AKADEMIA OBRONY NARODOWEJ

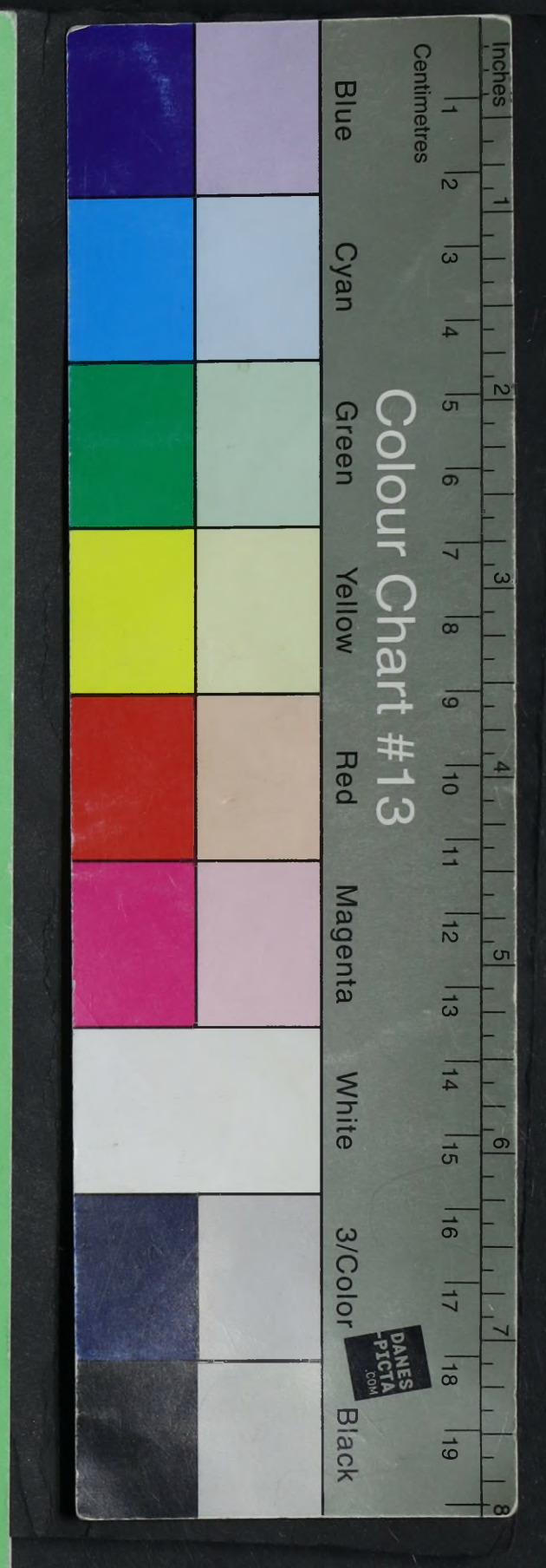
WYDZIAŁ WOJSK LĄDOWYCH
INSTYTUT ZARZĄDZANIA I DOWODZENIA

SYSTEMY TELEINFORMATYCZNE NA POTRZEBY KIEROWANIA REAGOWANIEM KRYZYSOWYM

pk.: „Teleinformatyka – kryzys"

Praca naukowo-badawcza

WARSZAWA



AKADEMIA OBRONY NARODOWEJ

WYDZIAŁ WOJSK LĄDOWYCH
INSTYTUT ZARZĄDZANIA I DOWODZENIA

SYSTEMY TELEINFORMATYCZNE NA POTRZEBY KIEROWANIA REAGOWANIEM KRYZYSOWYM

pk.: „Teleinformatyka - kryzys"

Praca naukowo - badawcza

Warszawa **2007**

Recenzent:

dr hab. inż. Józef JANCZAK

Opracował zespół autorski:

ppłk dr inż. Piotr DELA

- kierownictwo naukowe, nadzór merytoryczny i organizacja pracy zespołu; opracowanie wstępu, rozdziału 2, rozdziału 4, zakończenia

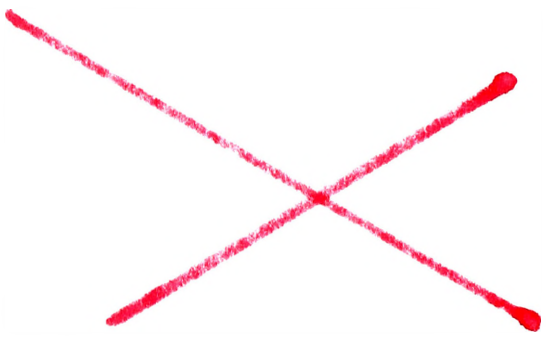
Członkowie:

płk dr inż. Marek STRZODA

- opracowanie rozdziału 1

płk dr inż. Andrzej WISZ

- opracowanie rozdziału 3



Okładka i oprawa: Akademia Obrony Narodowej – Wydział Wydawniczy
00-910 Warszawa, al. gen. A. Chruściela 103, tel.681-40-55, tel./faks 681-37-52

SPIS TREŚCI

WSTĘP

Rozwój ekonomiczny świata, otwarcie rynków i coraz bardziej dynamiczna wymiana towarowa powoduje znaczny wzrost zagrożeń związanych z postępem techniki. Jest to związane m. in. z powszechnym używaniem materiałów i środków zawierających substancje niebezpieczne dla zdrowia i życia ludzkiego. Silna konkurencja na rynkach międzynarodowych wymusza na producentach obniżanie kosztów produkcji poprzez np. redukcję kosztów magazynowania i transportu, a tym samym zmniejszenie wymagań bezpieczeństwa.

Innym rodzajem zagrożenia, coraz bardziej widocznym, jest sam rozwój cywilizacyjny. Gwałtowny wzrost ludności, zwiększenie populacji mieszkającej w miastach oraz uzależnienie ludzi w nich żyjących od dostaw wody, żywności i energii stwarza poważne zagrożenie związane z ewentualnymi awariami infrastruktury technicznej. Nieprawidłowe funkcjonowanie infrastruktury technicznej stanowi realne zagrożenie dla zdrowia i życia ludzkiego.

Coraz bardziej zauważalne są także zaburzenia klimatu powodowane m. in. zjawiskiem globalnego ocieplenia. Gwałtowne zjawiska przyrodnicze takie jak ulewy i huragany stwarzają zagrożenia dla ludzi w miejscach, w których one do tej pory nie występowały.

Innym aspektem powodującym różnego rodzaju zagrożenia są także zachodzące zmiany polityczne i ich wpływ na niezadowolenia grup lub jednostek. Rozwój cywilizacyjny spowodował, że jeden człowiek jest w stanie zagrozić wielu osobom. Duża ilość newralgicznych, z punktu widzenia zdrowia i życia ludzkiego, miejsc jest łatwym celem dla terrorystów. Do miejsc niebezpiecznych można przede wszystkim zaliczyć[1]:

- zakłady i magazyny przechowujące środki toksyczne;
- pojazdy transportujące te substancje;
- urządzenia infrastruktury technicznej i komunalnej, zwłaszcza w dużych miastach;
- ujęcia wody pitnej;
- zbiorniki wodne, tamy;
- laboratoria przechowujące niebezpieczne substancje biologiczne.

[1] Patrz T. Szmidtka, Charakterystyka zagrożeń mogących powodować zaistnienie sytuacji kryzysowych, konferencja naukowa „Łączność w sytuacjach kryzysowych o charakterze niemilitarnym na obszarze kraju, Warszawa, AON 2004

Można zatem stwierdzić, że pomimo coraz doskonalszych systemów zabezpieczeń, wzrasta ilość zagrożeń dla człowieka i jego otoczenia. Można także przypuszczać, że będzie ona zwiększać się coraz bardziej.

Wraz z rozwojem cywilizacyjnym nastąpił szybki rozwój narzędzi i technologii wspomagających człowieka w walce z zagrożeniami. Było to szczególnie widoczne w ostatnich latach XX wieku oraz na początku nowego stulecia, w którym to okresie nastąpił szybki rozwój technologii informatycznych, w tym teleinformatycznych systemów wspomagania zarządzania i dowodzenia. Posiadanie i wykorzystanie odpowiednich narzędzi, zdolnych do przechowywania, przetwarzania i przesyłania danych daje nowe możliwości i wprowadza w każdą działalność człowieka nową jakość. Ich wykorzystanie w kierowaniu reagowaniem kryzysowym przyczyni się do niwelowania skutków potencjalnych zagrożeń i katastrof.

Należy przypuszczać, że siły zbrojne, a w dużej mierze wojska lądowe posiadać będą znaczący udział w zapobieganiu skutkom różnego rodzaju katastrof. Będą one ważnym ogniwem realizującym proces kierowania reagowaniem kryzysowym. Z tego względu muszą być zdolne do realizacji wybranych etapów reagowania kryzysowego przy jednoczesnej możliwości współpracy z organami terenowymi (cywilnym). Z powyższego wynika, że należy podjąć kroki zmierzające do określenia przydatności posiadanych przez wojska lądowe systemów i sieci teleinformatycznych w zakresie kierowania reagowaniem kryzysowym, a także określenie możliwości wykorzystania cywilnych systemów i technologii w zakresie transmisji danych i mowy.

Stan wiedzy w przedstawionym obszarze wytworzył sytuację problemową, której rozwiązania podjął się zespół pracowników Instytutu Zarządzania i Dowodzenia Akademii Obrony Narodowej, rozpoczynając w ten sposób pierwszy etap badań naukowych.

Wyniki badań wstępnych oraz posiadana wiedza pozwoliły zespołowi autorskiemu zdefiniować **cel główny pracy** jako ***identyfikację możliwości i potrzeb wykorzystania systemów teleinformatycznych w procesie kierowania reagowaniem kryzysowym.***

Sformułowanie celu w przedstawionej powyżej postaci skutkowało określeniem szeregu **celów cząstkowych**, mających umożliwić jego osiągnięcie.

Cele cząstkowe:

1. Zidentyfikować uwarunkowania procesu kierowania reagowaniem kryzysowym.
2. Określić wymogi stawiane przed systemami teleinformatycznymi wykorzystywanymi w kierowaniu zarządzaniem kryzysowym.
3. Określić możliwości wykorzystania w procesie kierowania reagowaniem kryzysowym organicznych systemów teleinformatycznych wojsk lądowych.
4. Zidentyfikować możliwości wykorzystania, w procesie kierowania reagowaniem kryzysowym, cywilnych systemów teleinformatycznych przeznaczonych do transmisji danych i mowy.

Na potrzeby procesu badawczego zespół autorski ograniczył obszar badań wyznaczony wymienionymi celami i tematyką pracy do identyfikacji systemów możliwych do wykorzystania w wojskach lądowych.

Podczas dalszych badań, dążąc do osiągnięcia opisanych uprzednio celów, zespół autorski sformułował **główny problem badawczy** w postaci następującego pytania:

Jakie systemy teleinformatyczne są możliwe do wykorzystania w procesie zarządzania reagowaniem kryzysowym. W jakim zakresie można do tego wykorzystać cywilną infrastrukturę teleinformatyczną i organiczne systemy teleinformatyczne wojsk lądowych?

Kolejny etap badań oznaczał dla zespołu autorskiego przeprowadzenie ciągu analiz, porównań i analogii oraz dalsze studiowanie dostępnej literatury przedmiotu. W konsekwencji autorzy utwierdzili się w przekonaniu, iż istnieje konieczność dokonania podziału problemu głównego na szereg mniejszych, bardziej szczegółowych. Tą drogą zidentyfikowano i wyodrębniono następujące **problemy szczegółowe**:

1. Jakie są uwarunkowania procesu kierowania reagowaniem kryzysowym?
2. Jakie wymagania muszą spełniać systemy teleinformatyczne wykorzystywane w kierowaniu zarządzaniem kryzysowym?
3. W jakim zakresie można wykorzystać, w procesie zarządzania reagowaniem kryzysowym, systemy teleinformatyczne wojsk lądowych?

8

4. Jakie cywilne systemy teleinformatyczne można wykorzystać do transmisji danych i mowy w procesie zarządzania reagowaniem kryzysowym?

Wyniki dalszych studiów literatury przedmiotu oraz wnioski z doświadczeń wyniesionych z udziału w różnych ćwiczeniach i pracach badawczych, stanowiły dla zespołu autorskiego podstawę do sformułowania **hipotezy wstępnej**. Bazując na zdobytej wiedzy i wynikach minionego etapu badań, autorzy przyjęli, iż:

Zarządzanie reagowaniem kryzysowym to proces, w którym uczestniczy szereg różnorodnych organów decyzyjnych. Jego prawidłową realizację ułatwiłoby stworzenia (zastosowanie) zautomatyzowanego informatycznego systemu zarządzania. Systemy teleinformatyczne wykorzystywane przez wojska lądowe mogą być w tym procesie wykorzystywane w ograniczonym zakresie. Istniej możliwość wykorzystania cywilnych systemów teleinformatycznych w zakresie transmisji danych i mowy.

Następny etap badań zobligował zespół autorski do zastosowania szeregu metod badawczych zmierzających do rozwiązania zidentyfikowanych uprzednio problemów szczegółowych. Specyfika tych problemów rzutowała bezpośrednio na fakt, iż wśród użytych metod znalazły się głównie metody teoretyczne: analiza, synteza, wnioskowanie, porównanie, analogia oraz uogólnienie.

Analiza zastosowana została przede głównie w badaniach literatury dotyczącej problematyki systemów teleinformatycznych i kierowania reagowaniem kryzysowym w celu identyfikacji stanu obecnego oraz potencjalnych kierunków zmian w rozpatrywanych obszarach. Metoda ta umożliwiła określenie cech, związków i zależności badanych procesów, ze szczególnym uwzględnieniem oddziaływania otoczenia na przedmiot badań.

Syntezie poddane zostały wnioski z badań teoretycznych, które następnie porównywano z przyjętymi założeniami. W związku ze zbiorem szeregu faktów, z pogranicza wielu dziedzin, zastosowanie tego typu metody umożliwiło scalenie uzyskanych w toku badań wyników. Znalazły one swoje odzwierciedlenie w postaci wniosków i propozycji rozwiązań określonych problemów. Syntezą objęto wnioski wynikające z ćwiczeń prowadzonych w zarówno w Akademii Obrony Narodowej jak i jednostkach wojskowych.

W wydobywaniu podobieństw i różnic w rozwiązaniach z zakresu zarządzania informacją szczególnie pomocne było wykorzystanie **porównania**. Zastosowanie tej metody pozwoliło na wyodrębnienie cech wspólnych, różnic i cech charakterystycznych w procesach zachodzących w obiekcie badań. Metodę tę wykorzystano również w czasie interpretacji teoretycznej nowych faktów przez odwołanie się do wiedzy o faktach znanych (teorii), czyli przez konfrontację wiedzy nowej (powstałej z empirii) z wiedzą istniejącą. Ponadto porównanie było pomocne w tych wszystkich momentach prac badawczych, których istotą było identyfikowanie cech wspólnych, podobieństw oraz różnic poszczególnych podmiotów i zagadnień badawczych, a zwłaszcza w zakresie zasad i rozwiązań stosowanych w zarządzaniu.

Uogólnienie wykorzystane zostało w trakcie badań do ujawnienia cech i zjawisk powtarzalnych, a przez to do formułowania zasad uniwersalnych dotyczących wykorzystania systemów teleinformatycznych w reagowaniu kryzysowym. Uogólnienie wiążące się ściśle ze wskazanymi powyżej metodami – pozwoliło również na sformułowanie wniosków wyższego rzędu, wniosków ogólnych.

Ponadto, w ramach metod empirycznych, w celu uzyskania szerszego materiału badawczego, posłużono się metodą obserwacji bezpośredniej i pośredniej, uczestniczącej i zewnętrznej.

Rozwiązywanie problemów szczegółowych powodowało uzyskiwanie kolejnych faktów naukowych. Te zaś z kolei dawały możliwość zweryfikowania hipotezy wstępnej i przedstawienia potencjalnego rozwiązania głównego problemu w postaci **hipotezy roboczej**:

Zarządzanie reagowaniem kryzysowym to proces, w którym uczestniczy szereg różnorodnych organów decyzyjnych. Ich współdziałanie wymaga wymiany dużej ilości informacji. Prawidłową realizację procesu kierowania zarządzaniem kryzysowym ułatwiłoby stworzenie (zastosowanie) zautomatyzowanego informatycznego systemu zarządzania. System ten, bazujący na teleinformatycznej infrastrukturze stacjonarnej, dostarczałby organom decyzyjnym spójnej, wiarygodnej, trwałej i aktualnej informacji oraz udostępniał inne narzędzia automatyzujące pracę.

Należy przypuszczać, że większość systemów teleinformatycznych wojsk lądowych można w procesie kierowania reagowaniem kryzysowym wykorzystać. Jedynie

systemy kierowania środkami walki, ze względu na swoją specyfikę i przeznaczenie, będą w tym zakresie nieprzydatne. Zapewnienie współpracy pomiędzy wojskami lądowymi a organami cywilnymi (terenowymi) realizującymi proces kierowania reagowaniem kryzysowym może odbywać się poprzez wyposażenie organów cywilnych w systemy posiadane przez wojska lądowe, co umożliwi wymianę informacji w ramach zautomatyzowanego systemu dowodzenia.

Większość cywilnych systemów teleinformatycznych może być z powodzeniem wykorzystana do transmisji danych i mowy pomiędzy organami realizującymi proces kierowania reagowaniem kryzysowym. Należy przypuszczać, że duże znaczenie w tej współpracy będą odgrywały systemy: TETRA, telefonia GSM i systemy satelitarne.

Kolejny, czwarty etap badań, polegał na weryfikacji hipotezy w celu jej ostatecznego uzasadnienia i sprawdzenia.

Piąty, ostatni etap prac obejmował podsumowanie wyników badań, ich uogólnienie i syntezę. Zespół autorski przyjął określoną, wiarygodną interpretację rozwiązania problemu badawczego, która przedstawiona została w niniejszym opracowaniu.

Struktura pracy obejmuje wstęp, cztery rozdziały oraz zakończenie.

We **wstępie** zaprezentowano metodologiczne aspekty badań oraz konstrukcję opracowania pisarskiego pracy badawczej. Uzasadniono w nim także wybór tematu i przedstawiono przyjętą procedurę badań.

Rozdział pierwszy obejmuje wyniki badań dotyczących uwarunkowań procesu kierowania reagowaniem kryzysowym.

W **rozdziale drugim** przedstawiono wyniki badań dotyczące wymogów stawianych przed systemami teleinformatycznymi wykorzystywanymi w kierowaniu zarządzaniem kryzysowym.

Rozdział trzeci zawiera rezultaty badań dotyczących możliwości wykorzystania systemów teleinformatycznych wykorzystywanych w wojskach lądowych na potrzeby zarządzania reagowaniem kryzysowym.

Rozdział czwarty stanowi podsumowanie procesu badawczego dotyczącego systemów teleinformatycznych transmitujących dane i mowę, możliwych do wykorzystania w zarządzaniu reagowaniem kryzysowym.

***

Wyniki pracy naukowo-badawczej zawierają propozycje teoretyczne a ich wdrożenie wymaga podjęcia odpowiednich kroków organizacyjno-administracyjnych. Autorzy zamierzają wyniki badań poddać weryfikacji na konferencjach naukowych, sympozjach i seminariach naukowych oraz wykorzystać do opracowania materiałów dydaktycznych na potrzeby AON i innych placówek dydaktycznych sił zbrojnych RP.

1. KIEROWANIE REAGOWANIEM KRYZYSOWYM

Reagowanie kryzysowe odnosi się do sytuacji, w których istnieje zagrożenie bezpieczeństwa ludzi, mienia, środowiska lub infrastruktury określane jako kryzys. Współcześnie kryzys utożsamiany jest praktycznie ze wszystkimi aspektami funkcjonowania człowieka w świecie. Najczęściej postrzegamy go w kontekście różnych aspektów politycznych, w tym zwłaszcza zagrożeń demokracji, integralności terytorialnej, stabilności ekonomicznej, zdrowia i życia ludzi, zachowania dóbr kultury oraz ochrony środowiska naturalnego.

Przeprowadzona analiza literatury wykazała, że istnieje wiele definicji terminu *kryzys*. Jego opisu dokonuje się przez pryzmat dziedziny na potrzeby, której jest formułowana jego definicja. W swojej istocie etymologiczne korzenie terminu sięgają języka greckiego, w którym pojęcie *krisis* oznacza punkt zwrotny, przełomowy, rozstrzygnięcie[1]. Niezależnie od dostrzeganych różnic można wskazać, że dane zjawisko postrzegane jest jako kryzys wtedy, kiedy zaistnieje nagłe, realne i nieakceptowane przez jakiś podmiot zagrożenie jego interesów, celów działania lub bytu, którego skutki przynoszą niepożądane rezultaty. Autorzy jednej z publikacji wskazują, że na zaistnienie kryzysu składają się trzy elementy: presja czasu, ewentualność zasadniczego zagrożenia i zaskoczenie oraz fakt, że jest ono rezultatem zarówno niebezpieczeństwa jak i okoliczności, w jakich ono występuje[2].

W ujęciu bezpieczeństwa narodowego kryzys postrzegany jest szerzej i określany jako: *sytuacja będąca następstwem zagrożenia, prowadząca w konsekwencji do zerwania lub znacznego osłabienia więzi społecznych, przy równoczesnym poważnym zakłóceniu funkcjonowania instytucji publicznych, jednak w takim stopniu, że użyte środki niezbędne do zapewnienia lub przywrócenia bezpieczeństwa nie uzasadniają wprowadzenia żadnego ze stanów nadzwyczajnych przewidzianych w Konstytucji RP*[3].

W prezentowanym ujęciu przyjmuje się, że kryzys jest kategorią **bezpieczeństwa narodowego** i postrzega się go jako:

a) kulminację nagromadzonych zdarzeń, sytuacji, stanów rzeczy (zagrożeń, konfliktów, szans) w różnych dziedzinach życia społecznego, działalności państwa (kilku państw), lub organizacji, krytycznym rezultatem negatywnej działalności człowieka przeciw człowiekowi lub prawom natury, a także zjawisk wynikają-

---

[1] *Słownik wyrazów obcych,* PWN, Warszawa 1980, s. 401.
[2] *Zarządzanie kryzysowe w sytuacji klęski żywiołowej,* Zeszyt Problemowy 1(45)/2006, Towarzystwo Wiedzy Obronnej, Wyd. Elipsa, Warszawa 2006, s. 25.
[3] *Słownik terminów z zakresu bezpieczeństwa narodowego,* AON, Warszawa 2002, s. 61.

13

cych z działania sił natury lub awarii technicznych, którym przeciwdziałanie przekracza możliwości rutynowych działań służb ratowniczych i innych podmiotów;

b) sytuację niekorzystną, poważne załamanie, wzrost napięcia, nagłe i gwałtowne przesilenie, moment przełomu ku złemu lub lepszemu;
c) punkt zwrotny dla stanu normalnego lub innego stanu kryzysowego;
d) jakościową zmianę systemową w funkcjonowaniu jakiegoś podmiotu (systemu, organizacji, instytucji, państwa itd.);
e) szczególny splot okoliczności z zakresu zagrożeń i szans w dziedzinie bezpieczeństwa, w tym bezpieczeństwa narodowego.

Rozwinięciem powyższych odniesień jest wskazanie, że kryzys generuje **sytuacje kryzysowe,** czyli jest to (w ujęciu systemowym) sytuacja systemu charakteryzująca się kulminacją zagrożeń wewnętrznych lub/i zewnętrznych powodujących utratę normalności i możliwość zakłócenia podstawowych cech systemowych, np. stabilności, równowagi, sterowalności, efektywności itp.[4] W ujęciu bezpieczeństwa narodowego w definicji sytuacji kryzysowej wskazuje się, że jest to stan narastającej destabilizacji, niepewności i napięcia społecznego, charakteryzujący się naruszeniem więzi społecznych, możliwością utraty kontroli nad przebiegiem wydarzeń oraz eskalacji zagrożenia, a w szczególności jest to sytuacja stwarzająca zagrożenie dla życia, zdrowia, mienia, dziedzictwa kulturowego lub infrastruktury krytycznej, w tym spowodowana zdarzeniami terrorystycznymi. Stan taki powoduje także intensywne, trwałe i długofalowe pogorszenie funkcjonowania społeczeństwa i państwa. Charakteryzuje się eskalacją zagrożenia, utratą kontroli nad ograniczaniem skutków zdarzenia (sytuacji kryzysowej) przez poszczególne służby, inspekcje lub straże. Sytuacja taka, może również, powodować ujemne skutki w gospodarce, a także może mieć wpływ na stosunki zagraniczne.

W odniesieniu do powyższych charakterystyk można przyjąć, że **reagowanie kryzysowe** – to bieżące działania służb ratowniczych na wszelkie zdarzenia - zagrażające zdrowiu i życiu obywateli lub środowisku - zmierzające do ograniczenia lub zlikwidowania ich skutków oraz niesienia pomocy poszkodowanym.

Zarządzanie kryzysowe, jest to natomiast uporządkowana działalność polegającą na zapobieganiu sytuacjom kryzysowym lub przejmowaniu nad nimi kontroli i kształtowaniu ich przebiegu w drodze zaplanowanych działań oraz na odtworzeniu zasobów lub przywróceniu im ich pierwotnego charakteru.

---

[4] P. Sienkiewicz, P. Górny, *Analiza systemowa sytuacji kryzysowej*, Zeszyty Naukowe AON nr 1 4(45), Warszawa 2001, s. 31.

Przeprowadzony proces badawczy wykazał, że kwestie związane z reagowaniem na kryzys oraz kierowanie reagowaniem kryzysowym regulują różne akty normatywne, np.:

- Ustawa z dnia 21 czerwca 2002 roku *o stanie wyjątkowym* (Dz.U. Nr 113, poz. 985, Nr 153, poz. 1271 i z 2006 r. Nr 104, poz. 711);
- Ustawa z dnia 18 kwietnia 2002 r. *o stanie klęski żywiołowej* (Dz. U. z dnia 22 maja 2002 r.);
- Ustawa z dnia 8 września 2006 roku *o Państwowym Ratownictwie Medycznym* (Dz. U. Nr 191, poz. 1410).

Zasadniczym zaś dokumentem w tym zakresie jest **Ustawa z dnia 26 kwietnia 2007 r. *o zarządzaniu kryzysowym* (Dz. U. Nr 89, poz. 590).** Dokument ten wskazuje organy właściwe w sprawach zarządzania kryzysowego oraz ich zadania i zasady działania, a także zasady finansowania zadań zarządzania kryzysowego.

Zapisy tej ustawy określają także istotę **zarządzania kryzysowego** jako działalności organów administracji publicznej, będącej elementem kierowania bezpieczeństwem narodowym, która polega na zapobieganiu sytuacjom kryzysowym, przygotowaniu do przejmowania nad nimi kontroli na drodze zaplanowanych działań, reagowaniu w przypadku występowania sytuacji kryzysowych oraz na odtworzeniu infrastruktury lub przywróceniu jej pierwotnego charakteru[5].

Wskazane powyżej wyznaczniki kryzysu zdeterminowały kierunki badań w odniesieniu do głównego problemu badawczego. Wskazując na potrzeby systemów teleinformatycznych wspierających kierowanie reagowaniem kryzysowym w tej części procesu badawczego poszukiwano odpowiedzi na następujące problemy cząstkowe:

- *Jakie zagrożenia stwarzać będą wymagania architektury oraz warunki działania systemów informatycznych wspierających kierowanie?*
- *Jakie założenia, zasady, struktury oraz procedury wpływają na konfigurację oraz zasady wykorzystania systemów teleinformatycznych na potrzeby reagowania kryzysowego.*

Wyniki prowadzonych badań zawarto w kolejnych podrozdziałach, w których przedstawiono zasadnicze aspekty badań, ich wyniki, a przede wszystkim wnioski będące podstawą kreowania założeń, zasad oraz kształtu systemu informatycznego wspomagającego kierowanie reagowaniem kryzysowym. Dokonano także uogólnienia poszczególnych kwestii merytorycznych oraz przedstawiono je w formie wniosków w zakończeniu niniejszego rozdziału.

---

[5] Ustawa z dnia 26 kwietnia 2007 r. *o zarządzaniu kryzysowym* (Dz. U. Nr 89, poz. 590), art. 2.

1.1. Determinanty kierowania w sytuacjach kryzysowych

Teoria i praktyka działań w sytuacjach kryzysowych wykazały, że implikacją ich podejmowania jest sytuacja, która odbiega w sposób znaczący od tej, jaką określa się za normalną. Reagowanie kryzysowe jest formą działania inicjowanego zdarzeniami, które niosą z sobą zagrożenia dla życia ludzkiego lub środowiska naturalnego. W potocznym rozumieniu pojęcie *zagrożenie* rozumiane jest jako zapowiedź czegoś złego, groźba, stan niebezpieczny, stan groźny dla kogoś lub czegoś[6]. W szerszym ujęciu, a zwłaszcza w ujęciu bezpieczeństwa narodowego, postrzega się je jako zdarzenie, wywołane celowo lub losowo, które wywiera negatywny wpływ na funkcjonowanie politycznych i gospodarczych struktur państwa, na warunki bytowania ludności oraz stan środowiska naturalnego.

W ujęciu dokumentów normatywnych szczególną uwagę zwrócić należy w odniesieniu do **infrastruktury krytycznej**, poprzez którą rozumie się systemy oraz wchodzące w ich skład powiązane ze sobą funkcjonalnie obiekty, w tym obiekty budowlane, urządzenia, instalacje, usługi kluczowe dla bezpieczeństwa państwa i jego obywateli oraz służące zapewnieniu sprawnego funkcjonowania organów administracji publicznej, a także instytucji i przedsiębiorców[7]. Infrastruktura krytyczna obejmuje systemy:

1. Zaopatrzenia w energię i paliwa.
2. Łączności i sieci teleinformatycznych.
3. Finansowe.
4. Zaopatrzenia w żywność i wodę.
5. Ochrony zdrowia.
6. Transportowe i komunikacyjne.
7. Ratownicze.
8. Zapewniające ciągłość funkcjonowania administracji publicznej.
9. Produkcji, składowania, przechowywania i stosowania substancji chemicznych i promieniotwórczych, w tym rurociągi substancji niebezpiecznych.

Analiza literatury wykazała, że wyróżnia się najczęściej cztery grupy zagrożeń mogących w szybkim tempie doprowadzić do powstania sytuacji kryzysowych, mających wpływ na bezpieczeństwo i funkcjonowanie całego państwa lub jego poszczególnych regionów[8].

Ze względu na źródło zagrożeń podzielono je na cztery zasadnicze grupy:

---

[6] *Słownik języka polskiego*, t. 3, PWN, Warszawa 1998, s. 847.
[7] Ustawa z dnia 26 kwietnia 2007 r. *o zarządzaniu kryzysowym* (Dz. U. Nr 89, poz. 590), art. 3, ust.2.
[8] *Wizja sił zbrojnych,* Materiały z konferencji naukowej pod red. J. Kręcikija, BBN, Warszawa 2007.

1. **Zagrożenia naturalne** (wszelkie groźne zjawiska związane ze środowiskiem naturalnym).
2. **Zagrożenia techniczne** (związane z cywilizacyjnym i gospodarczym rozwojem społeczeństw).
3. **Terroryzm** (z powietrza, na morzu i na lądzie). Ze względu na rodzaj zastosowanego środka terroru na biologiczny, chemiczny, radiologiczny i informatyczny.
4. **Inne zagrożenia**, a przede wszystkim te związane z:
   - zasobami broni chemicznej i biologicznej przede wszystkim w krajach o nieustabilizowanej sytuacji politycznej;
   - niekontrolowanym przepływem broni masowego niszczenia i komponentów do jej wytwarzania, w tym substancji radioaktywnych;
   - międzynarodowym terroryzmem, sabotażem, kidnapingiem, narkomanią, zorganizowaną przestępczością itd.;
   - dużą liczbą konfliktów lokalnych o zróżnicowanym podłożu (fundamentalizm, nacjonalizm, wojny religijne);
   - niekontrolowaną i nielegalną imigracją;
   - starzejącym się arsenałem jądrowym i zawodnymi systemami ostrzegania.

1.1.1. Zagrożenia naturalne

Wśród zagrożeń powodowanych destrukcyjnym oddziaływaniem sił natury największe niebezpieczeństwo na obszarze kraju stwarzają **powodzie**.

Powódź, jest to wezbranie wody w rzekach, strugach, strumieniach, zbiornikach wodnych, kanałach lub na morzu, podczas którego woda „po wystąpieniu z brzegów" zalewa doliny rzeczne, albo doliny depresyjne i powoduje zagrożenie dla ludzi lub mienia. Powodzie mogą występować w okresie wiosennym (powodzie roztopowe, które mogą być spotęgowane zatorami lodowymi) jak również latem wskutek długotrwałych lub bardzo obfitych opadów deszczu. Powódź - wezbranie wód rzecznych, które prowadzi do szkód gospodarczych, strat w ludziach czy też strat moralnych. Wielkość powodzi określa się w 3-stopniowej skali: małe - o zasięgu lokalnym, średnie - o zasięgu regionalnym, nie mają wpływu na funkcjonowanie państwa, duże - o zasięgu krajowym, mają charakter klęski żywiołowej, zakłócają normalne funkcjonowanie państwa lub jego dużej części, istnieje wtedy konieczność pomocy międzynarodowej.

Powodzie są naturalnymi zjawiskami przyrodniczymi, charakteryzującymi się dużym działaniem destrukcyjnym w środowisku naturalnym. Trwają one długo na znacznym obszarze i wymagają znaczących sił i środków do prowadzenia akcji przeciwpowodziowych i przywrócenia środowiska do stanu pierwotnego. Powodzie występują cyklicznie podobnie jak większość zjawisk meteorologiczno-hydrologicznych[9]. Okresowo przybierają one katastrofalne rozmiary.

Zagrożeniem powodziowym objętych jest w Polsce około 2 miliony hektarów, co stanowi 7% powierzchni kraju. Ponadto, spośród istniejących w naszym kraju kilkudziesięciu sztucznych zbiorników wody, ponad 30 kwalifikowanych jest jako groźne w przypadku awarii urządzeń piętrzących. Katastrofalnym zatopieniem w takim przypadku zagrożony jest obszar o łącznej powierzchni, około 2,9 tys. km^2, na którym zamieszkuje około 700 tysięcy osób.

„Na terenie kraju istnieje 61 budowli hydrotechnicznych spiętrzających wodę, których funkcjonowanie niesie za sobą bardzo duże zagrożenia dla obszarów położonych poniżej zapory. Zagrożenie wynika z możliwości zerwania (pęknięcia) zapory jak i przelania się wody przez koronę zapory na skutek gwałtownej fali powodziowej. Potencjalnie duże zagrożenie mają te zapory, które piętrzą wodę na wysokość 5 m ponad zabudowany teren lub trwale spiętrzają wodę w zbiornikach, jeziorach lub stawach powyżej 1 mln m^3. Łącznie katastrofalnymi zatopieniami zagrożony jest obszar ponad 1,5 tys. km^2 zamieszkały przez około 1 mln osób. Na obszarze tym rozmieszczonych jest ponad 40 miast i osiedli oraz 150 zakładów pracy”[10].

Ochrona przed powodzią należy zarówno do zadań administracji rządowej, jak i samorządowej, które mają obowiązek podejmowania i realizacji – w ramach planowej gospodarki wodnej – przedsięwzięć inwestycyjnych oraz innych działań niezbędnych do zwiększenia stopnia zabezpieczenia ludności i gospodarki narodowej przed powodzią. Do przedsięwzięć tych należy przede wszystkim: modernizacja istniejących i budowa nowych wałów przeciwpowodziowych; budowa zbiorników retencyjnych; regulacja rzek i zabudowa potoków górskich oraz łamanie lodu na większych rzekach, które ułatwiają spływ wielkich wód i lodów.

---

[9] *Raport o stanie zagospodarowania przestrzennego, Instytut Gospodarki przestrzennej i komunalnej*, oprac. zbiorowe, Warszawa 2000.

[10] J.Prońko, *System kierowania reagowaniem kryzysowym w sytuacjach nadzwyczajnych zagrożeń dla ludzi i środowiska,* rozprawa doktorska, AON, Warszawa 2001.

Kolejnym zagrożeniem, które związane jest ze zjawiskiem powodzi są **potoki błotno-rumowiskowe.** Jest to strumień kształtujący się nagle w korytach górskich rzek, odznaczający się dużą (od 10 do 75%) zawartością ciał stałych (produktów erozji skał) i przyczyniający się do gwałtownego wzrostu poziomu wody.

Potok błotno-rumowiskowy powstaje pod wpływem obfitych i długotrwałych opadów deszczu, burzliwego topnienia lodowców lub sezonowej pokrywy śnieżnej, a także obsunięcia się do koryt rzek znacznych ilości gruzu i bloków skalnych.

W odróżnieniu od potoków zwykłych, potok błotno-rumowiskowy nie spływa w sposób ciągły, lecz kolejnymi falami. Jednorazowa objętość rumowiska niesionego przez taki potok dochodzi do setek tysięcy, czasami nawet milionów metrów sześciennych, przy czym rozmiary przenoszonych bloków skalnych mogą osiągnąć rozmiary 3-4 m średnicy i wagi 100-200 ton. Ze względu na olbrzymią masę i prędkość, potok błotno-rumowiskowy niszczy drogi, urządzenia, grunty orne itp.

Niszczącą siłę potoku błotno-rumowiskowego potęguje jego znaczna zdolność transportowa oraz niezwykła wartkość. Zazwyczaj potok błotno- rumowiskowy spływa kilkoma falami, przy czym jego prędkość dochodzi do około 15 km/h. Napotykając przeszkody pokonuje je, co nie przyczynia się do obniżania jego energii, a wręcz przeciwnie – do jej wzrostu.

Naturalne warunki rejonów górskich sprzyjają znacznemu powierzchniowemu spływowi wód i kształtowaniu się niszczących potoków błotno-rumowiskowych. Ponadto, w ostatnich latach, ma miejsce intensywna eksploatacja stoków górskich, w wyniku, której wzrasta częstotliwość pojawiania się potoków błotno-rumowiskowych, rumowiskowych, a także zwiększają się zarówno ich rozmiary, jak i obszar, na którym one występują.

Kolejne zagrożenie ze strony sił przyrody stanowią **silne wiatry**. Ocenia się, że na terenie Polski istniej małe prawdopodobieństwo powstania huraganów, lecz należy liczyć się z zagrożeniami powodowanymi silnymi wichurami, których prędkość przekraczać może nawet 100 km/godz.

Duża prędkość wiatru w wielu przypadkach stanowi zagrożenie dla życia ludzi, a także dla pewnych elementów infrastruktury technicznej. Głównymi skutkami silnej wichury są: powalone drzewa, zerwane trakcje energetyczne, uszkodzone budynki, uszkodzone pojazdy. Zdarzenia te mogą powodować przerwy w dostawach energii i wody, zakłócenia komunikacyjne, a także przerwanie łączności telefonicznej. W szczególnych przypadkach, „wtórne" skutki wichur (spadające przedmioty, walące drzewa, przewody energetyczne itp.) mogą po-

ważnie zagrozić życiu ludności znajdującej się na obszarze, który został objęty działaniem wichury.

W ostatnich latach nasiliły się zjawiska związane z powstawaniem lokalnych trąb powietrznych. Trudno jest określić obszary zagrożeń związanych z silnymi wiatrami. Zjawiska te praktycznie mogą pojawić się w każdej części kraju i to na znacznych przestrzeniach. Zminimalizowanie skutków wichury (huraganu) możliwe jest w znacznej mierze dzięki wcześniejszemu informowaniu o właściwych sposobach zachowania się w rejonie zagrożonym i podjęciu działań profilaktycznych.

Nowe jakościowo zagrożenia i powstające w związku z tym problemy niesie ze sobą występowanie **suszy.** Jest to długotrwały okres z brakiem opadów atmosferycznych lub nieznacznym opadem w stosunku do średnich wieloletnich wartości. Powoduje przesuszenie gleby, zmniejszenie lub całkowite zniszczenie upraw roślin alimentacyjnych (a co za tym idzie klęski głodu), zmniejszenie zasobów wody pitnej, a także zwiększone prawdopodobieństwo katastrofalnych pożarów. Występujący w takich sytuacjach zanik wilgotności lasów powoduje podwyższenie prawdopodobieństwa pożaru tych terenów. Takie zjawiska występują praktycznie corocznie, a w Polsce z całą gwałtownością w latach 1992 i 1994.

Przeprowadzona analiza zagrożeń wykazała, że współczesne **zagrożenia ekologiczne** naszego kraju wynikają w znacznej mierze z dużego prawdopodobieństwa załamania się bilansu wodnego oraz przekroczenia dopuszczalnych norm zanieczyszczenia wód i gleby. Objawem ujemnego bilansu wodnego jest obniżenie się w Polsce średniego poziomu wód gruntowych o 1,5 m. Wynika to z nierównomierności poziomu opadów i braku systemu magazynowania wód powierzchniowych. Polska pod względem zasobów wody już teraz zajmuje ostatnie miejsce w Europie. Niewielkie ilości wód powierzchniowych są na domiar złego zanieczyszczane przez przemysł, rolnictwo i ścieki miejskie.

W polskiej strefie klimatycznej, zjawisko długotrwałej i powszechnej suszy występowało sporadycznie i z reguły nie stanowi zagrożenia dla zdrowia i życia. Dotyczy ono jednak poszczególnych regionów, w których może być przyczyną strat materialnych, głównie w rolnictwie. Susze meteorologiczne w głównej mierze związane są z niskim poziomem opadów deszczu w dłuższym czasie. Odczuwalne są już okresy kilkutygodniowego braku opadu deszczu. Susze meteorologiczne są źródłem powstania m. in. suszy „hydrologicznej" i „ rolniczej".

Susze hydrologiczne związane są z występowaniem niedostatecznej ilością wody lub z całkowitym jej brakiem w ujęciach wodnych, rzekach, wodach gruntowych i studniach. W tym czasie może zaistnieć konieczność ograniczenia zużycia wody w aglomeracjach miej-

skich, przedsiębiorstwach i obiektach użytku publicznego. Z reguły, susza hydrologiczna jest skutkiem długotrwałej suszy meteorologicznej.

Kolejnym zagrożeniem naturalnym są **ruchy tektoniczne**, które są przyczyną 90% wszystkich trzęsień ziemi. Przez pojęcie trzęsienia ziemi rozumie się wstrząsy podziemne oraz drgania powierzchni ziemi spowodowane przyczynami naturalnymi (procesami tektonicznym, wybuchami wulkanów tzw. ruchami zapadowymi). Obszar, na którym powstaje wstrząs podziemny – ognisko trzęsienia ziemi – stanowi pewien wycinek skorupy ziemskiej, w którym zachodzi proces wyzwalania się energii nagromadzonej w dłuższym okresie. W centrum ogniska wyznacza się punkt, umownie zwany hipocentrum. Rzut hipocentrum na powierzchnię ziemi nosi nazwę epicentrum. Dawniej sądzono, że wszystkie trzęsienia ziemi powstają wyłącznie w skorupie ziemskiej. Obecnie wiadomo, że źródłem większości trzęsień jest płaszcz ziemi, którego konsystencja jest stała, a grubość wynosi 2900 km. Pod wpływem olbrzymich ciśnień lub podziemnych wybuchów w płaszczu ziemi powstają naprężenia powodujące trzęsienia ziemi, wyrażające się we wstrząsach podziemnych i drganiach powierzchni ziemi.

Na terenie Polski istnieje małe prawdopodobieństwo wystąpienia trzęsienia ziemi, tym niemniej zdarzało się odczuwać na pewnych terenach skutki silnych trzęsień, mających epicentrum w innych rejonach Europy. Pewnym zagrożeniem są także tzw. **trzęsienia ziemi zapadowe**, związane z osiadaniem wyrobisk górniczych – tąpnięć. Zagrożenie tego typu dotyczy przede wszystkim Górnego Śląska. Realne jest również zaistnienie w naszym kraju zagrożeń wynikających z wystąpieniem osuwisk i zapadlisk w terenie lessowym i krasowym oraz erozji brzegu morskiego. W ostatnich latach stwierdzono na terenie naszego państwa 12 tysięcy osuwisk, z czego 3 tysiące zagraża różnym obiektom budowlanym, a także szlakom komunikacyjnym. W miastach położonych na gruntach lessowych (np. Kłodzko, Lublin, Sandomierz, Jarosław, Zamość) zdarzały się katastrofy budowlane, będące wynikiem złej gospodarki wodnej. Na obszarach krasowych, obejmujących głównie tereny Jury Krakowsko-Częstochowskiej, Wyżyny Lubelskiej, Niecki Nidziańskiej i Zagłębia Górnośląskiego, występuje zagrożenie zapadliskami krasowymi.

Polskie warunki klimatyczne powodują także, że istotnym zagrożeniem może być występowanie **śnieżyc**, **zasp śnieżnych** i **oblodzenia**. Zaspy śnieżne zakłócają działalność transportu, gospodarki komunalno-energetycznej i łączności oraz znacznie utrudniają prace w gospodarstwach rolnych. Szczególnie niebezpieczne są zaspy śnieżne powstające w wyniku „zejścia z gór" lawin śnieżnych, osuwisk lub lawin błotnych lub kamiennych. Dysponując dużą siłą niszczycielską, lawina śnieżna może wyrządzić znaczne szkody w urządzeniach

przemysłowych, hydrotechnicznych, w liniach kolejowych i układzie dróg, w elektrycznych liniach przesyłowych i liniach łączności, budynkach mieszkalnych i publicznych.

Gwałtowne skoki temperatury powodują natomiast oblodzenia, polegające na pokryciu powierzchni konstrukcji i przedmiotów warstwą lodu lub mokrego śniegu. Odróżnia się następujące rodzaje oblodzeń: gołoledź, szadź oraz osady mokrego i zmarzniętego śniegu.

Ze względu na skutki, zaspy śnieżne i oblodzenia można podzielić na dwie grupy:

- do pierwszej grupy zalicza się wielkie zaspy śnieżne i oblodzenia, na skutek których następuje przerwanie dostawy energii elektrycznej i łączności telegraficzno- telefonicznej na dłuższy okres i na dużym obszarze, przerwanie ruchu kołowego na drogach, zakłócenie ruchu kolejowego oraz przerwanie pracy w wielu zakładach przemysłowych;
- do drugiej grupy zalicza się mniejsze zaspy śnieżne i oblodzenia, które powodują zakłócenia w dostawach energii elektrycznej, krótkotrwałe przerwy w łączności telegraficzno – telefonicznej oraz niewielkie zakłócenia w ruchu samochodowym.

Kolejnym istotnym zagrożeniem jest **epidemia**, czyli masowe szerzenie się określonej choroby, zwłaszcza zakaźnej, w zbiorowisku ludzkim na określonym obszarze. Mogą być one skutkiem zdarzeń katastrofalnych (np. powodzie, susze) jak i rozpowszechniania się chorób w określonych przedziałach czasowych (np. grypa) lub chorób wynikających z niezachowania ostrożności czy wymogów higienicznych.

W praktyce rozróżniamy dwa rodzaje rozprzestrzeniania się epidemii:

- z tzw. źródła punktowego (np. studnie, produkty spożywcze)
- poprzez kontakty osobiste

W zależności od rodzaju epidemii oraz jej rozległości mogą być podjęte różne działania, począwszy od obowiązkowych szczepień, skończywszy zaś na czasowej izolacji dużych grup ludzi, czy wydaniu zakazu wstępu na obszary objęte epidemią. W szczególnych przypadkach, mogą być również określone zasady zachowania się lub ograniczenia przebywania w zagrożonych rejonach.

Na terenie naszego kraju głównymi przyczynami epidemii mogą być choroby: „okresowe" (np. grypa), choroby związane z turystyką (np. cholera), a także zdarzenia kryzysowe (np. powodzie), powodujące efekt „wtórny" w postaci epidemii.

Niebezpieczne dla ludzi oraz środowiska naturalnego są także wszelkiego rodzaju **plagi zwierzęce**. Praktyka wskazuje, że mogą one występować okresowo, w zależności od pory roku. W warunkach normalnych, na pewnych obszarach i w określonych porach roku należy się liczyć ze znaczną dokuczliwością komarów. Po klęskach żywiołowych, głównie

podwoziach, można spodziewać się znacznej ilości szczurów, które wychodzą na powierzchnię. Zarówno w pierwszym jak i drugim przypadku, należy liczyć się z potencjalnym zagrożeniem roznoszenia chorób, stąd konieczność podjęcia działań zmniejszających ilość owadów czy gryzoni. Po powodzi we Wrocławiu podjęto działania mające na celu „odkomarzanie" tego miasta. Oczywiście, działania te muszą być rozpoczęte w odpowiednim okresie (tak, aby na przykład umożliwić likwidację larw), środkami nieszkodliwymi dla ludzi i zwierząt. Rejony objęte „odkomarzaniem" muszą być ściśle określone i podane do publicznej wiadomości. „Odkomarzanie" może być realizowane z powietrza oraz lądu. Wymaga ono dobrej organizacji i znajomości terenu, jego infrastruktury oraz rodzaju zagospodarowania.

1.1.2. Zagrożenia techniczne

Pierwszą kategorią zagrożeń technicznych są uwarunkowane różnymi przyczynami **pożary**. Ocenia się, że 80% wszystkich pożarów powstaje z winy człowieka, a najczęstszymi przyczynami ich powstawania jest: nieprzestrzeganie przepisów przeciwpożarowych podczas obchodzenia się z ogniem w miejscach pracy i wypoczynku, używania niesprawnego sprzętu, wypalania traw, a także podpaleń i sabotaży. W czasie burz lasy zapalają się od piorunów, najczęściej zaś palą się przy niesprzyjających warunkach atmosferycznych (wysoka temperatura powietrza, długotrwała susza).

Pożary lasów, których powierzchnia przekracza 2 km^2 oceniane są jako pożary wielkie. Zazwyczaj wybuchają one w okresie największego zagrożenia pożarowego w lasach.

Konsekwencją burzliwego rozwoju przemysłu chemicznego na świecie było pojawienie się nowej kategorii zagrożeń dla człowieka i środowiska – **toksycznych środków przemysłowych** oraz zagrożeń, jakich za sobą niosą **awarie chemiczne**[11]. Toksyczne środki przemysłowe są to gazy, ciecze i ciał stałe produkowane, przechowywane lub przewożone w celu zabezpieczenia i utrzymania produkcji wyrobów niezbędnych dla społeczeństwa. Ich właściwości chemiczno-fizyczne stwarzają jednak zagrożenie dla środowiska, roślin i zwierząt. Stosuje się je w bardzo wielu gałęziach przemysłu, np.: gumowym, celulozowo-papierniczym, metalurgicznym, a także przy produkcji nawozów sztucznych, farb i lakierów. W przypadku wydostania się tych środków, najczęściej wysokotoksycznych związków chemicznych, ze zbiorników, cystern lub aparatury technologicznej mogą powstawać zagrożenia dla ludzi i środowiska, mające często charakter katastrofy ekologicznej.

---

[11] P. Tyrała, *Zarządzanie kryzysowe. Ryzyko-bezpieczeństwo-obronność*, Wyd. Adam Marszałek Toruń 2001.

22

Wyciek substancji toksycznych do środowiska może nastąpić w wyniku awarii produkcyjnej, zniszczenia zakładu, zniszczenia zbiornika lub podczas transportu.

Analiza zagrożeń technicznych wykazała, że wraz ze wzrostem ilości środków komunikacji coraz większym źródłem zagrożeń jest transport substancji toksycznych związany z dostawą surowców do zakładów chemicznych, tranzytem oraz eksportem.

Na ryzyko wystąpienia skażenia chemicznego podczas transportu składa się wiele czynników. Najważniejsze z nich to:

- ilość transportów;
- stan techniczny pojazdów przewożących substancje toksyczne;
- brak wydzielonych i oznakowanych tras przewozów materiałów niebezpiecznych, w szczególności obwodnic w większości polskich miast;
- nieprzewidywalność miejsca awarii;
- brak monitoringu transportu;
- nieprzestrzeganie przez przewoźników przepisów związanych z bezpieczeństwem.

Ocenia się, że najpoważniejsze zagrożenie stanowi transport substancji niebezpiecznych w ruchu drogowym. Wynika to głównie z:

- dużej ilości substancji przewożonych w ten sposób;
- dużej różnorodności substancji niebezpiecznych przewożonych za pomocą transportu drogowego w porównaniu z transportem kolejowym;
- braku wyznaczonych i oznakowanych tras oraz skutecznej ich kontroli;
- złego stanu technicznego środków transportu drogowego;
- nieprzestrzegania przepisów o przewozie materiałów niebezpiecznych;
- dużego zagrożenia kolizjami na drogach;
- braku świadomości spedytorów i przewoźników o skutkach występujących zagrożeń;
- bardzo dużej szarej strefy przewozów tzn. transportu z zatajeniem przez przewoźnika zagrożenia wynikającego z właściwości przewożonego materiału;
- braku monitoringu transportu.

Mniejszym źródłem zagrożeń są natomiast przewozy substancji chemicznych transportem kolejowym. Ładunki niebezpieczne stanowią 8% przewozów kolei. W sieci PKP porusza się około 24 tys. cystern polskich oraz 6 tys. zagranicznych realizujących rocznie ok. 350 tys. przewozów materiałów niebezpiecznych. Roczny obrót substancjami niebezpiecznymi to ok. 14 mln ton, z czego 700 tys. ton to materiały o szczególnie groźnych właściwościach. Wypadki i awarie mogą zdarzyć się w każdym miejscu, gdzie przebiega szlak kolejowy. Niejednokrotnie transport materiałów niebezpiecznych odbywa się przez gęsto zaludnio-

ne tereny, a już paradoksem jest przewóz tych materiałów przez dworce pasażerskie. Substancje, których nie podejmuje się przewozić kolej, przewożone są transportem drogowym.

Zagrożeniem jest także transport morski środków niebezpiecznych. Odbywa się on po wyznaczonych trasach i jest kierowany głównie przez trzy porty: Świnoujście, Gdynia i Gdańsk. Transport materiałów ciekłych w większości dotyczy związków ropopochodnych, których w roku jest około kilkuset tysięcy ton. Poszczególne transporty sięgające kilku tysięcy ton dotyczą przewozów zarówno w zbiornikach, jak i w kontenerach.

Inne zagrożenia związane z transportem dotyczą głównie gazu ziemnego, ropy naftowej i jej produktów stanowi transport rurociągowy. W porównaniu z innymi sposobami transportu, zagrożenie w tym przypadku wynika głównie z bardzo dużej ilości substancji przesyłanych pod ciśnieniem sięgającym nawet kilkudziesięciu atmosfer. Wynikiem każdej awarii jest ogromna skala zanieczyszczeń środowiska. Zagrożenie to potęguje się w miejscach przechodzenia rurociągów przez rzeki. Realnie możliwe są awarie przyczyniające się do wycieku do środowiska od kilku do kilkunastu tysięcy ton związków ropopochodnych. Wydostania się znacznych ilości substancji niebezpiecznych do dużych rzek może spowodować ich skażenie na odcinkach przekraczających 100 km. Dotyczy to głównie: Narwi, Bugu, Wisły, Warty, Odry oraz rejonów Warszawy, Płocka, Gniezna, Poznania, Gorzowa, Krajnika.

Elementem zwiększającym ilość awaryjnych wycieków z rurociągów jest ich bardzo częste nawiercanie, związane z kradzieżami transportowanego paliwa.

Następną kategorią obiektów, będących potencjalnym źródłem skażeń, są **magazyny i składy**, w których są przechowywane, materiały łatwopalne, takie jak: paliwa, papier, bawełna, tkaniny syntetyczne, kauczuk, masy plastyczne, drewno, farby, lakiery, rozpuszczalniki i podobne substancje, a także składowane są duże ilości odpadów komunalnych bądź chemicznych. Obiekty te mogą być źródłem bardzo niebezpiecznych pożarów w wyniku, których wydzielać się będą do otoczenia substancje niebezpieczne dla zdrowia i życia człowieka. Pożary takie mogą powodować straty w ludności cywilnej spowodowane nie tylko oparzeniami oraz działaniem fali uderzeniowej powstającej przy wybuchu, ale także – zatruciem ludzi produktami spalania. We współczesnych miastach, pożary w coraz większym stopniu mogą stwarzać zagrożenie zatrucia toksycznymi produktami spalania materiałów pochodzenia chemicznego. Materiały te są składowane i produkowane na dużą skalę. Są wykorzystywane do celów konstrukcyjnych lub dekoracyjnych mieszkaniach, instytucjach fabrykach. Wiele z nich przy spalaniu tworzy związki toksyczne oraz powoduje silne zadymienie.

Produkty spalania mogą wywołać u ludzi zatrucia z objawami ujawniającymi się w różnej formie i w bardzo zróżnicowanym czasie. Na przykład, przy pożarze miasta o dużej

gęstości zabudowy u ludzi przebywających w strefie silnego zadymienia objawy zatrucia mogą wystąpić po około 30-45 minutach, a przy maksymalnie możliwych stężeniach dwutlenku węgla w produktach spalania – już po około 10 minutach. Podczas masowych pożarów nawet schrony nie stwarzają wystarczającej ochrony przed toksycznym działaniem produktów spalania.

Największe potencjalne źródło **skażeń promieniotwórczych** stanowią atomowe zakłady energetyczne. W ograniczonym zakresie, źródłem zagrożeń są również urządzenia techniki jądrowej wykorzystywane do celów przemysłowych naukowo-badawczych oraz odpady produkcyjne elektrowni. Uszkodzenie bądź zniszczenie siłowni jądrowych lub urządzeń i składów odpadów techniki jądrowej wywołałoby, bardzo groźne – zarówno dla ludzi jak i przyrody – zatrucia ziemi, wody i powietrza substancjami radioaktywnymi. O skali niebezpieczeństwa, jakie mogłyby wtedy powstać, świadczą awarie, które miały miejsce w niektórych atomowych zakładach energetycznych Europy i na świecie.

Na możliwość wystąpienia innych zagrożeń, wywołanych skażeniami radioaktywnymi wskazują też dotychczasowe wypadki z bronią jądrową. Według niepełnych danych takich wypadków zdarzyło się dotąd kilkadziesiąt.

Awarie siłowni jądrowych mogą być przyczyną powstania w ich okolicach rozległych stref silnych skażeń promieniotwórczych, które spowodują ogromne straty w ludziach oraz szkody ekologiczne nie mniej groźne niż te, wywołane działaniem broni jądrowej. Radioaktywne skażenie środowiska, zależne od stopnia zatrucia powietrza, terenu czy wody, stanowi śmiertelne niebezpieczeństwo dla wszystkich żywych organizmów. Chmury pyłu radioaktywnego, niesione z wiatrem na duże nieraz odległości i opadające na powierzchnię ziemi, stwarzają groźbę napromienienia wszystkiego, co się na niej znajduje. Przebywanie ludzi w skażonej promieniotwórczo strefie grozi powstaniem choroby popromiennej. Spożycie skażonej żywności i wody może spowodować zakażenia wewnętrzne, a w rezultacie również chorobę popromienną.

Gwałtowny rozwój środków transportu oraz infrastruktury spowodował, że coraz większą grupę zagrożeń stanowią **katastrofy komunikacyjne**. Mogą one wystąpić praktycznie w każdym rejonie, a zwłaszcza w miejscach o zwiększonym natężeniu ruchu. Zdarzenia te charakteryzują się poważnymi stratami materialnymi, duża liczbą ofiar, często występują problemy dojazdem do miejsca zdarzenia. Do usunięcia skutków takich zdarzeń użyta musi być angażowana znaczna ilość sił i środków, zgromadzonych w bardzo krótkim czasie. Do szybkiego podjęcia skutecznej akcji ratowniczej, niezbędny jest również efektywny system łącz-

ności, pozwalający na natychmiastowe poinformowanie o zaistnieniu katastrofy. Praktycznie, nie jest możliwe bezpośrednie zapobieganie tego typu zdarzeniom.

Należy liczyć się również z coraz większą częstotliwością występowania **katastrof budowlanych**. Część budynków mieszkalnych, wybudowana w latach międzywojennych, jest w znacznym stopniu wyeksploatowana. Jedną z przyczyn niszczenia budynków jest wilgoć, która na skutek braku izolacji poziomych powoduje korozję materiałów budowlanych. Inną przyczyną niszczenia budowli jest przeciążenie konstrukcji budowlanych połączone z nierównomiernym ich osiadaniem. Według informacji Głównego Urzędu Nadzoru Budowlanego statystycznie najwięcej, bo około 64%, niezamierzonych, gwałtownych zniszczeń obiektów budowlanych (katastrof budowlanych) dotyczy budownictwa mieszkaniowego, pozostałe związane są z obiektami przemysłowymi, gospodarczymi i obiektami innego rodzaju.

W aglomeracjach miejskich dużą uciążliwością, a jednocześnie zagrożeniem dla mieszkańców są **awarie urządzeń**, instalacji i sieci gazowej, rozdzielczej wodociągowej, kanalizacyjne, a także sieci ciepłowniczej i energetycznej. Biorąc pod uwagę stopień wyeksploatowania wymienionych elementów infrastruktury technicznej oraz niską jakość materiałów, których są one wykonane, spodziewać się należy szybkiego wzrostu liczby awarii tych urządzeń. Szczególnie niebezpieczne są awarie wszelkiego typu gazociągów, które powodują zagrożenie dla życia mieszkańców. Awarie linii energetycznych czy instalacji wodociągowych nie stanowią bezpośredniego zagrożenia, lecz są bardzo uciążliwe dla ludzi pozbawionych prądu czy wody. Należy pamiętać, że pozbawienie wody lub energii elektrycznej obiektów specjalnych (np. szpitali) może stanowić zagrożenie dla życia ludzi.

1.1.3. Zagrożenia terroryzmem

Istotnym elementem zagrożenia współczesnego społeczeństwa jest terroryzm. Na jego temat powstało wiele opracowań. Istnieje wiele definicji tego zjawiska, a w odniesieniu do bezpieczeństwa narodowego pod pojęciem terroryzmu można rozumieć metodę działania polegającą na przemocy wobec pojedynczych osób aparatu władzy (terroryzm indywidualny) lub wobec przypadkowych członków społeczeństwa, przez zamachy na urzędy, lokale publiczne, koszary (terroryzm zbiorowy)[12].

Terroryzm był stosowany od wieków jako metoda walki politycznej. Na szerszą skalę działalność terrorystyczna rozwinęła się w XIX w., w związku z ukształtowaniem się doktry-

ny i ruchu anarchizmu. Powstały wyspecjalizowane bojówki, związane z partiami politycznymi. Akty terroryzmu usprawiedliwia się niekiedy koniecznością walki narodowowyzwoleńczej.

W odniesieniu do nowych tendencji w środowisku bezpieczeństwa międzynarodowego, przynależności Polski do instytucji euroatlantyckich oraz udziału naszych wojsk w operacjach w Iraki i Afganistanie wzrasta zagrożenie dla obywateli i obiektów związane z zamachami terrorystycznymi.

Z dotychczasowych doświadczeń wynika, że celem ataków mogą stać się ośrodki władzy oraz infrastruktury gospodarczej i publicznej, a także obiekty, których zniszczenie stanowi poważne zagrożenie dla bezpieczeństwa, głównie takie jak: zapory wodne, zakłady przechowujące toksyczne środki przemysłowe i ujęcia wody[13].

Na szczególną uwagę zasługuje fakt, iż wykorzystanie strategii asymetrycznej w działaniach terrorystycznych może skutkować znacznymi stratami i naraża w sposób szczególny ludność cywilną.

Ataki terrorystyczne na Nowy Jork i Waszyngton 11 września 2001 roku wskazują na determinację terrorystów w osiąganiu zamierzonych celów.

Wykorzystanie różnego typu statków powietrznych, zarówno wojskowych jak i cywilnych, jako środków uderzeniowych na obiekty naziemne czy nawodne może powodować rozległe w skutkach straty prowadzące do powstania niekorzystnych warunków na terytorium całego kraju.

Aktem terroru powietrznego określa się[14]:

a) porwanie samolotu pasażerskiego lub innego statku powietrznego wypełnionego paliwem lub materiałem wybuchowym w celu zniszczenia określonego obiektu lub ataku na ludność cywilną poprzez uderzenie porwanym statkiem powietrznym w cel ataku;

b) użycie statku powietrznego (załogowego lub bezzałogowego) jako środka transportu do zrzucenia (rozpylenia) środków trujących (chemicznych lub biologicznych);

---

[12] Zob. *Encyklopedia multimedialna OMNIA*

[13] R. Kwećka, M. Gryga, *Siły specjalne w kontekście współczesnych zagrożeń,* AON, Warszawa 2002.

[14] R.Olszewski, *Reagowanie na zagrożenia z powietrza w czasie pokoju* [w:] *Bezpieczne niebo*, materiały z Konferencji Naukowej zorganizowanej w Akademii Obrony Narodowej 10 września 2002 r., AON, Warszawa 2002, s.51.

c) użycie statku powietrznego z ładunkiem jądrowym lub tzw.: „brudną bombą" w celu zniszczenia bardzo ważnego obiektu (np. elektrowni atomowej, zapory wodnej) lub skażenia terenu.

Ocenia się, że także akweny morskie są dogodnym obszarem do przeprowadzenia ataków terrorystycznych. Otwartość wód dla wszystkich „użytkowników" morza – za wyjątkiem wód wewnętrznych i wód terytorialnych – stwarza realne możliwości ataków terrorystycznych. Morze Bałtyckie w rejonie przyległym do wybrzeża polskiego jest akwenem o bardzo dogodnych warunkach hydrometeorologicznych do prowadzenia działań o charakterze terrorystycznym. Czynniki sprzyjające temu to:

a) głębokość wód na trasach komunikacji morskiej – dogodna do stawiania min dennych;
b) stosunkowo krótki okres występowania (praktycznie w strefie przybrzeżnej) zjawiska zlodzenia – uniemożliwiającego działania grup terrorystycznych z szybkich łodzi motorowych.

Prawdopodobnymi celami działań terrorystycznych w rejonie Morza Bałtyckiego mogą być:

a) obiekty i instalacje brzegowe monitorujące sytuację w strefie przybrzeżnej;
b) wieże wydobywcze i wiertnicze;
c) stałe obiekty infrastruktury morskiej i brzegowej (cywilne i wojskowe);
d) szlaki żeglugowe.

Analiza zagrożeń terrorystycznych wykazała, że w warunkach naszego kraju najbardziej prawdopodobny jest atak terrorystyczny na lądzie. Należy się liczyć głównie z atakiem w odniesieniu do obiektów:

a) w których urzędują władze państwowe i administracyjne;
b) innych państw rozmieszczonych na obszarze Polski;
c) ważnych ze względów ekonomiczno – finansowych oraz innych mających istotne znaczenie dla funkcjonowania państwa;
d) wojskowych oraz formacji uzbrojonych.

Obiekty centralnych władz państwowych i administracyjnych narażone w sposób szczególny na ataki terrorystyczne, to: urząd prezydenta, urząd premiera, parlament oraz urzędy ministerstw i innych instytucji państwowych, których funkcjonowanie decyduje o poziomie bezpieczeństwa państwa.

Z obiektów innych państw rozmieszczonych na obszarze Polski szczególnie narażone na akty terrorystyczne są placówki dyplomatyczne i konsularne (oraz rezydencje ich kierow-

ników) tych państw, które biorą aktywny udział w międzynarodowej koalicji antyterrorystycznej. Zagrożenie może dotyczyć również obiektów dużych firm reprezentujących interesy gospodarcze tych krajów.

Ewentualne ataki terrorystyczne na obiekty użyteczności publicznej zlokalizowane w dużych aglomeracjach miejskich lub w ich pobliżu, mogą skutkować nie tylko dużymi stratami materialnymi, ale również znacznymi ofiarami wśród ludności cywilnej. Zwiększone ryzyko ataku terrorystycznego dotyczy także:

a) zakładów posiadających materiały promieniotwórcze oraz toksyczne środki przemysłowe;
b) składów paliw płynnych, gazu oraz materiałów wybuchowych i amunicji, rafinerii, rurociągów i gazociągów;
c) dużych zapór wodnych i elektrowni;
d) lotnisk międzynarodowych i krajowych ;
e) ujęć wody pitnej;
f) dużych dworców kolejowych oraz metra;
g) teatrów, kin;
h) supermarketów i dużych domów towarowych.

Obiekty wojskowe, które mogą zostać zaatakowane przez terrorystów to:

a) bazy, składnice i składy broni, amunicji, materiałów wybuchowych oraz materiałów pędnych i smarów (MPS);
b) lotniska wojskowe i porty wojenne;
c) kompleksy, w których rozmieszczone są instytucje centralne, dowództwa Rodzajów Sił Zbrojnych (RSZ), korpusów zmechanizowanych (KZ) i okręgów wojskowych (OW).

Biologiczny atak terrorystyczny – bioterroryzm[15] – jest jednym ze współczesnych zagrożeń nie tylko dla oddziałów wojskowych, ale również dla ludności cywilnej. Atak przy użyciu środków biologicznych przeprowadzony nawet w odległym państwie, może być przyczyną znacznego wzrostu zachorowań na terytorium Polski. Niebezpieczeństwa wynikające z zastosowania broni biologicznej związane są z:

a) błyskawicznym rozprzestrzenianiem się drobnoustrojów (bakterii, wirusów);
b) powstawaniem psychoz zagrożenia i szerzeniem się strachu;
c) brakiem skutecznych lekarstw;
d) trudnością natychmiastowego zdiagnozowania przyczyny zachorowań i zgonów;
e) mylącymi objawami w okresie rozwijania się pełnego obrazu klinicznego choroby.

Przeprowadzona analiza wykazała także, że niezależnie od dotychczas stosowanych form ataków terrorystycznych, nie można wykluczyć aktów **terroru radiologicznego**. Potencjalnym źródłem zagrożeń są reaktory jądrowe. Obecnie eksploatowanych jest na świecie ok. 440 reaktorów energetycznych. Ponadto, działa podobna liczba reaktorów badawczych i do produkcji radioizotopów, jak również kolejne kilkaset reaktorów stanowiących podstawę napędu okrętów podwodnych i innych jednostek pływających.

Inne zagrożenie stanowi **terroryzm chemiczny**, którego istota polega na użyciu w ataku terrorystycznym bojowych środków trujących oraz niebezpiecznych substancji chemicznych (toksycznych środków przemysłowych).

Zasadniczo działania terrorystyczne, w których używa się broni chemicznej można podzielić na dwie grupy tj.:

---

[15] Bioterroryzm - jest to rodzaj terroryzmu (dywersji) z użyciem środków pochodzenia biologicznego. Do grupy tych środków należą przede wszystkim bakterie i wirusy. Choć o bioterroryźmie zrobiło się głośno po atakach we wrześniu i październiku 2001 roku bioterroryzm znany był od bardzo dawna. Pierwsze przesłanki dotyczą Aleksandra III Wielkiego, zwanego Macedońskim. W średniowieczu ciała zmarłych na dżumę (czarną śmierć) przerzucane były przez fortyfikacje obronne nieprzyjaciół. Największy rozwój broni B miał miejsce w czasie i po II wojnie światowej - zajmowały się rozwojem tego typu broni największe mocarstwa: nazistowskie Niemcy, ZSRR, Japonia, Stany Zjednoczone, Wielka Brytania i inne. Aktualnie Amerykanie wysuwają pewne doniesienia (powołując się na swój wywiad) o produkcji i rozwijaniu broni biologicznej przez niektóre z państw. Broń biologiczna jest bardzo skuteczna, prosta w produkcji, a zarazem strasznie tania, co pozwala nawet biednym krajom, czy organizacjom terrorystycznym na prowadzenie badań i jej produkcji. Ma ona szerokie spektrum zastosowań: począwszy od masowego niszczenia wrogich jednostek, przez morderstwa konkretnych osób do osiągania celów socjoekonomicznych. W pierwszym przypadku wykorzystywane są patogeny ludzie, szczególnie te, których leczenie w warunkach wojny jest trudne. Próby osiągnięcia drugiego celu są rzadko podejmowane, ale w historii pojawiły się pomyślne (dla terrorystów i wojsk) próby. W tym celu używane są czynniki chorobotwórcze wywołujące rzadkie choroby (podobnie jak w pierwszym przypadku). W trzecim przypadku wykorzystywane są patogeny zwierzęce i roślinne. Ewentualnie w celu spowodowania paniki w społeczeństwie (co ma ogromy wpływ na socjoekonomię) zostać mogą wykorzystane mikroorganizmy chorobotwórcze.

31

a) atak w celu spowodowania maksymalnych zniszczeń i ofiar wśród ludności cywilnej. W takim przypadku możliwy jest atak terrorystyczny na duże aglomeracje (centra handlowe, obiekty rekreacyjno - sportowe), zbiorniki i ujęcia wodne;
b) atak, który ma na celu przede wszystkim szantaż i szkody ekonomiczne[16].

Zagrożone mogą być również zakłady gromadzące na swoim terenie niebezpieczne środki chemiczne oraz transporty ze środkami chemicznymi z uwagi na możliwość uwolnienia wyżej wymienionych środków z cystern kolejowych i samochodowych.

W związku z tym, że większość substancji jest bezwonna i bezbarwna w stężeniach toksycznych, brak zewnętrznych symptomów użycia broni chemicznej stanowi problem w identyfikacji bojowych środków trujących i toksycznych środków przemysłowych.

Nowy, informatyczny, wymiar rozwoju społecznego powoduje, że coraz więcej dziedzin życia uzależnionych jest od działania komputerów i sieci teleinformatycznych. Systemy informatyczne stwarzają nowe możliwości, są jednak także celami **a**taków informatycznych, które sprowadzają się do fałszowania i blokowania informacji, manipulowania informacjami, zniszczenia informacji bądź systemu informacyjnego bez zmiany fizycznego stanu systemu, na który dokonywany jest atak. Działania takie powodują, że „atakowany" nie ma dostępu do informacji, bądź też dysponuje błędnymi informacjami i danymi, które bezpośrednio wpływają na jego proces decyzyjny.

Podstawowe metody ataków to:

a) włamania do systemu informatycznego przez Internet;
b) włamania do systemu informatycznego przez sieci wewnętrzne;
c) blokowanie systemów komputerowych uniemożliwiające ich uruchomienie;
d) zrywanie połączeń lub zakłócanie systemów łączności;
e) wprowadzanie oprogramowania szkodliwego, w celu destabilizacji pracy systemów informatycznych;
f) zakłócanie sieci radiowych różnego przeznaczenia;
g) przechwytywanie, rozkodowywanie i modyfikowanie zaszyfrowanych informacji;
h) podsłuch elektromagnetyczny;
i) prowadzenie kampanii propagandowych oraz operacji psychologicznych z wykorzystaniem usług oferowanych przez internet i sieci telefonii komórkowej;

---

[16] Przykładem może być atak wykonany poprzez skażenie określonego produktu przemysłowego czy spożywczego.

j) wystosowywanie do systemów informatycznych w krótkim okresie czasu dużej liczby żądań wykonania określonej usługi, w celu obniżenia ich sprawności funkcjonalnej;
k) kradzież danych osobowych.

Ataki na systemy informatyczne mogą być połączone z innymi rodzajami ataków terrorystycznych. Uderzenia mogą być skierowane w żywotnie ważne systemy, takie jak obsługa ruchu lotniczego, czy dystrybucja energii elektrycznej.

1.1.4. Inne zagrożenia

Przeprowadzone analizy wykazały, że do najbardziej prawdopodobnych zagrożeń wywołanych przez niekorzystne zjawiska polityczne, społeczne i ekonomiczne, określone jako inne zagrożenia, należy zaliczyć:

f) proliferacja broni masowego rażenia oraz przemyt innych materiałów niebezpiecznych;
g) niepokoje społeczne;
h) masowe migracje ludności;
i) przestępczość zorganizowana;
j) zbiorowe zakłócenia porządku publicznego.

W ostatniej dekadzie doszło do przyśpieszenia procesów globalizacji, nie tylko w aspekcie gospodarczym, lecz również w innych ważnych dziedzinach życia. Procesy te niosą ze sobą wielorakie skutki. Do negatywnych aspektów globalizacji należy między innymi rosnąca polaryzacja poziomu rozwoju i życia oraz stabilności pomiędzy bogatymi, a biednymi regionami i krajami. Pomiędzy różnymi grupami państw narastają także kontrowersje, napięcia na tle przyczyn i sposobów rozwiązywania problemów globalnych oraz regionalnych.

Wzrasta zagrożenie proliferacją broni masowego rażenia przez terrorystów, co wynika z tendencji do maksymalizacji liczby ofiar zamachów oraz dostępności technologii (zwłaszcza broni biologicznej i chemicznej, pozyskiwanej legalnie i na czarnym rynku). Utrzymuje się również zagrożenie ze strony krajów prowadzących własne programy produkcji broni masowego rażenia i środków ich przenoszenia (zwłaszcza balistycznych pocisków rakietowych). Postępujący proces umiędzynarodowienia przestępczości zorganizowanej przyczynia się do wzrostu zagrożeń wynikających z przemytu narkotyków, chorób mogących wywołać epidemię, przemytu materiałów niebezpiecznych, radioaktywnych oraz broni. Materiały oraz tech-

nologie, które mogą być zastosowane do budowy takiej broni i środków jej przenoszenia, stają się coraz bardziej dostępne, natomiast instrumenty oraz procedury wykrywania i zapobiegania nielegalnemu obrotowi tymi materiałami i technologiami są nadal mało skuteczne.

Szczególne zagrożenie dla bezpieczeństwa międzynarodowego stanowi fakt posiadania broni masowego rażenia przez takie państwa jak: Irak, Koreę Płn., Iran, Syrię, Sudan i Libię. Wyżej wymienione kraje prowadzą od lat konsekwentną politykę zmierzającą do ograniczenia amerykańskich i europejskich wpływów w tych regionach świata. Jednym z głównych działań sprzyjających realizacji tej polityki było pozyskanie i rozwój technologii do produkcji broni masowego rażenia. Ze względu na relatywnie niskie koszty wytwarzania i przechowywania oraz łatwość pozyskania technologii, państwa te weszły w posiadanie broni chemicznej już w latach 80 - tych. Obecnie część z nich posiada również broń biologiczną. Ocenia się, że potencjalnie największe zagrożenie związane jest z programami zbrojeniowymi państw Bliskiego Wschodu (Irak, Iran, Syria). Należy jednocześnie podkreślić, że weryfikacja postanowień traktatów ograniczających rozprzestrzenianie broni masowego rażenia jest niezwykle trudna i w praktyce zależy właściwie od dobrej woli politycznej państw – sygnatariuszy.

Z położenia geopolitycznego Polski wynika, że nasz kraj jest krajem tranzytowym pomiędzy wschodem i zachodem Europy i należy spodziewać się prób przemytu broni masowego rażenia przez nasze terytorium.

Niepokoje społeczne to szczególna forma zagrożeń w sferze bezpieczeństwa i porządku publicznego zapewniającego ochronę życia, zdrowia, mienia i innych wartości przed bezprawnymi działaniami oraz ochronę zasad współżycia społecznego i stosunków regulowanych normami prawa i zwyczajami. Mogą one być spowodowane planowanym oddziaływaniem na świadomość społeczną w celu wywołania emocji sprzyjających destabilizacji porządku publicznego. Niepokoje społeczne mogą narastać stopniowo w długim okresie czasu lub wybuchać nagle i rozwijać się lawinowo.

Zmiany zachodzące w wielu dziedzinach życia mogą powodować, że niektóre grupy społeczne tracą swoje wpływy, pogarszają się ich warunki bytowania lub nawet możliwości utrzymania. Wiele z tych grup w zmieniającej się rzeczywistości nie będzie w stanie podołać nowym wyzwaniom, zmienić rodzaj działalności, pozyskać nowe kwalifikacje, czy sprostać nowym wyzwaniom ekonomicznym.

Kryzysom zarówno militarnym jak i pozamilitarnym, w tym mającym swe źródło wewnątrz państwa, coraz częściej towarzyszą **migracje trans graniczne** na dużą skalę.

Migracje[17] można podzielić na:

a) imigrację – ze względu na przyczynę wyróżnia się 5 jej kategorii: osadnicy, profesjonaliści, pracownicy kontraktowi, pracownicy nieletni oraz ubiegający się o azyl (jeżeli prośby o azyl zostaną spełnione nabywają status uchodźcy);
b) reemigrację – dobrowolny powrót emigrantów do ojczyzny;
c) repatriację – powrót do kraju osób, które znalazły się poza terytorium kraju ojczystego m.in. z powodu zmian granic lub przymusowych wysiedleń.

Masowe przemieszczenia ludności mogą spowodować niebezpieczeństwo katastrofy humanitarnej i regionalnej destabilizacji. Potencjalne zagrożenie tworzy połączenie ewentualnych masowych migracji transgranicznych ze zorganizowaną działalnością przestępczą, przemytem broni, materiałów radioaktywnych, narkotyków i środków do ich produkcji.

Niekontrolowane migracje ludności do Polski mogą spowodować:

a) zwiększoną ilość rozbojów i kradzieży na terenie kraju (szczególnie w województwach przygranicznych oraz w stolicy państwa i województwie mazowieckim);
b) występowanie zbrojnych porachunków pomiędzy emigrantami;
c) zwiększenie zagrożenia epidemiologicznego;
d) powstanie zalążków ośrodków międzynarodowej przestępczości zorganizowanej;
e) powstanie struktur organizacyjnych międzynarodowego terroryzmu;
f) pogorszenie stosunków dyplomatycznych z wybranymi państwami (casus Czeczenii i związane z tym pogorszenie stosunków dyplomatycznych polsko-rosyjskich);
g) rozwój nielegalnego handlu oraz powstanie zaburzeń na rynku pracy;
h) rozwój żebractwa oraz agresywnych form wyłudzania pieniędzy.

Innym rodzajem zagrożeń jest **przestępczość zorganizowana**. Występuje ona w wielu krajach, w różnej formie, z różną intensywnością, a przedmiotem jej zainteresowania są różne obszary życia społecznego, ekonomicznego i politycznego.

Najbardziej rozwinęła się we Włoszech, USA, krajach bliskiego i dalekiego wschodu oraz w krajach Ameryki Południowej. Nową jakością są zorganizowane grupy przestępcze powstałe na terenach dawnego ZSRR.

---

[17] Przemieszczanie się ludności mające na celu zmianę miejsca pobytu. Migracje można podzielić ze względu na: zasięg, czas trwania, kierunek przemieszczania się.

35

Wzrost przestępczości zorganizowanej jest ściśle związany z sytuacją społeczno-polityczną państwa. Nadmierną dążność obywateli do pozyskiwania dóbr materialnych, pomijaniem innych wartości, dużym popytem na nielegalne dobra i usługi, a przy tym „cichym" społecznym przyzwoleniu.

Przyjmuje się, że występują trzy rodzaje organizacji przestępczych:

- grupa przestępcza – posiada luźne związki organizacyjne;
- zorganizowana grupa przestępcza;
- mafia – wysoce zorganizowana grupa przestępcza, działająca na zasadzie przemocy, szantażu itp., o dużych wpływach, powiązaniach z osobami na różnych szczeblach władzy, policją, biznesem, skupiająca zazwyczaj osoby jednej narodowości lub o wspólnym pochodzeniu, np. mafia włoska (sycylijska), rosyjska[18].

Szczególnym zagrożeniem ze strony przestępczości zorganizowanej jest udział (powiązania) pracowników (urzędników) administracji rządowej (samorządowej) w działaniach struktur przestępczych. **Korupcja**[19], jest działaniem, dzięki któremu grupy przestępcze dążą do zbudowania wzajemnych powiązań, działań legalnych i nielegalnych, aby w ten sposób maskować nielegalne interesy i wykorzystywać gospodarczą szarą strefę.

Ostatnia dekada to nasilenie się **zbiorowych zakłóceń porządku publicznego** – noszące znamiona zagrożeń mogących prowadzić do powstania sytuacji kryzysowej. Normą niemalże stały się burdy i chuligańskie ekscesy podczas imprez sportowych i rozrywkowych. Praktycznie każde spotkanie piłkarskie rozgrywane w Polsce traktowane powinno być jako impreza masowa o podwyższonym ryzyku[20].

Bezpieczeństwo imprez masowych stało się problemem międzynarodowym. Przemoc i ekscesy uczestników imprez masowych, zwłaszcza w czasie imprez sportowych, a w szczególności meczów piłki nożnej stały się powodem uchwalenia Europejskiej Konwencji w tej sprawie, w Strasburgu, w dniu 19 sierpnia 1985 r., którą ratyfikował nasz kraj. Podpisując konwencję Polska zobowiązała się do szeregu działań, które zostały zawarte w wielu aktach

---

[18] *Wielka Internetowa Encyklopedia Multimedialna*; http:// wiem.onet.pl/wiem/

[19] Zepsucie, demoralizacja; przekupstwo, łapownictwo, sprzedajność, Słownik wyrazów obcych, PWN, Warszawa 2995.

[20] Impreza masowa o podwyższonym ryzyku – to impreza masowa w czasie, której jak wynika z posiadanych informacji i dotychczasowych doświadczeń dotyczących zachowania osób uczestniczących, istnieje uzasadniona obawa wystąpienia aktów przemocy i agresji; to impreza sportowa, artystyczna lub rozrywkowa, na której liczba miejsc dla osób na stadionie, w innym obiekcie niebędącym budynkiem lub na terenie umożliwiającym przeprowadzenie imprezy masowej wynosi – nie mniej niż 300, a w przypadku hali sportowej lub innego budynku umożliwiającego przeprowadzenie imprezy – nie mniej niż 200. *Ustawa z dnia 22 sierpnia 1997 r. o bezpieczeństwie imprez masowych, Dz. U. Nr 106, poz. 680 z póź. zm.*

prawnych m.in. w ustawie o ochronie osób i mienia, ustawie o bezpieczeństwie imprez masowych i wielu innych.

Zgromadzenie się dużej ilości ludzi na stosunkowo niewielkim terenie może spowodować nasilenie się drobnej przestępczości kryminalnej (kradzieże kieszonkowe, włamania do samochodów uczestników imprezy) oraz występowania ekscesów chuligańskich[21].

Oczywistym jest, że nie można wykluczyć zaistnienia innych zagrożeń – ich lista jest spisem otwartym. Niektóre z nich, dziś określane jako niemilitarne, za kilka miesięcy (może lat) zakwalifikowane zostać mogą do grupy zagrożeń militarnych dla Rzeczypospolitej Polskiej. Może się to odnosić do zagrożeń terrorystycznych. Nie można wykluczyć (oby nigdy do tego nie doszło), że grupy terrorystyczne będą dysponowały takimi siłami i środkami, że tylko regularne i nieregularne działania sił zbrojnych będą w stanie powstrzymać je przed „sianiem" terroru.

1.2. System reagowania kryzysowego

Prowadzony proces badawczy wykazał, że systemowi reagowania kryzysowego poświęcono w ostatnich latach sporo uwagi. Zagadnienia te znajdowały odbicie w pracach Sejmu, Biura Bezpieczeństwa Narodowego organów rządowych oraz instytucji, których zadania dotyczą tych zagadnień.

Znalazło to, między innymi, odzwierciedlenie w zapisach Strategii Bezpieczeństwa Narodowego, gdzie zapisano, że *nowe wyzwania dyktują potrzebę utworzenia państwowego kompleksowego systemu reagowania kryzysowego, odpowiadającego na współczesne zagrożenia bezpieczeństwa zarówno międzynarodowego, jak i wewnętrznego. Odpowiednie instytucje państwowe będą prowadzić działania zmierzające do powołania zintegrowanego systemu kierowania i zarządzania na wypadek kryzysu. Niezbędne staje się spójne uregulowanie zadań i kompetencji organów i instytucji państwowych, a także organizacji społecznych działających na rzecz bezpieczeństwa państwa*[22]. W dokumencie tym wskazano także, że system ten powinien być zdolny do terminowej i efektywnej reakcji na każdą sytuację tak, aby adekwatnie do skali zagrożenia pozwolić na całkowitą jej neutralizację.

W przedstawianej już ustawie o zarządzaniu wskazuje się, że zadania i procedury mające na celu zapobieganie sytuacjom kryzysowym, przygotowanie do przejmowania nad nimi kontroli w drodze zaplanowanych działań oraz reagowanie w przypadku wystąpienia sytuacji

---

[21] J. Kamiński, *Środowiska i sytuacje agresywnego zachowania*, PWN, Warszawa 1984.
[22] *Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej*, rozdz. II, Warszawa 2003.

kryzysowych realizuje Narodowy System Pogotowia Kryzysowego (NSPK). Przez system ten należy rozumieć struktury i działania organów administracji rządowej oraz Sił Zbrojnych RP[23].

Analiza założeń i zasad tego systemu wykazała, że składa się on z dwóch zasadniczych podsystemów tworzonych poprzez:

– organy kierowania;

– siły i środki przewidziane do działań w sytuacjach kryzysowych.

Podsystemy te zawierają w sobie natomiast dwa wzajemnie uzupełniające się komponenty: **pozamilitarny** i **militarny**. Ich rola i udział w rozwiązaniu poszczególnych sytuacji kryzysowych mogą być różne, w zależności od charakteru tych sytuacji oraz ich miejsca i zasięgu.

W przypadku kryzysu o charakterze niemilitarnym, wywołanego klęską żywiołową, katastrofą naturalną lub techniczną, działaniami terrorystycznymi czy też innymi zjawiskami społecznymi, wiodącą rolę w jego rozwiązaniu (przeciwdziałaniu) odgrywają organy administracji rządowej i samorządowej oraz siły i środki cywilne.

W takim przypadku udział sił zbrojnych (wybranych organów dowodzenia i wydzielonych jednostek wojskowych) może ograniczyć się do udzielenia pomocy w ewentualnych działaniach ratowniczych, w likwidacji skutków zagrożenia lub utrzymaniu porządku publicznego i to tylko w przypadku, gdy użycie sił cywilnych okaże się niewystarczające, albo niemożliwe.

Natomiast podczas **kryzysu o charakterze polityczno–militarnym** (konflikt zbrojny, wojna) rolę wiodącą odgrywa podsystem militarny.

W powszechnej ocenie uznaje się, że zasadnicze części tego systemu już funkcjonują. Trwające natomiast prace normatywne oraz wdrożeniowe koncentrują się na doprecyzowaniu kompetencji poszczególnych ogniw, skorygowaniu (określeniu) relacji między nimi, uporządkowaniu i koordynacji planów ich działania, przebudowie rozwiązań nieprzystających do nowych realiów oraz stworzeniu brakujących elementów.

---

[23] Ustawa z dnia 26 kwietnia 2007 r. *o zarządzaniu kryzysowym* (Dz. U. Nr 89, poz. 590), art. 2, ust. 5.

1.2.1. Elementy podsystemu organów kierowania

Analiza struktury podsystemu organów kierowania zarządzaniem kryzysowym wykazała, że w jego skład wchodzą elementy wszystkich poziomów administracji publicznej i są to:

1. **Rada Ministrów**, która sprawuje zarządzanie kryzysowe na terytorium Polski. W przypadkach niecierpiących zwłoki zarządzanie kryzysowe sprawuje minister właściwy do spraw wewnętrznych, zawiadamiając niezwłocznie o swoich działaniach Prezesa Rady Ministrów. Przy Radzie ministrów tworzy się ***Rządowy Zespół Zarządzania Kryzysowego***. Zabezpieczenie prac tego zespołu oraz realizację zadań bieżących realizuje podległe Prezesowi Rady Ministrów ***Centrum Bezpieczeństwa.***
2. **Wojewoda,** który jest organem właściwym w sprawach zarządzania kryzysowego na terenie województwa. Swoje zadania w tym zakresie wojewoda realizuje przy pomocy urzędu wojewódzkiego oraz zespolonych służb, inspekcji i straży. Organem pomocniczym w zapewnieniu wykonywania zadań zarządzania kryzysowego jest ***Wojewódzki Zespół Zarządzania Kryzysowego***.
3. **Starosta**, który jest organem właściwym w sprawach zarządzania kryzysowego na terenie powiatu. Zadania te realizuje on przy pomocy komórki organizacyjnej starostwa powiatowego właściwej w sprawach zarządzania kryzysowego oraz przy pomocy powoływanego ***Powiatowego Zespołu Zarządzania Kryzysowego***.
4. **Wójt, burmistrz, prezydent miasta,** są organami właściwymi w sprawach zarządzania kryzysowego na terenie gminy. Zadania te realizują oni przy pomocy komórki organizacyjnej urzędu gminy (miasta) właściwej w sprawach zarządzania kryzysowego oraz przy pomocy powoływanego ***Gminnego Zespołu Zarządzania Kryzysowego***.

Analiza założeń działania wymienionych powyżej organów wykazała, że podstawową rolę w działaniach zarządzania kryzysowego spełniają organy władzy samorządowej szczebla gminy i powiatu.

Wynika to z założenia, że reakcja odpowiednich podmiotów powinna dotyczyć najniższych szczebli w obrębie odpowiedzialności, których zaistnieje sytuacja kryzysowa. Gminy realizują podstawowe zadania związane z ochroną ludności, skupiając swój wysiłek głównie na: ostrzeganiu, alarmowaniu i informowaniu ludności o zagrożeniach, prowadzeniu ewaku-

acji oraz zapewnieniu ewakuowanym pomocy medycznej i socjalnej głównie w zakresie zakwaterowania i wyżywienia.

Powiaty wykonują takie same zadania jak gminy, a ponadto koordynują działania reagowania kryzysowego na obszarze powiatu, wspierając je działaniem podległych sobie: służb, inspekcji, straży wspomaganych przez organizacje pozarządowe przewidziane w planie reagowania kryzysowego powiatu.

Województwo udziela natomiast niezbędnej pomocy władzom powiatowym, których możliwości w zaistniałej sytuacji nie zapewniają prowadzenia skutecznych działań. W przypadku powstania sytuacji kryzysowej obejmującej obszar większy niż jeden powiat, szczebel wojewódzki koordynuje prowadzenie działań.

W przypadku, gdy posiadane siły i środki wojewódzkie są niewystarczające do opanowania sytuacji kryzysowej Wojewoda występuje do władz centralnych o stosowną pomoc ze szczebla nadrzędnego (w tym o wprowadzenie stanu klęski żywiołowej na części lub całym obszarze województwa).

Analizując zasadnicze zadania oraz szczegółowe zasady funkcjonowania zespołów reagowania kryzysowego stwierdzono, że określa ustawa oraz rozporządzenie, które określa:

- sposób tworzenia gminnego zespołu reagowania, powiatowego i wojewódzkiego zespołu reagowania kryzysowego oraz rządowego zespołu koordynacji kryzysowej,
- sposób funkcjonowania zespołów,
- usytuowanie i sposób ich finansowania,
- warunki techniczne i standardy ich wyposażenia,
- tryb pracy zespołów,
- sposób dokumentowania działań i prac zespołów.

Do zadań zespołów należy w szczególności:

- ocena sytuacji kryzysowych i prognozowanie ich rozwoju,
- przygotowywanie propozycji działań i przedstawianie wniosków, co do wykonania lub korekty uprzednio zaplanowanych procedur reagowania,
- planowanie wsparcia organów niższego szczebla,
- przygotowywanie warunków koordynacji pomocy humanitarnej,
- przekazywanie do wiadomości publicznej stosownych informacji.

W skład poszczególnych zespołów wchodzą osoby zatrudnione w urzędach administracji rządowej i samorządowej, podległych im jednostkach organizacyjnych oraz przedsta-

wiciele społecznych organizacji ratowniczych i kierownicy (pracownicy, funkcjonariusze) zespolonych służb, inspekcji i straży.

Gminne, powiatowe i wojewódzkie zespoły reagowania kryzysowego, działają na podstawie planów pracy zatwierdzonych odpowiednio przez wójta, starostę i wojewodę. Pracami zespołów kierują ich szefowie. Do zadań szefów zespołów należy w szczególności:

- przygotowanie rocznego planu pracy zespołu;
- opracowanie regulaminu bieżących prac zespołu oraz działań w sytuacjach zagrożeń katastrofą naturalną lub awarią techniczną noszącą znamiona klęski żywiołowej;
- ustalanie przedmiotu i terminu posiedzeń;
- zawiadamianie o terminach posiedzeń;
- przewodniczenie posiedzeniom;
- zapraszanie na posiedzenia osób niebędących członkami zespołu;
- inicjowanie i organizowanie prac zespołu.

W przypadkach wymagających natychmiastowej analizy i oceny zagrożeń oraz koordynacji działań ratowniczych, szef może zarządzić posiedzenie zespołu reagowania kryzysowego w trybie natychmiastowym.

Grupy robocze zespołów reagowania kryzysowego o charakterze stałym pracują zgodnie z rozkładem czasu pracy obowiązującym w urzędzie, w którym są usytuowane, z zapewnieniem dobowych dyżurów.

W czasie obowiązywania stanu klęski żywiołowej zespoły reagowania kryzysowego pracują w składzie grup roboczych o charakterze stałym i czasowym, w urzędzie, w którym są usytuowane, w trybie ciągłym, z zapewnieniem zmianowej pracy osób wchodzących w ich skład.

W skład **Rządowego Zespołu Reagowania Kryzysowego** wchodzą[24]:

- Prezes rady Ministrów – przewodniczący,
- Minister Obrony Narodowej i minister właściwy do spraw wewnętrznych – zastępcy przewodniczącego;
- Minister Koordynator Służb Specjalnych.

W posiedzeniach Zespołu, na prawach członka, biorą udział w zależności od potrzeb, następujące osoby:

1. Ministrowie kierujący działami administracji rządowej:

[24] Ustawa z dnia 26 kwietnia 2007 r. *o zarządzaniu kryzysowym* (Dz. U. Nr 89, poz. 590), art. 8, ust. 2.

41

- administracja publiczna,
- budownictwo, gospodarka przestrzenna i mieszkaniowa,
- finanse publiczne,
- gospodarka,
- gospodarka morska,
- gospodarka wodna,
- instytucje finansowe,
- informatyzacja,
- kultura i ochrona dziedzictwa narodowego,
- łączność,
- oświata i wychowanie,
- rolnictwo,
- sprawiedliwość,
- środowisko, transport,
- zdrowie.

2. Główny Geodeta Kraju.
3. Główny Inspektor Sanitarny.
4. Główny Lekarz Weterynarii.
5. Komendant Główny Państwowej Straży Pożarnej.
6. Komendant Główny Policji
7. Komendant Główny Straży Granicznej.
8. Prezes Państwowej Agencji Atomistyki.
9. Prezes Urzędu Lotnictwa Cywilnego.
10. Szef Agencji Wywiadu.
11. Szef Agencji Bezpieczeństwa Wewnętrznego.
12. Szef Służby Cywilnej Kraju.
13. Szef służby Kontrwywiadu Wojskowego.

Prezydent Rzeczypospolitej Polskiej może skierować do prac Zespołu, na prawach członka, Szefa Biura Bezpieczeństwa Narodowego lub innego przedstawiciela. Może też zapraszać do udziału w posiedzeniach Zespołu inne osoby.

Wojewódzki zespół reagowania kryzysowego składa się z szefa, zastępców oraz grup roboczych o charakterze stałym i czasowym. Grupami roboczymi wojewódzkiego zespołu o charakterze stałym są:

- ❒ grupa bezpieczeństwa powszechnego i porządku publicznego;
- ❒ grupa planowania cywilnego;
- ❒ grupa monitorowania, prognoz i analiz.

Grupy robocze o charakterze stałym, stanowią wojewódzkie centrum zarządzania kryzysowego, będące komórką organizacyjną urzędu wojewódzkiego.

Grupami roboczymi wojewódzkiego zespołu o charakterze czasowym są:

- ❒ grupa operacji;
- ❒ grupa zabezpieczenia logistycznego;
- ❒ grupa opieki zdrowotnej i pomocy socjalno-bytowej.

Wojewoda kieruje Wojewódzkim Zespołem Reagowania Kryzysowego w czasie stanu klęski żywiołowej na terenie województwa. Wojewodzie podporządkowane są jednostki organizacyjne administracji rządowej i samorządu wojewódzkiego działające na obszarze województwa. Do działań zapobiegających skutkom klęsk żywiołowych na terenie województwa mogą być kierowane oddziały Sił Zbrojnych Rzeczpospolitej Polskiej.

Powiatowy zespół reagowania kryzysowego składa się z szefa, zastępcy oraz grup roboczych o charakterze stałym i czasowym. Grupami roboczymi powiatowego zespołu o charakterze stałym są:

- ❒ grupa planowania cywilnego
- ❒ grupa monitorowania, prognoz i analiz

Grupy robocze o charakterze stałym, stanowią powiatowe centrum zarządzania kryzysowego, będące komórką organizacyjną starostwa powiatowego lub komendy powiatowej państwowej straży pożarnej.

Na podstawie porozumienia między właściwym starostą a prezydentem miasta na prawach powiatu, centrum zarządzania kryzysowego, może być ulokowane na terenie powiatu lub miasta na prawach powiatu i obejmować zasięgiem działania obszar obu sąsiadujących jednostek samorządu terytorialnego.

Grupami roboczymi powiatowego zespołu o charakterze czasowym są:

- ❒ grupa operacji i organizacji działań;
- ❒ grupa zabezpieczenia logistycznego;
- ❒ grupa opieki zdrowotnej i pomocy socjalno-bytowej.

Grupy robocze o charakterze stałym tworzy się spośród osób zatrudnionych w starostwie powiatowym, powiatowych jednostkach organizacyjnych lub jednostkach organizacyjnych stanowiących aparat pomocniczy kierowników powiatowych służb, inspekcji i straży.

Zespół włącza się do akcji ratowniczej, gdy klęską zagrożony jest obszar kilku gmin położonych na terenie powiatu. W kierowaniu działaniami w stanie klęski żywiołowej staroście podlegają wójtowie oraz kierownicy jednostek organizacyjnych utworzonych przez powiat, kierownicy powiatowych służb, inspekcji i straży, również kierownicy jednostek ochrony przeciwpożarowej.

Gminny zespół reagowania składa się z szefa, zastępcy oraz grup roboczych o charakterze stałym i czasowym.

Grupami roboczymi gminnego zespołu o charakterze stałym są:

- ❒ grupa planowania cywilnego;
- ❒ grupa monitorowania, prognoz i analiz.

Grupy robocze stanowią gminne centrum reagowania, będące komórką organizacyjną urzędu gminy. Siedziba gminnego centrum reagowania powinna być odpowiednio oznakowana, a jego lokalizacja podana do publicznej wiadomości w sposób umożliwiający poinformowanie wszystkich mieszkańców gminy.

Grupami roboczymi gminnego zespołu o charakterze czasowym są:

- ❒ grupa operacji i organizacji działań;
- ❒ grupa zabezpieczenia logistycznego;
- ❒ grupa opieki zdrowotnej i pomocy socjalno-bytowej.

Szefa gminnego zespołu i jego zastępców wyznacza wójt spośród zatrudnionych w urzędzie gminy, gminnych jednostkach organizacyjnych lub w jednostkach pomocniczych, osób posiadających wykształcenie specjalistyczne w zakresie ratownictwa, ochrony przeciwpożarowej, inżynierii bezpieczeństwa cywilnego lub zarządzania kryzysowego, absolwentów wyższych szkół wojskowych, a także spośród funkcjonariuszy pożarnictwa, wyznaczonych do wykonywania zadań poza jednostkami organizacyjnymi państwowej straży pożarnej.

Gminny Zespół Reagowania, kierowany przez wójta, burmistrza lub prezydenta miasta jest odpowiedzialny za ochronę przed klęską żywiołową na terenie gminy. Wójt (burmistrz, prezydent miasta) może wydawać polecenia organom jednostek pomocniczych, kierownikom jednostek organizacyjnych utworzonych przez gminę, kierownikom jednostek ochrony przeciwpożarowej oraz kierownikom jednostek czasowo przekazanym do wykonywania zadań na terenie gminy.

Zasadniczym miejscem pracy przedstawionych powyżej zespołów są centra reagowania kryzysowego, ich zadania, stosownie do szczebla administracji, są następujące:

- zapewnienie koordynacji i wspomaganie realizacji zadań przez organ w rozwiązaniu danej sytuacji kryzysowej,

- zapewnienie funkcjonowania zespołu reagowania kryzysowego, w tym dokumentowanie jego prac,
- monitorowanie, ocena i prognozowanie zagrożeń na obszarze zainteresowania,
- analizowanie stanu sił i środków ratowniczych będących w dyspozycji,
- koordynacja (wspieranie) działań ratowniczych oraz dokumentowanie i utrwalanie ich przebiegu,
- zapewnienie współdziałania z centrami zarządzania kryzysowego ogniw nadrzędnych i podległych oraz z sąsiadami, a także ze stanowiskami (centrami) operacyjnymi służb, inspekcji i straży i innymi współpracującymi instytucjami.

Dodatkowo:

- Rządowe Centrum Reagowania Kryzysowego zapewnia stały kontakt z centrami kryzysowymi NATO i Unii Europejskiej oraz państw sąsiednich,
- powiatowe centrum ratownicze:
  - przyjmowanie i segregacja zgłoszeń przez dyspozytorów PSP i dyspozytorów medycznych oraz kierowanie do działań odpowiednich sił i środków,
  - obsługa jednolitego europejskiego numeru alarmowego 112.

Szczegółowe zadania Powiatowego Centrum Zarządzania Kryzysowego (PCZK) mogą być następujące:

- prowadzenie całodobowego monitoringu zagrożeń kryzysowych oraz informowanie szefa Powiatowego Zespołu Reagowania Kryzysowego o zaistniałej sytuacji;
- przyjmowanie, zbieranie i ewidencjonowanie oraz analizowanie informacji o stanie bezpieczeństwa miasta, współpraca z instytucjami realizującymi stały monitoring środowiska;
- opracowywanie wstępnej analizy zagrożeń dla potrzeb PZRK oraz udział w przygotowaniu kompleksowej analizy zagrożeń;
- udział w ostrzeganiu i alarmowaniu ludności Krakowa o zaistniałym (potencjalnym) zagrożeniu - współpraca w tym zakresie z lokalnymi mediami;
- nadzór nad systemem wczesnego ostrzegania i alarmowania ludności;
- przekazywanie dyżurnemu Straży Miejskiej polecenia dotyczącego wykonania monitoringu stanu wód w określonych punktach na rzekach i ciekach wodnych;
- tworzenie i aktualizowanie miejskiego planu reagowania kryzysowego;
- przygotowanie projektów decyzji koordynujących działania służb i instytucji odpowiedzialnych za bezpieczeństwo publiczne;

- przyjmowanie informacji o zagrożeniu, dokonywanie analizy i prognozy rozwoju sytuacji zagrożenia;
- przygotowanie i przeprowadzenie co najmniej raz w roku ćwiczeń Powiatowego Zespołu Zarządzania Kryzysowego w pełnym składzie.

Powiatowe Centrum Zarządzania Kryzysowego przygotowuje codzienne raporty o stanie bezpieczeństwa dla Prezydenta Miasta Krakowa. Raporty powstają na podstawie informacji i meldunków składanych przez podmioty i instytucje odpowiedzialne za bezpieczeństwo publiczne, m.in. ilości i rodzajów przestępstw, zagrożeń pożarowych, sanitarnych, powodziowych i innych. Zgodnie z odpowiednimi zapisami rozporządzenia pracownikami PCZK są pracownicy Wydziału Bezpieczeństwa i Zarządzania Kryzysowego Urzędu Miasta. Funkcjonowanie PCZK finansowane jest z budżetu miasta w ramach własnych zadań gminy

1.2.2. Elementy podsystemu sił i środków reagowania kryzysowego

Obok systemu zarządzania zasadniczym elementem państwowego kompleksowego systemu reagowania kryzysowego są siły i środki przewidziane do działań w sytuacjach kryzysowych.

Można wśród nich wymienić:

- siły i środki systemu ratowniczo-gaśniczego Państwowej Straży Pożarnej oraz Ochotniczej Straży Pożarnej,
- Policję,
- Straż Graniczną,
- Państwowe Ratownictwo Medyczne i jednostki ochrony zdrowia,
- formacje OC,
- społeczne organizacje ratownicze i inne podmioty ochrony ludności,
- inne „właściwe w tych sprawach" państwowe urzędy, agencje, inspekcje, straże i służby,
- siły zbrojne (w miarę potrzeb).

Sprawne zarządzanie i kierowanie wszystkimi dostępnymi siłami i środkami rzutuje bezpośrednio na ich efektywność, a to z kolei skutkuje minimalizowaniem strat i zniszczeń oraz wywiera decydujący wpływ na szybkie opanowanie (zneutralizowanie) sytuacji kryzysowej.

W zapobieganiu skutkom klęski żywiołowej lub ich usuwaniu są zobowiązane uczestniczyć: Państwowa Straż Pożarna i inne jednostki ochrony przeciwpożarowej, Policja, Pań-

stwowe Ratownictwo Medyczne oraz inne kompetentne w tych sprawach państwowe urzędy, agencje, inspekcje, straże i służby. Poniżej scharakteryzowano niektóre z nich, które działają na różnych szczeblach zarządzania kryzysowego.

Instytut Meteorologii i Gospodarki Wodnej - IMGW

IMGW to instytucja nadzorowana przez Ministra Środowiska. Ośrodek Gtówny IMGW w Warszawie nadzoruje działania pięciu oddziałów: w Gdyni, Katowicach, Krakowie, Poznaniu, Wrocławiu. IMGW odpowiada za osłonę hydrologiczno-meteorologiczną kraju wykonując pomiary, opracowując prognozy, ostrzeżenia. Inicjuje działania służb odpowiedzialnych za przeciwdziałanie skutkom katastrof naturalnych wysyłając ostrzeżenia do Rządowego Zespołu Koordynacji Kryzysowej, Krajowego Centrum Koordynacji Ratownictwa i Ochrony Ludności, Wojewódzkich Zespołów Reagowania Kryzysowego.

Regionalny Zarząd Gospodarki Wodnej - RZGW

Obszar Polski został podzielony zgodnie z geograficznym przebiegiem granic dorzeczy między siedem RZGW: w Gdańsku, Gliwicach, Krakowie, Poznaniu, Szczecinie, Warszawie i Wrocławiu. RZGW ma za zadanie: określanie ilości i stanu zasobów wodnych oraz stanu ochrony przed powodzią, opracowywanie planów ochrony przed powodzią, prowadzenie rejestrów cieków (uwzględniając jakość wody), koordynowanie działań związanych z ochroną przed powodzią i suszą, uzgadnianie planów zagospodarowania przestrzennego z uwzględnieniem warunków korzystania z wód dorzecza.

Wojewódzki Zarząd Melioracji i Urządzeń Wodnych - WZMiUW

WZMiUM to instytucja podległa samorządowi wojewódzkiemu. Jest odpowiedzialna za utrzymanie urządzeń melioracyjnych - watów, pompowni, regulacji rzek. W sytuacji zagrożenia powodziowego WZMiUW koordynuje działania techniczne w Wojewódzkim Zespole Reagowania Kryzysowego, polegające na zabezpieczeniu urządzeń wodnych przed powodzią, likwidacji przesiąków, naprawie wałów itp.

Policja

Policja w czasie klęski żywiołowej podlega kierownictwu zespołów reagowania kryzysowego właściwych szczebli. Choć nie jest zobowiązana do bezpośredniego działania w akcji ratowniczej, to w jej kompetencjach jest utrzymanie bezpieczeństwa i porządku publicznego. Realizacja tego zadania następuje przez alarmowanie ludności, udostępnianie środków

łączności innym służbom ratowniczym, zabezpieczanie mienia, organizowanie dróg i kierowanie ruchem w celu sprawnej organizacji dojazdów ewakuowanej ludności i służb ratowniczych. Policja wspomaga zespół w prowadzeniu akcji informacyjnej.

Zadania policji określa ustawa o policji. Do podstawowych zadań policji należą:

- ochrona życia i zdrowia ludzi oraz mienia przed bezprawnymi zamachami naruszającymi te dobra,
- ochrona bezpieczeństwa i porządku publicznego, w tym zapewnienie spokoju w miejscach publicznych oraz w środkach publicznego transportu i komunikacji publicznej, w ruchu drogowym i na wodach przeznaczonych do powszechnego korzystania,
- inicjowanie i organizowanie działań mających na celu zapobieganie popełnianiu przestępstw i wykroczeń oraz zjawiskom kryminogennym i współdziałanie w tym zakresie z organami państwowymi, samorządowymi i organizacjami społecznymi,
- wykrywanie przestępstw i wykroczeń oraz ściganie ich sprawców,
- nadzór nad strażami gminnymi (miejskimi) oraz nad specjalistycznymi uzbrojonymi formacjami ochronnymi w zakresie określonym w odrębnych przepisach,
- kontrola przestrzegania przepisów porządkowych i administracyjnych związanych z działalnością publiczną lub obowiązujących w miejscach publicznych,
- współdziałanie z policjami innych państw oraz ich organizacjami międzynarodowymi na podstawie umów i porozumień międzynarodowych oraz odrębnych przepisów,
- gromadzenie, przetwarzanie i przekazywanie informacji kryminalnych,
- prowadzenie krajowego systemu informatycznego.

Wykonując ustawowe zadania policjanci mają prawo:

- legitymowania osób w celu ustalenia ich tożsamości,
- zatrzymywania osób w trybie i przypadkach określonych w przepisach kodeksu postępowania karnego i innych ustaw,
- zatrzymywania osób pozbawionych wolności, które na podstawie zezwolenia właściwego organu opuściły areszt śledczy albo zakład karny i w wyznaczonym terminie nie powróciły do niego,
- zatrzymywania osób stwarzających w sposób oczywisty bezpośrednie zagrożenie dla życia lub zdrowia ludzkiego, a także dla mienia,

- przeszukiwania osób i pomieszczeń w trybie i przypadkach określonych w przepisach kodeksu postępowania karnego i innych ustaw,
- dokonywania kontroli osobistej, a także przeglądania zawartości bagaży i sprawdzania ładunku w portach i na dworcach oraz w środkach transportu lądowego, powietrznego i wodnego, w razie istnienia uzasadnionego podejrzenia popełnienia czynu zabronionego pod groźbą kary,
- obserwowania i rejestrowania przy użyciu środków technicznych obrazu zdarzeń w miejscach publicznych, a w przypadku czynności operacyjno-rozpoznawczych i administracyjno-porządkowych podejmowanych na podstawie ustawy – także i dźwięku towarzyszącego tym zdarzeniom,
- żądania niezbędnej pomocy od instytucji państwowych, organów administracji rządowej i samorządu terytorialnego oraz jednostek gospodarczych prowadzących działalność w zakresie użyteczności publicznej; wymienione instytucje, organy i jednostki obowiązane są, w zakresie swojego działania, do udzielenia tej pomocy, w zakresie obowiązujących przepisów prawa,
- zwracania się o niezbędną pomoc do innych jednostek gospodarczych i organizacji społecznych, jak również zwracania się w nagłych wypadkach do każdej osoby o udzielenie doraźnej pomocy, w ramach obowiązujących przepisów prawa,
- dokonywania kontroli rodzaju używanego paliwa przez pobranie próbek paliwa ze zbiornika pojazdu mechanicznego.

Straż Pożarna

Na szczeblu centralnym działa Krajowe Centrum Koordynacji Ratownictwa i Ochrony Ludności Komendy Głównej Państwowej Straży Pożarnej, kierowane przez Komendanta Głównego PSP. Na szczeblu wojewódzkim i powiatowym działają Wojewódzkie i Powiatowe Stanowiska Koordynacji Ratownictwa podległe odpowiednio komendantom wojewódzkim i powiatowym. Do zadań tych zespołów należy rozpoznawanie zagrożeń, organizowanie i prowadzenie akcji ratowniczych, wykonywanie pomocniczych specjalistycznych czynności ratowniczych w czasie klęsk żywiołowych. W akcji ratowniczej zobowiązane są również uczestniczyć jednostki ochotniczej straży pożarnej.

Zadania państwowej straży pożarnej określa ustawa, a do podstawowych zadań państwowej straży pożarnej należy:

- rozpoznawanie zagrożeń pożarowych i innych miejscowych zagrożeń,

- organizowanie i prowadzenie akcji ratowniczych w czasie pożarów, klęsk żywiołowych lub likwidacji miejscowych zagrożeń,
- wykonywanie pomocniczych specjalistycznych czynności ratowniczych w czasie klęsk żywiołowych lub likwidacji miejscowych zagrożeń przez inne służby ratownicze,
- kształcenie kadr dla potrzeb państwowej straży pożarnej i innych jednostek ochrony przeciwpożarowej oraz powszechnego systemu ochrony ludności,
- nadzór nad przestrzeganiem przepisów przeciwpożarowych,
- prowadzenie prac naukowo-badawczych w zakresie ochrony przeciwpożarowej oraz ochrony ludności
- współpraca z szefem krajowego centrum informacji kryminalnych w zakresie niezbędnym do realizacji jego zadań ustawowych.

Organizację i prowadzenie akcji ratowniczej określa rozdział 3 wspomnianej ustawy. Przedstawiono tu najważniejsze regulacje w niej zawarte:

- akcję ratowniczą organizuje i kieruje nią państwowa straż pożarna.
- podczas wykonywania pomocniczych specjalistycznych czynności ratowniczych w czasie klęsk żywiołowych lub likwidacji miejscowych zagrożeń, w przypadku akcji ratowniczych organizowanych przez inne służby ratownicze, jednostki organizacyjne państwowej straży pożarnej, biorące udział w tych akcjach ratowniczych obowiązane są przestrzegać wskazań lub instrukcji osób kierujących.
- strażacy biorący udział w akcji ratowniczej, w zakresie niezbędnym do prowadzenia tej akcji, mają prawo korzystania z:
  - dróg, gruntów i zbiorników wodnych państwowych, komunalnych i prywatnych,
  - komunalnych i prywatnych ujęć wodnych i środków gaśniczych.
- w okolicznościach uzasadnionych stanem wyższej konieczności strażak kierujący akcją ratowniczą ma prawo zarządzenia:
  - ewakuacji ludzi i mienia z terenu objętego akcją ratowniczą,
  - koniecznych prac wyburzeniowych i rozbiórkowych,
  - wstrzymania komunikacji w ruchu lądowym,
  - udostępnienia pojazdów, środków i przedmiotów niezbędnych do akcji ratowniczej,
  - zakazu przebywania osobom postronnym w rejonie akcji ratowniczej.

- ponadto, kierujący akcją ma prawo:
  - żądania niezbędnej pomocy od instytucji państwowych, jednostek gospodarczych, organizacji społecznych i obywateli,
  - odstąpienia od zasad działania uznanych powszechnie za bezpieczne.

Jednostki wojskowe

Minister Obrony Narodowej może przekazać do dyspozycji wojewody oddziały Sił Zbrojnych pozostające pod dowództwem przełożonych służbowych, lecz wykonujące zadania określone przez wojewodę. W przypadkach niecierpiących zwłoki decyzję o wprowadzeniu do akcji może podjąć samodzielnie dowódca jednostki wojskowej.

Zasadnicze zadania realizowane przez elementy sił zbrojnych to[25]:

- współudział w monitorowaniu zagrożeń;
- wykonywanie zadań związanych z oceną skutków zjawisk zaistniałych na obszarze występowania zagrożeń;
- wykonywanie zadań poszukiwawczo-ratowniczych;
- ewakuowanie poszkodowanej ludności i mienia;
- wykonywanie zadań mających na celu przygotowanie warunków do czasowego przebywania ewakuowanej ludności w wyznaczonych miejscach;
- współudział w ochronie mienia pozostawionego na obszarze występowania zagrożenia;
- izolowanie obszaru wystękiwania zagrożeń lub miejsca prowadzenia akcji ratowniczej.
- wykonywanie prac zabezpieczających, ratowniczych i ewakuacyjnych przy zagrożonych obiektach budowlanych i zabytkach;
- prowadzenie prac wymagających użycia specjalistycznego sprzętu technicznego lub materiałów wybuchowych będących w zasobach Sił Zbrojnych RP;
- usuwanie materiałów niebezpiecznych i ich unieszkodliwianie, z wykorzystaniem sił i środków będących do użycia;
- likwidowanie skażeń chemicznych oraz skażeń i zakażeń biologicznych;
- usuwanie skażeń promieniotwórczych;
- wykonywanie zadań związanych z naprawą i odbudową infrastruktury technicznej;
- współudział w zapewnieniu przejezdności szlaków komunikacyjnych;

- udzielanie pomocy medycznej i wykonywanie zadań sanitarnohigienicznych i przeciwepidemycznych;
- wykonywanie zadań ujętych w wojewódzkich planach reagowania kryzysowego.

Główny Inspektorat Sanitarny, Wojewódzkie Stacje Sanitarno - Epidemiologiczne

Po otrzymaniu informacji od zespołów reagowania kryzysowego inspekcje Sanepidu prowadzą działania w akcji prewencyjnej razem z innymi jednostkami. Przeprowadzają kontrole sanitarne na terenach zagrożonych oraz biorą udział w akcji informowania i edukacji poszkodowanych, przeprowadzają dezynfekcję oraz udostępniają środki dezynfekcyjne do samodzielnego wykorzystania.

Państwowa Inspekcja Ochrona Środowiska

Funkcjonowanie inspekcji ochrony środowiska określa ustawa. Do zadań inspekcji ochrony środowiska w szczególności należy:

- kontrola przestrzegania przepisów o ochronie środowiska i racjonalnym użytkowaniu zasobów przyrody,
- kontrola przestrzegania decyzji ustalających warunki użytkowania środowiska,
- udział w postępowaniu dotyczącym lokalizacji inwestycji,
- udział w przekazywaniu do użytku obiektów lub instalacji realizowanych jako przedsięwzięcie mogące znacząco oddziaływać na środowisko,
- kontrola eksploatacji instalacji i urządzeń chroniących środowisko przed zanieczyszczeniem,
- podejmowanie decyzji wstrzymujących działalność prowadzoną z naruszeniem wymagań związanych z ochroną środowiska lub naruszeniem warunków korzystania ze środowiska,
- współdziałanie w zakresie ochrony środowiska z innymi organami kontrolnymi, organami ścigania i wymiaru sprawiedliwości oraz organami administracji państwowej i rządowej, samorządu terytorialnego i obrony cywilnej, a także organizacjami społecznymi i opiekunami społecznymi,

[25] Ustawa z dnia 26 kwietnia 2007 r. *o zarządzaniu kryzysowym* (Dz. U. Nr 89, poz. 590), art. 25, ust. 3

- organizowanie i koordynowanie państwowego monitoringu środowiska, prowadzenie badań jakości środowiska, obserwacji i oceny jego stanu oraz zachodzących w nim zmian,
- opracowywanie i wdrażanie metod analityczno-badawczych i kontrolno-pomiarowych,
- inicjowanie działań tworzących warunki zapobiegania poważnym awariom oraz usuwania ich skutków i przywracania środowiska do stanu właściwego,
- kontrola przestrzegania przepisów o opakowaniach i odpadach opakowaniowych,
- kontrola przestrzegania przepisów o obowiązkach przedsiębiorców w zakresie gospodarowania niektórymi odpadami oraz o opłacie produktowej i opłacie depozytowej,
- kontrola przestrzegania przepisów i uzyskanych na ich podstawie zezwoleń, z wyłączeniem kontroli laboratoryjnej, w zakresie postępowania z organizmami genetycznie zmodyfikowanymi.

1.2.3. Procedury kierowania reagowaniem kryzysowym

Przez **zarządzanie kryzysowe** rozumie się uporządkowaną działalność polegająca na zapobieganiu sytuacjom kryzysowym lub przejmowaniu nad nimi kontroli i kształtowaniu ich przebiegu w drodze zaplanowanych działań oraz na odtworzeniu zasobów lub przywróceniu ich pierwotnego charakteru.

Jest ono procesem bardziej złożonym, niż zarządzanie realizowane w warunkach „normalnych", co wynika przede wszystkim z samej istoty zjawiska kryzysowego (zagrożenie życia ludności, straty w mieniu, zniszczenie lub uszkodzenie obiektów infrastruktury komunikacyjnej, w tym systemu łączności, niedostatek informacji, potrzeba działania w krótkim czasie i przy niedoborze sił i środków niezbędnych do skutecznej reakcji).

Organizując **„zintegrowany system kierowania i zarządzania na wypadek kryzysu"** należy mieć na uwadze jego uniwersalny (jednolity) charakter. Oznacza to, iż w warunkach „normalnych" funkcjonuje on jedynie w niezbędnym zakresie (głównie ze względów oszczędnościowych). Natomiast jego rozwinięcie następuje dopiero w sytuacji kryzysowej – w stopniu adekwatnym do jej skali (klęska żywiołowa, duża katastrofa, lokalny konflikt zbrojny), tak aby najwyższą gotowość oraz maksymalną wydolność osiągnął podczas największego zagrożenia (np. w czasie wojny). Jednak cały czas winien być to jeden i ten sam system, w którym zasadniczy skład osobowy, sprzęt i wyposażenie (zwłaszcza teleinforma-

tyczny), nie zmieniają się, a są jedynie uzupełniane (rozwijane) – stosownie do potrzeb wynikających z zaistniałej sytuacji i prognozowanego jej rozwoju (zmian).

Zarządzanie kryzysowe jest realizowane w czterech fazach:

- zapobiegania,
- przygotowania,
- reagowania,
- odbudowy.

Faza zapobiegania obejmuje eliminowanie lub redukowanie prawdopodobieństwa sytuacji kryzysowej oraz ograniczanie jej skutków. W fazie tej dokonuje się identyfikacji zagrożeń oraz realizuje się monitoring zjawisk mogących stanowić ich źródło. Prowadzona jest także analiza ryzyka wystąpienia określonych zagrożeń oraz opracowywana prognoza ich skutków. Na tej podstawie, uwzględniając dostępne zasoby, organizuje się działania zapobiegawcze. Zasadnicze zadania realizowane w tej fazie to:

- działania redukujące i eliminujące prawdopodobieństwo wystąpienia sytuacji kryzysowej,
- działania uprzedzające, mające na celu ograniczenie skutków sytuacji kryzysowej.

W **fazie przygotowania** planuje się procedury reagowania w najbardziej prawdopodobnych sytuacjach kryzysowych, a także podejmuje się działania mające na celu zapewnienie zasobów niezbędnych do skutecznego reagowania w tychże sytuacjach. Tworzy się również warunki do przetrwania ludności (przygotowanie ukryć, schronów, gromadzenie indywidualnych środków ochrony, organizacja miejsc tymczasowego zakwaterowania, dostaw wody, energii, żywności, odzieży, lekarstw, środków czystości itp.), oraz do sprawnego zarządzania po zaistnieniu sytuacji kryzysowej.

Organizuje się systemy: monitoringu oraz ostrzegania i alarmowania.

Szczególnego znaczenia dla sprawnej realizacji procesu zarządzania, w tym gromadzenia, przetwarzania i obiegu informacji, nabiera stworzenie wydolnego systemu teleinformatycznego.

Ważne miejsce w procesie przygotowania zajmuje szkolenie obsady poszczególnych ogniw systemu zarządzania, a także przygotowanie i przeszkolenie podmiotów przewidzianych do działań praktycznych. Zasadnicze zadania tej fazy to:

- działania planistyczne dotyczące sposobów reagowania na czas wystąpienia sytuacji kryzysowej,

- działania mające na celu powiększenie zasobów sił i środków niezbędnych do efektywnego reagowania.

Analizując zapisy dokumentów normatywnych oraz rozwiązań praktycznych stwierdzono, że długofalowy plan działania zespołu reagowania kryzysowego powinien być opracowywany w odniesieniu do następujących założeń:

Po pierwsze: dokonać należy oceny (analizy) zagrożenia swojego obszaru odpowiedzialności. W tym celu należy ustalić:

1) z jakimi zagrożeniami dla bezpieczeństwa ludności, jej mienia i środowiska należy się liczyć (szacowanie ryzyka zagrożeń, historia, skala zdarzeń)

2) jak bardzo nasz obszar odpowiedzialności (ludzie, infrastruktura, środowisko i in.) jest podatny na potencjalne zagrożenia;

3) wybrać z katalogu zagrożeń te, które zostaną uznane za znaczące dla naszego obszaru odpowiedzialności i wokół nich skupić główny wysiłek w dalszych działaniach.

Po drugie: opracować część główną „Planu reagowania kryzysowego", w której należy wstępnie i ogólnie określić

- podstawowe działania (zadania, obowiązki), do podjęcia których zobowiązane są instytucje i jednostki organizacyjne

- uczestniczące w procesie reagowania na sytuację kryzysową spowodowaną katastrofą lub innym zdarzeniem niebezpiecznym o dużej skali.

Po trzecie: przystąpić do opracowywania aneksów funkcjonalnych do planu reagowania kryzysowego obejmujących następujące zagadnienia szczegółowe (przykładowo):

- Ostrzeganie o zagrożeniach i alarmowanie
- Kierowanie działaniami
- Ratownictwo
- Ewakuacja
- Pomoc medyczna
- Pomoc społeczna
- Łączność
- Transport
- Zarządzanie zasobami
- Zapewnienie porządku publicznego
- Ocena i szacowanie szkód

Po czwarte: równolegle z opracowywaniem wyżej wymienionych aneksów funkcjonalnych jako elementów składowych planu reagowania kryzysowego w poszczególnych instytucjach i jednostkach organizacyjnych opracowywać „Standardowe procedury operacyjne" (np. dla Komendy Państwowej Straży Pożarnej, Komendy Policji, szpitala powiatowego, Powiatowego CZK, Urzędu Gminy, Wydziału Gospodarki Mieszkaniowej w Urzędzie Miasta, gminnego Zakładu Wodociągów i Kanalizacji, rejonowego Zakładu Usług Energetycznych i wielu innych jednostek organizacyjnych).

Plan kryzysowy powinna posiadać każda jednostka organizacyjna. Koniecznie należy przeprowadzić inwentaryzację istniejących planów i ustalić stopień ich zgodności z innymi planami odpowiedniego szczebla.

Planowanie zintegrowane.

Planowanie działania różnych podmiotów będących w gestii poszczególnych elementów administracji rządowej, samorządowej, służb lub jednostek wojskowych wymaga dużego wysiłku organizacyjnego w celu ich koordynowania. Idea zintegrowanego planowania wynika z tego, aby:

- w sposób zorganizowany i skuteczny, użyć sił i środków będących w dyspozycji różnych podmiotów, określić sposób ich użycia i zasady koordynowania ich działań wcześniej zaplanować;
- koszty wynikające ze zdarzenia o charakterze nadzwyczajnym nie były powiększane o bezzasadnie wykreowane;
- poprzez dysponowanie sił i środków nieadekwatnych do rzeczywistych potrzeb, należy posiadać odpowiednio elastyczne plany;
- skutecznie zarządzać podmiotami i osobami niezobligowanymi do podległości, nie naruszając ich suwerenności i uzyskać efekt synergii należy mieć plany, w procesie tworzenia których wynegocjowaliśmy zasady współdziałania;
- ograniczyć koszty tworzenia rezerw sprzętowo-materiałowych, powinniśmy mieć plany wykorzystania „zasobów obcych", na zasadach wynegocjowanych w procesie planowania;
- uniknąć, szczególnie w pierwszej fazie działań błędów wynikających z braku przygotowania;
- nie przeoczyć rozwijającego się zagrożenia, powinniśmy mieć jednoznacznie określony w planie, a przede wszystkim system zarządzania informacjami;

- być gotowym należy organizować ćwiczenia, które powinny polegać na trenowaniu procedur zawartych w planie.

Faza reagowania polega na podejmowaniu przedsięwzięć, zmierzających do przeciwdziałania narastaniu sytuacji kryzysowej, udzielenia pomocy poszkodowanym oraz do ograniczenia zniszczeń i strat wywołanych zjawiskami, które doprowadziły do tej sytuacji. Należy do nich przede wszystkim wszczęcie określonych procedur, stosownie do stopnia i zakresu zagrożenia, w tym skierowanie odpowiednich sił i środków do działań ratowniczych, co wymaga sprawnego kierowania i ścisłej koordynacji.

Wymienione działania prowadzone są do czasu ustania przyczyn, które spowodowały powstanie sytuacji kryzysowej, a zasadnicze zadania tej fazy dotyczą:

- działania polegającego na dostarczeniu pomocy poszkodowanym,
- działania hamującego rozwój występujących zagrożeń,
- działania ograniczającego straty i zniszczenia.

Szacowanie jest nader istotnym elementem reagowania na katastrofę. Jednak fundamentalne znaczenie mają prace w tym zakresie w ramach fazy zarządzania kryzysowego określanej jako „przygotowanie". Szacowanie jest procesem określania wpływu zagrożenia na społeczeństwo, potrzeb i priorytetów pomocy, dostępnych zasobów, potrzeb w zakresie odbudowy i dalszego rozwoju.

Dane są materiałem źródłowym do szacowania. Dane źródłowe wymagają jednak przetworzenia we wskaźniki i informacje.

Nadmiar danych prowadzi do przeładowania systemu ich przetwarzania. Niepełne dane nie oddają prawdziwego obrazu sytuacji.

Uwagi dotyczące szacowania:

- systemy szacowania na wypadek katastrof powinny być ustanowione zawczasu (jako część planu reagowania kryzysowego),
- dane powinny odpowiadać potrzebom użytkowników,
- wyznaczony koordynator do danych,
- staranny wybór osób wyznaczonych do zbierania danych,
- specyfikacja danych do zbierania,
- włączenie osób, które przetrwały katastrofę,
- zbieranie danych ukierunkowane na przyszłość (*doświadczenie*),
- skupienie na istotnych obszarach zagrożeń,
- wykorzystanie istniejących systemów,

- budowanie interdyscyplinarnych zespołów,
- standaryzacja sposobów zapisywania i prezentowania danych,
- wcześniejsze ustalenie komu będą potrzebne dane i jak je dostarczyć,
- ustalenie struktury danych wejściowych dla wsparcia procesu wypracowania decyzji,
- zapewnienie oszacowania krytycznych odcinków: ratownictwo medyczne, poszukiwania i ratownictwo, krytyczna.

Podczas oceny sytuacji w fazie reagowania na zagrożenia szczególne działania podejmować należy w odniesieniu do następujących przedsięwzięć oraz obszarów problemowych tak, aby można było dokonać:

- ustalenia granic obszaru dotkniętego katastrofą;
- identyfikacji blokad w transporcie lądowym, wodnym i powietrznym;
- identyfikacji wtórnych zagrożeń;
- oszacowania szkód w systemie łączności;
- sprecyzowania obszarów, z których nie napływają informacje;
- ustalenia statusu szpitali i innych ośrodków medycznych w rejonie katastrofy lub pobliskim;
- lokalizacji izolowanych lub ciężko poszkodowanych obszarów;
- nadania priorytetów obszarom wymagającym ratownictwa;
- zapewnienia działania centrów szacowania (zbierania danych);
- określenia dostępności istotnych zasobów;
- określenia potrzeb w zakresie tymczasowego schronienia;
- wsparcia działań lokalnej administracji;
- oszacowania statusu życiowych systemów: łączności, zaopatrzenia w wodę, elektryczności, dróg, kanalizacji i innych według własnego rozeznania.

Faza odbudowy to przywrócenie stanu sprzed sytuacji kryzysowej. Jest to osiągane poprzez uruchomienie programów pomocy indywidualnej i zbiorowej dla poszkodowanej ludności, doraźne zapewnienie funkcjonowania urządzeń i obiektów użyteczności publicznej i infrastruktury komunalnej, przywrócenie gotowości podmiotów ratowniczych oraz odtworzenie i uzupełnienie niezbędnych zasobów sprzętu i środków materiałowych.

Do zasadniczych zadań w tej fazie należą:

- działania mające na celu przywrócenie zdolności reagowania,
- działania mające na celu odbudowę zapasów służb ratowniczych,

- działania mające na celu odtworzenie kluczowej dla województwa infrastruktury telekomunikacyjnej, energetycznej, paliwowej, transportowej i dostarczania wody.

Dokonana w toku procesu badawczego analiza procedur działania poszczególnych zespołów odpowiedzialnych za kierowanie reagowaniem kryzysowym na wszystkich poziomach systemu pozwoliła na określenie wniosków, które po uogólnieniu można przedstawić w formie bezpośrednich dyrektyw ich funkcjonowania. Istota algorytmu postępowania zespołu sprowadza się do działania zgodnie z następującymi zaleceniami:

1. **Zauważyć zdarzenie** – czyli posiadać należy system monitorowania zagrożeń i alarmowego o nich powiadamiania, system obiegu informacji o zdarzeniach itp.
2. **Interpretować** - np. mieć wypracować czytelny i udokumentowany sposób kwalifikowania zdarzeń na takie, które muszą mieć dalszy ciąg i inne, którymi nie trzeba się bardzo zajmować.
3. **Przewidzieć skutki** – działać z wyobraźnią, lecz wspartą wiedzą i doświadczeniem.
4. **Wiedzieć jak pomóc** - np. znać możliwości reagowania na konkretne zagrożenie, posiadać wyczucie własnych możliwości, bazy danych i umiejętność ich wykorzystania.
5. **Zrealizować plan działania**, który może być już opracowany /procedura reagowania/ lub istniejący plan należy dostosować do zaistniałej sytuacji lub należy bardzo szybko zareagować na nowe uwarunkowania działania.
6. **Nie szkodzić, czyli „**Primum non nocere!", działajmy tak aby tylko nie pogorszyć sytuacji.

1.2.4. Dokumenty planistyczne kierowania reagowaniem kryzysowym

Prowadzony proces badawczy wykazał, że w konstruowaniu struktury oraz zasad funkcjonowania systemu teleinformatycznego wspierającego kierowanie reagowaniem kryzysowym wykazało, że szczególne znaczenie mają w tym zakresie dokumenty planistyczne kierowania reagowaniem kryzysowym. W dokumentach tych określa się bowiem zasadnicze obszary działania, podmioty realizujące poszczególne zadania oraz szereg zagadnień koordynacyjnych.

Planowanie działalności cywilnej to przedsięwzięcia planistyczne i organizacyjne oraz przygotowania rzeczowe, wykonywane zwłaszcza poprzez formułowanie planów i programów w zakresie zapobiegania, przygotowania, reagowania i odbudowy, zapewniające osią-

gnięcie właściwego stanu gotowości cywilnej i zarządzania kryzysowego na każdym stopniu podziału terytorialnego państwa.

Plan reagowania kryzysowego określa zespół przedsięwzięć na wypadek zagrożeń noszących znamiona klęski żywiołowej, a w szczególności:

- zadania w zakresie monitorowania zagrożeń;
- bilans sił ratowniczych i środków technicznych niezbędnych do usuwania skutków zagrożeń;
- procedury uruchamiania działań przewidzianych w planie oraz zasady współdziałania, a także sposoby ograniczania rozmiaru strat i usuwania skutków zagrożeń;

Plan reagowania kryzysowego jest uzgadniany z kierownikami jednostek organizacyjnych planowanych do użycia w realizacji przedsięwzięć określonych w planie w zakresie dotyczącym tych jednostek, a następnie zatwierdzany przez organ administracji publicznej wyższego stopnia.

Celem Planu Reagowania Kryzysowego Województwa jest zapewnienie społeczeństwu województwa podstawowych warunków ochrony przed skutkami katastrof naturalnych i awarii technicznych noszących znamiona klęski żywiołowej.

Plan jest zasadniczym dokumentem określającym zasady działania Wojewody, administracji zespolonej województwa oraz wszystkich innych uczestników procesu reagowania kryzysowego na szczeblu wojewódzkim. Elementami składowymi planu są[26]:

- ocena stanu zagrożenia województwa;
- sposoby reagowania podmiotów szczebla wojewódzkiego na sytuacje kryzysowe;
- ogólna procedura działań podejmowanych na szczeblu wojewódzkim w fazach reagowania i odbudowy;
- szczegółowe procedury specjalistyczne dotyczące postępowania jednostek organizacyjnych i instytucji szczebla wojewódzkiego w sytuacjach występowania wytypowanych zagrożeń;
- bilans sił i środków szczebla wojewódzkiego i możliwości ich wykorzystania w procesie reagowania kryzysowego.

Przedsięwzięcia zaplanowane w PRKWW stanowią kontynuację działań określonych w planach poszczególnych służb, inspekcji i straży, w sytuacjach określonych w ustawie o stanie klęski żywiołowej, które wymagają podjęcia nadzwyczajnych środków, we współdzia-

[26] Na przykładzie założeń i zasad działania organów administracji publicznej Województwa Wielkopolskiego.

łaniu różnych organów i instytucji oraz specjalistycznych służb i formacji działających pod jednolitym kierownictwem.

Ustalenia Planu Reagowania Kryzysowego Województwa Wielkopolskiego, w zakresie systemów łączności, ostrzegania i alarmowania ludności, obiegu informacji, organizacji monitorowania oraz szczegółowych rozwiązań w integralnych planach specjalistycznych, narzucają określone rozwiązania dla szczebla powiatowego i gminnego.

Wojewódzki Plan Reagowania Kryzysowego realizowany będzie w następujących przypadkach i w zakresie:

- po wprowadzeniu stanu klęski żywiołowej na obszarze województwa w pełnym zakresie,
- w sytuacji wystąpienia znamion klęski żywiołowej na terenie województwa – w ograniczonym zakresie.

W innych sytuacjach nie będących klęską żywiołową, a wymagających skoordynowanych działań - w zakresie zdefiniowanym w planach i procedurach szczegółowych będących elementem powyższego planu:

1. Wojewódzki plan postępowania awaryjnego w przypadku zdarzeń radiacyjnych.
2. Plan operacyjny ochrony przed powodzią.
3. Plan postępowania w czasie zagrożenia epidemiologicznego i epidemii oraz zwalczania bioterroryzmu.

Wojewódzki Plan Reagowania Kryzysowego opracowany jest przez pracowników Wydziału Zarządzania Kryzysowego, we współpracy z zasadniczymi podmiotami administracji zespolonej i niezespolonej biorącymi udział w reagowaniu kryzysowym. Plan jest zatwierdzony przez Ministra Spraw Wewnętrznych i Administracji.

Układ planu może być następujący:

WSTĘP

I. WNIOSKI Z OCENY ZAGROŻEŃ WOJEWÓDZTWA WIELKOPOLSKIEGO

1. Ocena zagrożeń;
2. Przyczyny zagrożeń;
3. Analiza zagrożeń;
4. Wnioski z oceny zagrożeń:

   Tabela 1.1.Ocena skutków zagrożeń,

   Tabela 1.2.Analiza zagrożeń pod kątem prawdopodobieństwa ich wystąpienia oraz skutków i konsekwencji prawnych.

61

II. ORGANIZACJA REAGOWANIA, PLANOWANE PRZEDSIĘWZIĘCIA ORAZ PRZYDZIAŁ OBOWIĄZKÓW

1. Zadania w zakresie monitorowania zagrożeń:

   Tabela II.1 Rodzaje i wykonawcy prowadzonego monitoringu;
2. Obieg informacji:

   Schemat II.1.Obieg informacji;
3. Informowanie, ostrzeganie i alarmowanie ludności:

   Schemat II.2.Ostrzeganie i alarmowanie;
4. Organizacja łączności;
5. Procedura uruchamiania działań Wojewódzkiego Zespołu Reagowania Kryzysowego:

   Schemat II.3. Etapy rozwijania WZRK;
6. Procedura ogólna:

   6.1. Procedura działań WZRK w fazie reagowania,

   Tabela II.2. Wykaz przydziału zadań,

   Tabela II.3. Plan przydziału funkcji w zakresie reagowania kryzysowego,

   Schemat II.4. Ogólna procedura reagowania kryzysowego,

   6.2. Działania w fazie odbudowy.

III. ZASOBY SIŁ I ŚRODKÓW MOŻLIWYCH DO WYKORZYSTANIA W USUWANIU SKUTKÓW KLĘSK ŻYWIOŁOWYCH

1. Informatyczna baza danych sił i środków województwa;
2. Zasady pozyskiwania zasobów finansowych;
3. Możliwości wykorzystania krajowych organizacji pozarządowych;
4. Możliwości przyjęcia międzynarodowej pomocy humanitarnej i ratowniczej;
5. Zasoby specjalistycznych sił i środków;
6. Udział formacji obrony cywilnej szczebla wojewódzkiego w sytuacjach kryzysowych;
7. Wykorzystanie regionalnych środków masowego przekazu w stanach klęsk żywiołowych:

   7.1. Podstawy prawne,

   7.2. Procedura przekazania mediom informacji w sytuacji niebędącej stanem klęski żywiołowej,

   Schemat III.1. Procedura przekazywania mediom rozporządzeń RM, komunikatów, sygnałów ostrzegawczych i alarmowych.

Szeregu interesujących wniosków w zakresie tworzenia zintegrowanego systemu kierowania zarządzaniem kryzysowym dostarczyła także analiza założeń funkcjonowania Systemu Państwowego Ratownictwa Medycznego. Zasadnicze znaczenie przy planowaniu rozmieszczenia jednostek tego systemu miała konieczność zapewnienia czasów dotarcia zespołów ratownictwa medycznego od miejsca zdarzenia od chwili przyjęcia zgłoszenia przez dyspozytora medycznego. Maksymalny czas dotarcia zespołów ratownictwa medycznego nie może być dłuższy niż 15 minut w mieście liczącym powyżej 10 tysięcy mieszkańców i nie dłuższy niż 20 minut poza tymi miastam.

Dokumenty planistyczne dotyczące tego obszaru działania mogą obejmować[27]:

- wprowadzenie i założenia wstępne;
- charakterystyka potencjalnych zagrożeń i analiza ryzyka wystąpienia katastrof naturalnych i awarii technicznych;
- liczba i rozmieszczenie jednostek systemu;
- sposób koordynowania jednostek systemu;
- kalkulacja kosztów działania ZRM;
- sposób współpracy jednostek systemu;
- Centra Powiadamiania Ratunkowego;
- Opis struktury systemu powiadamiania;
- Wykaz jednostek organizacyjnych szpitali wyspecjalizowanych w zakresie udzielania świadczeń zdrowotnych niezbędnych dla ratownictwa medycznego;
- Nadzór i kontrola realizowana przez Wojewodę.

Powyższe dokumenty zamieszczone zostały zgodnie z ustawowym wymogiem podania treści planu do publicznej wiadomości (art. 21 ust 13 ustawy z dnia 8 września 2006 roku o Państwowym Ratownictwie Medycznym - Dz. U. Nr 191, poz. 1410). Plan działania systemu został umieszczony na stronie internetowej *Biuletynu Informacji Publicznej* Wielkopolskiego Urzędu Wojewódzkiego w Poznaniu w dziale „ZDROWIE".

[27] *Biuletynu Informacji Publicznej* Wielkopolskiego Urzędu Wojewódzkiego, Poznań 2007.

63

1.3. Zasady planowania i realizacji kierowania reagowaniem kryzysowym

Prowadzone badania pozwoliły także na dokonanie analizy założeń oraz zasad realizacji przedsięwzięć związanych z reagowaniem kryzysowym. Ich porównanie, synteza zasadniczych aspektów oraz uogólnienie pozwoliło na przedstawienie zasadniczych z nich, które ujęto poniżej.

Elastyczność rozumiana jako gotowość sprostania każdemu zagrożeniu i w każdych warunkach. Należy zachować margines dla inwencji operacyjnej.

Funkcjonalność to wykorzystanie zasobów w dowolnej sytuacji na odcinku cywilnym jak i militarnym. Wymaga to ciągłego uaktualniania dokumentacji i doskonalenia procesu zarządzania kryzysowego.

Efektywność to podejście koszt – efekt. Umożliwia prowadzenie racjonalnych działań na poziomie minimalnych kosztów ludzkich i finansowo-materiałowych.

Adekwatność przestrzeganie tej zasady pozwala na angażowania stosownych zasobów i kompetencji do określonej sytuacji. Gwarantuje to działanie na najniższym koniecznym poziomie reagowania.

Powszechność odnosi się do włączania do systemu wszystkich poziomów władzy, instytucji, organizacji i podmiotów gospodarczych oraz wszystkich mieszkańców w tym mieszkańców innych państw na stałe zamieszkujących w Polsce.

Profesjonalizm personelu to wysoki poziom wiedzy specjalistycznej, doświadczenie, zdolności mediacyjne itd. Profesjonalizm gwarantuje najlepsze wywiązywanie się z obowiązków, autorytet, wiarygodność i akceptację społeczeństwa.

Wiarygodność jest wynikiem skuteczności systemu i może zapewnić (lub nie) akceptację społeczną, ma to szczególne znaczenie zwłaszcza na poziomie lokalnym.

Akceptacja społeczna to rezultat profesjonalnych działań. Brak profesjonalizmu i ignorancja w połączeniu z arogancją wywołują skutki odwrotne i znacznie podwyższają ryzyko.

Gotowość to możliwości i umiejętności i nie jest to stan jednorazowy. Gotowość to stan osiągany w permanentnej działalności celowej, ciągle modyfikowany i doskonalony.

Zdolność do improwizacji umiejętność gwarantująca realizację ciągu uporządkowanych działań w zależności od sytuacji. Z doświadczenia wynika, że im niższy szczebel organizacyjny tym więcej improwizacji.

Przejrzystość zapewnienie poprawności struktur działania w każdych warunkach bez konieczności sprawowania ciągłego nadzoru. Każdy element realizuje swoje zadania i nie stara się wkraczać w kompetencje innych.

Odpowiedzialność funkcjonalna oznacza odpowiedzialność organów i instytucji w zakresie sprawowanych funkcji. Poszczególne dziedziny działalności (funkcje) podporządkowane są władzy publicznej niezależnie od poziomu zarządzania. Odpowiedzialność odnosi się do wszystkich funkcji cywilnych istotnych dla gotowości cywilnej.

Odpowiedzialność terytorialna odnosi się do realizacji zadań gotowości cywilnej na poziomie jednostek administracyjnych: gmina, powiat, województwo. Jest ona zróżnicowana w zależności od szczebla zarządzania i sytuacji (pokój, wojna). Odpowiedzialność obejmuje wszystkie funkcje na wszystkich poziomach władzy.

W toku prowadzonych dociekań stwierdzono także, że w praktyce niedopuszczalny jest prymat jednej zasady nad innym. W odniesieniu do działań koncepcyjnych zmierzających do określenia kształtu systemu reagowania kryzysowego, jak również działań praktycznych wszystkie są równie ważne, wzajemnie się przenikają i uzupełniają. Każda zasada może być wręcz traktowana jako element systemu, który spełnia w nim ważną, jednoznaczną i tylko jemu przypisaną rolę.

WNIOSKI

Dokonane uogólnienia wniosków cząstkowych pozwoliły na sformułowanie kilku zasadniczych tez, które uznać można za wnioski zasadnicze lub wręcz wymagania, którym powinien odpowiadać system teleinformatyczny wspomagający kierowanie reagowaniem kryzysowym. Zasadnicze stwierdzenia, które przedstawiono poniżej, dotyczą zarówno aspektów związanych z architekturą systemu, jak również warunkami jego funkcjonowania.

Otrzymane wyniki badań pozwalają na stwierdzenie, że idealnym rozwiązaniem było by stworzenie jednego **zintegrowanego zautomatyzowanego systemu informatycznego**, który funkcjonował by we wszystkich służbach oraz podmiotach biorących udział w kierowaniu siłami i środkami podczas działań związanych z reagowaniem kryzysowym. Zespół badaczy zdaje sobie jednak sprawę, że nie jest możliwe zastosowanie takiego rozwiązania, dlatego koniecznym jest:

- opracowanie koncepcji informatycznego wsparcia kierowania reagowaniem kryzysowym, która w pierwszym rzędzie zawierać będzie wymagania jakie taki system powinien spełniać;

- opracowanie i wdrożenie interfejsów umożliwiających bezkolizyjne przekazywanie informacji pomiędzy różnymi systemami informacyjnymi wszystkich podmiotów biorących udział w kierowaniu reagowaniem kryzysowym;
- opracowanie środowiska informatycznego, które ujednolici dotychczasowe działania różnych organów i służb;
- opracowanie standardu informatycznego, który stanowić będzie podstawę formułowania w przyszłości specyfikacji sprzętowych i programowych;
- określenie harmonogramu działań koncepcyjnych oraz wdrożeniowych;
- oszacowanie kosztów związanych ze wszystkimi działaniami w tym zakresie oraz wskazanie źródeł ich finansowania.

Działania podejmowane w zakresie opracowania koncepcji rozwiązań teleinformatycznego wsparcia działań związanych z kierowaniem reagowaniem kryzysowym wymaga ścisłej korelacji i współdziałania wielu instytucji i podmiotów. Wymaga to ścisłego określenia zadań oraz odpowiedzialności każdego z nich za podejmowane prace. Za celowe wydaje się powoływanie zespołów projektowych zajmujących się poszczególnymi aspektami wsparcia teleinformatycznego. Koniecznym jest także powołanie stałego organu, który ponosił będzie odpowiedzialność za koordynowanie działań koncepcyjnych i wdrożeniowych w tym zakresie.

Wskazując na założenia opracowania systemu informacyjnego można wskazać, że powinien on, między innymi, zapewnić:

- skuteczne administrowanie w sytuacji wykraczającej poza granicę akceptowanego poziomu bezpieczeństwa;
- wdrażanie i utrzymywanie zdolności reagowania;
- zagwarantowanie realizacji procesów społecznych i gospodarczych w sytuacji zagrożenia na akceptowanym poziomie;
- zabezpieczenie racjonalnej i terminowej pomocy ofiarom klęsk i katastrof; zapewnienie wsparcia sektora cywilnego dla wysiłków militarnych i obrony cywilnej podczas działań zbrojnych; racjonalne wykorzystanie zasobów ludzkich, finansowych i materiałowych.

Istotnym wnioskiem jest także stwierdzenie, że rola i zadania osób i organizacji w zakresie reagowania kryzysowego powinny być jasno określone i dobrze zrozumiane, dobre wzajemne relacje ustanawiać można podczas wspólnych szkoleń, treningów i ćwiczeń.

2. UWARUNKOWANIA FUNKCJONOWANIA SYSTEMÓW TELEINFORMATYCZNYCH

Efektywne funkcjonowanie procesu kierowania reagowaniem kryzysowym zależy m. in. od skuteczności działania systemu dowodzenia, systemu zasilania i systemu łączności (w tym podsystemu wymiany informacji). Od podsystemu wymiany informacji, w skład którego wchodzą współdziałające (zarówno cywilne jak i wojskowe) sieci komputerowe oraz sieci telekomunikacyjne i teleinformatyczne, zależy skuteczność współpracy wojsk lądowych i ich cywilnych kooperantów. Z przeprowadzonych badań wynika, że głównym zadaniem podsystemu wymiany informacji jest zapewnienie przesyłania informacji na różne odległość, w różnej postaci, z wykorzystaniem różnych technologii transmisji danych (Ethernet, ATM, ISDN), różnorodnego medium transmisyjnego (kabel, światłowód, fale radiowe, podczerwień, laser) oraz protokołów komunikacyjnych (TCP/IP, NETBUI)[1].

W każdym procesie dowodzenia, kierowania czy też zarządzania niezmiernie ważne są dwie podstawowe funkcje systemu łączności (podsystemu wymiany informacji) a mianowicie przesyłanie danych pomiędzy elementami systemu dowodzenia (osobami funkcyjnymi i/lub zespołami funkcjonalnymi) oraz wspomaganie przetwarzania informacji w cyklu decyzyjnym. Podczas realizacji procesu kierowania reagowaniem kryzysowym podsystem wymiany informacji powinien być przygotowany do działania w różnorodnym i specyficznym otoczeniu zarówno wewnętrznym jak i zewnętrznym. Podstawowym elementem otoczenia wewnętrznego podsystemu wymiany informacji (systemu łączności) są jego użytkownicy (osoby funkcyjne, zarówno wojskowe jak i cywilne). Ze względu na dużą dynamikę zmian mogących zaistnieć w trakcie kryzysu oraz wysoki stopień rozproszenia potencjalnych zagrożeń podsystem wymiany informacji powinien świadczyć usługi transmisji danych oraz usługi dostępu do zasobów informacyjnych w strukturze systemu kierowania (dowodzenia) możliwie na najniższych szczeblach. Działające w rejonie kryzysu organy administracji publicznej i terenowej, istniejąca infrastruktura teleinformatyczna i potencjalny wpływ zaistniałej sytuacji kryzysowej na funkcjonowanie systemów teleinformatycznych stanowi otoczenie zewnętrzne. Oddziałuje ono na podsystem wymiany informacji poprzez zakres i skalę działań reagowania kryzysowego.

Przeprowadzone analizy pozwalają na stwierdzenie, że rejon w którym wykonywane są działania związane z reagowaniem kryzysowym wpływa bezpośrednio na funkcjonowanie

i możliwości systemów teleinformatycznych. Do czynników mających wpływ na systemy teleinformatyczne należy zaliczyć:

- wielkość rejonu (obszaru);
- charakter rejonu (gęstość zabudowy);
- istniejąca infrastruktura techniczna rejonu (w tym infrastruktura teleinformatyczna).

Wielkość i charakter obszaru działań (obszaru kryzysu) determinuje m. in. warunki propagacji fal radiowych i w istotny sposób ogranicza zasięg fal radiowych w zakresie UKF. Obszary o gęstej zabudowie (gęsto zaludnione i o dużym uprzemysłowieniu) charakteryzują się zakłóceniami elektromagnetycznymi.[2]

Analizy wykazały, że istotnymi czynnikami mającymi wpływ na podsystem wymiany informacji są także warunki klimatyczne, meteorologiczne i propagacyjne. Do ważnych czynników z tego zakresu należy zaliczyć odpowiednio:

- długość dnia i nocy;
- prognozę pogody oraz jej wpływ na istniejącą infrastrukturę (temperatura, opady atmosferyczne, wilgotność powietrza);
- stan atmosfery, troposfery (zjawisko rozproszenia w troposferze fal UKF)[3] i jonosfery (propagacja odbicia od warstw jonosfery)[4].

Wymienione czynniki mogą w istotnym stopniu zmniejszyć lub zwiększyć możliwości eksploatacyjne systemów teleinformatycznych, a także wywierać pośredni wpływ na personel obsługujący te systemy.

2.1. Wymagania stawiane wobec systemów teleinformatycznych

W procesie kierowania reagowaniem kryzysowym posiadane (wykorzystywane) systemy teleinformatyczne (w tym systemy łączności) muszą zapewnić sprawne funkcjonowanie stworzonego systemu kierowania (dowodzenia). Systemy te muszą umożliwić zachowanie istotnych właściwości stworzonego systemu kierowania, takich jak: jedność kierowania (*ang. Unity of Command*), ciągłość kierowania (*ang. Continuity of Command*), przejrzysta struktura systemu kierowania (*ang. Clear Chain of Command*), integracja kierowania (*ang. Integration of Command*) oraz decentralizacja kierowania (*ang. Decentralization of Command*).

---

[1] M. Sportack, „*Sieci Komputerowe*", wyd. cyt. s. 75-116.
[2] P. Daniluk, „*Radiowa służba stała i ruchoma*", Akademia Obrony Narodowej – Wydział Wydawniczy, Warszawa 2004, s. 35.
[3] Tamże, wyd. cyt., s. 148-153.
[4] P. Daniluk, „*Radiowa służba stała i ruchoma*", wyd. cyt., s. 148-153.

Z analizy literatury wynika, że wymagania stawiane przed systemami teleinformatycznymi można podzielić na dwie podstawowe grupy: **wymagania operacyjne** i **wymagania techniczno-eksploatacyjne**.

2.1.1. Wymagania operacyjne

Wymagania operacyjne wynikają w głównej mierze z faktu, że wykorzystywane systemy teleinformatyczne są systemami złożonymi i działają w ramach funkcjonowania innych systemów teleinformatycznych, zarówno podrzędnych, równorzędnych jak i nadrzędnych. Wykorzystywane systemy powinny być ze sobą w pełni kompatybilne (mieć możliwość wymiany pomiędzy sobą informacji). Z tego względu można wyróżnić trzy podstawowe wymagania operacyjne, a mianowicie: terminowość, wierność, skrytość. Wynikają one przede wszystkim z zadań stawianych przed stworzonym systemem kierowania reagowaniem kryzysowym i decydują o ich skuteczności operacyjnej[5].

Terminowość, stanowi zdolność systemów teleinformatycznych do przekazywania informacji (danych) w określonym czasie. Jest ona określana jako prawdopodobieństwo przesyłania informacji w czasie, który nie przekracza dopuszczalnych wartości dla ustalonych priorytetów przesyłanych informacji przy uwzględnieniu obciążenia systemów teleinformatycznych. Z badań wynika, że systemy teleinformatyczne powinny zapewnić dostęp do niezbędnych usług i informacji w czasie rzeczywistym lub zbliżonym do rzeczywistego (bazy danych, GIS, VoIP, SMTP, POP3)[6].

Wierność to zdolność systemów teleinformatycznych do odtworzenia w urządzeniach (systemach) odbiorczych nadanych informacji z zadaną dokładnością, przy uwzględnieniu istniejących zakłóceń i zniekształceń. W nowoczesnych systemach cyfrowych miarą jakości sygnału jest prawdopodobieństwo wystąpienia elementarnej stopy błędu lub stopień zniekształcenia kodowego informacji. Wierność transmisji w systemach cyfrowych jest określana przez średnie prawdopodobieństwo wystąpienia błędów na poziomie stopy błędów. Istotnymi miarami wierności (jakości) w systemach cyfrowych jest bitowa stopa błędów BER (*ang. Bit Error Ratio*) oraz symbolowa stopa błędów Pe. Bitowa stopa błędów pozwala określić prawdopodobieństwo wystąpienia błędu w strumieniu przesyłanych informacji.

Skrytość to zdolność systemów teleinformatycznych do przeciwstawienia się potencjalnym możliwościom podsłuchu przesyłanych (transmitowanych) danych. Skrytość dotyczy

---

[5] Praca zbiorowa pod kierunkiem J. Janczaka, „*System Łączności Brygady*", wyd. cyt., s. 14.
[6] J. Michniak, „*Dowodzenie i łączność*", wyd. cyt., s.177.

ochrony przesyłanych informacji, ochrony określonych relacji wymiany informacji oraz faktu i miejsca przekazu informacji. W klasycznych działaniach wojsk lądowych skrytość przekazywania informacji określana jest zazwyczaj poprzez trzy wskaźniki: współczynnik utajnienia kanałów (łączy) w systemach (sieciach) teleinformatycznych, prawdopodobieństwo wykrycia obiektu systemu łączności, wartość oczekiwaną ilości wykrytych obiektów w systemie łączności[7].

W kierowaniu reagowaniem kryzysowym skrytość przekazu informacji może odegrać decydujące znaczenie dla możliwości przeprowadzenia odpowiednich operacji. Dla przykładu można wymienić fakt wycieku informacji o wysadzaniu wału przeciwpowodziowego w 1997 r. Ludność, która dowiedziała się o tym przedsięwzięciu z mediów skutecznie zablokowała zaplanowane działania, co w konsekwencji doprowadziło do zalania Wrocławia.

2.1.2. Wymagania techniczno-eksploatacyjne

Wymagania techniczno-eksploatacyjne stawiane przed systemami teleinformatycznymi są związane ze sprawnością i właściwym funkcjonowaniem stworzonego, na potrzeby kierowania reagowaniem kryzysowym, systemu. Wymagania techniczno-eksploatacyjne definiują istotne właściwości wykorzystywanych środków teleinformatycznych oraz zasady ich funkcjonowania. Z przeprowadzonych badań wynika, że do głównych wymagań techniczno-eksploatacyjnych należy zaliczyć: **gotowość (dostępność), przepustowość systemu, trwałość, mobilność, bezpieczeństwo.**

Gotowość (dostępność) jest to zdolność systemu teleinformatycznego do terminowego przejścia z jednego stanu do innego, niezbędnego do zapewnienia kierowania reagowaniem kryzysowym. Dostępność osiąga się poprzez stworzenie odpowiedniej struktury organizacyjno-funkcjonalnej systemu teleinformatycznego, w skład której wchodzą także właściwe procedury oraz wyposażenie techniczne pozwalające na realizację wyznaczonych zadań. Do podstawowych wskaźników określających gotowość (dostępność) należy zaliczyć czas przejścia systemu teleinformatycznego do stanu pełnej wydajności i prawdopodobieństwo terminowego wykonania zaplanowanych przedsięwzięć w określonym czasie. Do osiągnięcia gotowości systemu teleinformatycznego niezbędny jest wysoki poziom wyszkolenia personelu technicznego utrzymującego ten system.[8]

---

[7] Praca zbiorowa pod kierunkiem J. Janczaka, „*System Łączności Brygady*", wyd. cyt., s. 15.
[8] Praca zbiorowa pod kierunkiem J. Janczaka, „*System Łączności Brygady*", wyd. cyt., s. 16.

Przepustowość systemu dotyczy w głównej mierze sieci szkieletowych (MAN, WAN, Storczyk). Przepustowość sieci (systemu) określana jest przez potencjalne możliwości tych sieci w zakresie transmisji odpowiednich strumieni danych w jednostce czasu. Jest ona ustalana dla poszczególnych relacji wymiany informacji (pary węzłów, kanału łączności, linii telekomunikacyjnych). Ważne jest także zapewnienie niezbędnego pasma transmisji danych możliwie na najniższych szczeblach kierowania, co umożliwi pozyskiwanie informacji o zaistniałej sytuacji u samego źródła. Do podstawowych wskaźników określających przepustowość systemu teleinformatycznego można zaliczyć: maksymalną szybkość transmisji, ilość podstawowych kanałów w relacji łączności, wartość oczekiwaną ilości kanałów w relacji łączności[9].

Trwałość systemu teleinformatycznego to jego zdolność do pracy podczas oddziaływania różnorodnych czynników zewnętrznych związanych w głównej mierze z niekorzystnym oddziaływaniem warunków meteorologicznych, terenowych, zakłóceń elektromagnetycznych itp. Odporność na zakłócenia systemu teleinformatycznego definiuje się jako zdolność tego systemu do realizacji zamierzonych (zaplanowanych) zadań w warunkach oddziaływania wszystkich rodzajów zakłóceń. Niezawodność systemu teleinformatycznego to nic innego jak zdolność do wykonania postawionych zadań przy zachowaniu odpowiednich wartości parametrów eksploatacyjnych.

Do podstawowych wskaźników określających trwałość systemu teleinformatycznego należy m. in. zaliczyć: współczynnik sprawności, średni czas poprawnej pracy systemu teleinformatycznego, prawdopodobieństwo że czas przerwy w pracy systemu nie przekroczy dopuszczalnej wartości.[10]

Mobilność systemu teleinformatycznego determinowana jest poprzez rodzaj środków w nim wykorzystywanych i stanowi właściwość systemu, która przejawia się zdolnością do właściwego i terminowego tworzenia podsystemu wymiany informacji. Mobilność można określić wskaźnikami: prawdopodobieństwem terminowego wykonania zadania w zakresie zmiany struktury i funkcjonalności systemu teleinformatycznego, granicznym czasem wykonania zadań kierowania reagowaniem kryzysowym z określoną niezawodnością[11].

Bezpieczeństwo systemu teleinformatycznego rozumiane jest jako zdolność tego systemu do przeciwstawienia się wszystkim rodzajom zagrożeń, w tym: podsłuchem, modyfika-

---

[9] Tamże, wyd. cyt., s. 17.
[10] Praca zbiorowa pod kierunkiem J. Janczaka, „*System Łączności Brygady*", wyd. cyt., s. 17.
[11] J. Michniak, „*Dowodzenie i łączność*", wyd. cyt., s.179.

cją i odmową usługi[12]. Zapewnienie bezpieczeństwa systemu teleinformatycznego (podsystemu wymiany informacji) należy do zadań najtrudniejszych i najbardziej skomplikowanych.

Pod względem technicznym system teleinformatyczny stworzony na potrzeby kierowania reagowaniem kryzysowym stanowić będzie środowisko złożone i różnorodne. Z tego też względu w celu projektowania, optymalizacji, eksploatacji oraz zarządzania systemami teleinformatycznymi należy posłużyć się odpowiednimi modelami matematycznymi i analitycznymi, dedykowanym oprogramowaniem (np. Comnet III, Opnet, , NetView, HP OpenView, itp.), a także wytycznymi zawartymi w dokumentach normatywnych. Stworzony system teleinformatyczny (podsystem wymiany informacji) będzie systemem rozproszonym, charakteryzującym się odpowiednimi właściwościami takimi jak:

- współdzieleniem zasobów;
- otwartością;
- współbieżnością;
- skalowalnością;
- przeźroczystością;
- tolerowaniem uszkodzeń.

Współdzielenie zasobów wynika z potrzeb uczestników procesu kierowania reagowaniem kryzysowym do współdzielenia informacji o aktualnej sytuacji. Cecha ta pozwala na równoległą pracę zespołową z wykorzystaniem tych samych obiektów informacji oraz usług systemowych. Zasoby informacyjne w rozproszonym systemach teleinformatycznych powinny być umieszczone są w określonych węzłach systemu. Dostęp do nich powinien być realizowany jest poprzez zdalną komunikację. Aktualnie wyróżniane są dwa podstawowe modele współdzielenia informacji w rozproszonych systemach teleinformatycznych a mianowicie: model oparty na architekturze klient-serwer i model bazujący na obiektach np. w technologii CORBA (*ang. Common Object Request Broker Architecture*)[13].

Otwartość systemu teleinformatycznego charakteryzuje jego zdolność dodawania nowych usług systemu, bez konieczności zmiany lub zwielokrotniania usług już istniejących. Otwartość systemu zapewniana jest m. in. poprzez specyfikację i dokumentowanie protokołów i interfejsów komunikacyjnych, co umożliwia zapewnienie kompatybilność poszczególnych urządzeń i całych systemów[14].

---

[12] W. Stallings, „*Ochrona danych w sieci i intersieci w teorii i praktyce*", Wydawnictwa Naukowo - Techniczne, Warszawa 1997, s. 19-20.
[13] J. Liberty, „*C++ - Księga Eksperta*", Wydawnictwo Helion, Gliwice 1999, s. 685-711.
[14] G. Coulouris, J. Dollimore, T. Kindberg, „*Systemy rozproszone - podstawy i projektowanie*", Wydawnictwa Naukowo-Techniczne, Warszawa 1998, s. 39-42.

Współbieżność systemu mówi o możliwości komunikowania się, w systemach rozproszonych, dużej liczby komputerów wyposażonych w jeden lub więcej układów mikroprocesorowych. Wykorzystanie w systemach teleinformatycznych architektur nadmiarowych (redundancji) oraz wyposażenie komputerów w układy wieloprocesorowe pozwala na zwiększenie mocy obliczeniowych, skrócenie czasu realizacji zadań oraz zwiększenie niezawodność systemu.

Skalowalność systemu mówi o możliwości modyfikacji i rozbudowy struktury systemu teleinformatycznego w zakresie usług przez niego świadczonych. Jest to nic innego jak możliwość przyłączania i odłączania urządzeń świadczących konkretne usługi. Skalowalność związana jest bezpośrednio z utrzymaniem wysokiej wydajności i niezawodności pracy całego systemu teleinformatycznego.[15]

Przeźroczystość systemu to jego zdolność do ukrywania przed użytkownikami systemu jego struktury organizacyjno-funkcjonalnej. Pozwala to postrzegać system teleinformatyczny jako jedną spójną całość. Przeźroczystość systemu w trakcie kierowania reagowaniem kryzysowym umożliwia na bezpośredni i przejrzysty dostęp do aktualnej i wiarygodnej informacji. Można wyróżnić przeźroczystość dostępu, położenia, współbieżności, zwielokrotniania, awarii, wędrówki, wydajności i skalowania[16].

Tolerowanie uszkodzeń to zdolność systemu teleinformatycznego do realizacji postawionych zadań oraz nieprzerwanej pracy w różnorodnych warunkach wywierających niekorzystny wpływ na funkcjonowanie systemu jako całości. Tolerowanie uszkodzeń przez system teleinformatyczny można uzyskać poprzez:

- zastosowanie urządzeń wykonanych w odpowiedniej technologii (dedykowanej do postawionych wymagań);
- zastosowanie architektury redundantnej.

Tolerowanie uszkodzeń przez system teleinformatyczny związany jest także z funkcjonowaniem w samym systemie określonych mechanizmów takich jak[17]:

- autokonfiguracji;
- identyfikacji zaistniałych uszkodzeń;
- przywracania funkcjonalności systemu po awarii.

---

[15] G. Coulouris, J. Dollimore, T. Kindberg, „*Systemy rozproszone - podstawy i projektowanie*", wyd. cyt., s. 43-45.
[16] G. Coulouris, J. Dollimore, T. Kindberg, „*Systemy rozproszone - podstawy i projektowanie*", wyd. cyt., s. 47-48.
[17] A. Silberschatz, P.B. Galvin, „*Podstawy systemów operacyjnych*", Wydawnictwa Naukowo-Techniczne, Warszawa 2001, s. 707 – 762.

2.2. Wymagania związane z obiegiem informacji

Wymagania związane z obiegiem informacji wynikają bezpośrednio z organizacji podsystemu informacyjnego. Podsystemem informacyjnym wewnątrz dowolnej organizacji nazywany jest zintegrowany zespół ludzi, środków i metod zbierania, kodowania, dekodowania, przechowywania, przetwarzania, odnajdywania i komunikowania a także aktualizacji i użytkowania niezbędnych danych dla potrzeb kadry kierowniczej, w celu podjęcia prawidłowych decyzji.[18] System taki jest w pewnym stopniu odzwierciedlony poprzez strukturę organizacyjną, która wskazuje na główne drogi przepływu danych, uwidaczniając jednocześnie hierarchię potrzebnych informacji na poszczególnych szczeblach organizacyjnych, a także wzajemne relacje pomiędzy komórkami i generowanymi przez nie danymi. Jest to tradycyjne ujęcie problemu zarządzania informacją.

Z przeprowadzonych badań wynika, że przed systemem informacyjnym organizacji, w tym także organizacji jaką są wojska lądowe, są stawiane z góry ustalone wymagania[19]:

- dostarczanie kompleksowych i aktualnych informacji, zapewnianie selektywnego i skutecznego wykorzystania informacji oraz właściwej wymiany informacji pomiędzy komórkami organizacyjnymi, przełożonymi i podwładnymi w obydwu kierunkach,
- prostotę w użytkowaniu i zapewnieniu stałej, automatycznej metody pozyskiwania informacji z ustalonych źródeł,
- umożliwienie natychmiastowego pozyskania danych, nawet z najniższego szczebla zarządzania, wyszukiwanie i kojarzenie informacji z różnych źródeł, przedstawienie danych i wyników ich analiz w różnych układach sprawozdawczych,
- przepływu informacji opartego na sprzężeniach zwrotnych.

Należy zauważyć, że w miarę potrzeb i możliwości podsystem informacyjny ulega przemianom w celu zabezpieczenia prawidłowego przetwarzania, gromadzenia i przesyłania informacji. Na przemiany te ma wpływ zarówno:

- zarządzanie informacją, którego realizacja sprawia, że pojawiają się nowe potrzeby informacyjne a tym samym konieczność określenia nowych powiązań komunikacyjnych,
- nowe metody przetwarzania, gromadzonych i przesyłania informacji.

---

[18] S. Pietrzak, Informacyjny system zarządzania przedsiębiorstwem, Ekonomika i Organizacja Przedsiębiorstwa, nr 6/1998, s. 7

[19] por. S. Pietrzak, Informacyjny system zarządzania przedsiębiorstwem, Ekonomika i Organizacja Przedsiębiorstwa, nr 6/1998, s. 7-8

Wykorzystanie samej technologii nie zagwarantuje skutecznego zarządzania informacją. Jej zastosowanie daje efekty, tylko wtedy, gdy jest ona właściwie zastosowana.[20] W tym celu organizacja musi dysponować odpowiednio wyszkolonym personelem, zdolnym do wykorzystania nowych technologii informacyjnych (sieci teleinformatycznych, zautomatyzowanych systemów dowodzenia). Posiadanie takich umiejętności staje się obligatoryjne i jest warunkiem sprawnego zarządzania informacją. Z przeprowadzonych badań wynika że warunkiem rzeczywistego stosowania tych narzędzi jest przekonanie pracowników (decydentów i operatorów), że są one im niezbędne podczas realizacji procesu kierowania reagowaniem kryzysowym. Niezbędne jest jednoczesne wykorzystanie wiedzy i doświadczenia personelu (operatorów), nowoczesnych metod archiwizowania informacji i sprawnej komunikacji pomiędzy uczestnikami danego procesu z wykorzystaniem sieci teleinformatycznych.

W literaturze przedmiotu można spotkać pojęcie „zarządzania wiedzą" co oznacza kształtowanie odpowiednich czynników motywujących pracowników (operatorów) do tworzenia wiedzy i wykorzystania jej w wyznaczonym kierunku. Istotne znaczenie ma racjonalizacja zasobów wiedzy ze względu na potrzeby organizacji i możliwości twórcze operatorów. Inna definicja tego pojęcia mówi, że jest to świadoma strategia dostarczania właściwej wiedzy odpowiednim ludziom w odpowiednim czasie i pomaganie im dzielić się nią i wykorzystywać w działaniu, dla poprawy funkcjonowania organizacji.[21]

Analiza literatury wykazała również, że w toku zarządzania informacją mamy do czynienia z tzw. wiedzę cichą i formalną. Źródłem powstawania wiedzy cichej jest doświadczenie personelu (operatorów) - co czasami skutkuje (pomimo świadomości jej istnienia) brakiem możliwości jej sformułowania, a przez to przekazania innym osobom. Sposobem na jej wydobycie jest w głównej mierze obserwacja i naśladownictwo a także nieformalne przekazywanie spostrzeżeń. Wiedza formalna jest wyrażona za pomocą słów, znaków, czy symboli. Wiedzę taką definiuje się jako zbiór informacji świadomych, które człowiek aktualizuje w swojej pamięci i na których może koncentrować uwagę, a także potrafi je przekazać na zewnątrz.[22] Powstanie dodatkowej wiedzy ma miejsce w wyniku interakcji pomiędzy tymi dwoma jej rodzajami. Należy pamiętać, że przetwarzanie wiedzy (informacji) jest działalnością ludzką, a tym samym działalnością nieograniczoną, stale podlegającą rozwojowi i trudno

---

[20] E. Kolbusz, Informacja jako przedmiot zarządzania, Informatyka w zarządzaniu, Zeszyt IIwZ, Studia Informatica 13/1999, s. 15

[21] J. Brzóska, K. Palucha, Zarządzanie wiedzą jako czynnik sukcesu restrukturyzowanego przedsiębiorstwa, Źródła sukcesów i porażek przedsiębiorstw. Aspekt strategiczny, Zeszyty naukowe Akademii Ekonomicznej we Wrocławiu, 870/2000, s. 364

[22] B. Stefanowicz, Wybrane zagadnienia infologicznej analizy danych, Zeszyty Naukowe Szkoły Wyższej im. P. Włodkowica, 12/1999, s. 27

przewidywalną. Można powiedzieć, że zarządzanie wiedzą nigdy się nie kończy, ponieważ wiedza, tak jak informacje, poprzez ich wykorzystanie stale zwiększa swoją wartość.

Połączenie wszystkich wymienionych elementów, wchodzących w zakres zarządzania informacją sprawia, że organizacja zaczyna świadomie i aktywnie wykorzystywać posiadane przez siebie zasoby. Dopiero zrozumienie konieczności zarządzania organizacją w oparciu o te zasoby uświadamia decydentom, że działalnością kierowanej przez nią organizacji jest nie tylko osiągnięcie zamierzonego celu, ale także zarządzanie informacją.

Istotnym z punktu widzenia podsystemu informacyjnego jest także określenie elementów składowych, które są przydatne do sklasyfikowania informacji, a przez to do jej prawidłowego zarządzania. Według Zbigniewa Ścibiorka struktura każdej informacji składa się z czterech następujących elementów[23]:

- treści informacji;
- nośnika treści;
- symboli, za pomocą których jest utrwalona;
- sposobu przenoszenia informacji.

Powiązanie powyższych elementów tworzy informację, która determinuje warunki jej przetwarzania, dystrybucji i wykorzystania, a więc warunki jaki występują w procesie kierowania z wykorzystaniem sieci teleinformatycznych.

Treścią informacji jest wszystko to, co dany osobnik chce przekazać innym. Do treści możemy zaliczyć: wiedzę, opis, odczucia lub inne wrażenia odnoszące się do danego przedmiotu, zjawiska lub stanu określone przyjętymi w powszechnym użytku symbolami. W procesie dowodzenia treścią informacji będzie treść meldunku (rozkazu, zarządzenia) przesyłanego pomiędzy uczestnikami wymiany informacji.

Nośnik treści informacji jest elementem materialnym, na którym informacja została utrwalona. Może to być papier, taśma magnetofonowa, klisza filmowa, dyskietka, płyta, taśma perforowana, pamięć komputera, obrazy, tablice oraz wszystkie inne elementy, na których możemy zapisać treść informacji. Nośnik informacji dobierany jest najczęściej w odniesieniu do procedur oraz możliwości technicznych danej organizacji. Czy więc jest nośnik w środowisku sieci teleinformatycznych? Przeprowadzone badania wykazały, że nośnikiem informacji są odpowiednie bazy danych, zdolne do przechowywania treści informacji a taką odpowiednie kanały transmisyjne. Zawartość baz danych powinna być w każdej chwili do-

[23] Z. Ścibiorek, *Podejmowanie decyzji*, Warszawa 2003, s. 73.

stępna odpowiednim osobom funkcyjnym stanowiska dowodzenia, a kanały transmisyjne powinny umożliwiać jej przesyłanie.

Następny element składowy wiadomości - symbole treści informacji - są umownymi znakami za pomocą których została zapisana dana informacja. W odniesieniu do najpopularniejszego narzędzia komunikowania interpersonalnego jakim jest język symbolami są odpowiednio: litery, cyfry, rysunki, znaki, dźwięki, sygnały świetlne itp. Stosowanie poszczególnych rodzajów symboli ma sens podczas komunikowania się tylko wtedy, jeśli wszyscy uczestnicy procesu wymiany informacji posługują się tymi samymi symbolami. Wszędzie tam, gdzie użytkownik chce ukryć przed innymi treść informacji stosuje symbole stanowiące określony kod. Dobierając symbole do zapisu informacji należy stosować pamiętać o zasadzie takiego ich doboru, aby jak najwierniej oddać istotę treści danej informacji. Język jest w tej sytuacji uniwersalnym narzędziem, którego poszczególne elementy – wyrazy i zdania, mogą być dobierane w różny sposób. Symbole mogą być także dobierane odpowiednio do możliwości percepcji odbiorcy, jak również środków za pomocą, których przekazywana będzie informacja.

Środowisko systemów teleinformatycznych jest środowiskiem w którym wielką uwagą poświęca się interoperacyjności tych systemów z systemami innych państw w ramach NATO. W organizacji tej szybka i bezbłędna wymiana informacji ma znaczenie fundamentalne. W celu wyeliminowania pomyłek błędnej interpretacji tekstu stworzono własny język wymiany informacji opublikowany jako ADatP-3 (Allied Data Publication Nr 3) [24]. Informacja zapisana w tym języku jest *spójna, dokładna, zaktualizowana i czytelna*. W standardzie tym zakres pojęciowy opisany jest wyłącznie za pomocą słów (z uwzględnieniem skrótów i kodów), których znaczenie zostało w sposób jednoznaczny zdefiniowane przez wszystkich zainteresowanych (kraje członkowskie). Baza pojęciowa jest uaktualniana raz na dwa lata. W tak stworzonym sztucznym języku opracowano strukturę (format) umożliwiająca przekazanie jak najwięcej informacji przez samo położenie słów w ramach zdefiniowanych formatów. Struktura ta, znana pod pojęciem FORMETS (NATO MESSAGE TEXT FORMATTING SYSTEM), określa zasady, składnie i słownictwo dla FORMATÓW TEKSTU WIADOMOŚCI (MTF), które można stosować w środowiskach wymagających pracy „ręcznej" jak i wspomaganej komputerowo. Uogólniając, FORMETS jest proceduralnym standardem informacyjnym dla środowiska znakowego, który obejmuje sztuczny język opisujący sposób wymiany wiadomości znakowych, składnię oraz zasady reprezentacji danych w formie sfor-

[24] Koncepcja systemu opisana została w normie STANAG 5500

malizowanej. Odpowiedzialną za tworzenie i uaktualnianie standardu jest natowska organizacja NC3O (NATO Consultation, Command and Control).

Ostatnim elementem struktury informacji jest sposób przenoszenia informacji. Najczęściej jest on wynikiem wymienionych już aspektów technicznych lub przyjętych w organizacji rozwiązań. Przekaz informacji odbywać się może w bezpośrednich relacjach interpersonalnych lub za pomocą różnego rodzaju urządzeń lub organizacji specjalizujących się w przesyłaniu informacji. Współczesny, dynamiczny rozwój techniczny powoduje, iż oprócz tradycyjnego przekazu informacji za pomocą poczty, prasy, telewizji, radia i telefonów szerokie zastosowanie ma przekaz pocztą elektroniczną, prądem elektrycznym lub impulsem elektromagnetycznym.

Różnorodność nośników oraz sposobów ich przekazywania generuje podział informacji, którego istota odnosi się do kryterium formy przedstawienia, wyróżniamy więc informacje:

- ustne;
- pisemne;
- audiowizualne;
- graficzne;
- dźwiękowe;
- sygnałowe;
- inne.

Istotnym kryterium jest także znaczenie informacji w każdym procesie decyzyjnym. Według niego wyróżniamy informacje:

- kluczowe, decydujące o najważniejszych elementach procesu podejmowania decyzji oraz determinujące poszukiwania rozwiązań optymalnych;
- istotne (obiektywne i subiektywne), wpływające na podejmowane decyzje;
- nieistotne, nie stanowiące podstawy procesów decyzyjnych oraz mające znikomy wpływ na proces podejmowania decyzji;
- rutynowe, czyli takie które zawsze pojawiają się okresowo w poszczególnych etapach działalności organizacji.

Z punktu widzenia wpływu informacji na podejmowane decyzje, wyróżniamy informacje:

- dotyczące działalności organizacji nie objętej zakresem bieżącego planowania;
- inicjujące i ustalające zadania, nie wyłączając koordynacji zadań cząstkowych;

- dostarczające danych dla przyjętej w organizacji strategii postępowania, a więc odpowiadające na pytanie: *jaki kierunek działania jest lepszy*;
- inspirujące proces podejmowania decyzji i odpowiadające na pytanie: *jakie problemy powinno się rozpatrzyć*;
- zasilające, uzupełniające poszczególne etapy procesu decyzyjnego;
- koordynacyjne, regulujące działania i procesy zachodzące pomiędzy poszczególnymi elementami organizacji;
- podające do wiadomości wyniki działania (kontrolne).

W specyficznym środowisku jaki jest proces kierowania (dowodzenia) realizowany w wojskach lądowych informację można podzielić także ze względu na pilność i ważność przekazu. Dzieli się ją na[25]:

- błyskawiczną (ang. flash – kod Z);
- natychmiastową (ang. immediate – kod O);
- priorytetową (ang. priority – kod P)
- rutynową (ang. routine – kod R).

Informacja z kategorią „*błyskawiczna*" przeznaczona jest dla początkowego kontaktu z przeciwnikiem lub dla komunikatów bojowych o najwyższym stopniu pilności. Z tego też względu forma informacji powinna być jak najkrótsza, co umożliwi jej szybką transmisję poprzez sieci teleinformatyczne. Zazwyczaj jest ona przekazywana w formie (postaci) z góry ustalonych kodów (sygnałów).

Kategoria „*natychmiastowa*" zarezerwowana jest dla bardzo ważnych wiadomości odnoszących się do sytuacji, które mają istotne znaczenie dla bezpieczeństwa wojsk własnych. Informacja ta, podobnie jak błyskawiczna, także jest przekazywana w postaci ustalonych wcześniej sygnałów.

Informacja z kategorią „*priorytetowa*" przekazuje wiadomości dotyczące prowadzenia toczących się operacji oraz dla innych ważnych i pilnych spraw dla których klauzula „rutynowa" jest niewystarczająca.

Ostatnia – najniższa kategoria ważności informacji – „*rutynowa*" jest wykorzystywana dla wszystkich rodzajów wiadomości, których treść nie jest wystarczająco pilna ani ważna.

Każda informacja zwiększa wiedzę odbiorcy o otaczającym świecie. Niesie ona ze sobą pewną wartość poznawczą. Wartość, która jest pojęciem samym w sobie i może ewentualnie stanowić treść rozważań filozoficznych. Niemniej jednak, z punktu widzenia każdej

---

[25] Zasady organizacji łączności współdziałania w operacjach wielonarodowych, SG WP, Warszawa 1999, s. 195

organizacji „konkretną wartość", jaką niesie informacja należy zamienić na pojęcie „użyteczności informacji". Inaczej mówiąc, w informacji ważne jest to w jakim stopniu jest ona przydatna i użyteczna dla adresata.

Według Roberta H.Gregory i Richarda L. Van Horn *wartość informacji zależy od czterech głównych czynników, a mianowicie: jej jakości, aktualności, ilości oraz powiązania z zadaniami możliwymi do podjęcia przez kierownictwo (dowództwo).*

Oceniając pierwszy z czynników - **jakość informacji** – należy porównać informację z rzeczywistością. Im informacja jest dokładniejsza (precyzyjniejsza), tym wyższa jest jej jakość i tym pewniej decydenci (sztaby i dowódcy) mogą na niej polegać przy podejmowaniu decyzji. Z punktu widzenia ekonomii, koszt pozyskania informacji rośnie wraz z jej jakością. Dla przykładu podwójne i potrójne sprawdzanie świeżo uzyskanej informacji z innymi danymi pozwala na weryfikację jej wiarygodność, lecz dodatkowy czas na to potrzebny i wykorzystane siły i środki podwyższają koszty. Potrzebny stopień dokładności będzie różny w zależności od sytuacji. W procesie dowodzenia głównym wyznacznikiem kosztu będzie czas potrzebny na zweryfikowanie informacji.

Informacja jest swoistego rodzaju „towarem", który ma swój koszt oraz odpowiednią wartość. W wyniku poniesionych kosztów otrzymujemy informację, która ma dla jej adresata pewną przydatność. Teoretycznie przydatność informacji powinna być większa niż nakład użyty dla jej uzyskania. Z tego też względu należy bardzo szczegółowo ustalić które informacje są newralgiczne w procesie dowodzenia i których koszt może być wysoki.

Wraz ze wzrostem ilości informacji rośnie koszt ich uzyskania. Jednocześnie należy być świadomym luki informacyjnej, która powoduje podejmowanie decyzji nieoptymalnych, w warunkach ryzyka, co również związane jest z kosztem. W przypadku procesu dowodzenia kosztem tym będzie niemożność osiągnięcia zamierzonego celu działania i w konsekwencji duże straty.

Wraz ze wzrostem informacji luka informacyjna będzie się zmniejszać, a koszt decyzji nieoptymalnych maleć. Z tego też względu zasadnym jest szacowanie kosztu decyzji nieoptymalnej i kosztu pozyskania odpowiednich informacji, Jest to w praktyce niezmiernie trudne ponieważ w praktyce nie ma właściwego miernika. Nie ma również miernika kosztu informacji jako funkcji jej ilości.

Następnym czynnikiem informacji, który bardzo silnie oddziaływuje na jej wartość jest **aktualność informacji.** Wszelkie działania korygujące należy podejmować, zanim wystąpi znaczne odchylenie od zamierzonego planu. Informacja zatem musi być dostarczana przez system informacyjny w czasie umożliwiającym podjęcie skutecznego działania. W tym

miejscu należy zwrócić uwagę na aspekt ochrony posiadanej informacji. Informacja musi być w odpowiedni sposób zabezpieczona zarówno przez jej utajnienie jak i właściwą dystrybucję.

Ilość informacji jest czynnikiem pozwalającym decydentowi (dowódcy) podjąć sprawną decyzję. W praktyce dowódca jest często zasypywany nieistotnymi i bezużytecznymi informacjami. Z olbrzymiej ilości otrzymywanych informacji pierwotnych muszą zostać wybrane informacje użyteczne w danym czasie i danej sytuacji. Z tego też względu w odniesieniu do każdego stanowiska dowodzenia nieodzowne jest stosowanie zasady selekcji informacji, określonej również mianem „zasada 20-80". Okazuje się, że tylko 20% informacji docierających do dowództwa (kierownictwa) dotyczy spraw kluczowych i w 80% przesądza o wynikach działalności. Określenie puli informacji o newralgicznym znaczeniu stanowi zasadę redukcji w odniesieniu do pracy z informacjami. Redukcja informacji polega na odpowiednim określeniu wagi gatunkowej każdej informacji dla danego rodzaju podejmowanej decyzji oraz na rezygnowaniu z informacji mało istotnych. Redukcja polega nie tylko na odrzuceniu nieprzydatnych informacji pierwotnych, lecz także na ich scalaniu, łączeniu, uogólnianiu cząstkowych informacji użytecznych.

Im większe zasoby informacji pierwotnych, tym trudniejszy jest wybór informacji przydatnych (newralgicznych).

Ostatni czynnik - **związek informacji z zadaniami** - wynika z celowości podejmowanego działania, opartego na właściwym rodzaju i typie informacji odznaczającej się wysoką użytecznością. Informacje otrzymywane przez decydentów (dowódców) powinny być powiązane z ich obowiązkami i zadaniami.

Dostarczany decydentowi zbiór informacji podstawowych musi być uporządkowany według ściśle określonych kryteriów warunkujących jej przydatność. Dostarczenie decydentowi (dowódcy) szczegółowych i rzetelnych, lecz bardzo licznych i oderwanych od siebie informacji, nie pozwala na pełne ich wykorzystanie, a wręcz może uniemożliwić wykorzystanie informacji newralgicznych. Informacje muszą być tak uporządkowane, aby w pełni opisywały konkretną sytuację, ponieważ tylko na tej podstawie decydenci mogą ustalić, co należy w zaistniałej sytuacji zrobić i jakie decyzje podejmować, aby osiągnąć zamierzone cele.

Informacje gromadzone w organizacji powinny być odpowiedniej jakości, tzn. obiektywne, istotne dla sprawy, dostępne w odpowiednim czasie, porównywalne, pełne, zwięzłe i cenne. Cenność informacji nie jest związana z ich liczbą ani też z pojemnością informacyjną wiadomości, lecz z jej znaczeniem dla sytuacji decyzyjnej i wagą podejmowanych dzięki nim decyzji. Cenność zależy w głównej mierze od posiadanego przez daną organizację potencjału

informacyjnego. O cenności informacji decyduje także układ odniesienia, którym jest zawsze określona sytuacja decyzyjna, a także koszt jej uzyskania we właściwym czasie.

Należy także pamiętać o tym, że informacje ulegają szybko starzeniu. Im starsza informacja tym prawdopodobnie mniejsza jej wartość (przydatność) dla organizacji. Trzeba zawsze brać pod uwagę to, że w praktyce podejmowania decyzji nie uzyskuje się najczęściej pełnej i wyczerpującej, tj. kompletnej informacji. Zawsze istnieć będzie luka informacyjna, stanowiąca różnicę między informacją pełną a dostępną.

W organizacji jaką są wojska lądowe proces decyzyjny rozłożony jest na wiele faz i etapów, realizowanych na różnych szczeblach dowodzenia. Skuteczność tego procesu, trafność podejmowanych decyzji, będzie zależała m.in. od jakości zarządzania posiadaną informacją. Przeprowadzone badania pozwalają na stwierdzenie, że zespoły realizujące proces zarządzania informacjami, a tym samym systemy teleinformatyczne przez nie wykorzystywane, powinny zapewnić:

- dostępność informacji;
- wiarygodność informacji;
- bezpieczeństwo informacji;
- spójność informacji;
- trwałość informacji;
- aktualność informacji.

Dostępność informacji wyraża się możliwością pozyskania odpowiedniej, będącej w posiadaniu informacji przez wszystkie organa biorące udział w procesie kierowania reagowaniem kryzysowym w celu prawidłowej realizacji cyklu decyzyjnego. Informacja ta powinna być dostarczana tylko tym organom, które są nią zainteresowane ze względu na swoje miejsce w procesie decyzyjnym.

Wiarygodność informacji powinna być zapewniona poprzez jej odpowiednią weryfikację, zarówno przez odpowiednie organa uczestniczące w procesie kierowania jak również przez zespół zajmujący się zarządzaniem informacją.

Bezpieczeństwo informacji polega w głównej mierze na jej odpowiednim zabezpieczeniu różnego rodzaju systemami utajniającymi, ale także poprzez odpowiedni system obiegu informacji. Konkretna informacja powinna trafiać tylko i wyłącznie do organów które są nią zainteresowane.

Niezmiernie istotnym wyznacznikiem jest spójność informacji. Jej zapewnienie polega na jednolitej świadomości informacyjnej wszystkich organów kierowania, co wyraża się po-

trzebą dostarczania tej samej informacji do wszystkich zainteresowanych. Należy unikać sytuacji, w której jeden z organów procesu kierowania posiada najnowsze informacje na konkretny temat, natomiast inne organy bazują na informacji przestarzałej.

Trwałość informacji wyraża się potrzebą jej zachowania w niezmienionej postaci przez dłuższy okres czasu. Jest to uwarunkowane nie tylko potrzebami procesu decyzyjnego ale także odpowiednimi przepisami prawnymi. Z tego względu struktura organizacyjna zespołu zarządzającego informacjami powinna uwzględniać potrzebą przechowywania posiadanej informacji w kilku miejscach, co powinno uchronić ją przed całkowitym zniszczeniem (utratą).

Aktualność informacji polega na stałym uaktualnianiu posiadanej bazy danych z informacjami i dostarczaniu odpowiednim organom dowodzenia tylko i wyłącznie najświeższej informacji. Jak zostało to przedstawione wcześniej wartość informacji zależy m.in. od jej aktualności, a tym samym odpowiednia reakcja na zaistniałe zjawiska może być możliwa tylko przy posiadaniu najnowszych (aktualnych) informacji.

WNIOSKI

Przeprowadzone badania pozwalają na stwierdzenie, że jednym z ważniejszych czynników oddziaływujących na funkcjonowanie i możliwości systemów teleinformatycznych wykorzystywanych w działaniach reagowania kryzysowego jest rejon (obszar) działań. Do czynników związanych z rejonem (obszarem), mających wpływ na systemy teleinformatyczne należy zaliczyć:

- wielkość rejonu (obszaru);
- charakter rejonu (gęstość zabudowy);
- istniejąca infrastruktura techniczna rejonu (w tym infrastruktura teleinformatyczna).

Istotnymi czynnikami mającymi wpływ na podsystem wymiany informacji, a tym samym na systemy teleinformatyczne, są także warunki klimatyczne, meteorologiczne i propagacyjne. Do ważnych czynników z tego zakresu należy zaliczyć odpowiednio:

- długość dnia i nocy;
- prognozę pogody oraz jej wpływ na istniejącą infrastrukturę (temperatura, opady atmosferyczne, wilgotność powietrza);

85

- stan atmosfery, troposfery (zjawisko rozproszenia w troposferze fal UKF)[26] i jonosfery (propagacja odbicia od warstw jonosfery)[27].

***

Wymagania stawiane przed systemami teleinformatycznymi można podzielić na dwie podstawowe grupy: **wymagania operacyjne** i **wymagania techniczno-eksploatacyjne**.

Do podstawowych wymagań operacyjnych należy zaliczyć: **terminowość, wierność, skrytość**. Główne wymagania techniczno-eksploatacyjne to: **gotowość (dostępność), przepustowość systemu, trwałość, mobilność, bezpieczeństwo.**

Systemem informacyjny wykorzystywany w kierowaniu reagowaniem kryzysowym musi spełnić także następujące wymagania[28]:

- dostarczanie kompleksowych i aktualnych informacji, zapewnianie selektywnego i skutecznego wykorzystania informacji oraz właściwej wymiany informacji pomiędzy komórkami organizacyjnymi, przełożonymi i podwładnymi w obydwu kierunkach,
- prostotę w użytkowaniu i zapewnieniu stałej, automatycznej metody pozyskiwania informacji z ustalonych źródeł,
- umożliwienie natychmiastowego pozyskania danych, nawet z najniższego szczebla zarządzania, wyszukiwanie i kojarzenie informacji z różnych źródeł, przedstawienie danych i wyników ich analiz w różnych układach sprawozdawczych,
- przepływu informacji opartego na sprzężeniach zwrotnych.

W stosunku do informacji, wykorzystywane w kierowaniu reagowaniem kryzysowym systemy teleinformatyczne powinny zapewnić:

- dostępność informacji;
- wiarygodność informacji;
- bezpieczeństwo informacji;
- spójność informacji;
- trwałość informacji;
- aktualność informacji.

---

[26] Tamże, wyd. cyt., s. 148-153.
[27] P. Daniluk, „*Radiowa służba stała i ruchoma*", wyd. cyt., s. 148-153.
[28] por. S. Pietrzak, Informacyjny system zarządzania przedsiębiorstwem, Ekonomika i Organizacja Przedsiębiorstwa, nr 6/1998, s. 7-8.

3. SYSTEMY TELEINFORMATYCZNE WOJSK LĄDOWYCH

Rozwój technologii informatycznych stał się ważnym czynnikiem decydującym o efektywności dowodzenia, a tym samym uzyskania przewagi w tym obszarze nad potencjalnym przeciwnikiem, jedynie metodami usprawniania podsystemu informacyjnego (zdobywanie, przechowywanie, przetwarzanie, obieg informacji, itp.). Usprawnianie cyklu decyzyjnego w procesie dowodzenia poprzez automatyzację wykonywania określonych czynności przez poszczególne komórki funkcjonalne stanowisk dowodzenia, na różnych poziomach dowodzenia, datuje się od początku lat sześćdziesiątych dwudziestego wieku. Wraz z rozwojem technik informatycznych i telekomunikacyjnych, coraz większymi możliwościami komputerów i sieci teleinformatycznych, możliwości automatyzacji procesu dowodzenia na tyle wzrosły, że zaczęto mówić o zautomatyzowanych systemach dowodzenia (ZSyD).

3.1. Istota i przeznaczenie zautomatyzowanych systemów wspomagania dowodzenia

Współczesne zautomatyzowane systemy dowodzenia określane są, w literaturze przedmiotu, jako systemy klasy **C^3I** (lub **C^4I**). W nomenklaturze NATO klasyfikuje się je następująco:

- **C2** – (*ang. Command & Control*)– klasyczne systemy dowodzenia, bez zastosowania środków automatyzacji;
- **C3I** – (*ang. Command, Control, Communications & Intelligence*) – systemy dowodzenia zintegrowane z systemami łączności i rozpoznania;
- **C4I** – (*ang. Command, Control, Communications, Computers & Intelligence*) - systemy dowodzenia zintegrowane z systemami łączności i rozpoznania wspomagane technologiami informatycznymi;
- **C4IEW** – (*ang. Command, Control, Communications, Computers, Intelligence & Electronic War*) - system *C4I,* w którym uwzględnia się wspomaganie obszaru walki elektronicznej.

Analiza literatury wykazała, że systemy klasy **C4I** umożliwiają:

- ciągłe monitorowanie bieżącej sytuacji na obszarze działań i jej jednoznaczną identyfikację przy jednoczesnym powiązaniu z oceną zagrożeń dla potrzeb cyklu decyzyjnego w procesie dowodzenia wojskami oraz sterowania środkami rażenia;
- sprawne przetwarzanie i obieg informacji, a tym samym szybszy proces planowania, co umożliwia podjęcie działań wyprzedzających w stosunku do potencjalnego przeciwnika;
- zapewnienie własnemu systemowi dowodzenia odporności na rozpoznanie, obezwładnianie środkami WE i destrukcyjne oddziaływanie przeciwnika, a tym samym zwiększenie żywotności wojsk.

W wojskach lądowych, na dzień dzisiejszy, wykorzystywane są dwa zautomatyzowane systemy dowodzenia, a mianowicie:

- zautomatyzowany system dowodzenia „Kolorado";
- zautomatyzowany system dowodzenia szczebla taktycznego „Szafran ZT".

Wymienione systemy często posiadają podsystemy obsługujące tylko określone poziomy dowodzenia. Istnieje także wiele systemów specjalistycznych, skonstruowanych dla potrzeb rodzajów wojsk. Do najważniejszy z nich należą:

- zautomatyzowany system kierowania ogniem artylerii „Topaz";
- zautomatyzowany system kierowania obroną przeciwlotniczą „Łowcza".

Przy tworzeniu zautomatyzowanych systemów dowodzenia preferowane jest modułowe podejście, przy jednoczesnej ewolucyjnej modernizacji i rozbudowie już istniejących systemów. Takie podejście do budowy systemów wynika w dużej mierze z dynamicznego rozwoju technologii informatycznych i konieczności nadążania za zmianami, przy minimalizowaniu wysokich kosztów i wymaganych nakładów pracy na ich budowę. W literaturze przedmiotu podejście te nazywane jest COTS (*ang. Commercial of the Shelfs*).

Z uwagi na potrzebę współdziałania poszczególnych systemów na wielu płaszczyznach, systemy te posiadają w coraz większym stopniu elementy zgodne z określonymi normami i standardami. Powszechną metodą jest organizowanie zewnętrznych interfejsów komunikacyjnych systemów dla innych systemów w celu zachowania interoperacyjności i kompatybilności. Takie podejście spowodowane było złymi doświadczeniami we współdziałaniu nie tylko systemów różnych państw, ale także systemów różnych szczebli i pionów dowodzenia jednego państwa. W krajach NATO stworzono specjalny program służący zachowaniu interoperacyjności pomiędzy zautomatyzowanymi systemami dowodzenia zainteresowanych państw. Biorąc pod uwagę specyfiką zautomatyzowanych systemów kierowania środkami

walki i ich ograniczoną przydatność w operacjach reagowania kryzysowego, zespół autorski uznał za bezzasadne dokonywanie ich oceny pod względem przydatności w kierowaniu reagowaniem kryzysowym.

3.1.1. System Kolorado

Kolorado[1] jest stacjonarnym systemem dowodzenia przeznaczonym na szczebel strategiczny i operacyjny na stanowiska dowodzenia naczelnego dowódcy, dowódcy wojsk lądowych i dowódców korpusów. Został on oparty na stacjonarnej infrastrukturze teleinformatycznej czasu „P" zbudowanej w oparciu o sprzęt i oprogramowanie komercyjne. W projekcie tym nie przewidziano tworzenia wozów dowodzenia i innych urządzeń technicznych (specjalistycznych).

W skład systemu wchodzą następujące podsystemy specjalistyczne:

- operacyjno-dowódczy;
- rozpoznania i WE;
- zabezpieczenia logistycznego;
- wojsk rakietowych i artylerii;
- wojsk obrony przeciwchemicznej;
- wojsk inżynieryjnych;
- wojsk obrony przeciwlotniczej;
- wojsk łączności i informatyki;
- organizacyjno-mobilizacyjny.

Interoperacyjność z innymi systemami wspomagania dowodzenia zapewniać będzie wykorzystanie następujących standardów:

- ATCCIS[2]– model danych;
- ADatP-3 – wymiana wiadomości;
- APP-6A[3] – zobrazowanie na mapie;
- VPF, CADRG – mapy numeryczne;
- DTED – model terenu.

---

[1] P.Dela, Wsparcie informatyczne procesu dowodzenia, Warszawa, AON 2004, s. 47
[2] *ang. Army Tactical Command and Control Information System*
[3] *ang. Allied Procedural Publication*

87

3.1.2. System Szafran[4]

Polowy zautomatyzowany system dowodzenia (PZSD) Szafran jest rozproszonym systemem informatycznym przeznaczonym do wspomagania czynności dowodzenia we wszystkich fazach cyklu decyzyjnego procesu dowodzenia. Do jego podstawowych zadań należy zaliczyć:

- utrzymywanie baz danych zawierających aktualne i spójne dane dotyczące:
  - sytuacji taktycznej,
  - wojsk własnych i sąsiadów,
  - przeciwnika,
  - warunków prowadzenia działań (teren, pogoda, itp.);
- sporządzanie dokumentów dowodzenia (meldunków, rozkazów, zarządzeń, sprawozdań, planów) z uwzględnieniem warunków pracy grupowej;
- wymianę dokumentów dowodzenia między stanowiskami dowodzenia przy ich jednoczesnej archiwizacji, w tym wymianę dokumentów sformalizowanych zapewniających przesyłanie informacji i współdziałanie z innymi systemami, w tym z systemami innych armii krajów NATO (standard ADatP-3)[5];
- zobrazowanie, na podkładzie mapy cyfrowej, na podstawie spójnej informacji utrzymywanej w bazie danych, sytuacji operacyjno-taktycznej, dostosowanej do danego szczebla dowodzenia;
- synchronizację zawartości baz danych między innymi poprzez wykorzystanie wymiany dokumentów sformalizowanych i mechanizmu wymiany zgodnego z wymaganiami w NATO;
- realizację ustalonych zadań typu „kalkulacji sztabowych" i udostępnianie ich wyników osobom funkcyjnym na stanowisku dowodzenia;
- integrację zautomatyzowanych systemów dowodzenia i sterowania (kierowania) środkami walki rodzajów wojsk i służb;
- współdziałanie z zautomatyzowanymi systemami dowodzenia pozostałych rodzajów sił zbrojnych.

Polowy zautomatyzowany system dowodzenia (PZSD) dostarcza poszczególnym osobom funkcyjnym komórek organizacyjnych stanowisk dowodzenia usługi wspomagające realizację czynności w cyklu decyzyjnym procesu dowodzenia. Usługi te są udostępniane na

---

[4] Na podstawie P. Dela, Wsparcie informatyczne procesu dowodzenia, Warszawa, AON 2004, s. 60
[5] Stanag 5500.

zautomatyzowanych stanowiskach pracy (ZSP). Stanowiska te są wyposażone w informatyczne środki dowodzenia z odpowiednim oprogramowaniem użytkowym wspomagającym wykonywanie zadań określonej osoby funkcyjnej lub komórki organizacyjnej dowództwa na stanowiskach dowodzenia. Są one zlokalizowane odpowiednio: w zautomatyzowanych wozach dowódczo-sztabowych (ZWDSz), zautomatyzowanych wozach sztabowych (ZWSz) lub pomieszczeniach wykorzystywanych do pracy obsady operacyjnej stanowisk dowodzenia.

Zautomatyzowane stanowiska pracy w zautomatyzowanych wozach dowódczo-sztabowych umożliwiają pracę zarówno na postoju jak i w ruchu. Natomiast w zautomatyzowanych wozach sztabowych zapewnią pracę tylko na postoju.

W skład polowego zautomatyzowanego systemu dowodzenia wchodzi oprogramowanie systemowe, specjalistyczne i środki techniczne.

W polowym zautomatyzowanym systemie dowodzenia (PZSD) wykorzystywane są następujące środki techniczne:

- zautomatyzowane wozy dowódczo-sztabowe - ZWDSz-10,
- zautomatyzowane wozy sztabowe – ZWSz (ZWSZ-10S, ZWSz-20),
- terminale pokładowe montowane w wozach bojowych i pojazdach,
- urządzeń typu LANBOX .

Zautomatyzowany wóz dowódczo-sztabowy - ZWDSz-10 zostanie zbudowany na bazie kołowego transportera opancerzonego. W chwili obecnej nie została wybrana platforma dla tego wozu. Zapewni on dowodzenie w trybie zautomatyzowanym i klasycznym, na postoju oraz w ruchu. Będzie stanowił główny element stanowisk dowodzenia batalionów, a na szczeblach pułków, brygad i dywizji będzie wozem dowodzenia (WD) dowódców i ich zastępców, wykorzystywanych między innymi do wyjazdu na rekonesans lub na WSD lub PDO.

Wyposażenie ZWDSz-10 będzie składało się z dwóch zautomatyzowanych stanowisk pracy, serwera bazy danych oraz komputera komunikacyjnego, przeznaczonego dla zapewnienia potrzeb wymiany danych poprzez radiostacje. Oprócz wyposażenia informatycznego, wyposażenie ZWDSz-10 będzie zawierało cyfrową łącznicę obiektową (CŁO) i trzy radiostacje. Na burtę ZWDSz-10 zostaną wyprowadzone poprzez konwertery światłowodowe trakty CŁO oraz wyjścia z urządzenia komunikacyjnego. Będą one wykorzystywane do łączenia się z innymi ZWDSz-10, wozami sztabowymi (ZWSz), terminalami TPP-10W, urządzeniami typu LAN-BOX (lub stacjami roboczymi rozwijanymi w namiotach lub obiektach stacjonarnych).

Zautomatyzowane wozy sztabowe - ZWSz są budowane na bazie nadwozi kontenerowych stosowanych obecnie w podsystemie cyfrowej łączności (STORCZYK - 2000).

Zautomatyzowany wóz sztabowy (rys.3.1) składa się z następujących elementów:

- samochodu ciężarowo-terenowego STAR 944-DK;
- nadwozia kontenerowego typ „890";
- przyczepy jednoosiowej typu D-622 z dwoma agregatami prądotwórczymi ZP6-1/230-20.

Wyposażenie kontenera ZWSz może być dostosowane do jego przeznaczenia. Część wyposażenia jest jednak stała, niezależna od wersji wykonania. Do tych elementów należą m.in. urządzenia zasilania, i urządzenia podtrzymywania mikroklimatu (klimatyzacja). Urządzenia informatyczne zamontowane w ZWSz są połączone ze sobą w lokalnej sieci komputerowej wozu. Na burcie nadwozia kontenerowego wyprowadzone są złącza sieci komputerowej wozu służące do zapewnienia połączeń z innymi elementami sieci lokalnej stanowiska dowodzenia. Tymi elementami mogą być między innymi inne ZWSz, urządzenia typu LAN-BOX, przenośne komputery- notebooki (także w wykonaniu komercyjnym)[6].

Rys 3.1. Zautomatyzowany wóz sztabowy (ZWSz)
Źródło: J. Michniak, Polowy zautomatyzowany system dowodzenia (PZSD), Warszawa, AON 2004

Dla zapewnienia komunikacji pomiędzy stanowiskami dowodzenia wykorzystywane są kanały łączności wydzielone z systemu telekomunikacyjnego. W celu dowiązania się do systemu łączności można wykorzystywać węzeł WP-40, router komercyjny lub cyfrową łącznicę obiektową (CŁO), w składzie której znajduje się router. W celu zwiększenia niezawodności działania możliwe jest wykorzystanie obu tych urządzeń.

[6] Współpracę ZWSz z urządzeniami komercyjnymi testowano w trakcie ćwiczenia „Akademicki Pierścień 2004"

W zautomatyzowanym wozie sztabowym (ZWSz) istnieje również możliwość zamontowania dodatkowych środków łączności takich jak: radiostacje wąsko lub szerokopasmowe, radiolinie dowiązania lub urządzenia do rozwijania bezprzewodowej sieci lokalnej.

W nadwoziu kontenerowym ZWSz istnieje możliwość zamontowania między innymi 2-3 zautomatyzowanych stanowisk pracy, drukarki, serwera bazy danych, serwera komunikacyjnego i/lub adaptera komunikacyjnego. Zostało to osiągnięte poprzez zastosowanie sprzętu o zunifikowanych wymiarach. Zastosowanie urządzeń grzewczych i klimatyzacyjnych umożliwiło zastosowanie w nich komercyjnego sprzętu informatycznego w wykonaniu profesjonalnym. Jest to w większości sprzęt o podwyższonych parametrach środowiskowych przeznaczony głównie do zastosowań telekomunikacyjnych.

Aktualnie wdrażane są wykonania dwóch wersji zautomatyzowanego wozu sztabowego tj.: **ZWSz-10S** i **ZWSz-20**.

Zautomatyzowany wóz sztabowy ZWSz-10S przeznaczony jest jako centralny element stanowiska dowodzenia na szczeblu dywizji i brygady. Jest przewidywany dla centrum wsparcia dowodzenia, które przy wykorzystaniu sprzętu i zainstalowanego oprogramowania będzie planowało, organizowało i kontrolowało funkcjonowanie zautomatyzowanego systemu dowodzenia na stanowisku dowodzenia. W ZWSz-10S znajdą się: serwer bazy danych, serwer komunikacyjny, trzy zautomatyzowane stanowiska pracy, adapter komunikacyjny, drukarka i urządzenia sieciowe, tworzące lokalną sieć komputerową wozu. Wyposażenie ZWSz-10S zapewnia wymianę dokumentów i elementów danych poprzez mobilną cyfrową sieć telekomunikacyjną. Zautomatyzowane stanowiska pracy w ZWSz-10S są przeznaczone dla osób funkcyjnych zespołu łączności i informatyki, a w szczególności dla: oficera – specjalisty bezpieczeństwa, administratora systemu i operatora.

Zautomatyzowany wóz sztabowy ZWSz-20 jest przeznaczony dla zespołu Informacyjnego Centrum Wsparcia Dowodzenia lub/i Zespołu Planowania Centrum Dowodzenia, gdzie wykorzystywany będzie do wprowadzania, redagowania, kreślenia i drukowania dokumentów bojowych oraz ich archiwizacji. Wóz ten będzie odpowiadał za wymianę dokumentów z elementami ugrupowania operacyjnego (bojowego) nie wyposażonymi w zautomatyzowane systemy dowodzenia. ZWSz-20 będzie również wykorzystywany do przygotowywania dokumentów papierowych podczas pracy w trybie klasycznym.

Wyposażenie ZWSz-20 w wersji pilotowej składa się z serwera bazy danych, serwera komunikacyjnego, dwóch zautomatyzowanych stanowisk pracy, drukarki i urządzeń sieciowych tworzących lokalną sieć komputerową wozu. Ponadto na wyposażeniu wozu może znajdować się skaner, ploter i fax. Zautomatyzowane stanowiska pracy przeznaczone są do

wprowadzania dokumentów papierowych do systemu informatycznego (poprzez skanowanie) a także do edycji i wydruku dokumentów wychodzących. Zautomatyzowany wóz sztabowy ZWSz-20 będzie dołączany do aparatowni ruchomego węzła łączności (RWŁC 10/K poprzez WP-40) lub ZWSz-10S łączem światłowodowym.

Rys. 3.2. Widok wnętrza ZWSz-10S
Źródło: http://www.altair.com.pl/files/r0704s.htm

Oprogramowanie PZSD składa się trzech zasadniczych poziomów:

· oprogramowania systemowego,

· oprogramowania usługowego i narzędziowego,

· oprogramowania użytkowego.

Oprogramowanie systemowe stanowią systemy operacyjne (SOLARIS, LINUX i Windows 2000) stosowane zarówno na serwerach jak i w stacjach roboczych.

Oprogramowanie usługowe zawiera komercyjne pakiety oprogramowania zapewniające między innymi funkcjonowanie baz danych, poczty elektronicznej, pracy grupowej i zarządzanie siecią komputerową.

Oprogramowanie narzędziowe stanowią biblioteki procedur oprogramowania systemowego i narzędziowego wykorzystywane przez oprogramowanie użytkowe.

Oprogramowanie użytkowe odpowiada za realizację funkcji specyficznych dla wspomagania czynności cyklu decyzyjnego procesu dowodzenia w wojskach lądowych. Wnosi ono nową jakość do procesu dowodzenia poprzez zastąpienie tradycyjnych prac sztabowych na mapach i papierze, pracą interaktywną przy komputerach połączonych w ramach lokalnej sieci komputerowej stanowiska dowodzenia. W celu zachowania interoperacyjności z innymi systemami oprogramowanie to spełnia standardy i zalecenia agencji NATO w zakresie:

· obowiązujących dokumentów (STANAG 2014, STANAG 5500),
· wiadomości sformalizowanych (APP9, AdatP-3),
· znaków taktycznych (APP6A),
· modelu danych (ATCCIS),
· map numerycznych (VPF, CADRG)
· modelu terenu (DTED).

Oprogramowanie użytkowe dostarcza osobom funkcyjnym poszczególnych komórek organizacyjnych stanowisk dowodzenia obsługę następujących podstawowych usług:

- administrowania i zarządzania systemem;
- utrzymywania i zarządzania bazą danych;
- sporządzania i wymiany dokumentów i elementów danych;
- zobrazowania graficznego na podkładzie mapy rastrowej.

Wymiana informacji pomiędzy stanowiskami dowodzenia i pododdziałami dotyczy wyłącznie przesyłania dokumentów bojowych oraz sygnałów dowodzenia, alarmowania i powiadamiania.

PZSD zapewnia wymianę i obieg następujących dokumentów:

- rozkazodawczych, a w tym:
  - rozkazy bojowe/operacyjne wraz z załącznikami,
  - rozkazy administracyjne/logistyczne wraz z załącznikami,
  - zarządzenia bojowe/operacyjne wraz z załącznikami,
  - zarządzenia przygotowawcze wraz z załącznikami,
- sprawozdawczych, a w tym:
  - meldunki okresowe,
  - meldunki doraźne,
- wiadomości, a w tym:
  - wiadomości sformatowane (ADatP-3),

- wiadomości niesformalizowane.

Wszystkie dokumenty wychodzące i wchodzące na stanowisku dowodzenia, w ramach PZSD, są rejestrowane przez system automatycznie.

3.2. Elementy składowe infrastruktury teleinformatycznej (systemu łączności) wojsk lądowych

Z przeprowadzonych badań wynika, że jednym z najważniejszych elementów infrastruktury teleinformatycznej (systemu łączności) wojsk lądowych jest podsystem wymiany informacji. Zazwyczaj tworzą go cztery odmienne elementy o dużym stopniu mobilności do których należą: sieci telekomunikacyjne, sieci komputerowe, sieci pocztowe, oraz sieci sygnalizacyjne. Z uwagi na charakter pracy zespół autorski nie analizował sieci pocztowych i sygnalizacyjnych.

Nowoczesny system teleinformatyczny tworzony jest z następujących elementów: rozległego systemu transmisyjnego WAS (*ang. Wide Area Subsystem*) tworzącego bazową sieć transmisyjną, lokalnego systemu abonenckigo LAS (*ang. Local Area Subsystem*) tworzącego sieć abonencką na SD oraz systemu dostępu bezprzewodowego MS (*ang. Mobile Subsystem*) obsługującego obiekty ruchome związane z LAS i WAS[7].

Sieci telekomunikacyjne, stanowią podstawę podsystemu wymiany informacji. Umożliwiają one wymianę informacji zarówno pomiędzy zespołami funkcjonalnymi w ramach funkcjonujących (rozwiniętych) komórek organizacyjnych (stanowisk dowodzenia), jak i w ruchu. Potrzeby informacyjne procesu kierowania reagowaniem kryzysowym stawiają istotne wymagania, które są zaspokajane poprzez zastosowanie różnorodnych technologii wymiany informacji. Są to systemy i urządzenia transmisyjne i komutacyjne tworzące podsystemy WAS, LAS i MS. Z przeprowadzonych analiz wynika, że w kierowaniu reagowaniem kryzysowym, można wykorzystać następujące systemy teleinformatyczne wojsk lądowych: **sieć radiową pola walki KF i UKF, sieć radioliniowo-kablową, sieć kablową oraz sieci radiodostepu**[8].

***

Sieci radiowe pola walki stanowią podstawowy rodzaj łączności podczas działań bojowych na szczeblu taktycznym. Sieci te, oprócz transmisji mowy, mogą także stanowić platformę transmisji danych o ograniczonej przepustowości (do 2400 b/s). Radiostacje pola walki są urządzeniami o różnych zakresach częstotliwości. Wyróżnić można następujące zakresy

[7] M. Siedlecki, „*Perspektywiczny system teleinformatyczny Wojsk Lądowych*", wyd. cyt., s. 9-10.

funkcjonowania: KF (fale krótkie) 1,5 – 30 MHz oraz UKF (fale ultrakrótkie). Zakres UKF wykorzystywany jest w sieciach radiowych pracujących w częstotliwościach powyżej 30 MHz został podzielony na następujące podzakresy częstotliwości[9]:

- podzakres VHF (*ang. Very High Frequency*) - 30-87,5 MHz;
- podzakres UHF (*ang. Ultra High Frequency*) - 220-520 MHZ;
- podzakres SHF (*ang. Super High Frequency*) - 3-30 GHz;
- podzakres EHF (*ang. Extremely High Frequency*) - 30-300 GHz.

***

Sieci radiowe KF służą do zapewnienia łączności zespołom funkcjonalnym oraz osobom funkcyjnym znajdującym się w ruchu w odległościach przekraczających zasięg środków łączności UKF. Sieci KF mogą dublować określone relacje łączności funkcjonujące w sieciach radiowych UKF. Takie rozwiązanie jest stosowane w przypadku gdy odległości pomiędzy SD przekraczają zasięgi radiostacji UKF. Radiostacje KF umożliwiają łączność na średnie i duże odległości. Zasięg radiostacji KF z wykorzystaniem fali przyziemnej wynosi do kilkudziesięciu kilometrów. Wykorzystanie efektu odbicia fal radiowych od jonosfery pozwala na uzyskanie zasięgów rzędu 300-3000 km[10].

***

Sieci radiowe UKF zapewniają łączność zespołom funkcjonalnym oraz wybranym osobom funkcyjnym znajdującym się w ruchu. Sieci te są wykorzystywane są przez osoby funkcyjne znajdujące się na rozwiniętych miejscach pracy (stanowiskach dowodzenia) w przypadku braku sprawności sieci stacjonarnych lub sieci radioliniowo-kablowej, sieci kablowej, sieci komputerowej itp. Radiostacje UKF posiadają możliwość integracji sieci radiowych z siecią radioliniowo-kablową za pomocą radiodostępu. Sieci radiowe UKF umożliwiają wysoką jakość łączności przy jednoczesnej dużej odporność na zakłócenia. Niewielki zasięg radiostacji UKF, który w warunkach działań wojennych utrudnia przeciwnikowi rozpoznanie i zakłócenie ich pracy, ogranicza ich wykorzystanie w kierowaniu reagowaniem kryzysowym tylko do niewielkiego obszaru. Radiostacje UKF zapewniają, z wykorzystaniem fali przyziemnej, zasięg do maksymalnie 35-50 km[11]. Zastosowanie technologii skaczącej częstotliwości w znaczny sposób redukuje te zasięgi.

***

---

[8] Praca zbiorowa pod kierunkiem J. Janczaka, „*System Łączności Brygady*", wyd. cyt., s. 24.
[9] P. Daniluk, „*Radiostacje sieci pola walki*", Przegląd Wojsk Lądowych Nr 7/2005, Warszawa 2005, s. 77.
[10] Praca zbiorowa pod kierunkiem J. Janczaka, „*System Łączności Brygady*", wyd. cyt., s. 11.
[11] P. Daniluk, „*Sieci ultrakrótkofalowe pola walki*", Przegląd Wojsk Lądowych Nr 5/2005, Warszawa 2005, s. 81.

Sieć radioliniowo-kablowa oparta jest na wykorzystaniu torowych środków transmisyjnych. Charakteryzuje się ona znaczną odpornością na rozpoznanie i oddziaływanie systemów walki elektronicznej przeciwnika, co w warunkach reagowania kryzysowego nie ma większego znaczenia. Sieć ta wymaga odpowiednio długiego czasu na pełne rozwinięcie, co stanowić może istotne ograniczenie. Z drugiej strony sieć radioliniowo-kablowa zapewnia znacznie więcej usług niż sieci radiowe przy jednoczesnej dużej przepustowość, dochodzącej do 8 Mb/s. Sieć radiloliniowo-kablowa budowana jest na bazie aparatowni transmisyjnych RWŁC-10T oraz komutacyjnych RWŁC-10K, z wykorzystaniem radiolini R-432 i R-450 systemu STORCZYK[12].

***

Sieć kablowa służy do wymiany informacji pomiędzy osobami funkcyjnymi i zespołami funkcjonalnymi w ramach miejsca pracy (rozwiniętego stanowiska dowodzenia) - sieci kablowe wewnętrzne; oraz pomiędzy miejscami pracy (stanowiskami dowodzenia) - sieci kablowe dalekosiężne. Sieci kablowe dalekosiężne stanowią zazwyczaj uzupełnienie wykorzystywanych sieci radiowych. Wewnętrzne sieci kablowe są wykorzystywane jako podstawowy środek wymiany informacji w miejscu pracy (na stanowisku dowodzenia) i zapewniają dostęp do sieci radioliniowo-kablowej.

***

Sieci radiodostępu umożliwiają sprzężenie poprzez radiostację i *blok sprzężenia radiowego* (BSR) abonenta ruchomego sieci radiowej z siecią radioliniowo-kablową. W strukturze sieci radiodotępu tworzone są *radiowe punkty dostępu* (RPD) oraz *radiowe punkty abonenckie* (RPA). RPD stanowią podstawowy element sieci *jednokanałowego i wielokanałowego radiodostępu simpleksowego*. BSR pracujący w ramach RPD powinien zapewniać realizację automatycznie zestawianych połączeń: RPA z dowolnym radioliniowo-kablowym punktem abonenckim i odwrotnie, radioliniowo-kablowego punku abonenckiego z takim samym punktem abonenckim przez sieci radiowe, RPA z innym RPA innej sieci radiowej poprzez sieć radioliniowo-kablową. W celu budowy radiodostępu na potrzeby kierowania reagowaniem kryzysowym można wykorzystać jednokanałowy radiodostęp simpleksowy (JRS), aparatownie wielokanałowego radiodostępu simpleksowego (AWRS) oraz wóz dostępu radiowego (WDR) systemu KROKUS[13].

***

[12] Praca zbiorowa pod kierunkiem J. Janczaka i P. Daniluka, „*Środki dowodzenia*", wyd. cyt., s. 18.
[13] J. Michniak, „*Dowodzenie i łączność*", wyd. cyt., s.185.

Sieć komputerowa służy do wymiany informacji w formie transmisji danych pomiędzy osobami funkcyjnymi i zespołami funkcjonalnymi wyposażonymi w komputery (lub inne urządzenia np. telefony IP) poprzez użycie medium transmisyjnego jakim jest kabel, światłowód, fale radiowe itp. Sieci komputerowe zapewniają wspomaganie przetwarzania informacji w cyklu decyzyjnym procesu dowodzenia (kierowania)[14]. Umożliwiają dostęp do odpowiednich baz danych a także dostęp do współdzielonych zasobów sieciowych takich jak: drukarki, plotery urządzenia pamięci masowych. Pozwalają dotrzeć do współdzielonych zasobów sieciowych z rożnych lokalizacji poprzez usługi zdalnego dostępu. W zależności od realizowanych funkcji, wykorzystywanych urządzeń sieciowych oraz obsługiwanego obszaru można wyróżnić lokalne sieci komputerowe rozwijane zazwyczaj na stanowiskach dowodzenia (*ang. LAN – local area network*)) i rozległe sieci komputerowe (*ang. WAN – wide area network*) zapewniające transmisje danych pomiędzy poszczególnymi sieciami lokalnymi. Przeprowadzone badania wykazały, że znaczenie sieci komputerowych w każdej działalności wojsk, także w kierowaniu reagowaniem kryzysowym, będzie rosło. Będzie to zasługą coraz większej przepustowości sieci komputerowych przy jednoczesnym wzroście jakości i ilości usług przez nie świadczonych.

Lokalna sieć komputerowa umożliwia wyminę informacji pomiędzy osobami funkcyjnymi oraz zespołami funkcjonalnymi w ramach stanowiska dowodzenia.

Sieci komputerowe stanowisk dowodzenia powinny być wyposażane w następujące elementy:

- systemy przetwarzania;
- systemy przechowywania;
- systemy transmisji danych;
- układy połączeń kablowych i bezprzewodowych.

Systemy przetwarzania to między innymi zautomatyzowane systemy dowodzenia których głównym zadaniem jest wspomaganie pracy operatorów na stanowisku dowodzenia. Należy zaznaczyć, że w skład systemów przetwarzania wchodzę zarówno serwery umieszczone w Centralnym Węźle Dystrybucyjnym (opisanym w dalszej części opracowania) jak i poszczególne stacje robocze rozmieszczone na stanowiskach pracy operatorów.

Systemy przechowywania to dedykowane serwery zdolne do przechowywania informacji opracowywanej na stanowisku dowodzenia. Serwery te muszę się charakteryzować

[14] Praca zbiorowa pod kierunkiem J. Janczaka, „*System Łączności Brygady*", wyd. cyt., s. 8.

dużą niezawodnością i zapewniać ciągłą dostępność danych dla operatorów. Z tego też względu niezbędne jest przechowywanie tej samej informacji w różnych miejscach.

Systemy transmisji danych i układy połączeń kablowych i bezprzewodowych to nic innego jak fizyczna realizacja sieci komputerowej na stanowisku dowodzenia. W skład każdej sieci oprócz odpowiednich połączeń wchodzą urządzenia aktywne (switche, routery, huby) zdolne do transmisji danych na ustalonych przez administratora sieci (zespół łączności i informatyki) zasadach.

Sieci komputerowe stanowisk dowodzenia muszą spełniać szereg następujących wymagań[15]:

- łatwość i szybkość rozwijania sieci w każdych warunkach atmosferycznych i terenowych;
- możliwość rozwijania sprzętu zarówno w namiotach, budynkach jak i na pojazdach;
- niezawodność działania w trudnych i zmiennych warunkach otoczenia;
- dużą mobilność sprzętu (łatwość transportowania);
- konieczność ograniczenia emisji elektromagnetycznej (ujawniającej).

Istotnym wymaganiem stawianym sieciom komputerowym rozwijanym w warunkach polowych jest niski poziom emisji ujawniającej oraz jej odporność na zagrożenia elektromagnetyczne. Wymagania te zawarte są odpowiednio w normach NO-06-A200, NO-06-A500, (MIL Std 461D), MIL Std 188-125-2.

Sieci komputerowe pracujące na stanowiskach dowodzenia, na dzień dzisiejszy, są wykonane w głównej mierze w standardzie transmisji Ethernet IEEE802.3. Standard ten jest najszybciej rozwijającym się na świecie standardem transmisji przewodowej. Jego wykorzystanie w sieciach komputerowych rozwijanych na stanowiskach dowodzenia pozwala na uzyskiwanie dużych szybkości transmisji. W zastosowaniach militarnych do transmisji danych w tym standardzie wykorzystywane są dwa podstawowe rodzaje kabli:

- polowe kable skrętkowe kategorii piątej w standardach Ethernet 10 Base T i Ethernet 100 Base Tx;
- polowe kable światłowodowe w standardach Ethernet 10 Base FL i Ethernet 100 Base Fx .

Polowe kable skrętkowe pozwalają na transmisję danych na odległość do 90m, natomiast polowe kable światłowodowe wielomodowe mogą transmitować dane na odległość od 500 do 4000m (wg STANAG 4290).

---

[15] M. Dras, Systemy sprzętowe do budowy polowych sieci teleinformatycznych na stanowiskach dowodzenia, materiały z sympozjum „Sieci teleinformatyczne stanowisk dowodzenia wojsk lądowych szczebla taktycznego", wyd. AON Warszawa 2005, s. 31

Rozległa sieć komputerowa, budowana jest zazwyczaj na bazie sieci radioliniowo-kablowej, do której dołączone są sieci lokalnych stanowisk dowodzenia. Do tworzenia sieci rozległej mogą być wykorzystane węzły pakietowe WP-40, będące elementami wyposażenia aparatowni transmisyjnych (RWŁC-10T) oraz komutacyjnych (RWŁC-10K). Węzły pakietowe umożliwiają budowę sieci rozległej z użyciem protokołów TCP/IP na bazie połączeń komutowanych systemu STORCZYK. Rozległa sieć komputerowa może zostać zbudowana również na bazie systemu KROKUS. W ramach systemu KROKUS wykorzystywane mogą zostać stacjonarne lub mobilne (kontenerowe) obiekty: aparatownie komutacyjno-dostępowe (AK-D), komutacyjno-bazowe (AK-B), transmisyjne (AT), zarządzania (AZSSŁ). Z przeprowadzonych badań wynika, że w operacjach reagowania kryzysowego do tworzenia sieci rozległej powinna być wykorzystana istniejąca cywilna infrastruktura teleinformatyczna, która po złączeniu z siecią radioliniowo-kablową (aparatowniami transmisyjnymi i komutacyjnymi) zapewni organom funkcjonalnym usługi transmisji danych, obrazu, mowy itp. Należy przypuszczać, że stopień wykorzystania stacjonarnej infrastruktury teleinformatycznej zależeć będzie w głównej mierze od charakteru wykonywanej operacji reagowania kryzysowego, istniejącej infrastruktury w obszarze działa i stopnia jej zniszczenia (dostępność dla organów reagowania kryzysowego).

W praktyce budowa rozległej sieci komputerowej stanowi poważny problem natury technicznej i organizacyjnej. Powodowane to jest specyfiką planowanych do wykorzystania sieci oraz warunkami ich eksploatacji. Sieci te muszą zapewnić niezawodną eksploatację w różnych warunkach środowiskowych, często bardzo ekstremalnych[16].

3.3. Środki i urządzenia techniczne wykorzystywane do organizacji sieci teleinformatycznych wojsk lądowych

Określoną strukturę organizacyjno-funkcjonalną sieci teleinformatycznej można utworzyć, z różnych urządzeń technicznych (telekomunikacyjnych i informatycznych). Niezależnie jednak od technologii wykonania, z technicznego punktu widzenia w sieci teleinformatycznej można wyodrębnić następujące grupy urządzeń:

- teletransmisyjne;
- komutacyjne;
- informatyczne;

---

[16] K. Sejdak, „*Lokalne sieci komputerowe na stanowisku dowodzenia*", Przegląd Wojsk Lądowych Nr 10/2003, Warszawa 2003, s. 19.

99

- przetwórcze.

Wymienione urządzenia w sieci teleinformatycznej na ogół rzadko występują samodzielnie. Wynika to stąd, że zestawy urządzeń teletransmisyjnych przekazują swe międzywęzłowe kanały transmisyjne do eksploatacji przez urządzenia komutacyjne, stwarzając warunki do okresowego wykorzystania tych kanałów przez różnych użytkowników. Ze względu na potrzeby wykorzystania różnych urządzeń przez różnych użytkowników albo wykorzystania kilku urządzeń w tym samym czasie, konieczne jest tworzenie dość złożonych zestawów funkcjonalnych, które są podstawowymi komponentami sieci teleinformatycznej.

W celu określenia struktury sieci teleinformatycznej niezbędne jest poddanie analizie możliwości, jakie oferują nowoczesne zestawy funkcjonalne urządzeń telekomunikacyjnych i informatycznych. Zestawy takich urządzeń pozwolą na funkcjonowanie określonej sieci teleinformatycznej wojsk lądowych.

3.3.1. Środki i urządzenia transmisyjne

Środki i urządzenia przeznaczone do transmisji informacji mogą być rozpatrywane jako środki i urządzenia:

- radiowe (radiostacje);
- radioliniowe (radiolinie);
- kablowe i kable;
- satelitarne.

3.3.1.1. Środki i urządzenia radiowe

Na podstawie wyników z przeprowadzonych badań przyjęto, że radiostacje wykorzystywane w wojskach lądowych funkcjonują w sieciach i kierunkach radiowych jako urządzenia różnych zakresów częstotliwości, gdzie:

- **radiostacje KF** wykorzystują najczęściej zakres 1,5–30 MHz i umożliwiają stosowanie nowoczesnych technik pracy. Radiostacje takie docelowo powinny pozwalać na ograniczony radiodostęp i transmisję danych, a zasięg takich urządzeń powinien być rzędu 300 – 3 000 km;

- **radiostacje UKF** pracują na częstotliwościach powyżej 30 MHz (dla radiostacji starszych generacji zakres ten zaczyna się od 20 MHz), najczęściej z zastosowaniem skoku częstotliwości przy zapewnieniu zasięgu do 35–50 km.

Stosując kryterium częstotliwości, radiostacje zakresu UKF dzieli się na:

- **radiostacje podzakresu VHF** (standardowo podzakres 30–88 MHz), których praca, szczególnie w sieciach dowodzenia wojsk lądowych, powinna być wspomagana usługami świadczącymi przez urządzenia radiodostępowe. Maksymalna moc radiostacji pokładowych i bazowych powinna wynosić do 50 W, przy zasięgu stacji bazowych około 15 km oraz zasięgu bezpośrednim do 50 km;
- **radiostacje podzakresu UHF** (standardowo podzakres 220–400 MHz), które są reprezentowane przede wszystkim przez urządzenia lotnicze zakresu decymetrowego oraz radiotelefony do łączności lokalnej (wewnętrznej) i środki telekomunikacyjne sieci szerokopasmowych dostępowych;
- **radiostacje podzakresu SHF**, które pracują na częstotliwościach rzędu GHz jako radiotelefony o zasięgu lokalnym (np. w obrębie jednostki lub stanowiska dowodzenia) lub wąskopasmowe terminale satelitarne.

Przenośne, pokładowe i modułowe radiostacje UKF powinny zapewniać zasięg łączności do 35–40 kilometrów. Radiostacje tego typu powinny umożliwiać przesyłanie fonii, transmisję danych (w przypadku wersji cyfrowych) oraz pośredniczyć w trafiku radiowym jako stacje bazowe lub retransmisyjne.

Radiostacje tego typu powinny funkcjonować jako cyfrowe oraz analogowe, co wykazały wyniki analiz sieci funkcjonujących w wybranych armiach państw NATO. W technice cyfrowej powinny mieć także możliwość pracy w trybie skoku częstotliwości.

Radiostacje KF powinny być wykorzystywane do zapewnienia łączności na średnie i dalekie odległości (powyżej 35–50 km) oraz dla użytkowników z dużym rozproszeniem. Należy wykorzystywać częstotliwości między 1,5 i 30 MHz. Praca w takich sieciach odbywa się na fali powierzchniowej i przestrzennej (najlepiej pod jak najmniejszym kątem) dla średnich i dalekich zasięgów.

W wojskach lądowych radiostacje są wykorzystywane w różny sposób, zarówno w sieciach jak i kierunkach radiowych, przy czym mogą funkcjonować z wykorzystaniem radiodostępu. Jako punkty jednokanałowego simpleksowego dostępu radiowego powinny zapewnić użytkownikom tego podsystemu możliwość korzystania z sieci radioliniowo-kablowej przy stosowaniu pracy fonem i transmisji danych.

W skład sieci wykorzystujących radiodostęp powinny wchodzić radiowe punkty dostępu (RPD) oraz radiowe punkty abonenckie (RPA).

Radiowe punkty dostępowe są zasadniczym elementem jednokanałowego radiodostępu simpleksowego. Realizują one dostęp drogą radiową (w sieciach lub kierunkach radiowych) do sieci radiliniwo-kablowej, zapewniając wymianę informacji jawnych, niejawnych fonicznych i w formie graficznej oraz transmisję danych. Dostęp tego typu oferuje połączenia z abonentami tej samej sieci lub sieci radioliniowo-kablowej.

Blok sprzężenia radiowego (BSR), pracujący w ramach RPD, powinien realizować automatyczne zestawianie połączeń:

- radiowego punktu abonenckiego (RPA) z dowolnym radioliniowo-kablowym punktem abonenckim i odwrotnie;
- radioliniowo-kablowego abonenta z takim samym abonentem poprzez sieć łączności radiowej;
- radiowych punktów abonenckich z innym takim punktem innej sieci za pośrednictwem sieci radioliniwo-kablowej.

Wyposażenie punktu abonenckiego powinno umożliwiać prowadzenie rozmów i transmisję danych w sieciach jednokanałowego radiodostępu simpleksowego oraz w sieciach radiowych.

Nowym rodzajem radiostacji są radiostacje szerokopasmowe, zapewniające transmisję danych o przepływnościach do 512 kbit/s. Przykładem jest radiostacja HCDR (ang. The High Capacity Data Radio).

3.3.1.2. Środki i urządzenia radioliniowe

Radiolinie stanowią środek łączności, coraz częściej zastępujący łączność kablową, przy zapewnieniu porównywalnych wartości przepustowości. Pozwalają one przesyłać coraz większe ilości informacji w coraz krótszym czasie. Bardzo duża mobilność radiolinii i wielowariantowość wykorzystania powodują bezsprzeczne wypieranie kabla przez nowoczesne odmiany tych urządzeń w coraz liczniejszych zastosowaniach. Coraz większe wymagania przepustowości oraz kierunkowości działania radiolinii spowodowały wykorzystywanie przez te urządzenia coraz wyższych częstotliwości, co z kolei spowodowało znaczne zmniejszenie anten. Miniaturyzacja objęła również same urządzenia nadawczo-odbiorcze.

Powszechnie stosowaną radiolinią cyfrową w wojskach lądowych jest R-432, trwają natomiast prace nad wdrożeniem urządzeń serii R-450.

Radiolinia R-432 (R-432E/ R-432AE) jest środkiem łączności mogącym funkcjonować w nowoczesnych systemach szerokopasmowych w ramach aparatowni łączności typu RWŁC-10/T, które z kolei stanowią zasadnicze elementy węzłów łączności stanowisk dowodzenia brygad, dywizji oraz węzłów sieci pomocniczej.

Radiolinia R-450 (R-450A, R-450A1, R-450B, R-450B1, R-450C) jest urządzeniem najnowszej generacji horyzontowych radiowych linii telekomunikacyjnych dużej pojemności. Radiolinia tego typu jest przeznaczona do zastosowania na szczeblach taktycznych i operacyjnych, w systemach mobilnych i stacjonarnych. Obsługuje rozszerzone pasma częstotliwości i trakty o zwiększonej przepustowości. Może funkcjonować w aktualnie eksploatowanych sieciach opartych na technologii TDM, jak i w systemach o rozwiązaniach typu ATM. W zależności od konfiguracji umożliwia ona trzy zasadnicze rodzaje pracy:

- **pierwszy (punkt–wielopunkt)** – szerokopasmowy dostęp obiektów ruchomych (WD, WDSz, przemieszczających się aparatowni RWŁC-10/T) do sieci radioliniowo-kablowej lub innej o charakterze stacjonarnym, maksymalnie do 32 obiektów;
- **drugi (wielopunkt–wielopunkt)** – radiowy system pakietowy, maksymalnie 64 obiekty o łącznej przepustowości 4096 kbit/s;
- **trzeci (punkt–punkt)** – tworzenie linii radiowych małej i średniej pojemności (do 2048 kbit/s), zarówno między obiektami znajdującymi się w ruchu, jak i na postoju.

3.3.1.3. Środki i urządzenia kablowe

W celu dokonania identyfikacji środków i urządzeń kablowych określono dwa obszary wykorzystania identyfikowanych środków:

- wewnętrzne sieci teleinformatyczne (stanowisk dowodzenia);
- kablowe linie telekomunikacyjne (zwane też dalekosiężnymi).

Urządzeniami kablowymi, które mogą być wykorzystane do budowy wewnętrznych sieci teleinformatycznych, są:

a) polowy kabel lekki (PKL), służacy do jednorazowych połączeń lokalnych, składa się z dwóch żył oddzielnie izolowanych (PKL 1 x 2). Zbudowany jest z miedzi i stali. Izolację wykonano z polwinitu. Impedancja falowa – 760 Ω. Długość odcinka (bębna) – 750 m. Waga odcinka – 10,5 kg.

b) polowy kabel miejscowy (PKM), przeznaczony jest do transmisji sygnałów z przepustowością binarną do 10 Mbit/s w polowych sieciach łączności, z lokalnymi sieciami komputerowymi włącznie. Wspólny ekran chroni przed wpływem zewnętrznych zakłóceń

elektromagnetycznych i zapewnia prawidłową transmisję sygnałów analogowych i cyfrowych.

Konstrukcja kabla zapewnia mechaniczne rozwijanie i zwijanie bez uszkodzeń, podwieszanie na podporach naturalnych i sztucznych oraz układanie na ziemi, jak też możliwość pokonywania przeszkód wodnych przy zanurzeniu w wodzie do 10 m. Zbudowano go z 10 wiązek parowych skręconych w jedną grupę (PKM 10 x 2) z miedzi. Impedancja falowa kabla – 760 Ω. Izolację wykonano z polietylenu. Długość odcinka kabla – 100 m. Waga 1 km tego kabla – 260 kg.

c) telefoniczno-telegraficzny kabel węzłowy (TTWK), o podobnym zastosowaniu jak PKM (był to poprzednik kabla PKM), zbudowany z 10 (TTWK 10 x 2) lub 5 (TTWK 5 x 2) wiązek parowych skręconych w jedną grupę z drutu z miedzi. Waga 1 km kabla wynosi odpowiednio: 450 i 375 kg.

d) polowy kabel skrętkowy typu PKS 2 x 2 x 0,34 jest dwuparową skrętką ekranowaną kategorii 5 przeznaczoną do transmisji sygnałów cyfrowych z szybkością do 100Mb/s. Miedziany ekran chroni kabel przed wpływem zakłóceń elektromagnetycznych i zapewnia poprawność transmisji sygnałów. Dodatkowy oplot ze strun fortepianowych zapewnia dużą odporność kabla na zrywanie, dając dopuszczalną siłę naciągu kabla do 1200 N. Konstrukcja kabla zapewnia możliwość jego wielokrotnego zwijania i rozwijania, podwieszanie na podporach oraz pokonywanie nim przeszkód wodnych o głębokości do 10 m. Kabel na obu końcach jest zakończony kroploszczelnymi wtykami wielostykowymi (zgodnie ze standardem MIL-26482) z kapturkami zabezpieczającymi. Miejsce połączenia złącza z kablem jest dodatkowo uszczelnione kształtką termokurczliwą.

e) polowy kabel światłowodowy CTOS (PKŚ CTOS), wykorzystywany do transmisji sygnałów optycznych pomiędzy różnego rodzaju aparatowniami i koncentratorami zawierającymi elementy funkcjonalno-techniczne lokalnych sieci informatycznych, przystosowany do częstego i wielokrotnego zwijania i rozwijania w warunkach pola walki. Posiada tłumienność 1,3dB/km dla fali 130 nm, a szerokość pasma przenoszenia wynosi 500 MHz/km.

Do budowy kablowych linii telekomunikacyjnych (dalekosiężnych) wykorzystuje się:

a) polowy kabel akustyczny (PKA) –dalekosiężny dwużyłowy (PKA 1 x 2) kabel z miedzi. Izolację wykonano z polwinitu lub polietylenu. Długość odcinka – 800 m. Waga odcinka – 56 kg. Kabel jest zakończony półzłączem.

b) polowy kabel dalekosiężny (PKD) to kabel jednoczwórkowy (PKD 1 x 4). Posiada impedancję falową rzędu 115–117 Ω. Rezystancja żyły w 1 km wynosi mniej niż 57 Ω.

Średnica kabla – 11,4 mm. Długość odcinka – 250 m. Masa odcinka kabla – 48 kg. Odmiana tego kabla – PKD 2 x 2 – charakteryzuje się: impendancją falową 120 Ω, rezystancją żyły w 1 km 57 Ω. Kabel składa się z czterech żył w izolacji z polietylenu. Długość odcinka kabla – 250 m, ciężar 1 km – 144 kg.

3.3.1.4. Środki i urządzenia satelitarne

Na podstawie wyników badań zespół autorski przyjął potrzebę funkcjonowania w sieci teleinformatycznej wykorzystywanych do kierowania reagowaniem kryzysowym satelitarnych linii telekomunikacyjnych. Istnienie tego typu linii telekomunikacyjnych znacznie zwiększy zasięg organizowanych relacji wymiany informacji.

Ogólnie można wyróżnić dwa podstawowe rodzaje środków satelitarnych, wykorzystywanych do budowy satelitarnych linii telekomunikacyjnych. Jedne mogą być stosowane w wojskowych sieciach łączności satelitarnej (TACSAT), drugie są wykorzystywane w cywilnych (ogólnodostępnych) sieciach łączności satelitarnej.

Urządzenia pracujące w sieciach TACSAT charakteryzują się pracą typu półdupleks (odbiór lub tylko nadawanie) na dwóch częstotliwościach, jedna do kontaktu z satelitą, druga do odbierania sygnału z satelity.

Reprezentantami urządzeń pracujących w militarnych jednokanałowych sieciach satelitarnych są wojskowe terminale radiotelefoniczne typu: HST-4, AN/PSC-3, AN/URC-101/104/110 oraz LST-5C. Urządzenia takie pracują w najniższych zakresach częstotliwości przeznaczonych do komunikacji poprzez satelitę, tj. w paśmie 225–400 MHz, co umożliwia również wykorzystanie ich do łączności z innymi radiostacjami, lotniczymi w pasmach decymetrowych 222–395 MHz (praca emisjami z modulacją AM) oraz radiotelefonicznymi cywilnymi. Pozwalają one, jako urządzenia przenośne, na prowadzenie łączności jednokanałowej – telefonicznej, transmisji danych oraz odbioru sygnałów wzorcowych (nawigacyjnych).

Radiostacje takie pracują z modulacją amplitudy, częstotliwości i impulsu, z mocą wyjściową nadajnika standardową dla urządzeń przenośnych, tj. 2–18 watów. Radiostacje tych sieci, określane mianem „urządzeń terminalowych", występują w następujących wersjach:

- plecakowej (najczęściej jako radiostacja plecakowa pracująca nie tylko via satelita, ale również z wykorzystaniem fali przyziemnej);
- pokładowej.

Inny rodzaj urządzeń radiowej łączności satelitarnej stanowią terminale jednokanałowego dostępu satelitarnego INMARSAT, który jest systemem komercjalnym, ogólnodostępnym, sprawdzonym podczas wielu lat eksploatacji, wykorzystywanym przez bardzo różnych użytkowników.

Korzystanie z terminala umożliwia realizację rozmów telefonicznych, wymianę informacji radiotelefaksowych, transmisję danych o szybkości 2400, 5600, 9600 bit/s, pracę faksymilów, selektywne wywołania grupowe, łączność w niebezpieczeństwie – bezzwłoczne połączenia w trybie awaryjnym, przesyłanie obrazów stałych i ruchomych oraz emisję częstotliwości wzorcowych, sygnałów czasu, banku danych meteorologicznych i innych sygnałów serwisowych. Terminal abonencki składa się z komputera przenośnego (typu laptop), urządzenia radiowego, anteny warstwowej i manipulatora z klawiaturą, a w niektórych wersjach także z drukarki. Wszystko to mieści się w niewielkiej walizce. Można wyodrębnić różne warianty wyposażenia urządzeń do pracy w tym systemie satelitarnym:

- **standard A** – wersja mobilna o mocy 35 dBW wymagająca oddzielnego pojazdu do zainstalowania urządzenia z anteną paraboliczną lub helikalną o średnicy 0,9 m;
- **standard B** – zestaw pracuje telefonią, telefaksem oraz transmisją danych; standardowo odbywa się praca w trybie bazowym (stacjonarnym) w 10 kanałach (fonicznych, faksowych, transmisji danych).
- **standard C** – najmniejszy i najprostszy zestaw z anteną dookólną, z tego powodu występują ograniczenia dla przesyłania pełnej transmisji danych i obrazów.

3.3.2. Środki i urządzenia komutacyjne

Urządzenia komutacyjne (w tym kanałotwórcze) są reprezentowane przez:

- łącznice średniej pojemności (ŁC-240, ŁC-480);
- łącznice DGT 3450 – 1 WW;
- łącznico-krotnice o małej pojemności (ŁK-24);
- krotnice cyfrowe różnego typu (KX-30, KX-30 PCM).

Łącznica cyfrowa (ŁC-240, ŁC-480) jest podstawowym urządzeniem stacjonarnych i mobilnych sieci telekomunikacyjnych funkcjonujących obecnie w wojskach lądowych. Przeznaczona jest do wykorzystania na szczeblach taktycznych i operacyjnych. Łącznica cyfrowa stosowana jest do budowy sieci telekomunikacyjnej systemu „STORCZYK". Może spełniać funkcję węzła tranzytowego lub, przy współpracy z KX-30, węzła końcowego dużej pojemności dla urządzeń przetwórczych analogowych i cyfrowych.

Łącznica cyfrowa służy do komutacji kanałów cyfrowych o przepływnościach od 16 do 2048 kbit/s, będących wielokrotnością 16 kbit/s. Przy współpracy z krotnicą KX-30 umożliwia oddawanie kanałów i grup kanałów według tych samych wartości. Pozwala ona automatycznie zestawiać połączenia dla wszystkich urządzeń przetwórczych typu CA (centrali abonenckiej), a poprzez lokalne stanowisko operatora (LSO) dla wszystkich urządzeń przetwórczych MB (miejskiej baterii) oraz współpracujących central analogowych.

Wśród podstawowych parametrów łącznicy na uwagę zasługują:

- 8 uniwersalnych przyłączy o przepływnościach 64–2048 kbit/s do połączenia krotnic lub innych łącznic;
- bezblokadowa komutacja 480 (dla ŁC-240) lub 960 (dla ŁC-480) kanałów;
- kanały podstawowe o szybkości 16 lub 32 kbit/s;
- możliwość łatwej rozbudowy węzła;
- kontrola i sterowanie z pulpitu operatora lub z systemu utrzymaniowego;
- dokumentacja stanu ruchu i realizowanych połączeń.

Łącznica DGT 3450-1WW przeznaczona jest do organizowania wojskowych sieci telekomunikacyjnych na szczeblach operacyjnych i taktycznych. Może spełniać następujące funkcje:

- węzła telekomunikacyjnego mobilnych sieci telekomunikacyjnych związku taktycznego lub operacyjnego;
- węzła tranzytowo-końcowego w wielobocznej sieci telekomunikacyjnej;
- bramy sieci telekomunikacyjnej strategicznej do taktycznej DSTG (STANAG 4578 ed. 2) pomiędzy sieciami EuroISDN a sieciami taktycznymi;
- centrali dyspozytorskiej stanowisk dowodzenia;
- krotnicy cyfrowej z możliwością dołączenia traktów 2 Mbit/s oraz traktów ze stykiem Eurocom.

Łącznica DGT 3450-1WW zapewnia realizację połączeń dla linii: abonenckich analogowych, abonenckich ISDN oraz cyfrowych systemowych.

Łącznico-krotnica ŁK-24 umożliwia:

- organizowanie węzłów telekomunikacyjnych o małej pojemności;
- przyjęcie 3 uniwersalnych traktów o przepływnościach 64, 128, 2048 kbit/s, umożliwiających podłączenie krotnic lub innych łącznic;
- obsługę 24 linii abonenckich.

Do urządzeń kanałotwórczych należą:

107

Krotnica cyfrowa KX-30, która pozwala zwielokrotnić linie abonenckie w jeden trakt dołączony do łącznicy (np. ŁC-480) lub radiolinii cyfrowej (np. R-432, R-450).

Krotnica cyfrowa KX-30 umożliwia obsługę:

- przyłącza cyfrowego do współpracy z łącznicą bezpośrednio lub poprzez trakt cyfrowy 512 kbit/s;
- 30 linii abonenckich;
- aparatów analogowych o wybieraniu dekadowym, aparatów MB (miejskiej baterii) oraz aparatów cyfrowych;
- modułów komputerowych MK-16 i MK-32 oraz cyfrowych środków radiowych o kanale o przepustowości 16 kbit/s.

Krotnica KX-30/PCM umożliwiająca współpracę sieci polowej z siecią publiczną. Przeznaczona do zwielokrotnienia strumienia o przepływności 2048 kbit/s w postaci 30 kanałów cyfrowych i analogowych różnych typów oraz do odprowadzenia części kanałów ze strumienia międzycentralowego.

Krotnica ma następujące możliwości oddawania kanałów cyfrowych:

- na poziomie pojedynczych kanałów 64 kbit/s lub par kanałów 64 kbit/s;
- na poziomie grup kanałów 64 kbit/s w postaci strumieni o przepływności 128, 256, 512, 1024 kbit/s.

Ma także możliwości oddawania kanałów analogowych:

- w postaci łącza abonenckiego typu CA z wybieraniem dekadowym;
- w postaci łącza międzycentralowego, współpracującego z translacjami centralowymi.

3.3.3. Środki i urządzenia informatyczne

Do urządzeń informatycznych wykorzystywanych w wojskach lądowych możemy zaliczyć:

- koncentrator LANBOX LB10K;
- koncentrator LANTELBOX;
- WAN Box ZWT KTSAwp;
- LAN Access Box ZWT KTSAwp;
- WAN Access Box ZWT KTSAwp;
- LAN Backbone Box ZWT KTSAwp;
- węzły pakietowe WP-40;

- router Box ZWT KTSAwp.

Polowy koncentrator sieciowy LANBOX LB10K, będący elementem przełączającym w wewnętrznych sieciach informatycznych, rozwijanych na stanowiskach dowodzenia. Koncentrator jest przeznaczony do koncentracji ruchu w sieciach LAN, pracujących w systemie Ethernet. Zapewnia cyfrową transmisję sygnałów po liniach kablowych, po torach miedzianych poprzez polowe kable skrętkowe PKS 2 x 2 x 0,34 a po torach światłowodowych poprzez polowy kabel światłowodowy PKŚ CTOS.

Koncentrator LANTELBOX jest polowym, przenośnym urządzeniem teleinformatycznym służącym do rozwinięcia wewnętrznej sieci teleinformatycznej z 30 abonentami końcowymi telefonicznymi oraz z 10 terminalami komputerowymi. Wewnętrzna sieć teleinformatyczna, rozwinięta przy pomocy koncentratora LANTELBOX, pracuje w standardzie ISDN dla połączeń telefonicznych i dla połączeń terminali komputerowych w standardach Ethernet 10BaseT i 100BaseTx.

WAN Box ZWT KTSAwp jest zestawem intrfejsów stykowych przeznaczonym do współpracy z urządzeniami teletransmisyjnymi. Posiada multiplekser traktu E1 (G.703) oraz bramę VoIP umożliwiającą łączenie telefonii IP z siecią telefoniczną ISDN poprzez styk 30B+D typu PRI.

LAN Access Box ZWT KTSAwp z dwoma wbudowanymi przełącznikami Ethernet, przeznaczony jest do rozwinięcia wewnętrznej sieci teleinformatycznej stanowisk dowodzenia z możliwością podłączenia terminali komputerowych i aparatów telefonicznych IP. Porty tych przełączników umożliwiają zasilanie aparatów telefonicznych IP.

WAN Access Box ZWT KTSAwp jest wyposażony w router sieci WAN, przełącznik Ethernet, serwer pokładowy oraz odbiornik GPS. Wyposażenie tego urządzenia umożliwia rozwinięcie bezprzewodowych wewnętrznych sieci teleinformatycznych na stanowiskach dowodzenia według. standardu 802.11 (access point i bridge) oraz złącza polowego kabla światłowodowego. Może funkcjonować jako brama pomiędzy siecią kablową i siecią bezprzewodową LAN. Jednocześnie jest routerem z obsługą VPN wykorzystującym szyfrowanie IPSec.

LAN Backbone Box ZWT KTSAwp jest wyposażony w dwa programowalne przełączniki Ethernet oraz zespół konwerterów światłowodowych i półzłącza burtowe polowego kabla światłowodowego. Posiada miejsce na sprzętowe moduły IPCrypto.

Węzły pakietowe WP-40A i WP-40A2 są przeznaczone do tworzenia rozległej (szkieletowej) sieci TCP/IP na bazie połączeń komutowanych obecnie funkcjonującego

w wojskach lądowych systemu „STORCZYK". Zapewniają komputerom, sieciom lokalnym i elementom systemu zarządzania bezpośredni lub komutowany dostęp do tak utworzonej sieci i wymianę danych pomiędzy jej elementami.

W skład WP-40A i WP-40A2 wchodzi router sieci TCP/IP bazującej na cyfrowej, utajnionej sieci komutacji kanałów typu „STORCZYK".

WP-40A i WP-40A2 łączy się z innymi elementami sieci IP za pomocą 47 kanałów transmisji danych. Trzydzieści spośród nich wykorzystuje łącza komutowane doprowadzone traktem cyfrowymi o szybkości 512 kb/s do najbliższej łącznicy typu ŁC-240A lub łącznicokrotnicy ŁK-24A (również ŁC-240C i ŁC-480C). Czternaście innych kanałów jest wyposażonych w interfejsy V.24 (11 z nich o prędkości do 57,6 kb/s, trzy – do 38,8 kb/s). Służą one do podłączenia urządzeń końcowych sieci (DTE), a szczególnie elementów systemu utrzymania i zarządzania.

Pozostałe kanały to dwa światłowodowe styki V.35 (o szybkości 128 kb/s) i światłowodowe łącze typu Ethernet 10 Mb/s (o maksymalnej przepływności 256 kb/s).

Router Box ZWT KTSAwp może pełnić rolę routera sieci WAN, multipleksera traktu E1 (G.703), konwertera światłowodowego i przełącznika (switch'a) 1Gbit Ethernet.

3.3.4. Środki i urządzenia przetwórcze (abonenckie)

Abonenci sieci teleinformatycznej szczebla taktycznego powinni, za pomocą swoich urządzeń przetwórczych, korzystać z takich usług, jak:

- telekonferencja (dawniej tzw. połączenie okólnikowe);
- priorytetowe zestawianie połączeń;
- przeniesienie numeru (abonenta) w inny punkt sieci;
- przeniesienie połączenia na inny numer (do innego abonenta);
- przekazanie informacji do nieobecnego abonenta (tzw. poczta głosowa, usługa dostępna tylko w niektórych typach urządzeń);
- automatyczne przełączanie połączenia na inny aparat („numer"), w przypadku gdy wywoływany abonent się nie zgłasza;
- tworzenie zamkniętych grup abonentów (dostępność numerów w sieci);
- skrócenie wybierania numerów abonentów i wielu innych.

Rezultaty badań przeprowadzonych przez zespół autorski wskazują, że wprowadzanie zautomatyzowanych systemów dowodzenia wymusza wyposażanie osób funkcyjnych stanowisk dowodzenia w informatyczne urządzenia przetwórcze.

Typowymi informatycznymi urządzeniami przetwórczymi są komputery, które powinny umożliwić:

- sprawne działanie zaimplementowanego oprogramowania (kalkulacje czasowo-przestrzenne, priorytetowanie informacji, przetwarzanie i zobrazowanie danych o wojskach własnych i przeciwniku, symulacje wariantów działania i skutków ich wdrożenia, obsługiwanie procesów komunikacyjnych);
- ciągłe śledzenie i zobrazowanie bieżących informacji od przełożonego, podwładnych i sąsiadów;
- gromadzenie dużych zbiorów informacji i łatwy do nich dostęp osób upoważnionych;
- szybkie wykorzystanie i przetwarzanie informacji;
- bezpieczeństwo informacji;
- niezawodność pracy w niesprzyjających warunkach otoczenia;
- szybki dostęp stanowiska pracy do sieci telekomunikacyjnej pasa działań bojowych lub innego stanowiska pracy.

Do grupy urządzeń przetwórczych zalicza się takie, które wymagają dołączenia do sieci telekomunikacyjnej poprzez linię kablową (przewodową lub światłowodową).

Typowym urządzeniem przetwórczym jest aparat telefoniczny. Współczesne polowe aparaty telefoniczne to:

- aparaty telefoniczne analogowe, umożliwiające współpracę z urządzeniami komutacyjnymi (praktycznie dowolnego typu), zapewniające wymianę informacji fonicznej jawnej;
- aparaty telefoniczne cyfrowe, umożliwiające współpracę z urządzeniami komutacyjnymi, zapewniające wymianę informacji fonicznej jawnej lub utajnionej;
- tzw. cyfrowe punkty abonenckie, umożliwiające współpracę z urządzeniami komutacyjnymi, zapewniające wymianę informacji fonicznej jawnej lub utajnionej, umożliwiające korzystanie z wielu dodatkowych funkcji oferowanych przez urządzenia komutacyjne.

Do grupy urządzeń przetwórczych zalicza się także cyfrowe aparaty telefoniczne (CAT) oraz aparaty cyfrowe (AC-16), manipulatory jako cyfrowe punkty abonenckie CPA oraz modemy komunikacyjne (MK) przeznaczone do pracy w kanale cyfrowym o przepływności 16 kbit/s dla MK-16 i 64 kbit/s dla MK-64.

W badaniach uwzględniono urządzenia przetwórcze (abonenckie), takie jak:

- aparaty telefoniczne analogowe i cyfrowe typu ATS;
- zintegrowane aparaty cyfrowe (AC) z indywidualnym utajnianiem dla pracy fonicznej i transmisji danych (TD);

- moduły MK-16A dla terminali komputerowych;
- terminale CAT i CPA;
- cyfrowy terminal abonencki ISDN – TAI-S.

Poniżej przedstawiono charakterystykę wybranych urządzeń przetwórczych, podano ich podstawowe parametry oraz określono zakres zastosowania.

Aparat telefoniczny stacjonarny **ATS-1** jest analogowym urządzeniem przetwórczym przeznaczonym do stosowania w stacjonarnych miejscach pracy osób funkcyjnych. Jest przystosowany do współpracy z urządzeniami komutacyjnymi o napięciu zasilania od 24 V do 60 V przez jedno- lub dwutorową linię kablową o rezystancji pętli do 1 Ω.

Oprócz realizacji standardowych funkcji aparatu telefonicznego ATS-1 cechuje się dodatkowymi specyficznymi właściwościami, takimi jak:

- elektrohermetyczna obudowa, zapewniająca spełnienie wymagań ochrony przed przenikaniem informacji na zewnątrz;
- układy elektroniczne nie zawierające elementów indukcyjnych;
- możliwość pracy w jedno- lub w dwutorze;
- blokada uniemożliwiająca korzystanie z aparatu osobom nieuprawnionym.

Aparat ATS-2 jest wzbogacony o wiele funkcji dodatkowych, niemających jednak bezpośredniego wpływu na parametry czy bezpieczeństwo pracy w porównaniu z aparatem ATS-1.

Aparat cyfrowy AC-16 umożliwia współpracę z urządzeniami komutacyjnymi poprzez pojedynczą parę przewodów metodą adaptacyjnego tłumienia echa na odległość do 11 km oraz cyfryzację mowy z szybkością 16 lub 32 kbit/s. Opracowano także wersję aparatu z wbudowanym urządzeniem utajniającym. Aparat można podłączyć do komputera poprzez złącze typu RS-232C. Możliwa jest współpraca asynchroniczna z szybkością 9,6 i 19,2 kbit/s lub synchroniczna z szybkością 16 i 32 kbit/s. Zastosowane udogodnienia obejmują również współpracę z telefaksem, identyfikację abonenta, korzystanie z 36 klawiszy programowanych do bezpośredniego wybierania abonentów lub konferencji oraz wybieranie w trakcie rozmowy dodatkowego abonenta, przekształcanie rozmowy w konferencję lub przekazanie połączenia.

Modem komunikacyjny MK-16 (MK-32) umożliwia dupleksową transmisję danych na odległość do 6 km z wykorzystaniem linii kablowych. Posiada on interfejs typu RS-232C umożliwiający transmisję asynchroniczną 9,6 kbit/s lub synchroniczną 16 kbit/s (dla MK-16) lub 32 kbit/s (dla MK-32).

Terminale abonenckie typu **CAT** (cyfrowy aparat telefoniczny) i **CPA** (cyfrowy punkt abonencki) są aparatami telefonicznymi przeznaczonymi do prowadzenia rozmów fo-

nicznych i transmisji danych w systemie łączności utajnionej. Spełniają one wymagania kompatybilności elektromagnetycznej i występują w wersji polowej i stacjonarnej, a mianowicie:

- CAT-UP – do zastosowania w warunkach polowych (UP – urządzenie przenośne);
- CAT-US – do zastosowania w warunkach stacjonarnych (US – urządzenie stacjonarne).

Cyfrowy punkt abonencki występuje w wersji z utajnianiem pod nazwą CPA-U. Podstawowe parametry tych urządzeń to: modulacja delta, przepływność – 16 kbit/s, transmisja danych – 9600 bit/s, linia abonencka – dwuprzewodowa, zasięg łączności - 6 km, zasilanie - z linii abonenckiej, technologia – montaż powierzchniowy.

Cyfrowy terminal abonencki ISDN – TAI-S jest przeznaczony do realizacji rozmów telefonicznych oraz utajnionej transmisji danych o klauzuli do TAJNE. Zapewnia współpracę z urządzeniami komutacyjnymi ISDN.

Rugedyzowane stanowisko komputerowe jest obudową RSK-1 dającą ochronę środowiskową i ekranowanie elektromagnetyczne dla umieszczonych wewnątrz standardowych komputerów notebook w obudowach plastikowych. W obudowie umieszczono zewnętrzny, odporny środowiskowo monitor RMK-1 oraz szczelną, odporną na uszkodzenia klawiaturę z myszą. Szczelna obudowa tego monitora wykonana jest z jednego bloku aluminiowego i służy również jako radiator do układów scalonych znajdujących się wewnątrz. Wszystkie złącza i ekranowane kable przyłączeniowe monitora są wykonane zgodnie z standardami wojskowymi. Jako komputery stacji roboczych można stosować standardowe plastikowe komputery notebook pracujące w zamkniętych, stalowych obudowach RSK-1, chroniących je przed wpływami otoczenia i zapobiegające emisji ujawniającej. Zewnętrzne ekranowane monitory mają dużą jasność, większą niż ekrany komputerów notebook. Monitor oraz klawiatura są przenoszone w stalowym pudełku ochraniającym. Wszystkie złącza komputera notebook są wyprowadzone na tylną ściankę obudowy RSK-1 i poprzez złącza wojskowe (RJ-45, USB) umożliwiając dołączenie do niego dodatkowych urządzeń zewnętrznych.

Notebook rugedyzowany ROCKY III przeznaczony jest do pracy w trudnych warunkach terenowych. Posiada obudowę ze stopu magnezowo-aluminiowego zapewniającą podwyższoną wytrzymałość mechaniczną i klimatyczną.

Terminal rugedyzowany PANTHER jest przenośnym terminalem przeznaczonym do zastosowań w pojazdach, wozach bojowych, wozach dowodzenia i dowódczo-sztabowych. Może być wykorzystywany zarówno do pracy w warunkach mobilnych, jak i dzięki niewiel-

kim wymiarom jako urządzenie przenośne. Ma obudowę ze stopu magnezowo-aluminiowego zapewniającą podwyższoną wytrzymałość mechaniczną i klimatyczną.

Rugedyzowany komputer osobisty PDA jest przenośnym komputerem osobistym, charakteryzuje się niewielkimi wymiarami oraz małą wagą. Obudowa ze stopu magnezowo-aluminiowego zapewnia podwyższoną wytrzymałość mechaniczną i klimatyczną.

Komputer typu SPARTAKUS jest urządzeniem przetwórczym, przeznaczonym do pracy w transporterach kołowych i gąsienicowych, wozach dowodzenia i wozach dowódczo-sztabowych. Dzięki zastosowaniu innowacyjnej technologii oraz przemyślanej konstrukcji umożliwia instalację dodatkowych interfejsów, kart i innych urządzeń. Posiada obudowę ze stopu magnezowo-aluminiowego zapewniającą podwyższoną wytrzymałość mechaniczną i klimatyczną.

WNIOSKI

Z przeprowadzonych badań wynika, że jednym z najważniejszych elementów infrastruktury teleinformatycznej (systemu łączności) wojsk lądowych jest podsystem wymiany informacji. Zazwyczaj tworzą go cztery odmienne elementy do których należą: sieci telekomunikacyjne, sieci komputerowe, sieci pocztowe, oraz sieci sygnalizacyjne.

Pierwszy z wymienionych elementów systemu łączności - sieci telekomunikacyjne - mogą być z powodzeniem wykorzystywane w kierowaniu reagowaniem kryzysowym. Sieci te to przede wszystkim: sieć radiowa KF i UKF, sieć radioliniowo-kablowa, sieć kablowa oraz sieć radiodostępu. Należy zauważyć, że wraz ze wzrostem mobilności danego środka maleje jego zdolność transmisyjna (pasmo transmisyjne). Dla mobilnego środka jakim jest radiostacja rodziny PR4G praktyczna przepustowość dla transmisji danych wynosi tylko 2400 b/s. W przypadku radiolinii R450 systemu „Storczyk" przepustowość ta wynosi 8 Mb/s.

Współpraca wojsk lądowych z terenowymi organami administracji publicznej w ramach kierowania reagowaniem kryzysowym przy wykorzystaniu wojskowych sieci telekomunikacyjnych jest możliwa wtedy, gdy organa administracji publicznej zostaną w te środki wyposażone.

Przeprowadzone badania wykazały, że coraz większego znaczenia w procesie dowodzenia (kierowania) nabierają możliwości transmisyjne sieci komputerowych. Sieci te służą one do wymiany informacji pomiędzy osobami funkcyjnymi i zespołami funkcjonalnymi wyposażonymi w komputery (lub inne urządzenia np. telefony IP) poprzez użycie medium

transmisyjnego jakim jest kabel, światłowód, fale radiowe itp. Umożliwiają dostęp do odpowiednich baz danych a także dostęp do współdzielonych zasobów sieciowych takich jak: drukarki, plotery urządzenia pamięci masowych. Wyróżniane są lokalne sieci komputerowe rozwijane zazwyczaj na stanowiskach dowodzenia (*ang. LAN – local area network*)) i rozległe sieci komputerowe (*ang. WAN – wide area network*) zapewniające transmisje danych pomiędzy poszczególnymi sieciami lokalnymi.

Sieci komputerowe wykorzystywane w wojskach lądowych są tworzone na bazie technologii cywilnych (komercyjnych), a tym samym są one w pełni kompatybilne z sieciami komputerowymi wykorzystywanymi przez administrację publiczną i inne organizacje użytku publicznego. Z tego też względu ich wykorzystanie w kierowaniu reagowaniem kryzysowym wydaje się najbardziej zasadne.

Innym aspektem rozpatrywanym w trakcie badań był dostęp, wszystkich organów biorących udział w kierowaniu reagowaniem kryzysowym, do informacji. Analizy wykazały, że informacja ta powinna być:

- dostępna;
- wiarygodna;
- bezpieczna;
- spójna;
- trwała ;
- aktualna.

Niektóre z powyższych cech informacji mogą być zapewnione poprzez odpowiednią strukturę organizacyjno funkcjonalną organów kierowania. Inne tylko poprzez zastosowanie odpowiednich narzędzi (systemów) teleinformatycznych. Aktualnie jedynym systemem mogącym spełnić przedstawione powyżej cechy jest zautomatyzowany system dowodzenia „Szafran". Z tego też względu zasadnym byłoby wyposażenie wszystkich organów decyzyjnych procesu kierowania reagowaniem kryzysowym w ten system. Transmisja danych pomiędzy stanowiskami dowodzenia (kierowania) powinna odbywać się w głównej mierze poprzez stacjonarne sieci komputerowe zarówno cywilne, komercyjne, resortowe jak i rozwijane na bazie węzłów łączności stanowisk dowodzenia i sieci radioliniowo-kablowej wojsk lądowych.

4. CYWILNE I RESORTOWE SYSTEMY TELEINFORMATYCZNE WYKORZYSTYWANE W REAGOWANIU KRYZYSOWYM

Analiza literatury i obserwacje przeprowadzone w trakcie wielu ćwiczeń związanych z reagowaniem kryzysowym, pozwoliły zespołowi autorskiemu na przyjęcie trzech podstawowych kryteriów oceny systemów teleinformatycznych wykorzystywanych do transmisji danych i mowy. Kryteria te to odpowiednio: mobilność systemu, zakres (usługi) systemu i zasięgu systemu. W trakcie badań poddano ocenie następujące systemy:

- systemy telefonii bezprzewodowej (a szczególnie systemy DECT);
- systemy telefonii komórkowej GSM i UMTS;
- systemy trankingowe;
- systemy satelitarne;
- sieci radiowe ViMAX;
- systemy dyspozytorskie.

4.1. Systemy telefonii bezprzewodowej

Telefonia bezprzewodowa umożliwia łączność z przenośnego aparatu telefonicznego ze stacją bazową, w celu połączenia się z zarówno z siecią użytku publicznego **PSTN** (*ang.* – *Public Switched Telephony Network)* jak i z dowolną centralą abonencką[1]. Standard **DECT** (*ang. Digital Enhanced Cordless Telephony*) został opracowany przez „Europejski Instytut Norm Telekomunikacyjnych". Według przyjętych założeń system został przystosowany zarówno do transmisji mowy jak i danych. W wersji podstawowej wykorzystywanych jest 10 kanałów radiowych w zakresie częstotliwości 1880 do 1900 MHz. Europejski Instytut Norm Telekomunikacyjnych przewidział także możliwość użytkowania kolejnych 23 kanałów. Poprzez zwielokrotnienie czasowe TDMA w jednym kanale może być jednocześnie transmitowanych aż do 12 niezależnych rozmów telefonicznych. Sygnały w obu kierunkach przesyłane są na przemian tym samym kanałem.

[1] Patrz P. Daniluk, Możliwości wykorzystania systemów radiokomunikacyjnych w sytuacja kryzysowych, Materiały z konferencji „Łączność w sytuacjach o charakterze niemilitarnym na obszarze kraju, Warszawa, AON 2004.

16

Standard DECT to wynik współpracy krajów europejskich, a jego główne zasady funkcjonowania podobne są do zasad wykorzystywanych w telefonii komórkowej, a mianowicie[2]:

- struktura systemu składa się z mikrokomórek o zasięgu działania do kilkuset metrów;
- jedna lub wiele stacji bazowych są połączone z centrum sterowania, które z kolei jest dołączone do dowolnej stacjonarnej sieci telefonicznej;
- zadaniem systemów opartych o DECT jest przede wszystkim obsługa obszarów o dużej gęstości zaludnienia;
- istnieje możliwość tworzenia jedno i wielokomórkowych sieci z usługami przełączaniem rozmów pomiędzy stacjami bazowymi w trakcie realizacji połączenia;
- stosowanie identyfikacji użytkowników oraz utajniania przesyłanego sygnału;
- funkcjonowanie styku umożliwiającego współpracę z innymi systemami telekomunikacyjnymi. Umożliwia to dogodne podłączenie abonentów systemu DECT do telefonicznej publicznej sieci stałej, pakietowej sieci X.25 oraz realizowanie dostępu do usług ISDN;
- możliwość integracji systemów opartych na DECT z systemem cyfrowej telefonii komórkowej GSM oraz UMTS;
- możliwość pracy w systemie hybrydowy, w którym niektóre stacje bazowe GSM byłyby zastąpione przez stacje bazowe DECT.

4.2. System telefonii komórkowej GSM i UMTS

U podstaw tworzenia **systemu GSM**[3] (*ang. Global System of Mobile Communication*) stanęło wiele różnorodnych założeń. Istotnymi założeniami z punktu widzenia kierowania reagowaniem kryzysowym to[4]:

- standard jednolity dla całej Unii Europejskiej;
- system całkowicie oparty na technologiach cyfrowych;
- system o ograniczonych możliwościach transmisji danych;
- system z dwoma podsystemami - 900 MHz i 1800 MHz;
- hierarchiczna struktura przestrzenna umożliwiająca śledzenie położenia terminali ruchomych.

---

[2] Tamże.
[3] Porównaj www.wikipedia.pl.
[4] Patrz P. Daniluk, Możliwości wykorzystania systemów radiokomunikacyjnych w sytuacja kryzysowych.

Podczas tworzenia standardu GSM opierano się głównie na doświadczeniach związanych z rozwojem standardu ISDN. Z tego względu istnieje wiele podobieństw pomiędzy tymi sieciami, a mianowicie:

- w strukturze obu sieci znajdują się centrale telefoniczne, które wykorzystują te same łącze do przenoszenia różnych typów informacji (np. głosu, danych) pomiędzy abonentami sieci. Kontrola połączeń wykonywana jest za pomocą protokołu sygnalizacyjnego SS7;
- głos o częstotliwości od 300 do 3400 Hz kodowany jest cyfrowo i w takiej postaci jest transmitowany w sieci;
- zdefiniowane zostały usługi zintegrowane z siecią. Należą do nich między innymi: przesyłanie faksu, krótkich wiadomości tekstowych SMS, poczty głosowej, identyfikacji numeru dzwoniącego itp.

Podstawowym założeniem podczas projektowania standardu GSM była pełna mobilność abonenta, co wymagało uwzględnienia:

- dodatkowych elementów infrastruktury sieci odpowiedzialnych za przechowywanie informacji o aktualnym położeniu abonenta, śledzenie zmian jego położenia i utrzymywanie odpowiedniej jakości transmisji;
- roamingu, czyli możliwość korzystania z innych sieci GSM;
- połączenia telefonu z siecią poprzez system stacji bazowych. Transmisja odbywa się na wielu częstotliwościach, z których każda jest podzielona na 8 tzw. szczelin czasowych.

Aktualnie wykorzystywanych jest aż pięć standardów GSM, różniących się przede wszystkim używanym pasmem radiowym i rozmiarami komórki. Są to odpowiednio: GSM 400, GSM 850, GSM 900, GSM-1800 i GSM 1900. W Europie a tym samym w Polsce używany jest standard GSM 900/1800.

System GSM może świadczyć następujące usługi:

- transmisja mowy;
- transmisja danych;
- przesyłanie wiadomości SMS i MMS;
- dostęp do cieci INTERNET.

System UMTS[5] (*ang. – Universal Mobile Telecommunication System*) jest systemem telefonii komórkowej trzeciej generacji. Zapewnia on zintegrowaną łączność szerokopasmowa abonentom ruchomym.

---

[5] Porównaj www.wikipedia.pl.

M8

Wśród najważniejszych założeń, które były przyjęte podczas jego opracowania, należy wymienić[6]:

- możliwość funkcjonowanie w różnych środowiskach technologicznych – pikokokomórki, makrokomórki i komórki satelitarne;
- transmisja danych typu dupleks realizowana z podziałem czasowym / kodowym / częstotliwościowym;
- szeroka współpraca z systemami stacjonarnymi PSTN.

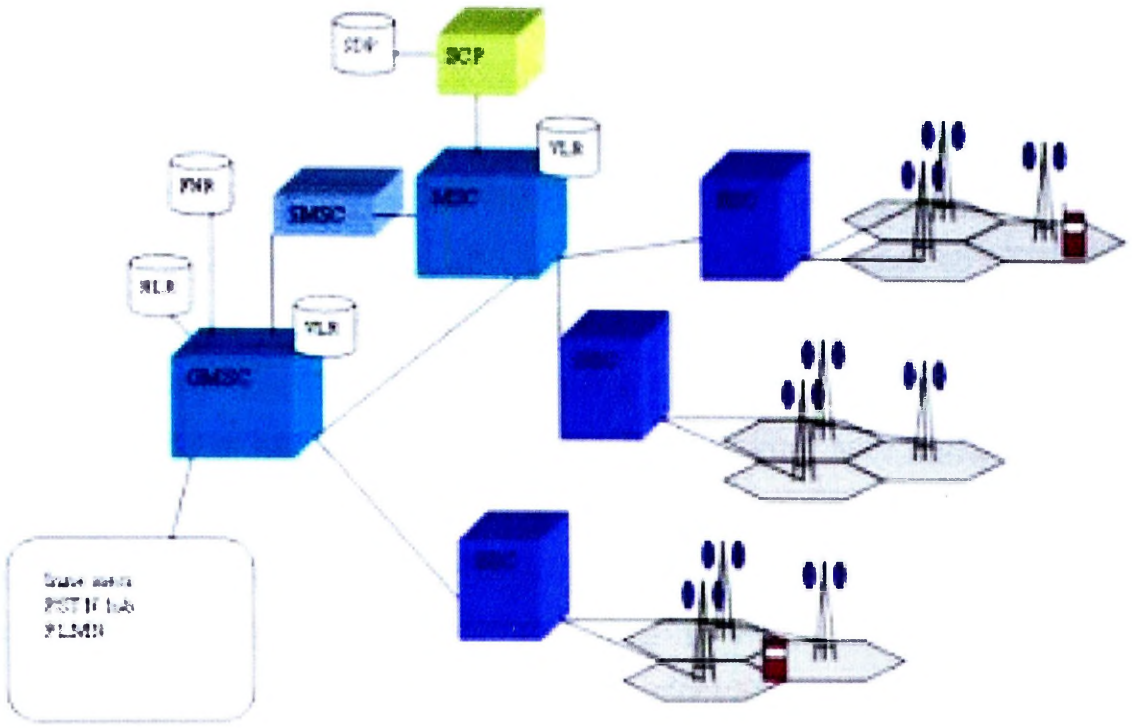
Czterema podstawowymi filarami tego systemu są powszechnie znane hasła:

- transmisja 2 Mbit/s dla każdego użytkownika;
- wszędzie i zawsze w sieci;
- jeden numer dla jednego abonenta, jedne abonent z jednym numerem;
- wykorzystanie pasma powyżej 300 MHz.

Powyżej przedstawione filary systemy pozwoliły na przyjęcie następujących koncepcji projektowych i wdrożeniowych systemu UMTS[7]:

1. transmisję danych określono jako najważniejszą usługę a jej przepływność zależy od kilku uwarunkowań (odległościowych, sprzętowych), a mianowicie:
   - do 2 Mbit/s dla pikokomórek (obszar firmy, biura, centra handlowego lub komunikacyjnego) - zasięg do kilkuset metrów dla terminali stałych lub ruchomych przemieszczanych z prędkością kilku km/h,
   - do 384 kbit/s dla mikrokomórek (obszar zabudowany, zasięg 1-2 kilometrów) przy wykorzystaniu terminali poruszających się z prędkością do 100 - 120 km/h,
   - do 144 kbit/s dla makrokomórek (obszary największych komórek GSM o promieniu do 20 kiloemtrów) dla terminali poruszających się z prędkością do 500 km/h;
2. w obszarze rodzaju usług realizowanych w sieci:
   - transmisja danych,
   - szeroki dostęp do internetu,
   - komutacja kanałów i pakietów,
   - możliwość lokalizacji abonenta.

[6] Patrz P. Daniluk, Możliwości wykorzystania systemów radiokomunikacyjnych w sytuacja kryzysowych.
[7] Tamże.



Rys. 4.1. Architektura sieci GSM
Źródło: http://www.gsmcenter.pl

4.3. Łączność trankingowa

Obecnie funkcjonujące w różnego rodzaju służbach systemy to zazwyczaj analogowe systemy dyspozytorskie, posiadające na stałe przydzielone kanały radiowe. Brak odpowiedniego zarządzania kanałami częstotliwościowymi doprowadza do sytuacji, że pewne kanały są aktualnie zajęte dla usiłujących z nich korzystać użytkowników, pomimo tego że inne przydzielone innym użytkownikom kanały nie są wykorzystywane[8]. Z tego też względu jednym z wielu typów systemów radiokomunikacji ruchomej zdobywających coraz większą popularność ze względów praktycznych są systemy trankingowe, pozwalające zracjonalizować zarządzanie udostępnionymi zasobami radiowymi, co w konsekwencji umożliwia wykorzystanie szerszej gamy usług z prywatnością rozmów włącznie.

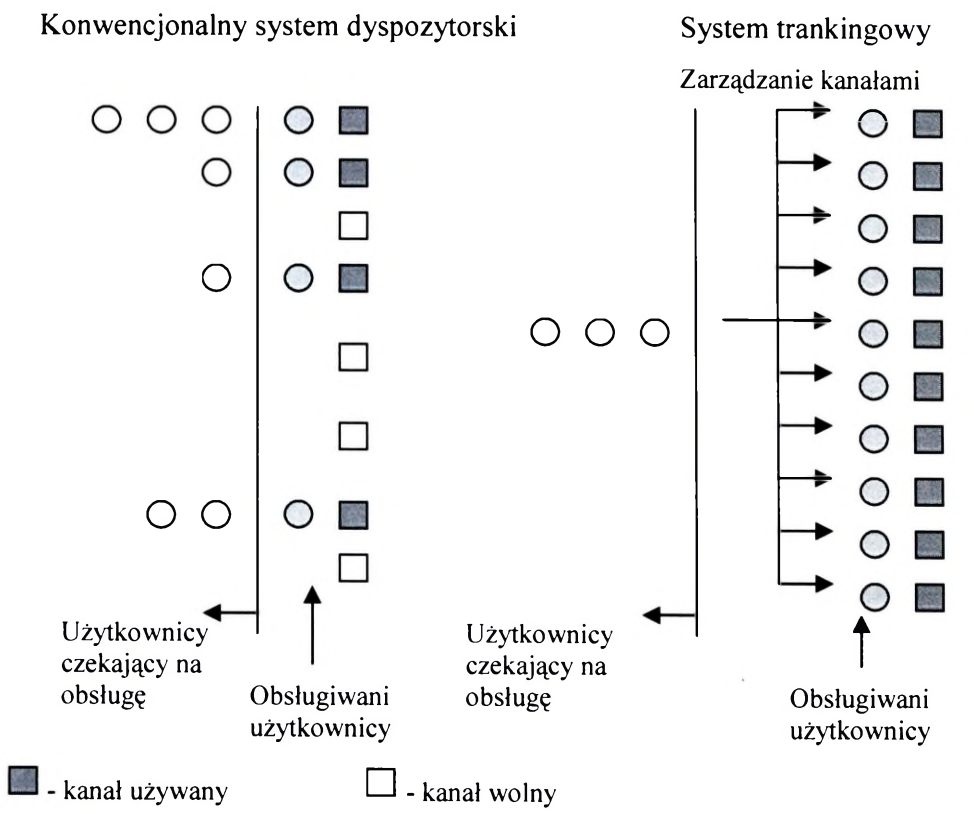
Systemy trankingowe funkcjonują w świecie od początku lat 80. Większość z nich stanowią systemy analogowej transmisji sygnałów mowy, z dość ograniczoną możliwością transmisji danych.[9]

Początki systemów trankingowych sięgają do wczesnych systemów dyspozytorskich, które ewoluowały od systemów posiadających tylko jedną stacją bazową. Systemy te posiada-

[8] K. Wesołowski, Systemy radiokomunikacji ruchomej, Warszawa, WKŁ 2003, str. 308.
[9] D. Rutkowski, System trankingowy TETRA, Przegląd telekomunikacyjny nr 5/2000.

ły przydzielony wspólny jeden kanał, dzięki któremu stacje ruchome słyszały się nawzajem. Następnymi systemami były złożone systemy analogowe, które ewaluowały do w pełni cyfrowego systemu o standardzie zachodnioeuropejskim TETRA, umożliwiającego transmitować jednocześnie głos, jak też dane. Po gwałtownym rozwoju radiowych systemów trankingowych w latach osiemdziesiątych stały się one wówczas alternatywą dla powszechnie stosowanych systemów dyspozytorskich, dając dużo większe możliwości funkcjonalne ich użytkownikom.

Przyjęte rozwiązanie trankingu umożliwia przydział kanału na żądanie użytkownika, z puli wolnych kanałów, będącej w dyspozycji systemu i zwrotu kanałów po zakończeniu jego użytkowania. Jest to koncepcja, stanowiąca podstawę funkcjonowania systemów komórkowych i sieci telefonicznych. System ten oparty jest na prawdopodobieństwie, że ustalona niewielka liczba kanałów może być użytkowana przez znacznie większą liczbę użytkowników, jeżeli ich żądania przydziału kanałów napływają przypadkowo i w czasie niezależnym od siebie. Prawdopodobieństwo, iż każdy użytkownik będzie żądał przydziału kanału w tym samym momencie jest bardzo małe. W związku z tym natężenie żądań przydziału kanału w systemie trankingowym może się zmieniać w dłuższym przedziale czasu, a szansa uzyskania połączenia jest zmienna. Ideę trankingu można obrazowo przedstawić na rysunku 4.2 porównując go z konwencjonalnym systemem dyspozytorskim.



Rys. 4.2. Zasada porządkowana kanałów w konwencjonalnym systemie dyspozytorskim oraz w systemie trankingowym.
Źródło: System radiokomunikacji ruchomej, Warszawa 2003, str. 309.

Przedstawiony rysunek wyraźnie obrazuje równowagę w liczbie użytkowników i liczbie kanałów obsługiwanych aktualnie przez system trankingowy. Liczba osób czekających na połączenie jest też znacznie niższa niż w systemie dyspozytorskim. Na uwagę zasługuję fakt, iż w systemie trankingowym poszczególne kanały nie są przyporządkowane konkretnemu użytkownikowi, z tego względu zwiększona zostaje pojemność oraz niezawodność systemu. Natomiast w chwili, gdy wszystkie kanały zostaną zajęte, niezrealizowane połączenia zostają automatycznie ustawiane w kolejkę. Można oczywiście ograniczyć długość połączenia, dzięki czemu przyporządkowanie kanałów następować będzie szybciej.

Dla operatora i pośrednio również dla użytkowników ważna jest jakość rozwiązań stosowanych w systemie, która decyduje o kosztach budowy i kosztach świadczonych usług.

Cechą charakterystyczną tradycyjnych systemów trankingowych i dyspozytorskich jest stosowanie, w stacjach ruchomych, trybu duosimpleksowego. W trakcie rozmowy parze abonentów systemu przydzielona jest para kanałów częstotliwościowych – „w górę" oraz „w dół". Istnieje również możliwość korzystania z jednego z przydzielonych kanałów, tzn. abonent może albo mówić albo słuchać. Stacja bazowa odbiera sygnał od abonenta nadającego na jednym kanale, a do użytkownika słuchającego nadaje na drugim kanale. Dzięki temu sposobowi korzystania z zasobów radiowych jest możliwe realizowanie połączeń grupowych bez konieczności wybierania numeru indywidualnych członków grupy.[10]

Klasyczny system dyspozytorski najczęściej składał się ze stacji bazowej oraz określonej liczby stacji ruchomych. Rozmowy realizowane były w otwartym kanale, więc użytkownik systemu mógł stwierdzić, które kanały nie są obecnie wykorzystywane i samodzielnie decydował o wyborze wolnego kanału. W przypadku wystąpienia konfliktu między terminalami o pierwszeństwie realizacji połączenia decydował dyspozytor.

Podstawową zaletą systemu trankingowego jest jego pojemność przy ustalonej liczbie kanałów. Można zredukować liczbę kanałów wymaganych do obsługi grupy użytkowników oraz obniżyć koszty połączenia, co pozwala na ekonomiczne i efektywne wykorzystanie widma częstotliwości. Elastyczność i łatwa konfiguracja systemu umożliwia w przypadku powiększenia się liczby użytkowników dowolną rozbudowę bez ponoszenia dużych kosztów. Wysoka niezawodność, to kolejna zaleta systemu trankingowego, ponieważ awaria jednego kanału nie powoduje blokady połączeń innych użytkowników, a jedynie spadek jakości oferowanych usług. Dużą zaletą trankingu jest również możliwość realizacji połączeń priorytetowych oraz prowadzenie rozmów poufnych, dzięki czemu zajęty wcześniej przez innych

[10] K. Wesołowski, Systemy radiokomunikacji ruchomej, str. 310.

użytkowników kanał nie jest zakłócany, jak również podsłuchiwany przez innych użytkowników sieci. Natomiast pod względem ekonomicznym i technicznym zasadniczą zaletą tego systemu jest możliwość konfiguracji sieci opierając się na strukturze logicznych grup, co umożliwia współużytkowanie takiego systemu przez wiele niezależnych od siebie grup użytkowników.

Stale rosnące wymagania użytkowników sieci radiowych, a w szczególności służb bezpieczeństwa publicznego, spowodowały konieczność opracowania nowoczesnego systemu łączności. Jednocześnie fakt jednoczenia się krajów europejskich spowodował, że powstała potrzeba stworzenia jednolitej płaszczyzny komunikacyjnej dla służb bezpieczeństwa i ratownictwa poszczególnych państw, aby umożliwić efektywną ich współpracę w sytuacjach kryzysowych nie tylko na poziomie krajowym, ale również międzynarodowym.[11] TETRA czyli *ang. Terrestrial Trunked Radio*, to nazwa całego zespołu otwartych standardów – interfejsów i usług, opracowanych przez ETSI – Europejski Instytut Norm Telekomunikacyjnych. TETRA to pierwszy w pełni otwarty, międzynarodowy standard cyfrowej radiokomunikacji ruchomej do zastosowań profesjonalnych.[12]

Właściwe kierunki rozwoju standardu Tetra wyznacza organizacja TETRA MoU (*ang. TETRA Memarandum of Understanding*), powstała w listopadzie 1994 r., która zrzesza ponad 100 organizacji z całego świata. Do firm, które interesują się rozwojem systemu, należą: producenci, operatorzy, użytkownicy sieci, instytucje naukowe, homologacyjne oraz administracje państwowe.[13]

Europejski Instytut Norm Telekomunikacyjnych zaakceptował prace nad zaawansowanym standardem TETRA, co spowodowało, że poszczególni producenci zaczynają wdrażać własne rozwiązania zgodne z tym standardem, jak również na etapie końcowym są prace nad drugą wersją standardu mogącego transmitować dane z większą szybkością. Spowodowane jest to potrzebą opracowania profesjonalnego cyfrowego systemu łączności radiowej dla potrzeb różnego rodzajów służb publicznych i administracji rządowej odpowiedzialnych za bezpieczeństwo.

Systemy cyfrowej łączności trankingowej, które zgodne są ze standardem TETRA, zalecane jest przez Ministerstwa Spraw Wewnętrznych większości krajów europejskich, w szczególności dla takich służb jak:

---

[11] R. Piątek, TETRA – paneuropejski standard cyfrowej łączności trankingowej, Wiadomości Telekomunikacyjne nr 11/1999r, str. 784.
[12] J. Krasoń, TETRA – Otwarty standard cyfrowej łączności rankingowej, Wiadomości Telekomunikacyjne nr 3/2000.
[13] Z. Jóskiewicz, TETRA - System łączności radiowej dla transportu publicznego, Warszawa 2005r.

- policja,
- straż graniczna,
- pogotowie ratunkowe,
- straż pożarna,
- służby bezpieczeństwa.

Możliwość korzystania z tego systemu przewidziana jest również dla innych użytkowników, np: przedsiębiorstw komunalnych, wodociągowych, ciepłowniczych, oraz służb energetycznych.

Głównym zadaniem twórców standardu TETRA było zdefiniowanie systemu, który mógłby być używany, co najmniej w całej Europie. Do realizacji tego zamierzenia konieczne było znalezienie pasma częstotliwości dogodnej dla wszystkich krajów Europy. Po przeprowadzonych badaniach, okazało się, że w Europie w zakresie poniżej 1 GHz nie istnieje pasmo częstotliwości o szerokości 220 MHz, które byłoby powszechnie dostępne. Zaproponowano przydział kilku mniejszych, nieprzylegających do siebie pasm.

- 410 – 439 MHz,
- 450 – 470 MHz,
- 870 – 888 MHz,
- 915 – 933 MHz.

Do realizacji systemów przeznaczonych dla bezpieczeństwa publicznego w całej europie zostało zarezerwowane i udostępnione przez NATO pasmo częstotliwości w zakresie 380 – 400 MHz. W późniejszym okresie przewiduje się wykorzystanie dodatkowego zakresu 410 – 430 MHz dla systemów publicznych.[14]

Pierwszy system zgodny ze standardem TETRA zainstalowany został i uruchomiony przez firmę Motorola w 1996 r. na wyspie Jersey.

Podczas opracowywania standardu TETRA wykorzystano doświadczenia z eksploatacji dotychczasowych, analogowych systemów trankingowej łączności radiowej typu dyspozytorskiego i cyfrowej telefonii komórkowej GSM. Prowadzone prace w tej dziedzinie doprowadziły w rezultacie do stworzenia systemu, który oferuje bardzo bogaty zestaw usług użytecznych w sektorze bezpieczeństwa publicznego. System ten poza usługami podstawowymi, do których zalicza się teleusługi, usługi przenoszenia i usługi krótkich wiadomości, oferuje również szereg usług dodatkowych uzupełniające usługi podstawowe.

---

[14] R. Piątek, TETRA – paneuropejski standard cyfrowej łączności trankingowej, str. 785.

Usługi w standardzie TETRA zostały podzielone na dwie kategorie: teleusługi i usługi przenoszenia.

W ramach teleusług oferowanych jest pięć różnych połączeń głosowych:

- połączenia indywidualne – połączenia punkt-punkt obejmujące dwóch indywidualnymi użytkowników,
- połączenia grupowe – obejmujące połączenia punkt-wiele punktów, gdzie łączność odbywa się pomiędzy wywołującym użytkownikiem a określoną grupą rozróżnianą przez nadany im numer grupowy. Transmisja realizowana jest w trybie półdupleksowym,
- połączenia bezpośrednie – obejmujące połączenia punkt-punkt, między dwoma terminalami ruchomymi. Komunikacja odbywa się bez pośrednictwa stacji bazowej, jednocześnie wymagane jest, aby co najmniej jeden terminal był objęty zasięgiem stacji bazowej na innym kanale od tego, na który jest odbywa się połączenie bezpośrednie,
- połączenie grupowe potwierdzane – polegające na połączenie punkt-wiele punktów, między użytkownikiem i grupą użytkowników rozróżnianą dzięki nadanemu numerowi grupowemu. Potwierdzenie obecności przez użytkownika realizowane jest podczas połączenia,
- połączenie rozsiewcze – komunikacja punkt-wiele punktów, polegająca na tym że wywoływani użytkownicy mogą tylko słuchać użytkownika wywołującego.

Kolejnymi usługami oferowanymi przez standard TETRA, są tak zwane usługi przenoszenia, do których należą[15]:

- cyfrowa transmisja mowy oraz danych bez zabezpieczenia w trybie komutacji kanałów, szybkość transmisji między 7,2 a 28,8 kbit/s,
- transmisja danych z bardzo małym zabezpieczeniem kodowym realizowana w trybie komutacji kanałów, szybkość transmisji między 4.8 a 19,2 kbit/s,
- transmisja danych z bardzo wysokim zabezpieczeniem kodowym realizowana w trybie komutacji kanałów z szybkością między 2,4 a 9,6 kbit/s,
- pakietowa transmisja danych pomiędzy dwoma punktami,
- pakietowa transmisja między dwoma punktami w standardowym formacie (trybie bezpołączeniowym),
- pakietowa transmisja danych z wykorzystaniem trybu bezpołączeniowego realizowana między dwoma punktami lub metodą rozsiewczą.

---

[15] K. Wesołowski, Systemy radiokomunikacji ruchomej, str. 316.

Bardzo przydatną usługą systemu TETRA jest możliwość ustalania priorytetów oraz zawieszenie aktualnych rozmów w celu połączenia z abonentem oczekującym. Połączenia priorytetowe mogą być przerwane na rzecz aktualnie realizowanych. Standard TETRA pozwala również na uzyskiwanie potwierdzenia autentyczności abonenta oraz możliwość dyskretnego podsłuch przez upoważnionego użytkownika systemu. Umożliwia także na identyfikację wywołującego użytkownika, dynamiczne tworzenie grup w zależności od potrzeb, adresowanie za pomocą numerów abonentów, automatyczne lokalizowanie pojazdów i osób, połączenia telefoniczne z abonentami innych sieci, przekazywanie użytkowników pomiędzy sieciami (roaming), rozmowy konferencyjne oraz pocztę głosową.

Szczególnie przydatne z punktu widzenia zarządzania kryzysowego są usługi oferowane w zakresie transmisji danych. Zastosowanie tych usług daje niespotykane do tej pory możliwości efektywnego działania. Użytkownik w zakresie posiadanych uprawnień miałby dostęp do niezbędnych informacji pobieranych z udostępnionych baz danych. Zakres transmitowanych danych mógłby obejmować:

- dostęp do wszelkiego rodzaju baz danych bezpośrednio z radiotelefonu,
- dostęp do map terenu i planów budynków,
- dostęp do zdjęć osób poszukiwanych,
- transmisja wolnozmiennych obrazów z miejsca zdarzenia,
- współpraca z systemami komputerowego wspomagania dowodzenia,
- współpraca z siecią ISDN lub Internetem.

4.4. Systemy satelitarne

Współczesne systemy satelitarne pozwalają na współdziałanie różnorodnych systemów (sieci) teleinformatycznych (telekomunikacyjnych). U podłoża nowoczesnych systemów satelitarnych stanęła koncepcja UPT (*ang.– Universal Personal Telecommunications*) według której łączność satelitarna jest ważnym elementem łączności stacjonarnej.

Do głównych założeń jakie stanowiły o rozwoju systemów satelitarnych należy zaliczyć[16]:

- coraz niższy koszt użytkowania terminali;
- miniaturyzacja urządzeń jak i samych satelitów;
- kompatybilność z innymi systemami – szczególnie stacjonarnymi.

[16] Patrz P. Daniluk, Możliwości wykorzystania systemów radiokomunikacyjnych w sytuacja kryzysowych.

Idea telekomunikacji satelitarnej liczy już prawie pół wieku. W 1959 roku *International Telecommunications Union* przyznała pierwsze zakresy częstotliwości dla transmisji satelitarnej. Rok później na orbicie umieszczono pierwszego satelitę telekomunikacyjnego „Echo 1". Od tego czasu powstało wiele systemów satelitarnych, nowych standardów transmisji satelitarnej, przydzielano nowe częstotliwości.

W każdym systemie satelitarnym można wyróżnić trzy elementy składowe:[17]

- moduł naziemny,
- moduł kosmiczny,
- kanał radiowy.

W skład modułu naziemnego wchodzą:

- terminale abonenckie - ruchome i stacjonarne,
- szkieletowa sieć naziemna ze stacjami bazowymi,
- adaptery sieciowe i stacje kontrolne.

Terminale abonenckie posiadają antenę do nadawania i odbierania danych z satelity oraz urządzenia do przetwarzania sygnałów radiowych wysokiej częstotliwości na odpowiednie sygnały. W systemach komunikacji osobistej S-PCN (*ang. Satellite Personal Communication Network*), w których założono możliwość przemieszczania się abonenta z terminalem, dąży się do minimalizacji terminali abonenckich. Z tego też względu przetwarzanie sygnału przerzuca się na inne elementy sieci.

W nowoczesnych systemach satelitarnych terminalem abonenckim może być również telefon przenośny (modem komputerowy) posiadający możliwość łączenia się z innymi sieciami, takimi jak GSM czy Internet. Zasada pracy terminala abonenckiego polega na przesyłaniu danych do najbliższego, w danym momencie, satelity. Satelita przesyła dane dalej poprzez następne satelity lub do odpowiadającej mu naziemnej stacji bazowej. Jeżeli adresatem wiadomości (połączenia) jest abonent znajdujący się w sieci naziemnej stacja bazowa przesyła tą wiadomość dalej do punktu będącego połączeniem z naziemną siecią telekomunikacyjną. Punkt taki zwany jest adapterem sieciowym (*ang. gateway*). Od niego wiadomość przesyłana jest już według zasad obowiązujących w sieci naziemnej. W przypadku, gdy wiadomość ma być przesłana do innego posiadacza terminala abonenckiego sieci satelitarnej, wędruje ona przez naziemną sieć szkieletową do stacji bazowej najbliższej satelity, który z kolei będzie w stanie przetransmitować ją do owego terminala abonenckiego.

---

[17] www.kt.agh.edu.pl

Moduł kosmiczny systemu satelitarnego składa się z określonej liczby satelitów umieszczonych na orbitach okołoziemskich. W większości systemów satelitarnych wszystkie satelity krążą po orbitach tego samego typu tzn. w tej samej odległość od Ziemi i tym samym kącie nachylenia

Satelity klasyfikowane są ze względu na typy orbit. Wyróżniane są typy[18]:

- **LEO** (*ang. Low Earth Orbit*) – są to orbity o wysokości od 500 do 2000 km nad powierzchnią Ziemi. Na wysokości poniżej 500 km atmosfera ziemska jest zbyt gęsta co powodowałoby zbyt duże tarcia w ruchu satelity. Powyżej 2000 km zaczyna się pierwsza ze stref Van Allena w których cząstki o bardzo dużych energiach mogą spowodować uszkodzenie elektronicznych elementów satelity. Mała wysokość lotu satelity oznacza jego dużą prędkość co oznacza, że satelita przez krótki okres czasu pozostaje w zasięgu stacji naziemnej - około 10-30 minut.
- **MEO** (*ang. Medium Earth Orbit*) – są to orbity o wysokość od 8 do 12 tys. km nad powierzchnią Ziemi. Satelita pozostaje nad horyzontem danego punktu kuli ziemskiej przez kilka godzin. Budowa systemu obejmującego cała powierzchnią Ziemi wymaga od 10 do 20 satelitów krążących po kilku różnych orbitach. Czasy transmisji pomiędzy Ziemią a satelitą są większe niż z orbit LEO.
- **HEO** (*ang. Highly Eliptical Orbit*) – to orbity silnie eliptyczne o odległości od Ziemi od ok. 500 km do ok. 50 tys. km. Dzięki eliptycznej orbicie satelita jest widoczny z danego obszaru na kuli ziemskiej, przez pewien czas, jako prawie nieruchomy. Umożliwia to tworzenie systemów o podobnych cechach jak systemy oparte na satelitach geostacjonarnych. Systemy te sprawdzają się dobrze w terenach górskich lub silnie zurbanizowanych. Dla stworzenia systemu regionalnego bazującego na orbitach HEO potrzeba od 2 do 10 satelitów.
- **GEO** (*ang. GEOstationary orbit*) – są to orbity o wysokości od Ziemi równej, w płaszczyźnie równikowej, 35 786 km. Satelita krążący po takiej orbicie ma tą samą prędkość kątową co obracająca się Ziemia, dzięki czemu jest widziany w jednym miejscu. Do stworzenia systemu globalnego – bez obszarów podbiegunowych - wystarczą tylko trzy satelity. Duża odległość od powierzchni Ziemi powoduje jednak duże opóźnienia w transmisji danych i konieczność stosowania dużych mocy sygnałów.

Wraz z rozwojem telekomunikacji satelitarnej wzrastały także potrzeby na pasmo częstotliwości przydzielone tym systemom. Przyjęto następujący podział[19]:

---

[18] www.wikipedia.pl

- pasmo L - 1-2 GHz,
- pasmo S - 2-4 GHz,
- pasmo C - 4-8 GHz,
- pasmo X - 8-12 GHz,
- pasmo Ku - 12-18 GHz,
- pasmo K - 18-27 GHz,
- pasmo Ka - 27-40 GHz,
- pasmo V - powyżej 40 GHz.

W ostatnim czasie coraz większego znaczenia nabierają satelity nawigacyjne, których głównym zadaniem jest ustalanie pozycji terminali odbierających od nich sygnał oraz podawanie dokładnego czasu. Najpopularniejszym i najstarszym satelitarnym systemem nawigacyjnym, sfinansowany przez Departament Obrony USA, jest system **GPS Navstar (***ang. Global Positioning System NAVigational Satellite Time And Ranging*). Pierwszy satelita tego systemu został wystrzelony w 1978 roku. Pełną funkcjonalność system uzyskał dopiero w 1995 roku. Człon systemu stanowią co najmniej 24 satelity krążące po 6 orbitach. Wysokość orbit wynosi 20200 km nad powierzchnią Ziemi a ich inklinacja jest równa 55°. Każdy satelita okrąża Ziemię dwukrotnie w ciągu doby. Z każdego miejsca na powierzchni Ziemi jest widocznych jednocześnie co najmniej 5 satelitów. Główna stacja kontrolna (*ang. Master Control Station*) znajduje się w Colorado Springs, a 4 stacje monitorujące (*ang. Monitor Stations*) znajdują się odpowiednio na Hawajach, Wyspach Wniebowstąpienia, Kwajalein i Diego Garcii. W skład systemu wchodzi także 6 stacji narodowych NGA (*ang. National Geospatial Agency*), odpowiednio w Argentynie, Bahrajnie, Australii, Ekwadorze, Wielkiej Brytanii i USA. Głównym zadaniem systemu naziemnego jest odbieranie sygnałów od satelitów i obliczanie na tej podstawie poprawek do ich pozycji, które następnie są odsyłane z powrotem do satelitów.

Istnieją dwie wersje systemu Navstar. Pierwszym z nich jest system PPS (*ang. Precise Positioning System*), który jest dostępny tylko dla sił zbrojnych USA i NATO oraz sprzymierzonych. Druga wersja systemu - SPS (*ang. Standard Positioning System*) jest mniej dokładna. Korzystanie z systemu SPS jest bezpłatne i powszechnie wykorzystywane w komercyjnych systemach nawigacyjnych.

Satelity wykorzystują dwa rodzaje sygnałów: C/A na nośnej L1 = 1575.42 MHz (pasmo sygnału - 1.023 MHz) odbierany przez wszystkie urządzenia GPS (SPS i PPS) oraz sy-

---

[19] www.kt.agh.edu.pl

gnał P na nośnej L2 = 1227.60 MHz (pasmo sygnału 10.23 MHz) odbierany tylko przez urządzenia PPS.

Do ustalenia trójwymiarowej pozycji obiektu czasu wystarczą sygnały z czterech satelitów. Odbiornik GPS śledzi co najmniej 5 satelitów. Jest to spowodowane potrzebą zwiększenia dokładności obliczeń oraz na wypadek utraty sygnału od jednego z satelitów. Sygnały zawierają informacje na temat satelity z którego pochodzą i czasu nadania. Przesyłana jest także poprawka aktualnej pozycji satelity obliczona przez naziemne stacje kontrolne. Na podstawie sygnałów odbiornik GPS może obliczyć:[20]

- prawdziwe pozycje satelitów w danym momencie czasu,
- odległości odbiornik-satelita, na podstawie czasu transmisji sygnału od satelity do odbiornika,
- swoją pozycję.

Innym systemem nawigacji satelitarnej jest rosyjski system **GLONASS** (*ros. Globalnaja Nawigacjonnaja Satelitarnaja Sistemma*). Działa on na zasadach podobnych do systemu NAVSTAR. W systemie tym występują także dwa kanały: standardowy i precyzyjny. Kanał standardowy posiada dokładność 60 metrów dla pomiarów dwuwymiarowych i 75 metrów dla trójwymiarowych. Każdy satelita nadaje w swoim paśmie częstotliwości, przez co nie potrzebne jest stosowanie CDMA. Docelowo w systemie miały funkcjonować 24 satelity. Liczba ta nigdy nie została osiągnięta. Rosjanie wystrzeliwali, co prawda, nowe satelity, ale te znajdujące się na orbitach ulegały częstym awariom. W efekcie nigdy nie osiągnięto zamierzonej sprawności i funkcjonalności systemu.

Przedstawione powyżej systemy nawigacji satelitarnej są uzależnione od pojedynczych państw, co nie jest bez znaczenia w przypadku kryzysu i wojny. Dodatkowo systemy te, dla zastosowań komercyjnych, są obarczone dosyć małą precyzją. Z tego też względu Unia Europejska zaproponowała projekt systemu pozbawionego powyższych wad. Cały projekt początkowo nosił nazwę **GNSS**[21] (*ang. Global Navigation Satellite System*). W ramach tego projektu należy wyróżnić dwa odmienne kierunki rozwoju, a mianowicie system **EGNOS** (*ang. European Geostationary Navigation Overlay Service*) i projekt **GALILEO**. EGNOS w głównej mierze wspomaga działanie istniejących już systemów nawigacji satelitarnej. Do odbiorników GPS współpracujących w systemie EGNOS wysyłane są sygnały korekcyjne z satelitów geostacjonarnych znajdujących się nad Europą. Sygnały te zawierają odpowiednie korekty pozycji uzyskiwanych z sieć Navstar, co zwiększa ich dokładność. Głównym zada-

[20] Tamże

niem systemu EGNOS jest weryfikacja danych pochodzących z sieci Navstar pod względem sprawności satelitów lub błędów podczas transmisji. Dane z sieci EGNOS mogą być zastosowane wszędzie tam, gdzie wymagana jest ich duża wiarygodność, a w szczególności tam gdzie niedokładność wskazań aktualnej pozycji mogłaby doprowadzić do katastrofy i utraty zdrowia i życia ludzkiego. System EGNOS opiera się na trzech satelitach geostacjonarnych i naziemnych stacjach pomiarowo-kontrolnych.

Projekt **GALILEO**[22] został zapoczątkowany w 1998 roku. Kontrolę nad nim sprawują Komisja Europejska i Europejska Agencja Kosmiczna. GALILEO ma być cywilnym systemem nawigacji satelitarnej, w pełni niezależnym od wojskowych systemów Navstar i Glonass. Segment kosmiczny ma składać się z 30 satelitów krążących po trzech orbitach na wysokości 23 616 kilometrów i inklinacji 56°. Oprócz danych o pozycji i dokładnym czasie w sygnale przekazywane będą także informacje o wiarygodności tych danych i ewentualnych awariach systemu. Umożliwi to zastosowanie danych z sieci Galileo w sytuacjach kryzysowych, w których ze względu bezpieczeństwa wymagana jest duża precyzja współrzędnych.

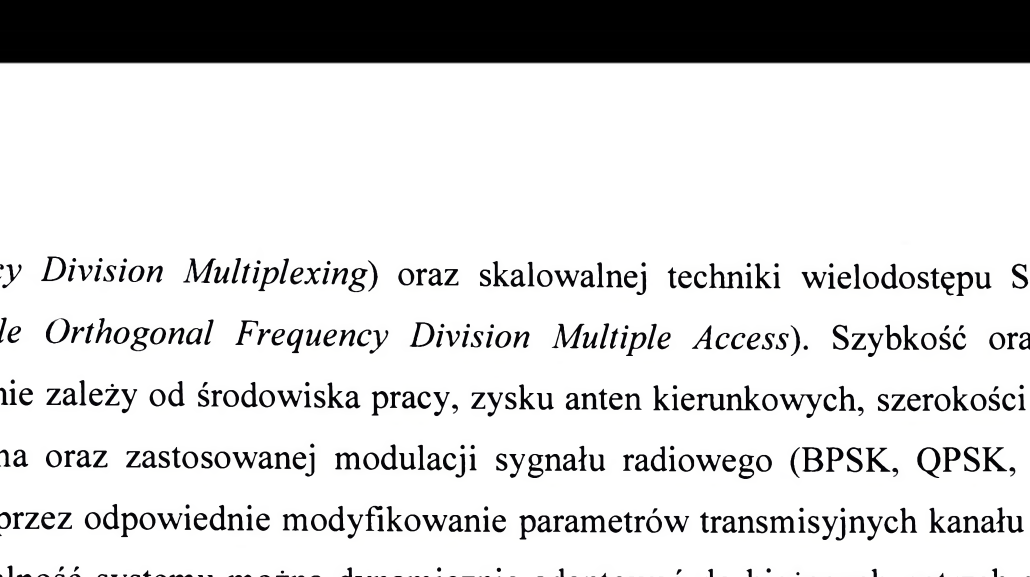
W grudniu 2005 roku został wystrzelony pierwszy testowy satelita Galileo, o nazwie Giove-A. Planowana gotowość systemu ma nastąpić w roku 2012.

4.5. Sieci radiowe WiMAX

Sieć radiowa WiMAX IEEE 802.16 (*ang. World Interoperability for Microwave Access*) stanowi grupę standardów systemu bezprzewodowej szerokopasmowej transmisji danych (802.16, 802.16a, 802.16d). Standard ten stanowi konkurencję dla systemów 2G/3G oraz technologii transmisji danych typu: HSCSD, GPRS, EDGE, UMTS/HSDPA[23]. WiMAX może zapewnić dostęp do sieci szerokopasmowej IP na potrzeby poszczególnych użytkowników przemieszczających się z niewielką prędkością przy zachowaniu autonomicznego trybu pracy stacji bazowej. Obecnie trwają końcowe prace nad standardem 802.16e, który ma stanowić podstawę całkowicie mobilnego systemu WiMAX. Standard ten pozwala na wykorzystanie technologii WiMAX w sieciach stałych oraz komórkowych. Istotną zaletą standardu 802.16e są zaawansowane mechanizmy QoS (*ang. Quality of Service*) w postaci ERTPS (*ang. Extended Real-Time Polling Service*). Implementacja tego typu funkcji pozwala na udostępnienie w systemie WiMAX usług czasu rzeczywistego (VoIP, IP TV, przekaz multimedialny). Cele te osiągane są między innymi poprzez wykorzystanie modulacji OFDM (*ang. Orthogo-*

[21] Tamże.
[22] Tamże.

nal Frequency Division Multiplexing) oraz skalowalnej techniki wielodostępu SOFDMA (*ang. Scalable Orthogonal Frequency Division Multiple Access*). Szybkość oraz zasięg transmisji silnie zależy od środowiska pracy, zysku anten kierunkowych, szerokości udostępnionego pasma oraz zastosowanej modulacji sygnału radiowego (BPSK, QPSK, 16QAM, 64QAM). Poprzez odpowiednie modyfikowanie parametrów transmisyjnych kanału radiowego, funkcjonalność systemu można dynamicznie adaptować do bieżących potrzeb stacjonarnych użytkowników systemu. Teoretycznie zasięg obszaru usługowego stacji bazowej WiMAX wynosi do 50 km. Natomiast prędkość transmisji danych może osiągnąć 74,8 Mbit/s. Sieci radiowe WiMAX mogą działać w zakresie 2-11 GHz oraz 2-66 GHz. WiMAX jest technologią przeznaczoną do budowy bezprzewodowych sieci transmisji danych dla metropolii MAN (*ang. Metropolitan Area Network*). W Polsce na potrzeby systemu WiMAX przeznaczone jest pasmo 200 MHz w zakresie częstotliwości 3,6-3,8 GHz (w innych krajach europejskich wykorzystywane jest pasmo 3,4-3,6 GHz). System WiMAX funkcjonuje już w kilkunastu Polskich dużych miastach[24]. Elementy stacjonarnej infrastruktury systemu WiMAX przedstawia rysunek nr 4.3.



Rys. 4.3. - Elementy stacjonarnej infrastruktury systemu WiMAX
Źródło: www.networld.pl/artykuly/51968.html

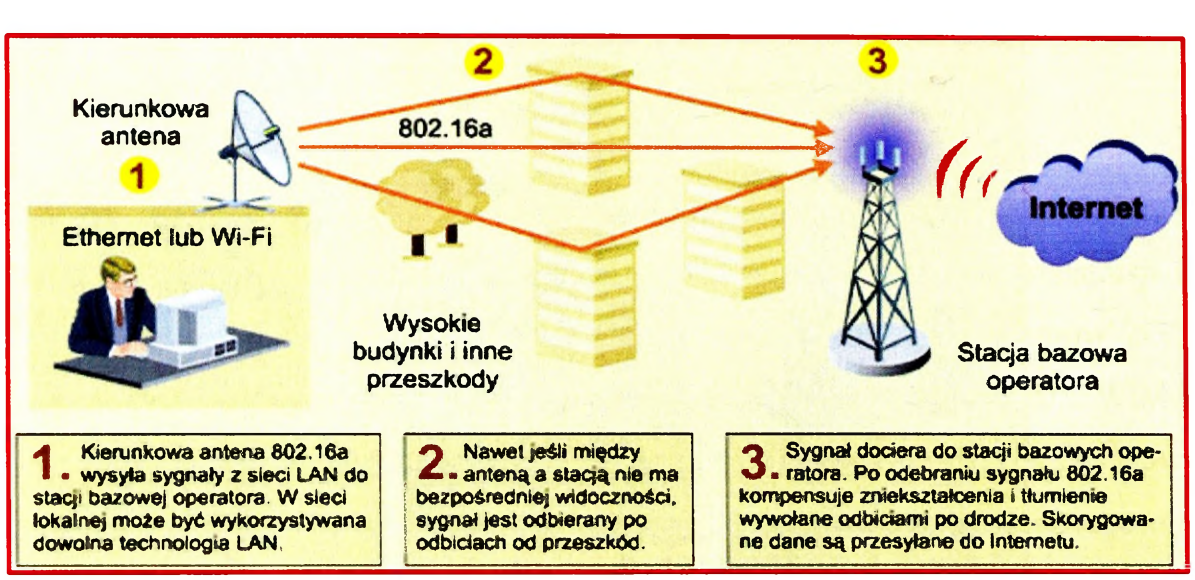
Istotną cechą wszystkich rozwiązań standardu WiMAX jest zapewnienie wydajnej transmisji danych w sieci IP nawet przy braku bezpośredniej widoczności anten. Nawet w przypadku kiedy stacja bazowa systemu WiMAX nie znajduje się w polu widzenia anteny odbiorczej. Dodatkowo sygnał radiowy w sieciach radiowych systemu WiMAX może być

[23] A. Urbanek, „*WiMAX czy HSDPA?*", NetWorld Nr 06/2006, Warszawa, IDG Poland S.A. 2006, s. 1-2.
[24] A. Urbanek, „*WiMAX gotowy do wdrożenia*", NetWorld Nr 09/2005, Warszawa, IDG Poland S.A.2005, s. 1-3.

odbierany po wielokrotnym odbiciu od budynków i innych przeszkód terenowych. Mimo zniekształceń interferencyjnych sygnału radiowego generowanych przez kolejne odbicia, technologia 802.16a pozwala stacji bazowej WiMAX na właściwą interpretację przesyłanych danych. Dodatkowo możliwości systemu zwiększa standard IEEE 802.16e poprzez:

- przekazywanie połączeń między stacjami bazowymi,
- identyfikację i uwierzytelnianie użytkownika podczas poruszania się między stacjami bazowymi,
- szyfrowanie danych algorytmem 3DES,
- wdrożenie hybrydowej retransmisji HARQ (*ang. Hybrid ARQ*) wraz z zastosowaniem zaawansowanych adaptacyjnych anten kierunkowych AAS (*ang. Adaptive Antenna System*);
- wdrożenie technologii MIMO (*ang. Multiple Input Multiple Output*) dla terminali stacjonarnych[25].

Wielodrogowość sygnału radiowego w systemie WiMAX (standard 802.16 a) przedstawia rysunek nr 4.4.



Rys. 4.4. - Wielodrogowość sygnału radiowego w systemie WiMAX
Źródło: www.networld.pl/artykuly/51968.html

Technologia WiMAX może zapewnić wymianę informacji pomiędzy organami reagowania kryzysowego oraz stanowiskami służb bezpieczeństwa publicznego i ratownictwa. Technologia dostępu radiowego WiMAX może tworzyć sieci WMAN oraz integrować sieci i wzajemnie się uzupełniać z sieciami radiowymi WLAN (standard IEEE 802.11). Standard

[25] Tamże, s. 3-4.

WiMAX umożliwia również integrację w sieci WMAN kablowych sieci LAN poprzez interfejs radiodostępu w standardzie IEEE 802.16.

Na przepustowość oraz zasięg sytemu WiMAX wpływa wiele czynników i parametrów. Do parametrów i czynników tych można zaliczyć: sprzęt komunikacyjny o odmiennych parametrach, a także różnych uwarunkowaniach propagacji sygnału radiowego w określonym środowisku, dostęp do odpowiedniej szerokości kanału radiowego 3,5 MHz (kanał simpleksowy) lub 7 MHz (kanał dupleksowy), rodzaj stosowanej modulacji (BPSK, QPSK, 16QAM, 64QAM), wielkość mocy nadawania i czułość odbiornika, kierunkowość oraz sektorowanie współpracujących anten. Przykładowo dla pasma o szerokości 7 MHz użyteczna przepływność może wynosić 3-18 Mbit/s, natomiast maksymalny zasięg 5-30 km. Wyższe przepływności osiąga się w kanałach radiowych w paśmie 7 MHz do 36 Mbit/s (sumaryczna przepływność dupleksowa). W paśmie 14 MHz osiąga się przepływność do 72 Mbit/s. Natomiast przy braku radiowej widoczności anten zasięgi i przepustowość systemu WiMAX są znacznie mniejsze[26]. Przykładowe przepływności i zasięgi systemu WiMAX dla określonych modulacji i pasma 7 MHz przedstawia rysunek nr 4. 5.

Rodzaj modulacji	BPSK	QPSK	16QAM	64QAM
Zasięg stacji bazowej	30 km	25 km	14 km	5 km
Przepustowość radiowa (brutto)	4 Mb/s	8 Mb/s	16 Mb/s	24 Mb/s
Przepustowość efektywna (użyteczna)	3 Mb/s	6 Mb/s	12 Mb/s	18 Mb/s

- zasięg uwzględnia różne typy modulacji
- dla mocy nadawania: TxP = +20 dBm (64QAM) i +26 dBm (QPSK)
- przy czułości odbiornika: - 75 dBm (64QAM) i -91 dBm (BPSK)
- anteny typowe: sektorowa o zysku 14 dBi (po stronie bazowej) oraz panelowa -18 dBi (po stronie odbiorcy)
- dostępność na poziomie 99,95%
- zachowana widoczność radiowa anten
- praca w trybie dupleksowym FDD

BPSK *(Binary Phase Shift Keying)*
QPSK *(Quadrature Phase Shift Keying)*
QAM (Quadrature Amplitude Modulation)

Rys. 4.5. - Przepływności i zasięgi systemu WiMAX dla określonych modulacji i pasma 7 MHz
Źródło: www.networld.pl/artykuly/51968.html

Ze względu na różnorodność i wzajemne zależności parametrów wpływających na pracę systemu WiMAX, można jedynie w dużym przybliżeniu określać zasięgi użyteczne dla określonych środowisk propagacji sygnału radiowego[27]. Przewidywane zasięgi użyteczne

[26] A. Urbanek, „*WiMAX czy HSDPA,* s. 1-2.
[27] A. Urbanek, „*WiMAX gotowy do wdrożenia*", s. 3-4.

systemu WiMAX w różnych środowiskach propagacji sygnału radiowego przestawia tabela nr 4.1.

Tabela nr 4.1.

Przewidywane zasięgi użyteczne systemu WiMAX

Typ środowiska	Zasięg (km)
Brak widoczności anten (metropolia)	2
Brak widoczności anten (teren podmiejski)	2,5
Brak widoczności anten (obszary wiejskie)	4
Bezpośrednia widoczność anten	15

Źródło: www.networld.pl/artykuly/48938.html.

4.6. Systemy dyspozytorskie

Bezpośrednim poprzednikiem przedstawionych wcześniej systemów trankingowych były systemy dyspozytorskie. Pracowały one i do dziś pracują w zakresie ultrakrótkofalowym krótkim dla służb morskich, MSZ, MSWiA oraz MON.

Celem takich systemów jest zapewnienie łączności dla rozproszonej grupy abonentów tej samej organizacji. Szczególnie dotyczy to organizacji, działających na rozległym obszarze, takich jak:

- leśnictwo, budownictwo, transport;
- policja, straż pożarna, pogotowie ratunkowe, energetyka, gazownictwo, służby portowe (lotnicze, morskie).

W zależności od wagi tych systemów oraz celu ich funkcjonowania, można wyodrębnić dwa podstawowe zakresy radiowe[28]:

- specjalnie przydzielane pasma międzynarodowe (104 MHz, 166 MHz) oraz krajowe (31 – 47 MHz, 156 – 174 MHz);
- ogólnodostępne dla mniej ważnych zastosowań (27 MHz, 41 MHz, 432 MHz).
- Cechy wspólne tych systemów zawierają się w następujących aspektach:
- abonenci sieci są pracownikami (członkami) tej samej organizacji;
- organizacja jest operatorem sieci i ponosi koszty jej eksploatacji;
- sieć składa się z wielu stacji ruchomych oraz jednej lub kilku stacji bazowych;
- operator stacji bazowej posiada prawo wydawania poleceń innym stacjom;
- większość połączeń odbywa się między dyspozytorem a abonentami stacji ruchomych;

[28] Patrz P. Daniluk, Możliwości wykorzystania systemów radiokomunikacyjnych w sytuacja kryzysowych.

- nieliczne są sytuacje wychodzenia z sieci radiotelefonicznej do sieci stacjonarnej publicznej;
- połączenia trwają krótko;
- jakość łączności jest nienajlepsza.

Rozpatrując organizację sieci dyspozytorskich na potrzeby operacji kryzysowych należy pamiętać o kilku ich istotnych wadach, a mianowicie:

- brak prywatności rozmów;
- nieefektywne wykorzystanie pasma;
- niska jakość łączności wynikająca głównie z rodzaju modulacji;
- potrzeba samodzielnego utrzymywania łączności;
- ograniczone możliwości automatyzacji pracy.

Zalety analizowanych systemów, w aspekcie operacji kryzysowych, są następujące:

- znaczne zasięgi dla zakresów najniższych UKF (30 – 47 MHz);
- możliwości współpracy z wieloma innymi służbami pracującymi w podobnym zakresie częstotliwości (pasmo 31 – 47 MHz, 112 – 174 MHz oraz 420 – 470 MHz);
- bardzo znaczne zasięgi dla zakresu 1607, 5 kHz – 27 500 kHz (dla zastosowań krajowych - w nocy rzędu 200- 300 km, w dzień 300 – 500 km);
- osobowa identyfikacja, w wielu sytuacjach bardziej niezawodna niż elektroniczna lub automatyczna;
- możliwość bezpośredniego kontrolowania (monitorowania) działania kierownictw regionalnych (wojewódzkich) przez centrum krajowe (nasłuch lub praca aktywna).

WNIOSKI

Jak zauważono wcześniej, podsystem informacyjny stanowi podstawę każdego procesu decyzyjnego i decyduje o jego sprawności i skuteczności. Z tego też względu jego możliwości w zakresie transmisji, przechowywania i obróbki danych powinny być jak najlepsze.

O skuteczności podsystemu informacyjnego decydować będzie wiele różnorodnych czynników. Jednym z nich jest możliwości wykorzystania posiadanej infrastruktury teleinformatycznej, zarówno będącej w posiadaniu wojsk lądowych jak i znajdującej się w rejonie działania (kryzysu). Przeprowadzone badania wykazały, że postęp techniczny i technologiczny w dziedzinie teleinformatyki znacznie ułatwił możliwości wykorzystania cywilnej i resortowej infrastruktury teleinformatycznej. Powszechna dostępność systemów satelitarnych,

szybki rozwój sieci GSM i UMTS, a także innych sieci teleinformatycznych takich jak np. internet czy WiMAX spowodował, że na terytorium Europy trudno dziś znaleźć miejsce w którym nie można by skorzystać z jednej z wymienionych technologii.

Możliwości wykorzystania istniejącej infrastruktury teleinformatycznej są tym większe im bardziej otwarte są systemy wykorzystywane w wojskach lądowych. Badania wykazały, że podejście COTS (*ang. commercial of the shelves*), polegające na wykorzystaniu technologii komercyjnych w wojskowych systemach teleinformatycznych, w znacznym stopniu ułatwiło współpracę cywilnych, resortowych i wojskowych systemów teleinformatycznych. Należy zauważyć jednocześnie, że obserwowany jest ciągły wzrost znaczenia technologii transmisji danych na niekorzyść klasycznych systemów telekomunikacyjnych.

Podsumowując wyniki badań przedstawione w niniejszym rozdziale można stwierdzić, że praktycznie wszystkie systemy teleinformatyczne znajdujące się na obszarze operacji można wykorzystać w kierowaniu reagowaniem kryzysowym. Jedne z nich charakteryzują się dużą dostępnością, inne dużą przepustowością, jeszcze inne są tanie w eksploatacji lub też są odporne na zakłócenia. To jaka część infrastruktury teleinformatycznej zostanie wykorzystania zależy od charakteru operacji i przyjętych w niej priorytetów.

ZAKOŃCZENIE

Rozwój cywilizacyjny, oprócz niewątpliwych dobrodziejstw, przyniósł także wiele zagrożeń, które mogą oddziaływać na społeczeństwa w postaci różnorodnych kryzysów. Skuteczne radzenie sobie z nimi jest jednym z wyznaczników nowoczesnego społeczeństwa i gwarantem przetrwania. Źródła kryzysów mogą być różne i w różny sposób oddziaływać na społeczeństwo. Mogą to być kryzysy wywołane m. In. działalnością terrorystyczną, katastrofą ekologiczną czy też wrogim oddziaływaniem ekonomicznym innego państwa.

Do niwelowania skutków kryzysów należy wykorzystać wszystkie możliwe środki w tym także systemy teleinformatyczne. Ich szybki rozwój zrewolucjonizował podejście do zarządzania (kierowania) i umożliwił wprowadzenie nowej jakości w dostępie do informacji.

Dostrzegając wagę problemu związanego z kierowaniem reagowaniem kryzysowym zespół autorski podjął się opracowania ważnego problemu jakim są możliwości wykorzystania i współpracy systemów teleinformatycznych na potrzeby kierowania reagowaniem kryzysowym realizowanym przez wojska lądowe. Stosując niezbędne metody empiryczne i teoretyczne oraz określoną we wstępie procedurę badawczą autorzy starali się wyczerpująco rozwiązać główny problem badawczy oraz udzielić odpowiedzi na wszystkie postawione we wstępie szczegółowe pytania badawcze.

Otrzymane wyniki badań pozwalają na stwierdzenie, że idealnym rozwiązaniem było by stworzenie jednego **zintegrowanego zautomatyzowanego systemu informatycznego**, który funkcjonował by we wszystkich służbach oraz podmiotach biorących udział w kierowaniu siłami i środkami podczas działań związanych z reagowaniem kryzysowym. Zespół badaczy zdaje sobie jednak sprawę, że nie jest możliwe zastosowanie takiego rozwiązania, dlatego koniecznym jest:

- opracowanie koncepcji informatycznego wsparcia kierowania reagowaniem kryzysowym, która w pierwszym rzędzie zawierać będzie wymagania jakie taki system powinien spełniać;
- opracowanie i wdrożenie interfejsów umożliwiających bezkolizyjne przekazywanie informacji pomiędzy różnymi systemami informacyjnymi wszystkich podmiotów biorących udział w kierowaniu reagowaniem kryzysowym;
- opracowanie środowiska informatycznego, które ujednolici dotychczasowe działania różnych organów i służb;

- opracowanie standardu informatycznego, który stanowić będzie podstawę formułowania w przyszłości specyfikacji sprzętowych i programowych;
- określenie harmonogramu działań koncepcyjnych oraz wdrożeniowych;
- oszacowanie kosztów związanych ze wszystkimi działaniami w tym zakresie oraz wskazanie źródeł ich finansowania.

System teleinformatyczny powinien, między innymi, zapewnić:

- skuteczne administrowanie w sytuacji wykraczającej poza granicę akceptowanego poziomu bezpieczeństwa;
- wdrażanie i utrzymywanie zdolności reagowania;
- zagwarantowanie realizacji procesów społecznych i gospodarczych w sytuacji zagrożenia na akceptowanym poziomie;
- zabezpieczenie racjonalnej i terminowej pomocy ofiarom klęsk i katastrof; zapewnienie wsparcia sektora cywilnego dla wysiłków militarnych i obrony cywilnej podczas działań zbrojnych; racjonalne wykorzystanie zasobów ludzkich, finansowych i materiałowych.

Oprócz powyższego zespół autorski sformułował następujące wnioski końcowe i uogólnienia:

- Wymagania stawiane przed systemami teleinformatycznymi można podzielić na dwie podstawowe grupy: **wymagania operacyjne** i **wymagania techniczno-eksploatacyjne**. Do podstawowych wymagań operacyjnych należy zaliczyć: **terminowość, wierność, skrytość**. Główne wymagania techniczno-eksploatacyjne to: **gotowość (dostępność), przepustowość systemu, trwałość, mobilność, bezpieczeństwo.**
- Systemem informacyjny wykorzystywany w kierowaniu reagowaniem kryzysowym musi spełnić wymagania[1]:
  - dostarczanie kompleksowych i aktualnych informacji, zapewnianie selektywnego i skutecznego wykorzystania informacji oraz właściwej wymiany informacji pomiędzy komórkami organizacyjnymi, przełożonymi i podwładnymi w obydwu kierunkach,
  - prostotę w użytkowaniu i zapewnieniu stałej, automatycznej metody pozyskiwania informacji z ustalonych źródeł,

[1] por. S. Pietrzak, Informacyjny system zarządzania przedsiębiorstwem, Ekonomika i Organizacja Przedsiębiorstwa, nr 6/1998, s. 7-8

- umożliwienie natychmiastowego pozyskania danych, nawet z najniższego szczebla zarządzania, wyszukiwanie i kojarzenie informacji z różnych źródeł, przedstawienie danych i wyników ich analiz w różnych układach sprawozdawczych,
- przepływu informacji opartego na sprzężeniach zwrotnych.

- W stosunku do informacji, wykorzystywane w kierowaniu reagowaniem kryzysowym systemy teleinformatyczne powinny zapewnić:
  - dostępność informacji,
  - wiarygodność informacji,
  - bezpieczeństwo informacji,
  - spójność informacji,
  - trwałość informacji,
  - aktualność informacji.
- Współpraca wojsk lądowych z terenowymi organami administracji publicznej w ramach kierowania reagowaniem kryzysowym przy wykorzystaniu wojskowych sieci telekomunikacyjnych jest możliwa wtedy, gdy organa administracji publicznej zostaną w te środki wyposażone.
- Coraz większego znaczenia w procesie kierowania nabierają możliwości transmisyjne sieci komputerowych. Sieci te służą one do wymiany informacji pomiędzy osobami funkcyjnymi i zespołami funkcjonalnymi wyposażonymi w komputery (lub inne urządzenia np. telefony IP). Umożliwiają dostęp do odpowiednich baz danych a także dostęp do współdzielonych zasobów sieciowych takich jak: drukarki, plotery urządzenia pamięci masowych.
- Możliwości wykorzystania istniejącej infrastruktury teleinformatycznej jest tym większa im bardziej otwarte są te systemy. Badania wykazały, że podejście COTS (*ang. commercial of the shelves*), polegające na wykorzystaniu technologii komercyjnych w wojskowych systemach teleinformatycznych, w znacznym stopniu ułatwiło współpracę cywilnych, resortowych i wojskowych systemów teleinformatycznych. Należy zauważyć jednocześnie, że obserwowany jest ciągły wzrost znaczenia technologii transmisji danych na niekorzyść klasycznych systemów telekomunikacyjnych.

BIBLIOGRAFIA:

1. Antoniewicz R., Kobryń D., Transmisja danych w systemach telekomunikacji ruchomej – zmiany w systemie GSM, Przegląd Telekomunikacyjny, 2/2000

2. Bem D. J., Satelitarne systemy dostępowe, Przegląd Telekomunikacyjny, 8-9/2000

3. Beynon-Davies P., Inżynieria systemów informacyjnych, Wydawnictwo Naukowo-Techniczne, Warszawa 1999.

4. Bogucki J., Satelity niskoorbitowe, Przegląd Telekomunikacyjny, 12/1998

5. Brzezina J. M., Dańko Z., Interoperacyjność systemu AGS, część I, Przegląd Sił Powietrznych, nr 03/2005, Poznań 2005.

6. Brzozowski J., Działania bojowe w rejonach zurbanizowanych we współdziałaniu z jednostkami obrony terytorialnej, Akademia Obrony Narodowej – Wydział Wydawniczy, Warszawa 1998.

7. Bujak A., Sobolewski G., Teren zabudowany środowiskiem walki XXI wieku, Akademia Obrony Narodowej – Wydział Wydawniczy, Warszawa 2005.

8. Burawski Z., Wsparcie inżynieryjne operacji w terenie zurbanizowanym na poziomie taktycznym, Rola terenu zurbanizowanego we współczesnych operacjach, Akademia Obrony Narodowej – Wydział Wydawniczy, Warszawa 2005.

9. Coulouris G., Dollimore J., ,Kindberg T., Systemy rozproszone - podstawy i projektowanie, Wydawnictwa Naukowo-Techniczne, Warszawa 1998.

10. Daniluk P., Radiostacje pola walki, Akademia Obrony Narodowej – Wydział Wydawniczy, Warszawa 2002.

11. Daniluk P., Radiowa służba stała i ruchoma, Akademia Obrony Narodowej – Wydział Wydawniczy, Warszawa 2004.

12. Daniluk P., Radiowe systemy łączności ruchomej, Akademia Obrony Narodowej – Wydział Wydawniczy, Warszawa 2004.

13. David S. A., Richard E. H., Power to the Edge, Command Control in the Information Age, Command and Control Research Program, Publication 2003.

14. Dąbrowski M., Ewolucja systemów komórkowych – systemy trzeciej generacji, Przegląd Telekomunikacyjny, 5/1999

15. Dąbrowski M., Systemy komórkowe do roku 2010, Przegląd Telekomunikacyjny, 8-9/2001

16. Dąbrowski M.., Ewolucja systemów komórkowych - system trzeciej generacji, Przegląd Telekomunikacyjny, 5/1999

17. Dela P., Wprowadzenie do systemu formatowania wiadomości w NATO AdatP-3, Akademia Obrony Narodowej – Wydział Wydawniczy, Warszawa 2005.

18. Dras M., Systemy sprzętowe do budowy polowych sieci teleinformatycznych na stanowiskach dowodzenia, Sieci teleinformatyczne stanowisk dowodzenia szczebla taktycznego Wojsk Lądowych, Akademia Obrony Narodowej - Wydział Wydawniczy, Warszawa 2006.

19. Fiołna Z., Powiązania informacyjne wewnątrz i na zewnątrz stanowiska dowodzenia brygady zmechanizowanej, Projektowanie struktury organizacyjnej dowództwa brygady zmechanizowanej (pancernej), Akademia Obrony Narodowej - Wydział Wydawniczy, Warszawa 2002.

20. FM-3-06.11 - Combined Arms Operations in Urban Terrain.

21. Hołubowicz W., Płóciennik P., Cyfrowe systemy telefonii komórkowej GSM, Holkom, Poznań 1998

22. Jakubczak R., Janczak J., Obrona terytorialna polski na progu XXI w, Dom Wydawniczy Bellona, Warszawa 1998.

23. Jakubczak R., Operacyjny obszar sztuki wojennej obrony terytorialnej, Zeszyty Naukowe AON nr 2(51), Akademia Obrony Narodowej - Wydział Wydawniczy, Warszawa 2003.

24. Janczak J., Zakłócanie Informacyjne, Akademia Obrony Narodowej – Wydział Wydawniczy, Warszawa 2002.

25. JP-3.0, Doctrine for Joint Operation.

26. Katulski R. J., Gajewski S., Marczak A., Stefański J., UMTS – telekomunikacja bezprzewodowa na progu XXI wieku, Przegląd Telekomunikacyjny, 1/2001

27. Katulski R. J., Mikołajski M., Uwarunkowania rozwojowe w telekomunikacji satelitarnej, Przegląd Telekomunikacyjny, 7/2003

28. Katulski R. J., Mikołajski M., Współczesna telekomunikacja satelitarna, Przegląd Telekomunikacyjny, 2-3/2003

29. Katulski R. J., Rozwój i możliwości użytkowe systemu INMARSAT, Przegląd Telekomunikacyjny, 12/2000

30. Kołakowski J., Cichocki J., UMTS – System telefonii komórkowej trzeciej generacji, WKŁ, Warszawa 2003

31. Korzeniowski S., Wpływ specyficznych właściwości terenu zabudowanego na prowadzenie działań bojowych, Rola terenu zurbanizowanego we współczesnych operacjach, Akademia Obrony Narodowej – Wydział Wydawniczy, Warszawa 2005.

32. Kossobudzki L., System TETRA, Telekomunikacja i Techniki Informacyjne Nr 3-4/2005, Instytut Łączności, Warszawa 2005.

33. Krasoń J., TETRA – otwarty standard cyfrowej łączności trankingowej, Przegląd Telekomunikacyjny, 3/2000

34. Kubiński M.Działania aeromobilne w terenie zurbanizowanym, Rola terenu zurbanizowanego we współczesnych operacjach, Akademia Obrony Narodowej – Wydział Wydawniczy, Warszawa 2005.

35. Liberty J., C++ - Księga Eksperta, Wydawnictwo Helion, Gliwice 1999.

36. Łaszczuk A., Wsparcie geoinformacyjne działań w terenie zurbanizowanym, Rola terenu zurbanizowanego we współczesnych operacjach, Akademia Obrony Narodowej – Wydział Wydawniczy, Warszawa 2005.

37. Łokociejewski M., Nowak A., Wrzosek M., Scheffs W., Rosłan G., Rozpoznanie Wojskowe, część I, podstawy teoretyczne, Akademia Obrony Narodowej – Wydział Wydawniczy, Warszawa 2003.

38. Michniak J., Dowodzenie i Łączność, Akademia Obrony Narodowej – Wydział Wydawniczy, Warszawa 2005.

39. Michniak J., Stanowiska dowodzenia w wojskach lądowych, Akademia Obrony Narodowej – Wydział Wydawniczy, Warszawa 2003.

40. Multilateral Interoperability Programme, The C2 Information Exchange Data Model, C2IEDM, MAIN-UK-DMGW, Edition 6.15e, MIP – 2006.

41. Posobiec J., Wybrane zagadnienia działania wojsk zmechanizowanych i pancernych w terenie zurbanizowanym, Rola terenu zurbanizowanego we współczesnych operacjach, Akademia Obrony Narodowej – Wydział Wydawniczy, Warszawa 2005.

42. Praca zbiorowa pod kierunkiem Janczaka J. i Daniluka P., Środki Dowodzenia, Akademia Obrony Narodowej – Wydział Wydawniczy, Warszawa 2003.

43. Praca zbiorowa pod kierunkiem Janczaka J., System Łączności Brygady, Akademia Obrony Narodowej - Wydział Wydawniczy, Warszawa 2004.

44. Sejdak K., Lokalne sieci komputerowe na stanowisku dowodzenia, Przegląd Wojsk Lądowych Nr 10/2003, Warszawa 2003.

45. Siedlecki M., Perspektywiczny system teleinformatyczny Wojsk Lądowych, Przegląd Wojsk Lądowych Nr 10/2005, Warsazwa 2005.

46. Sienkiewicz P., Bezpieczeństwo informacyjne w erze globalizacji, Akademia Obrony Narodowej – Wydział Wydawniczy, Zeszyty Naukowe AON nr 3-4(48-49) 2002.

47. Silberschatz A., Galvin P.B., Podstawy systemów operacyjnych“, Wydawnictwa Naukowo-Techniczne, Warszawa 2001.

48. Słowik J., Wybrane aspekty systemu dowodzenia brygady obrony terytorialnej, Współdziałanie systemów dowodzenia Wojsk Operacyjnych i Wsparcia Krajowego, Akademia Obrony Narodowej – Wydział Wydawniczy, Warszawa 2005.

49. Słowik J., Wybrane determinanty organizacji systemu dowodzenia brygady obrony terytorialnej, Akademia Obrony Narodowej – Wydział Wydawniczy, Warszawa 2003.

50. Smoleński L., Zientalski M., Rozwój mediów i systemów transmisyjnych, Przegląd Telekomunikacyjny, nr 1/2000, Wydawnictwo SIGMA-NOT, Warszawa 2000.

51. Sobolewski G., Obszary współdziałania Lądowych Wojsk Operacyjnych i Wojsk Wsparcia Krajowego , Współdziałanie systemów dowodzenia Wojsk Operacyjnych i Wsparcia Krajowego, Akademia Obrony Narodowej – Wydział Wydawniczy, Warszawa 2005.

52. Sobolewski G., Teren zurbanizowany środowiskiem operacji militarnych XXI wieku, Rola terenu zurbanizowanego we współczesnych operacjach, Akademia Obrony Narodowej – Wydział Wydawniczy, Warszawa 2005.

53. Sobolewski G., Wspólne działania obronne wojsk operacyjnych i obrony terytorialnej, Akademia Obrony Narodowej – Wydział Wydawniczy, Warszawa 2004.

54. Sportack M., Sieci Komputerowe, Księga Eksperta, Wydawnictwo Helion, Gliwice 1999.

55. Szafran H., Narodowe zadania wojskowego wsparcia krajowego i ich realizacja, Współdziałanie systemów dowodzenia Wojsk Operacyjnych i Wsparcia Krajowego, Akademia Obrony Narodowej – Wydział Wydawniczy, Warszawa 2005.

56. Tomaszewski B., Nowosielski L., Dalecki R., Taktyczna sieć wymiany informacji z zastosowaniem szerokopasmowych radiostacji sieci IP – HCDR, materiały informacyjne firmy SILTEC.

57. Urbanek A., WiMAX czy HSDPA?, NetWorld Nr 06/2006, IDG Poland S.A., Warszawa 2006.

58. Urbanek A., WiMAX gotowy do wdrożenia, NetWorld Nr 09/2005, IDG Poland S.A., Warszawa 2005.

59. Wesołowki K., Systemy radiokomunikacji ruchomej, Wydawnictwa Komunikacji i Łączności WKŁ, Warszawa 2003.

60. Wojciechowicz W., Ochrona infrastruktury krytycznej państwa, Myśl Wojskowa, Redakcja Czasopism Wojskowych, Warszawa 2001.

61. Wołejszo J., Fiołna Z., Dowodzenie brygadą zmechanizowaną (pancerną) w obronie, Akademia Obrony Narodowej – Wydział Wydawniczy, Warszawa 2002.

62. Wołejszo J., Wybrane aspekty projektowania struktur organizacyjno-funkcjonalnych ośrodków decyzyjnych, Akademia Obrony Narodowej – Wydział Wydawniczy, Warszawa 2002.

63. Wołejszo J., Wybrane aspekty projektowania struktury organizacyjnej zespołu dowodzenia stanowiska dowodzenia brygady zmechanizowanej, Akademia Obrony Narodowej – Wydział Wydawniczy, Warszawa 2002.

64. Wrzosek M, Struktura strumienia informacyjnego w taktycznym systemie rozpoznania wojsk lądowych, część II, Zeszyty Naukowe AON nr 3-4 (48-49), Akademia Obrony Narodowej – Wydział Wydawniczy, Warszawa 2002.

65. Wrzosek M., Determinanty oceny rozpoznawczej w działaniach w terenie zurbanizowanym, Rola terenu zurbanizowanego we współczesnych operacjach, Akademia Obrony Narodowej – Wydział Wydawniczy, Warszawa 2005.

66. Wrzosek M., Dezinformacja jako komponent operacji informacyjnych, Akademia Obrony Narodowej - Wydział Wydawniczy, Warszawa 2005.

67. Wrzosek M., Struktura strumienia informacyjnego w taktycznym systemie rozpoznania wojsk lądowych, część I, Zeszyty Naukowe AON nr 2 (47), Akademia Obrony Narodowej – Wydział Wydawniczy, Warszawa 2002.

ZAŁĄCZNIK 1

ARKUSZ OBSERWACJI

Przedmiot obserwacji:

Narzędzia teleinformatyczne wykorzystywane w kierowaniu reagowaniem kryzysowym w ćwiczeniu dowódczo-sztabowym „Pierścień 2005"

Cel obserwacji:

- Określenie przydatności organicznych systemów teleinformatycznych wojsk lądowych w kierowaniu reagowaniem kryzysowym,
- Określenie możliwości wykorzystania cywilnych systemów teleinformatycznych na potrzeby kierowania reagowaniem kryzysowym,

Uwarunkowania organizacyjno-techniczne:

- Obserwacji dokonać w formie obserwacji nieuczestniczącej, bezpośredniej i pośredniej
- Obserwować pracę ćwiczących zespołów ze szczególnym uwzględnieniem współpracy ćwiczących dowództw z PZRK Pułtusk i Ciechanów;
- Dokonać analizy stosowanych rozwiązań.

Miejsce

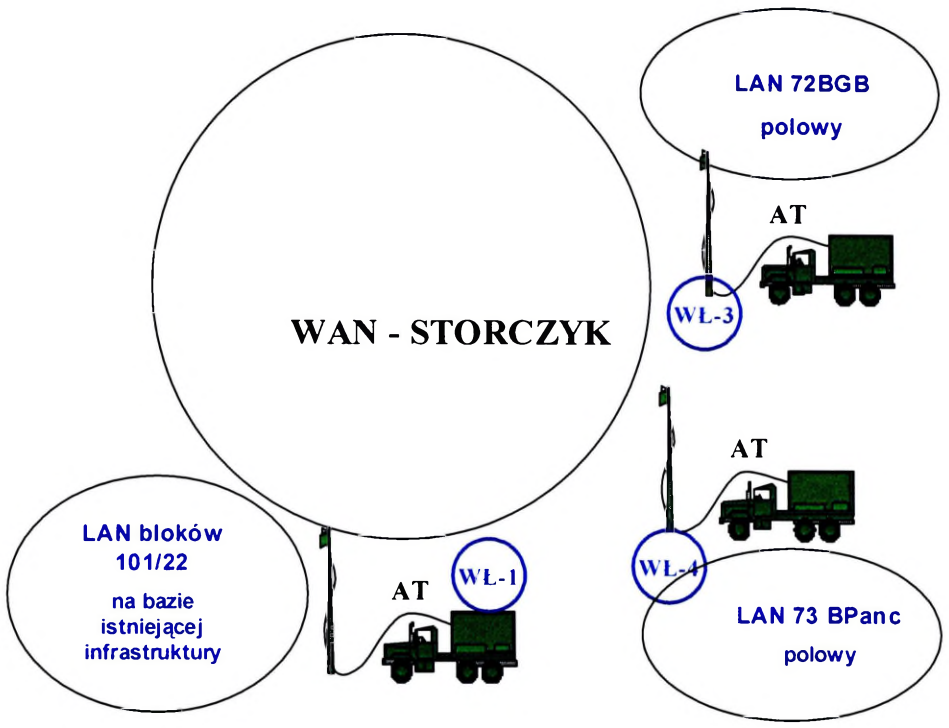
AON

Czas

Czerwiec 2005

SPRAWOZDANIE Z OBSERWACJI

Na potrzeby ćwiczenia zostały utworzone trzy lokalne sieci komputerowe etherten z protokołem TCP/IP. Jedna z nich zbudowana była w oparciu o stacjonarny sprzęt sieciowy i komputerowy w budynkach 22 i 101. Budynki połączone były światłowodem. Pozostałe dwie sieci polowe zbudowane były w oparciu o mobilne środki informatyczne. Działały one na potrzeby 72 BGB i 73 BPanc. Połączenie między tymi trzema sieciami zapewniały aparatownie transmisyjne działające w ramach sieci radioliniowo-kablowej. Ogólny schemat połączeń sieciowych przedstawiono na rysunku 1.



Rysunek 1. Uproszczony schemat połączeń sieci komputerowych

Wymiana informacji pomiędzy ćwiczącymi dowództwami a PZRK Pułtusk odbywała się poprzez zastosowanie radiolinii o przepustowości 34 Mb/s. Radiolinia ta była wpięta w sieć rozległą Storczyk i świadczyła następujące usługi:

- transmisja danych;
- transmisja mowy;
- transmisja obrazu;
- wideokonferencja;
- telekonferencja.

Załącznik 1

WNIOSKI

Na podstawie przeprowadzonych badań można sprecyzować następujące wnioski:

1. Sprzęt wykorzystywany do współdziałania ćwiczących dowództw z PZRK wykonany był w technologii COTS ;
2. Usługi świadczone na potrzeby współdziałania były wystarczające. Nie zaobserwowano problemów z przepustowością łącza;
3. Zastosowane rozwiązanie ograniczało mobilność. Czas potrzebny na zwinięcie i rozwinięcie radiolinii wynosił około 2 godzin.
4. Największą zaletą wykorzystywanych rozwiązań była możliwość przeprowadzenia wideo konferencji co w zdecydowany sposób przyspieszyło proces kierowania reagowaniem kryzysowym;
5. Wszystkie sieci pracowały w oparciu o protokół TCP/IP;
6. Praktycznie każdy organ dowodzenia pracujący w sieciach komputerowych rozwiniętych na potrzeby ćwiczenia miał dostęp do strumienia danych z wideo konferencji.

ZAŁĄCZNIK 2

ARKUSZ OBSERWACJI

Przedmiot obserwacji:

Narzędzia teleinformatyczne wykorzystywane w kierowaniu reagowaniem kryzysowym w ćwiczeniu dowódczo-sztabowym „Pierścień 2006"

Cel obserwacji:

- Określenie przydatności organicznych systemów teleinformatycznych wojsk lądowych w kierowaniu reagowaniem kryzysowym,
- Określenie możliwości wykorzystania cywilnych systemów teleinformatycznych na potrzeby kierowania reagowaniem kryzysowym,

Uwarunkowania organizacyjno-techniczne:

- Obserwacji dokonać w formie obserwacji nieuczestniczącej, bezpośredniej i pośredniej
- Obserwować pracę ćwiczących zespołów ze szczególnym uwzględnieniem współpracy ćwiczących dowództw z PZRK Pułtusk i Ciechanów;
- Dokonać analizy stosowanych rozwiązań.

Miejsce

9 pdow

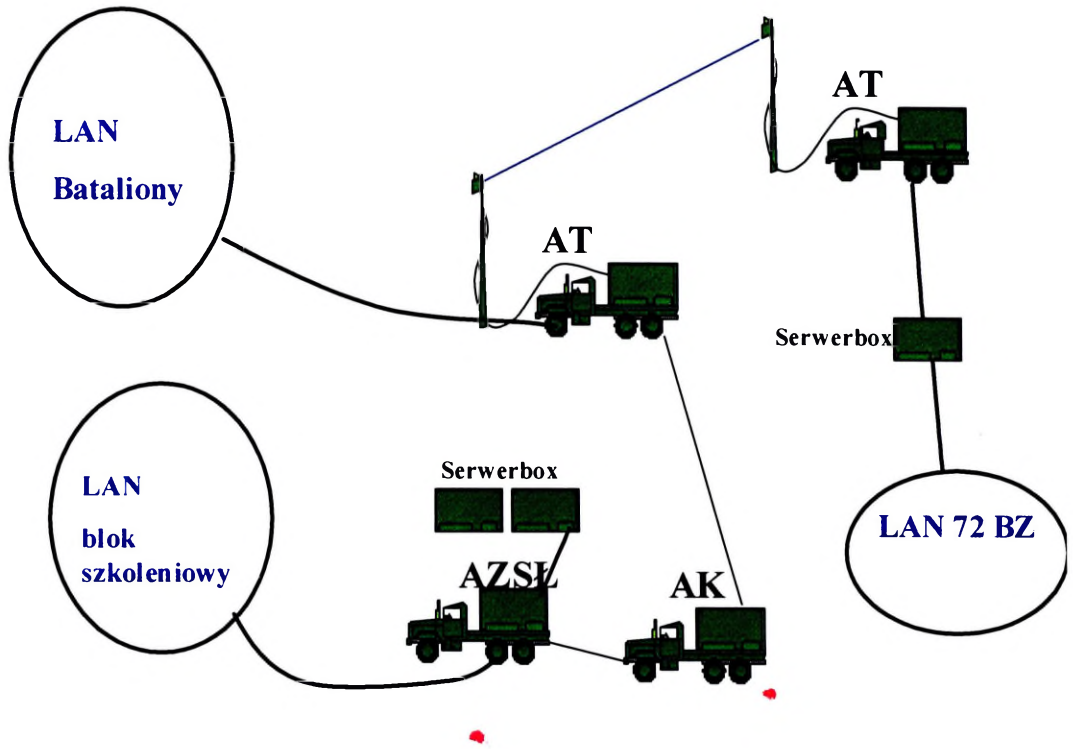
Czas

Czerwiec 2006

Załącznik 2

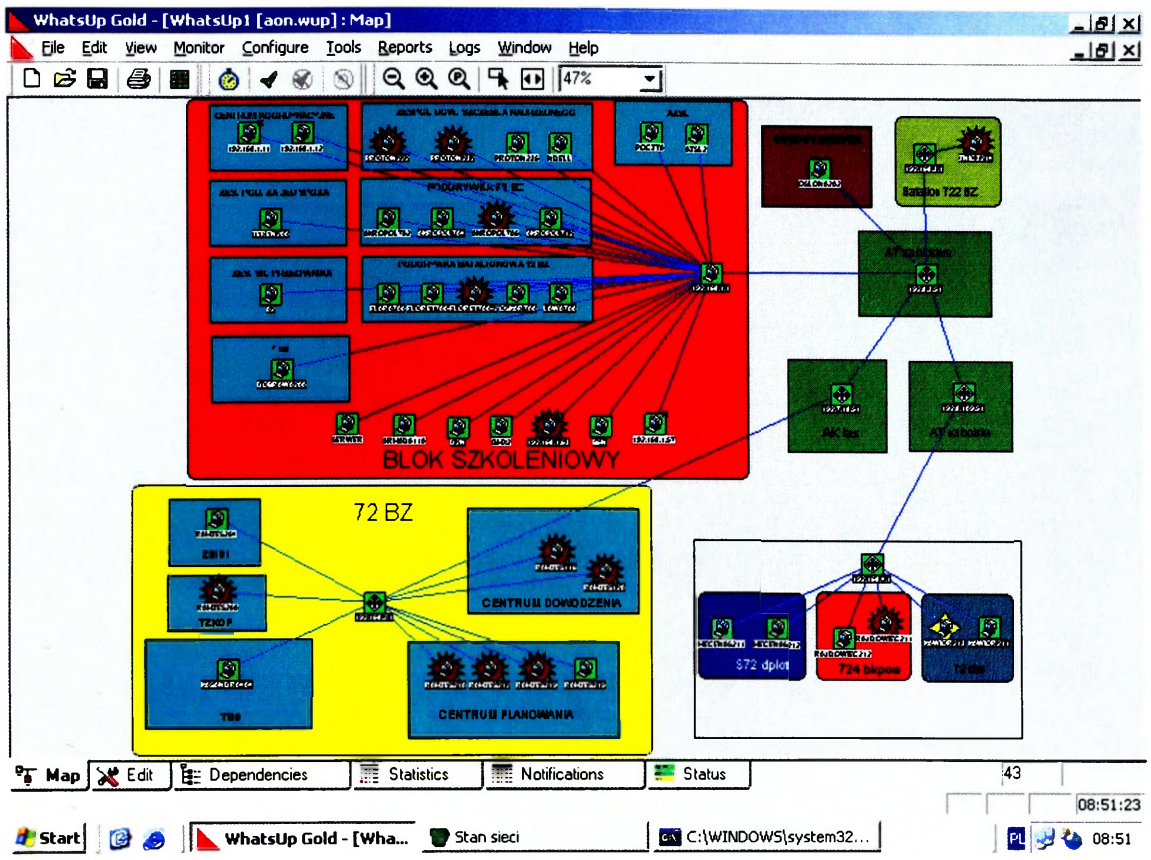
SPRAWOZDANIE Z OBSERWACJI

Na potrzeby ćwiczenia zostały utworzone trzy lokalne sieci komputerowe etherten z protokołem TCP/IP. Jedna z nich zbudowana była w oparciu o stacjonarny sprzęt sieciowy i komputerowy w bloku szkoleniowym 9 pdow. Pozostałe dwie sieci polowe zbudowane były w oparciu o mobilne środki informatyczne. Działały one na potrzeby 72 BZ i batalionów 72 BZ. Połączenie między tymi trzema sieciami zapewniały aparatownie transmisyjne działające w ramach sieci radioliniowo-kablowej. Ogólny schemat połączeń sieciowych przedstawiono na rysunkach 1, 2 i 3.

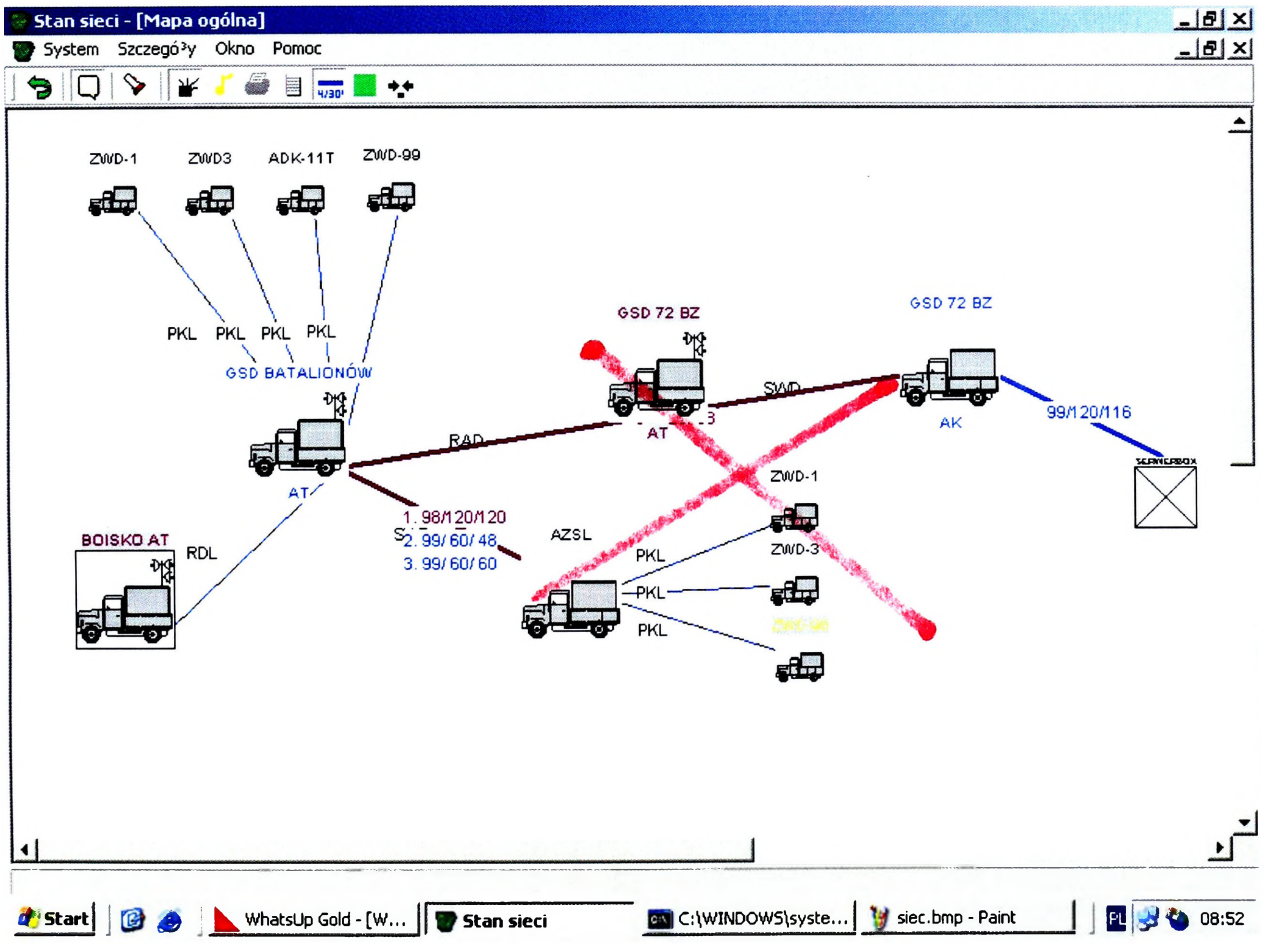


Rysunek 1. Uproszczony schemat połączeń sieci komputerowych

Załącznik 2



Rysunek 2. Schemat sieci komputerowej wykorzystywanej na ćwiczeniu



Rysunek 3. Schemat sieci radioliniowo-kablowej wykorzystywanej na ćwiczeniu

Wymiana informacji pomiędzy ćwiczącymi dowództwami a PZRK Ciechanów odbywała się poprzez zastosowanie systemów satelitarnych o przepustowości 512 kb/s. Terminal satelitarny był połączony z siecią rozległą Storczyk i świadczył usługi:

- transmisja danych;
- wideokonferencja.

WNIOSKI

Na podstawie przeprowadzonych badań można sprecyzować następujące wnioski:

1. Sprzęt wykorzystywany do współdziałania ćwiczących dowództw z PZRK wykonany był w technologii komercyjnej (cywilnej);
2. Usługi świadczone na potrzeby współdziałania były nie wystarczające. Zaobserwowano problemy z przepustowością łącza (głównie w trakcie wideo konferencji);
3. Zastosowane rozwiązanie nie ograniczało mobilności. Czas potrzebny na zwinięcie i rozwinięcie systemu wynosił około 15 minut.
4. Największą zaletą wykorzystywanych rozwiązań była możliwość przeprowadzenia wideo konferencji (z kompresją danych) co w zdecydowany sposób przyspieszyło proces kierowania reagowaniem kryzysowym;
5. Praktycznie każdy organ dowodzenia pracujący w sieciach komputerowych rozwiniętych na potrzeby ćwiczenia miał dostęp do strumienia danych z wideo konferencji.