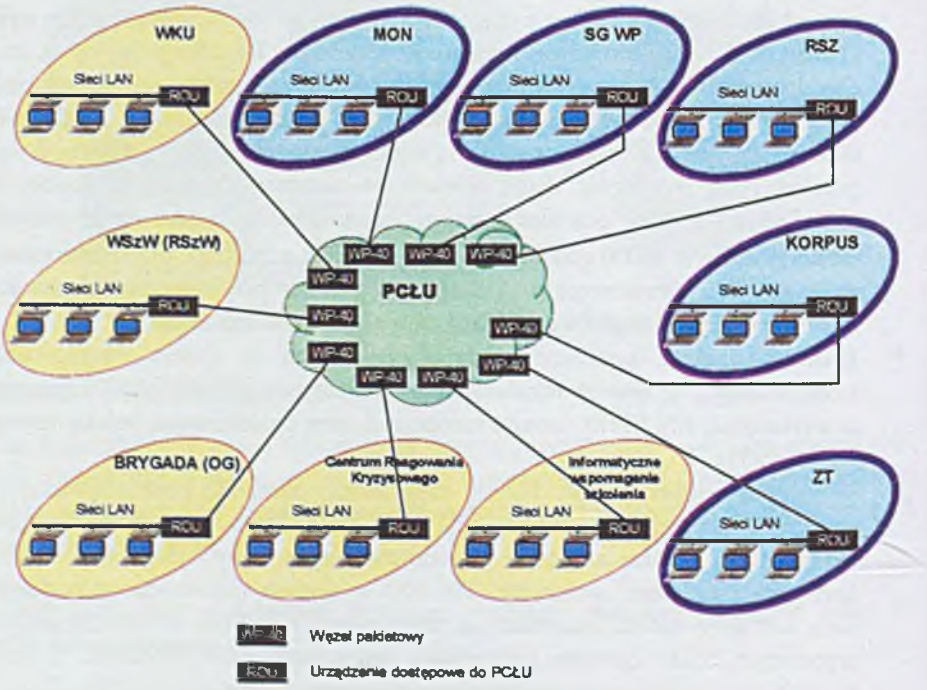
spełnia wymagania strefy 2, 3 dopuszcza się wyposażenie węzła bez użycia zabezpieczeń.

- W celu osiągnięcia docelowego (czwartego) poziomu interoperacyjności systemu NATO należy podczas budowy sieci wymiany danych kierować się wymaganiami zawartymi w dyrektywie bezpieczeństwa AD-70-1 i zaleceń AM SG 719 F (sprawy instalacyjne) AM SG 720B, AM SG 788A (serwery stacje robocze urządzenia aktywne sieci).
- Docelowo infrastruktura teleinformatyczna powinna być kompatybilna z infrastrukturą NATO.

Główne inwestycje

SEC–WAN

Obecnie w siłach zbrojnych rozpoczął się proces budowy rozległej sieci do przetwarzania danych niejawnych o nazwie SEC-WAN. Sieć obejmuje swoim zasięgiem wszystkie instytucje resortu obrony narodowej, w których zachodzi konieczność wymiany informacji niejawnych od poziomu Instytucji Urzędu MON do poziomu związku taktycznego (Rys. 22).



Rys. 22 Struktura organizacyjno – funkcjonalne sieci SEC-WAN

Wyróżnić w niej można cztery zasadnicze grupy użytkowników:

- Instytucje Urzędu MON;
- Sztab Generalny WP;
- Okręgi Wojskowe, Rodzaje Sił Zbrojnych;
- Związki Taktyczne.

Infrastrukturę techniczną sieci tworzą:

- Sieć podkładowa: Podsystem Cyfrowej Łączności Utajnionej (PCŁU) z aktualnie wdrażanymi węzłami WP-40;
- Węzły sieci wyposażone w: routery jako elementy dostępowe do szkieletu sieci, huby, switche jako elementy aktywne sieci LAN i serwery poczty X.400 (zgodnie ze STANAG 4406 i zaleceniami ACP-123 i ACP-127;
- Lokalne sieci komputerowe LAN;
- Stacje robocze;
- Punkty ekspedycyjne;
- Techniczne środki zabezpieczenia informacji przed ulotem.

Zastosowany do budowy sieci sprzęt musi spełniać kryteria jakościowe infrastruktury przeznaczonej do przetwarzania niejawnego przedstawione w pkt. 3.3.

Sieć SEC-WAN będzie budowana etapami:

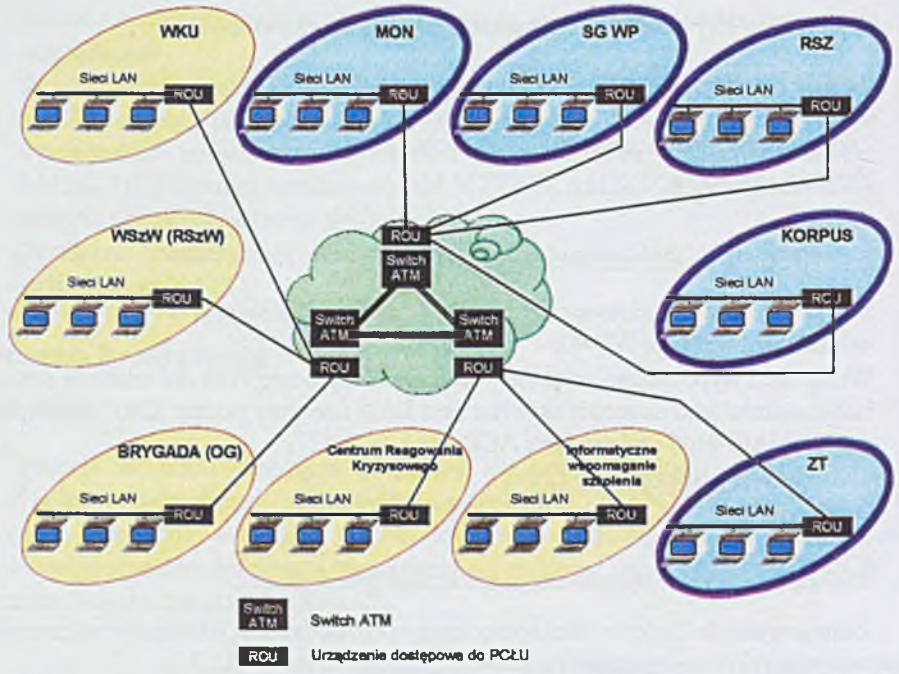
Etap I – powiązanie techniczne i informacyjne SGWP z dowództwami RSZ, OW, ZO i ZT oraz wybrane punkty ekspedycyjne;
Etap II – dołączenie dowództwa brygad;
Etap III – dołączenie pozostałych jednostek wojskowych.

Wymiana danych w sieci będzie odbywać się z wykorzystaniem protokołu TCP/IP. Rozwój infrastruktury technicznej stacjonarnej sieci SEC-WAN będzie ewoluować w kierunku technologii szerokopasmowych np. ATM, jako integrator usług z indywidualnym utajnianiem u użytkownika sieci. Struktura sieci SEC-WAN umożliwia współpracę z mobilnymi sieciami komputerowymi rozwijanymi na stanowiskach dowodzenia poprzez interfejsy V-35 urządzenie WP-40 i routery sieci mobilnej.

MIL-WAN

Sieć MIL_WAN z założenia jest przeznaczona do wymiany informacji jawnych i eksploatacji systemów informatycznych operujących na danych jawnych. Ze względu na funkcje jakie ma spełniać sieć wymiany danych zakłada się, że szkielet sieci komputerowej obejmuje swym zasięgiem siedziby instytucji urzędu MON, SGWP, Dowództw Okręgów Wojskowych oraz Rodzajów Sił Zbrojnych (Rys. 23).

Budowana sieć ma zabezpieczyć następujące główne usługi: pocztę elektroniczną, transfer plików, transfer ruchomych i nieruchomych obrazów.



Rys. 23 Struktura organizacyjno funkcjonalna sieci MIL-WAN

Zakłada się, że po wdrożeniu biurowych systemów informatycznych sieć przejmie również usługi telefaksowe oraz będzie integratorem dotychczas zbudowanych sieci LAN na różnych szczeblach dowodzenia SZ RP.

Realizację sieci MIL-WAN przewiduje się w trzech głównych etapach:

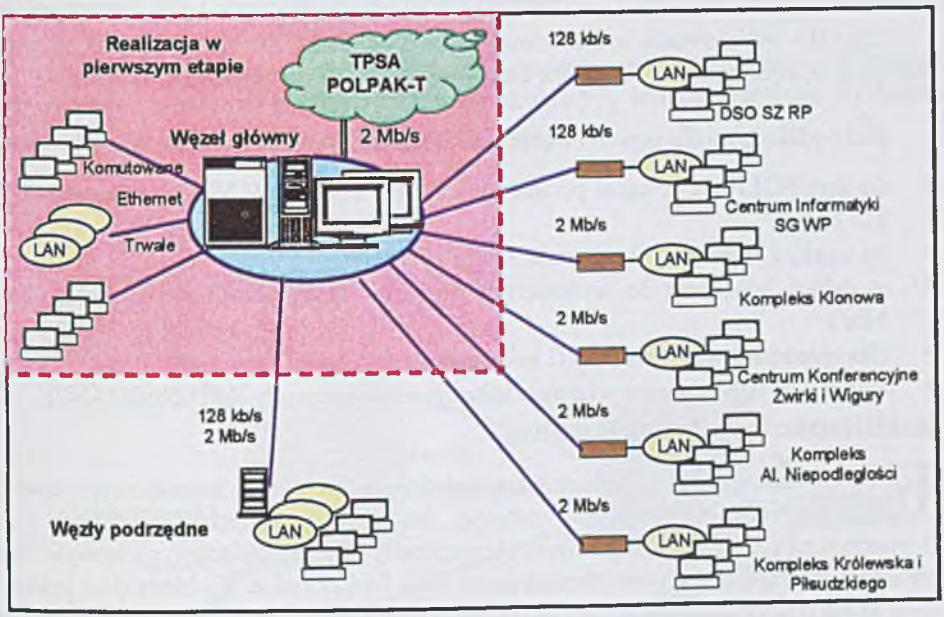
Etap I – Integracja sieci LAN w obiektach instytucji centralnych MON i SGWP. Etap ten jest w trakcie realizacji.
Etap II – Integracja sieci obiektowych poprzez budowę sieci MAN w garnizonie Warszawa.
Etap III – Budowa sieci na terytorium kraju.

Planowany termin realizacji inwestycji – rok 2002.

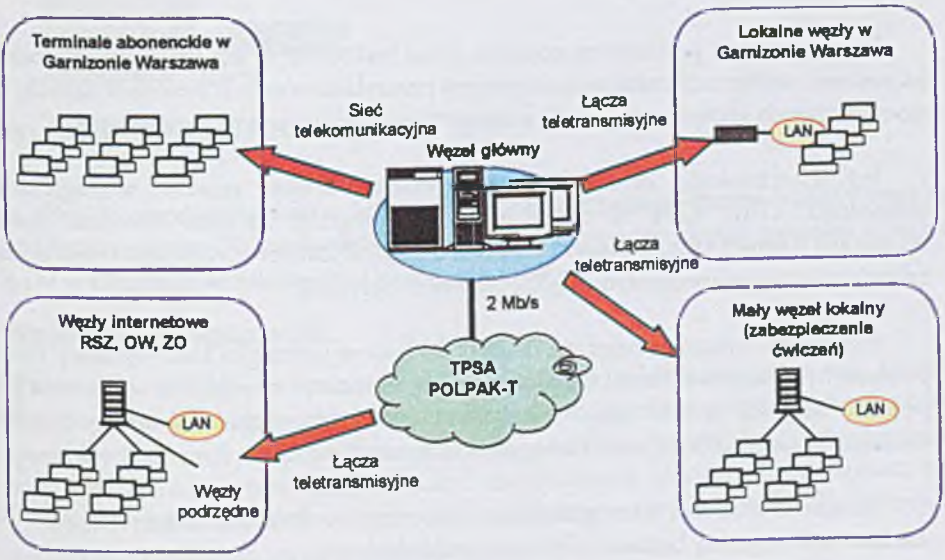
INTERNET

Praca sieci INTER-MON w wojsku jako podkładowej INTERNETU datuje się od roku 1997 kiedy to rozpoczął pracę węzeł pilotowy sieci. Swoim zasięgiem obejmował niewielu użytkowników z garnizonu Warszawa. Węzeł pilotowy dołączono do sieci INTRNET poprzez łącze 128 kb/s dzierżawione z TPSA (POLPAK-T). Abonęci dołączeni za pomocą łączy modemowych trwałych (czterodrut) i komutowanych (28,8 kb/s) Wówczas przystąpiono do prac związanych z budową infrastruktury technicznej

sieci podkładowej oraz opracowano wymagania funkcjonalne na węzeł główny sieci INTER-MON.



Rys. 24 Struktura organizacyjno-funkcjonalna sieci INTER-MON



Rys. 25 Ogólna struktura organizacyjno-funkcjonalna sieci INTER-MON

Rozwój sieci zaplanowano w dwóch etapach (Rys. 24):

Etap I – zbudowanie węzła głównego w oparciu o sprzęt informatyczny i oprogramowanie dostarczone przez jedną firmę.

Etap II – wbudowanie infrastruktury sieci INTER-MON łączącej węzeł główny z punktami dostępowymi w Warszawie oraz węzłami lokalnymi w RSZ, OW, i KZ.

Sieć podkładowa dla potrzeb węzła głównego zapewnia następujące relacje:

- do sieci POLPAK_T łącze podstawowe 2 Mb/s (G703, V.35), łącze zapasowe 128 kb/s;
- do węzłów lokalnych 3 łącza stałe 2 Mb/s;
- w dalszej kolejności do wysuniętych punktów dostępowych 4 łącza stałe 2 Mb/s.
- Obecnie realizowany jest etap II inwestycji.
- Rodzaje sił zbrojnych we własnym zakresie rozwijają węzły INTERNETOWE.

Możliwości integracji usług.

Etap III budowy sieci zakłada stworzenie jednej wspólnej sieci szkieletowej w oparci o węzły ATM, realizującej wymianę informacji jawnych, niejawnych oraz dostarczającej usług informatycznych. Argumentem przemawiającym na korzyść takiej struktury są względy zarówno ekonomiczne jak i funkcjonalne. Problem tkwi jednak w tym, że nie dysponujemy obecnie zweryfikowanymi sposobami, metodami, urządzeniami które pozwoliłyby stworzyć bezpieczną, jednorodną sieć resortową zgodną z ustawą o ochronie informacji niejawnych.

Innym istotnym problemem stojącym przed budowaną w ten sposób siecią rozległą jak również strukturami metropolitalnymi jest przesyłanie różnych strumieni danych, tzn. nie tylko danych komputerowych ale również danych video i danych głosowych.

Jedyną technologią, która jest w stanie obecnie spełnić stawiane wymagania jest technologia ATM. ATM nie tylko umożliwia integrację różnych strumieni danych, udostępnia również szeroki zakres przepustowości (od 2Mbps do 2,5Gbps) oraz posiada zaimplementowane mechanizmy QoS (Quality of Services).

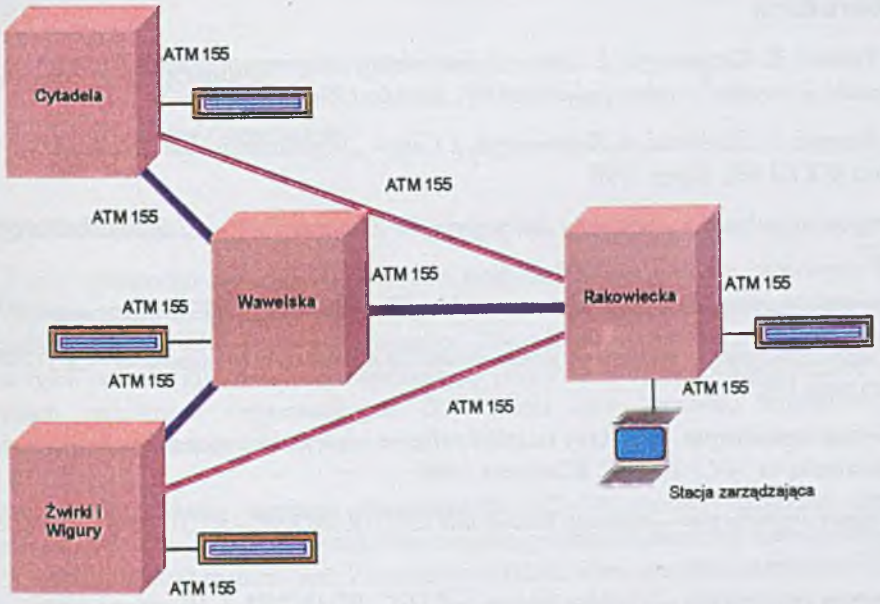
Pierwszym z przedsięwzięć na drodze do budowy rozległej sieci wymiany danych powinna być budowa szkieletu miejskiej sieci teleinformatycznej (MAN) w Warszawie dla potrzeb instytucji urzędu MON oraz instytucji wojskowych, spełniającej powyższe wymagania odnośnie możliwości integracji strumieni danych.

Szkielet budowanej sieci powinien być oparty o istniejące trasy kablowe. Jako medium wykorzystany będzie światłowód jednomodowy.

Sieć szkieletowa musi zapewni wysoki poziom odporności na uszkodzenia. Awaria jednego łącza będzie automatycznie wykrywana i sieć natychmiast dokona przekierowania ruchu.

Szkielet sieci będzie umożliwiał jednoczesną transmisję wielu niezależnych strumieni danych. Zakłada się, że poprzez sieć szkieletową transmitowane będą dane komputerowe, głos i obrazy wideo (wideokonferencje).

Budowa sieci może być realizowana etapami co przewidziano dobierając odpowiednie urządzenia, tak aby rozbudowa struktury o kolejne węzły nie wymagała wymiany całych urządzeń a jedynie ich rozszerzenie.



Rys. 26 Topologia sieci MAN.

Rys. 26 przedstawia obiekty, które byłyby objęte pierwszym etapem budowy węzłów sieci metropolitalnej. W następnym etapie można będzie rozbudować strukturę o węzły ATM w Okręgach Wojskowych i Dowództwie MW.

Wnioski i propozycje.

Inwestycje związane z tworzeniem infrastruktury teleinformatycznej są bardzo kosztowne. Wymagają one maksymalnego wykorzystania posiadanych zasobów sprzętowych a przede wszystkim jednoznacznego określenia priorytetów. Ściśle określone muszą być też relacje wysokości nakładów do uzyskanych efektów. Ważną sprawą jest wybieranie produktów skalowalnych tzn. takich które zapewnią realizację bieżących potrzeb jak i możliwość przyszłej rozbudowy.

Należy położyć szczególny nacisk na następujące elementy inwestycji:

- Dostosowanie infrastruktury telekomunikacyjnej do transmisji danych: wprowadzanie central cyfrowych wyposażonych w moduły ISDN, pracujących z systemem sygnalizacji SS7, skalowalnych w kierunki technologii szerokopasmowych (ATM), wyposażenie abonentów w terminale ISDN, wprowadzenie węzłów pakietowych WP-40 do systemu PCŁU;
- Zgodność infrastruktury z normami obowiązującymi w Wojsku Polskim oraz wymaganiami NATO.

Literatura

A. Sawicki, K. Kaczmarczyk, J, Cebo – „Infrastruktura teleinformatyczna Sił Zbrojnych i kierunki jej rozwoju" – referat Infofestiwal 96', Kraków 1996

A. Barczak, P. Zaskórski, K. Kaczmarczyk, j. Cebo – „Wojskowa sieć wyminy danych" – referat WKTiI 98', Zegrze 1998

„Program organizacyjno – użytkowy sieci rozległej Sił Zbrojnych RP" – CI SG WP, Warszawa 1997

„Program organizacyjno – użytkowy budowy MIL_WAN" – CI SG WP, Warszawa 1997

„Wstępne założenia na budowę sieci komputerowych w resorcie Obrony Narodowej" CI SG WP, Warszawa 1997

„Program organizacyjno – użytkowy instalacji połączeń międzyobiektowych w kompleksie Rakowiecka 4a" – CI SG WP, Warszawa 1996

„Program organizacyjno – użytkowy budowy sieci INTER-MON" – CI SG WP, Warszawa 1998

„Program organizacyjno – użytkowy budowy sieci SEC_WAN" ZŁI, Warszawa 1999

„Struktura Techniczno funkcjonalna infrastruktury teleinformatycznej dla potrzeb ZSyD" – CI SG WP 1999

8

8. Zautomatyzowany System Dowodzenia SZ RP

płk dr inż. Lech Kwiatek

płk dr inż. Andrzej Grochalski

Wprowadzenie

W celu sprawnego dowodzenia w czasie pokoju, kryzysu i wojny organizuje się system dowodzenia stanowiący zgodnie z zasadami taktyki i sztuki operacyjnej uporządkowaną całość złożoną z organów dowodzenia i środków dowodzenia, sprzężonych ze sobą informacyjnie, zapewniający podejmowanie stosownych decyzji na wszystkich poziomach organizacyjnych dowodzenia oraz sprawną, terminową i bezwzględną ich realizację.

Zautomatyzowany System Dowodzenia (ZSyD) stanowi integralną część systemu dowodzenia. Tworzą go wzajemnie ze sobą powiązane elementy funkcjonalne i organizacyjne, ludzkie i materiałowe. Zasadniczymi składowymi elementami systemu są:

- Organa dowodzenia rozmieszczone w przygotowanych miejscach pracy zorganizowanych jako: SD, ZSD, WSD, itp.;
- Infrastruktura informatyczna i telekomunikacyjna obszaru;
- Siły i mobilne środki informatyki i łączności wykorzystywane w dynamice działań.

ZSyD SZ RP musi zapewnić realizację w czasie „P" i „W" podstawowych funkcji: opracowywania, przetwarzania, wymiany i przechowywania informacji istotnych dla dowodzenia. W warunkach stałej gotowości system ten powinien wspomagać działalność szkoleniową, planistyczną, ewidencyjno-sprawozdawczą, a także przygotowywanie i przebieg ćwiczeń oraz prace związane z osiąganiem i utrzymywaniem wyższych stanów gotowości bojowej. Ma także służyć do utrzymywania aktualnej informacji, niezbędnej w sprawnym kierowaniu procesami rozwijania wojsk do działań na zaplanowanych kierunkach.

W stanie osiągania podwyższonej gotowości bojowej system powinien wspomagać kierowanie mobilizacyjnym i operacyjnym rozwinięciem SZ, a następnie dowodzenie na stanowiskach dowodzenia rozwijanych w oparciu o wcześniej przygotowaną

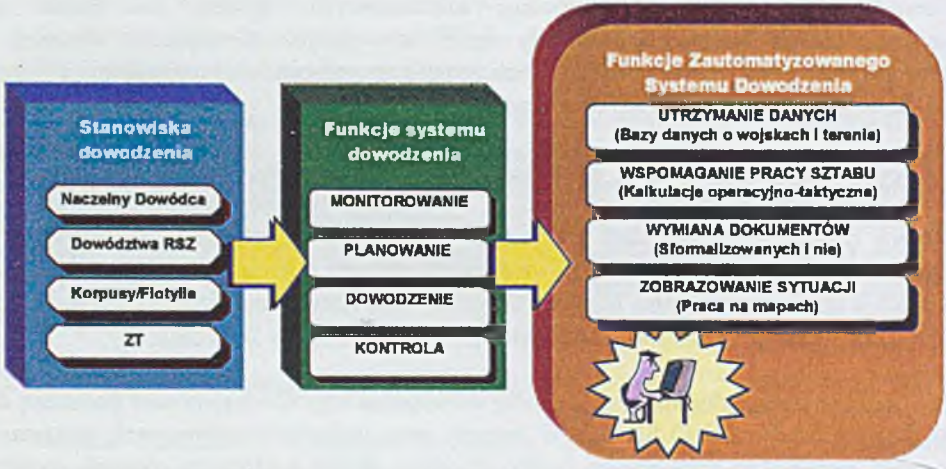
Grafiki Operacyjnej (PGO), bazy danych o wojskach i wybrane zadania kalkulacyjno-obliczeniowe.

Uzupełnieniem tych wysiłków jest budowa zautomatyzowanego systemu dowodzenia szczebla taktycznego. W bieżącym roku Państwowy Instytut Telekomunikacji rozpoczął prace technologiczne nad ZSyD WLąd szczebla ZT, związane z budową rodziny zautomatyzowanych wozów dowodzenia.

Model ZSyD

Zgodnie z istniejącymi poglądami, Zautomatyzowany System Dowodzenia stwarza warunki do skrócenia procesu podejmowania decyzji, a zatem także wyprzedzania potencjalnego przeciwnika w realizacji cyklu dowodzenia. Podnosi także jego jakość poprzez usprawnienie wymiany, gromadzenia, przetwarzania i udostępniania informacji między osobami funkcyjnymi i zespołami dowódczo-sztabowymi. Nie likwiduje jednak wysiłku oraz odpowiedzialności ludzi za podejmowane decyzje. System ma realizować powtarzalne, praco i czasochłonne czynności, umożliwiając zespołom skoncentrowanie się na istotnych czynnościach decyzyjnych, których nie można zautomatyzować i trzeba wykonać w sposób tradycyjny.

Zasadniczymi elementami ZSyD SZ RP są powiązane wzajemnie zautomatyzowane systemy: ND SZ RP, WLąd, MW i WLOP.



Rys. 27 Funkcje systemu dowodzenia w systemie zautomatyzowanym

Pomimo wzajemnych różnic proces dowodzenia w tych systemach jest podobny i obejmuje wykonywanie następujących funkcji dowodzenia: monitorowanie, analiza i ocena sytuacji, planowanie działań, dowodzenie wojskami i kontrola realizacji postawionych zadań. ZSyD wspomaga ich realizację poprzez swoje funkcje: utrzymania

danych, informatycznego wspomagania pracy sztabu, wymiany dokumentów i zobrazowania sytuacji (Rys. 27).

Oprogramowanie użytkowe systemu można podzielić na oprogramowanie:

- Baz danych, umożliwiający zakładanie i utrzymywanie danych;
- Wymiany informacji, sformalizowanych i niesformalizowanych dokumentów dowodzenia (zarówno tekstowych, jak i graficznych);
- Grafiki operacyjnej, umożliwiający pracę na mapach numerycznych;
- Specjalistyczne, umożliwiające prowadzenie kalkulacji operacyjno-taktycznych.

ZSyD powinien posiadać ustalony zestaw jednolitych narzędzi do wytwarzania, gromadzenia, przetwarzania, zobrazowywania i przekazywania informacji.

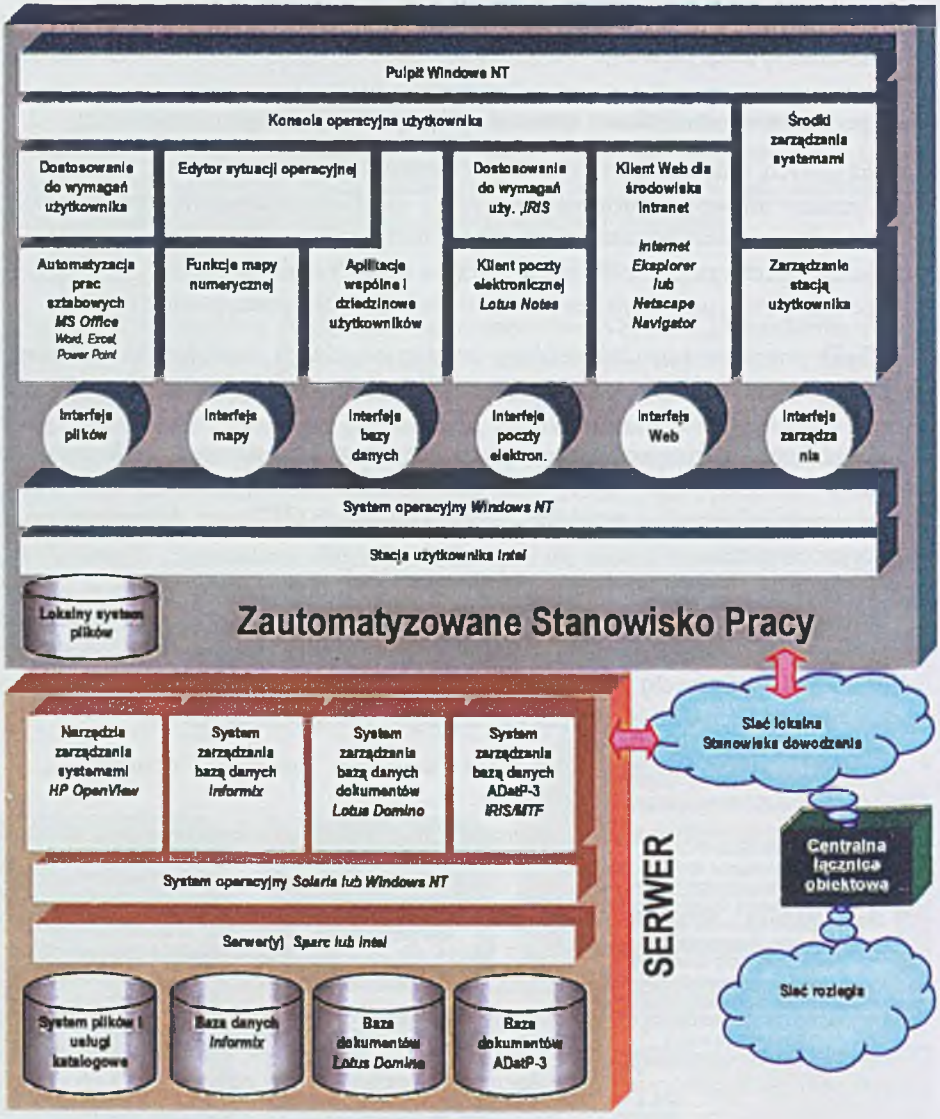
Zasadniczym elementem systemu jest **podsystem baz danych**, na który składają się bazy danych oraz oprogramowanie umożliwiające utrzymywanie danych obejmujących: informacje o wojskach, terenie i obiektach OPT oraz dokumenty i normy operacyjno-taktyczne.

Podsystem wymiany informacji stanowi element ZSyD zapewniający przesyłanie sformalizowanych i niesformalizowanych dokumentów dowodzenia (tekstowych i graficznych) między jego abonentami przy wykorzystaniu technicznych środków łączności, transmisji danych i informatyki. Przeznaczony jest do:

- Organizowania wymiany informacji wewnątrz stanowisk dowodzenia i pomiędzy stanowiskami dowodzenia;
- Ewidencji, porządkowania i utrzymywania jednolitości informacji niezbędnych w dowodzeniu.

Podsystem Grafiki Operacyjnej jest przeznaczony do zobrazowywania rozmieszczenia obiektów terenowych i wojsk na podkładzie mapy cyfrowej. Umożliwia operowanie mapą podkładową, przeglądanie i nanoszenie sytuacji operacyjno-taktycznej, wyświetlanie informacji opisowej zawartej w bazach danych o wojskach i terenie oraz pracę grupową na mapie. Podsystem ten ma umożliwić w przyszłości funkcje: zobrazowania rzeczywistych lub symulowanych działań wojsk na mapach numerycznych, edycję informacji opisowych o wojskach i terenie, prowadzenie kalkulacji operacyjno-taktycznych oraz przesyłanie sytuacji operacyjno-taktycznej.

Podsystemy specjalistyczne przeznaczone są dla poszczególnych komórek organizacyjnych stanowisk dowodzenia wykonujących zarówno wspólne, jak i swoje specjalistyczne zadania. W skład oprogramowania użytkowego wchodzą grupy zadań ogólnego przeznaczenia oraz użytkowe specjalistyczne, dedykowane dla poszczególnych grup (G1-G6) wchodzących w skład stanowiska dowodzenia.



Rys. 28 Ogólna struktura oprogramowania ZSyD WLąd

Elementami oprogramowania użytkowego są moduły:

- Kompleksowej oceny terenu;
- Symulacji działań wojsk;
- Oceny sił i środków przeciwnika oraz sił i środków własnych;
- Zobrazowania informacji o wojskach przeciwnika;
- Planowania użycia sił i środków rozpoznania i walki radioelektronicznej;

- Oceny możliwości realizacji zadań: WRiA, WInż, WOPChem, WOPL, WŁiI;
- Planowania użycia: WRiA, WInż, WOPChem, WOPL, WŁiI;
- Oceny i planowania zabezpieczenia logistycznego wojsk;
- Zasilania bazy danych organizacyjno-etatowej;
- Planowania i kierowania mobilizacyjnego.

Pod względem architektonicznym system posiada strukturę dwuwarstwową, obejmującą warstwę usług lokalnych i sieciowych. Poszczególni użytkownicy pracują w oparciu o Zautomatyzowane Stanowiska Pracy (ZSP), będące elementami sieci komputerowych poszczególnych stanowisk dowodzenia.

Ogólna struktura oprogramowania systemowego i użytkowego została przedstawiona na Rys. 28. W zależności od szczebla oraz stanowiska dowodzenia będzie użytkowana różna liczba serwerów oraz ZSP.

W warunkach stacjonarnych zostanie zbudowana odpowiednia infrastruktura teleinformatyczna, której elementami będą:

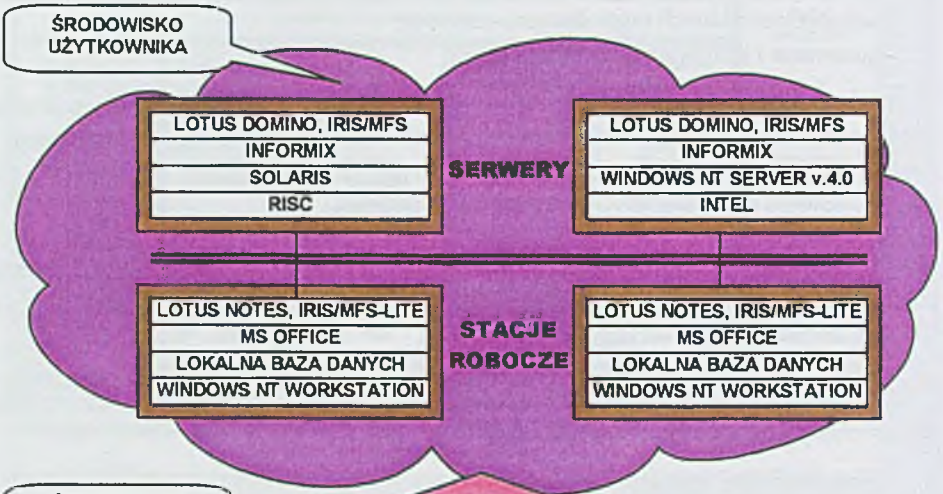
- System cyfrowej łączności utajnionej;
- Lokalne sieci komputerowe z serwerami baz danych i dokumentów oraz infrastrukturą wymiany danych w ramach stanowisk dowodzenia;
- Zautomatyzowane stanowiska pracy osób funkcyjnych wraz z oprogramowaniem systemowym, serwisowym oraz użytkowym.

Charakterystyka rozwiązań technologicznych

Współczesne systemy informatyczne, szczególnie zaliczane do klasy ZSyD stają się coraz bardziej złożone funkcjonalnie, logicznie i technicznie. Ich budowa i wdrażanie jest zawsze wieloletnim przedsięwzięciem, angażującym wiele zespołów analitycznych, projektowych i produkcyjnych oraz poważne środki finansowe. Cykl rozwojowy i wdrożeniowy takich systemów, najczęściej wieloetapowy, trwa wiele lat i wymaga rygorystycznego zarządzania. Systemy informatyczne muszą nadążać za zmieniającą się rzeczywistością, szybko reagować na zmiany wymagań i być odporne na fluktuacje kadrowe i organizacyjne zarówno zespołów projektowych, jak i użytkowników. Sprostanie tym wymaganiom wymusza standaryzację procesu projektowania i stosowanie narzędzi automatyzacji do wspomagania zarządzania projektowaniem, wytwarzania i utrzymywania systemów informatycznych.

Bezpieczeństwo przetwarzania powoduje konieczność stosowania do budowy szkieletu systemów wojskowych wysoce profesjonalnych i bezpiecznych systemów operacyjnych oraz środków sprzętowych i programowych. Brak na rynku komputerowym idealnego narzędzia technologicznego, obejmującego pełny cykl projektowy, powoduje konieczność zastosowania „ciągów technologicznych" do wspomagania wytwarzania oprogramowania.

Aktualną bazę technologiczną budowy ZSyD ND SZ RP i WLąd przedstawiono na rysunku (Rys. 29).



UPPER-CASE	System Architect		
LOWER-CASE	LOTUS NOTES	MS VISUAL STUDIO	POWER STUDIO
Języki programowania	LOTUS SCRIPT (JAVA)	C++ (JAVA)	C++ (JAVA)
Dokumentowanie	Repozytorium projektu, pliki		

Rys. 29 Baza technologiczna budowy ZSyD SZ RP i WLąd

Uwarunkowania wdrożeniowe

Budowa ZSyD jest warunkowana:

- Stworzeniem stacjonarnej i mobilnej infrastruktury telekomunikacyjnej zabezpieczającej odpowiednie usługi wymiany danych,
- Wyposażeniem komórek funkcjonalnych stanowisk dowodzenia wszystkich szczebli w odpowiednią infrastrukturę informatyczną, a w tym w:
    - Lokalną sieć komputerową z serwerami baz danych, serwerami plików, serwerami dokumentów multimedialnych, serwerami poczty elektronicznej oraz serwerami zarządzania i ochrony systemu przed nieuprawnionym dostępem do informacji, a także z odpowiednimi stacjami roboczymi i urządzeniami zewnętrznymi do bezpośredniej obsługi osób funkcyjnych,

- Oprogramowanie systemowe tworzące platformę aplikacyjną dla poszczególnych klas funkcjonalnych komputerów w sieciach lokalnych (serwerów, stacji graficznych, stacji roboczych), obejmujące system operacyjny i systemowe oprogramowanie usługowe,
- Oprogramowanie użytkowe serwerów i stacji roboczych, wyspecjalizowane według przeznaczenia serwerów i stacji roboczych w podsystemach i komórkach funkcjonalnych - stosowanie do zakresu rozwiązywanych problemów w cyklu dowodzenia i roli poszczególnych osób funkcyjnych.

Pełne wdrożenie rozwiązań informatycznych jest uwarunkowane możliwościami finansowymi w obszarze telekomunikacji i informatyki.

Wnioski i propozycje

Budowa **ZSyD SZ RP obejmującego ZSyD ND i RSZ powinna być prowadzona zgodnie z dostępnymi standardami i zaleceniami NATO** w zakresie technicznym, proceduralnym i operacyjnym, a także skali wdrożenia w praktyce sztabowej. Należy kłaść nacisk na konieczność integracji i współdziałania ZSyD Rodzajów Sił Zbrojnych. W budowie ZSyD SZ RP należy uwzględnić programy bezpieczeństwa państwa w tym ustawy „O powszechnym obowiązku obrony" i „O kompetencjach organów władzy publicznej w zakresie obronności państwa", a także wymogi Dowództwa Połączonych Sił Zbrojnych NATO.

Cykl badawczo-rozwojowy powinien bazować na strategii przyrostowej, składającej się z czasowo-przesuniętych podcykli realizacji podsystemów funkcjonalnych. Kolejne podcykle powinny obejmować systemy kolejnych szczebli dowodzenia wraz z ich otoczeniem terminalowym w jednostkach bezpośredniego podporządkowania. W ramach podcyklu należy wykonać komplet obiektów z wyposażeniem telekomunikacyjnym i informatycznym. Dopuszcza się etapowe wykonanie oprogramowania w ramach podcyklu. Pierwszy etap obejmuje wtedy oprogramowanie niezbędne do wykonania weryfikacji funkcjonalności w zakresie ogólnej koncepcji systemu, ukompletowania i funkcjonalności obiektów wraz z ich wyposażeniem, obiegu dokumentów, baz danych, ochrony informacyjnej i zarządzania systemem, a w tym:

- Kompletną platformę aplikacyjną (system operacyjny z oprogramowaniem usług użytkowych, w tym systemów zarządzania danymi, poczty elektronicznej i automatyzacji prac biurowo-sztabowych);
- Oprogramowanie baz danych z pakietem zadań technologicznych i pakietem podstawowych zadań informacyjnych;
- Oprogramowanie automatyzacji prac sztabowych, w tym wytwarzania i obiegu sformalizowanych i niesformalizowanych dokumentów;
- Oprogramowanie zarządzania zasobami informacyjnymi i aplikacjami, w tym centralnego zarządzania konfiguracjami i diagnostyką;

- Oprogramowanie ochrony bezpieczeństwa informacyjnego systemu.

Kolejne etapy powinny przebiegać współbieżnie i obejmować specjalistyczne oprogramowanie zadań użytkowych.

Literatura

Baza techniczno-narzędziowa wspomagania projektowania ZSyD. Opracowanie zbiorowe pod kierownictwem płk. dr hab. E. Kołodzińskiego, WAT, 1997r.

Projekt koncepcyjny i projekt ZTT dla ZSyD WLąd. Opracowanie zbiorowe pod kierownictwem płk. dr P. Zaskórskiego, CI SG WP, 1997r.

Standaryzacja systemów dowodzenia i kierowania środkami walki w NATO. Myśl Wojskowa, 6(1997) - Stokalski A., Zaskórski P.

Interoperability of Command & Control Information Systems based on International Standards in Communications and Information Systems. AFCEA Conf., Brno, Nov. 1995r. K. Wagner.

Proudfoot M.: An Architecture for a NATO Automated Command and Control System. AFCEA Conf., Brussels, Oct., 1992r.

Architektura funkcjonalno-techniczna zautomatyzowanych systemów dowodzenia wojsk lądowych. VI Wojskowa Konferencja Telekomunikacji i Informatyki - Kołodziński E., Pietkiewicz T., Stokalski A.

Architektura ZSyD MW. V Konferencja Naukowa, Jelenia Góra 1999 - R.Rugała.

Technologie projektowo-wdrożeniowe wytwarzania aplikacji i kierunki ich standaryzacji. InfoFestival'96, Kraków - P.Zaskórski, L.Bartłomiejczyk

9

9. Informatyzacja logistyki

ppłk mgr inż. Leszek Karaś

kpt. mgr inż. Marek Józefczak

Wprowadzenie

Struktury organizacyjne logistyki Sił Zbrojnych RP ulegały w ostatniej dekadzie ciągłej przebudowie. Obecnie pojawiły się nowe wyzwania wynikające z pełnoprawnego uczestnictwa Polski w strukturach NATO. Z tego powodu zachodzi potrzeba uwzględnienia w nowej koncepcji funkcjonowania logistyki wymogów interoperacyjności. Przykładem może być konieczność następującego podziału zadaniowo-kompetencyjnego logistyki SZ RP:

- Logistyka producenta (ang. ***production logistics***);
- Logistyka konsumenta (ang. ***consumer logistics***);
- Logistyka kooperacyjna (ang. ***cooperative logistics***).

Podział ten ma zapewnić utrzymywania potencjału logistycznego zgodnie z wymaganymi standardami oraz możliwość współdziałania z odpowiednimi strukturami logistycznymi NATO (tzw. NPLO - *NATO Production and Logistics Organizations* - Organizacje NATO do spraw produkcji i logistyki).

Logistyka kooperacyjna łączy relacjami kompetencyjnymi, formalno-prawnymi i strukturami organizacyjnymi obie wyżej wymienione. Wypracowuje zasady i procedury wzajemnego współdziałania. Jest to nadrzędne ogniwo o charakterze decyzyjno-koordynującym.

Głębokie zmiany struktur organizacyjno-funkcjonalnych logistyki i zasad funkcjonowania na wszystkich szczeblach organizacyjnych SZ powodują konieczność wprowadzenia radykalnych zmian w istniejących systemach informatycznych. Na dzień dzisiejszy nie są one adekwatne do obecnych potrzeb informacyjnych organów kierowania logistyką SZ RP i jednostek wykonawczych. Wymogiem czasu staje się stworzenie **zintegrowanego systemu logistycznego** (ZSL), w sposób kompleksowy i zunifikowany wspomagający informatycznie wszystkie procesy logistyczne w resorcie ON występujące obecnie i te, które mogą wystąpić w związku z przyjętymi zobowiązaniami państwa członka NATO.

Stan aktualny

Logistyka SZ RP posiada wiele dedykowanych problemowo, autonomicznych rozwiązań informatycznych adekwatnych do minionych struktur organizacyjno-funkcjonalnych.

Wiodącą rolę informatycznego wspomagania procesów logistycznych na wszystkich szczeblach kierowania zasadniczo spełniają dwie klasy systemów:

1. **LOGIS** – systemy dedykowane dla szczebla centralnego i okręgowego, wspierają procesy kierowania zaopatrzeniem w środki materiałowe, bojowe, uzbrojenie i sprzęt wojskowy (UiSW) i odtwarzania ich resursów eksploatacyjnych (kierowanie gospodarką remontową).
2. **SIGMAT** – systemy dedykowane do obsługi jednostek wykonawczych typu składnica specjalistyczna w zakresie zaopatrywania w następujące klasy materiałowe:
   - środki bojowe;
   - techniczne środki materiałowe;
   - mundury i żywność;
   - materiały pędne i smary (MPS);
   - środki medyczne.

Ich rozwój zdeterminowany był przez:

- Specjalistyczne zorientowanie poszczególnych komórek organizacyjnych logistycznych na wszystkich szczeblach;
- Obowiązujące procedury planowania i dystrybucji (system nakazowo-rozdzielczy oraz podporządkowany mu system sprawozdawczy i obieg informacji logistycznej);
- Brak jednolitej, centralnej bazy indeksowo-kodowej obejmującej wszystkie klasy materiałowe, uzbrojenia i techniki wojskowej;
- Brak rozległej sieci wymiany danych dostępnej dla wszystkich szczebli kierowania i dowodzenia.

Stąd też systemy mają charakter ściśle ukierunkowany na poszczególne, specjalistyczne piony funkcjonalne.

W obecnym stanie do podstawowych mankamentów tych systemów należy zaliczyć:

- Autonomiczność rozwiązań (nie tworzą kompleksowego, zintegrowanego systemu);
- Dedykowanie do wyspecjalizowanych pionów funkcjonalnych i organizacyjnych, których część już nie istnieje;
- Brak systemu informowania logistycznego (SIL) dla szczebla Rejonu Logistycznego (RL) i Rejonowej Bazy Materiałowej (RBM);

- Nie wystarczająca lub zdezaktualizowana funkcjonalność systemów (np. w zakresie prowadzenia ewidencji ilościowo-wartościowej na potrzeby pionu głównego księgowego, planowania potrzeb materiałowych itp.);
- Doraźny sposób prowadzenia ewidencji ilościowo-wartościowej;
- Dezaktualizacja procedur planistycznych;
- Podporządkowanie zawartości informacyjnej systemu sprawozdawczego poprzednim strukturom kierowania i obiegu informacji w logistyce SZ RP;
- Płynność aktów prawnych sankcjonujących funkcjonowanie służb logistycznych (obowiązujące akty prawne mają charakter tymczasowy).

W szczególności systemy szczebla centralnego i okręgowego klasy LOGIS ze względu na radykalne przeobrażenia w funkcjonowaniu logistyki SZ RP wymagają modyfikacji oraz nie pokrywają potrzeb informacyjnych tych szczebli, szczególnie w zakresie bieżącego informowania logistycznego ze względu na brak odpowiedniej infrastruktury sieciowej i dedykowanego do tego celu oprogramowania użytkowego.

Systematyka i klasyfikacja SI logistyki

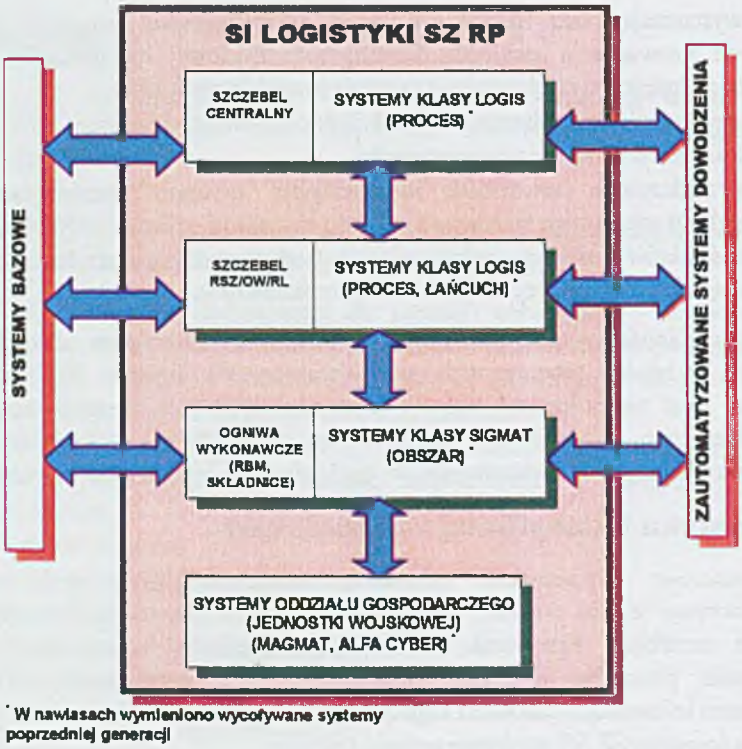
Komputerowe wspomaganie kierowania procesami logistycznymi w SZ RP realizowane jest za pomocą wielu systemów informatycznych występujących na wszystkich szczeblach kierowania i dowodzenia. Spełniają funkcje komputerowego wspomagania procesów zbierania, przechowywania, przetwarzania, dystrybucji i zobrazowania informacji o zasobach logistycznych dla potrzeb zarządzania, dowodzenia i kierowania logistyką SZ RP w okresie pokoju i wojny.

W zależności od ich umiejscowienia w strukturze organizacyjnej SZ RP można SI logistyki można podzielić na systemy szczebla (Rys. 30):

- Centralnego (strategicznego);
- Rodzajów sił zbrojnych (strategiczno-operacyjnego);
- Okręgowego (operacyjnego);
- Związku taktycznego;
- Oddziału (JW, ogniwo wykonawcze - np. składnica, szpital).

Z punktu widzenia klasy modelu użytkowania, ich funkcjonowania, współzależności informacyjnej i odrębności organizacyjno-zadaniowej możemy wyróżnić następujące grupy systemów:

- Systemy bazowe;
- Terytorialne logistyczne systemy informatyczne;
- Systemy dziedzinowe;
- Systemy obiektowe;
- Systemy autonomiczne;
- Systemy dowodzenia (zautomatyzowane systemy kierowania zabezpieczeniem logistycznym).



Rys. 30 Wykorzystanie systemów logistycznych w SZ RP

Systemy bazowe obejmują procesy utrzymywania i dystrybucji jednolitych i ustandaryzowanych (powielanych) w skali SZ zasobów informacyjnych, głównie w zakresie bazy: indeksowo-kodowej, etatowo-normatywnej i organizacyjno-strukturalnej współużytkowanej przez SI różnych pionów i komórek organizacyjno-funkcjonalnych. Z punktu widzenia zawartości informacyjnej systemy te dzielimy na:

- Organizacyjno-adresowe, a w tym:
  - Baza indeksowo-kodowa środków materiałowych, bojowych uzbrojenia i sprzętu wojskowego;
  - Jednolity kod adresowy jednostek wojskowych;
  - Ewidencja obiektów operacyjnego przygotowania terenu;
- Etatowo-należnościowe, a w tym:
  - Zabezpieczenie materiałowo-mobilizacyjnych potrzeb wojsk;
  - Tabele należności, przydziały gospodarcze, normatywy;
  - Ewidencja i zarządzanie stanami etatowymi wojsk;
  - Gospodarowanie zasobami mobilizacyjnymi.

Systemy dziedzinowe wspomagają realizację funkcji kierowania czasu „P" w pionach funkcjonalnych logistyki i zawierają dane niezbędne dla potrzeb ich bieżącej działalności (są to głównie systemy ewidencji stanowej). Systemy te stanowią rdzeń informacyjny dla systemów dowodzenia.

Do tej grupy można zaliczyć następujące systemy klasy LOGIS:

- Zarządzanie zasobami obronnymi państwa utrzymywanymi w strukturach SZ;
- Kierowanie zaopatrzeniem wojsk w środki bojowe;
- Grupa systemów kierowania zaopatrywaniem w środki materiałowe;
- Kierowanie eksploatacją i remontami uzbrojenia i sprzętu wojskowego;
- Ewidencja i użytkowanie budynków oraz infrastruktury terenów wojskowych;
- Ewidencja i sprawozdawczość w zakresie infrastruktury i sprzętu kwaterunkowego.

Systemy obiektowe przeznaczone są do komputerowego wspomagania obsługi jednostek organizacyjnych (obiektów typu składnica, oddział gospodarczy itd.).

Przykładowymi systemami w tej grupie są systemy klasy SIGMAT:

- Składnicowy SI zaopatrywania w środki bojowe;
- Składnicowy SI zaopatrywania w techniczne środki materiałowe;
- Składnicowy SI zaopatrywania w żywność i przedmioty mundurowe;
- Składnicowy SI zaopatrywania w materiały pędne i smary;
- Składnicowy SI zaopatrywania w środki medyczne;
- Systemy obsługi szpitala wojskowego.

Systemy autonomiczne są to systemy komputerowo wspomagające osoby funkcyjne lub wydzielone komórki organizacyjne w zakresie specjalistycznych funkcji realizowanych na danym stanowisku pracy. Przykładowymi systemami w tej grupie są: system orzecznictwa Wojskowych Komisji Lekarskich oraz sprawozdawczość i statystyka wojskowo-medyczna.

Systemy dowodzenia i kierowania środkami walki stanowią hierarchicznie najwyżej zorganizowany kompleks systemów SZ RP, charakteryzujący się dużą dynamiką zadaniowo-funkcjonalną. Ich integralną część stanowią podsystemy logistyczne:

- Zautomatyzowanego systemu dowodzenia Wojskami Lądowymi;
- Zautomatyzowanego systemu dowodzenia Marynarką Wojenną.
- Zautomatyzowanego systemu dowodzenia Wojskami Lotniczymi i Obrony Powietrznej.

Zakres funkcjonalny

Systemy informatyczne logistyki swoim działaniem obejmują następujące obszary funkcjonalne:

Kierowanie i dowodzenie zabezpieczeniem logistycznym - wspierają procesy kierowania działalnością poszczególnych jednostek logistycznych danego szczebla (w układzie poziomym) i dowodzenia w układzie hierarchicznym (w układzie pionowym).

Zabezpieczenie materiałowe - wspierają procesy zasilania wojsk wszystkimi klasami materiałowych zasobów logistycznych.

Zabezpieczenie techniczne - wspierają procesy pozyskiwania, użytkowania, eksploatacji i remontów uzbrojenia i sprzętu wojskowego.

Zabezpieczenie komunikacyjne - wspierają procesy realizacji przewozów wojskowych, kierowanie ruchem w sieci komunikacyjnej oraz zabezpieczenia jej odpowiedniego stanu technicznego.

Zabezpieczenie infrastruktury - wspierają procesy przygotowania i utrzymania obiektów stacjonarnych niezbędnym wojskom do zakwaterowania i szkolenia oraz dla potrzeb działań operacyjnych.

Zabezpieczenie medyczne - wspierają procesy utrzymania odpowiedniego stanu zdrowia żołnierzy, zabezpieczenia pola walki w środki medyczne i opatrunkowe, opieki lekarskiej i transportu rannych.

Systemy ze względu na okres ich powstawania, różne instytucje kierujące wykorzystują następujące platformy sprzętowo-programowe:

EMC ODRA - GEORGE 3 - PLAN, COBOL, PLAN;
MERA 660 - RT-11 - DIBOL;
AS 400 – OS/400 – COBOL/400 firmy IBM (generator aplikacji SYNON/2E);
IBM PC – SCO UNIX – INFORMIX 4GL;
IBM PC – DOS, WINDOWS - MS Access, dBase, Clipper, Magic.

Perspektywy rozwoju

Obecnie podejmowane są działania zmierzające do stworzenia wieloszczeblowego, **zintegrowanego sytemu logistycznego** (ZSL) w sposób kompleksowy i zunifikowany wspomagający informatycznie wszystkie procesy logistyczne. Powinien on posiadać otwartą architekturę zapewniającą dynamiczną zmianę funkcjonalności (*ang. functional flexibility*), aby na bazie elementarnych funkcji logistycznych (*ang. basic logistic kernel*) możliwe było łatwe i szybkie tworzenie nowych usług. Współczesny ZSL powinien realizować zasadę JIT (*ang. Just In Time*), tzn. zapewnić dostarczenie właściwego materiału (usługi, informacji), we właściwej ilości, odpowiedniej jakości, we właściwe miejsce, we właściwym czasie.

Jego funkcjonalność można generalnie ująć jako zintegrowany system kompleksowego i zunifikowanego zarządzania zasobami przedsiębiorstwa klasy ERP (*ang. Enterprise Resource Planning*). Zapewnia informatyczną obsługę zasadniczych grup procesów logistycznych związanych z planowaniem logistycznym, gospodarką materiałową, dystrybucją, gospodarką remontową, zarządzanie produkcją, zarządzaniem jakością, zarządzaniem usługami i wzajemnie powiązanych informacyjnie poprzez podsystemy:

- SIL - System Informowania Logistycznego (*ang. LIS-Logistic Information System*);
- SWPD - System Wspierający Podejmowanie Decyzji (*ang. DSS-Decision Support System*).

Wspiera mechanizmy handlu elektronicznego (*ang. electronic commerce*) w oparciu o standard EDIFACT. Spełnia wymogi sieci INTRANET/INTERNET, w pełni wykorzystuje mechanizmy oferowane przez technologię WWW. Cechuje się w pełni rzeczywistą trójwarstwową architekturą typu klient/serwer: warstwa graficznego interfejsu użytkownika, warstwa aplikacji zrealizowana w oparciu o maszynę wirtualną i warstwa serwerów baz danych. Zapewnia to rzeczywistą separację logiki aplikacji (funkcji transformacji danych elementarnych w wynikowe) od sposobu fizycznej alokacji danych.

Współczesny ZSL cechuje całościowe ujęcie elementarnych procesów logistycznych i wyraża się zapewnieniem dedykowanej obsługi informatycznej na wszystkich etapach realizacji pełnego łańcucha dostaw (*ang. Supply Chain Managemnt*).

Dalsze prace związane z rozwojem projektowanych i eksploatowanych systemów informatycznych w pionie Logistyki SZ mogą przebiegać jedną z dwóch dróg:

1. W oparciu o posiadaną bazę technologiczną i zasoby kadrowe prowadzić samodzielnie dalsze prace rozwojowe posiadanych SI;
2. Dokonać zakupu komercyjnego systemu logistycznego klasy ERP wraz z dedykowanym środowiskiem rozwoju aplikacji, które umożliwi przeprowadzenie prac adaptacyjnych pod kątem potrzeb logistyki SZ RP oraz prowadzenie dalszych prac rozwojowych.

Każde z tych rozwiązań ma swoje wady i zalety.

W pierwszym przypadku konieczne staje się zaangażowanie dużych zespołów projektowo-wdrożeniowych do prowadzenia projektów (wiele platform systemowych, różne technologie realizacji systemów, różne instytucje kierujące), konieczność wspierania technologii już zaniechanych bądź uznanych za nie perspektywiczne. W tym przypadku tempo prac będzie stosunkowo niewielkie z powodu ścisłego związku aplikacji z jej wykonawcami wynikające z braku dedykowanego środowiska rozwoju aplikacji. Wiele istotnych informacji związanych z projektem zostało utraconych z powodu dużej rotacji w zespołach projektowych oraz specyficznych procedur jego dokumentowania. Wobec powyższych przesłanek zbudowanie w pełni zintegrowanego systemu według tego wariantu jest obarczone bardzo dużym ryzykiem odnośnie efektu **finalnego, czasu**

realizacji przedsięwzięcia i związanych z tym nakładów finansowych. Zaletą tego podejścia jest możliwość rozłożenia nakładów finansowych niezbędnych do uzyskania systemu zintegrowanego w dłuższym okresie czasu.

Drugie rozwiązanie pozwala na wejście w posiadanie w pełni zintegrowanego systemu w stosunkowo w krótkim czasie (całe przedsięwzięcie powinno trwać maksymalnie ok. 2 lat). **Bazuje ono na sprawdzonym rozwiązaniu co praktycznie wyklucza ryzyko odnośnie efektu finalnego.** Wymagane są tylko prace adaptacyjne w zakresie parametryzacji i konfiguracji wersji podstawowej systemu. Jednak wybór tego wariantu wiąże się z poniesieniem stosunkowo **dużych nakładów finansowych w stosunkowo krótkim czasie.**

Logistyka SZ RP powinna być obecnie traktowana w ujęciu globalnym gdyż stanowi obecnie ogniwo składowe logistyki NATO tworząc tzw. logistykę wielonarodową (*ang. multinational logistics*). Ma służyć zabezpieczeniu potencjału obronnego Polski ale również operacji międzynarodowych. Wymaga więc systemu organizacyjnego zapewniającego realizację celów ponadnarodowych i systemu informatycznego, który można wykorzystać w globalnych strukturach informacyjnych.

Dla logistyki SZ RP wynikają też wyzwania z realizacji funkcji państwa gospodarza (*ang. HNS-Host Nation Support*) po przyjęciu do struktur NATO. Obecnie już istnieje konieczność prowadzenia sprawozdawczości logistycznej w zunifikowanej formie na potrzeby NATO poprzez coroczne wypełnianie Kwestionariusza Planowania Obronnego (*ang. DPQ-Defense Planing Questionnaire*) co wymaga prowadzenia jednolitego rachunku kosztów wszystkich klas zasobów logistycznych na wszystkich szczeblach kierowania.

Jednak zanim zespoły projektowe przystąpią do realizacji prac implementacyjnych związanych z budową ZSL powinno zapaść szereg istotnych ustaleń. Do najważniejszych należy zaliczyć określenie zasadniczych wymagań jakim ma sprostać logistyka SZ RP i jakie konkretnie zadania i przedsięwzięcia ma zabezpieczać w jakich strukturach organizacyjnych (trwająca restrukturyzacja).

Jednak nawet przybliżone oszacowania zadań do informatycznego zabezpieczenia na odpowiednim poziomie technologicznym determinują koszty budowy ZSL, które należy rozłożyć na okres co najmniej pięciu lat oraz zapewnić dofinansowanie ze źródeł zewnętrznych.

Wnioski i propozycje

Główne kierunki rozwoju SI logistyki SZ RP powinny być skupione na:

- Wyborze wariantu ewolucji SI logistyki SZ RP ;
- Wprowadzeniu jednolitych zasad rachunku kosztów wszystkich zasobów logistycznych na wszystkich szczeblach kierowania;

- Precyzyjnym i sformalizowanym określeniu struktur informacyjnych systemu informowania logistycznego poszczególnych szczebli kierowania logistyką SZ RP;
- Określeniu kryteriów jakie ma spełniać podsystem wsparcia podejmowania decyzji;
- Wypracowaniu procedur planowania potrzeb materiałowych;
- Precyzyjnym określeniu zasad i procedur obowiązujących organa decyzyjne logistyki kooperacyjnej, która jest ogniwem łączącym logistykę producenta i logistykę konsumenta;
- Określeniu wariantu dostępu do globalnej sieci wymiany informacji;
- Ujednoliceniu platform sprzętowo-programowych;
- Stworzeniu wieloszczeblowego, **zintegrowanego systemu logistycznego** (ZSL), w sposób kompleksowy i zunifikowany wspierający procesy logistyczne na wszystkich szczeblach kierowania logistyką SZ RP.

Literatura

Zautomatyzowany System Dowodzenia Wojsk Lądowych (Projekt koncepcyjny).

Wojskowy Przegląd Logistyczny nr 2/99, „Potencjał logistyczny państwa".

Dokumentacja techniczna systemu R3 firmy SAP.

10

10. Komputerowe wspomaganie procesów mobilizacji i uzupełnień w Siłach Zbrojnych RP

kpt. mgr inż. Mirosław Kozak

Wprowadzenie

Budowa komputerowego systemu wspomagania kierowania działalnością mobilizacyjną i uzupełnieniową może być przykładem realizacji wieloszczeblowego systemu informatycznego. Projekt obejmujący cztery poziomy organizacyjne funkcjonowania systemu musiał uwzględniać różne potrzeby użytkowników na każdym z poziomów jak i sposób jego wykorzystania w systemie dowodzenia Sił Zbrojnych RP.

Prace analityczne stosowanych rozwiązań tradycyjnych pozwoliły określić zadania oraz zakres funkcjonalny systemów wspomagania, co umożliwiło w fazie projektowania na szybką realizację poszczególnych modułów systemu mobilizacyjno-uzupełnieniowego. Jednak, by w pełni uświadomić sobie skalę przedsięwzięcia, konieczne jest szczegółowe przybliżenie zadań zarówno systemu mobilizacji, jak i uzupełnień.

Zadaniem systemu mobilizacji i uzupełnień jest usprawnienie planowania i kierowania procesem mobilizacji i uzupełnień - zakładania i prowadzenia aktualnej ewidencji mobilizacyjnej i uzupełnieniowej oraz sporządzania sprawozdań i innych dokumentów bojowych przez organy dowodzenia odpowiedzialne na poszczególnych szczeblach za działalność mobilizacyjno-uzupełnieniową.

Charakterystyka systemu komputerowego wspomagania mobilizacji i uzupełnień

Centrum Informatyki SG WP, przy udziale instytucji merytorycznie odpowiedzialnych za realizowanie procesów mobilizacji i uzupełnień w WP: Zarządu Mobilizacji i Uzupełnień oraz Departamentu Kadr i Szkolnictwa Wojskowego MON, opracowało systemy informatyczne przeznaczone do wspomagania działalności mobilizacyjno-uzupełnieniowej terenowych organów administracji wojskowej.

System mobilizacyjno-uzupełnieniowy zapewnia realizację funkcji: gromadzenia, opracowywania, zobrazowywania, wymiany danych niezbędnych do realizacji wszystkich

zadań i procesów z zakresu problematyki mobilizacyjno-uzupełnieniowej na wszystkich szczeblach kierowania i dowodzenia wojskami lądowymi.

System wspomaga komórki mobilizacyjno-uzupełnieniowe w zakresie:

- Prowadzenia ewidencji podległych jednostek wojskowych;
- Planowania zadań mobilizacyjnych i uzupełnieniowych;
- Kierowania mobilizacyjnym rozwinięciem wojsk;
- Administrowania rezerwami osobowymi i środkami transportu z gospodarki narodowej (zapotrzebowanie i rozdział);
- Prowadzenia ewidencji stanów etatowych i faktycznych obsady osobowej i sprzętu;
- Prowadzenia ewidencji strat bezpowrotnych i warunkowych;
- Oceny ukompletowania wojsk lądowych na poszczególnych szczeblach;
- Uzupełniania posiadanych zasobów poborowymi, żołnierzami rezerwy i środkami transportowymi;
- Tworzenia, przekazywania i przyjmowania dokumentów bojowych, w tym: oceny i analizy rozwoju sytuacji mobilizacyjnej w wojskach lądowych, oceny stanu ukompletowania jednostek rozwijanych mobilizacyjnie oraz przygotowania danych do meldunków i sprawozdań o przebiegu mobilizacji oraz propozycji związanych z zapewnieniem sprawnego kierowania jej przebiegiem;
- Utrzymania współpracy z jednostkami organizacyjnymi administracji państwowej i gospodarki narodowej w zakresie zabezpieczenia mobilizacyjnego rozwinięcia jednostek wojskowych;
- Wykonywania innych zadań wynikających z obowiązujących dyrektyw, zarządzeń, rozkazów oraz instrukcji dotyczącej mobilizacyjnego rozwinięcia wojsk;
- Kontroli wykonywania zadań.

Celem budowy systemu jest:

- Skrócenie czasu obiegu informacji mobilizacyjnych i uzupełnieniowych i zapewnienie wysokiego poziomu aktualności istotnych dla systemu informacji;
- Zapewnienie efektywnego mechanizmu przekazywania danych w ramach stanowisk dowodzenia i między szczeblami w wojskach lądowych;
- Zapewnienie ciągłego i efektywnego gospodarowania zasobami mobilizacyjnymi i uzupełnieniowymi w związku z ponoszonymi stratami;
- Zapewnienie efektywnego przechodzenia z systemu dowodzenia pokojowego na wojenny, w tym efektywnego kierowania procesami związanymi z narastaniem gotowości bojowej oraz mobilizacyjnego rozwijania wojsk;
- Zapewnienie efektywnego nadzoru nad prawidłowym funkcjonowaniem poboru i uzupełniania w wojskach lądowych;

- Zapewnienie warunków organizacyjno-technicznych do efektywnego szkolenia sztabów w zakresie dowodzenia z wykorzystaniem środków i metod automatyzacji;
- Integracja dotychczas niezależnie funkcjonujących systemów informatycznych: kadrowego , mobilizacyjno - uzupełnieniowego, funkcjonującego na szczeblu WKU oraz innych systemów w tym głównie systemów funkcjonujących w gospodarce narodowej.
- Unifikacja systemu na wszystkich szczeblach dowodzenia wojsk lądowych.

System mobilizacji oparty jest na bazach danych przechowywanych na poszczególnych szczeblach dowodzenia w odpowiednich komórkach organizacyjnych odpowiedzialnych za proces mobilizacji wojsk. Część danych potrzebnych do realizacji zadań podsystemu uzupełniania utrzymywana jest w systemach organizacyjno-kadrowych. Dane te dotyczą: stanu etatowego i ewidencyjnego zasobów, strat i braków.

W chwili obecnej systemy te są na etapie eksploatacji użytkowej lub eksploatacji próbnej. W trakcie prac zrealizowano następujące systemy:

System wspomagający działalność WKU w zakresie gospodarki zasobami osobowymi i środkami transportowymi. System ma budowę modularną tzn. wyróżnione są w nim podsystemy realizujące odrębne funkcjonalnie zadania. W skład systemu wchodzą moduły: ewidencji poborowych, ewidencji podoficerów i szeregowych rezerwy, ewidencji i mobilizacji środków transportowych i mobilizacji podoficerów i szeregowych rezerwy.

System do wspomagania prac Sekcji 3 WKU w zakresie ewidencji i administracji zasobami oficerów i chorążych rezerwy oraz wspomagania procesu nadawania przydziałów mobilizacyjnych.

System do wspomagania procesu sprawozdawczości mobilizacyjno-uzupełnieniowej bazując na danych sprawozdawczych wytworzonych przez poszczególne moduły systemów ewidencyjnych.

Do dnia dzisiejszego system został zainstalowany i wdrożony do eksploatacji użytkowej w 20 WKU i RSzW. W każdym z WKU przeprowadzono instalacje oprogramowania systemowego oraz użytkowego oraz przeprowadzono szkolenie użytkowników. Wdrożenia systemów odbywają się w instytucjach, którym udało się przygotować infrastrukturę sieci oraz zakupić niezbędne oprogramowanie narzędziowe i systemowe, co spowodowało duże rozproszenie wdrażanych systemów i nie pozwoliło zamknąć procesem wdrażania określonego jednolitego terenu (np.: wszystkie WKU WARSZAWA).

Wszystkie systemy zaprojektowano przy użyciu nowoczesnego i wysokowydajnego narzędzia jakim jest generator aplikacji MAGIC. Pozwolił on stworzyć systemy w pełni

uniezależnione od sprzętu, bazy danych oraz systemu operacyjnego. Zaprojektowane systemy są systemami konwersacyjnymi, ukierunkowanymi na bezpośrednich użytkowników tj. komórki organizacyjne WKU. Dane podsystemu przechowywane są w bazie danych przechowywanej na twardym dysku komputera centralnego, oraz po zeskładowaniu, na zewnętrznych nośnikach magnetycznych takich jak dyskietki lub taśma magnetyczna. Przetwarzanie w systemie odbywa się w trybie interakcyjnym - każdy użytkownik systemu osobiście uczestniczy w jego użytkowaniu.

Oprogramowanie systemu umożliwia realizację następujących zadań:

- Utrzymywanie słownikowych danych stałych;
- Utrzymywanie opisu cech osobowych;
- Tworzenie i utrzymywanie danych o zapotrzebowaniach;
- Utrzymywanie danych o stanie zasobów - poprzez możliwość przeglądania zestawień z terenowych organów administracji wojskowej;
- Udostępnianie danych aktualizacyjnych dla innych użytkowników (podsystemów) w szczególności systemowi organizacyjno-etatowym.
- Drukowanie zestawień użytkowych - w postaci zapotrzebowań, decyzji uzupełnieniowych oraz zestawień ze stanu zasobów uzupełnieniowych dostarczanych z TOAW (WKU/RSzW/RSzW - na szczeblu korpusu i dowództwa wojsk lądowych);
- Drukowanie zestawień użytkowych: raportów generowanych przez użytkowników systemu według dowolnych kryteriów na podstawie informacji znajdujących się w bazie danych i dokumentów opracowywanych w poszczególnych sekcjach WKU.

System bazuje na aktualnie obowiązujących w WP dokumentach ewidencyjnych i mobilizacyjnych.

Perspektywy rozwoju

Kolejne instalacje i wdrożenia systemów mobilizacyjno - uzupełnieniowych uzależnione są od opracowania przez Zarząd Łączności i Informatyki jednoznacznych wytycznych w zakresie budowy lokalnych sieci komputerowych dla potrzeb WKU i RSzW oraz pozyskania odpowiednich środków na ich realizację. Poważnym ograniczeniem we wdrażaniu tak dużego i rozproszonego systemu jest właśnie brak środków finansowych niezbędnych do szybkiego i całkowitego zamknięcia procesu wdrażania, są to zarówno środki na budowę sieci komputerowych (o czym wspomniałem powyżej), jak i zakup odpowiedniego oprogramowania.

O skali przedsięwzięcia świadczą szacowane ilości potrzeb sprzętowych i programowych dla pozostałych nie skomputeryzowanych WKU i RSzW. W skali WP potrzeby sprzętowo-systemowe wynoszą około130 serwerów z SCO UNIX dla 25 użytkowników, 2500 terminali znakowych, 100 komputerów klasy PC z systemem Windows 95 i około 200 różnych pakietów oprogramowania Magic.

Ocenę funkcjonowania wdrażanych systemów będzie można dokonać po wdrożeniu systemów na obszarze terytorialnie podległym jednemu RSzW albo OW z jednoczesnym zapewnieniem sprawnego przepływu informacji między poszczególnymi instytucjami użytkującymi systemy .

Wnioski

W tym materiale nakreślono zakres informacyjny i zasięg organizacyjny systemów wspomagania procesów mobilizacji i uzupełnień. Nie trzeba nikogo przekonywać, jak ważne miejsce zajmują one w obszarze oddziaływania systemów informatycznych Sił Zbrojnych RP. Bez dostępu do informacji o możliwości uzupełniania strat, bez szybkiego procesu mobilizacji, nie jest dziś możliwe budowanie nowoczesnej, sprawnie działającej armii.

Wdrożenie komputerowego systemu pozwoli na podniesienie stopnia interoperacyjności i kompatybilności z systemami kierowania NATO.

Pozostaje więc postawić pytanie, na jak długi okres można rozłożyć proces wdrażania tego typu systemów, jeśli system jest gotowy i przeszedł już odpowiednie testy u użytkownika.

11

11. System bieżącego wspomagania kierowania instytucją wojskową

ppłk mgr inż. Sylwester Getka

Halina Majchrzyk

Wprowadzenie

W każdej instytucji wojskowej (jednostce organizacyjnej MON) występują trzy podstawowe, niżej wymienione grupy użytkowników systemu:

- Kierownictwo - osoby, które podejmują decyzje w ramach przydzielonych im zasobów ludzkich, materiałowych, finansowych oraz w systemach hierarchicznych w zakresie jednostek (instytucji) podległych służbowo i funkcjonalnie;
- Specjaliści branżowi - osoby, które przygotowują propozycje decyzji w zakresie realizacji zadań statutowych;
- Referenci zabezpieczenia funkcjonowania jednostki (instytucji) - osoby, które realizują zadania związane z procesami informacyjnymi: zaopatrzenia, eksploatacji (sprzedaży), kadrowymi, płacowymi, rozliczeń finansowo-księgowych, magazynowych, bibliotecznych, ewidencji korespondencji, itp..

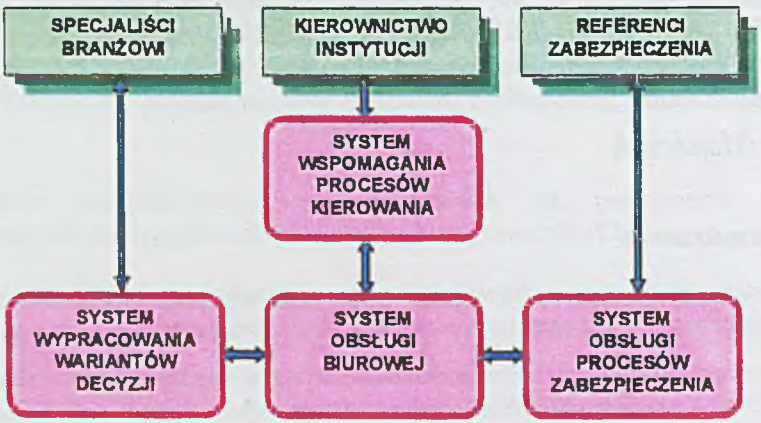
Po dokonaniu szczegółowych analiz zadań realizowanych przez instytucje i jednostki wojskowe można wnioskować, że grupa użytkowników - specjaliści branżowi, ma własne, niepowtarzalne zadania (w stosunku do innych jednostek MON).

Grupę użytkowników - kierownictwo można podzielić, w ramach wojska, na dwie podgrupy: kierownictwo, któremu podlegają hierarchicznie pod względem służbowym i funkcjonalnym instytucje lub jednostki wojskowe niższego szczebla oraz kierownictwo bez takiej podległości.

Grupa użytkowników nazwanych referentami zabezpieczającymi działalność jednostki organizacyjnej MON jest również uzależniona od stopnia samodzielności gospodarczej jednostki. W jednostkach będących oddziałami gospodarczymi tych użytkowników jest więcej i wykonują oni więcej zadań.

Na podstawie tej klasyfikacji, wyłączając użytkowników będących specjalistami branżowymi, należy budować system umożliwiający wspomaganie działalności bieżącej następujących typów jednostek organizacyjnych MON:

- bez jednostek podległych z funkcjami oddziału gospodarczego;
- bez jednostek podległych z funkcjami pododdziału gospodarczego;
- z jednostkami podległymi i z funkcjami oddziału gospodarczego;
- z jednostkami podległymi i z funkcjami pododdziału gospodarczego.



Rys. 31 Ogólna struktura użytkowania systemu w jednostce organizacyjnej MON.

Podstawą opracowania systemu bieżącego wspomagania kierowania instytucją wojskową są decyzje podejmowane przez kierownictwo. Decyzje podstawowe podejmowane są w następujących formach:

- Rozkaz dzienny;
- Plan przedsięwzięć danej jednostki organizacyjnej;
- Plan przedsięwzięć jednostek organizacyjnych podległych;
- Dekretacja i akceptacja dokumentów.

Propozycje tych decyzji przedstawiane są przez kierowników komórek organizacyjnych, specjalistów oraz referentów. Kolejnym, istotnym elementem dla kierownictwa jest zasada sprzężenia zwrotnego, czyli informowanie o stanie realizacji podjętych decyzji i stanie obiektów będących przedmiotem kierowania w danej jednostce organizacyjnej MON i ewentualnie jej jednostek podległych.

Ze względu na bardzo szeroki zakres zadań, które powinien wspomagać taki system trudno jest przedstawić uniwersalną koncepcję zadowalającą wszystkich potencjalnych użytkowników.

Stan aktualny

System bieżącego wspomagania kierowania instytucją wojskową, jednostką organizacyjną MON, posiadającą samodzielny etat, pieczęć herbową i ustalony zakres zadań statutowych, umożliwia udostępnianie kierownictwu wszechstronnej, dokładnej i aktualnej informacji ułatwiającej podejmowanie decyzji i skuteczne wykonywanie funkcji planistycznych, kontrolnych i operacyjnych.

Kancelaria jest podstawowym elementem funkcjonalnym w systemie, spełniającym funkcje ewidencjonowania, przechowywania i udostępniania dokumentów uprawnionym użytkowników. Przechowuje ona i udostępnia dokumenty zaewidencjonowane w roku bieżącym oraz dokumenty z lat poprzednich. Spełnia następujące funkcje:

- Ewidencjonuje wszystkie dokumenty wchodzące, wychodzące i wewnętrzne,
- Przekazuje dokumenty wchodzące do szefa instytucji, celem zapoznania się i dokonania dekretacji i przydzielenia dysponenta dokumentu,
- Dokonuje aktualizacji ewidencji dokumentu po dokonaniu dekretacji przez szefa instytucji i informuje zainteresowanych użytkowników o dekretacji szefa instytucji,
- Dokonuje obsługi procesu wypożyczenia i zwrotu dokumentów,
- Dokonuje obsługi procesu wysyłania do adresatów dokumentów wychodzących z instytucji,
- Dokonuje kontroli terminowości zwrotu przez użytkowników wypożyczonych dokumentów,
- Przygotowuje wykazy i protokoły dla potrzeb przeprowadzenia kontroli kwartalnych i rocznych przechowywania i obiegu dokumentów u wszystkich użytkowników posiadających i wytwarzających dokumenty,
- Przekazuje dokumenty, po zakończeniu roku kalendarzowego, do zbioru zasobów dokumentów (biblioteki) oraz przygotowuje i przekazuje dokumenty do archiwum państwowego (resortowego, okręgowego itp.).

Z systemem tym powiązane są elementy zewnętrzne, do których należą poczta, archiwum i instytucje zewnętrzne, będące adresatami i nadawcami dokumentów.

Poczta spełnia funkcje usługowe w zakresie telefaksów, przyjmowania i przekazywania przesyłek pocztowych.

Archiwum (państwowe, resortowe) współpracuje z systemem okresowo. Do archiwum przekazywane są dokumenty własne, o wieczystym okresie przechowywania, które nie są już wykorzystywane w bieżącej działalności instytucji, a w przypadku likwidacji instytucji do archiwum przekazywane są wszystkie dokumenty.

Instytucje zewnętrzne są adresatami i nadawcami dokumentów kierowanych do instytucji.

Projekt usprawnienia systemu kierowania

Celem informatyzacji instytucji wojskowej jest zastąpienie tradycyjnego systemu ewidencyjnego informatycznym systemem ewidencyjno-sprawozdawczym oraz komputerowe wspomaganie prac sztabowo-biurowych. Na obecnym etapie przyjęto koncepcję budowy jednoszczeblowego, autonomicznego systemu dla każdej jednostki organizacyjnej MON, obejmującego jej kierownictwo i wszystkie komórki organizacyjne. Powinno to znacznie uprościć jego konstrukcję oraz sposób wymiany danych.

Celem budowy systemu jest:

- Skrócenie czasu, usprawnienie i sformalizowanie obiegu informacji przy równoczesnym odciążeniu personelu od czasochłonnego i mało efektywnego ręcznego wyszukiwania informacji z różnych źródeł,
- Automatyzacja procesu przechowywania i udostępniania dokumentów archiwalnych,
- Usprawnienie i przyspieszenie realizacji prac sztabowo-biurowych,
- Usprawnienie procesu wydawniczego.

Podstawowe zadania każdej jednostki organizacyjnej MON obejmują: zadania statutowe (wynikające z zakresu obowiązków) oraz zadania rutynowe (typowe dla profilu działania każdego biura). Komputerowe wspomaganie realizacji zadań statutowych będzie miało charakter automatyzacji procesów związanych z gromadzeniem, wyszukiwaniem i udostępnianiem danych niezbędnych do realizacji tych zadań. Druga grupa zadań realizowanych przez system dotyczy wspomagania prac sztabowo-biurowych.

System bieżącego wspomagania kierowania instytucją

W związku z zadaniami realizowanymi w każdej instytucji system został podzielony na trzy podsystemy: obsługi biurowej, obiegu dokumentów i zarządzania instytucją. Każdy z nich może funkcjonować niezależnie lub współpracować ze sobą umożliwiając sprawne kierowanie i funkcjonowanie instytucji wojskowej. W każdej instytucji można wyróżnić dwa rodzaje obiegu informacji. Jeden dotyczy obiegu dokumentów, a drugi obiegu informacji związanej z bieżącym funkcjonowaniem instytucji.

Każdy z podsystemów tego systemu może być wdrażany i eksploatowany autonomicznie. Pełny efekt funkcjonalny uzyskuje się jednak po wdrożeniu całego systemu. Podsystem obsługi biurowej i obiegu dokumentów może współdziałać z instytucjami zewnętrznymi przy wykorzystaniu poczty elektronicznej, sieci Internet i usług telefaksowych, zaś pozyskane dokumenty mogą być bezpośrednio udostępniane użytkownikom w tych podsystemach. Przetwarzanie danych zorganizowane jest w technologii pracy grupowej, tak aby poszczególni użytkownicy mogli korzystać ze wspólnych zasobów (w ramach posiadanych uprawnień nadanych im przez administratora systemu) oraz wymieniać informacje pomiędzy sobą.

Podsystem obsługi biurowej zapewnia komunikację pomiędzy wszystkimi użytkownikami systemu poprzez realizację funkcji poczty elektronicznej i wspomaganie w zakresie innych usług typu biurowego. Funkcje realizowane w nim przenikają się wzajemnie z funkcjami podsystemu obiegu dokumentów (informacji). W dużym stopniu podsystem ten jest źródłem powstawania informacji lub dokumentów (edytor tekstu), które są później przekazane i przetwarzane w podsystemie obiegu dokumentów. Podsystem zapewnia możliwość korzystania z zewnętrznej **poczty elektronicznej** oraz sieci **Internet**.

Podsystem ten będzie elementem zapewniającym prawidłowe funkcjonowanie instytucji w zakresie zadań ogólnych. Funkcje te w tradycyjnych systemach spełniają sekretariaty i obsługa administracyjna. W nowoczesnych systemach wykorzystywane są tzw. pakiety biurowe, które funkcjonują w systemie sieci komputerowej. Pakiety te wspomagają obsługę procesów biurowych za pomocą funkcji poczty elektronicznej, harmonogramowania czasu pracy, prowadzenie notatników, ewidencji kontrahentów, edytorów tekstowych i graficznych, telekonferencji i innych funkcji pomocnych w pracy biurowej.

Realizacja zadań związanych z obsługą biurową w systemie odbywa się przy wykorzystaniu wbudowanych możliwości pakietu Lotus Notes. Zalicza się do nich graficzny edytor tekstu, pocztę elektroniczną, systemowe mechanizmy wymiany danych OLE, OLE2 i DDE.

Podsystem obiegu dokumentów jest specyficznym elementem systemu wspomagania kierowania instytucją wojskową. Wydzielenie takiego podsystemu było możliwe dzięki zastosowaniu narzędzia Lotus Notes, które w łatwy sposób umożliwia realizację funkcji obiegu informacji (dokumentów).

Dokumenty są podstawą formalno-prawną funkcjonowania instytucji. Odzwierciedlają jej działanie i współdziałanie z innymi instytucjami. Każdy dokument musi zawierać adresata, nadawcę, datę jego wytworzenia, treść dokumentu oraz podpis szefa instytucji lub osoby przez niego upoważnionej. Dokumenty, pod względem ich wytworzenia i adresata, dzielą się na: zewnętrzne obce - wchodzące do instytucji, zewnętrzne własne - wysyłane z instytucji, i wewnętrzne - wykorzystywane we własnej instytucji.

W podsystemie obiegu dokumentów użytkownicy i wykonawcy realizują zadania wynikające z treści dokumentów lub dekretacji na nich, a także opracowują projekty nowych dokumentów i dokonują niezbędnych uzgodnień z innymi zainteresowanymi osobami tworzącymi ten dokument. Wykonawca dokumentu odpowiada za treść merytoryczną, stopień poufności i kategorię archiwalną dokumentu. Dokumenty, z punktu widzenia dostępności, dzielą się na ogólnodostępne i dedykowane określonym użytkownikom.

Podsystem jest przeznaczony dla jednej instytucji, z centralną organizacją ewidencji dokumentów. Zapewni realizację wszystkich czynności procesu obiegu dokumentów od momentu wytworzenia lub rejestracji do chwili zniszczenia lub przekazania do archiwum. Zawiera dane o historii wykorzystywania dokumentu przez użytkowników w całym tym okresie. Ważną rolę w tym podsystemie, szczególnie w zakresie funkcji ewidencyjnych, pełni moduł Kancelaria, który jednocześnie jest częścią składową podsystemu zarządzania instytucją.

Zaewidencjonowane dokumenty przydzielane są głównym adresatom (dysponentom) przez szefa instytucji. Są oni głównymi dysponentami tych dokumentów. Użytkownikami systemu są wszyscy ci, którzy uczestniczą w procesie obiegu dokumentów, a w szczególności kadra kierownicza i te osoby, do których kierowane są przez dysponentów dokumenty. Rozpoczęcie każdego roku kalendarzowego odbywa się czynnością przeniesienia danych z rejestru roku zakończonego do zbioru ewidencji zasobów dokumentów instytucji.

Te dwa podsystemy ze względu na realizowane w nich funkcje mogą obejmować całą instytucję lub poszczególnych użytkowników w ramach jednej konkretnej komórki organizacyjnej.

Podsystem zarządzania instytucją przeznaczony jest dla potrzeb bieżącego kierowania instytucją przez jej szefa, kierowników komórek organizacyjnych dla potrzeb kierowania działalnością tych komórek oraz personelu administracyjnego dla realizacji procedur obsługi zabezpieczenia działalności instytucji. Został on podzielony na moduły, które są przeznaczone do eksploatacji w poszczególnych komórkach organizacyjnych.

W podsystemie tym podejmowane są decyzje dotyczące realizacji zadań i wykorzystania przydzielonych zasobów osobowych, finansowych i materiałowych. Decyzje podejmowane są w formie poleceń, dokumentów, planów i rozkazu dziennego, będącego dokumentem archiwalnym, sformalizowanym i obligatoryjnym, w którym zawarte są podstawowe decyzje szefa (dowódcy) dotyczące działalności instytucji (JW).

System wspomagania kierowania instytucją wojskową jest zaprojektowany w technologii Lotus Notes, który to produkt **nie jest systemem zarządzania relacyjną bazą danych**. Konsekwencją tego faktu jest to, że dane utrzymywane w tym systemie nie są zorganizowane w postaci konkretnych tabel, czyli zbiorów danych, składających się na bazę danych w sposób tradycyjny, ale w postaci formularzy ekranowych, obejmujących wiele pól zawierających konkretne informacje. Poszczególne formularze powiązane ze sobą i pogrupowane tematycznie stanowią bazę danych w rozumieniu Lotus Notes, często nazywaną bazą dokumentów. Odpowiedzialnym za użytkowanie i eksploatację systemu jest administrator systemu. Powiązanie z innymi systemami i instytucjami realizowane jest poprzez zbiory słownikowe, zapewniające spójność semantyczną oraz środki techniczne umożliwiające przekazywanie dokumentów i innych informacji za pomocą poczty elektronicznej, telefaksu i Internetu.

System przeznaczony jest dla kierownictwa instytucji, kierowników wszystkich komórek organizacyjnych oraz pracowników komórek zabezpieczających bieżącą działalność instytucji. System jest użytkowany codziennie w czasie godzin pracy. Jest on systemem wielodostępnym eksploatowanym w oparciu o punkt informatyczny oraz punkty abonenckie usytuowane w miejscach pracy potencjalnych użytkowników danej instytucji. Punkt informatyczny jest wyodrębnioną komórką, której zadaniem jest zapewnienie technicznej i funkcjonalnej sprawności eksploatacji SI. Jest to system konwersacyjny, zapewniający bezpośredni dostęp do zasobów komputera jednocześnie wielu użytkownikom pracującym w różnych miejscach.

Z punktu widzenia użytkownika istotne jest aby jednoznacznie przydzielono mu odpowiedni zestaw danych, które będzie mógł wykorzystywać oraz odpowiedni zestaw narzędzi programowych, których będzie używał w swojej codziennej pracy. Przydzielenie to realizowane jest przez przypisanie każdemu użytkownikowi odpowiednich uprawnień umożliwiających wykonywanie zadań. Użytkownikami systemu są tylko te osoby, które zostały zarejestrowane przez administratora systemu i nadane zostały im przez niego uprawnienia do korzystania z określonych funkcji i zbiorów poszczególnych podsystemów.

Szef instytucji (dowódca) reprezentuje ją na zewnątrz i kieruje całokształtem jej działalności poprzez swoich zastępców, którzy działają w jego imieniu w zakresie określonych dziedzin działalności oraz poprzez kierowników komórek organizacyjnych.. Jest on również głównym dysponentem dokumentów i wszystkich przydzielonych dla instytucji zasobów. W systemie spełnia również funkcję rozdziału korespondencji (dokumentów) wraz z dekretacją dla poszczególnych dysponentów dokumentu lub użytkowników tych dokumentów.

Użytkownicy i wykonawcy dokumentów realizują zadania wynikające z dokumentów oraz opracowują projekty nowych dokumentów i dokonują niezbędnych uzgodnień z innymi zainteresowanymi tworzonym dokumentem. Po podpisaniu projektu dokumentu przez szefa lub upoważnioną osobę, projekt dokumentu staje się obowiązującym. Wykonawca dokumentu odpowiada za treść merytoryczną, stopień poufności i kategorię archiwalną dokumentu.

Sekretariat (sekretariaty) w instytucji spełnia funkcje zabezpieczenia bieżącej działalności szefa (szefów) instytucji oraz zapewnia komunikację pomiędzy szefem a podległymi mu komórkami (innymi sekretariatami) w zakresie przekazywania poleceń i przyjmowania od tych komórek informacji dla szefa. Z sekretariatem współdziała kancelaria i administracja instytucji, której głównym zadaniem jest zabezpieczenie administracyjne bieżącego działania instytucji.

Kierownicy komórek organizacyjnych podejmują decyzje w ramach przydzielonych kompetencji, przedstawiają propozycje decyzji i dokumentów dla szefa instytucji (dowódcy) oraz realizują, poprzez swoich podwładnych, zadania określone dla

danej komórki. Szefowie komórek organizacyjnych są zarazem dysponentami dokumentów, którzy udostępniają dokumenty podwładnym, celem wykonania zadań wynikających z tych dokumentów.

Administrator systemu odpowiedzialny jest za bezpieczeństwo, poprawność użytkowania i eksploatacji systemu oraz za spójność semantyczną tego systemu z systemami eksploatowanymi w resorcie obrony narodowej. Do wypełnienia tej funkcji administrator wykorzystuje odpowiednie oprogramowanie systemowe i moduły słownikowe (pomocnicze) podsystemów tego systemu.

Administrator systemu zakłada wszystkim użytkownikom pliki identyfikacyjne (plik ID) umożliwiające logowanie się do systemu, a następnie nadaje im uprawnienia do realizacji zadań wynikających z ich obowiązków. Z punktu widzenia kierowania instytucją system informatyczny należy widzieć jako narzędzie zapewniające komputerową realizację ściśle określonych funkcji dotyczących w sensie ogólnym zarządzenia instytucją.

Pojedyncza funkcja (zadanie) ma ustalony algorytm realizacji, opiera się na ustalonym zestawie danych udostępnianych i aktualizowanych w komputerowej ewidencji. Wszystkie elementy przetwarzania będą realizowane siłami i sprzętem instytucji zarówno w fazie wdrażania systemu (tworzenie słowników, przenoszenie danych z ewidencji tradycyjnej) jak i stałej eksploatacji systemu (wprowadzanie danych na bieżąco, aktualizacja zbiorów, rozprowadzanie wyników).

Zastosowane procedury realizacji zadań mają wbudowany mechanizm kontroli, umożliwiający sprawdzanie spełnienia wymogów, wynikających z przepisów oraz sprawdzania możliwości zrealizowania danego zamierzenia, ze względu na posiadane zasoby materiałowe, finansowe, osobowe, etatowe itp. Dokumenty wejściowe i wynikowe odpowiadają formie i treści obowiązujących dokumentów.

Wnioski

Zaprojektowany system jest systemem uniwersalnym, powielanym dla wszystkich instytucji wojskowych typu departament, zarząd, szefostwo, sztab, jednostka wojskowa, instytut itp. Pomimo wykonywania przez te instytucje, w zakresie ogólnym, tych samych zadań, to w każdej z tych instytucji występują różne akcenty i ważność niektórych z tych zadań. Z tego też względu system ten należy w pierwszym etapie wdrożyć eksperymentalnie w czterech typach instytucji: departamencie ministerstwa, zarządzie SG, jednostce wojskowej i w Centrum Informatyki SG WP. Po uzyskaniu uwag i wniosków, a także przeszkoleniu użytkowników, wprowadzić udoskonalenie systemu, tworząc pakiet programowy, stanowiący podstawę generowania wersji systemu, odpowiadającego potrzebom danej instytucji.

Zastosowane procedury w rozwiązaniach projektowych, generalnie rzecz biorąc są zgodne z obowiązującymi przepisami. Z tego też względu niektóre czynności muszą być powielane również metodą tradycyjną. Przykładem może być dokument rozkazu

dziennego, który do bieżącej działalności jest w pełni wystarczający i przydatny, to jednak zgodnie z obowiązującymi przepisami musi być drukowany, rejestrowany i przechowywany w kancelarii w formie dokumentu papierowego. Nie wystarczający jest też podpis elektroniczny wypożyczenia dokumentu z kancelarii, ale musi być dokonany podpis na specjalnych dokumentach ewidencyjnych w kancelarii. Wdrożenie tego systemu przyczyni się do wypracowania nowych zasad funkcjonowania instytucji z zastosowaniem technik informatycznych.

Wdrożony system powinien usprawnić pracę jednostek organizacyjnych MON we wszystkich podstawowych obszarach ich działalności oraz przyczynić się do uzyskania następujących efektów:

- Przyspieszenie i lepszy nadzór nad realizacją poleceń w stosunku do osób funkcyjnych i komórek organizacyjnych;
- Wprowadzenie nowoczesnych metod organizacji pracy komórek organizacyjnych dzięki zastosowaniu elektronicznego systemu biurowego;
- Dostęp do kompletnych i zintegrowanych danych dla wielu różnych grup użytkowników, niezbędnych w ich codziennej pracy;
- Zastosowanie oficjalnego obiegu dokumentów w postaci elektronicznej, wraz z możliwością jego kontroli;
- Szybki dostęp do różnorodnych informacji, zgromadzonych w jednym miejscu;
- Wysoki poziom ochrony danych przed nieupoważnionym dostępem.

Literatura

System wspomagania kierowania instytucją wojskową – Projekt koncepcyjny, Centrum Informatyki Sztabu Generalnego WP 1997 r.,

Wielodostępny system wspomagania działalności bieżącej jednostek organizacyjnych MON – moduł sekretariat – Projekt koncepcyjny, Centrum Informatyki Sztabu Generalnego WP 1998 r.,

James A.F. Stoner, R. Edward Freeman, Daniel R. Gilbert, jr., Kierowanie – Wyd. II zmienione, Polskie Wydawnictwo Ekonomiczne, Warszawa 1997 r.

12

12. System bieżącego monitorowania gotowości operacyjnej SZ RP

ppłk mgr inż. Karol Krzyżanek

ppłk mgr inż. Grzegorz Pokorski

kpt. mgr inż. Grzegorz Sobiech

Wprowadzenie

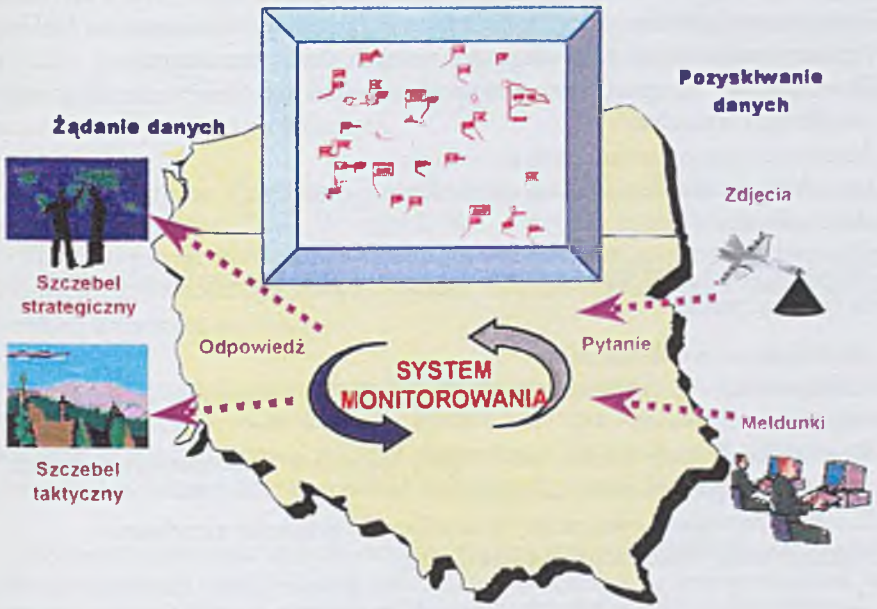
Współczesne pole walki charakteryzuje się znaczną dynamiką działań bojowych, która wymusza skracanie czasu reakcji systemu dowodzenia wojskami na zaistniałe zdarzenia. Zwiększenie operatywności sztabów jest możliwe między innymi poprzez wprowadzenie metod i środków informatycznych do procesów pozyskiwania informacji przez organy dowódczo-sztabowe oraz do organizacji i sterowania procesami obiegu informacji w czasie prowadzenia operacji.

Automatyzacja zadań wykonywanych w komórkach funkcjonalnych poszczególnych szczebli dowodzenia w cyklu dowodzenia, planowania, organizowania i prowadzenia działań bojowych, pozwoli na znaczne podniesienie jakości i operatywności systemu dowodzenia.

Wojska lądowe nie posiadają obecnie kompleksowego systemu informatycznego, który umożliwiałby śledzenie, analizowanie i przedstawianie w dogodnej postaci (np. tabela, opis, mapa) bieżącego stanu operacyjnego sił zbrojnych (własnych bądź obcych). Działające już w wojsku systemy informatyczne zajmują się zbieraniem i przetwarzaniem informacji w wąskim zakresie - brak jest systemu dającego pełny obraz gotowości bojowej (ukompletowania, położenia i aktywności jednostek wojskowych w określonym czasie i miejscu). Próbą budowy takiego systemu jest projektowany w CI SG WP Zautomatyzowany System Dowodzenia szczebla operacyjnego i taktycznego. Jak na razie informacje te są zbierane, przesyłane i opracowywane metodami tradycyjnymi, w postaci meldunków i sprawozdań przekazywanych telefonicznie, bądź faksem między odpowiednimi służbami.

Ocena gotowości operacyjnej SZ opiera się na danych pozyskanych za pośrednictwem dyżurnych służb operacyjnych oraz jednostek rozpoznania (Rys. 32). Ze

względu na dużą ilość informacji spływających każdego dnia do dyżurnej służby operacyjnej oraz wojsk rozpoznania i walki radioelektronicznej (RiWRE), dużej wagi nabiera nie tylko odpowiednia agregacja dostarczanych danych, ale też przedstawienie ich w postaci dogodnej dla dowódców i sztabów wojskowych.



Rys. 32 System monitorowania gotowości operacyjnej

Dyżurna służba operacyjna

DSO realizuje zadania związane ze specyfiką działania służb operacyjnych. Obejmują one zagadnienia związane ze zbieraniem i przechowywaniem informacji, formułowaniem i przekazywaniem sprawozdań w postaci sformalizowanej i niesformalizowanej.

Do podstawowych funkcji DSO należą:

- Pozyskiwanie informacji o sytuacji operacyjnej SZ RP;
- Gromadzenie informacji na temat sił i środków oraz dyslokacji wojsk wydzielonych do wykonywania określanych zadań;
- Zbieranie informacji o najważniejszych przedsięwzięciach wykonywanych w SZ.

DSO zostanie wyposażona w SI o strukturze wielostanowiskowej, rozproszonej przestrzennie, obejmującej szczeble: operacyjny, operacyjno-taktyczny i taktyczny. DSO wyposażone będą w zautomatyzowane stanowiska pracy, zainstalowane w ogniwach

struktury wojsk lądowych i połączone ze sobą systemem telekomunikacyjnym. System informatyczny, wspomagający pracę DSO, będzie umożliwiał:

- Edycję zbieranych informacji (sprawozdań);
- Wspomaganie prac analitycznych;
- Zapewnienie łączności współdziałania z instytucjami współdziałającymi z DSO;
- Przekazywanie poleceń do podległych dyżurnych służb operacyjnych;
- Dokonywanie wstępnej selekcji i prezentację dostarczanej informacji wg określonych kryteriów;
- Archiwizowanie przetwarzanych informacji;
- Umożliwienie wielokierunkowej łączności w pionie DSO za pomocą poczty elektronicznej.

Skrócenie czasu przebiegu procesów informacyjnych dyżurnych służb operacyjnych można osiągnąć przez:

- Sformalizowanie dokumentów;
- Automatyzację gromadzenia, wyszukiwania i przetwarzania informacji z rozproszonych źródeł;
- Wprowadzenie bazy danych, zawierającej informacje zabezpieczające bieżącą pracę poszczególnych osób funkcyjnych;
- Zautomatyzowanie funkcji przesyłania informacji pomiędzy szczeblami;
- Automatyzację funkcji zobrazowania danych.

Zasadniczymi źródłami informacji są służby dyżurne brygad i służby operacyjne dywizji. Za pomocą utajnionej sieci łączności przekazują dane (sprawozdania, meldunki, komunikaty) w formie sformalizowanych dokumentów bojowych. Możliwe jest również przekazywanie dokumentów niesformalizowanych, w tym graficznych (mapy, zdjęcia), multimedialnych (dźwięk, obraz ruchomy) i wszystkich innych reprezentowanych w postaci elektronicznej. Dodatkowymi źródłami informacji dla DSO są instytucje resortu ON oraz administracji państwowej, posiadające wiadomości przydatne w wykonywaniu zadań służb operacyjnych.

System musi być zasilany danymi z istniejących już systemów informatycznych SZ RP oraz z nowo projektowanych i wdrażanych systemów.

Z eksploatowanych obecnie systemów informatycznych będą pozyskiwane dane o:

- Siłach i środkach rozpoznania SZ własnych oraz państw obcych;
- Przedsięwzięciach szkoleniowych;
- Stanie sił i środków, strukturach etatowych, bojowych SZ;
- Mobilizowanych siłach i środkach SZ;
- Siłach i środkach transportowych, stanie dróg i lotnisk;
- Skażeniach;
- Zasobach łączy i traktów dzierżawionych, rezerwowych i planowanych przeznaczonych dla SZ;

- Obsadzie personalnej kierowniczych stanowisk w SZ.

Na początku 1997 r. uruchomiono nitkę pilotową systemu teleinformatycznego Dyżurnej Służby Operacyjnej SZ RP, obejmującą DSO Sztabu Generalnego, okręgów wojskowych, 1 DZ (wraz z podległymi brygadami) i 6 BDSz. Celem przedsięwzięcia było zapoznanie użytkowników z pracą systemu zbudowanego w technologii pracy grupowej, weryfikacja przyjętych rozwiązań oraz wyznaczenie kierunków dalszej pracy nad systemem. W ten sposób powstał projekt koncepcyjny systemu, obejmujący zakres zagadnień ujęty w zadaniu projektowym.

Zbierane w trakcie eksploatacji doświadczenia pozwoliły dokonać wielu zmian w funkcjonowaniu systemu DSO. W ciągu 1998 r. rozwijano oprogramowanie użytkowe, modyfikowano projekt koncepcyjny systemu, skonstruowano rozproszoną hierarchiczną bazę danych odzwierciedlającą strukturę dyżurnych służb operacyjnych. Zmieniono także architekturę techniczną systemu.

Na szczeblu centralnym użytkowane jest oprogramowanie tworzenia sprawozdań dobowych i tygodniowych, w dalszej kolejności udostępnione będą funkcje tworzenia meldunków dyżurnych łączności OW i operacyjnego łączności oraz wstawka oficera operacyjnego mobilizacji do sprawozdania dobowego na szczeblu centralnym.

Oprogramowanie, oraz sposób skonfigurowania systemu, umożliwia rozwinięcie go na dowolną strukturę wojsk, oferując prócz zadań związanych ze sprawozdaniami, także możliwość przesyłania dowolnych informacji (tekst, obraz, dźwięk) i poczty elektronicznej. Oprogramowanie i użyte narzędzia są wystarczająco elastyczne i nie stanowi problemu dopasowanie systemu do nowej struktury Sił Zbrojnych -.

Niedostatek sprzętu komputerowego i ochronnego, a także ograniczona infrastruktura utajnionej sieci transmisji danych, ograniczają postęp w rozszerzeniu nitki pilotowej na pozostałe jednostki wojsk lądowych i użytkowe wdrożenie systemu.

W dalszych pracach nad systemem przewiduje się budowę bazy dokumentów i bazy danych podstawowych szczebli dowodzenia oraz budowę interfejsu komunikacji zewnętrznej. Interfejs komunikacji zewnętrznej to pakiet programów służących do wymiany informacji pomiędzy systemem a otoczeniem, w tym dających możliwość udostępniania danych osobom funkcyjnym Sztabu Generalnego i Ministerstwa Obrony Narodowej. W chwili obecnej wszystkie informacje dotyczące np. struktury, dyslokacji, zadań jednostek, zasobów łączności, meldunki i inne przechowywane są w postaci papierowej, bądź uzyskiwane drogą telefoniczną ze źródeł. W przyszłości będą pozyskiwane z rozproszonej bazy danych. W tym celu należy jednak przeprowadzić szereg przedsięwzięć organizacyjnych i technicznych, np. określić zakresu i postać potrzebnych informacji, uruchomić utajnioną sieci wymiany danych obejmującej miejsca fizycznego przechowywania danych, uzgodnić tryb udostępniania danych, a także stworzyć warunki nieprzerwanej pracy sprzętu (np. instalacje ppoż., zasilanie awaryjne).

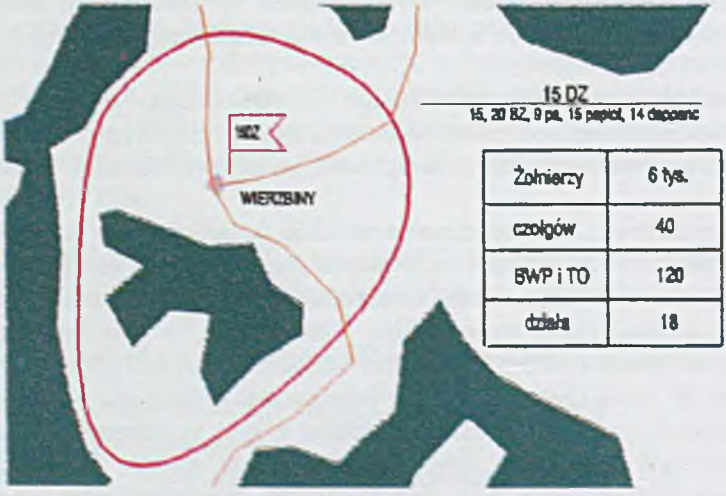
Informacje niedostępne przez sieć i nie ulegające szybkiej dezaktualizacji, będą przechowywane w postaci elektronicznej w DSO.

Wojska RiWRE

W skład zintegrowanego systemu rozpoznania (ZSR) wchodzi wielostanowiskowy, rozproszony system informatyczny wspomagający realizację zadań bojowo-rozpoznawczych. Wielostanowiskowość i rozproszenie przestrzenne uwarunkowane jest liczebnością oraz dyslokacją ogniw struktury organizacyjnej tego systemu.

Mikrokomputerowy system wspomagania bieżącej pracy bojowo-rozpoznawczej ma realizować wymagane zadania poprzez automatyzację procesów:

- Zbierania, przetwarzania i składowania informacji z prowadzonego rozpoznania;
- Opracowywania i przesyłania na stanowisko koordynacji ZSR nakazanych i doraźnych meldunków z prowadzonego rozpoznania przez wydzielone jednostki;
- Archiwizowania zdobytych informacji rozpoznawczych (opracowanych dokumentów) we wszystkich jednostkach wydzielonych do systemu;
- Odbioru i składowania informacji napływającej do stanowiska koordynacji;
- Opracowywania dokumentów bojowych oraz przesyłania ich do określonych adresatów;
- Okresowe archiwizowanie dokumentów oraz bazy danych;
- Wspomagania optymalnego wykorzystania sił i środków rozpoznawczych SZ RP działających w ramach ZSR.



Rys. 33 Powiązanie grafiki z danymi z rozpoznania

Funkcjonowanie systemu (zbieranie, przesyłanie informacji) oparto na sformalizowanych dokumentach bojowych. Istnieje możliwość wprowadzenia do

systemu informacji z dokumentów niesformalizowanych np. tekst niesformalizowany, mapy (Rys. 33), zdjęcia itp.

System umożliwia wykorzystywanie raz wprowadzonych danych wszędzie tam, gdzie jest to niezbędne.

Wprowadzenie narzędzi informatycznych do systemu rozpoznania pozwoli na:

- Przyspieszenie procesu zbierania, przetwarzania i obiegu bieżącej informacji rozpoznawczej wewnątrz ZSR
- Przyspieszenie przesyłania informacji do odbiorców zewnętrznych;
- Usprawnienie oraz przyspieszenie procesów opracowywania dokumentów bojowych;
- Usprawnienie procesów archiwizacji informacji bojowych przechowywanych w bazie danych;
- Usprawnienie wyszukiwania informacji w zbiorach archiwalnych;
- Usprawnienie planowania i koordynacji w zakresie wykorzystania sił i środków rozpoznawczych w bieżącej działalności bojowej;
- Usprawnienie pracochłonnego procesu graficznego opracowywania dokumentów bojowych i sprawozdawczych.

W chwili obecnej system jest w fazie testowania przed wdrożeniem w jednostkach rozpoznawczych i na SK ZSR. Oprogramowanie umożliwia m.in. formatowanie i automatyczne przesyłanie meldunków, utrzymanie wielopoziomowej bazy meldunków, wyszukiwanie informacji, archiwizowanie bazy i zarządzanie archiwum. Składane przez jednostki rozpoznawcze meldunki przechowywane są w postaci podzielonych na fragmenty cząstek ocechowanych tzw. kodami tematycznymi - indeksami pozwalającymi na wyszukiwanie opisów zdarzeń spełniających zadane warunki. Kody tematyczne opracowywane są na szczeblu centralnym i podlegają automatycznej dystrybucji w systemie. Jest gotowe również oprogramowanie tworzenia meldunku dziennego dla DSO SZ RP.

W obecnej postaci system przede wszystkim usprawnia funkcjonowanie stanowiska koordynacji ZSR. Następnym krokiem będzie zautomatyzowanie tworzenia meldunków bojowych przez oficera dyżurnego jednostki rozpoznawczej. Nastąpi to poprzez zmodyfikowanie i dostosowanie do potrzeb systemu używanego w jednostkach rozpoznawczych oprogramowania wspomagającego pracę grup analizy danych.

W dalszej kolejności przewiduje się również że system będzie mógł dostarczać informacje do odpowiednich systemów armii sojuszniczych NATO.

Rozwiązania

Zarówno w DSO jak i jednostkach rozpoznawczych jako platformę programową zastosowano pakiet pracy grupowej Lotus Notes. Najważniejszymi elementami

systemu są edytor dokumentów tekstowych i edytor dokumentów graficznych. Zastosowanie Lotus Notes pozwoliło zbudować wieloszczeblowy system przepływu sformalizowanych dokumentów pomiędzy ściśle określonymi komórkami i osobami funkcyjnymi. Lotus Notes dysponuje wieloma cechami i funkcjami, które są istotne ze względu na bezpieczeństwo i niezawodność pracy, łatwość i elastyczność tworzenia i dystrybucji oprogramowania oraz wykorzystanie istniejącej infrastruktury teleinformatycznej. Do najważniejszych zalet Lotus Notes należy zaliczyć:

- Dostępność na wszystkich stosowane w SZ platformach sprzętowych;
- Wysoki poziom zabezpieczenia danych (kontrola dostępu i szyfrowanie danych);
- Możliwość stworzenia hierarchicznej struktury użytkowników (przesyłanie informacji w określonych relacjach);
- Poczta elektroniczna (przesyłanie informacji w dowolnych relacjach);
- Wielokierunkowa, selektywna replikacja danych na poziomie pola;
- Możliwość tworzenia zaawansowanych aplikacji realizujących złożone funkcje;
- Dostęp do każdej relacyjnej bazy danych przy pomocy wytworzonej aplikacji lub oddzielnego pakietu Notes Pump;
- Możliwość posługiwania się dokumentami sformalizowanymi (replikacja dotyczy wówczas tylko zmian w polach dokumentu);
- Możliwość współpracy z oprogramowaniem innych producentów, udostępniającym inne funkcje, np. przeglądarkami internetowymi.

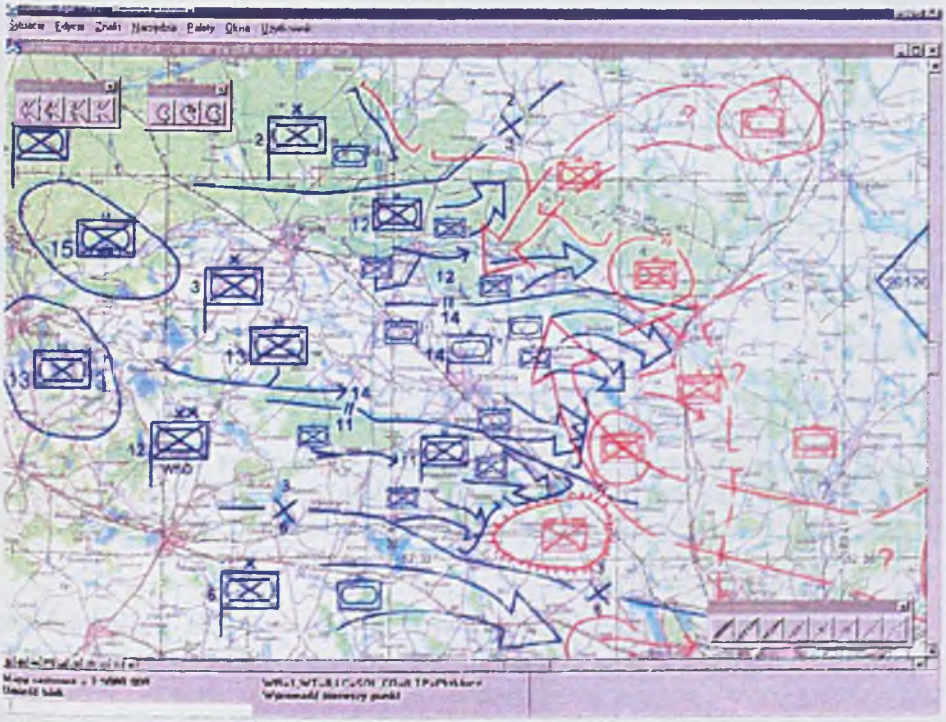
Obsługa oprogramowania wytworzonego w oparciu o Lotus Notes jest łatwa w użyciu między innymi dzięki funkcjom realizowanym automatycznie (np. wszystkie funkcje komunikacyjne, śledzenie zdarzeń w systemie, operacje na dokumentach).

Z punktu widzenia systemu monitorowania gotowości operacyjnej najważniejszymi cechami pakietu Lotus Notes są: aparat komunikacyjny; system zabezpieczeń, możliwość tworzenia złożonych aplikacji oraz możliwość wykrywania zdarzeń w systemie przez tzw. agentów - aplikacje rezydentne, podejmujące akcje zależne od występującego zdarzenia.

Jako edytor dokumentów graficznych jest wykorzystywany Pakiet Grafiki Operacyjnej (PGO, Rys. 34). Jest to komputerowy pakiet programowy, zbudowany dla zobrazowania ugrupowań wojsk własnych i przeciwnika na podkładzie mapy cyfrowej. Pakiet umożliwia działanie na mapie podkładowej oraz realizację wszelkich funkcji związanych z rysowaniem sytuacji operacyjno-taktycznej wojsk.

PGO umożliwia wyświetlanie wybranego fragmentu obszaru mapy, powiększanie i pomniejszanie tego obszaru. Zrealizowany jest również dostęp do opisowej bazy danych o terenie. Dzięki temu po wskazaniu elementu graficznego możemy uzyskać informacje o dowolnym obiekcie np. dane o miejscowości (nazwa, liczba ludności, status administracyjny), dane o właściwościach obiektów ważnych ze strategicznego punktu widzenia np. dane o mostach (materiał konstrukcyjny, nośność, szerokość, wysokość) itp.

Zobrazowanie sytuacji operacyjno-taktycznej jest przedstawione z użyciem umownych znaków taktycznych w sposób analogiczny, jak na topograficznych mapach podkładowych. Za pomocą tych znaków można narysować dowolną sytuację operacyjno-taktyczną. Można dowolnie zmieniać wielkość znaków, a także ich kolor i grubość. W PGO przygotowano zestaw narodowych znaków umownych oraz znaków NATO, pogrupowanych tematycznie w paletach narzędziowych. Znaki wprowadzamy poprzez określenie ich położenia na mapie.



Rys. 34 Przykładowa sytuacja operacyjna

Narysowane obiekty graficzne umieszczone są w pliku na oddzielnych warstwach według szczebli, oddzielnie dla wojsk własnych i przeciwnika. Struktura warstwowa umożliwia wygodne wyświetlanie lub wyłączanie wyświetlania obiektów zgrupowanych na określonych warstwach.

Najważniejsze operacje działania na sytuacji operacyjno-taktycznej to:

- Rysowanie i edycja sytuacji operacyjno-taktycznej;
- Synteza sytuacji uzyskanych od podległych jednostek;
- Jej zwrotna dekompozycja dla jednostek podległych;
- Dostęp do aktualnych informacji z baz danych o terenie i o wojskach;
- Możliwość wykonywania różnego rodzaju kalkulacji operacyjno-taktycznych.

Poza samym przeglądaniem, rysowaniem i manipulacją elementami graficznymi istnieje możliwość powiązania tych elementów z informacją opisową zawartą w bazie danych o wojskach.

PGO umożliwia pracę wielu operatorów nad jednym zadaniem. Odbywa się to w ten sposób, że operator pracuje na własnym zbiorze graficznym, a zbiory opracowywane przez innych operatorów wyświetlane są w tle. Zbiory lub ich fragmenty opracowane przez poszczególnych operatorów można połączyć w jeden zbiór tworząc pełny dokument. Mechanizm kreślenia na ploterze umożliwia podział rysunku na odpowiednie fragmenty, wykreślenie ich na pojedynczych arkuszach (papieru lub map) w celu późniejszego sklejenia. Kreślenie może się odbywać na arkuszach map topograficznych wszystkich skal używanych w wojsku.

Narysowana sytuacja może być przesłana do innego komputera. Przesłać można cały rysunek lub jego fragment. Przesyłany jest opis charakterystycznych parametrów znaków. Umożliwia to wymianę danych z innymi systemami pracującymi z innymi formatami plików graficznych.

Wnioski

Najważniejszym czynnikiem utrudniającym wdrażanie systemów jest trwająca od 1992 r. restrukturyzacja Sił Zbrojnych RP. Jest to szczególnie widoczne w przypadku systemu dyżurnych służb operacyjnych, gdzie przez okres projektowania koncepcyjnego zmieniało się wszystko: podporządkowanie DSO, liczba okręgów i rodzajów sił zbrojnych, nazewnictwo i zakres kompetencji komórek organizacyjnych MON i Sztabu Generalnego.

Kolejną barierą w pracach wdrożeniowych systemów są duże koszty wdrożenia systemów. Zakres przetwarzanych i przesyłanych informacji nakłada wysokie wymagania na ochronę przed emisją i nieuprawnionym dostępem do danych. Wymusza to stosowanie bezpiecznych i bardzo drogich rozwiązań. Dotyczy to zarówno sprzętu komputerowego (kabiny przeciwemisyjne, bezpieczne stanowiska komputerowe), osprzętu sieciowego (utajniona sieć zbudowana na światłowodach), jak też oprogramowania (system operacyjny o odpowiednim poziomie bezpieczeństwa, oprogramowanie umożliwiające szyfrowanie informacji) i zabezpieczeń organizacyjnych (ograniczenie dostępu osób nieupoważnionych).

Systemy monitorowania stanowią pierwszą próbę przybliżenia idei wspomagania pracy ogniw systemu dowodzenia. W trakcie eksploatacji próbnej i użytkowej systemy poddane zostaną szczegółowej weryfikacji pod kątem poprawności przyjętych rozwiązań parametrów eksploatacyjnych i wyposażenia technicznego. Mogą one stanowić zalążek budowy zautomatyzowanego systemu dowodzenia wojskami lądowymi.

Literatura

„Koncepcja zintegrowanego systemu dowodzenia i kierowania rozpoznaniem i WRE", Centrum Informatyki Sztabu Generalnego WP

„Mikrokomputerowy system wspomagania bieżącej pracy bojowo-rozpoznawczej zintegrowanego systemu rozpoznania - projekt koncepcyjny", Centrum Informatyki Sztabu Generalnego WP

„Projekt koncepcyjny systemu informatycznego dyżurnych służb operacyjnych. Szczebel centralny", Centrum Informatyki Sztabu Generalnego WP

Zaskórski P. Pokorski G. Sobiech G., „Grafika i mapa cyfrowa w zautomatyzowanych systemach dowodzenia" – materiały konferencyjne „Automatyzacja dowodzenia '97", WOSR, Jelenia Góra, 1997

13

13. Polityka bezpieczeństwa w systemach informatycznych

kpt. mgr inż. Sławomir Choromański

ppor. mgr inż. Krzysztof Olszewski

ppor. mgr inż. Piotr Sajdakowski

Wprowadzenie

Podstawą efektywnego podejścia do zadań bezpieczeństwa systemów informatycznych w instytucji są odpowiednio sformułowane: cele, strategie i polityka bezpieczeństwa informacji. Wspomagają one działania instytucji i zapewniają spójność wszystkich zabezpieczeń. Cele identyfikują to, co ma być osiągnięte; strategie określają, jak osiągnąć cele, a polityka określa to, co ma być wykonane.

Cele, strategie i polityka mogą być opracowane hierarchicznie od poziomu komórek organizacyjnych instytucji do poziomu eksploatacyjnego systemów informatycznych. Powinny odzwierciedlać potrzeby instytucji i brać pod uwagę występujące ograniczenia, przy czym jednorodność powinna być zapewniona na każdym poziomie i pomiędzy poziomami.

Bezpieczeństwo wchodzi w skład odpowiedzialności na każdym poziomie kierowniczym instytucji i w każdej fazie cyklu życia systemów. Cele, strategie i polityka powinny być weryfikowane i aktualizowane w oparciu o wyniki cyklicznych przeglądów bezpieczeństwa (np. analizy ryzyka, przeglądów bezpieczeństwa) oraz zmian w celach działania instytucji.

Na politykę bezpieczeństwa składają się podstawowe zasady bezpieczeństwa i wytyczne dla instytucji jako całości. Powinna ona odzwierciedlać wszechstronne uwarunkowania, które obejmują prawa jednostki, wymagania prawne i normy.

Polityka bezpieczeństwa instytucji w zakresie systemów informatycznych powinna odzwierciedlać podstawowe zasady bezpieczeństwa w kierowaniu instytucją podczas korzystania z infrastruktury i systemów informatycznych.

Polityka bezpieczeństwa danego systemu informatycznego powinna odzwierciedlać zasady bezpieczeństwa i zarządzenia zawarte w polityce bezpieczeństwa instytucji w zakresie systemów informatycznych. Powinna także zawierać konkretne wymagania w zakresie bezpieczeństwa, wdrażanych zabezpieczeń i ich użycia. Zastosowane podejście musi być efektywne w stosunku do potrzeb i możliwości instytucji.

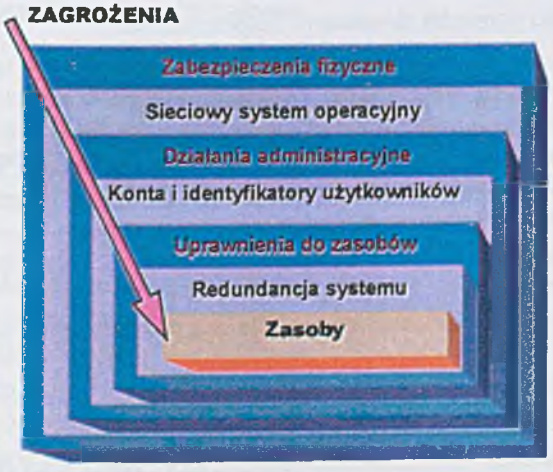
Przyjęte kierunki działań nad bezpieczeństwem systemów informatycznych powinny zawierać dziedziny bezpieczeństwa, takie jak: poufność, integralność, dostępność, rozliczalność, autentyczność i niezawodność. Wyrażane są one zwykle w języku naturalnym, lecz mogą być formułowane z użyciem języka matematycznego.

Cele, strategie i polityki określają poziom bezpieczeństwa w instytucji, próg akceptacji ryzyka oraz wymagania planowania awaryjnego w instytucji.

Polityka bezpieczeństwa

Generalną zasadą bezpieczeństwa jest ochrona niejawnych informacji przed niepowołanym dostępem, zniszczeniem lub ujawnieniem. Bezpieczeństwo systemów musi być zapewnione w trzech następujących obszarach:

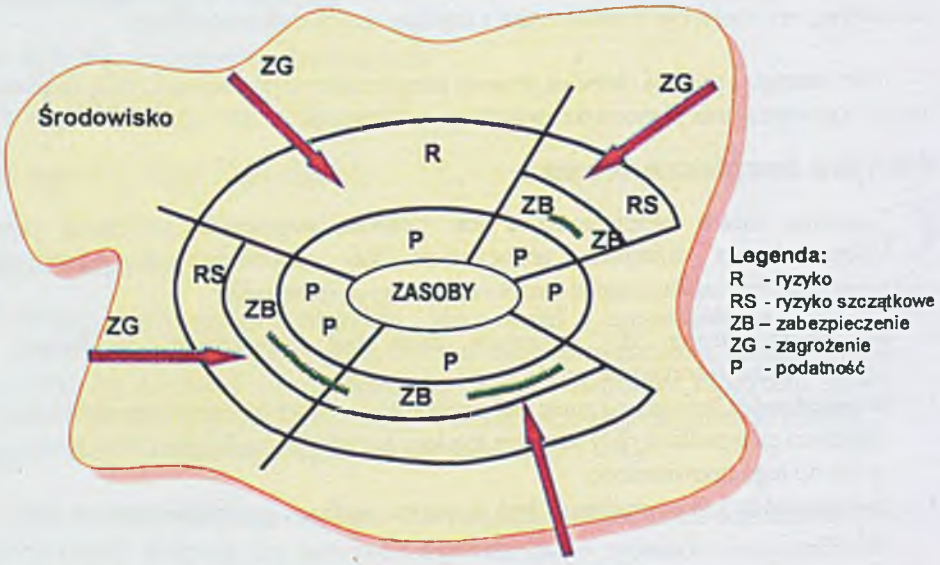
- **Poufność:** Dostęp do informacji musi być ograniczony do kręgu użytkowników autoryzowanych.
- **Integralność:** Informacja musi być zachowana w swej postaci oryginalnej, za wyjątkiem przypadków, gdy jest ona legalnie aktualizowana lub usuwana przez osoby do tego upoważnione.
- **Dostępność:** Informacja musi być dostępna osobom upoważnionym na ich żądanie.



Rys. 35 Warstwy zabezpieczeń systemu informatycznego

Bezpieczeństwo systemów informatycznych jest problemem wielowymiarowym. W związku z tym, aby określić i wdrożyć globalną jednorodną strategię oraz utrzymać politykę bezpieczeństwa systemów informatycznych, instytucja powinna wziąć pod uwagę wszelkie niezbędne aspekty. Zabezpieczenia tworzą kolejne warstwy, które stanowią kolejne zapory przed potencjalnymi zagrożeniami wobec zasobów (Rys. 35). Zbiór zagrożeń ulega stałym zmianom w czasie i jest znany tylko częściowo.

Wyniki analizy zagrożeń i zabezpieczeń można przedstawić przy pomocy modelu graficznego (Rys. 36).



Rys. 36 Zależności pomiędzy elementami bezpieczeństwa

Model ten reprezentuje:

Środowisko - otoczenie zawierające zagrożenia, które stale się zmieniają i są tylko częściowo znane,

Zasoby - dobra instytucji podlegające ochronie,

Podatności - łatwość nielegalnego dostępu przy istniejącym systemie zabezpieczenia,

Zabezpieczenia - sposoby wybrane dla ochrony zasobów i redukcji konsekwencji ich utraty,

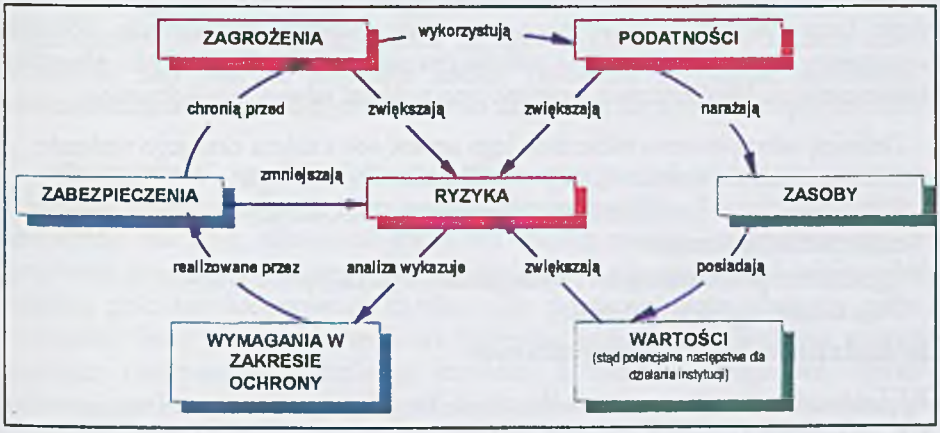
Zagrożenia - ciągłe oddziaływanie środowiska w celu wyrządzenia szkody w zasobach,

Zabezpieczenia - podjęte środki zaradcze, które zmniejszają ryzyko,

Ryzyko szczątkowe - dopuszczalny stopień ryzyka akceptowany w instytucji.

Niektóre zabezpieczenia mogą być skuteczne poprzez redukcję ryzyka związanego z wieloma zagrożeniami i wieloma podatnościami. Zredukowanie ryzyka szczątkowego do akceptowalnego poziomu wymaga wtedy kilku zabezpieczeń. Jeżeli ryzyko uważa się za akceptowalne, nie wdraża się zabezpieczeń, nawet jeśli zagrożenia takie występują. W innych przypadkach mogą istnieć podatności, ale nie ma znanych zagrożeń, które mogłyby je wykorzystać. Jednym ze sposobów wzrostu zabezpieczania jest monitorowanie środowisk zagrożeń, które mogłyby wykorzystać podatność.

Rys. 37 ilustruje zasadnicze związki pomiędzy elementami bezpieczeństwa często związanymi z zarządzaniem ryzykiem.



Rys. 37 Związki w zarządzaniu ryzykiem

Wymagania na bezpieczeństwo

Wymagania na zabezpieczenie systemu informatycznego w możliwie największym zakresie oraz wdrożenie najlepszych procedur można zapewnić, opierając się na standardzie brytyjskim B57799:1995 *Code of Practice for Information Security Management*. U podstaw koncepcji leży podział problematyki zabezpieczenia na poszczególne obszary (dziedziny), a następnie określenie wymagań w danym obszarze. Powinno się określić wymagania na zabezpieczenia w następujących obszarach:

- Organizacji zabezpieczeń;
- Klasyfikacji i kontroli zasobów;
- Zabezpieczenia kadrowego;
- Zabezpieczenia fizycznego;
- Zarządzania komputerami i sieciami;
- Kontroli dostępu do systemu;
- Rozwoju i konserwacji systemu;
- Planowaniu ciągłości działań;

- Zgodności.

Wszystkie sprawy związane z zagrożeniami bezpieczeństwa oraz ze sposobami podnoszenia jego poziomu muszą być regulowane dokumentami instytucji, m. in. przez:

- Podział odpowiedzialności za bezpieczeństwo informacji;
- Środki zabezpieczenia, kształcenia i szkolenia w zakresie zabezpieczeń;
- Zgłaszanie incydentów w zakresie zabezpieczeń;
- Planowanie procesów utrzymania ciągłości działania;
- Kontrolę zgodności działań z polityką bezpieczeństwa.

Kierownictwo powinno ustalić jasny kierunek działań i demonstrować wsparcie oraz zaangażowanie w dziedzinie zabezpieczenia informacji poprzez opracowanie organizacji polityki bezpieczeństwa. Zarząd powinien wydać pisemne oświadczenie dotyczące zajmowanego stanowiska w sprawie polityki bezpieczeństwa informacji dla wszystkich działów instytucji. Jako minimum, powinno ono zawierać następujące informacje:

- Definicję zabezpieczenia informacji, jego ogólne cele i zakres oraz jego ważność jako mechanizmu umożliwiającego współdzielenie informacji;
- Oświadczenie o zamierzeniach kierownictwa wspierających cele i zasady zabezpieczeń informacji;
- Zgodność z prawodawstwem i wymaganiami wynikającymi z umów;
- Planowanie ciągłości działalności.

Zarządzanie bezpieczeństwem

W celu identyfikacji potrzeb w dziedzinie bezpieczeństwa instytucji konieczne jest systemowe podejście. Dotyczy to także upowszechnienia w instytucji problemu bezpieczeństwa systemów informatycznych i kierowanie nim. Proces ten jest określany jako zarządzanie bezpieczeństwem systemów informatycznych i składają się na niego następujące działania:

- Opracowanie planu działania instytucji w zakresie bezpieczeństwa systemów informatycznych;
- Identyfikacja stanowisk i ich odpowiedzialności w instytucji;
- Zarządzanie ryzykiem, w skład którego wchodzi identyfikacja i określenie zasobów podlegających ochronie, zagrożeń, podatności, wpływów, ryzyk, zabezpieczeń, ryzyka szczątkowego, ograniczeń;
- Planowanie awaryjne i planowanie odtwarzania po katastrofach;
- Wybór i wdrożenie zabezpieczeń.

Poniżej przedstawiono główne elementy składające się na proces zarządzania bezpieczeństwem systemów informatycznych.

Zasoby. Prawidłowe zarządzanie zasobami (dobrami) jest niezbędne dla osiągnięcia celu działania instytucji i jest ono głównym zadaniem osób odpowiedzialnych za kierowanie instytucją na wszystkich poziomach. Atrybuty zasobów, które należy wziąć pod uwagę to ich wartość, wrażliwość oraz związane z nimi zabezpieczenia.

Zagrożenie (stan ciągłego oddziaływania zewnętrznego ukierunkowanego na utratę posiadanego dobra) musi wykorzystać istniejącą podatność zasobów w celu faktycznego wyrządzenia szkody tym zasobom. Zasoby podlegają wielu rodzajom zagrożeń. Zagrożenia są pochodzenia naturalnego lub celowe, mogą być przypadkowe lub rozmyślne. Należy zidentyfikować wszystkie rodzaje zagrożeń oraz określić ich poziom i prawdopodobieństwo występowania. Dla wielu rodzajów zagrożeń środowiskowych opracowane zostały dane statystyczne. Dane te należy wykorzystać podczas określania zagrożeń w instytucji.

Podatność związana z zasobami oznacza określoną słabość fizyczną, organizacyjną, proceduralną, osobową, zarządzania, administracji, sprzętu komputerowego, oprogramowania lub informacji. Podatność może być wykorzystana przez zagrożenie, co może spowodować szkodę dla systemu informatycznego lub celów działania instytucji. Podatność jako taka nie powoduje szkody, podatność jest jedynie warunkiem lub zbiorem warunków, sprzyjających wzrostowi zagrożenia dla zgromadzonych zasobów.

Następstwa są konsekwencją niepożądanego zdarzenia, spowodowanego rozmyślnie lub przypadkowo, który wpływa na stan zasobów. Konsekwencją może być zniszczenie zasobów, zniszczenie części lub całości systemu informatycznego, utrata poufności, integralności, dostępności, rozliczalności, autentyczności lub niezawodności. Możliwe pośrednie konsekwencje to także straty finansowe, utrata udziału w rynku lub wizerunku firmy. Zmierzenie wielkości następstw pozwala na utrzymanie równowagi pomiędzy następstwami niechcianego incydentu, a kosztami zabezpieczeń użytych do ochrony przed tym incydentem. Określanie kosztów następstw jest ważnym elementem określania ryzyka i wyboru zabezpieczeń.

Ryzyko jest prawdopodobieństwem określającym możliwość wykorzystania określonej podatności przez dane zagrożenie w celu spowodowania straty lub zniszczenia zasobu, a przez to negatywnego bezpośredniego lub pośredniego wpłynięcia na kondycję instytucji. Jedno lub wiele zagrożeń może wykorzystać jedną lub wiele podatności. Dowolna zmiana w zasobach, zagrożeniach, podatnościach i zabezpieczeniach może mieć znaczący wpływ na ryzyko. Wczesne wykrywanie i świadomość zmian w środowisku i systemie zwiększa możliwości podjęcia odpowiednich działań w celu redukcji ryzyka.

Zabezpieczenia to praktyki, procedury lub mechanizmy, które mogą chronić przed zagrożeniem, redukować podatność, ograniczać następstwa, wykrywać niepożądane incydenty i ułatwiać odtwarzanie. Efektywna ochrona wymaga zwykle kombinacji różnych zabezpieczeń w celu utworzenia warstw ochronnych dla zasobów.

Ryzyko szczątkowe. Ryzyko jest zwykle redukowane częściowo przez zabezpieczenia. Częściowa redukcja jest najczęściej wszystkim, co można osiągnąć, a im więcej chce się osiągnąć, tym większe trzeba ponieść koszty. Proces ten znany jest jako

akceptacja ryzyka (ryzyko szczątkowe), przy którym poniesione straty do wymaganych nakładów są małe (opłacalne).

Ograniczenia są zwykle ustalane lub uznawane przez kierownictwo instytucji, w zależności od zmian zachodzących w środowisku. Mogą mieć one charakter: organizacyjny, finansowy, środowiskowy, osobowy, czasowy, prawny, techniczny, kulturowy i społeczny. Wszystkie te czynniki należy brać pod uwagę wybierając i wdrażając zabezpieczenia.

Procesy zarządzania bezpieczeństwem systemów informatycznych

Zarządzanie bezpieczeństwem systemów informatycznych jest trwałym procesem składającym się z pewnej liczby specjalistycznych działań. Niektóre przedsięwzięcia, takie jak zarządzanie konfiguracją i zarządzanie zmianami, podejmowane są często w innych obszarach funkcjonowania instytucji.

Zarządzanie konfiguracją. Podstawowym celem bezpieczeństwa w zarządzaniu konfiguracją jest zapewnienie, aby zmiany w systemie nie obniżały efektywności zabezpieczeń i całkowitego bezpieczeństwa instytucji. W niektórych przypadkach mogą zaistnieć powody dokonania zmian, które przejściowo obniżą poziom bezpieczeństwa. W tych sytuacjach należy określić stopień obniżenia poziomu bezpieczeństwa, a kierownictwo powinno podjąć decyzję opartą o wyniki analizy. Zmiany w systemie powinny być rejestrowane w dokumentach, takich jak plany awaryjne i plany odtwarzania po katastrofie. Jeśli zmiana jest znacząca, może zaistnieć konieczność weryfikacji części lub wszystkich zabezpieczeń systemu.

Zarządzanie zmianami. Przed planowaniem lub wprowadzeniem zmian w systemie informatycznym, należy określić ich przyszły wpływ na bezpieczeństwo instytucji.

Zarządzanie ryzykiem. Proces zarządzania ryzykiem polega na porównywaniu określonego ryzyka z zyskami i kosztami zabezpieczeń oraz tworzeniu strategii wdrożenia i polityki bezpieczeństwa w zakresie systemów informatycznych zgodnej z polityką bezpieczeństwa instytucji. Zabezpieczenia są wybierane dla odpowiednich ryzyk, potencjalnych następstw i ponoszonych kosztów. W związku z tym należy uważnie wybierać zabezpieczenia, tak aby nie tylko zredukować zidentyfikowane ryzyko, lecz aby nie wprowadzić nowego.

Analiza ryzyka stanowi część zarządzania ryzykiem. W kontekście bezpieczeństwa systemów informatycznych, analiza ryzyka składa się z analizy wartości zasobów, zagrożeń i podatności. Ryzyko określane jest poprzez potencjalne następstwa spowodowane naruszeniem poufności, integralności, dostępności, rozliczalności,

autentyczności i niezawodności. Wynikiem analizy ryzyka jest określenie prawdopodobnych następstw dla zasobów.

Uświadamianie i rozliczanie. Uświadamianie w zakresie bezpieczeństwa jest kluczowym elementem skutecznych działań. Brak świadomości i słaba praktyka personelu w tej dziedzinie może znacząco zredukować skuteczność zabezpieczeń. Pracownicy instytucji są generalnie uważani za jedne z najsłabszych ogniw w zabezpieczeniach. Skuteczne zabezpieczenia wymagają rozliczalności i bezpośredniego przyjęcia do wiadomości obowiązków osób funkcyjnych z zakresu bezpieczeństwa. Obowiązki i rozliczalność powinny być przypisane do właścicieli zasobów, dostawców zasobów i użytkowników systemów informatycznych.

Monitorowanie. Używanie zabezpieczeń powinno być monitorowane w celu zapewnienia ich prawidłowego działania, upewnienia się, że zmiany w środowisku nie wpłynęły na efektywność działania zabezpieczeń oraz, że zapewniona jest rozliczalność. Automatyczne narzędzia do przeglądania i analizy dzienników działań są pomocne w zapewnieniu zamierzonej skuteczności zabezpieczeń. Narzędzia te mogą także być użyte do wykrywania niepożądanych zdarzeń, a ich użycie ma efekt odstraszający. Ogólne funkcje audytu systemu mogą dostarczyć użytecznych danych z punktu widzenia poprawy bezpieczeństwa informacji.

Planowanie awaryjne i odtwarzanie po katastrofie. Plany awaryjne zawierają informacje o tym, jak prowadzić działalność w instytucji, gdy procesy ją wspomagające (w tym systemy informatyczne) zostały zakłócone lub niedostępne. Plany te powinny opisywać wszystkie możliwe składniki różnych scenariuszy sytuacji awaryjnych, w tym: czasu trwania awarii, utraty różnych funkcji. Należy podać sposób powrotu do stanu sprzed awarii lub który istniałby, gdyby przerwa w działaniu nie nastąpiła.

Wnioski

Intencją tego opracowania jest przedstawienie podstawowych zasad, które powinny być stosowane przez osoby odpowiedzialne za stworzenie, wdrożenie i nadzór nad bezpieczeństwem informacji. Omawiane zasady bezpieczeństwa są uważane za szczególnie ważne. Zapewniają one dobry start do bezpiecznego zarządzania informacją.

Nie ma jednego, najlepszego zalecenia w zakresie zapewnienia bezpieczeństwa. Każda kategoria użytkowników lub specjalistów przetwarzania danych w określonym środowisku będzie mieć różne potrzeby, problemy i priorytety uzależnione od realizowanych funkcji, organizacji i interesów oraz środowiska przekazywania informacji. Wymaga to opracowania szeregu indywidualnych interpretacji wskazówek dla poszczególnych grup pracowników, aby propagować efektywniej zalecenia w zakresie bezpieczeństwa.

Literatura

B57799:1995, Code of Practice for Information Security Management;

PN-I-13335-1:1999, Pojęcia i modele bezpieczeństwa systemów informatycznych;

ISO/IEC TR 13335-2:1997, Managing and planning IT Security.

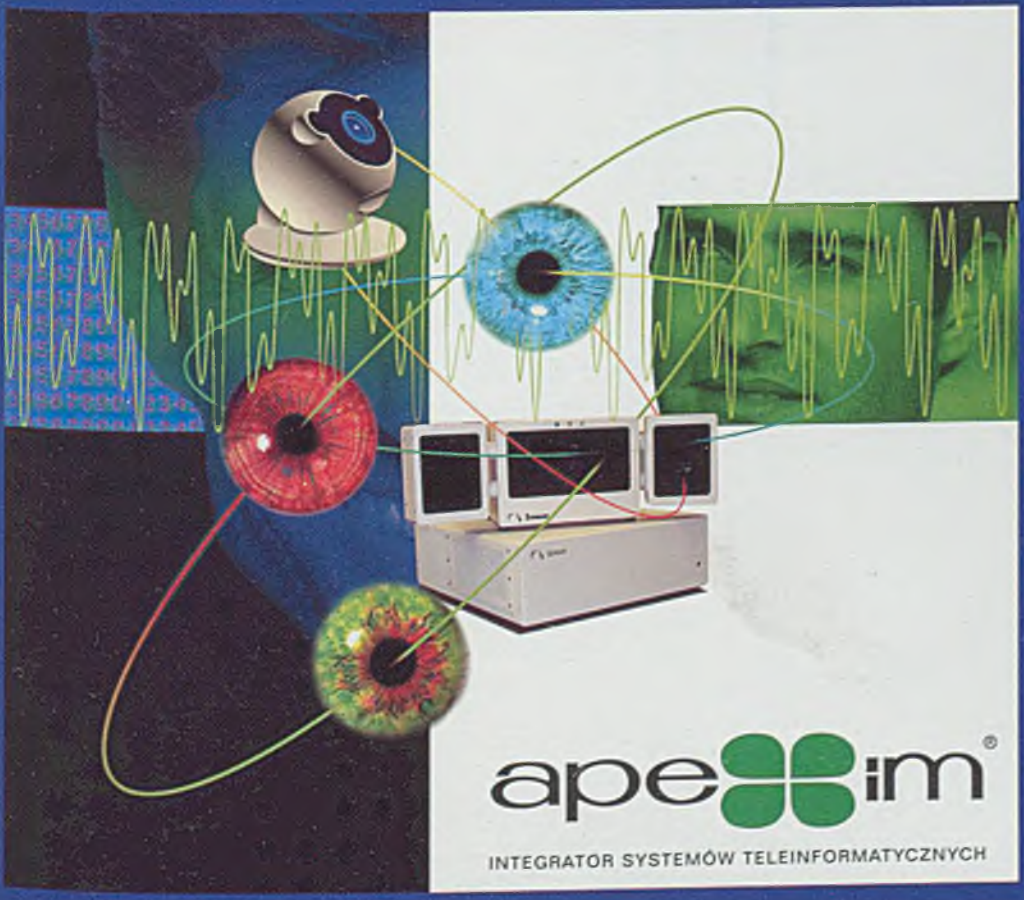
14

14. Prezentacje Firm Sponsorujących Jubileusz Centrum Informatyki Sztabu Generalnego WP

Sensar ... Secure™

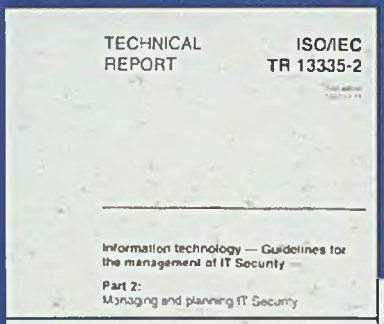
Nr 1

biometrycznych technologii identyfikacji osób



apeXim®

INTEGRATOR SYSTEMÓW TELEINFORMATYCZNYCH


TECHNICAL REPORT

ISO/IEC TR 13335-2

Information technology — Guidelines for the management of IT Security

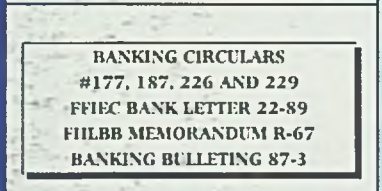
Part 2: Managing and planning IT Security

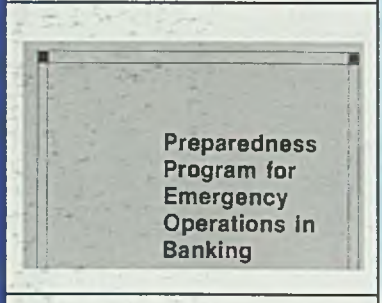

FIPS PUB 87

FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION

1981 MARCH 27

GUIDELINES FOR ADP CONTINGENCY PLANNING


BANKING CIRCULARS
#177, 187, 226 AND 229
FFIEC BANK LETTER 22-89
FHLBB MEMORANDUM R-67
BANKING BULLETING 87-3


Preparedness Program for Emergency Operations in Banking


DZIENNIK USTAW
RZECZYPOSPOLITEJ POLSKIEJ

Nr 11

apexim®

Integrator Systemów Teleinformatycznych

Bezpieczeństwo

Systemów Teleinformatycznych

Information Technology Security

- Analiza i doradztwo
- Organizacja i technologia
- Szkolenia i treningi

APEXIM S.A.

Warszawa 02-699, ul. Kłobucka 25
tel: (0-22) 607 61 00
fax: (0-22) 607 62 00
e-mail: apexim@apexim.com.pl
http://www.apexim.com.pl

TELEINFORMATYKA
broń XXI wieku

Współczesny system obronny opiera się na teleinformatyce. Komputery i sieci to jego mózg i układ nerwowy.

Od lat współpracujemy z Siłami Zbrojnymi w zakresie budowy nowoczesnych rozwiązań teleinformatycznych na potrzeby Armii. Oferujemy najnowsze światowe technologie, stosowane w armiach innych członków NATO. Projektowane, dostarczane i wdrażane przez nas systemy zapewnią szybką integrację i pełną kompatybilność polskiego systemu obronnego z systemami armii sojuszniczych.

Oferujemy:

sieci korporacyjne i rozległe

szerokopasmowe, szybkie sieci w standardzie ATM

globalne zarządzanie systemami teleinformatycznymi

zaawansowane systemy do wizualizacji, symulacji i wspomagania dowodzenia

„utwardzone" komputery dla wszystkich rodzajów wojsk

teleinformatyczne systemy bezpieczeństwa

„inteligentne budynki", okablowanie strukturalne i światłowodowe

monitoring wizyjny

i inne

ATM S.A. INTEGRATOR SYSTEMÓW TELEINFORMATYCZNYCH

ul. Grochowska 21a, 04-186 Warszawa, tel. (0-22) 612 30 20, 610 60 73, fax (0-22) 610 41 44, 612 18 50; customer@atm.com.pl, http://www.atm.com.pl

Oddział Gdańsk Plac Kaszubski 8, 81-360 Gdynia, tel. (0-58) 661 88 23, tel./fax (0-58) 661 84 18
Oddział Katowice ul. Kolista 25, 40-486 Katowice, tel. (0-32) 735 03 22, fax (0-32) 735 03 21
Oddział Kraków ul. Rzeźnicza 13/15, 31-540 Kraków, tel./fax (0-12) 421 51 33 w. 211
Oddział Poznań ul. 27 Grudnia 7/18, 61-737 Poznań, tel. (0-61) 851 91 01, fax (0-61) 853 33 74
Oddział Szczecin ul. Monte Cassino 24, 70-467 Szczecin, tel./fax (0-91) 423 29 43
Oddział Wrocław ul. Powstańców Śląskich 95, 53-332 Wrocław, tel. (0-71) 780 41 86, fax (0-71) 780 41 89, komertel (0-3912) 3890

fot. płk. M. Iwański, Biuro East News

Produkty

- Infrastruktura teleinformatyczna.
- Systemy logistyczne (m.in. Oracle Applications).
- Systemy paszportyzacji i zarządzania systemem łączności.
- Systemy informacji przestrzennej (GIS).
- Systemy oparte o EDI.

INFORMATYKA DLA WOJSKA
GRUPA COMPUTERLAND

ługi

Wdrożenia systemów, szkolenia i serwis.
Tworzenie systemów dedykowanych
„pod klucz" – zespoły projektowe.
Polonizacja i kastomizacja najlepszych
rozwiązań światowych.
Outsourcing lub project management.
Bezpieczeństwo systemów teleinforma-
tycznych.

Potencjał i przygotowanie

- Sektor obronny w Grupie ComputerLand (w ramach sektora publicznego).
- Przygotowana kadra do ścisłej współpracy z resortem Obrony Narodowej w zakresie IT, w tym również dotyczącej prac niejawnych na rzecz obronności państwa.
- Doświadczenie w realizacji dużych ogólnokrajowych projektów i obsłudze organizacji o ogólnopolskim zasięgu działania.
- Umowa pomiędzy Centrum Informatyki Sztabu Generalnego WP a jedną z firm Grupy ComputerLand (Positive SA) o stałej współpracy metodycznej w zakresie bezpieczeństwa IT.

INFORMATYKA DLA WOJSKA

Sektor publiczny

„Być niekwestionowanym strategicznym partnerem naszych Klientów dzięki wprowadzaniu przez najlepszych specjalistów niezawodnych systemów informacyjnych, przynoszących Klientom korzyści biznesowe i organizacyjne".

ul. Jana Kazimierza 62 A, 01-248 Warszawa, tel. (48 22) 532 97 77, fax (48 22) 532 98 88,
http://www.computerland.pl, e-mail: info@computerland.pl

GRUPA ComputerLand

03-301 Warszawa, ul. Jagiellońska 74, tel./fax: (0-22) 676-92-92, 676-95-34, 811-03-91, 811-10-13
e-mail: cons@consortia.com.pl

DOSTAWCA KOMPLEKSOWYCH ROZWIĄZAŃ INFORMATYCZNYCH

SPECJALIZACJA FIRMY

- dostawca kompleksowych rozwiązań w oparciu o sprzęt komputerowy, teletransmisyjny oraz oprogramowanie uznanych na rynku producentów,
- dostawca kompleksowych rozwiązań w zakresie sieci radiokomunikacyjnych,
- dostawca kompleksowych rozwiązań fiskalnych systemów kasowych dla sieci handlowych, sklepów i gastronomii,
- dostawca zintegrowanego systemu **TETRA CS/3** do wspomagania zarządzania, przeznaczonego dla średnich oraz dużych firm,
- wykonawca profesjonalnych usług serwisowych.

OFERTA FIRMY

KOMPLEKSOWE ROZWIĄZANIA INFORMATYCZNE

Integracja i dostawa kompleksowych rozwiązań informatycznych.

Wśród urządzeń komputerowych, oferowanych przez **CONSORTIĘ**, znajdują się między innymi: duże i średnie serwery, stacje robocze, terminale, drukarki, osprzęt do budowy sieci LAN, osprzęt do budowy telekomunikacyjnych sieci rozległych, WAN.

Zintegrowane oprogramowanie do wspomagania zarządzania przedsiębiorstwem brytyjskiej firmy **Sage Tetra International Ltd.**

Dostawa oprogramowania systemowego i narzędziowego.

SYSTEMY RADIOKOMUNIKACYJNE

Kompleksowe rozwiązania w zakresie radiokomunikacji ruchomej i lądowej dla dużych, średnich i małych firm.

Pełny wybór radiotelefonów przenośnych, samochodowych i bazowych. Możliwość realizacji dużych projektów dla sieci łączności radiowej, także trunkingowej.

Oferowany sprzęt radiokomunikacyjny pracuje w pasmach LB, MB, VHF i UHF.

FISKALNE SYSTEMY KASOWE

Systemy kasowe typu POS w architekturze PC wraz z oprogramowaniem kasowym pracującym pod kontrolą systemu operacyjnego UNIX.

Systemowe kasy fiskalne typu ECR dla małych i średnich placówek handlowych oraz branży gastronomicznej.

Szeroka gama kasowych urządzeń wspomagających takich jak: skanery, wagi, drukarki rachunków, drukarki kuchenne, terminale, szuflady, kasety na pieniądze itp.

USŁUGI SERWISOWE

Serwis w zakresie systemów komputerowych, mainframe, serwerów, stacji roboczych, urządzeń peryferyjnych oraz fiskalnych systemów kasowych, wykonywany na terenie całego kraju.

Biuro w Gdyni	ul. Korzeniowskiego 20, 81-376; tel./fax (0-58) 620-31-77
Biuro w Katowicach	ul. Chorzowska 73a, 40-101; tel./fax (0-32) 58-78-42
Biuro w Krakowie	ul. Lublańska 34, 31-476; tel./ (0-12) 616-25-03, fax 616-25-04
Biuro we Wrocławiu	ul. Racławicka 15/17, 53-149; tel./fax (0-71) 361-54-21

HOGART

Information Technology Partner

HOGART oferuje Siłom Zbrojnym RP, członkowi NATO, najnowocześniejsze światowe rozwiązania informatyczne.

J.D. Edwards – amerykański zintegrowany system informatyczny, jest przeznaczony dla wojskowej logistyki stacjonarnej, która jest informacyjnym elementem bazowym dla logistyki mobilnej.

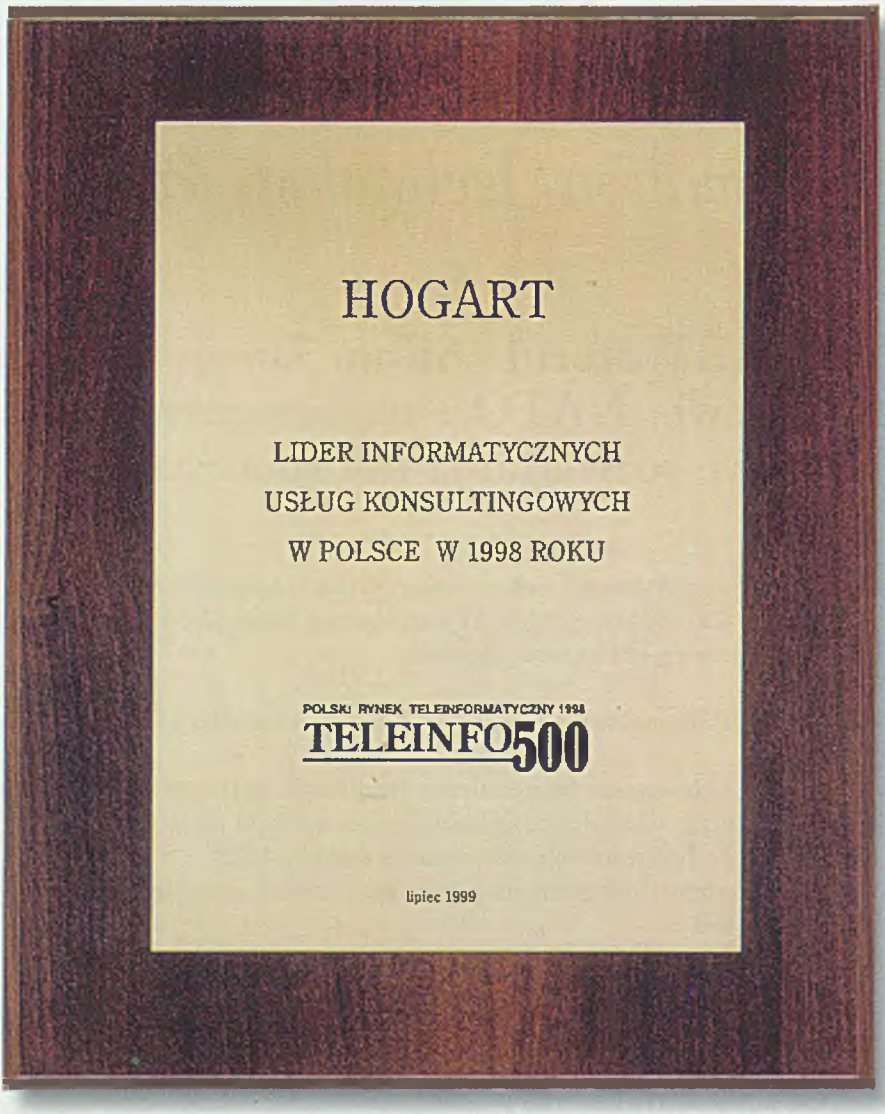
Dziedziny wojskowego zastosowania J.D. Edwards to między innymi:

- dowodzenie i kierowanie hierarchiczną strukturą logistyczną wojsk (bazy logistyczne, oddziały gospodarcze, rejonowe bazy materiałowe);
- kierowanie służbami: uzbrojenia, umundurowania, MPS (w tym sterowanie dynamicznymi parametrami paliw), transportowymi, żywnościowymi;
- kierowanie łańcuchem dostaw, zarządzanie finansami i produkcją.

J.D. Edwards przeznaczony jest dla Zarządu Logistyki Sztabu Generalnego WP, a także dla Dowództwa Wojsk Lądowych, Dowództwa Wojsk Lotniczych i Obrony Powietrznej oraz Dowództwa Marynarki Wojennej RP.

W Polsce jedynym autoryzowanym partnerem i dystrybutorem J.D. Edwards jest firma Normax, wchodząca w skład grupy HOGART.

TELEINFO 500 uznało firmę HOGART za największą firmę informatyczną oferującą usługi konsultingowe w Polsce w 1998 roku.



Warszawa

HOGART
ul. Gwiaździsta 19
01-651 Warszawa
tel. (22) 639 26 00
fax (22) 639 26 05

Gdynia

HOGART
Plac Kaszubski 8
81-350 Gdynia
tel. (58) 666 23 00
fax (58) 666 23 02

Kraków

HOGART
ul. Kalwaryjska 69
30-504 Kraków
tel. (12) 656 47 39
fax (12) 656 33 53

Poznań

HOGART
ul. Wierzbięcice 1
61-569 Poznań
tel. (61) 833 79 33
fax (61) 833 79 49

http://www.hogart.com.pl

OPTIMUS S.A. INTEGRACJA istnieje na polskim rynku informatycznym od roku 1996 i jest integralną częścią firmy OPTIMUS S.A. Obecnie zatrudnia 170 pracowników w pięciu oddziałach na terenie całego kraju. W firmie pracują inżynierowie legitymujący się certyfikatami takich firm jak: Novell, Microsoft, Mod-Tap. Nasze osiągnięcia znajdują swe potwierdzenie wśród wielu użytkowników. Dzięki zorganizowanej dystrybucji oraz rozległej sieci serwisu w krótkim czasie docieramy do każdego miejsca na terenie całego kraju.

Polskie przedsiębiorstwo OLM powstałe z połączenia potencjałów OPTIMUS S.A. oraz LOCKHEED MARTIN CORPORATION zapewnia naszym Siłom Zbrojnym dostęp do najnowocześniejszych i sprawdzonych w armiach NATO zintegrowanych systemów informacyjnych. Oferujemy zarówno uznane na świecie rozwiązania systemowe jak i polskie technologie oraz zasoby kadrowe.

Wstąpienie Polski do NATO wymaga od Polskich Sił Zbrojnych oraz Przemysłu Obronnego modernizacji i restrukturyzacji. Jednym z najważniejszych zadań będzie wdrożenie nowoczesnych zintegrowanych rozwiązań teleinformatycznych celem zapewnienia pełnej kompatybilności z systemami używanymi przez Sojusz Północnoatlantycki.
Stwarza to konieczność budowy sprawnych i zgodnych ze standardami natowskimi systemów dowodzenia, kontroli oraz wymiany informacji.

W oferowanych przez Optimus S.A. rozwiązaniach korzystamy ze sprawdzonych na świecie technologii, dostarczanych przez takich potentatów z branży IT jak : *Lockheed Martin Corporation IT, Intel, IFS, SCO, Oracle...* Współpraca z takimi partnerami zapewnia nam dostęp do najlepszych produktów, wsparcia technicznego, wiedzy oraz bogatego doświadczenia.

Oferta OPTIMUS S.A. INTEGRACJA dedykowana Polskim Siłom Zbrojnym obejmuje pełen zakres usług informatycznych począwszy od integracji systemów definiowanej jako kompleksowa usługa zawierająca analizę potrzeb, konsultacje, dostawę, instalację sprzętu i oprogramowania, projektowanie rozwiązań „pod klucz", szkolenia oraz wsparcie techniczne a kończąc na pełnej ofercie sprzętowej.

OPTIMUS S.A.
33-300 Nowy Sącz, ul. Nawojowska 118, tel. 018 444 05 55, fax 018 444 05 03, www.optimus.pl, www.onet.pl
Oddziały: Bydgoszcz, ul. Jagiellonska 103, tel. 052 346 00 92, fax 052 341 08 27 Gdańsk, ul. Pomorska 96, tel. 058 556 1611, fax 058 557 60 79 Mysłowice, ul. Mikołowska 31, tel. 032 222 60 41, fax 032 762 44 17 Warszawa, ul. Wynalazek 4, tel. 022 640 48 01, fax 022 640 07 61 Wrocław, ul. Mydlana 1, tel. 071 345 00 00, fax 071 345 02 90

Do szeregu oferowanych przez Optimus S.A. Integracja i OLM ITG S.A. całościowych rozwiązań systemowych należy zaliczyć między innymi:

- C4ISR
- Dowodzenie i kierowanie C2
- Logistyki i sieci transportowych
- Kontroli i monitorowania granic
- Zarządzania w sytuacjach kryzysowych
- Symulacji i treningu
- Bezpiecznej łączności
- Bezpieczeństwa informacji
- Zabezpieczenia szczególnie ważnych obiektów
- Zobrazowania i przetwarzania dokumentów
- System zabezpieczania dostępu do zasobów komputera
- System videokonferencji multimedialnych
- IFS- zestaw zintegrowanych rozwiązań informatycznych
- System zarządzania szpitalem ADT
- Akcesoria – komputery, serwery, stacje graficzne, drukarki

Należy podkreślić również, że oferowany sprzęt jest wolny od tzw.„problemu roku 2000"

ZACHĘCAMY DO WSPÓŁPRACY

Współpracując z OPTIMUS S.A. INTEGRACJA oraz OLM ITG S.A. macie Państwo do dyspozycji wyszkolony zespół specjalistów, dysponujący doświadczeniem i metodyką w zakresie projektowania, doboru i integrowania rozwiązań informatycznych .

Nasza filozofia jest prosta: zatrudniamy najlepszych ludzi i ściśle współpracujemy z naszymi klientami, tak aby opracować dla nich najlepsze rozwiązania.

Współpraca klientów z OPTIMUS S.A. INTEGRACJA i OLM ITG S.A. daje dostęp do wiedzy popartej doświadczeniem oraz do najnowocześniejszej technologii producentów światowej klasy sprzętu komputerowego i produktów sieciowych (całej gamy sprzętu pasywnego, aktywnego oraz sieciowych systemów operacyjnych).

Rozumiemy, iż każde przedsięwzięcie informatyczne jest inwestycją o charakterze strategicznym. Dlatego staramy się precyzyjnie określić i zrozumieć cele projektu informatycznego, a następnie projekt ten rzetelnie zaplanować i sprawnie przeprowadzić jego wdrożenie.

Stabilność ekonomiczna i potencjał organizacyjny firmy OPTIMUS S.A. przy stałym jej rozwoju daje pewność, że proponowane przez nas długofalowe rozwiązania będą w stanie spełnić wszystkie potrzeby i wymagania.

OPTIMUS S.A.
33-300 Nowy Sącz, ul. Nawojowska 118, tel. 018 444 05 55, fax 018 444 05 03 , www.optimus.pl, www.onet.pl
Oddziały: Bydgoszcz, ul. Jagiellońska 103, tel. 052 346 00 92, fax 052 341 08 27 Gdańsk, ul. Pomorska 96, tel. 058 556 1611, fax 058 557 60 79 Mysłowice, ul. Mikołowska 31, tel. 032 222 60 41, fax 032 762 44 17 Warszawa, ul. Wynalazek 4, tel. 022 640 48 01, fax 022 640 07 61 Wrocław, ul. Mydlana 1, tel. 071 345 00 00, fax 071 345 02 90

Tworzenie i realizacja optymalnych
systemów teleinformatycznych

Myślimy **globalnie**

Potrafimy - wykorzystać światowe technologie dla Twojego rozwoju
Wiemy - że mają realizować Twoje cele
Rozumiemy - jak ważne jest dla Ciebie bezpieczeństwo inwestycji

EnerGis - system zarządzania obiektami (GIS)
ad:Office (Lotus Notes) - system zarządzania obiegiem dokumentów i przepływem pracy

systemy serwerowe w technologii RISC i Intel
sieci LAN/WAN, Intranet
systemy telekomunikacyjne i radiotelekomunikacyjne
kompleksowa infrastruktura systemu informatycznego
systemy wysokiej dostępności
systemy zarządzania infrastrukturą informatyczną
systemy bezpieczeństwa
systemy zobrazowania wielkoformatowego
centra monitorowania oraz reagowania w sytuacjach kryzysowych

STER PROJEKT
Integrator systemów

STER-PROJEKT Spółka Akcyjna CENTRALA: ul. Magazynowa 1, 02-652 Warszawa, tel. (0-22) 60 77 200, fax (0-22) 60 77 100, SALON FIRMOWY: Al. Solidarności 68, 00-240 Warszawa, tel. (0-22) 831 68 61, 831 58 89, fax (0-22) 831 73 29; ODDZIAŁY: Wołomin tel. (0-22) 76 39 200, fax (0-22) 76 39 100; Kielce tel./fax (0-41) 345 42 95, 346 24 40, 346 24 41; Łódź tel./fax (0-42) 639 96 60; GRUPA STER-PROJEKT: Bydgoszcz tel./fax (0-52) 342 47 18, 342 26 15, fax (0-52) 345 34 99; Gdańsk tel./fax (0-58) 346 21 12, 301 52 33; Kraków tel. (0-12) 618 53 93, fax (0-12) 421 66 60; Poznań tel./fax (0-61) 826 04 64/80; Wrocław tel./fax (0-71) 372 33 67, 343 96 15; Ster-Projekt Konsulting Sp. z o.o. tel. (0-22) 60 77 200, fax (0-22) 60 77 190

SUN MICROSYSTEMS W PROGRAMACH OBRONNYCH

W ciągu ostatnich dziesięcioleci wojskowe systemy obronne jako pierwsze wdrażały złożone technologie informatyczne. Wystarczy wymienić choćby technologie wykorzystywane w sieci Internet, które zostały stworzone w latach sześćdziesiątych na potrzeby amerykańskiej armii.

Historia działalności firmy Sun na rynku zastosowań militarnych sięga już ponad dziesięciu lat. Sun dostarcza sprzęt, oprogramowanie oraz usługi, zapewniające strukturę informatyczną dla systemów dowodzenia i kierowania. Firma współpracuje z wieloma międzynarodowymi i lokalnymi partnerami, mającymi doświadczenie w dostarczaniu aplikacji dla wszystkich rodzajów służb wojskowych i dla wszystkich rodzajów wojsk. Sun stworzył też stały zespół konsultantów, których zadaniem jest wspieranie lokalnych projektów z dziedziny wojskowej, opartych na technologii firmy Sun Microsystems.

Ze względu na dużą wagę, jaką firma Sun Microsystems przywiązuje do odbiorców wojskowych, za kontakty z sektorem wojskowym odpowiedzialna jest wydzielona jednostka Sun Microsystems Federal.

Rozwiązania firmy Sun

Najwyższa wydajność przy niskich kosztach

Wysoce skalowalne, wieloprocesorowe serwery SMP oraz stacje robocze pozwalają obsłużyć aplikacje HPC wymagajace najwyższej wydajności. Serwery z linii Sun Enterprise (od serwerów dla grup roboczych, aż po wysokowydajny serwer klasy mainframe Sun Enterprise 10000) zapewniają skalowalność oraz wydajność, gwarantujac jednocześnie wszystkie korzyści otwartego przetwarzania sieciowego. Serwery odznaczają się także doskonałymi cechami RAS (niezawodność, dostępność i łatwość serwisowania), dzięki którym Sun gwarantuje stałą dostępność danych i aplikacji, wymaganą przez aplikacje o znaczeniu krytycznym. Wszystkie produkty pracują w jednym, skalowalnym, 64-bitowym środowsku operacyjnym Solaris, nie ma wiec kłopotów z migracja od systemów podstawowych, do coraz bardziej wydajnych rozwiazań, w miarę jak zwiększa się zapotrzebowanie na moc obliczeniowa. Stała dostępność danych gwarantują także niezawodne systemy pamięci masowej z rodziny Sun StorEdge, pozwalające przechowywać i archiwizować terabajty danych.

Zwiększanie wydajności pracy

Technologia Java - otwarta, standardowa i uniwersalna platforma dla przetwarzania sieciowego - pozwala przyspieszyć i zwiększyć wydajność procesu tworzenia aplikacji. Dzięki Javie aplikacje dla Internetu i intranetu mogą być uruchamiane na istniejącym sprzęcie i w istniejącej architekturze softwarowej. Architektura „odchudzonych" klientów sieciowych pozwala szybciej wdrażać aplikacje w całym przedsiębiorstwie.

Dzięki „odchudzonych" klientów sieciowych opartych na Javie, Sun oferuje także nowatorskie urządzenia sieciowe Sun Ray 1, które będąc w pełni niezależne od platformy sprzętowej, pozwala na bezpieczny dostęp do indywidualnych zasobów pracownika z dowolnego miejsca w ramach sieci korporacyjnej.

Praca w wydajnym środowisku operacyjnym

Agencje rządowe i wojskowe wymagają dostępu do zasobów sieciowych z dowolnego miejsca i w każdej chwili, przy pełnym z bezpieczeństwie rozwiązania. Środowisko operacyjne Sun Solaris stanowi niezawodna, skalowalna i bezpieczną platformę do uruchamiania aplikacji wymagających najwyższej niezawodności. Jedną z podstawowych cech środowiska Solaris jest pełna 64-bitowość jądra, a także niezawodność klasy mainframe i ściślejsza integracja ze środowiskami PC. Co więcej Solaris, dostępny dla platformy Intel i SPARC, jest łatwy w instalowaniu i administrowaniu.

Technologia Solaris PC Netlink zwiększa niezawodność i skalowalność istniejących środowisk opartych na Windows NT, zapewniając pełną implementację usług sieciowych NT w środowisku Solaris. Dzięki temu serwery NT i Solaris mogą w łatwy sposób współpracować w ramach jednej sieci LAN.

Przy rozwiązaniach wymagających najwyższych standardów bezpieczeństwa, Sun Microsystems oferuje środowisko Trusted Solaris, charakteryzujące się zabezpieczeniami przed zagrożeniami zewnętrznymi i wewnętrznymi, znacznie bardziej rozbudowanymi niż w jakimkolwiek innym środowisku UNIXowym, które uzyskało certyfikat bezpieczeństwa na poziomie E3/F-C2 oraz E3/F-B1. Dodatkowo konsultanci firmy Sun, wspomagają projektowanie kompleksowych, zaawansowanych systemów zabezpieczających.

Wdrożenia i zastosowania

Najbardziej rozwinięte systemy dowodzenia i kierowania posiada armia Stanów Zjednoczonych. Dlatego też rynek USA jest największym odbiorca Sun Microsystems Federal i tam też koncentruje się najwięcej wdrożeń, chociaż Firma rozwija się dynamicznie w pozostałych krajach członkowskich NATO, w Kanadzie, Australii i Tajlandii.

Programy firmy Sun obejmują siły lądowe, lotnictwo, marynarkę wojenna oraz wywiad wojskowy. Istnieja też połączone programy dla wszystkich rodzajów służb wojskowych. W sumie San bierze udział w ponad 110 programach na całym świecie.

Program ASOC

Celem programu ASOC jest zwiększenie bezpieczeństwa wschodnioeuropejskiej przestrzeni powietrznej, co staje się coraz istotniejsze wraz ze wzrostem ruchu powietrznego na tym obszarze. Szczegółowe zamierzenia obejmują: zwiększenie współpracy lotnictwa cywilnego i wojskowego, podniesienie efektywności operacyjnej oraz wprowadzenie zgodności z systemami NATO.

Podstawą projektu ASOC jest system monitoringu przestrzeni powietrznej, składający się z oprogramowania i sprzętu dzięki któremu możliwa jest integracja informacji spływających z 18 wojskowych i cywilnych stacji radarowych. Cały system pracuje w oparciu o serwery i stacje robocze firmy Sun Microsystems.

Program CHS-2

Realizację programu CHS-2 (Common Hardware/Software 2) rozpoczęto w 1995 roku. W ramach kontraktu o wartości 1,5 mld dolarów Sun Microsystems dostarczy 29,000 systemów komputerowych (stacji roboczych i serwerów), zaś do 2005 roku firma będzie prowadziła serwis techniczny i programowy.

Głównym celem programu CHS-2 jest modyfikacja obecnych wersji systemów dowodzenia i kierowania w wojskach lądowych Stanów Zjednoczonych. Systemy te koordynują działanie wywiadu wojskowego, przemieszczanie jednostek, artylerii, zaopatrzenia i obrony przeciwlotniczej. System obejmuje następujące składniki: System Kontroli Manewrów, System Danych Taktycznych dla Artylerii, System Wszechstronnej Analizy, System Logistyczny i Zaopatrzenia, System Obrony Powietrznej. Każdy z systemów musi na bieżąco komunikować się z czterema pozostałymi, musi także pozwalać na wymianę informacji pomiędzy różnymi rodzajami wojsk.

O wyborze rozwiązań Sun zadecydowały czynniki takie jak otwartość systemów, ich niezawodność, elastyczność i skalowalność umożliwiająca stopniowe dodawanie mocy obliczeniowej w miarę pojawiających się potrzeb.

Program OPUS

System OPUS jest w pełni zgodny z wymaganiami stawianymi przez członków NATO i obejmuje zarządzanie kryzysowe, zarządzanie zasobami obronnymi oraz zapewnia pełną współpracę wielonarodowych sił zbrojnych.

System OPUS został zrealizowany w latach 1990-1993 i obejmuje 18 stanowisk dowodzenia, 350 stacji roboczych, 700 terminali znakowych i 125 stacji graficznych. System służy do zbierania, wymiany i obrazowania informacji na potrzeby dowodzenia wojskami, pozwalając na wymianę ponad 40 typów sformalizowanych meldunków bojowych. OPUS opiera się na architekturze SPARC firmy Sun Microsystems oraz środowisku operacyjnym Sun Solaris.

System umożliwia dostęp do danych za pomocą ujednoliconego środowiska, zaś użytkownicy systemu mogą uruchamiać wszystkie aplikacje z jednego stanowiska pracy. Dzięki możliwości pracy z ogromnymi zestawami danych pochodzącymi z różnych źródeł, system daje użytkownikom kompleksowy, na bieżąco aktualizowany, przegląd sytuacji na danym terenie. Jednocześnie system umożliwia szybką komunikację pomiędzy poszczególnymi centrami dowodzenia w systemie 24-godzinnym. Pozwala to na podejmowanie lepszych decyzji i szybsze wprowadzanie ich w życie.

Program I-CASE

I-CASE (Integrated Computer-Aided Software Engineering Program) pozwala na stworzenie zintegrowanego środowiska inżynierii oprogramowania. System obejmuje szereg narzędzi wspierających produkcję, testowanie, wdrażanie i utrzymanie systemów informatycznych, przy jednoczesnym wspieraniu istniejących systemów opartych na języku COBOL. Tworzenie oprogramowania możliwe jest w grupach inżynierów liczących od 2 do 300 osób.

Dziesięcioletni kontrakt zawarty został w 1990 roku na sumę 1.5 miliarda dolarów. Umożliwia tworzenie wielkich systemów bazujących na języku Ada, udostępniając także narzędzia pozwalające na konfigurowanie, zarządzanie, tworzenie baz danych, testowanie i analizę stworzonych systemów. System ten zdecydowanie obniży koszty tworzenia oprogramowania dla armii.

Narzędzia te dostarczyło ponad 50 znanych światowych producentów, w tym Cayenne Technologies, Informix, Oracle, Sybase, Netscape, NEXT Software, Powersoft, Unife i wiele innych. Wszystkie rozwiązania dostępne są na platformie sprzętowo-programowej firmy Sun Microsystems, która zapewnia znakomite środowisko do tworzenia i integracji złożonych systemów informatycznych.

Program GCCS

Globalny System Dowodzenia i Kierowania (GCCS - Global Command and Control System) daje możliwość uzyskiwania informacji i dowodzenia armią Stanów Zjednoczonych, w dowolnym miejscu na świecie. Infrastruktura GCCS składa się z serwerów UNIXowych Sun Enterprise pracujących w środowisku Solaris i terminali klientów, w tym komputerów PC.

Podstawowe funkcje, jakie umożliwia program GCCS to planowanie kryzysowe, dowodzenie poszczególnymi służbami wojskowymi, wywiad wojskowy, logistyka, wsparcie dla lotnictwa, planowanie działań personelu pomocniczego oraz informacje dodatkowe. Dzięki połączeniu wszystkich tych funkcji na jednej, niezawodnej platformie sprzętowej firmy Sun, stworzony został spójny i efektywny system dowodzenia i kierowania całą armią Stanów Zjednoczonych.

BIURA SPRZEDAŻY W KRAJU:

Sun Microsystems Poland
Ul. Hankiewicza 2
02-103 Warszawa
tel. (+22) 874-78-00
fax. (+22) 658-40-60
WWW:http://www.sun.com.pl
E-mail: info@Poland.Sun.Com

Sun Microsystems Poland Oddział Gliwice
Ul. Kościuszki 22
tel: (+32) 231-82-94
tel/fax: (+32) 231-85-22
WWW:http://www.sun.com.pl
E-mail: info@Poland.Sun.Com

Sun microsystems

DOPIERO SIEĆ TO KOMPUTER

© 1996 Sun Microsystems, Inc. Wszystkie prawa zastrzeżone. Sun, Sun Microsystems, logo Sun, Sun Microsystems Computer Company, The Network is the Computer, SunScreen, Sun Security Manager, Solaris, JavaBeans oraz Java są znakami handlowymi lub zastrzeżonymi znakami handlowymi firmy Sun Microsystems, Inc. w Stanach Zjednoczonych i innych krajach. Wszystkie znaki handlowe SPARC zostały użyte zgodnie z licencją i są znakami handlowymi lub zastrzeżonymi znakami handlowymi SPARC International, Inc. w Stanach Zjednoczonych i innych krajach. Produkty oznaczone znakiem SPARC są oparte na architekturze stworzonej przez firmę Sun Microsystems.

SAS Institute

System SAS
- Informacyjna Architektura Biznesu

SAS Institute, założony w 1976 roku, **należy do grona dziesięciu największych producentów oprogramowania na świecie.** Firma, której dochody za **1998** rok wyniosły **871,4** min. USD, zatrudnia ponad **5000** osób obsługujących **3,5** miliona użytkowników w **120** krajach świata.

SAS Institute od chwili rozpoczęcia działalności **specjalizuje się w rozwijaniu oprogramowania umożliwiajcego dostarczanie informacji**. Obecnie jest ono przede wszystkim wykorzystywane do budowy i eksploatacji systemów typu **Data Warehouse** (Hurtowni Danych), a także jest stosowane w takich dziedzinach jak **wspomaganie podejmowania decyzji, systemy informowania kierownictwa, systemy OLAP, Data Mining**, czy **Business Intelligence**. Rozwój SAS Institute opiera się o stały rozwój technologiczny, na który firma corocznie przeznacza **30-45%** swoich przychodów (trzykrotnie więcej niż średnia w branży oprogramowania). Wszystkie produkty SAS Institute są spójne i wzajemnie się uzupełniają umożliwiając zestawianie systemów o wymaganej przez klientów funkcjonalności.

Oddział **SAS Institute** utworzony w Polsce w 1993 roku **zapewnia wszechstronne wsparcie techniczne i wdrożeniowe** oferowanych produktów, natomiast działające w jego ramach Centrum Szkoleniowe realizuje pełen wachlarz szkoleń z zakresu oprogramowania i metodyki SAS Institute.

Oferta oprogramowania SAS Institute, dopasowana funkcjonalnie i cenowo do potrzeb organizacji dowolnej wielkości, adresowana jest do wszystkich sektorów gospodarki - bankowości, ubezpieczeń, telekomunikacji, energetyki, przemysłu, handlu, uczelni i ośrodków badawczych, instytucji publicznych i wojskowych .

SAS Institute
ul. Jutrzenki 177
02-231 Warszawa

tel.: (22) 873 92 00
fax: (22) 873 92 04

e-mail:polska@spl.sas.com
http: //www.sas.com/poland

SAS Institute

Wybrani użytkownicy Systemu SAS w **amerykańskim sektorze publicznym** i **wojskowym.**

U.S. Department of Agriculture
Agricultural Marketing Service APHIS
Agricultural Research Service
Economic Research Service
Forest Service
National Agricultural Statistics Service
National Computer Center
National Finance Center

U.S. Department of Commerce
Office of the Secretary
Bureau of Census
Bureau of Economic Analysis
Economics & Statistics Administration
International Trade Administration
National Institute of Standards and Technology
National Oceanic and Atmospheric Administration
National Climatic Data Center
National Marine Fisheries Service
Patent and Trademark Office

U.S. Department of Defense
Defense Finance and Accounting Agency
Defence Information Systems Agency
Defence Mapping Agency
Defence Logistics Agency
Defence Information Processing Center
Defence Information Services Organization
Defence Ceeta
Defense Contract Audit Institute
Defense Intelligence Agency
Defence Personnel Support Center
National Imagery and Mapping
National Photographic Interpretation CenterOffice of the Inspector General
Defense Mega Centers ñ
Chambersburg
Huntsville
AIPC
LSSC St. Louis
Rock Island Arsenal
San Diego/DISA
Dayton/Wright
Patterson AFB
McClellan AFB
Warner Robins AFB
Bureau of Naval Personnel Columbus
OCHAMPUS
U.S. Department of the Air Force
Air Force Services Agency
Armstrong Laboratory/Data Services
Brooks AFB
Falcon AFB
Langley AFB
Scott AFB
Tinker AFB
Wright Patterson AFB
HQ Air Force Space Comman
HQ Air Force Personnel Center
HQ National Air Intelligence Center
HQ Strategic Air Command
HQ ACC Directorate of Operations Analysis
HQ Air Force Recruiting Service
HQAAFES
Joint Staff/AFSAA/Sak
Tricare Southwest

USSTRATCOM
U.S. Department of the Army
Brooke Army Medical Center
Cold Regions Test Center
Defense Supply Service
Fitzsimons Army Depot
Army Missile Command
Army Personnel Command
Army Air Defense
Aberdeen Proving Ground
Walter Reed Army Institute of Research
Walter Reed Army Medical Center
William Beaumont Army Medical Center
Army Air Defense Artillery Test Division
Center for Healthcare Education & Studies
Fort Benning
Fort Bragg
Fort Buchanan
Fort Campbell
Fort Carson
Fort Dix
Fort Drum
Fort Gordon
Fort Hood
Fort Huachuca
Fort Knox
Fort Leavenworth Fort Lee
Fort Lewis
Fort McCov
Fort McPherson
Fort Monroe
Fort Polk
Fort Richardson
Fort Riley
Fort Rucker
Fort Sill
Fort Steward SBIS Integration & Test Lab
SBIS Integration Logistic Support
SBIS System Development
Army DCSOPS
Army Healthcare Systems
Army Medical Research and Materials Command
Army Soldier Systems Command
Army Yuma Proving Ground
U.S. Department of the Navy
U.S. Marine Corps
Marine Corps Logistics Base
Join Warfare Analysis Center
Naval Air Warfare Center/Aircraft Division
Naval Facilities Engineering Command
Naval Health Research Center
Naval Inventory Control Point Naval Medical Research Institute
Naval Postgraduate School
Naval Research Lab
Naval Supply Center
Naval Surface Warfare
Naval Undersea Warfare Center
Naval Warfare Assessment Division
Navy Personnel Research & Development Center
Navy Public Works Center
BUMED

U.S. Department of Education
OSERS/RSA
Center for Statistics

U.S. Department of Energy
Bonneville Power Administration
Federal Energy Regulatory Commission
Albuquerque Operations
Pittsburgh Energy Technology Center
Fermilab
Lawrence Livermore National Lab
UC Berkeley Lab
Westinghouse Electric
Westinghouse Savannah River Company

U.S. Department of Health and Human Services
Health Care Financing Administration
ALOSH Computer Center
Bureau of Health Professions
Environmental Management Office
Indian Health Service, OIRM, DDPS
National Cancer Institute
National Center for Toxicological Research
Centers for Disease Control
Food and Drug Administration
National Institutes of Health
Administration for Children and Families

U.S Department of Housing and Urban Development

U.S. Department of the Interior
Bureau of Indian Affairs
Bureau of Land Management
Bureau of Reclamation
Bureau of Mines
Minerals Management Service
U.S. Geological Survey
Fish and Wildlife Service
National Park Service
National Biological Service
National Wetlands Research Center

U.S. Department of Justice
Bureau of Prisons
Administrative Office of the US Courts
Immigration and Naturalization Service
Drug Enforcement Agency
Federal Bureau of Investigation
Civil Rights Division
Federal Bureau of Prisons
US Sentencing Commission

U.S. Department of Labor
Bureau of Labor Statistics
Pension Benefit Guaranty Corporation

U.S. Department of State

U.S. Department of Transportation
U.S. Coast Guard
Federal Aviation Administration
Federal Aviation Administration Technical Center
Transportation Computer Center
Vehicle Research & Test Center

U.S. Department of Treasury
Bureau of Alcohol, Tobacco, and Firearms
Comptroller for the Currency
U.S. Customs Service
Bureau of Engraving and Printing
Financial Management Service
IRS
IRS Data Center
IRS National Computer Center
U.S. Mint
Bureau of the Public Debt
U.S. Secret Service
Office of Lab and Scientific Services
Office of Thirft

Supervision
U.S. Department of Veterans Affairs
Data Processing Center
VA Central Office
Bedford VA Medical Center
Cleveland VA Medical Center
Indianapolis VA Medical Center
NEPEC-VA Medical Center
The Boston Development Center
VA Hines Hospital
VA Hospital National CustomerFeedback Center
VA Medical Center
Health Services Research
Little Rock VA Medical
Veteranis Health Administration
Veteranis Administration
Veteranis Affairs Quality Management Institute
West Haven VA Medical Center
Executive Office of the President
Office of Management and Budget

Independent Agencies
Agency for International Development
Central Intelligence Agency
Commodity Futures Trading Commission
Environmental Protection Agency
Federal Communications Commission
Federal Emergency Management Agency
Federal Deposit Insurance Corporation
Federal Reserve System Board of Governors
Federal Trade Commission
General Accounting Office
Library of Congress
NASA
National Science Foundation
National Transportation Safety Board

Nuclear Regulatory Commission
Office of Personnel Management
Prospective Payment Assessment Commission
Social Security Administration
Smithsonian Institution
Securites and Exchange Commission
Tannessee Valley Authority
U.S. Information Agency
U.S. Agency for International Development
U.S. International Trade Commission
U.S. Postal Service
Postal Rate Commission
U.S. Government Printing Office
U.S. Office of Personnel Management

SPIS TREŚCI

SPIS RYSUNKÓW

SPIS TABEL

Skład komputerowy Wydawcy.
Druk DSG. Zam. 485. 1999


PROKOM
SOFTWARE S.A.


IBM


apeXim
Integrator Systemów Teleinformatycznych


HEWLETT
PACKARD


BE DIRECT
DELL
HOME


SAS
SAS Institute


GRUPA
ComputerLand


COMPAQ


SAP


STER
PROJEKT
Integrator systemów


OPTIMUS SA
INTEGRACJA


Sun
microsystems


atm


CONSORTIA


HOGART


ORACLE


CISCO SYSTEMS
ENABLING THE
INTERNET GENERATION


INFORMIX


UNISYS


BONAIR


decsoft


CABLETRON
SYSTEMS