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

AKADEMIA OBRONY NARODOWEJ

Ppłk mgr inż. Grzegorz ŚWIDZIKOWSKI

BEZPIECZEŃSTWO INFORMACJI W SIECI TELETRANSMISYJNEJ DYWIZJI ZMECHANIZOWANEJ

Rozprawa doktorska

Nr ewid. 58650

WARSZAWA 2005

Colour Chart #13 Blue Cyan Green Yellow Red Magenta White 3/Color Black DANES-PICTA.COM

AKADEMIA OBRONY NARODOWEJ

WYDZIAŁ WOJSK LĄDOWYCH

BIBLIOTEKA GŁÓWNA – ARCHIWUM
Nr ewid. 58650
II
Akademii Obrony Narodowej

ppłk mgr inż. Grzegorz ŚWIDZIKOWSKI

BEZPIECZEŃSTWO INFORMACJI W SIECI TELETRANSMISYJNEJ DYWIZJI ZMECHANIZOWANEJ

Rozprawa doktorska

Pod kierownictwem naukowym:

płk. prof. dr. hab. inż. Józefa MICHNIAKA

Warszawa 2005

SPIS TREŚCI

WSTĘP 4

1. ZAŁOŻENIA METODOLOGICZNE 9

1.1. Ogólne założenie poznawcze oraz obszar i przedmiot badań 9

1.2. Problemy badawcze 11

1.3. Cele badawcze i hipoteza robocza 13

1.4. Metody badawcze i teren badań 15

1.5. Organizacja i przebieg badań 22

2. UWARUNKOWANIA TAKTYCZNE I ORGANIZACYJNO-TECHNICZNE FUNKCJONOWANIA SIECI TELETRANSMISYJNEJ DYWIZJI ZMECHANIZOWNEJ 25

2.1. Identyfikacja uwarunkowań wynikających z rodzaju działań taktycznych dywizji zmechanizowanej 26

2.2. Identyfikacja elementów organizacyjno-eksploatacyjnych polowego systemu łączności dywizji zmechanizowanej 35

2.3. Sieć teletransmisyjna dywizji zmechanizowanej jako obszar badań 44

2.4. Struktura organizacyjno-techniczna pomocniczych węzłów łączności sieci teletransmisyjnej dywizji zmechanizowanej 76

2.5. Struktura organizacyjno-techniczna linii telekomunikacyjnych (odcinków międzywęzłowych) sieci teletransmisyjnej dywizji zmechanizowanej 81

2.6. Wybór wariantu sieci teletransmisyjnej poddanego ocenie pod względem bezpieczeństwa przesyłanej informacji 85

3. WYMAGANIA NARODOWE I SOJUSZNICZE STAWIANE BEZPIECZNEJ SIECI TELETRANSMISYJNEJ DYWIZJI ZMECHANIZOWANEJ 88

3.1. Wymagania bezpieczeństwa stawiane wojskowemu polowemu systemowi łączności 88

3.2. Wymagania bezpieczeństwa stawiane sieci teletransmisyjnej dywizji zmechanizowanej 92

4. ZAGROŻENIA WPŁYWAJĄCE NA BEZPIECZEŃSTWO INFORMACJI W SIECI TELETRANSMISYJNEJ DYWIZJI ZMECHANIZOWANEJ 108

4.1. Podział i charakterystyka zagrożeń bezpieczeństwa informacji w sieci teletransmisyjnej dywizji zmechanizowanej 109

4.2. Gradacja zagrożeń bezpieczeństwa informacji w polowych wojskowych sieciach telekomunikacyjnych 124

4.3. Identyfikacja zagrożeń dla sieci teletransmisyjnej dywizji zmechanizowanej 143

5. KONCEPCJA PRZEDSIĘWZIĘĆ ORGANIZACYJNO-EKSPLOATACYJNYCH ZAPEWNIAJĄCYCH SPEŁNIENIE WYMAGAŃ BEZPIECZEŃSTWA INFORMACJI W SIECI TELETRANSMISYJNEJ DYWIZJI ZMECHANIZOWANEJ 149

5.1. Środki ochrony informacji w polowych wojskowych systemach telekomunikacyjnych 150

5.2. Ocena bezpieczeństwa informacji w sieci teletransmisyjnej dywizji zmechanizowanej 181

ZAKOŃCZENIE 198

BIBLIOGRAFIA 204

ZAŁĄCZNIKI 210

WSTĘP

Trwające od kilkunastu lat przemiany społeczno-ekonomiczne oraz wstąpienie naszego kraju do Organizacji Paktu Północnoatlantyckiego wywarły ogromny wpływ na bezpieczeństwo Polski. Przyczyniły się do innego spojrzenia na tę problematykę oraz doprowadziły do przewartościowania założeń polityki militarnej, którego następstwem była nowelizacja narodowej doktryny obronnej. Zmianie poglądów w tej dziedzinie towarzyszyły i w dalszym ciągu towarzyszą przeobrażenia w strukturach organizacyjnych, wyposażeniu, dyslokacji oraz samej koncepcji użycia sił zbrojnych RP.

Realizacja przedsięwzięć w odniesieniu do bezpieczeństwa kraju wymaga jeszcze rozwiązania całego szeregu bardzo istotnych problemów. Jednym z nich, a może nawet najważniejszym jest zapewnienie kierowania przygotowaniami i prowadzeniem obrony państwa. Do tego celu potrzebny jest zintegrowany w zakresie techniki i usług, jednolity, nowoczesny i sprawny system kierowania państwem i dowodzenia siłami zbrojnymi, a w tym bezpieczny, niezawodny, zintegrowany oraz nowoczesny system łączności i informatyki odporny na oddziaływania zewnętrzne i wewnętrzne.

Pod pojęciem bezpiecznego systemu[1] należy rozumieć taki system, który zapewnia pożądane warunki tajności korespondencji, co z kolei nieodłącznie wiąże się z ochroną informacji w systemach łączności i informatyki.

Systemy te w sferze obronności państwa odgrywają bowiem bardzo ważną rolę, ze względu na wartość przekazywanych w nich informacji. Dotyczą one między innymi danych pochodzących z rozpoznania, mówiących o możliwościach potencjalnego przeciwnika, danych o sytuacji wojsk własnych, ich dyslokacji, ugrupowaniu i zabezpieczenia logistycznym. O powadze omawianego problemu i to nie tylko w odniesieniu do sektora obronnego może świadczyć następujące sformułowanie:

Bezpieczeństwo i ochrona informacji jest jednym z najważniejszych problemów związanych z powszechnym stosowaniem nowoczesnych systemów teleinformatycznych, a niebezpieczeństwa wynikające z niedostatecznego poziomu ochrony informacji

[1] Ustawa o ochronie informacji niejawnych z dnia 22.01.1999 r. (Dz. U Nr 11, poz. 95) z późniejszymi zmianami (2001, Dz. U Nr 22, poz. 247)

są główną przeszkodą na drodze rozwoju powszechnego społeczeństwa informacyjnego[2].

Z tej też przyczyny celowe, a nawet konieczne jest zapewnienie bezpieczeństwa informacjom z tego zakresu zgodnie z wymaganym przez nie poziomem klauzuli tajności. Wymóg powyższy jest obowiązujący dla każdego wytwarzającego, przetwarzającego, przechowującego i przesyłającego informacje klasyfikowane[3] systemu bez względu na fakt, czy funkcjonuje on w okresie pokoju, kryzysu lub konfliktu zbrojnego.

Potwierdzeniem prawdziwości przedstawionego powyżej sformułowania, poszerzonego o problematykę bezpieczeństwa informacji sojuszniczych, niech będzie cytat pochodzący ze „Strategii bezpieczeństwa narodowego", w którym stwierdza się:

W związku z wejściem do Sojuszu Północnoatlantyckiego wzrosła odpowiedzialność Polski za ochronę informacji niejawnych nie tylko krajowych, ale i powierzonych nam przez sojuszników. Sprawność i bezpieczeństwo systemów przekazywania i przetwarzania informacji odgrywa coraz ważniejszą rolę w funkcjonowaniu struktur państwa i społeczeństwa[4].

Wspomnianym wcześniej przeobrażeniom towarzyszyły i stale towarzyszą zmiany ustawowe, nowelizacja dotychczas obowiązujących, czy opracowanie nowych dokumentów normatywnych, takich jak różnego rodzaju dyrektywy, wytyczne, regulaminy i instrukcje, które z jednej strony zapewniają dostosowanie zawartych tam zapisów do ustaleń i wymagań przyjętych lub przyjmowanych przez organizację Traktatu Północnoatlantyckiego, z drugiej zaś uwzględniają zmieniające się uwarunkowania techniczno-eksploatacyjne i wymagania w zakresie organizacji systemu bezpieczeństwa w wojskowych sieciach i systemach telekomunikacyjnych.

Uchwalona w 1999 roku nowa ustawa „O ochronie informacji niejawnych" (Dz. U Nr 11, poz. 95 z późniejszymi zmianami 2001, Dz. U Nr 22, poz. 247) wprowadziła formalny wymóg wycofania z dniem 01.04.2000 r. wszystkich uprzednio obowiązujących w tej materii unormowań i przepisów. Jednocześnie narzucała w ww.

---

[2] M. Szeżyńska, Konspekt do wykładu „Bezpieczeństwo informacji", Instytut Systemów Elektronicznych Politechniki Warszawskiej, Warszawa 2002

[3] Uwaga: za informację klasyfikowaną uważana jest każda informacja opatrzona klauzulą tajności

[4] www.iniejawna.pl/przepisy/rozne/strategia_bnrp.html

terminie opracowanie i wdrożenie nowych normatywów, które obejmowałyby wszystkie obszary szeroko pojętego bezpieczeństwa, w tym bezpieczeństwa systemów łączności i informatyki uwzględniających wymagania oraz standardy sojusznicze.

Dokonane zmiany w pragmatyce organizacji systemu bezpieczeństwa informacji wojskowych systemów telekomunikacyjnych legły u podstaw przeprowadzonej przez autora analizy literatury z zakresu bezpieczeństwa informacji w wojskowych sieciach czy systemach telekomunikacyjnych. Jej efekt można nazwać zaskakującym. Poza aktualnie obowiązującymi aktami normatywnymi (m.in. dyrektywy i wytyczne) literatura (stan na koniec 2002 roku) analizowanego przedmiotu uwzględniająca specyfikę i działalność sił zbrojnych RP lub ważniejsze opracowania naukowo-badawcze w tym zakresie jest bardzo skąpa i przede wszystkim ogólna[5]. Stan ten jest najprawdopodobniej następstwem przyjętych w wojsku polskim obostrzeń i ograniczeń w dostępie do normatywów, w oparciu o które można prowadzić merytoryczne rozważania.

Jeśli zatem przyjmiemy, że jedna z analizowanych prac „Bezpieczeństwo informacji w SZ RP – aspekty strategiczne" zawiera ocenę aktualnie obowiązujących standardów i wymagań bezpieczeństwa na szczeblu strategicznym, to uwagę należy przenieść na niższe szczeble dowodzenia.

Stąd też zdaniem autora obszar bezpieczeństwa informacji odnoszący się *„stricte"* do taktycznych sieci i systemów telekomunikacyjnych jest obszarem „dziewiczym", któremu z naukowego punktu widzenia należy przydać właściwe znaczenie i rangę. Biorąc zatem pod uwagę cytowane stanowisko oraz własne doświadczenia w dziedzinie bezpieczeństwa informacji, które wynikają z realizowanych na niwie służbowej zadań autor, uważa, że zasadne jest podjęcie tematu o następującym brzmieniu:

„Bezpieczeństwo informacji w sieci teletransmisyjnej dywizji zmechanizowanej".

Intencją autora niniejszej dysertacji jest przedstawienie zarówno zagrożeń dla bezpieczeństwa informacji w sieci teletransmisyjnej dywizji zmechanizowanej, jak również przedsięwzięć organizacyjno-eksploatacyjnych i technicznych, które w myśl

---

[5] J. Michniak, A. Wisz, Bezpieczeństwo i ochrona informacji w wojskowych sieciach telekomunikacyjnych i zautomatyzowanych systemach dowodzenia, AON, Warszawa 2000; P. Sienkiewicz, A. Dańczak, Bezpieczeństwo informacji w SZ RP – aspekty strategiczne. Praca studyjna, AON, Warszawa 2002

aktualnie obowiązujących narodowych i sojuszniczych aktów normatywnych przeciwdziałają tym zagrożeniom. Analiza prawidłowości ich wdrożenia do systemu ochrony pozwoli bowiem na dokonanie oceny bezpieczeństwa informacji w sieci teletransmisyjnej w świetle wymagań zawartych w dokumentach normatywnych.

Określenie głównego celu dysertacji dla tak sformułowanego jej tytułu przyczyniło się do określenia struktury pracy, która obejmuje wstęp, pięć rozdziałów oraz zakończenie.

We wstępie zawarto wprowadzenie w problematykę dysertacji oraz uzasadnienie wyboru tematu wraz z konstrukcją opracowania pisarskiego pracy.

Rozdział pierwszy – metodologiczny poświęcony został założeniom leżącym u podstaw wyboru i aspektów prowadzonych badań. Przedstawia ponadto przyjętą na potrzeby niniejszej dysertacji procedurę badawczą.

W rozdziale drugim – identyfikującym, zaprezentowano różne podejścia i interpretacje pojęcia polowego systemu łączności, sieci telekomunikacyjnej, które umożliwiły autorowi przyjęcie definicji sieci teletransmisyjnej dywizji zmechanizowanej w czasie działań taktycznych.

Rozdział trzeci przedstawia wyniki uzyskane w procesie badania narodowych i sojuszniczych aktów prawnych oraz dokumentów normatywnych określających wymagania w zakresie bezpieczeństwa informacji w sieci teletransmisyjnej na szczeblu dywizji zmechanizowanej.

W rozdziale czwartym zaprezentowano naukowe podejście do koncepcji podziału zagrożeń oraz zawarto wyniki badań, które pozwoliły autorowi na określenie stopnia ich istotności w odniesieniu do rozpatrywanego w ramach pracy obszaru problemowego.

Rozdział piąty stanowi zwarty zapis koncepcji przedsięwzięć organizacyjno-eksploatacyjnych i technicznych wchodzących w skład systemu ochrony sieci teletransmisyjnej, których praktyczne zastosowanie w badanych konfiguracjach sieci teletransmisyjnej stanowiło podstawę do przeprowadzenia przez autora oceny bezpieczeństwa informacji w tej sieci na poziomie dywizji zmechanizowanej.

W zakończeniu ujęto wnioski z przeprowadzonych badań oraz zasugerowano ewentualne rozwiązania zidentyfikowanych sytuacji problemowych. Rozważono po-

nadto możliwość wystąpienia nowych zagrożeń dla bezpieczeństwa informacji w sieci teletransmisyjnej wynikających między innymi z postępu technicznego i technologicznego.

1. ZAŁOŻENIA METODOLOGICZNE

1.1. OGÓLNE ZAŁOŻENIE POZNAWCZE ORAZ OBSZAR I PRZEDMIOT BADAŃ

Przekazywanie informacji jest ważnym obszarem procesu dowodzenia[6] i odbywa się pomiędzy osobami funkcyjnymi i zespołami funkcjonalnymi stanowisk dowodzenia w różnym ich usytuowaniu wzajemnym w systemie dowodzenia, w różnych formach, różnymi metodami przekazu i w czasie określonym potrzebami systemu dowodzenia. Wymiana informacji pomiędzy osobami funkcyjnymi systemu dowodzenia jest równoznaczna z istnieniem pomiędzy nimi więzi informacyjnych. Ich charakterystyka prowadzi do określenia postaci i ilości przekazywanych informacji w systemie dowodzenia, co w dalszej kolejności pozwala na określenie niezbędnych potrzeb w zakresie organizacji i funkcjonowania systemu łączności będącego podsystemem systemu dowodzenia.

Powala to wnioskować, że istnieje zatem wymóg posiadania podsystemu przekazywania (transmisji) informacji, który zdolny będzie zapewnić ciągłość, terminowość oraz skrytość jej przesyłania we wszystkich relacjach dowodzenia.

Analizując pojęcie skrytości definiowane[7] jako *uniemożliwienie lub maksymalne utrudnienie przeciwnikowi zrozumienia treści wiadomości przekazywanych przez techniczne środki łączności i informatyki oraz uniemożliwienie wykrycia rejonów rozmieszczenia stanowisk dowodzenia i ich węzłów łączności oraz węzłów telekomunikacyjnych sieci*, można stwierdzić iż wymusza to realizację szeregu przedsięwzięć, których zakres nazywany jest ogólnie systemem ochrony i obrony sieci telekomunikacyjnej każdego szczebla dowodzenia.

Głównym zadaniem tego systemu jest zapewnienie bezpieczeństwa przekazywanych na odległość informacji, ale również urządzeniom, za których pośrednictwem przekaz jest realizowany. Kolejne, nie mniej istotne to fizyczna ochrona elementów dowodzenia i sieci telekomunikacyjnej oraz ich maskowanie.

---

[6] J. Kręcikij, Współczesne kierowanie wojskami. Proces dowodzenia, AON, Warszawa 2002, s. 67

[7] J. Michniak, A. Wisz, Bezpieczeństwo i ochrona informacji w wojskowych sieciach telekomunikacyjnych i zautomatyzowanych systemach dowodzenia, op. cit s. 7

Jeśli jednak system ochrony i obrony rozpatrywany będzie tylko w aspekcie samej informacji, to wówczas można w jego strukturze wyróżnić grupę przedsięwzięć organizacyjno-eksploatacyjnych i technicznych, które w literaturze fachowej i periodykach specjalistycznych nazywane są *bezpieczeństwem informacji*[8].

Obszar i przedsięwzięcia zapewniające bezpieczeństwo informacji stają się tym istotniejsze im rośnie wartość podlegającej ochronie informacji. W przypadku sieci oraz systemów telekomunikacyjnych funkcjonujących w resorcie Obrony Narodowej miernikiem tej wartości jest klauzula tajności[9] informacji. Im wyższa, tym większe obostrzenia i rygory dla sieci, w której są przesyłane.

Niezbędne wymagania bezpieczeństwa informacji w wojskowych sieciach telekomunikacyjnych sprecyzowane i opublikowane zostały w postaci dyrektyw, wytycznych, zaleceń oraz innych dokumentów normatywnych już po wstąpieniu naszego kraju do Organizacji Paktu Północnoatlantyckiego. Stąd też należy sądzić, że wszystkie, lub znamienita ich większość uwzględniają w swoich treściach standardy NATO.

Analizując wymienione powyżej uwarunkowania podczas precyzowania sytuacji problemowej, autor stwierdził, że aktualnie obowiązujące wymagania i związane z nimi przedsięwzięcia w zakresie bezpieczeństwa informacji wymagają głębokiej analizy i oceny stosowanych środków ochrony informacji oraz prawidłowości ich wdrożenia do sieci teletransmisyjnej.

Jeśli chcemy osiągnąć wytyczone cele w postaci oceny bezpieczeństwa informacji w sieciach telekomunikacyjnych szczebla taktycznego to najstosowniejsze wydaje się dokonanie analizy i weryfikacji realizowanych w tym zakresie poszczególnych przedsięwzięć organizacyjno-eksploatacyjnych i technicznych w oparciu o rzeczywistą sieć teletransmisyjną dywizji zmechanizowanej

W dysertacji procesem badawczym objęto sieć teletransmisyjną dywizji zmechanizowanej, która stanowić będzie obszar badań. Przyjęcie sieci teletransmisyjnej szczebla dywizji zmechanizowanej wynika z przeprowadzonej przez autora analizy aktualnych i planowanych struktur organizacyjnych na szczeblu związku taktycznego

---

[8] m.in. R. Bogusz, Bezpieczeństwo przetwarzania informacji: aktywna ochrona przed emisją ujawniającą", IT Security Magazine nr 1-2, 2000

[9] Ochrona informacji niejawnych – zbiór dokumentów normatywnych, Wojskowe Biuro Bezpieczeństwa Łączności i Informatyki, Łączn. Wewn. S4/2002, Warszawa 2002

pod względem organizacji oraz funkcjonowania sieci zapewniających wymianę informacji w relacjach dowodzenia. Oddaje ona bowiem pełne spektrum procesów zachodzących w ramach planowania, organizowania i funkcjonowania systemu przekazywania informacji zgodnego z wymaganiami systemu dowodzenia oraz stanowi doskonały obszar do prowadzenia badań.

W toku precyzowania problemu naukowego przyjęto, że główny przedmiot badań stanowić będzie zespół przedsięwzięć organizacyjno-eksploatacyjnych i technicznych stanowiących o bezpieczeństwie informacji, a w szczególności zagrożenia dla podlegającej ochronie informacji i środki oraz metody im przeciwdziałające.

Wdrożone nowe, zgodne ze standardami NATO, wymagania w zakresie bezpieczeństwa informacji w sieci teletransmisyjnej wymuszają dokonanie analizy prawidłowego działania zastosowanych zgodnie z zaleceniami przedsięwzięć zabezpieczających informację w warunkach działań taktycznych. Wyniki prowadzonej analizy zmierzać powinny do określenia oceny aktualnego stanu bezpieczeństwa informacji w sieci teletransmisyjnej dywizji zmechanizowanej oraz wskazać ewentualne obszary czy przedsięwzięcia, w których należy dokonać zmian lub korekt.

1.2. PROBLEMY BADAWCZE

Zmienione uwarunkowania oraz wymagania wynikające z wprowadzenia nowych lub znowelizowanych dokumentów normatywnych skłaniają do rozważenia, czy zalecane w nich środki, metody i przedsięwzięcia, szczególnie w odniesieniu do sieci teletransmisyjnej dywizji zmechanizowanej zapewniają bezpieczeństwo przesyłania informacji na poziomie wymaganym dla określonej klauzuli tajności.

Problem ten jest na tyle aktualny, że szczególnie w początkowym okresie ich obowiązywania, występowały kłopoty zarówno interpretacyjne, jak i zrozumienia treści niektórych przepisów.

Mając na uwadze określony wcześniej przedmiot badań, a także przedstawioną wyżej sytuację problemową, główny problem badawczy dysertacji został wyrażony w postaci następującego pytania:

Czy lub w jakim stopniu stosowane w sieci teletransmisyjnej dywizji zmechanizowanej, w myśl narodowych i sojuszniczych dokumentów normatywnych, przedsię-

wzięcia organizacyjno-eksploatacyjne i techniczne zapewniają bezpieczeństwo przesyłanej w niej informacji w trakcie prowadzenia przez nią działań taktycznych?

Jako przedsięwzięcia organizacyjno-eksploatacyjne i techniczne autor przyjmuje wszelkie czynności realizowane w następujących obszarach:

- bezpieczeństwo personalne,
- ochrona fizyczna,
- ochrona techniczna,
- ochrona organizacyjno-proceduralna,

które zapewnią lub poprawią poziom bezpieczeństwa informacji w sieci teletransmisyjnej dywizji zmechanizowanej.

Poszukiwanie naukowych rozstrzygnięć w odniesieniu do obszaru i przedmiotu badań oraz określonego głównego problemu badawczego wymagało przyjęcia i rozwiązania szczegółowych problemów badawczych w postaci poniższych pytań problemowych:

1. *Jaka jest aktualna struktura organizacyjno-eksploatacyjna sieci teletransmisyjnej dywizji zmechanizowanej w trakcie prowadzenia działań taktycznych?*
2. *Na jakie zagrożenia narażona jest informacja w sieci teletransmisyjnej dywizji zmechanizowanej?*
3. *Jakie czynniki zewnętrzne i wewnętrzne oraz jakie elementy (parametry) sieci teletransmisyjnej dywizji zmechanizowanej mają wpływ na możliwość ujawnienia informacji przesyłanej w tej sieci?*
4. *Jaki jest aktualny poziom bezpieczeństwa informacji w sieci teletransmisyjnej dywizji zmechanizowanej?*
5. *Czy realizowane w sieci teletransmisyjnej dywizji zmechanizowanej Sił Zbrojnych RP przedsięwzięcia organizacyjno-eksploatacyjne i techniczne w zakresie bezpieczeństwa informacji są zgodne z wymaganiami sojuszniczymi?*
6. *Czy istnieje konieczność wprowadzenia nowych przedsięwzięć w celu utrzymania lub podniesienia poziomu bezpieczeństwa informacji w sieci teletransmisyjnej dywizji zmechanizowanej?*

7. *Jakie potencjalne zagrożenia dla bezpieczeństwa informacji wynikają z potrzeb dowodzenia i kierunków rozwojowych sieci teletransmisyjnej szczebla taktycznego?*

Wymienione poszczególne problemy cząstkowe stanowią pochodną problemu głównego i dotyczą zasadniczych elementów szerokiego spektrum zagadnień wchodzących w skład bezpieczeństwa informacji w sieci teletransmisyjnej dywizji.

1.3. CELE BADAWCZE I HIPOTEZA ROBOCZA

Ogólna wymiana opinii, poglądów autora z pracownikami pionów bezpieczeństwa łączności i informatyki różnego szczebla dowodzenia wojsk lądowych oraz wstępne studiowanie narodowych i sojuszniczych dokumentów normatywnych legło u podstaw przeprowadzenia badań i opracowania ich wyników w formie dysertacji. Jednocześnie zamiarem autora było prawidłowe zorganizowanie procesu naukowego poznania, które umożliwi osiągnięcie wyznaczonego celu badań.

Systematyzując układ pracy, który umożliwiłby osiągnięcie głównego problemu badawczego niniejszej dysertacji przyjęto określoną chronologię postępowania. Sprowadza się ona do udzielenia odpowiedzi na pytania w następujących aspektach:

1. Faktograficznym – jakie aktualne wymagania i wynikające z nich przedsięwzięcia zapewniają bezpieczeństwo informacji w sieci teletransmisyjnej dywizji zmechanizowanej?
2. Diagnostycznym - jakie czynniki (zagrożenia) wpływają na konieczność ich zastosowania?
3. Prognostycznym – czy wymagają one udoskonalenia bądź modyfikacji?
4. Praktycznym – co należy zmienić lub poprawić, aby informacja w sieci teletransmisyjnej uznana była za bezpieczną?

Te elementy stanowiły podstawę do sprecyzowania głównego celu badawczego, którym jest:

Określenie aktualnego poziomu bezpieczeństwa oraz na tej podstawie zdefiniowanie niezbędnych przedsięwzięć organizacyjno-eksploatacyjnych zapewniających bezpieczeństwo informacji w sieci teletransmisyjnej dywizji zmechanizowanej w cza-

sie prowadzenia działań taktycznych przy uwzględnieniu wymagań narodowych i sojuszniczych w tej dziedzinie.

Tak sformułowany cel główny determinował określenie szeregu celów cząstkowych mających umożliwić jego osiągnięcie. Cele te sprecyzowano następująco:

1. *Identyfikacja elementów struktury organizacyjno-funkcjonalnej sieci teletransmisyjnej dywizji zmechanizowanej pod kątem spełnienia przez nią wymagań bezpieczeństwa informacji w działaniach taktycznych.*
2. *Określenie oraz analiza występujących w sieci teletransmisyjnej dywizji zmechanizowanej rodzajów zagrożeń w aspekcie bezpiecznego przesyłania informacji w trakcie prowadzenia działań taktycznych.*
3. *Wyodrębnienie elementów sieci teletransmisyjnej dywizji zmechanizowanej mających wpływ na bezpieczeństwo informacji .*
4. *Określenie aktualnego poziomu bezpieczeństwa informacji w sieci teletransmisyjnej dywizji zmechanizowanej w działaniach taktycznych.*
5. *Wypracowanie wymagań i standardów w zakresie bezpieczeństwa informacji w sieci teletransmisyjnej dywizji zmechanizowanej.*
6. *Przedstawienie koncepcji potrzeb organizacyjno-eksploatacyjnych niezbędnych do zapewnienia wymaganego poziomu bezpieczeństwa informacji przesyłanej w sieci teletransmisyjnej dywizji zmechanizowanej.*
7. *Zaprezentowanie koncepcji przedsięwzięć organizacyjno-eksploatacyjnych zapewniających wymagane bezpieczeństwo informacji w sieci teletransmisyjnej dywizji zmechanizowanej.*

Wynikiem prowadzonej przez autora analizy dokumentów normatywnych[10], obserwacji pośredniej i bezpośredniej organizowanych przedsięwzięć w zakresie bezpieczeństwa informacji[11] w sieci teletransmisyjnej dywizji zmechanizowanej oraz zebrane wnioski wynikające z badania poglądów ekspertów[12] uzyskane podczas udziału w pracach badawczych, seminariach, konferencjach naukowych pozwoliły na przyjęcie oraz sformułowanie hipotezy roboczej, która w toku prowadzenia badań podlegała weryfikacji. Jej istota i zasadnicze znaczenie można określić następującym stwierdzeniem:

---

[10] Patrz bibliografia – dokumenty normatywne.
[11] M. Bryczkowski, „Bezpieczeństwo systemów sieciowych", magazyn Postępy Kryminalistyki nr 1, 1997, s. 12
[12] Patrz – załącznik nr 5

Analiza aktualnego bezpieczeństwa informacji w sieci teletransmisyjnej dywizji zmechanizowanej w trakcie prowadzenia przez nią działań taktycznych stanie się podstawą określenia i wypracowania nowych jakościowo rozwiązań oraz przedsięwzięć organizacyjno-eksploatacyjnych polegających na spełnieniu wymagań narodowych oraz sojuszniczych w takich obszarach jak:

- *bezpieczeństwo personalne;*
- *ochrona fizyczna;*
- *ochrona techniczna;*
- *ochrona organizacyjno-proceduralna;*

w celu wyeliminowania niekontrolowanego „wypływu" informacji z tej sieci i tym samym podniesienie poziomu ochrony informacji przy jednoczesnym spełnieniu wymagań sojuszniczych.

Zasadniczym zadaniem postawionym sobie przez autora rozprawy, stosownie do przyjętej hipotezy roboczej, było takie przeprowadzenie badań, aby ich wyniki pozwoliły na ocenę aktualnego bezpieczeństwa informacji oraz wskazanie tych przedsięwzięć organizacyjno-eksploatacyjnych i technicznych, których modyfikacja pozwoliłaby na podniesienie poziomu ochrony informacji w sieci teletransmisyjnej dywizji zmechanizowanej i jednocześnie ograniczałaby potencjalną możliwość utraty kontroli podczas jej przesyłania.

1.4. METODY BADAWCZE I TEREN BADAŃ

Wieloaspektowość oraz pewna ograniczona liczba płaszczyzn poddanych rozważaniom problemów badawczych w znacznym stopniu determinowała dobór zarówno empirycznych jak i teoretycznych metod badawczych[13]. Ich zastosowanie na wszystkich etapach prac badawczych, w stosunku do uzyskanych pierwotnych i wtórnych materiałów badawczych w zakresie poszczególnych problemów naukowych, umożliwiło systemową identyfikację poszczególnych elementów przedmiotu oraz założonego celu badań, w tym związków i zależności pomiędzy nimi oraz otoczeniem.

[13] E. Wiśniewski, Metodyka wojskowych badań naukowych, AON, Warszawa 1998. cz. 1, s. 43

W toku procesu badawczego stosowano metody empiryczne[14] takie jak:

1. Sondaż diagnostyczny.
2. Obserwacji niestandaryzowanej.
3. Badanie dokumentów.

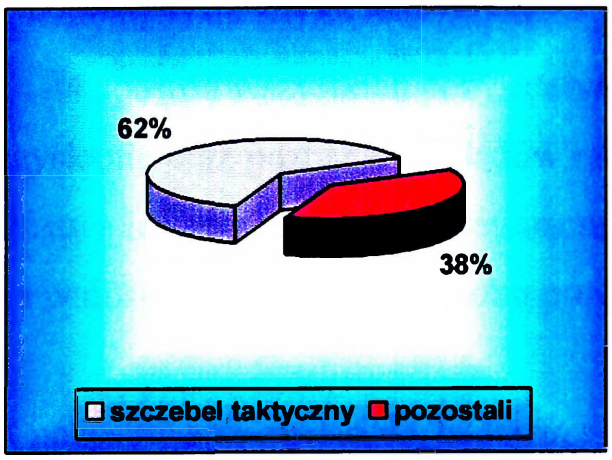
Stosując metodę sondażu diagnostycznego, autor prowadził badania prowadził zarówno techniką ankiety jak i wywiadu.

W ramach badań empirycznych prowadzonych techniką ankiety (kwestionariusz ankiety) zebrano opinie etatowego personelu bezpieczeństwa łączności i informatyki szczebla taktycznego (dywizja, brygada) oraz Oddziału Bezpieczeństwa Łączności i Informatyki Dowództwa Wojsk Lądowych, Centrum Analiz Kryptograficznych i Bezpieczeństwa Teleinformacyjnego i Wojskowego Biura Bezpieczeństwa Łączności i Informatyki w zakresie oceny stopnia istotności występujących w sieci teletransmisyjnej zagrożeń dla bezpieczeństwa informacji. Badaniami objęto 71 żołnierzy zawodowych, co stanowi około 65 % stanu etatowego wymienionych powyżej jednostek organizacyjnych. W celu uwiarygodnienia uzyskanych wyników w stosunku do respondentów narzucono pewne ograniczenia, które winny umożliwić uzyskanie ocen jak najbardziej zbliżonych do rzeczywistości w zakresie zagrożeń bezpieczeństwa informacji w polowych systemach telekomunikacyjnych wojsk lądowych. Do ograniczeń powyższych możemy zaliczyć:

- respondent jest etatowym pracownikiem organów bezpieczeństwa łączności i informatyki szczebla taktycznego wojsk lądowych;
- jego staż pracy w tych strukturach wynosi minimum 3 lata;
- posiada doświadczenia w zakresie zasad organizacji bezpiecznego systemu (sieci), które wynika z udziału w ćwiczeniach lub treningach sztabowych z udziałem i bez udziału wojsk (minimum 2-krotnego).

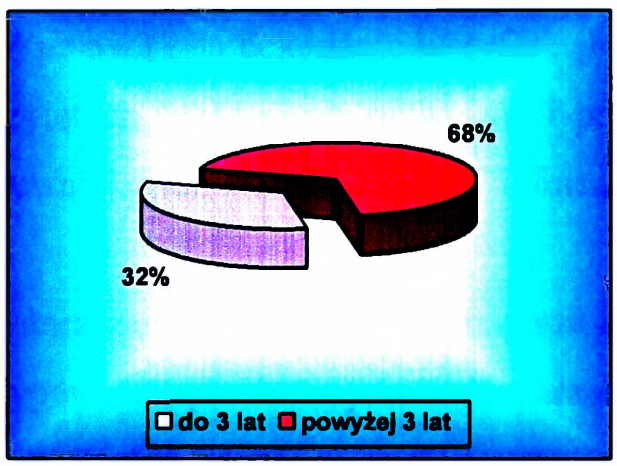
Charakterystykę respondentów objętych badaniami, uwzględniającą narzucone ograniczenia przedstawiono poniżej (rys. 1.4.1, 1.4.2, 1.4.3).

[14] M. Cieślarczyk, P. Krawczyk, Z. Korulczyk, Poradnik metodyczny autorów prac kwalifikacyjnych, WWLiOP AON, Warszawa 2002, s. 72-73



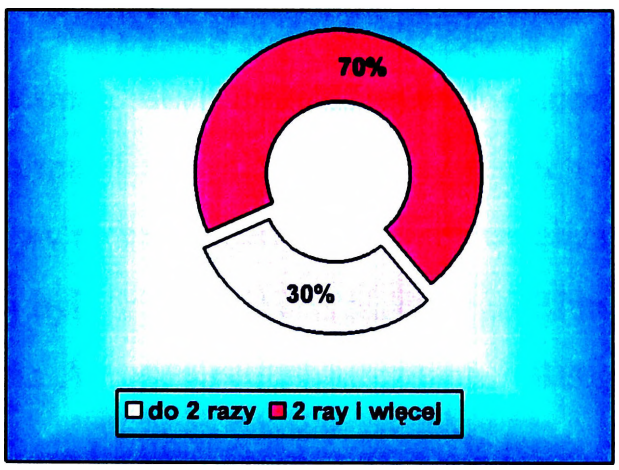
Rys. 1.4.1 Charakterystyka stanowiska służbowego respondentów

Źródło: opracowanie własne na podstawie badań metodą sondażu diagnostycznego techniką ankiety - załącznik nr 4



Rys. 1.4.2 Charakterystyka stażu służbowego w organach bezpieczeństwa respondentów

Źródło: opracowanie własne na podstawie badań metodą sondażu diagnostycznego techniką ankiety - załącznik nr 4



Rys. 1.4.3 Charakterystyka udziału respondentów w ćwiczeniach lub treningach sztabowych z udziałem i bez udziału wojsk

Źródło: opracowanie własne na podstawie badań metodą sondażu diagnostycznego techniką ankiety - załącznik nr 4

Biorąc pod uwagę wymagania narzucone respondentom, autor w toku dalszych badań uwzględnił tylko 44 spośród wszystkich pozyskanych ankiet. Celem zastosowania tej techniki było uzyskanie oraz poznanie poglądów respondentów na problematykę zagrożeń bezpieczeństwa informacji w sieci teletransmisyjnej dywizji zmechanizowanej oraz weryfikacja wniosków uzyskanych w toku prowadzonych badań teoretycznych.

Znaczące źródło pozyskiwania materiału badawczego stanowił sondaż diagnostyczny prowadzony techniką wywiadu[15] eksperckiego (załącznik nr 5), w którym narzędziem był kwestionariusz wywiadu. Celem zastosowania tej metody było poznanie poglądów oraz opinii na zasadnicze problemy związane z bezpieczeństwem informacji. Uzyskany materiał pozwolił na dokonanie weryfikacji poprawności wnioskowania autora w zakresie przyjętych przez niego rozwiązań i przedsięwzięć organizacyjno-eksploatacyjnych zapewniających bezpieczeństwo informacji w sieci teletransmisyjnej.

Przyjęte przez autora założenie, że sondaż diagnostyczny techniką wywiadu będzie miał charakter typowo ekspercki, wymuszało narzucenie potencjalnym respondentom szeregu ograniczeń, do których zaliczyć można:

- długoletni (min. 10 lat) staż pracy na stanowiskach związanych z ochroną informacji niejawnych w sieciach i systemach telekomunikacyjnych;
- kierowanie i odpowiedzialność za organizację przedsięwzięć bezpieczeństwa informacji co najmniej na szczeblu dywizji;
- współudział w opracowywaniu dokumentów normatywnych z zakresu bezpieczeństwa informacji w wojskowych systemach łączności i informatyki lub sprawczy wpływ na przeprowadzenie ich nowelizacji.

Pod uwagę brani byli pracownicy Wojskowego Biura Bezpieczeństwa Łączności i Informatyki, Centrum Analiz Kryptograficznych i Bezpieczeństwa Teleinformacyjnego, Zarządu Łączności i Informatyki Sztabu Generalnego, Dowództwa Wojsk Lądowych, Instytutu Dowodzenia Wydziału Wojsk Lądowych AON oraz komórek odpowiedzialnych za bezpieczeństwo informacji na szczeblu dywizji. Założone warunki spełniało blisko 10 osób, lecz tylko dwie z nich wyraziły chęć udziału w procesie ba-

[15] Cz. Kupisiewicz, Podstawy dydaktyki ogólnej, PWN, Warszawa 1976, s. 31.

dawczym. Ich opinie i twierdzenia nie rzutowały więc w sposób znaczący na wyprowadzone przez autora oceny i wnioski wynikające z procesu badań.

W toku zasadniczego etapu prac badawczych zastosowano obserwację techniką zewnętrzną przy użyciu narzędzia, jakim był arkusz obserwacji (załącznik nr 3).

Obserwację zewnętrzną zastosowano do badania wybranych problemów badawczych, szczególnie struktury organizacyjnej oraz funkcjonowania sieci teletransmisyjnej dywizji zmechanizowanej i procesu planowania przedsięwzięć związanych z ochroną informacji. Metoda obserwacji umożliwiła rozpoznanie, wyróżnienie i ocenę sieci teletransmisyjnej dywizji oraz procesów w niej zachodzących. W jej ramach zbierano głównie wiadomości z zakresu funkcjonalności sieci, jej elementów składowych, które potencjalnie stanowią źródła niekontrolowanego (nieautoryzowanego) wypływu informacji podlegającej ochronie. Metoda ta pozwoliła również na:

- poznanie relacji i powiązań zachodzących między elementami badanego systemu a otoczeniem;
- kompleksowe ujęcie wszystkich elementów zachodzących procesów i występujących między nimi powiązań i zależności;
- ukierunkowanie działalności badawczej przy opracowywaniu oceny bezpieczeństwa informacji w sieci teletransmisyjnej dywizji zmechanizowanej.

Przedmiot obserwacji w kontekście rozważanych problemów stanowiły następujące ćwiczenia i treningi dowódczo-sztabowe (z udziałem i bez udziału wojsk), które opatrzone zostały kryptonimami: „Opal 99"; „Akademicki Pierścień 2003"; „Donośna Surma 2003"; „Jantar 2004"; „Odra 2004" oraz sieć teletransmisyjna dywizji wielonarodowej biorącej udział w misji stabilizacyjnej PKW w Iraku[16].

Metoda badania dokumentów polegająca na analizie i ocenie dostępnej literatury oraz obowiązujących normatywów umożliwiła autorowi zdefiniowanie standardów oraz wymagań narodowych i sojuszniczych w zakresie bezpieczeństwa informacji, które stanowiły podstawę realizacji głównego celu niniejszej dysertacji.

Reasumując, zastosowanie metod empirycznych zapewniło pozyskanie niezbędnej informacji i wiedzy, która pozwoliła:

---

[16] Organizacja i funkcjonowanie sieci teletransmisyjnej rozwiniętej w Iraku były m.in. przedstawiane w ramach konferencji międzynarodowej zorganizowanej przez Instytut Zarządzania i Dowodzenia „Łączność w operacjach reagowania kryzysowego" w październiku 2003r.

- określić strukturę organizacyjno-eksploatacyjną sieci teletransmisyjnej dywizji zmechanizowanej w działaniach taktycznych;
- precyzyjnie określić wymagania oraz zagrożenia w zakresie bezpieczeństwa informacji w sieci teletransmisyjnej dywizji zmechanizowanej;
- wyodrębnić te elementy sieci teletransmisyjnej, które są wrażliwe i mogą stać się punktami niekontrolowanego (nieplanowanego) ujawnienia przekazywanej w sieci informacji;
- ustalić przedsięwzięcia organizacyjno-eksploatacyjne eliminujące zdefiniowane zagrożenia oraz czynniki wpływające na poziom bezpieczeństwa informacji w strukturze sieci teletransmisyjnej dywizji zmechanizowanej w zależności od warunków prowadzenia działań taktycznych;
- określić potencjalne kierunki rozwoju sieci teletransmisyjnej wynikające z potrzeb dowodzenia oraz związanych z tym przedsięwzięć organizacyjno-eksploatacyjnych w zakresie zapewnienia bezpieczeństwa przesyłanym informacjom.

Metody teoretyczne (analiza, wnioskowanie, definiowanie, synteza, porównanie, analogia i uogólnienie) stosowane były we wszystkich etapach badań, szczególnie w okresie poprzedzającym badania właściwe, a także w etapie końcowym.

Analiza oraz wnioskowanie stanowiły uzupełnienie badania dokumentów dotyczących problematyki polowej sieci teletransmisyjnej szczebla taktycznego oraz związanych z nią przedsięwzięć organizacyjno-eksploatacyjnych i technicznych w zakresie bezpieczeństwa informacji mających celu identyfikację stanu wiedzy i kierunków przeobrażeń w rozpatrywanym obszarze badań. Poszczególne rodzaje analizy (elementarna, przyczynowa, logiczna) stosowano w trakcie prowadzonych badań umożliwiających identyfikację sieci teletransmisyjnej. Rozważaniom poddano jej elementy składowe oraz zachodzące między nimi relacje i powiązania, które wpływają z jednej strony na jej strukturę i organizację, z drugiej zaś na szeroko pojmowane aspekty bezpieczeństwa informacji.

Analizie, a następnie wnioskowaniu, poddano następujące problemy:

- strukturę sieci teletransmisyjnej dywizji zmechanizowanej oraz uwarunkowania jej funkcjonowania w działaniach taktycznych;

- wymagania systemów dowodzenia szczebli taktycznych nakładane na sieć teletransmisyjną wraz ze spójnymi z nią wymaganiami w zakresie ochrony informacji;
- struktury wewnętrzne i zewnętrzne więzi informacyjnych zapewniających obieg informacji w sieci teletransmisyjnej dywizji;
- charakter oraz strukturę organizacyjno-funkcjonalną pomocniczego węzła łączności sieci teletransmisyjnej w kontekście elementów mogących przyczynić się do utraty kontroli nad przesyłaną informacją;
- charakter oraz podział zagrożeń bezpieczeństwa informacji w sieci;
- przedsięwzięcia zapewniające przeciwdziałanie zagrożeniom informacji stanowiącym o jej bezpieczeństwie;
- możliwe i niezbędne kierunki zmian w organizacji i strukturze przedsięwzięć zapewniających bezpieczeństwo informacji.

Nieodłącznym elementem tej metody w trakcie prowadzonego procesu badawczego było zamieszczanie po każdym rozdziale dysertacji wniosków. Jednak biorąc pod uwagę kryteria rodzaju zadań stanowiących przesłanki oraz zdań będących konkluzjami, wnioskowanie (zawodne) realizowane było głównie przez analogię.

Definiowanie wykorzystano na początku badań, szczególnie przy formułowaniu definicji sieci teletransmisyjnej, zagrożeń dla bezpieczeństwa informacji i innych.

Analogię stosowano zwłaszcza przy formułowaniu wniosków o występujących podobieństwach.

Synteza pozwoliła połączyć w jedną całość podlegające analitycznemu badaniu elementy składowe sieci teletransmisyjnej, które będą uwzględniały uzyskane w wyniku analizy wnioski w zakresie zastosowania niezbędnych przedsięwzięć organizacyjno-eksploatacyjnych zapewniających spełnienie wymagań w zakresie bezpieczeństwa informacji w sieci teletransmisyjnej dywizji zmechanizowanej (synteza przyczynowa).

Na wszystkich etapach prac badawczych używano porównania, którego istotą była identyfikacja cech wspólnych, podobieństw oraz różnic poszczególnych zagadnień badawczych, zwłaszcza w zakresie rozwiązań funkcjonujących w procesie określania struktur sieci i interpretacji pojęć i przedsięwzięć bezpieczeństwa informacji.

Uogólnienie wykorzystane zostało w trakcie badań do ujawnienia cech i zjawisk powtarzalnych, a przez to do formułowania zasad uniwersalnych dotyczących problematyki organizacji bezpieczeństwa informacji w polowych sieciach i systemach łączności i informatyki.

1.5. ORGANIZACJA I PRZEBIEG BADAŃ

Przyjęty przedmiot badań wzbogacony o dotychczasową wiedzę oraz nakreślone założenia poznawcze zadecydowały o przyjęciu określonej struktury, organizacji i przebiegu badań, które zapewniłyby osiągnięcie zamierzonego celu w postaci rozwiązania głównego problemu badawczego oraz wyszczególnionych problemów cząstkowych.

Wymienione determinanty przyczyniły się do prowadzenia naukowych rozstrzygnięć w ramach trzyetapowego procesu badawczego (rys. 1.5.1).

Etap pierwszy nazywany również wstępnym można scharakteryzować jako pojawienie się potrzeby rozwiązania problemu. Innymi słowy jest to identyfikacja oraz sprecyzowanie problemu wymagającego zastosowania rozwiązań naukowych.

Wyniki prowadzonych wstępnych badań naukowych i analiza literatury oraz dokumentów normatywnych obejmujących przyjęty obszar i przedmiot dociekań naukowych pozwoliły na określenie zasadniczego celu badań oraz celów cząstkowych będących jego implikacją. Pozwoliło to jednocześnie na dokładniejsze, w miarę szczegółowe, sporządzenie koncepcji organizacji i przebiegu badań właściwych.

Pełnemu usystematyzowaniu wiedzy w rozpatrywanym obszarze dociekań służyło gromadzenie i bardzo uważne studiowanie dostępnej literatury przedmiotu, dokumentów normatywnych oraz aktów prawnych. Pozwoliło to autorowi na pełniejszą identyfikację wpływających oraz zachodzących w przedmiocie badań procesów i zjawisk. Szczególną uwagę zwrócono na te opracowania, które umożliwiały wyodrębnienie i scharakteryzowanie występujących podstawowych pojęć oraz definiujące narodowe, a także sojusznicze standardy i wymagania w kontekście przedmiotu i podmiotu badań.



Rys. 1.5.1 Przebieg procesu badawczego

Źródło: opracowano na podstawie J. Pieter, „Zarys metodologii pracy naukowej", PWN, Warszawa 1975

Określeniu stanu faktycznego w zakresie oceny stanu bezpieczeństwa informacji służyła analiza aktów prawnych i normatywów regulujących organizację wszystkich przedsięwzięć realizowanych dla zapewnienia ochrony informacji. Wnioski otrzymane podczas analizy oraz syntezy tych opracowań, aktów i dokumentów normatywnych posłużyły do poszukiwania porównań i analogii w rozwiązywaniu poszczególnych problemów badawczych.

W ten sposób zgromadzony wtórny materiał badawczy stanowił podstawę do sformułowania hipotezy roboczej.

Podczas studiowania literatury poddano również analizie opracowania w przedmiocie metodologii badań naukowych. Tak pozyskana wiedza dała początek drugiemu etapowi prac badawczych, w ramach którego dokonano doboru metod badawczych, właściwych dla poszczególnych problemów naukowych oraz zorganizowano i przeprowadzono dalsze badania teoretyczne i empiryczne. Szczególną uwagę, na tym etapie, poświęcono gromadzeniu, selekcji materiału badawczego oraz opracowaniu wyników otrzymanych w toku badań. Uzyskane rezultaty prowadzonych prac badawczych stanowiły podstawę do naukowych rozstrzygnięć zmierzających do weryfikacji hipotezy roboczej, a zwłaszcza jej naukowego uzasadnienia.

Trzeci, końcowy etap prac badawczych, polegał na zebraniu wszystkich uzyskanych wyników w trakcie przeprowadzonych dotychczas badań w jeden zintegrowany i całościowo spójny zbiór, co umożliwiło ich logiczne uogólnienie oraz systematyzację.

Przedstawiona powyżej struktura i chronologia działań miały na celu przyjęcie przejrzystego układu prezentacji wyników badań w formie rozprawy naukowej.

2. UWARUNKOWANIA TAKTYCZNE I ORGANIZACYJNO-TECHNICZNE FUNKCJONOWANIA SIECI TELETRANSMISYJNEJ DYWIZJI ZMECHANIZOWANEJ

Temat niniejszej dysertacji ***„Bezpieczeństwo informacji w sieci teletransmisyjnej dywizji zmechanizowanej"***, wymusza, zdaniem autora, przedstawienie usytuowania – roli i miejsca, a następnie samego pojęcia ***sieci teletransmisyjnej*** na poziomie dywizji zmechanizowanej, które podlegać będzie analizie oraz jednocześnie stanowić ma obszar badań w aspekcie bezpieczeństwa informacji w niej przesyłanej.

Sieć teletransmisyjna na poziomie dywizji zmechanizowanej jest jednym z podstawowych elementów wojskowego polowego systemu telekomunikacyjnego. Struktura organizacyjna i funkcjonalna wojskowego polowego systemu telekomunikacyjnego jest zróżnicowana zarówno w kontekście uwarunkowań taktycznych (np. realizowanych zadań – natarcie, obrona, itd.), jak również w podejściu naukowym o czym mogą świadczyć odbiegające od siebie stanowiska niektórych znawców problemu.

Zatem przed przystąpieniem do rozpatrywania problemu podstawowego, zasadne wydaje się przedstawienie oraz krótkie scharakteryzowanie działań taktycznych, jakie w myśl obowiązujących dokumentów normatywnych, wyników badań naukowych oraz doświadczeń wynikających z działania wojsk lądowych w ramach misji pokojowych lub stabilizacyjnych prowadzi lub może prowadzić dywizja zmechanizowana. Towarzyszyć temu będzie wyodrębnienie tych elementów, które determinują oraz w sposób zasadniczy wpływają na proces planowania, organizacji i eksploatacji sieci teletransmisyjnej dywizji, przy jednoczesnym określeniu czynników mających znaczenie dla zapewnienia bezpieczeństwa przesyłanej w niej informacji.

2.1. IDENTYFIKACJA UWARUNKOWAŃ WYNIKAJĄCYCH Z RODZAJU DZIAŁAŃ TAKTYCZNYCH DYWIZJI ZMECHANIZOWANEJ

Dywizja zmechanizowana występująca w tytule dysertacji może prowadzić działania taktyczne lub uczestniczyć w nich. Obejmują one wszelkie działania pododdziałów, oddziałów i związków taktycznych wojsk operacyjnych mające na celu efektywne wykorzystanie ich możliwości bojowych[17].

Podstawowym czynnikiem, wpływającym na podjęcie lub zaniechanie przez dywizję zmechanizowaną jakichkolwiek działań jest zadanie[18] otrzymane od przełożonego. Zadanie to otrzymane w formie rozkazu operacyjnego określa jednoznacznie cel działania, pas odpowiedzialności, ramy czasowe, siły i możliwości wojsk przeciwnika i rodzaj działań taktycznych, które dywizja ma wykonać, jak również stanowi bodziec dający sygnał do rozpoczęcia przedsięwzięć wchodzących w skład procesu dowodzenia[19] .

W tym kontekście rozkaz operacyjny traktować można zatem jako *określenie zadań dla podwładnych, innych elementów zabezpieczających oraz wsparcia działań, pośród których wyróżniana jest organizacja i struktura sieci dowodzenia rozumianej jako sieć łączności zapewniającej wymuszony obieg informacji w zaplanowanych i zorganizowanych relacjach dowodzenia*[20].

Sieć łączności i jej elementy składowe, w ramach której planowana, a następnie organizowana jest sieć teletransmisyjna dywizji zmechanizowanej podlega szeregowi determinantów wynikających z czynników zarówno wewnętrznych jak i zewnętrznych, do których jako zasadnicze zalicza się:

- możliwości oddziaływania sił przeciwnika na sieci telekomunikacyjne wojsk własnych;

---

[17] M. Huzarski i inni, Aspekty narodowe i sojusznicze w teorii taktyki ogólnej wojsk lądowych pk. „Garda", AON, Warszawa 2000, s. 18

[18] J. Kręcikij, Współczesne kierowanie wojskami. Proces dowodzenia, AON, Warszawa 2002, s. 79

[19] Proces dowodzenia przyjmowany jest jako proces informacyjno-decyzyjny realizowany w cyklach decyzyjnych przez dowództwa rozmieszczone w sieci stanowisk dowodzenia, polegający na cyklicznym zbieraniu i opracowywaniu informacji, a następnie ich przetwarzanie w informacje decyzyjne, które w formie zadania doprowadza się do wykonawców – J. Michniak, Dowodzenie i łączność, AON, Warszawa 2004, s. 24

[20] M. Strzoda, N. Prusiński, System dowodzenia. Terminologia cz. 1, AON, Warszawa 2002

- rodzaj prowadzonych działań taktycznych i przyjęte ugrupowanie bojowe dywizji;
- przydzielony pas odpowiedzialności;
- ukształtowanie i charakter terenu prowadzonych działań;
- możliwości techniczne środków transmisyjnych.

Odnosząc się do pierwszego z wyszczególnionych determinantów oraz uwzględniając uwarunkowania współczesnego pola walki i wymagania systemu dowodzenia, możemy stwierdzić, iż współczesna sieć teletransmisyjna winna charakteryzować się odpornością na oddziaływanie zarówno ogniowe jak i radioelektroniczne przeciwnika. Ponadto mając na uwadze element zaskoczenia, a także aspekt powodzenia działania dywizji, sieć teletransmisyjna winna cechować się skrytością przekazywania informacji.

Problematyka związana z drugim zasadniczym determinantem tj. rodzajem prowadzonych przez dywizję działań taktycznych jest bardziej złożona i wymaga głębszego rozpatrzenia. Zasadniczo w literaturze przedmiotu oraz w aktualnie obowiązującym „Regulaminie działań wojsk lądowych" spotykamy następującą klasyfikację działań taktycznych (załącznik nr 1):

- rozstrzygające,
- pomocnicze,
- pokojowe.

Przyjęcie i wprowadzenie powyższej klasyfikacji jest następstwem analizy dokumentów normatywnych i myśli naukowej głównych krajów Organizacji Paktu Północnoatlantyckiego (szczególnie armii Niemiec) oraz drugiego aspektu - zobowiązań naszego państwa wynikających z członkostwa w Organizacji Narodów Zjednoczonych i związanego z tym udziału naszych wojsk w misjach pokojowych.

Główną kategorią rozstrzygających działań taktycznych jest walka stanowiąca zorganizowane w czasie i przestrzeni bezpośrednie fizyczne i informacyjne oddziaływanie na przeciwnika[21].

[21] M. Huzarski i inni, Taktyka ogólna wojsk lądowych, AON, Warszawa 2001, s. 45

Do niedawna wyróżniano dwa[22] podstawowe rodzaje walki tj. obronę i natarcie. Aktualne poglądy, prezentowane w najnowszych publikacjach[23] poświęconych rozważaniom z zakresu taktyki i działań taktycznych, dodają jeszcze działania opóźniające.

Obecnie obowiązujące poglądy doktrynalne (wynikające z przyjętej doktryny obronnej państwa) definiują pojęcie obrony jako *zamierzony lub wymuszony rodzaj walki prowadzonej w celu udaremnienia lub odparcia uderzeń przeciwnika oraz utrzymania zajmowanego w przypadku dywizji pasa obrony*[24]. W ramach obrony przewiduje się ponadto zadanie maksymalnych strat przeciwnikowi celem stworzenia sprzyjających warunków do rozpoczęcia działań zaczepnych, które umożliwiłyby odrzucenie przeciwnika z naszego terytorium lub obszaru bronionego w ramach sojuszu.

Zgodnie z obowiązującą klasyfikacją działań taktycznych natarcie zaliczane jest do rozstrzygających rodzajów walki i prowadzone głównie w formie zwrotów zaczepnych z zamiarem rozbicia wojsk przeciwnika w opanowanym przez niego obszarze oraz odzyskanie zajmowanego terenu. *Istotą natarcia jest zdecydowany ruch wojsk do przodu, do obiektu określonego w zadaniu. Ruch ten wyzwalany jest wszechstronnym rażeniem wojsk przeciwnika*[25].

Wyodrębnienie i zaliczenie działań opóźniających do podstawowych rodzajów walki zostało dokonane w wyniku uwzględnienia wielu przesłanek, w tym zwłaszcza wymagań sojuszniczych. Zaklasyfikowanie tego typu działań budziło i budzi nadal wiele kontrowersji wśród teoretyków walki zarówno rodzimych jak i głównych państw NATO.

Przez działania opóźniające[26] należy rozumieć *szereg starć o charakterze obronnym i zaczepnym z szeroko stosowanym manewrem, których ostatecznym celem jest stworzenie wojskom własnym warunków przejścia do innych działań lub zatrzymanie natarcia przeciwnika*. Działania opóźniające mogą prowadzić samodzielne oddziały jako oddziały wydzielone związków taktycznych, na przedpolu obrony własnej lub w ramach obrony ruchowej tych związków, a także w czasie ich odwrotu.

---

[22] M. Huzarski i inni, Taktyka ogólna..., op. cit. s. 45, M. Huzarski i inni, Aspekty narodowe i ..., op. cit. s. 27
[23] R. Chrobak i inni, Działania bojowe dywizji, AON, Warszawa 2003, M. Huzarski, Zagadnienia taktyki wojsk lądowych, A. Marszałek, Toruń 1999, s. 24
[24] Regulamin DWLąd, Warszawa 1991, s. 78
[25] Regulamin działań WLąd., op. cit. s. 101
[26] Z. Ścibiorek, Działania opóźniające, Warszawa, 1996, s. 14

Działania te umożliwiają niewielkimi siłami, na stosunkowo dużym obszarze, prowadzenie wysoce manewrowej i bardzo aktywnej walki obronnej, co pozwala siłom głównym na realizowanie innych zadań, w tym także na przygotowanie się do podjęcia działań rozstrzygających[27].

W cytowanej dotychczas literaturze przedmiotu oraz w innych publikacjach w ramach walki poza wymienionymi jej podstawowymi rodzajami wyszczególniane są następujące działania:

- aeromobilne,
- specjalne,
- wycofanie,
- informacyjne,
- nieregularne.

Drugim wymienianym rodzajem działań taktycznych są działania pomocnicze, w których strukturze, zarówno w podejściu naukowym jak i doktrynalnym, wyróżniamy przemieszczanie i rozmieszczanie wojsk.

Przemieszczanie oznacza wszelkie ruchy wojsk w skali taktycznej w celu przyjęcia w innym rejonie zamierzonego ugrupowania bojowego lub ześrodkowania sił i środków czyli przemieścić się to nic innego jak zmienić miejsce, zająć inne położenie lub wykonać ruch w inne miejsce[28]. Tak rozumiane pojęcie przemieszczania obejmuje zarówno obszar marszu jak i przewozu, czy też przerzut wojsk.

Kolejnym rodzajem pomocniczych działań taktycznych jest rozmieszczanie, które obejmuje *przebywanie wojsk w garnizonach stałych oraz rejonach ześrodkowania (wyjściowy, odpoczynku, czasowego pobytu), z zachowaniem odpowiedniego stopnia gotowości bojowej*[29].

Ostatnim trzecim, zgodnie z przyjętą klasyfikacją, rodzajem działań taktycznych są działania pokojowe, które są następstwem zmieniającego się charakteru środowiska międzynarodowego objawiającego się stale rosnącą liczbą złożonych, wewnątrzpaństwowych, międzypaństwowych oraz wielostronnych konfliktów politycznych i zbroj-

---

[27] Z. Ścibiorek, W. Lidwa, Działania obronno-opóźniające w przygranicznym pasie przesłaniania, AON, Warszawa 1999, s. 33
[28] W. Lidwa, Przemieszczanie wojsk, AON, Warszawa 1995, s. 5
[29] Regulamin DWLąd. Op. cit., s. 142

nych. Wewnętrzny podział, jak również nazewnictwo tego typu działań taktycznych ,jest bardzo różnorodne. W literaturze przedmiotu[30] najczęściej można je spotkać jako:

- utrzymanie pokoju,
- wymuszanie pokoju,
- rozgradzanie stron,
- działania demonstracyjne,
- działania humanitarne,
- inne.

Przedstawiony powyżej podział i krótka charakterystyka działań taktycznych oraz wyniki badań uzyskane podczas obserwacji zewnętrznej niestandaryzowanej stały się punktem wyjściowym do przeprowadzenia przez autora analizy dokumentacji wybranych, współcześnie prowadzonych ćwiczeń i treningów sztabowych szczebla dywizji zmechanizowanej („Opal 99"; „Akademicki pierścień 2003"; „Donośna surma 2003"; „Jantar 2004"; „Odra 2004") oraz misji stabilizacyjnej realizowanej przez Dywizję Wielonarodową w Iraku w aspekcie rozpatrywanego obszaru, który stanowi o uwarunkowaniach wpływających na planowanie oraz organizację sieci teletransmisyjnej.

Z przeprowadzonej analizy wynika jednoznacznie, że sieć teletransmisyjna jest planowana i w pełni rozwijana tylko i wyłącznie podczas prowadzenia przez dywizję zmechanizowaną rozstrzygających (obrona, natarcie) i pokojowych (misja w Iraku) działań taktycznych. Ten wniosek pozwolił na zawężenie dalszego toku rozważań prowadzonych w ramach dysertacji do wymienionych powyżej działań taktycznych realizowanych przez dywizję zmechanizowaną.

Jednocześnie rezultatem analizy ww. dokumentacji oraz literatury przedmiotu[31] było określenie elementów ugrupowania bojowego dywizji zmechanizowanej prowadzącej podstawowe działania taktyczne:

- stanowiska dowodzenia z ich węzłami łączności,
- pierwszy rzut,

---

[30] m.in. M. Huzarski, Zagadnienia taktyki..., op.cit. s.24, M. Huzarski i inni, Taktyka ogólna..., op. cit. s. 119

[31] m. in. S. Koziej, „Teoria walki zbrojnej", AON, Warszawa 1993, s. 89; Z. Ścibiorek, „Obrona związku taktycznego", AON, Warszawa 1993, s. 123

- odwód,
- zgrupowanie oddziałów artylerii,
- oddziały przeciwlotnicze,
- elementy (system) rozpoznania,
- odwód inżynieryjny,
- odwód przeciwchemiczny,
- elementy logistyczne,
- pomocnicze węzły łączności i odcinki międzywęzłowe linii telekomunikacyjnych.

Elementem pozwalającym na rozróżnienie podstawowych działań taktycznych jest występowanie oddziału zaporowego charakterystycznego tylko dla ugrupowania bojowego tworzonego w ramach obrony.

Potrzeba rozpatrywania ilości poszczególnych elementów ugrupowania bojowego dywizji przy planowaniu sieci teletransmisyjnej wynika bowiem z określenia liczby i charakteru więzi informacyjnych, które niezbędne są do zapewnienia i utrzymania wymaganych relacji rozwijanych w ramach systemu dowodzenia.

Ponadto biorąc pod uwagę, że rozpatrywane rodzaje działań taktycznych wchodzą w skład walki zbrojnej, która na współczesnym polu walki realizowana jest przy *spełnieniu następujących elementarnych czynników jak*: *rażenie, ruch i informacja*[32], to podczas planowania sieci teletransmisyjnej niezbędnie należy uwzględnić również drugi z wymienionych czynników. Ruch bowiem oznacza wszelkie przesunięcia sił oraz środków. Najważniejszymi wskaźnikami w rozpatrywanym kontekście są *odległość i czas przesunięcia oraz ich iloraz, czyli prędkość lub tempo natarcia*[33].

Stąd też przy uwzględnieniu rzeczywistej dynamiki walki i wynikających z niej terminowych zmian rozmieszczenia sił ugrupowania bojowego dywizji, rekonfiguracja pojedynczych elementów lub całej sieci teletransmisyjnej odbywałaby się mniej więcej zgodnie z cyklem przemieszczania stanowisk dowodzenia tj. 4 – 6 h dywizja, 3 – 4 h brygada[34].

---

[32] M. Huzarski i inni, Taktyka ogólna wojsk..., op. cit., s. 24
[33] S. Koziej, Teoria walki zbrojnej, AON, Warszawa 1993, s. 93
[34] Z. Fiołna, P. Daniluk, Koncepcja struktur organizacyjno-technicznych..., op. cit. s. 47

Kolejnym czynnikiem, wynikającym z przeprowadzonej przez autora analizy dokumentacji przywoływanych uprzednio ćwiczeń i treningów sztabowych, mającym wpływ na sposób organizacji sieci teletransmisyjnej jest przestrzenne rozmieszczenie poszczególnych elementów ugrupowania bojowego tworzonych z organicznych oraz przydzielonych oddziałów i pododdziałów dywizji.

Podstawowe działania taktyczne, do których zaliczana jest obrona i natarcie charakteryzowane są przez takie pojęcie jak pas odpowiedzialności[35], w ramach którego wyróżnia się szerokość i głębokość pasa działania dywizji zmechanizowanej.

Z przeprowadzonej analizy literatury przedmiotu pod tym kątem wynika, że zarówno szerokość jak i głębokość pasa działania dywizji zmechanizowanej na przestrzeni ostatnich dziesięcioleci podlegała ciągłym modyfikacjom, polegającym przed wszystkim na zwiększaniu obszaru odpowiedzialności dywizji co obrazuje tabela 2.1.1.

Tabela 2.1.1

Zwiększenie pasa odpowiedzialności dywizji

Wyszczególnienie	II wojna światowa	Wojna koreańska	Lata 70-te	Dywizja 86'	XXI wiek
Szerokość pasa	7 km	21 km	25 km	60 km	120 km
Głębokość pasa	21 km	21 km	70 km	100 km	200 km

Źródło: opracowanie własne na podstawie wykładu J. Michniaka – „System łączności komponentu wojsk lądowych", PSOS, AON, 2004.

Przedstawione powyżej szerokości i głębokości pasa odpowiedzialności dywizji zmechanizowanej można rozpatrywać w dwóch aspektach – historycznym i poglądowym. Historycznym bowiem informacje i dane pochodzą z rzeczywistych wojen, konfliktów i operacji, co pozwala empirycznie stwierdzić - jak było. Aspekt poglądowy nakazuje odpowiedzieć na pytanie: jak jest i co z teraźniejszości wynika dla przyszłych działań taktycznych związku taktycznego szczebla dywizji.

Dokonując porównania cytowanego zestawienia z wnioskami płynącymi z przeprowadzonej analizy dokumentacji wybranych i wcześniej przywoływanych ćwiczeń

[35] Z. Ścibiorek, Obrona związku taktycznego (oddziału), AON, Warszawa 1993, s. 51; Główne problemy natarcia, AON, Warszawa 1993, s. 15

i treningów sztabowych autor stwierdza, że maksymalna szerokość pasa odpowiedzialności w rozpatrywanych przypadkach wynosiła 60 km. Ta sama wielkość odnosi się również do głębokości pasa odpowiedzialności dywizji zmechanizowanej podczas prowadzenia przez nią obu podlegających rozpatrzeniu podstawowych działań taktycznych.

Diametralnie inna sytuacja ma miejsce w przypadku rozpatrywania działań pokojowych realizowanych przez związek taktyczny szczebla dywizji. Tutaj każde działania wykonywane są w różnorodnym i specyficznym dla danego rejonu środowisku. Mają czasami zgoła inny charakter, jak również odmienne ograniczenia czy uwarunkowania realizacji zadania, których w żaden sposób nie da się sparametryzować, tak jak czyni się to w stosunku do rozstrzygających działań taktycznych. Potwierdzeniem tak postawionej tezy niech będzie przykład obszaru odpowiedzialności przydzielonego Dywizji Wielonarodowej w ramach misji stabilizacyjnej w Iraku: jego powierzchnia nie jest liczona w dziesiątkach czy nawet setkach kilometrów kwadratowych, lecz sięga blisko 80000 km^2. Ze względu na niepowtarzalność rozwiązań organizacyjnych, strukturalnych oraz uwarunkowań wymienionych wcześniej, każdy przypadek działań pokojowych musi być traktowany i rozpatrywany indywidualnie.

Korelacja omawianego czynnika przestrzennego (szerokość i głębokość pasa odpowiedzialności dywizji) z ukształtowaniem i rzeźbą terenu działań taktycznych stanowi kolejny determinant, który winien być uwzględniany podczas planowania sieci teletransmisyjnej. Uwarunkowanie powyższe ściśle związane jest z możliwościami techniczno-eksploatacyjnymi wykorzystywanych w ramach sieci urządzeń teletransmisyjnych.

Ze względu na główny problem badawczy – bezpieczeństwo informacji w sieci teletransmisyjnej dywizji zmechanizowanej - obszar zainteresowania zostanie ograniczony do rozstrzygających (podstawowych) oraz pokojowych działań taktycznych. Takie podejście i zawężenie obszaru badań wynika przede wszystkim z faktu, że tylko w trakcie tego typu działań rozwijana jest w pełni sieć telekomunikacyjna dywizji zmechanizowanej, a tym samym jej integralny element – sieć teletransmisyjna, która stanowi kanwę rozważań oraz prowadzenia badań w zakresie bezpieczeństwa informacji. Pozwoli to zatem na rozważenie wszelkich możliwych konfiguracji sieci tele-

transmisyjnej dywizji zmechanizowanej w trakcie prowadzenia przez nią podstawowych działań taktycznych przy optymalnie rozwiniętej sieci telekomunikacyjnej.

Reasumując prowadzone dotychczas rozważania dotyczące uwarunkowań i czynników wpływających na sposób organizacji sieci teletransmisyjnej dywizji zmechanizowanej zaliczyć można do nich następujące parametry przestrzenno-czasowe oraz konfiguracyjne:

- *możliwości rażenia ogniowego i radioelektronicznego wojsk przeciwnika;*
- *liczbę i charakter więzi informacyjnych pomiędzy stanowiskami dowodzenia;*
- *ilość i charakter działania elementów ugrupowania bojowego dywizji zmechanizowanej;*
- *wymagania jakościowe wymiany informacji w poszczególnych relacjach (w tym np. terminowość, wierność i skrytość przekazania informacji);*
- *szerokość i głębokość pasa odpowiedzialności dywizji zmechanizowanej;*
- *możliwości techniczne środków transmisyjnych.*

A zatem można stwierdzić, iż bezpieczeństwo informacji przesyłanej w sieci teletransmisyjnej zawiera się w przedstawionych powyżej wymaganiach jakościowych wymiany informacji.

Jego spełnienie następuje w wyniku realizacji szeregu przedsięwzięć organizacyjno-eksploatacyjnych, które mają na celu zapewnienie atrybutów (cech) bezpieczeństwa informacji[36] takich jak:

- *poufność*,
- *integralność*,
- *dostępność*,
- *rozliczalność,*
- *autentyczność,*
- *niezawodność*.

[36] A. Gałach, K. Szczypiorski , „Bezpieczeństwo systemów teleinformatycznych", CITCOM PW, Warszawa 2002, s. 37

2.2. IDENTYFIKACJA ELEMENTÓW STRUKTURY ORGANIZACYJNO-TECHNICZNEJ POLOWEGO SYSTEMU ŁĄCZNOŚCI DYWIZJI ZMECHANIZOWANEJ

Polowy system łączności dywizji zmechanizowanej traktowany jest jako element składowy systemu dowodzenia na współczesnym obszarze działań z użyciem wojsk i stanowi organizacyjno-techniczny zespół sił i środków łączności oraz informatyki pracujących według ustalonych zasad. Jego rozwinięcie i funkcjonowanie ma na celu zapewnienie dowodzenia wojskami i kierowania środkami walki, co wynika z najbardziej charakterystycznych cech systemu dowodzenia dywizji[37], do których można zaliczyć:

- przetwarzanie i przesyłanie dużej ilości informacji pomiędzy elementami systemu dowodzenia;
- duże odległości pomiędzy elementami systemu dowodzenia;
- przemieszczanie się osób funkcyjnych oraz stałych i doraźnie funkcjonujących stanowisk dowodzenia;
- działania rozpoznawcze przeciwnika mające na celu m.in. zdobycie informacji o systemie dowodzenia;
- celowe destrukcyjne (niszczące lub obezwładniające) ogniowe i radioelektroniczne działanie przeciwnika na organa dowodzenia i elementy systemu łączności.

Wymienione powyżej cechy stanowią determinant wymuszający konieczność stosowania w systemie dywizji urządzeń telekomunikacyjnych, które zapewniają duże zasięgi łączności przy odpowiednio dużej przepustowości poszczególnych relacji w sieci, stosowanie alternatywnych dróg oraz alternatywnych środków technicznych do przesyłania informacji, stosowanie środków zapewniających przekazywanie informacji w trakcie przemieszczania.

Zasadniczym zadaniem realizowanym przez system łączności dywizji zmechanizowanej jest zapewnienie dostarczania aktualnych i wiarygodnych informacji oraz możliwość natychmiastowego, lub w nakazanym terminie, przekazywania podejmowanych decyzji i poleceń wykonawczych do podwładnych oraz wszelkich informacji

[37] J. Janczak, Mobilne sieci łączności – album schematów, AON, Warszawa 2003, str. 26

niezbędnych do realizacji celu operacji (walki), zgodnie z adresem nadanym w punkcie źródłowym.

Prof. J. Michniak zdefiniował *wojskowy polowy system łączności jako zespół elementów w postaci węzłów telekomunikacyjnych, węzłów łączności stanowisk dowodzenia, stacji i samodzielnych urządzeń telekomunikacyjnych oraz pocztowych sprzężonych ze sobą w ściśle określony sposób drogami przesyłowymi wraz z urządzeniami zwielokratniającymi, łączeniowymi, końcowymi, wzmacniakowymi, regenerującymi, łączności specjalnej, sprzętem specjalistycznym i pomocniczym oraz organami kierowania wraz z całą infrastrukturą zabezpieczenia logistycznego i operacyjnego systemu, współpracujący ze sobą według przyjętych zasad*[38].

W literaturze przedmiotu spotkać się można z różnym podejściem do klasyfikacji wewnętrznej i podziału wojskowych polowych systemów łączności. Przykładowo A. Barczak[39] w swojej publikacji wyróżnia w systemie łączności następujące podsystemy:

- podsystem przekazywania informacji;
- podsystem zarządzania (kierowania) systemem łączności;
- podsystem zasilania;
- zabezpieczenia albo wsparcia logistycznego oraz uzupełniania stanu osobowego, zabezpieczenia bojowego i odwodu sił oraz środków.

Kolejne spojrzenie na wojskowy polowy system łączności i informatyki w swojej pracy przedstawia M. Kowalewski[40]. Wyróżnia on bowiem w jego strukturze następujące elementy, takie jak:

- polowe węzły łączności;
- telekomunikacyjne linie łączności (dowiązania, bezpośrednie i międzywęzłowe);
- podsystem lądowej radiokomunikacji ruchomej (LRR);
- podsystem wojskowej poczty polowej (WPP);
- podsystem zasilania (zabezpieczenia);

---

[38] J. Michniak, Kierowanie mobilnymi systemami łączności wojsk lądowych Cz. I Główne problemy, AON, Warszawa 2003, s. 58
[39] A. Barczak i inni, Planowanie systemu łączności, DW Bellona, Warszawa 1999, s. 65
[40] M. Kowalewski, System łączności dywizji, Rozprawa habilitacyjna, AON, Warszawa 1994, s. 164

– podsystem kierowania.

Nieco inne spojrzenie na strukturę funkcjonalną polowego systemu łączności związku taktycznego reprezentuje J. Mazurkiewicz[41], który wyróżnia w nim:

– podsystem kierowania;
– sieć łączności;
– odwód łączności;
– podsystem zabezpieczenia bojowego łączności;
– podsystem zabezpieczenia logistycznego łączności;
– podsystem gotowości bojowej i uzupełnień osobowych łączności.

Tenże autor we wspólnej publikacji z W. Kulmą, wyróżnia podsystem przekazywania informacji rozumiany jako sieć łączności, gdzie sieć łączności związku taktycznego definiowana jest jako *element składający się z następujących rodzajów sieci: telekomunikacyjnej, pocztowej oraz sygnalizacyjnej*[42].

Natomiast prof. J. Michniak[43], wyróżnia (wydziela) następujące elementy systemu łączności:

– elementy kierowania;
– elementy podsystemu przekazywania informacji (sieć łączności) zorganizowane w sieć telekomunikacyjną i sieć pocztową, a na niższych szczeblach dowodzenia także sieci sygnalizacyjne;
– elementy zasilania systemu (zabezpieczenia operacyjnego, zabezpieczenia logistycznego, odwodu łączności).

Zaprezentowane powyżej stanowiska znawców problemu pozwalają zatem autorowi niniejszej dysertacji na wyciągnięcie wniosku, iż tak rozumiany element podsystemu przekazywania informacji, jakim jest ***sieć łączności szczebla dywizji składa się z dwóch oddzielnych (ze względu na sposób przekazywania informacji) lecz wzajemnie uzupełniających się członów (makroskładników):***

– ***sieci telekomunikacyjnej***
– ***sieci poczty polowej.***

---

[41] J. Mazurkiewicz, Leksykon łączności, AON, Warszawa 1996, s. 188
[42] J. Mazurkiewicz , W. Kulma, System dowodzenia i łączności związku taktycznego, op. cit., str. 69
[43] J. Michniak, Kierowanie mobilnymi systemami op. cit., s. 76

Tak pojmowana sieć łączności dywizji powinna zapewnić przekazywanie informacji imperatywnych (zarządzeń, rozkazów i poleceń) i deskryptywnych (meldunków sytuacyjnych, sprawozdań, raportów, opisów oraz wielu innych) według następujących kryteriów podziału[44]:

a) ze względu na treść i obszar merytoryczny, którego dotyczą:
   - operacyjnych (dowodzenia),
   - rozpoznawczych,
   - logistycznych (i innych specjalistycznych),
   - organizacyjnych,
   - pozostałych,

b) ze względu na czas dostarczenia:
   - błyskawicznych,
   - pilnych,
   - zwykłych,

c) ze względu na stopień dostępności dla użytkowników:
   - tajnych,
   - poufnych,
   - zastrzeżonych,
   - jawnych,

d) ze względu na kierunek transmisji w danym węźle (punkcie) sieci:
   - wchodzących,
   - wychodzących,
   - przechodzących (retransmitowanych).

Biorąc za podstawę dalszych rozważań przedstawiony powyżej podział należy przyporządkować do niego w rozpatrywanym w niniejszej dysertacji obszarze definicję sieci telekomunikacyjnej.

Prof. J. Michniak przyjmuje, że *sieć telekomunikacyjna jest to zespół aparatów przetwórczych, linii i stacji transmisyjnych, central komutacyjnych (telefonicznych,*

[44] Z. Fiołna, P. Daniluk, Koncepcja struktur organizacyjno-technicznych taktycznych sieci łączności wojsk lądowych. Struktura organizacyjno-techniczna sieci łączności dywizji, pk. „Kros-2.2", AON, Warszawa 2002, s. 32

telegraficznych, pakietów), radiostacji oraz innych urządzeń telekomunikacyjnych znajdujących się na określonym obszarze, powiązanych ze sobą technicznie i przeznaczonych do świadczenia usług telekomunikacyjnych, w ramach których należy uwzględniać wszystkie urządzenia i linie telekomunikacyjne[45].

Urządzenia telekomunikacyjne[46] w tym ujęciu to urządzenia do przetwarzania zapisu informacji na sygnały, transmisji sygnałów, zestawiania i rozłączania łączy oraz do kontroli powyższych czynności.

W ujęciu prezentowanym przez J. Mazurkiewicza oraz W. Nowickiego sieć telekomunikacyjna traktowana jest jako *zespół funkcjonalnie powiązanych ze sobą urządzeń telekomunikacyjnych, znajdujących się na określonym obszarze i przeznaczonych do świadczenia usług telekomunikacyjnych, różnych lub określonych rodzajów*[47]. W jej strukturze wyróżniają między innymi następujące rodzaje podsystemów:

- teletransmisyjny,
- telekomutacyjny,
- telefoniczny,
- radiokomunikacyjny,
- telegraficzny,
- teledacyjny,
- teleinformatyczny,
- telemetryczny,
- telewizyjny.

Odmienny pogląd na wewnętrzną strukturę sieci telekomunikacyjnej (rys. 2.2.1) ma J. Janczak[48], który w jej składzie wyróżnia:

- sieć radioliniowo-kablową,
- sieć radiodostępu.
- sieci radiowe pola walki.

---

[45] J. Michniak, Kompendium łączności, AON, Warszawa 1992, str. 78
[46] Zob. Leksykon naukowo-techniczny, WNT, Warszawa 1984, str. 1040
[47] J. Mazurkiewicz, Leksykon..., op. cit. str. 173; W. Nowicki, Glosarium telekomunikacyjne, op. cit. s. 50
[48] J. Janczak, Mobilne sieci łączności – album schematów, AON, Warszawa 2003, s. 34



Rys. 2.2.1 Struktura mobilnej sieci telekomunikacyjnej.
Źródło: J. Janczak, Mobilne sieci łączności – album schematów, AON, Warszawa 2003

Zdaniem A. Barczaka sieć telekomunikacyjna budowana jest jako *zbiór węzłów łączności o różnych funkcjach i przeznaczeniu oraz połączeń międzywęzłowych tworzonych z różnych rodzajów linii teletransmisyjnych: przewodowych (w tym światłowodowych), radioliniowych i radiowych (w tym radiotelefonicznych)* [49].

Zaś autorzy ustawy *Prawo telekomunikacyjne* postrzegają sieć telekomunikacyjną jako *urządzenia telekomunikacyjne i linie telekomunikacyjne, zestawione i połączone w sposób umożliwiający przekaz sygnałów pomiędzy określonymi zakończeniami sieci, za pomocą przewodów, fal radiowych bądź optycznych lub innych środków wykorzystujących energię elektromagnetyczną*[50].

Sieć telekomunikacyjna w ujęciu leksykalnym *to zespół aparatów przetwórczych, linii i stacji teletransmisyjnych, central telefonicznych i telegraficznych, radiostacji oraz urządzeń telekomunikacyjnych znajdujących się na określonym obszarze (kontynentu, kraju, okręgu), powiązanych ze sobą i przeznaczonych do świadczenia usług telekomunikacyjnych*[51].

Opierając się na cytowanych pojęciach definiujących sieć telekomunikacyjną można zatem za prof. J. Michniakiem pozwolić sobie na stwierdzenie, że *zawiera ona potencjał typowych kanałów telekomunikacyjnych, rozdysponowany do eksploatacji w ramach poszczególnych wyspecjalizowanych usług telekomunikacyjnych, gdzie kanał*

[49] A. Barczak, Planowanie systemu łączności, op. cit. str. 66
[50] E. Ura, Prawo telekomunikacyjne – komentarz, Wydawnictwo Prawnicze, Warszawa 2001, s. 14
[51] A. Topulos, Ilustrowany leksykon techniczny, Wydawnictwo Naukowo-techniczne, Warszawa 1983, s. 498

telekomunikacyjny rozumiany jako środek techniczny lub zespół takich środków oraz ewentualnie wolnej przestrzeni, przystosowany do przesyłania na odległość sygnałów elektrycznych poddawanych podczas procesu takiego przesyłania ograniczeniu natury technicznej określonego rodzaju lub określonych rodzajów, a spełniających odpowiednie wymagania dotyczące jakości odbioru przekazywanych wiadomości[52].

Po przeprowadzeniu wnikliwej analizy przedstawionych powyżej stanowisk cytowanych przedstawicieli świata nauki oraz mając na uwadze całą złożoność sieci telekomunikacyjnej, autor niniejszej dysertacji pozwala sobie na przyjęcie uogólnienia, ***że cytowani powyżej autorzy rozpatrują ją w dwóch płaszczyznach tzn. węzłów oraz linii telekomunikacyjnych, zwanych czasami przez niektórych znawców tematu sieciami łączy***[53].

Pierwszą z tych płaszczyzn stanowi węzeł łączności, który w ujęciu J. Mazurkiewicza *to złożony element wojskowej sieci łączności, stanowiący organizacyjno-techniczne połączenie sił i środków łączności oraz środków zautomatyzowanego systemu dowodzenia, rozwijany w garnizonach oraz w warunkach polowych w celu zapewnienia łączności dowództwom i instytucjom wojskowym*[54]. Węzeł łączności zapewnia tworzenie, komutację kanałów i informacji (pakietów), utajnianie informacji w kanałach i traktach grupowych a, także dystrybucję przesyłek pocztowych. Ze względu na przeznaczenie wyróżnia:

- węzły łączności stanowisk dowodzenia;
- pomocnicze, rejonowe i zapasowe węzły łączności;
- podstawowe węzły sieciowe (PWS) zwane także węzłami bazowymi;
- garnizonowe węzły łączności różnych kategorii;
- wojskowe węzły pocztowe.

W ujęciu E. Piedziuka węzeł łączności to *element systemu łączności*[55]. Jest to organizacyjno-techniczne połączenie sił, środków łączności i środków zautomatyzowanego dowodzenia wojskami, zapewniające tworzenie, przełączanie oraz komutację ka-

---

[52] J. Michniak, Kierowanie mobilnymi ..., op. cit., s. 72

[53] Sieci łączy – zbiorowość zespolonych ze sobą łączy telekomunikacyjnych oraz urządzeń przetwórczych (abonenckich) zapewniających użytkownikom sieci określone rodzaje usług

[54] J. Mazurkiewicz, Leksykon..., op. cit., str. 229

[55] E. Piedziuk, Słownik pojęć z zakresu telekomunikacji, ASG WP, Warszawa 1987, s. 132

nałów wiadomości, utajnianie informacji w kanałach i traktach sieci pierwotnej i wtórnej[56].

Kolejne, choć nieco odmienne podejście w zakresie definiowania węzła łączności przedstawia E. Piotrkiewicz, którego zdaniem, jest to *jeden z podstawowych elementów wojskowego systemu łączności, rozwijany w garnizonach oraz w warunkach polowych, w rejonie stanowisk dowodzenia*[57]. W zależności od szczebla dowodzenia w jego skład wchodzą: centrala (stacja) telefoniczna, centrala (stacja) telegraficzna, przełączalnia, rozmównica telefoniczna, wojskowa stacja pocztowa, lądowisko dla samolotów i śmigłowców łączności, aparatownie transmisji danych i informacji oraz radioodbiorcze oddzielne radiostacje i odbiorniki radiowe, grupa (grupy) środków nadawczych (lub centrum) i sztabowe aparatownie z wyposażeniem poczty polowej i inne.

Uwzględniając ewolucję sprzętową (technologiczną), wynikającą z szerokiego wykorzystania w sprzęcie łączności techniki cyfrowej oraz pojęciową, która jest następstwem doświadczeń ostatnich konfliktów zbrojnych, autor uważa, że najbardziej adekwatnym określeniem współczesnego polowego węzła łączności będzie definicja prof. J. Michniaka traktująca go jako ***złożony element sieci telekomunikacyjnej stanowiący organizacyjno-techniczne połączenie sił i środków łączności oraz informatyki. Jest rozwijany w miejscu skrzyżowania się lub zbiegu różnych linii telekomunikacyjnych w celu zapewnienia tworzenia kanałów, ich komutacji oraz komutacji pakietów i utajniania informacji***[58].

Ze względu na ich przeznaczenie polowe węzły łączności pełnią funkcje[59]:

- węzłów telekomunikacyjnych sieci operacyjno-taktycznej występujących na szczeblu korpusu wojsk lądowych jako węzły sieciowe lub pomocnicze węzły sieciowe;
- węzłów telekomunikacyjnych sieci taktycznej występujących na szczeblu dywizji zmechanizowanej jako pomocnicze węzły łączności;

---

[56] J. Mazurkiewicz, Leksykon łączności..., op. cit., s. 170, 174
[57] E. Piotrkiewicz, Leksykon wiedzy wojskowej..., op. cit., s. 476
[58] J. Michniak, Kierowanie mobilnymi systemami łączności..., op. cit. s. 78
[59] J. Michniak, Kierowanie mobilnymi systemami łączności..., op. cit. s. 80

– węzłów łączności stanowisk dowodzenia, gdzie węzeł telekomunikacyjny uzupełnia się o elementy poczty polowej oraz środki do organizacji bezpośrednich linii telekomunikacyjnych i wewnętrznej sieci telefonicznej oraz informatycznej stanowisk dowodzenia.

Drugą, zgodnie z przyjętymi uprzednio kryteriami, płaszczyznę rozpatrywania sieci telekomunikacyjnej stanowią linie telekomunikacyjne.

W określeniu W. Nowickiego ten makroskładnik sieci telekomunikacyjnej - linie telekomunikacyjne - *to zespół środków technicznych rozmieszczonych między dwoma miejscowościami, umożliwiający jednoczesną wymianę i/lub jednoczesne przekazywanie wielu wiadomości*[60].

Linia telekomunikacyjna to *tor lub zespół takich torów, łącznie ze stacjami teletransmisji (przelotowymi, odgałęźnymi i końcowymi) oraz łącznie ze wszelkimi akcesoriami konstrukcyjnymi służącymi do przesyłania informacji na odległość, rozmieszczonych wzdłuż określonej trasy*[61].

W definicyjnym rozumieniu środki techniczne to przede wszystkim tory telekomunikacyjne, które tworzą wiązki torów o długościach na ogół mniejszych lub znacznie mniejszych od długości samej linii telekomunikacyjnej. Tor telekomunikacyjny należy przy tym rozumieć *jako konstrukcję techniczną będącą układem elektrycznym biernym, w zasadzie linearnym, umożliwiającą realizację kanału telekomunikacyjnego, a ten traktowany jest jako środek techniczny lub zespół takich środków oraz ewentualnie wolnej przestrzeni przystosowany do przesyłania na odległość sygnałów elektrycznych poddawanych podczas procesu takiego przesyłania ograniczaniu natury technicznej określonego rodzaju lub określonych rodzajów i spełniający odpowiednie wymagania dotyczące jakości odbioru przekazywanych wiadomości*[62].

Zidentyfikowane w toku dotychczasowych rozważań elementy organizacyjno-eksploatacyjne polowego systemu łączności dywizji zmechanizowanej stanowić będą podstawę do zdefiniowania i określenia sieci teletransmisyjnej, która stanowi główny obszar prowadzonych przez autora badań.

---

[60] W. Nowicki, Glosarium telekomunikacji, zalecane terminy, ich definicje, odpowiedniki obcojęzyczne, komentarze, zeszyt 2, Biuletyn informacyjny nr 2-3 (276-277) IŁ, Warszawa-Międzeszyn, 1990, s. 37
[61] J. Michniak, Kierowanie mobilnymi..., op. cit., s. 80
[62] W. Nowicki, Głosarium telekomunikacji..., op. cit. s. 31

2.3. SIEĆ TELETRANSMISYJNA DYWIZJI ZMECHANIZOWANEJ JAKO OBSZAR BADAŃ

Posiadając tak usystematyzowaną wiedzę oraz zdefiniowane pojęcie sieci łączności z jej integralnym elementem siecią telekomunikacyjną (węzły i linie telekomunikacyjne), której zasadniczym zadaniem jest zapewnienie przesyłania (transmisji) informacji we wszystkich relacjach dowodzenia, współdziałania i alarmowania, zasadnym jest zidentyfikowanie obszaru badań niniejszej dysertacji i zdefiniowanie pojęcia sieci teletransmisyjnej związku taktycznego.

Pierwszym krokiem w tym kierunku jest określenie samego pojęcia teletransmisji – co ono oznacza i jak jest definiowane? Słowo transmisja pochodzące z języka łacińskiego *„transmissio"* oznacza przesyłkę lub przekazywanie[63].

Zgodnie z poglądami W. Nowickiego teletransmisja stanowi *dział telekomunikacji dotyczący przesyłania sygnałów elektrycznych na odległość przy użyciu środków technicznych służących albo do prowadzenia fal elektromagnetycznych, albo do ich możliwie dużego ukierunkowania w przestrzeni otwartej*[64]. Zastrzega się on przy tym jednocześnie, że prowadzenie fal elektromagnetycznych rozumianych jako dział telekomunikacji nie należy identyfikować z pojęciem transmisji oznaczającej odpowiedni proces telekomunikacyjny elementarny. W trakcie dalszej analizy pojęcia teletransmisji wyróżnia:

- teletransmisję przewodową,
- teletransmisję radiową,
- teletransmisję optyczną,
- teletransmisję świetlną,
- teletransmisję światłowodową,
- teletransmisję falowodową,
- teletransmisję analogową,
- teletransmisję cyfrową.

---

[63] W. Kopaliński, Słownik wyrazów obcych i zwrotów obcojęzycznych, Wiedza Powszechna, Warszawa, 1983, s. 431

[64] W. Nowicki, Glosarium Telekomunikacji, Zeszyt 1, Instytut Łączności, Warszawa 1991, s. 77

Przeprowadzając analizę przedstawionego powyżej podziału można pokusić się o stwierdzenie, że dokonany jest on w oparciu o środowisko, w którym przekazywany (transmitowany) jest sygnał elektryczny. Natomiast w odniesieniu do ostatnich dwóch tzn. teletransmisji analogowej lub cyfrowej mowa jest tutaj raczej o postaci sygnału lub medium transmisyjnym – analogowym lub cyfrowym.

Bardzo zbliżoną definicję teletransmisji przedstawia W. Majewski, który uważa ją za dziedzinę telekomunikacji *zajmującą się przesyłaniem sygnałów na odległość za pomocą wąskich strug energii, a więc poprzez tory przewodowe, radiowe lub radioliniowe*[65].

Definicja pojęcia teletransmisji prezentowana przez J. Mazurkiewicza określa ją jako dział telekomunikacji, *dotyczący przekazywania sygnałów elektrycznych na odległość przy użyciu środków technicznych służących do prowadzenia fal albo ich możliwie dużego ukierunkowania w przestrzeni otwartej. Prowadzenie fal elektromagnetycznych bądź ich ukierunkowanie realizowane jest za pomocą torów telekomunikacyjnych. W szczególności ukierunkowanie uzyskuje się w telekomunikacyjnych torach radiowych*[66].

W ujęciu amerykańskim transmisja jest *procesem przesyłania energii elektrycznej z punktu do punktu wzdłuż toru (linii telekomunikacyjnej)* [67]. Teletransmisja stanowi medium, które umożliwia dowolnym dwóm abonentom sieci wymianę informacji wytwarzanej przez urządzenie jednego terminala i odbieranej przez drugie. Medium to zwane czasami torem lub linią telekomunikacyjną może przyjąć postać łącza kablowego, kabla współosiowego, światłowodowego lub wolnej przestrzeni, jak to ma miejsce w systemach radiowych. Teletransmisja jest zatem tym elementem, który zapewnia ruch (przesył) informacji na określoną odległość.

W ujęciu leksykalnym teletransmisja stanowi dział telekomunikacji *zajmujący się przesyłaniem sygnałów w celu przekazania określonych danych, najczęściej przy wykorzystaniu torów przewodowych (transmisja przewodowa) lub drogą radiową (transmisja radiowa)* [68].

---

[65] W. Majewski, Teletransmisyjne systemy cyfrowe, Wydawnictwo Komunikacji i Łączności, Warszawa 1976, s. 13
[66] J. Mazurkiewicz, Leksykon..., op. cit. s. 202
[67] J. Griffith, C[4]ISR Handbook for Integrated Planning, Department of Defense, Washington 1998, s. 2-37
[68] A. Topulos, Leksykon..., op. cit. s. 554

Reasumując i dokonując uogólnienia do dalszych rozważań, autor przyjął następująco zdefiniowane pojęcie teletransmisji:

Teletransmisja stanowi jeden z działów telekomunikacji, który obejmuje swoim zakresem proces przekazywania na odległość sygnałów zawierających w sobie dane (informacje) za pomocą linii telekomunikacyjnych przewodowych (kablowych, światłowodowych, falowodowych, itp.) i/lub radiowych (radioliniowych).

Jeśli przyjmiemy do dalszych rozważań tak zdefiniowane pojęcie teletransmisji, to następstwem winno być przybliżenie, a później zdefiniowanie sieci teletransmisyjnej dywizji zmechanizowanej.

W literaturze przedmiotu można spotkać się z następującą definicją sieci teletransmisyjnej, która traktuje *sieć jako całokształt wzajemnie powiązanych pod względem zadań, miejsca i czasu działania węzłów i linii łączności różnego przeznaczenia, rozwijanych wg jednolitego planu w celu zapewnienia przekazywania informacji w systemach dowodzenia wojskami i kierowania środkami walki*[69].

Nieco inne spojrzenie na sieć teletransmisyjną prezentuje prof. J. Michniak, który twierdzi, że stanowi ona najistotniejszy składnik sieci telekomunikacyjnej obejmujący *zbiorowość wyspecjalizowanych linii telekomunikacyjnych i wyspecjalizowanych central komutacyjnych rozwiniętych na danym obszarze (czy szczeblu dowodzenia) za pomocą wszystkich rodzajów środków teletransmisyjnych*[70].

Tak rozumiana współczesna sieć teletransmisyjna dywizji, aby spełnić stawiane przed nią przez system dowodzenia oraz warunki współczesnego obszaru działań z użyciem wojsk wymagania operacyjne i techniczne, w myśl literatury przedmiotu[71] winna charakteryzować się następującymi własnościami:

- odpornością na oddziaływanie przeciwnika (ogniowe i elektroniczne);
- skrytością przekazywania informacji;
- krótkim czasem adaptacji (rekonfiguracji) do zmiennych warunków otoczenia sieci;

---

[69] J. Mazurkiewicz, Leksykon..., op. cit., s. 174

[70] J. Michniak, Model organizacyjny polowej sieci łączności związku taktycznego w latach 1995-2005, AON, Warszawa 1995, s. 16

[71] m.in. J. Michniak, A. Wisz, Bezpieczeństwo i ochrona informacji....., op. cit., s. 12; Z. Fiołna, P. Daniluk, Koncepcja struktur organizacyjnych..., op. cit., s. 72

- pełną automatyzacją procesów przekazywania informacji;
- niezawodnym systemem zarządzania zasobami sieci;
- możliwością korzystania z „zasobów telekomunikacyjnych" obszaru operacji (wykorzystania infrastruktury stacjonarnej w wymaganym zakresie);
- możliwością świadczenia usług dla dowolnego uprawnionego abonenta na całym obszarze funkcjonowania sieci;
- możliwością współpracy z dotychczas stosowanymi urządzeniami i sieciami łączności;
- wysoką mobilnością;
- możliwością rozwoju i współpracy z następną generacją urządzeń lub sieci.

A zatem aby ustalić strukturę i organizację sieci teletransmisyjnej przedstawione oraz poddane analizie zostaną wybrane warianty sieci teletransmisyjnych planowanych lub rozwijanych w ramach ćwiczeń, treningów sztabowych, operacji stabilizacyjnych na szczeblu dywizji.

Jako pierwsza zaprezentowana zostanie sieć teletransmisyjna opracowana na potrzeby ćwiczenia pk. „Jantar 2004". Zasadnicze przedsięwzięcie, które miała zrealizować dywizja w ramach tego ćwiczenia, sprowadzało się do obrony wyznaczonego pasa wybrzeża o szerokości blisko 40 kilometrów, z zadaniem załamania operacji desantowej przeciwnika i utrzymania nakazanego pasa obrony.

Myśl przewodnia dowódcy dywizji[72] zawarta została w następującym sformułowaniu – „We współdziałaniu z Marynarką Wojenną, Wojskami Lotniczymi i Obrony Powietrznej oraz Sztabem Generalnym WP uniemożliwić prowadzenie operacji desantowej przeciwnika i załamać jego natarcie na przedniej linii obrony. W przypadku włamania się przeciwnika w głąb obrony dywizji działaniami pierwszego rzutu na kolejnych rubieżach opóźniania powstrzymać jego natarcie celem ostatecznego załamania działań przeciwnika dla zabezpieczenia wykonania kontrataku przez odwód przełożonego.

Strukturę organizacyjną ćwiczącej dywizji stanowiły zarówno jej organiczne jak i przydzielone oddziały oraz pododdziały, w skład której wchodziły:

---

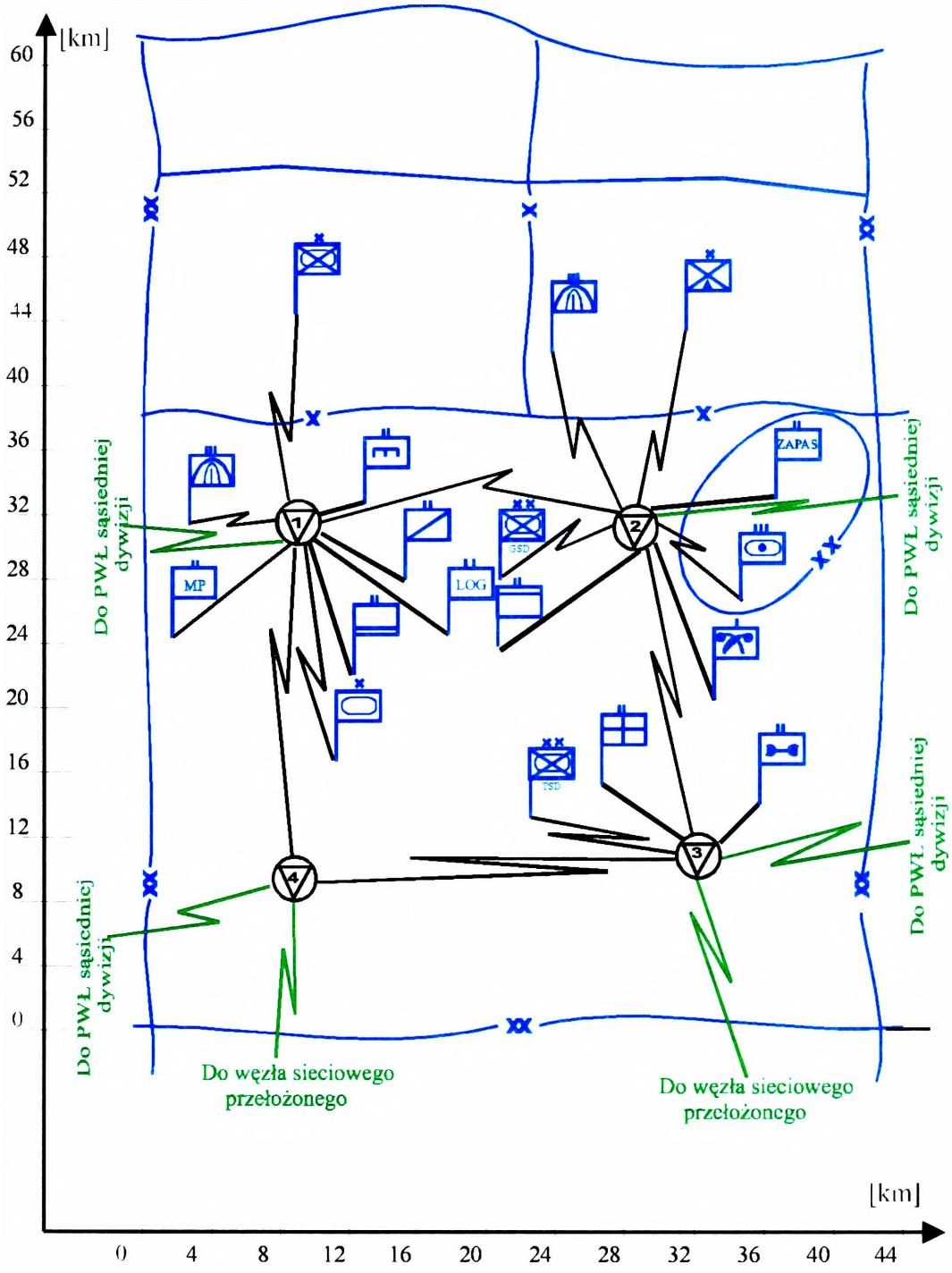
[72] Dokumentacja ćwiczenia dowódczo-sztabowego pk. „Jantar 2004"

- Brygada Zmechanizowana (BZ),
- Brygada Pancerna (BPanc),
- Brygada Strzelców Podhalańskich (BSP),
- pułk artylerii (pa),
- 2 x pułk przeciwlotniczy (pplot),
- batalion rozpoznawczy (br),
- batalion saperów (bsap),
- batalion dowodzenia (bdow),
- batalion zaopatrzenia (bzaop),
- batalion medyczny (bmed),
- batalion remontowy (brem),
- batalion ochrony (bochr),
- batalion zapasowy (bzapas),
- kompania chemiczna (kchem).

Zgodnie z przyjętym zamiarem, zobrazowanym w rozkazie operacyjnym dowódcy, dywizja w ramach prowadzonego ćwiczenia, przyjęła ugrupowanie bojowe, które obejmowało:

- stanowiska dowodzenia,
- pierwszy rzut,
- odwód,
- zgrupowanie oddziałów artylerii,
- oddziały przeciwlotnicze,
- elementy rozpoznania,
- odwód inżynieryjny,
- oddział zaporowy,
- odwód przeciwchemiczny,
- elementy logistyczne,
- pomocnicze węzły łączności wraz z liniami łączności.

Głębokość tak przyjętego ugrupowania w ramach pasa odpowiedzialności dywizji wynosiła ponad 60 km, zaś szerokość ponad 40 km.



Rys. 2.3.1 Schemat organizacyjny sieci teletransmisyjnej dywizji zmechanizowanej - ćwiczenie pk. „Jantar 2004"

Źródło: opracowano na podstawie dokumentacji ćwiczenia dowódczo-sztabowego pk. „Jantar 2004"

Sieć stanowisk dowodzenia dywizji zgodnie z przyjętym wariantem działania obejmowała:

- główne stanowisko dowodzenia (GSD),
- tyłowe stanowisko dowodzenia (TSD).

Zaplanowana i zorganizowana na potrzeby niniejszego ćwiczenia sieć teletransmisyjna funkcjonowała w oparciu o cztery pomocnicze węzły łączności (rys. 2.3.1), które połączone były ze sobą w układzie wielobocznym.

Każdy z pomocniczych węzłów łączności poza połączeniami wewnątrz sieci dywizyjnej dowiązany jest do podobnego węzła łączności sąsiada – w tym przypadku do sieci teletransmisyjnych dywizji mających przyległe (z prawej i lewej strony) obszary odpowiedzialności. Ponadto oba węzły rozwinięte w obszarze tyłowym oznaczone numerami 3 i 4 dowiązane zostały do sieci teletransmisyjnej przełożonego.

Z przedstawionego na rysunku 2.3.1 schematu struktury organizacyjnej sieci wynika, że tylko i wyłącznie tyłowe stanowisko dowodzenia organizowane jest na szczeblu dywizji. W ramach sieci teletransmisyjnej liniami telekomunikacyjnymi realizowanymi w oparciu o środki radioliniowe do poszczególnych pomocniczych węzłów łączności dowiązane są pojedynczymi traktami radioliniowymi oba stanowiska dowodzenia dywizji, GSD brygad oraz pułków artylerii i przeciwlotniczych. Każdy z czterech PWŁ dowiązany jest ponadto dwoma traktami radioliniowymi do dwóch swoich odpowiedników w ramach wewnętrznej dywizyjnej sieci teletransmisyjnej oraz pojedynczymi do pomocniczych węzłów łączności jednostek sąsiadujących.

Szczegółowe zestawienie ilości radioliniowych linii telekomunikacyjnych oraz środków radioliniowych niezbędnych do ich realizacji indywidualnie przez każdy z rozwiniętych pomocniczych węzłów łączności sieci teletransmisyjnej dywizji zawiera tabela 2.3.1.

Takie tabelaryczne zestawienie traktów i środków radioliniowych pozwala na określenie indywidualnej struktury organizacyjnej (ilości stacji i sprzętu) niezbędnego do zapewnienia rozwinięcia wszystkich wymienionych powyżej dalekosiężnych linii radiowych przez poszczególne pomocnicze węzły łączności, która jednocześnie stanowi szkielet strukturalno-organizacyjny sieci teletransmisyjnej dywizji.

Tabela 2.3.1

Wykaz oraz ilościowe zestawienie relacji radioliniowych rozwijanych w ramach dywizyjnej sieci teletransmisyjnej – ćwiczenie „Jantar 2004"

	PWŁ nr 1	PWŁ nr 2	PWŁ nr 3	PWŁ nr 4
SD DZ				
TSD DZ				
SD BSP				
SD BZ				
SD BPanc.				
SD pa				
SD 1 pplot				
SD 2 pplot				
PWŁ sąsiada				
PWS przełożonego				
Wewnętrzne trakty radioliniowe				
Ilość traktów radioliniowych	6	7	4	5

Źródło: opracowanie własne na podstawie dokumentacji ćwiczenia "Jantar 2004"

Drugim elementem zobrazowanym na schemacie sieci teletransmisyjnej (rys. 2.3.1) są kablowe linie telekomunikacyjne, którymi do pomocniczych węzłów łączności sieci teletransmisyjnej dowiązane są stanowiska dowodzenia pododdziałów (bataliony, kompanie) ćwiczącej dywizji. W tym przypadku również każde z stanowisk dowodzenia pododdziałów dowiązuje się tylko do jednego najbliżej znajdującego PWŁ traktem kablowym. Zestawienie relacji kablowych realizowanych w ramach poszczególnych pomocniczych węzłów łączności zawiera tabela 2.3.2.

Z przyjętej na potrzeby ćwiczenia struktury oraz organizacji sieci wynika, iż jako zasadę przyjęto, że węzły łączności stanowisk dowodzenia oddziałów pierwszorzutowych, odwodu oraz pozostałych jednostek wchodzących w skład ugrupowania bojowego dywizji dowiązane są do sieci teletransmisyjnej dywizji traktami radioliniowymi, co zapewnia im możliwość wymiany informacji w całym obszarze prowadzonych przez dywizję działań. Natomiast można stwierdzić, że dołączanie do sieci stanowisk

dowodzenia samodzielnych pododdziałów (batalion, kompania) jest ona zorganizowane w oparciu o linie kablowe.

Tabela 2.3.2

Wykaz oraz ilościowe zestawienie traktów przewodowych realizowanych przez poszczególne pomocnicze węzły łączności – ćwiczenie „Jantar 2004"

	PWŁ nr 1	PWŁ nr 2	PWŁ nr 3	PWŁ nr 4
SD bdow	←	→		
SD br	←	→		
SD bsap	←	→		
SD blog	←	→		
SD brem	←	→	→	
SD bzaop	←	→		
SD bochr	←	→		
SD bmed	←	→	→	
SD bzapas	←	→		
PDO kchem	←	→		
Ilość traktów przewodowych	5	3	2	0

Źródło: opracowanie własne na podstawie dokumentacji ćwiczenia "Jantar 2004"

Kolejny przykład sieci teletransmisyjnej, który zostanie zaprezentowany w ramach niniejszej dysertacji, opracowany został w dwóch wariantach przez sztab dywizji w ramach ćwiczenia dowódczo-sztabowego pk. „Opal 99".

W skład organizacyjny dywizji wchodziły[73]:

- 3 x Brygada Zmechanizowana,
- Brygada Pancerna,
- pułk artylerii,
- pułk przeciwlotniczy,
- batalion rozpoznawczy,
- batalion saperów,
- batalion dowodzenia,
- batalion zaopatrzenia,
- batalion medyczny,
- batalion remontowy,

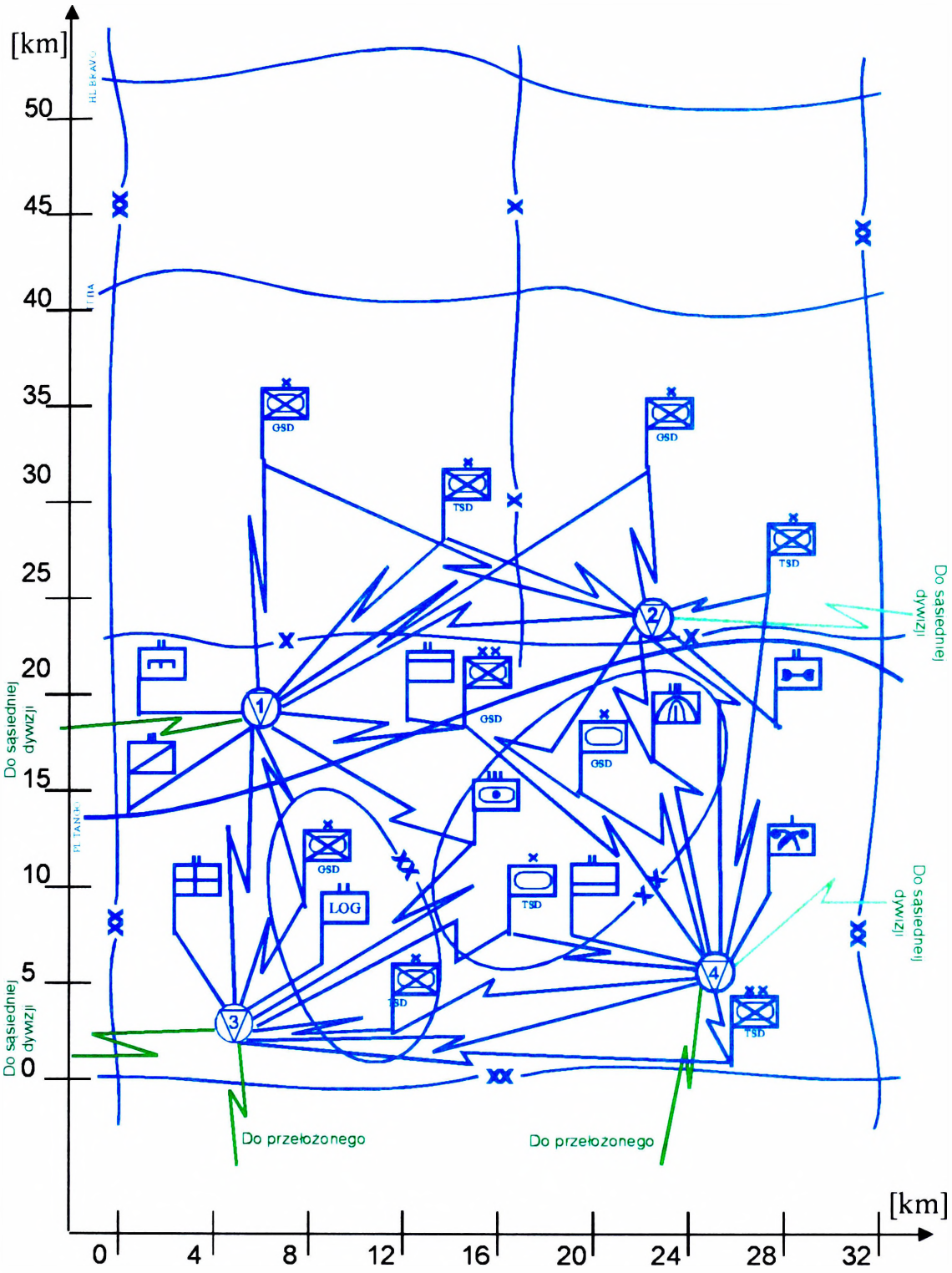
[73] Dokumentacja ćwiczenia dowódczo-sztabowego „Opal 99"

– kompania chemiczna.

Podobnie jak w poprzednio rozpatrywanym wariancie zasadniczym celem dywizji była organizacja obrony wyznaczonego pasa. Główne zadanie dywizji podczas ćwiczenia, to prowadząc działania opóźniające siłami pierwszorzutowych brygad, związać walką siły przeciwnika w celu ostatecznego zatrzymania nacierających wojsk na linii PL TANGO (rys. 2.3.2), a tym samym stworzenia sprzyjających warunków do przeprowadzenia przez przełożonego natarcia dla odzyskania utraconego obszaru oraz całkowitego rozbicia sił przeciwnika. Ugrupowanie bojowe broniącej przydzielonego pasa dywizji było podobne jak w poprzednim przykładzie, z tą istotną różnicą, że uwzględniono w nim główne i tyłowe stanowiska dowodzenia zarówno szczebla dywizji, jak i ćwiczących brygad oraz ze względu na strukturę cztero-brygadową dywizji. W prezentowanym poniżej wariancie wyróżniono dwa odwody. Podstawę każdego z nich stanowiły siły jednej brygady.

Ugrupowanie bojowe oraz zaplanowana sieć teletransmisyjna dywizji w czasie prowadzenia działań obronnych przedstawiona została na rys. 2.3.2.

Przydzielony dywizji pas obrony miał szerokość 32 km, a jego głębokość - ponad 50 km. Sieć teletransmisyjna dywizji rozwinięta została w oparciu o cztery pomocnicze węzły łączności, z których każdy traktem radioliniowym dowiązany został do dwóch sąsiednich węzłów z zachowaniem maksymalnych odległości pomiędzy nimi. Traktami radioliniowymi (dwoma) sieć dowiązana została do każdego z sąsiednich związków taktycznych, a z dwóch pomocniczych węzłów znajdujących się najgłębiej w strefie tyłowej dywizji wyprowadzone zostały trakty radioliniowe stanowiące dowiązanie do sieci teletransmisyjnej przełożonego.



Rys. 2.3.2 Schemat organizacji sieci teletransmisyjnej dywizji zmechanizowanej podczas ćwiczenia pk. „Opal 99"

Źródło: dokumentacja ćwiczenia dowódczo-sztabowego pk. „Opal 99"

Pełne zestawienie traktów radioliniowych realizowanych w ramach sieci przez poszczególne pomocnicze węzły łączności zawiera tabela 2.3.3.

Tabela 2.3.3

Wykaz oraz ilościowe zestawienie relacji radioliniowych rozwijanych w ramach dywizyjnej sieci teletransmisyjnej – ćwiczenie „Opal 99"

	PWŁ nr 1	PWŁ nr 2	PWŁ nr 3	PWŁ nr 4
GSD DZ				
TSD DZ				
GSD 1BZ				
TSD 1 BZ				
GSD 2 BZ				
TSD 2 BZ				
GSD 3 BZ				
TSD 3 BZ				
GSD BPanc.				
TSD BPanc				
SD pa				
SD pplot				
PWŁ sąsiada				
PWS przełożonego				
Wewnętrzne trakty radioliniowe				
Ilość traktów radioliniowych	9	9	9	11

Źródło: opracowanie własne na podstawie dokumentacji ćwiczenia "Opal 99"

Drugim elementem wyszczególnionym na schemacie sieci teletransmisyjnej, który zapewnia dowiązanie do niej stanowisk dowodzenia organicznych pododdziałów dywizji szczebla batalionu oraz kompanii chemicznej stanowią pojedyncze trakty kablowe, których pełen wykaz oraz zestawienie dowiązań do poszczególnych pomocniczych węzłów łączności przedstawia tabela 2.3.4.

Tabela 2.3.4

Wykaz oraz ilościowe zestawienie traktów przewodowych realizowanych przez poszczególne PWŁ – ćwiczenie „Opal 99".

	PWŁ nr 1	PWŁ nr 2	PWŁ nr 3	PWŁ nr 4
SD br	← →			
SD bsap	← →			
SD blog	←	—	→	
SD brem	←	—	→	
SD bzaop	←	—	—	→
SD bmed	←	—	→	
PDO kchem	←	—	—	→
Ilość traktów przewodowych	3	1	2	2

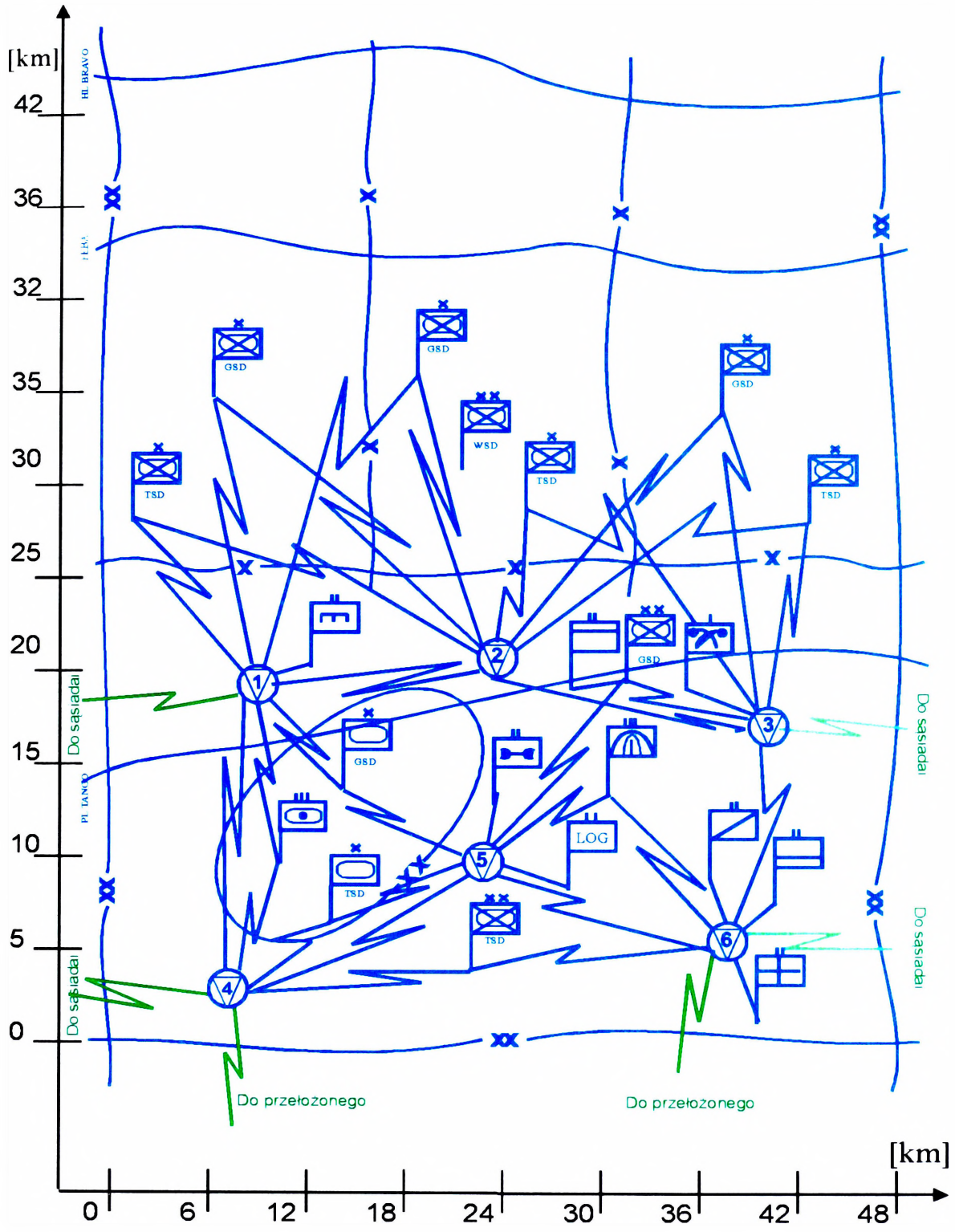
Źródło: opracowanie własne na podstawie dokumentacji ćwiczenia "Opal 99"

Kolejna sieć teletransmisyjna, która poddana zostanie analizie w zakresie jej topologii uwzględniającej ilość zarówno pomocniczych węzłów łączności jak i linii teletransmisyjnych opracowana została w ramach ćwiczenia „Donośna surma 2003".

Obejmuje ona strukturę i organizację sieci w ramach prowadzonej przez dywizję obrony w pasie o szerokości blisko 50 km oraz głębokości ponad 40 km. Struktura organizacyjna dywizji[74] jest identyczna jak w poprzednim przykładzie. Istotną różnicę stanowi ugrupowanie bojowe. W pierwszym rzucie znajdują się trzy brygady zmechanizowane. Jednostką będącą w odwodzie jest brygada pancerna rys.2.3.3.

Sieć teletransmisyjna dywizji w obronie w tym przypadku, oparta została na sześciu pomocniczych węzłach łączności. Tradycyjnie dwa węzły znajdujące się najbliżej dywizyjnej linii rozgraniczenia, zarówno z lewej jak i z prawej strony ugrupowania bojowego, dowiązane zostały traktami radioliniowymi do jednostek sąsiadujących. Natomiast dwa pomocnicze węzły łączności rozwinięte najgłębiej w strefie tyłowej dywizji traktami radioliniowymi dowiązane zostały do sieci teletransmisyjnej przełożonego.

[74] Dokumentacja ćwiczenia „Donośna surma 2003"



Rys. 2.3.3 Schemat organizacji sieci teletransmisyjnej dywizji zmechanizowanej w ramach ćwiczenia pk. „Donośna Surma 2003"

Źródło: dokumentacja ćwiczenia dowódczo-sztabowego pk. „Donośna Surma 2003"

Trakty radioliniowe połączeń wewnętrznych (międzywęzłowych) oraz pozostałe relacje radioliniowe realizowane przez poszczególne węzły sieci w formie tabelarycznego zestawienia zawarte zostały w tabeli 2.3.5.

Tabela 2.3.5

Wykaz oraz ilościowe zestawienie relacji radioliniowych rozwijanych w ramach dywizyjnej sieci teletransmisyjnej – ćwiczenie „Donośna surma 2003"

	PWŁ nr 1	PWŁ nr 2	PWŁ nr 3	PWŁ nr 4	PWŁ nr 5	PWŁ nr 6
GSD DZ						
TSD DZ						
GSD 1BZ						
TSD 1 BZ						
GSD 2 BZ						
TSD 2 BZ						
GSD 3 BZ						
TSD 3 BZ						
GSD BPanc.						
TSD BPanc						
SD pa						
SD pplot						
PWŁ sąsiada						
PWS przełożone-go						
Wewnętrzne trakty radioliniowe						
Ilość traktów radioliniowych	7	9	6	8	6	6

Źródło: opracowanie własne na podstawie dokumentacji ćwiczenia "Donośna Surma 2004"

Następnym elementem sieci teletransmisyjnej dywizji są tory telekomunikacyjne realizowane za pomocą linii kablowych. W topologii sieci przedstawionej na rysunku 2.3.3 ten rodzaj dowiązania do sieci teletransmisyjnej dywizji realizowany jest w stosunku do pododdziałów szczebla batalionu oraz jedynej w strukturze organizacyjnej dywizji - kompanii chemicznej. Pododdziałem, który ze względu na specyfikę realizowanych zadań oraz miejsce rozwinięcia stanowiska dowodzenia bezpośrednio przy GSD dywizji nie posiada bezpośredniego dowiązania do sieci teletransmisyjnej dywizji jest batalion dowodzenia. Dowiązanie do systemu dywizji w tym przypadku realizowane jest poprzez węzeł łączności GSD dywizji.

Tabela 2.3.6

Wykaz oraz ilościowe zestawienie traktów przewodowych realizowanych przez poszczególne PWŁ – ćwiczenie „Donośna surma 2003".

	PWŁ nr 1	PWŁ nr 2	PWŁ nr 3	PWŁ nr 4	PWŁ nr 5	PWŁ nr 6
SD br	← →					
SD bsap	← →					
SD blog	←	—	—	—	→	
SD brem	←	—	—	→		
SD bzaop	←	—	—	—	—	→
SD bmed	←	—	—	—	→	
PDO kchem	←	—	—	—	—	→
Ilość traktów przewodowych	3	1	2			2

Źródło: opracowanie własne na podstawie dokumentacji ćwiczenia "Donośna Surma 2004"

Dotychczas przedstawiane warianty sieci teletransmisyjnych odnosiły się do działań prowadzonych przez dywizję w ramach organizacji działań obronnych związku taktycznego. W ramach treningu sztabowego pk. „Odra 2004" dywizja w skład, której wchodziły następujące jednostki organizacyjne[75]:

- 2 x Brygada Zmechanizowana,
- Brygada Pancerna,
- pułk artylerii,
- pułk przeciwlotniczy,
- batalion rozpoznawczy,
- batalion saperów,
- batalion dowodzenia,
- batalion zaopatrzenia,
- batalion medyczny,
- batalion remontowy,
- batalion chemiczny,
- kompania chemiczna.

otrzymała zadanie wykonania drugiego typu działań rozstrzygających – natarcia, którego zasadniczym celem było odzyskanie utraconego obszaru i przywrócenie stanu

[75] Dokumentacja treningu sztabowego pk. „Odra 2004"

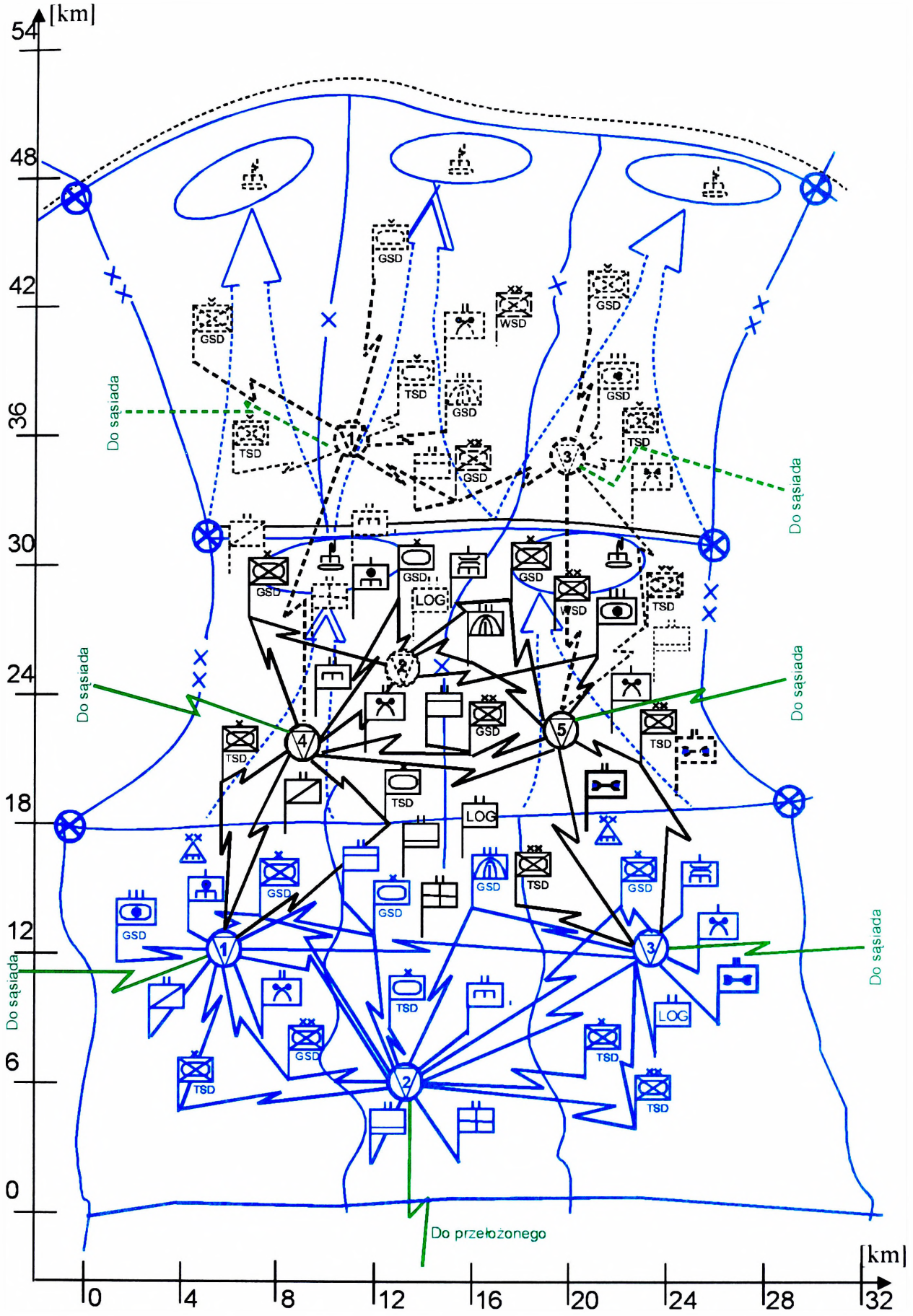
faktycznego sprzed konfliktu. Działania zaczepne prowadzone przez dywizję zmechanizowaną realizowane były w specyficznym środowisku pola walki - w warunkach zagrożenia użyciem broni masowego rażenia. Z tego też powodu strukturalne oddziały i pododdziały dywizji wzmocnione zostały siłami batalionu chemicznego.

Celem wykonania zadania dywizja zmechanizowana przyjęła ugrupowanie bojowe, w którym możemy wyróżnić:

- stanowiska dowodzenia,
- pierwszy rzut,
- odwód,
- zgrupowanie oddziałów artylerii,
- oddziały przeciwlotnicze,
- elementy rozpoznania,
- odwód inżynieryjny,
- oddział zabezpieczenia ruchu,
- odwód przeciwchemiczny,
- elementy logistyczne,
- pomocnicze węzły łączności wraz z liniami łączności.

Analiza struktury i organizacji sieci teletransmisyjnej dywizji opracowanej w ramach prowadzonego treningu „Odra 2004" (rys. 2.3.4) pozwala stwierdzić, że topologia sieci zależna jest od dynamiki prowadzonej walki oraz umożliwia wyróżnienie kolejno po sobie następujących etapów wpływających na jej strukturę tj.:

- etap I - ześrodkowanie;
- etap II - osiągnięcie obiektu I;
- etap III - osiągnięcie obiektu II.



Rys. 2.3.4 Schemat organizacji sieci teletransmisyjnej dywizji zmechanizowanej w ramach treningu sztabowego pk. „Odra 2004"

Źródło: dokumentacja treningu sztabowego pk. „Odra 2004"

Podstawowe zasady organizacji sieci teletransmisyjnej w poszczególnych etapach prowadzonego natarcia pozostają niezmienne. Pomocnicze węzły łączności traktami radioliniowymi dowiązane są do sieci sąsiadów oraz do sieci przełożonego. Stanowiska dowodzenia oddziałów (główne oraz tyłowe) dowiązane są także traktami radioliniowymi do dwóch najbliższych pomocniczych węzłów łączności dywizyjnej sieci teletransmisyjnej.

Zasadniczą różnicę w stosunku do pozostałych dwóch etapów stanowi sieć teletransmisyjna rozwijana w rejonie ześrodkowania (na rys. 2.3.4 oznaczona kolorem niebieskim). Tylko w tym etapie bowiem organiczne oraz przydzielone pododdziały dywizji dowiązane są do sieci teletransmisyjnej traktami kablowymi. Ponadto w rejonie ześrodkowania „szkielet" sieci stanowią tylko trzy pomocnicze węzły łączności.

W etapie drugim (na rys. 2.3.4 oznaczona kolorem czarnym), w którym dywizja osiąga powodzenie i zdobywa obiekt I struktura sieci teletransmisyjnej rozbudowywana jest o kolejne dwa węzły (przyporządkowane numery 4 i 5). Jednak fizycznie w ramach sieci teletransmisyjnej funkcjonują tylko cztery pomocnicze węzły łączności. Stan ten jest następstwem konieczności przemieszczenia węzła oznaczonego numerem 2 za przemieszczającymi jednostkami dywizji z takim wyliczeniem czasowym, aby osiągnął on gotowość do pracy jeszcze przed rozpoczęciem ostatniego etapu - wprowadzenia z odwodu do pierwszego rzutu brygady pancernej celem spotęgowania tempa natarcia.

W trzecim etapie oznaczonym na rys. 2.3.4 kolorem czarnym (linia przerywana), w ramach którego dywizja miała osiągnąć obiekt II struktura sieci teletransmisyjnej w fazie początkowej również opierała się o rozwinięte trzy pomocnicze węzły łączności. Przemieszczeniu stanowisk dowodzenia jednostek pierwszorzutowych towarzyszyło również przemieszczenie i rozwinięcie węzłów oznaczonych numerami 1 oraz 3. Wzmacniają one strukturę sieci teletransmisyjnej i zapewniają dowiązanie się do niej pojedynczymi traktami radioliniowymi jednostkom pierwszorzutowym przed osiągnięciem przez dywizję obiektu drugiego.

Ilość pomocniczych węzłów łączności oraz traktów (radioliniowych linii dowiązania) przez nie realizowanych w poszczególnych etapach wykonywania przez dywizję zadania przedstawiona została w tabeli 2.3.7.

Tabela 2.3.7

Zestawienie ilościowe traktów radioliniowych realizowanych przez pomocnicze węzły łączności sieci teletransmisyjnej w poszczególnych etapach treningu sztabowego „Odra 2004".

	PWŁ 1	**PWŁ 2**	**PWŁ 3**	**PWŁ 4**	**PWŁ 5**
Etap 1 Rejon ześrodkowania	8	12	7		
Etap 2 Obiekt I	5	6	5	9	8
Etap 3 Obiekt II	8	2	7	4	5

Źródło: opracowanie własne na podstawie dokumentacji treningu sztabowego "Odra 2004"

Jak już wcześniej wspomniano, tylko w rejonie ześrodkowania poza traktami radioliniowymi rozwijane były trakty kablowe, którymi do sieci teletransmisyjnej dowiązano pododdziały dywizji. W pozostałych etapach, uwzględniając dynamikę działania dywizji i zmiany w konfiguracji sieci teletransmisyjnej tego typu relacje nie były rozwijane. Podstawowym determinantem, który legł u podstaw tego stanowiska był czas niezbędny na rozwijanie traktów kablowych oraz ograniczona liczba środków. Stąd też tabela 2.3.8 zawiera relacje kablowe rozwijanie w ramach sieci teletransmisyjnej tylko dla rejonu ześrodkowania dywizji.

Tabela 2.3.8

Ilościowe zestawienie traktów kablowych stanowiących linie dowiązania do poszczególnych pomocniczych węzłów łączności w ramach treningu sztabowego „Odra 2004"

	PWŁ 1	**PWŁ 2**	**PWŁ 3**
Trakty kablowe	**3**	**3**	**4**

Źródło: opracowanie własne na podstawie dokumentacji treningu sztabowego "Odra 2004"

Wszystkie przedstawiane do tej pory przykłady sieci teletransmisyjnej planowane oraz realizowane w ramach narodowych i międzynarodowych ćwiczeń, treningów

dowódczych i sztabowych obejmowały warianty sieci rozwijanych na potrzeby rozstrzygających (obrona, natarcie) działań taktycznych prowadzonych przez dywizję zmechanizowaną.

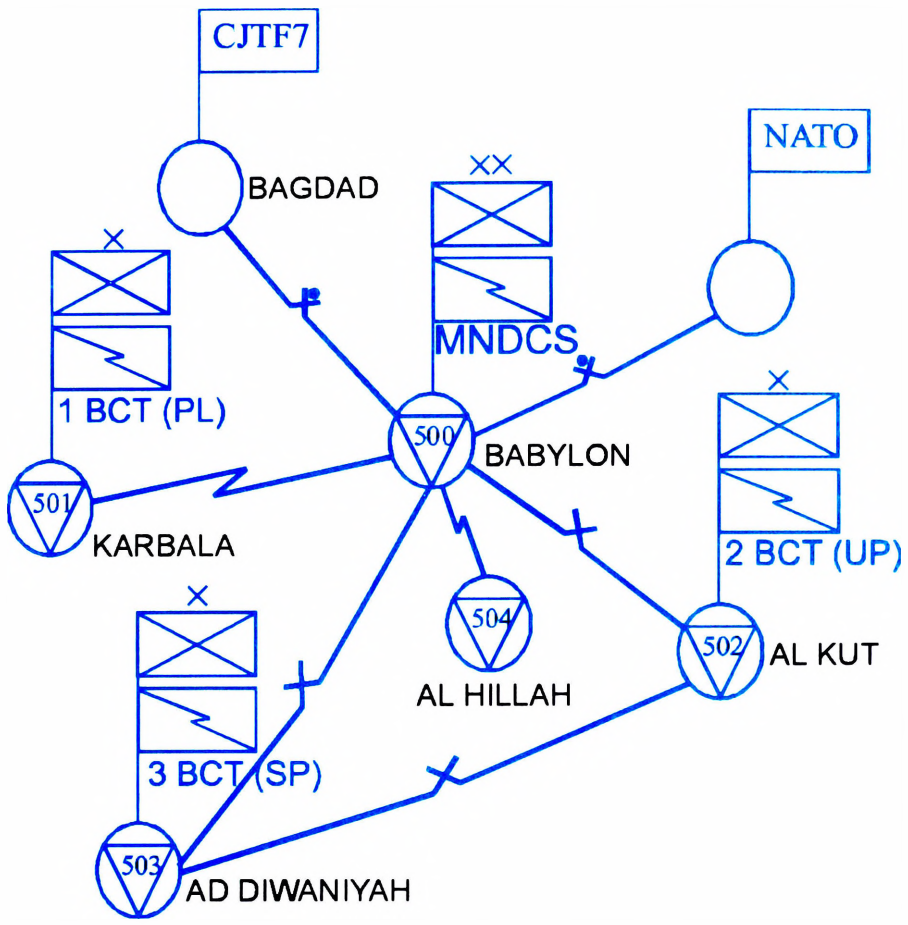
Zgoła odmienny charakter oraz zadania realizowane są przez pododdziały, oddziały i związki taktyczne w ramach drugiego rozważanego w niniejszej dysertacji rodzaju działań taktycznych, którymi są działania pokojowe. Jeśli działania rozstrzygające w ramach narodowych lub sojuszniczych doktryn i dokumentów normatywnych można uznać za sformalizowane, to o działaniach i operacjach pokojowych powiedzieć tego nie można. Wieloletnie doświadczenia w rozwiązywaniu problemów i konfliktów narodowych, czy też międzynarodowych pozwoliły na pewnego rodzaju usystematyzowanie wiedzy na temat użycia i statusu wojsk biorących udział w działaniach pokojowych. Jednak niepowtarzalność każdej operacji pokojowej, jej cel, charakter oraz środowisko (lokalne i globalne), w jakim działania są realizowane przez siły międzynarodowe charakteryzuje się niepowtarzalną i niesklasyfikowaną specyfiką.

Dotychczasowe doświadczenia wyniesione przez nasze narodowe siły zbrojne z udziału w działaniach pokojowych są ogromne. Jednak aktualnie realizowana przez wojska lądowe misja „stabilizacyjna" w Iraku jest pierwszym tak poważnym wyzwaniem. Wynika ono przede wszystkim z faktu, że wojsko polskie, działające w strukturach międzynarodowych, odpowiedzialne jest za organizację i funkcjonowanie systemu dowodzenia na szczeblu związku taktycznego - dywizji wielonarodowej. Stąd też w gestii narodowej odpowiedzialności znajduje się między innymi zadanie organizacji sieci teletransmisyjnej, która stanowiąc integralny element sieci telekomunikacyjnej winna zapewnić systemowi dowodzenia realizację zadania takiego jak obieg i wymiana informacji w relacjach dowodzenia, współdziałania, itd.

Schemat struktury organizacyjnej[76] sieci teletransmisyjnej dywizji wielonarodowej, który funkcjonował w czasie pierwszej zmiany Polskiego Kontyngentu Wojskowego w Iraku, przedstawiony został na rys. 2.3.5.

---

[76] G. Świdzikowski, Bezpieczeństwo informacji w mobilnych systemach telekomunikacyjnych - materiały pokonferencyjne – załącznik - prezentacje, Warszawa, AON, 2004



Rys. 2.3.5 Struktura sieci teletransmisyjnej dywizji wielonarodowej w Iraku podczas I zmiany Polskiego Kontyngentu Wojskowego w Iraku

Źródło: Bezpieczeństwo informacji w mobilnych systemach telekomunikacyjnych - materiały pokonferencyjne, Warszawa, AON, 2004

Dokonując porównania, zarówno w kontekście struktury, jak również organizacji tej sieci, z sieciami teletransmisyjnymi przedstawionymi uprzednio, można zauważyć oraz wyodrębnić następujące zasadnicze różnice:

- struktura sieci zbudowana była w oparciu o układ gwiaździsty;
- nie występują typowe dla działań rozstrzygających elementy ugrupowania bojowego dywizji;
- w strukturze sieci teletransmisyjnej występują tylko i wyłącznie główne stanowiska dowodzenia szczebla dywizji i podległych brygad;
- pomocnicze węzły łączności rozwinięte zostały w rejonie dyslokacji stanowisk dowodzenia (bazy);
- zastosowane środki teletransmisyjne nie opierają się tylko i wyłącznie o radiolinie horyzontowe.

Uwarunkowania organizacyjne, a w tym przede wszystkim względy bezpieczeństwa personelu zapewniającego funkcjonowanie sieci teletransmisyjnej wymusiły

już na etapie planowania określenie miejsca rozwijania pomocniczych węzłów łączności sieci w bezpośredniej bliskości (na obszarze stanowiska dowodzenia dywizji oraz strukturalnie przyporządkowanych trzech brygad). Sieć została zbudowana w układzie gwiaździstym, co oznacza, że z „centralnego punktu" - pomocniczego węzła łączności rozwiniętego w rejonie stanowiska dowodzenia dywizji, wyprowadzane są linie dowiązania do stanowisk dowodzenia podległych brygad. Wyjątek stanowi bezpośrednia linia dowiązania pomiędzy pomocniczymi węzłami łączności rozwiniętymi w rejonach dyslokacji brygad dowodzonych przez Hiszpanów i Ukraińców.

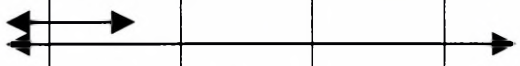
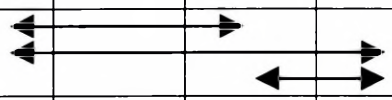
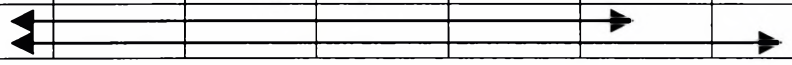
Ze względu na charakter i formę realizowanych zadań w ramach misji stabilizacyjnej w Iraku oddziały i pododdziały dywizji nie tworzą charakterystycznego dla działań rozstrzygających ugrupowania bojowego. Z tej przyczyny również inna jest topologia sieci teletransmisyjnej.

Rozwijana w ramach działań obronnych, czy też podczas natarcia sieć teletransmisyjna budowana jest w oparciu o telekomunikacyjne linie dowiązania, które realizowane są za pośrednictwem radioliniowych (horyzontowych) środków teletransmisyjnych. Stosowanie wymienionych środków w tych przypadkach spełnia wymaganie, jakim jest umożliwienie dowiązania się do sieci poszczególnych elementów ugrupowania bojowego bez względu na miejsce ich rozmieszczenia w pasie obrony lub natarcia dywizji. W przedstawionych przykładach pas ten z reguły wynosił około 40 km szerokości i do 60 km głębokości.

Inaczej z punktu widzenia organizacji sieci teletransmisyjnej sytuacja przedstawia się w przypadku zapewnienia jej funkcjonowania na potrzeby dywizji wielonarodowej w Iraku, której obszar odpowiedzialności obejmuje teren o powierzchni blisko 80 000 km^2. Rozpatrywany problem związany jest przede wszystkim ze standardowymi możliwościami technicznymi sprzętu teletransmisyjnego (patrz rys. 2.5.1). Tory telekomunikacyjne stanowiące linie dowiązania dywizyjnej sieci teletransmisyjnej do przełożonego (CJTF7, NATO) z tego powodu wymagają również zastosowania innego środka teletransmisyjnego. Rodzaje torów telekomunikacyjnych przedstawionych w schemacie na rys. 2.3.5 stanowiących wewnętrzne linie sieci teletransmisyjnej oraz linie dowiązania w relacjach z przełożonym zawarte zostały w tabeli nr 2.3.9.

Tabela nr 2.3.9

Ilość i struktura linii dowiązania sieci teletransmisyjnej Dywizji Wielonarodowej w Iraku podczas I-szej zmiany Polskiego Kontyngentu Wojskowego.

	PWŁ 500	PWŁ 501	PWŁ 502	PWŁ 503	PWŁ 504	CJTF7	NATO
Radioliniowa (horyzontowa) linia dowiązania							
Radioliniowa (troposferyczna) linia dowiązania							
Satelitarna linia dowiązania							

Źródło: opracowanie własne na podstawie G. Świdzikowski, Bezpieczeństwo informacji w mobilnych systemach telekomunikacyjnych - materiały pokonferencyjne – załącznik - prezentacje, Warszawa, AON, 2004

Jak wynika z powyższego zestawienia linie dowiązania realizowane w relacjach pomiędzy elementami dywizji, w których komponent narodowy stanowił większość realizowane były w oparciu o radioliniowe linie horyzontowe – identyczne z wykorzystywanymi w omawianych wcześniej sieciach teletransmisyjnych. Natomiast w relacjach stanowisko dowodzenia dywizji – stanowiska dowodzenia brygad pod dowództwem hiszpańskim i ukraińskim oraz pomiędzy nimi realizowane były za pomocą troposferycznych środków radioliniowych.

Linia dowiązania sieci dywizyjnej do przełożonego (CJTF7) oraz dowiązania do systemu NATO w celu wymiany informacji realizowana była w oparciu o środki satelitarne.

Przedstawione dotychczas wszystkie warianty sieci teletransmisyjnej opierają się na narodowych standardach i koncepcjach organizacji sieci teletransmisyjnej dywizji zmechanizowanej w trakcie prowadzenia przez nią wybranych działań taktycznych.

Trochę odmienną koncepcję organizacji i struktury sieci teletransmisyjnej możemy zauważyć w rozwiązaniach stosowanych przez armię Niemiec. Podstawę sieci teletransmisyjnej w definicyjnym rozumieniu przyjętym w ramach niniejszej dysertacji stanowi system AUTOKO 90.

Przedstawiony na rysunku 2.4.2 schemat sieci teletransmisyjnej dywizji zmechanizowanej w operacji obronnej[77], choć bardzo pobieżnie traktuje aspekty taktyczne

[77] Prezentacja Das Automatisierte Kommunikationsnetz (derzeit: AUTOKO 90)

(poszczególne elementy ugrupowania bojowego dywizji), pozwala jednak na wyodrębnienie kilku charakterystycznych różnic, do których możemy zaliczyć:

- ilość pomocniczych węzłów łączności,
- występowanie stacji retranslacyjnych,
- wyodrębnienie ze struktury pomocniczego węzła łączności stacji radiodostępowych.

Jeśli za podstawę organizacji sieci teletransmisyjnej polskiej dywizji zmechanizowanej przyjmiemy założenia pochodzące z uprzednio cytowanej literatury przedmiotu[78], na których opierały się prezentowane i omawiane schematy sieci, to łatwo zauważyć, że maksymalna liczba występujących w niej pomocniczych węzłów łączności wynosiła 6.

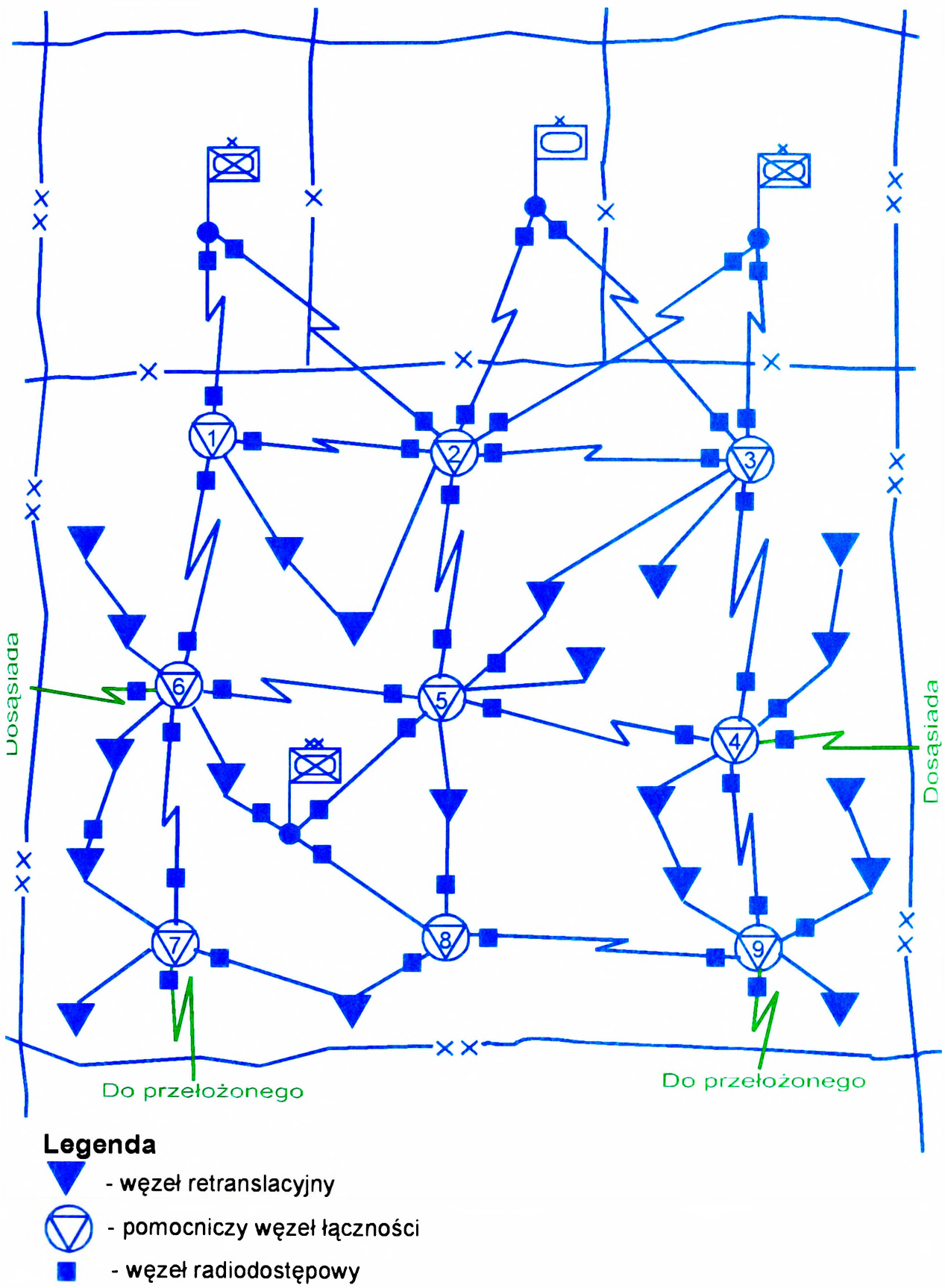
Przedstawiony na rys. 2.3.6 wariant sieci niemieckiej jest bardziej rozbudowany, gdyż w jego strukturze można wyróżnić 9 pomocniczych węzłów łączności (*niem. knotenvermittlung*). W innych dostępnych materiałach[79] na temat systemu AUTOKO 90 można znaleźć stwierdzenie, że docelowo sieć teletransmisyjna rozwijana na szczeblu dywizji bazować będzie na rozwiniętych 12 pomocniczych węzłach łączności. Ponadto kolejnym elementem, który nie występuje w strukturze sieci teletransmisyjnej wg poglądów narodowych jest węzeł retranslacyjny. Jego podstawowym zadaniem jest zapewnienie dowiązania stanowisk dowodzenia, czy ważnych osób funkcyjnych, do sieci teletransmisyjnej, które posiadanymi technicznymi środkami łączności nie są w stanie lub nie mogą dowiązać się do niej bezpośrednio.

Ostatnia zasadnicza różnica organizacyjna pomiędzy analizowanymi sieciami teletransmisyjnymi polega na tym, że w myśl narodowych rozwiązań stacje radiodostępowe stanowią integralną część stanowisk dowodzenia i pomocniczych węzłów łączności. W omawianym wariancie sieci rozwijanej w ramach systemu AUTOKO 90, spełniając te same zadania i funkcje rozmieszczane są one poza elementami stanowiącymi strukturę stanowiska dowodzenia, czy też pomocniczego węzła łączności.

---

[78] m.in. Cyfrowa sieć telekomunikacyjna związku taktycznego wojsk lądowych Storczyk – poradnik łącznościowca, Warszawa, Sztab Generalny WP, 2002, s. 11

[79] AUTOKO 90 – Film reklamowy firmy Siemens



Rys. 2.3.6 Wariant sieci teletransmisyjnej dywizji zmechanizowanej Bundeswehry
Źródło: Prezentacja Das Automatisierte Kommunikationsnetz

Uwzględniając wszystkie wymienione elementy struktury organizacyjnej sieci teletransmisyjnej dywizji Bundeswehry i dokonując jej porównania z podobnymi rozwiązaniami narodowymi (tylko w aspekcie ilości rozwijanych elementów sieci teletransmisyjnej) można stwierdzić, że bardziej złożona jest struktura sieci niemieckiej.

Z drugiej jednak strony biorąc pod uwagę funkcjonalność, należy stwierdzić, że obie sieci realizują te same zadania i spełniają wszystkie wymagania stawiane przez system dowodzenia.

Przyjąwszy zatem jako punkt wyjścia wyniki przeprowadzonej analizy w zakresie struktury sieci telekomunikacyjnej, pojęcie teletransmisji oraz definicję sieci teletransmisyjnej, autor dokonał określenia elementów struktury organizacyjnej sieci teletransmisyjnej, uwzględniając jako determinanty:

- rolę i zadania realizowane przez węzły łączności stanowisk dowodzenia oraz pomocnicze węzły łączności;
- czynniki wpływające na treść, formę i postać informacji lub danych;
- proces przekazywania na odległość informacji i danych.

Analiza podstawowych elementów struktury organizacyjnej sieci telekomunikacyjnej dywizji zmechanizowanej, jakimi są węzły łączności, pozwala dokonać między nimi rozróżnienia według kryterium roli i realizowanych przez nie zadań. Zgodnie z tym kryterium węzły łączności stanowisk dowodzenia dywizji zmechanizowanej oraz jej organicznych lub przydzielonych jednostek winny zapewnić ich użytkownikom łączność wewnętrzną[80] (Główne Stanowisko Dowodzenia - GSD, Tyłowe Stanowisko Dowodzenia – TSD, Wysunięte Stanowisko Dowodzenia - WSD) pomiędzy jego elementami oraz miejscami pracy poszczególnych osób funkcyjnych lub zespołów, czy sekcji w ramach świadczenia określonych usług telekomunikacyjnych, jak również łączność zewnętrzną z abonentami innych stanowisk i punktów dowodzenia. Ponadto węzły te uzupełnia się o wewnętrzne sieci teleinformatyczne danego stanowiska dowodzenia oraz elementy wojskowej poczty polowej[81].

Natomiast pomocnicze węzły łączności, które w ramach taktycznej sieci łączności dywizji rozwijane są w miejscu skrzyżowania się lub zbiegu różnych rodzajów linii telekomunikacyjnych, mają zapewnić optymalny transfer informacji pomiędzy węzłami łączności stanowisk dowodzenia oraz zapewnić dostęp abonentom sieci w trakcie ich przemieszczania się (ruchomym).

---

[80] J. Michniak, Model organizacyjny..., op. cit. s. 46
[81] J. Michniak, Kierowanie mobilnymi..., op. cit., s. 80

Tabela nr 2.3.10

Zadania realizowane przez polowe węzły łączności sieci telekomunikacyjnej

Lp.	Realizowane zadania	WŁ SD	PWŁ
1	Tworzenie i obsługa bezpośrednich połączeń dalekosiężnych	+	
2	Obsługa komutowanych połączeń dalekosiężnych	+	+
3	Tworzenie i obsługa ruchu lokalnego	+	
4	Tworzenie i obsługa lokalnej sieci informatycznej	+	
5	Obsługa poczty polowej	+	
6	Dowiązanie do innych węzłów	+	+
7	Obsługa abonentów ruchomych	+	+
8	Poszukiwanie alternatywnych dróg połączeniowych	+	+
9	Zapewnienie styku międzysystemowego	+	+
10	Utajnianie informacji	+	+
11	Tworzenie dalekosiężnych linii telekomunikacyjnych	+	+
12	Transfer informacji	+	+

Źródło: opracowanie własne na podstawie analizy literatury J. Michniak, „System łączności związku taktycznego i oddziału", AON, Warszawa 1996; M. Lenert, E. Smakulski, „Model systemu łączności korpusu wojsk lądowych", AON, Warszawa 1993

Zasadnicze różnice pomiędzy węzłami łączności (tabela nr 2.3.10), które wynikają z analizy przyjętego kryterium zadaniowego wpływają lub są odzwierciedleniem ich struktury organizacyjnej. Potwierdzeniem tej tezy jest fakt, że wyłączną specyfiką węzłów łączności stanowisk dowodzenia jest grupa wozów dowodzenia, za pomocą których między innymi realizowane są bezpośrednie łącza dalekosiężne rozumiane jako różnego rodzaju relacje radiowe.

Ponadto mimo posiadanych przez pomocnicze węzły łączności możliwości technicznych nie realizują one obsługi ruchu lokalnego, gdyż pełnią one jedynie funkcje umożliwiające dowiązanie się węzłów łączności różnego szczebla stanowisk dowodzenia do sieci taktycznej.

Dodatkowym kryterium umożliwiającym pełniejsze rozróżnienie roli i funkcji węzłów łączności stanowiących integralny element sieci telekomunikacyjnej jest informacja - to co z nią się dzieje lub może się dziać na poszczególnych węzłach łączności w całym cyklu procesu dowodzenia.

Stanowiska dowodzenia wraz z integralnymi elementami węzła łączności jak wewnętrzne sieci abonenckie i lokalne sieci komputerowe są miejscem zbierania, przetwarzania i przechowywania informacji. Ostatnim elementem procesu dowodzenia jest jej przesyłanie zarówno do podwładnych, przełożonych oraz jednostek współdziałających. Natomiast prowadząc identyczną analizę zadań pomocniczych węzłów łączności w aspekcie procesu obiegu informacji w relacjach dowodzenia, współdziałania oraz ostrzegania i alarmowania, można stwierdzić, że realizują one tylko i wyłącznie ostatni z wymienionych elementów tzn. przesyłanie informacji.

Tabela nr 2.3.11

Zadania węzłów łączności wg kryterium informacyjnego

Lp.	Informacja	WŁ SD	PWŁ
1	Zbieranie	+	
2	Przetwarzanie	+	
3	Modyfikowanie	+	
4	Przechowywanie	+	
5	Przesyłanie	+	+

Źródło: opracowanie własne na podstawie literatury przedmiotu (bibliografia)

Wynikiem przeprowadzonej zgodnie z przyjętymi powyżej kryteriami analizy może być uogólnienie, które sprowadza się do stwierdzenia, że strukturalnie i organizacyjnie pomocniczy węzeł łączności stanowi ten element sieci teletransmisyjnej, którego zasadniczym zadaniem jest umożliwienie dowiązania liniami telekomunikacyjnymi węzłów łączności stanowisk dowodzenia rozlokowanych w rejonie odpowiedzialności dywizji oraz zapewnienie dostarczenia (skierowania) opracowanych już informacji w bezpieczny sposób do adresata. Jest to swoista forma retranslacji, która nie wpływa na treść i formę przekazywanej informacji a stanowi jedynie jej warstwę transmisyjną.

Drugim podstawowym elementem po pomocniczym węźle łączności w sieci teletransmisyjnej dywizji zmechanizowanej są linie telekomunikacyjne.

Mając na uwadze cytowane uprzednio definicje sieci teletransmisyjnej i zadane ograniczenia wynikające z przyjętego kryterium zadaniowego oraz wpływu

na treść i formę informacji, to tylko i wyłącznie dla potrzeb niniejszej pracy w dalszych rozważaniach sieć teletransmisyjna będzie traktowana jako:

Całokształt wzajemnie powiązanych pod względem zadań, miejsca i czasu działania pomocniczych węzłów łączności oraz linii telekomunikacyjnych różnego przeznaczenia, rozwijanych wg jednolitego planu w celu zapewnienia transmisji informacji przekazywanych w systemach dowodzenia dywizji i kierowania środkami walki.

W myśl tak przyjętej dla potrzeb niniejszej dysertacji definicji sieci teletransmisyjnej można identyfikować ją ze współczesnym modelem organizacyjnym dwóch sieci[82]: radioliniowo-kablowej oraz sieci radiodostępu dywizji zmechanizowanej. Jej organizacja, jak wynika z prezentowanych wcześniej wariantów sieci, opiera się przede wszystkim na sieci radioliniowo-kablowej o strukturze wielobocznej, którą tworzy od 3 do 6 pomocniczych węzłów łączności[83] (PWŁ) rozlokowanych odpowiednio względem ugrupowania bojowego i połączonych między sobą liniami transmisyjnymi o dużej przepustowości. Zasadnicze elementy sieci radiodostępu, jak stacje dostępowe, stanowią integralną część pomocniczych węzłów łączności.

Sieć radiodostępu ma stanowić swoisty sposób integracji podsystemów łączności radiowej i radioliniowej. Jak dotychczas nie wypracowano w siłach zbrojnych RP jednolitego stanowiska, które pozwoliłyby określić jednoznacznie zasady organizacji oraz strukturę sieci radiodostępu. Aktualnie planowana i propagowana przez pracowników Wojskowej Akademii Technicznej koncepcja realizacji radiodostępu ma polegać na utworzeniu radiowych stacji bazowych, które mają na celu umożliwić:

- realizację połączeń abonentów mobilnych z abonentami stacjonarnymi;
- realizację połączeń między abonentami mobilnymi należącymi do różnych sieci radiowych za pośrednictwem sieci radioliniowo-kablowej;
- realizację połączeń między abonentami tej samej sieci radiowej, z których jeden pracuje stacjonarnie z dowiązaniem do sieci radioliniowo-kablowej i nie może korzystać ze środków radiowych ze względów bezpieczeństwa.

---

[82] J. Janczak, Mobilne sieci łączności.., op. cit., str. 12
[83] Z. Fiołna, P. Daniluk, Koncepcja struktur organizacyjno-technicznych..., op. cit., s. 43

Jednocześnie zarówno w środowisku naukowym jak i technicznym rozpatrywane są dwa warianty możliwości realizacji technicznej, do których można zaliczyć[84]:

- jednokanałowy radiodostęp simpleksowy (JRS) realizowany za pomocą radiostacji TRC 9500 oraz bloku sprzężenia radiowego (BSR) i wykorzystującego numerację abonentów „7 + 2";
- wielokanałowy radiodostęp simpleksowy (WRS), który w wariancie docelowym, stanowić ma autonomiczny podsystem łączności radiowej zapewniający integrację usług pomiędzy systemem łączności radioliniowo-przewodowej i systemem łączności radiowej zgodną z systemem STORCZYK siedmiocyfrową numerację abonentów mobilnych, oparty w głównej mierze o aparatownie WRS.

Jeżeli pierwszy z przedstawionych wariantów jest aktualnie na etapie praktycznego testowania, to drugie z wymienionych rozwiązań technicznych dalej pozostaje w fazie rozważań teoretycznych.

Simpleksowy radiodostęp jednokanałowy zgodnie z obecnymi poglądami realizowany ma być w oparciu o radiostacje pokładowe wozów dowodzenia i wozów dowódczo-sztabowych i ma oferować usługi radiodostępu abonentom należącym do danej sieci radiowej, w której pracuje radiostacja dostępowa. Elementami podsystemu radiodostępu jest punkt radiodostępowy (RPD) oraz radiowe punkty abonenckie (RPA), w stosunku do których punkt radiodostępowy oferuje usługi telekomunikacyjne.

Jak wcześniej wspomniano wozy dowodzenia i wozy dowódczo-sztabowe nie są elementami pomocniczych węzłów łączności, a tym samym nie można ich przypisywać zgodnie z przyjętymi kryteriami do rozpatrywanej sieci teletransmisyjnej.

W związku z powyższym do dalszych rozważań w ramach niniejszej dysertacji, autor przyjął, iż elementem sieci teletransmisyjnej będzie aparatownia wielokanałowego dostępu simpleksowego (AWRS). Jako podsystem autonomiczny łączności radiowej, którego zasadniczym celem i zadaniem ma być integracja systemów i usług telekomunikacyjnych realizowanych przez podsystem łączności radiowej i radiolinio-

[84] Z. Fiołna, Organizacja taktycznych sieci łączności – materiały z sympozjum naukowego, AON, Warszawa 2001, s. 25

wo-kablowej, można przyjąć z dużym prawdopodobieństwem, że aparatownie AWRS będą funkcjonowały w strukturach węzłów łączności stanowisk dowodzenia jak i pomocniczych węzłów łączności, stanowiąc tym samym element sieci teletransmisyjnej dywizji zmechanizowanej.

Zgodnie z przeznaczeniem sieci teletransmisyjnej do pomocniczych węzłów łączności dowiązywane są węzły łączności stanowisk dowodzenia i punktów dowodzenia elementów ugrupowania bojowego dywizji zmechanizowanej. Węzły łączności Głównego Stanowiska Dowodzenia, Tyłowego Stanowiska Dowodzenia dywizji oraz stanowisk dowodzenia brygad dowiązywane są z reguły do dwóch pomocniczych węzłów łączności traktami radioliniowymi oraz dla zwiększenia niezawodności sieci łączności, powinny być dowiązane w miarę możliwości traktem kablowym do najbliższego pomocniczego węzła łączności.

Węzły łączności stanowisk dowodzenia pułków rodzajów wojsk tj.: pułku artylerii, pułku artylerii przeciwpancernej, pułku rakiet przeciwlotniczych są również dowiązywane do dwóch pomocniczych węzłów łączności traktami radioliniowymi, a w zależności od potrzeb lub możliwości – również traktami kablowymi.

Przyjęta powyżej definicja sieci teletransmisyjnej uwzględniająca założone na wstępie niniejszej dysertacji ograniczenia i oddająca pośrednio znaczenie cytowanych uprzednio określeń oraz pojęć transmisji i teletransmisji w powiązaniu z przeprowadzoną analizą dokumentacji wybranych ćwiczeń oraz treningów sztabowych pozwala autorowi na stwierdzenie, że podstawowymi elementami struktury organizacyjnej są:

- ***pomocnicze węzły łączności;***
- ***linie telekomunikacyjne (linie dowiązania).***

2.4 STRUKTURA I ORGANIZACJA POMOCNICZYCH WĘZŁÓW ŁĄCZNOŚCI SIECI TELETRANSMISYJNEJ DYWIZJI ZMECHANIZOWANEJ

Po zdefiniowaniu struktury organizacyjnej sieci teletransmisyjnej dywizji zmechanizowanej w działaniach taktycznych w toku dalszych rozważań przeprowadzona zostanie szczegółowa analiza wyodrębnionych poszczególnych elementów strukturalnych sieci. Pierwszym z nich jest pomocniczy węzeł łączności.

W literaturze przedmiotu[85] w strukturze pomocniczego węzła łączności wyróżniane następujące rodzaje aparatowni:

- Ruchomego Węzła Łączności Cyfrowej (RWŁC-10/K) zwanej także aparatownią komutacyjną (AK),
- Ruchomego Węzła Łączności Cyfrowej (RWŁC-10/T) zwanej także aparatownią transmisyjną (AT),
- Aparatownia Wielodostępu Radiowego Simpleksowego (AWRS);
- Polowy terminal satelitarny (Pasat).

które wchodzą w skład następujących zespołów funkcjonalnych (rys. 2.5.1):

- grupy środków teletransmisyjnych,
- centrum komutacji.

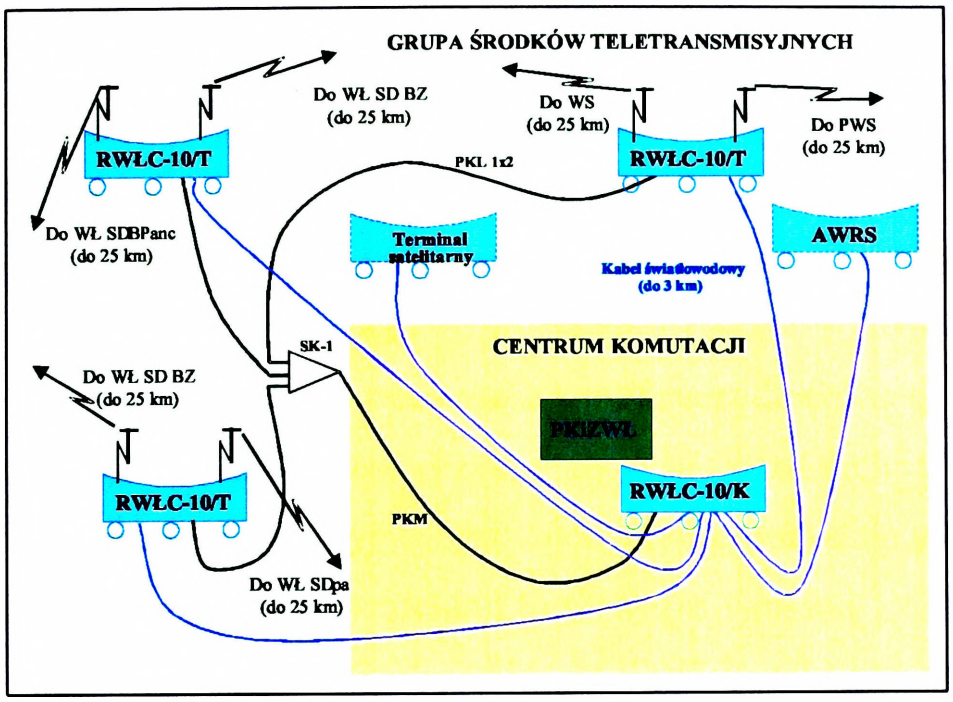
Grupę środków teletransmisyjnych w przedstawionym wariancie struktury pomocniczego węzła łączności stanowią trzy aparatownie teletransmisyjne oraz jedna aparatownia wielokanałowego radiodostępu.

Ponadto autorzy omawianego wariantu pomocniczego węzła łączności sieci teletransmisyjnej w grupie środków teletransmisyjnych wyróżniają terminal satelitarny. Jednak, jak sami zauważają polowy terminal satelitarny lub ewentualnie zamiennie stosowana stacja troposferyczna może wejść w skład pomocniczego węzła łączności tylko w sytuacjach szczególnych. Jej zasadniczym celem jest zapewnienia łączności w relacjach z przełożonym lub dowództwem (np. NATO) pod auspicjami, którego dana operacja lub zadanie jest realizowane. Przykładem praktycznego zastosowania tego

---

[80] m.in. „Projektowanie, budowa oraz rozwijanie stacji łączności utajnionej stacjonarnych i polowych węzłów łączności" – Szefostwo Wojsk Łączności sygn. Łączn. 624/76, s.36; J. Janczak, Mobilne sieci łączności – album schematów, AON, Warszawa 200, s. 27; Cyfrowa sieć telekomunikacyjna związku taktycznego wojsk lądowych „Storczyk" – poradnik łącznościowca, Warszawa, Sztab Generalny WP, 2002, s. 41

rozwiązania może być omawiana i prezentowana na rys. 2.3.5 sieć teletransmisyjna Dywizji Wielonarodowej w Iraku.



Rys.2.4.1 Struktura pomocniczego węzła łączności sieci teletransmisyjnej dywizji (wariant)

Źródło: J. Janczak, Mobilne sieci łączności – album schematów, AON, Warszawa 2003

Koncepcje dotyczące przeznaczenia i wykorzystania czy to terminalu satelitarnego, czy też stacji troposferycznej, z którymi można aktualnie się spotkać[86] wskazują jednak, że tego typu środki łączności planowane będą raczej do zapewnienia bezpośrednich relacji dowodzenia – stąd też wydaje się uzasadnione stwierdzenie, że bardziej odpowiednim miejscem ich rozwinięcia niż pomocniczy węzeł łączności jest węzeł lub węzły łączności stanowisk dowodzenia określonego szczebla dowodzenia.

Jeśli jednak w procesie planowania systemu teletransmisyjnego dywizji przyjęty zostanie wariant dyslokacji polowego terminala satelitarnego i umieszczenie go w strukturze pomocniczego węzła łączności, to nie należy przyjmować tego wariantu jako standardowego rozwiązania, które dotyczy wszystkich pomocniczych węzłów łączności rozwijanych w ramach organizacji danej sieci. Ilość terminali, miejsce ich rozwinięcia i sposób wykorzystania uwarunkowany jest indywidualnymi wymaganiami systemu dowodzenia.

[86] G. Świdzikowski, Bezpieczeństwo informacji w mobilnych systemach telekomunikacyjnych wojsk lądowych – materiały pokonferencyjne, załącznik nr 2, Warszawa, AON, 2004

Jeśli przyjmiemy, że wymienione w grupie środków teletransmisyjnych aparatownie i urządzenia stanowią podstawę sieci teletransmisyjnej, to wówczas struktura i organizacja każdego pomocniczego węzła łączności zależna jest od dwóch zasadniczych elementów takich jak:

- ilość rozwijanych w ramach danego węzła dalekosiężnych linii radiowych i kablowych,
- możliwości technicznych aparatowni teletransmisyjnej[87] rozwijanej w ramach pomocniczego węzła łączności.

Oba wymienione czynniki determinujące strukturę pomocniczego węzła łączności są na równi istotne. Jeśli jednak przyjmiemy i ściśle zdefiniujemy możliwości techniczne aparatowni teletransmisyjnej oraz założymy, że wszystkie aparatownie charakteryzują się tymi samymi możliwościami to wówczas struktura pomocniczego węzła łączności zależna będzie przede wszystkim od ilości wymienionych powyżej linii dowiązań.

W związku z powyższym do dalszych rozważań pozwalających na dokonanie oceny bezpieczeństwa informacji w sieci teletransmisyjnej przyjęty zostanie wariant rozmieszczenia terminala satelitarnego na jednym pomocniczym węźle łączności.

Podstawowy środek teletransmisyjny w omawianym wariancie struktury pomocniczego węzła łączności stanowią cyfrowe zestawy urządzeń radioliniowych oraz traktów przewodowych i światłowodowych. Zamontowane na aparatowniach transmisyjnych urządzenia radioliniowe, przewodowe i światłowodowe przeznaczone są do organizowania teletransmisyjnych linii międzywęzłowych, linii dowiązania do systemu teletransmisyjnego szczebla nadrzędnego oraz do węzłów łączności stanowisk dowodzenia dywizji, brygad, pułków, batalionów itp. oraz/lub innych elementów ugrupowania bojowego dywizji.

Indywidualnie każda aparatownia transmisyjna[88] funkcjonalnie umożliwia jednoczesne przyjęcie:

- do trzech traktów radioliniowych,

---

[87] Aparatownia teletransmisyjna to stacja telekomunikacyjna zawierająca urządzenia teletransmisyjne, wchodzące w skład linii telekomunikacyjnej, w których przesyłane sygnały elektryczne poddawane są odpowiedniemu przetwarzaniu. Przy czym przetwarzanie sygnału może polegać na ich wzmacnianiu, regeneracji, przemianie częstotliwościowej - Krystyn Plewko, Biuletyn informacyjny 2-3, Instytut Łączności, Warszawa 1990, s. 39

[88] Polowy system łączności cyfrowej „STORCZYK 2000" - materiały reklamowe firmy „TRANSBIT"

- do ośmiu traktów kablowych,
- do czterech traktów światłowodowych,
- do 30 abonentów analogowych i cyfrowych,
- utajnianie maksymalnie sześciu linii dowiązania.

Ponadto w grupie środków transmisyjnych wyróżniona została aparatownia wielokanałowego radiodostępu simpleksowego, której podstawowym zadaniem jest zapewnienie dowiązania do sieci teletransmisyjnej dywizji abonentów mobilnych. Jak wcześniej już wspomniano system radiodostępu wielokanałowego jest aktualnie na etapie opracowania koncepcji jego funkcjonowania oraz zasad eksploatacji. Z tej też przyczyny do dalszych rozważań w ramach niniejszej dysertacji przyjęte zostanie, że aparatownia AWRS zapewni dowiązanie się do jednego pomocniczego węzła łączności maksymalnie 8 abonentom ruchomym,

Ostatnim elementem wyróżnionym w grupie środków transmisyjnych jest polowy terminal satelitarny, który zapewnienia uprawnionym (wydzielonym) abonentom sieci wymianę informacji z osobami funkcyjnymi pracującymi zarówno w ramach sieci (znajdujących się w obszarze działania dywizji) jak i poza nią.

Drugim funkcjonalnym elementem pomocniczego węzła łączności jest centrum komutacji. Stanowi ono zespół wzajemnie ze sobą powiązanych łącznic cyfrowych znajdujących się na wyposażeniu aparatowni komutacyjnej i aparatowni transmisyjnych.

Podstawową funkcją centrum komutacji jest automatyczne zestawianie (i rozłączanie) dalekosiężnych połączeń tranzytowych dla zgłoszeń generowanych przez dowiązane do taktycznej sieci łączności węzły stanowisk dowodzenia oraz dla zgłoszeń generowanych przez abonentów miejscowych (personel pomocniczego węzła łączności). Zestawianie (rozłączanie) połączeń powinno się odbywać niezależnie od rozmieszczenia abonentów w sieci łączności i rodzajów (typów) posiadanych przez nich urządzeń końcowych.

Aparatownia komutacyjna w ramach pomocniczego węzła łączności umożliwia[89]:

- przyjęcie traktów od 3 aparatowni transmisyjnych,

[89] Polowy system łączności cyfrowej „STORCZYK 2000" - materiały reklamowe firmy „TRANSBIT"

- przyjęcie do szesnastu cyfrowych traktów kablowych,
- przyjęcie do czterech traktów światłowodowych,
- do 90 abonentów analogowych i cyfrowych,
- utajnianie 12 linii (niezależnie od typu).

Pomocniczy węzeł łączności powinien być zarządzany i sterowany[90] przez jednego operatora, ze stanowiska pracy znajdującego się w aparatowni komutacyjnej. Stanowisko powinno być wyposażone w zespół urządzeń łączności służbowej, urządzeń zbierania, rejestrowania i zobrazowania danych o stanie łączności i stanie sieci łączności, urządzenie rejestrowania i przekazywania komend i sygnałów, umożliwiające efektywne kierowanie węzłem łączności.

Stanowisko powinno zapewniać[91]:

- sterowanie urządzeniami własnej aparatowni komutacyjnej oraz podległymi aparatowniami transmisyjnymi;
- kontrolę stanu łączności dalekosiężnej przez wyświetlanie mapy aktualnego stanu traktów z podaniem przepływności, jakości (stopy błędów), natężenia ruchu, numerów węzłów sąsiednich, przy czym trakty niesprawne powinny być oznaczone kolorem czerwonym. Operator powinien posiadać możliwość zamknięcia każdego traktu w pętlę w aparatowni komutacyjnej lub aparatowni transmisyjnej (także w radioliniach, regeneratorach lub konwerterach światłowodowych) w celu przeprowadzenia pomiarów przez łącznicę lub też skierowania traktu na dodatkowy przyrząd pomiarowy;
- kontrolę stanu aparatów abonenckich i linii do tych aparatów (jeżeli aparaty takie są rozwijane);
- kontrolę działania sieci przez wyświetlanie listy aktualnie realizowanych połączeń, z sygnalizacją (kolorem czerwonym) przypadków nieprawidłowych, wynikających z błędów abonentów (wybieranie numerów nieistniejących, nie zgłaszanie się abonenta wywoływanego) lub z winy sieci (przerwanie traktów, uszkodzenia linii i aparatów itp.);

---

[90] Z. Fiołna, P. Daniluk, Koncepcja sieci łączności wojsk lądowych w działaniach taktycznych perspektywicznego pola walki...op. cit. s. 79

[91] J. Janczak, Mobilne sieci łączności – album schematów.... op. cit. s. 98

- obsługę łączy do systemów publicznych (jeżeli dany PWŁ takie łącza przyjmuje);
- dokumentowanie wyżej wymienionych danych dla celów rozstrzygania ewentualnych konfliktów i reklamacji.

Przedstawiona powyżej struktura organizacyjna i funkcjonalna pomocniczego węzła łączności oraz wyposażenie i możliwości techniczne poszczególnych jego elementów składowych pozwalającą na określenie indywidualnej struktury organizacyjnej pomocniczych węzłów łączności każdej z rozpatrywanych wcześniej sieci teletransmisyjnych dywizji zmechanizowanej w ramach prowadzonych przez nią działań obronnych oraz natarcia.

2.5 STRUKTURA ORGANIZACYJNO-TECHNICZNA LINII TELEKOMUNIKACYJNYCH (ODCINKÓW MIĘDZYWĘZŁOWYCH) SIECI TELETRANSMISYJNEJ DYWIZJI ZMECHANIZOWANEJ

Drugim z wyodrębnionych elementów będących w składzie zarówno sieci telekomunikacyjnej jak i teletransmisyjnej dywizji zmechanizowanej są linie telekomunikacyjne.

Podczas analizy literatury przedmiotu autor spotkał się w publikacjach z różną ich klasyfikacją. Podstawa wyróżnienia w każdej z cytowanej sytuacji zależna była od przyjętego kryterium. Stąd też jeśli jako kryterium przyjęta zostanie pełniona przez linie telekomunikacyjne w danej sieci funkcja, to wówczas wyróżniane są linie abonenckie i dalekosiężne[92]. Natomiast w odniesieniu do ich przeznaczenia klasyfikacja jest następująca: linie bezpośrednie, międzywęzłowe oraz linie dowiązań[93].

Kolejnym determinantem umożliwiającym dokonanie wyróżnienia może być rodzaj środka teletransmisyjnego w oparciu, o który budowana jest linia telekomunikacyjna, to wówczas możemy dokonać następującego rozróżnienia:

- linia przewodowa,
- linia światłowodowa,
- linia radiowa,

---

[92] J. Mazurkiewicz, W. Kulma, System dowodzenia..., op. cit., s. 197
[93] M. Kowalewski, System łączności...., op. cit., s. 267-276

– linia radioliniowa,
– linia satelitarna,
– linia świetlna,
– linia mieszana,
– inne.

Z drugiej strony dokonywany jest podział, którego podstawą jest kryterium organizacji linii telekomunikacyjnych. Jest on czytelniejszy i bardziej przejrzysty patrząc się na zagadnienie od strony praktycznej. Zgodnie z cytowanym kryterium linie mogą tworzyć sieci telekomunikacyjne o architekturze[94]:

– układu gwiaździstego,
– układu złożonego,
– układu wielobocznego (wielowęzłowego),
– układu mieszanego.

W układzie gwiaździstym, linie telekomunikacyjne rozwijane są od centralnego węzła telekomunikacyjnego sieci (najczęściej był to węzeł łączności głównego stanowiska dowodzenia danego szczebla dowodzenia) do podległych i współdziałających organów dowodzenia.

W układzie złożonym linie telekomunikacyjne tworzą kilka wzajemnie połączonych układów gwiaździstych rozwijanych na bazie węzłów łączności stanowisk dowodzenia danego szczebla dowodzenia. Połączenie pojedynczych układów gwiaździstych sieci telekomunikacyjnej zapewnia się pojedynczymi liniami telekomunikacyjnymi łączącymi węzły łączności poszczególnych układów gwiaździstych.

W układzie wielobocznym (wielowęzłowym) linie telekomunikacyjne tworzą układ przestrzennie rozmieszczony, który z uwagi na swoją konfigurację może być nazywany: kratą, siatką, wielobokiem itp. Taki układ powstaje, gdy w punktach przecięcia się linii telekomunikacyjnych rozwijane są węzły telekomunikacyjne przeznaczone do sprzęgnięcia potencjału transmisyjnego tych linii w kompleksowy układ umożliwiający zestawienie odpowiednich rozpływów traktów, czy też kanałów i ich dystrybucji w zależności od potrzeb na odpowiednie kierunki (relacje) łączności.

---

[94] J. Michniak, Kierowanie mobilnymi..., op. cit., s. 83

W układzie mieszanym linie telekomunikacyjne rozwijane są przede wszystkim w układzie wielobocznym, a w najważniejszych relacjach uzupełniane liniami telekomunikacyjnymi rozwiniętymi w układzie gwiaździstym.

Wybór jednego z opisanych powyżej wariantów organizacji sieci w głównej mierze ***determinuje ciągłość działania wojskowej polowej sieci telekomunikacyjnej, a tym samym jej podstawowego elementu sieci teletransmisyjnej na określonym obszarze pola walki (operacji) oraz zależny jest od ilości posiadanych sił i środków łączności.***

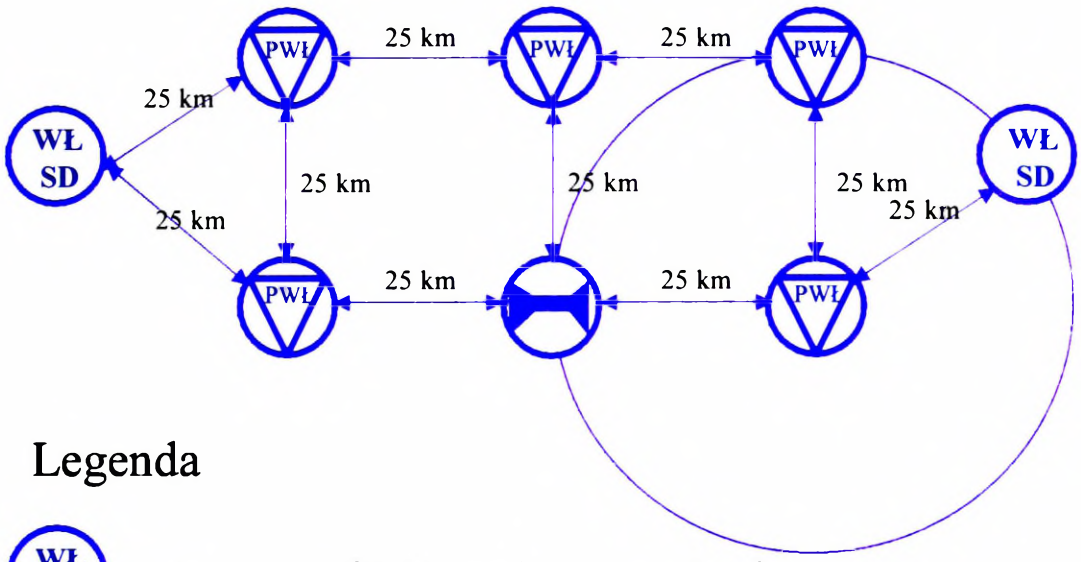
Posiadając tak usystematyzowaną wiedzę w zakresie kryteriów pozwalających na przeprowadzenie klasyfikacji oraz organizacji linii telekomunikacyjnych autor dokonał ich porównania z wnioskami, które uzyskał podczas analizy dokumentacji rozpatrywanych w rozdziale 2.3 ćwiczeń oraz treningów sztabowych.

Pozwoliło to na sformułowanie następujących wniosków:

1. Stosując jako kryterium pełnioną przez linię telekomunikacyjną funkcję to w strukturze sieci teletransmisyjnej wyróżnić możemy tylko i wyłącznie linie dalekosiężne. Zgodnie z przyjętymi podczas definiowania pojęcia sieci teletransmisyjnej linie abonenckie są domeną węzłów łączności stanowisk dowodzenia
2. Przy zastosowaniu determinanta jakim jest przeznaczenie linii telekomunikacyjnych, wówczas w poddanych analizie wariantach sieci teletransmisyjnych wyróżniono linie międzywęzłowe (pomiędzy poszczególnymi pomocniczymi węzłami łączności) oraz linie dowiązań (element ugrupowania bojowego – pomocniczy węzeł łączności). Pod uwagę nie są brane linie bezpośrednie, które z reguły rozwija się w relacjach pomiędzy stanowiskami dowodzenia.
3. W rozpatrywanych przykładach sieci teletransmisyjnej autor wyodrębnił linie przewodowe, światłowodowe, radiowe, radioliniowe, satelitarne, których występowanie determinowały zastosowane środki teletransmisyjne.
4. Podstawą organizacji linii telekomunikacyjnych jest układ wielowęzłowy (patrz rys. 2.5.1).

Ponadto, jak już wcześniej wspomniano na strukturę i organizację sieci teletransmisyjnej, a w tym na występujące w niej linie telekomunikacyjne mają wpływ środki

transmisyjne - ich rodzaj oraz możliwości techniczne. Od nich bowiem między innymi zależy maksymalna długość linii telekomunikacyjnej, która warunkuje odległość pomiędzy poszczególnymi pomocniczymi węzłami łączności. W literaturze przedmiotu[95] przyjmuje się, że odległości te wynoszą do 25 km (rys. 2.5.1) i zależą od rzeźby, pokrycia i ukształtowania obszaru, na którym rozwijana jest sieć teletransmisyjna.



Rys. 2.5.1 Maksymalne odległości pomiędzy węzłami łączności sieci teletransmisyjnej dywizji zmechanizowanej
Źródło: J. Janczak, Mobilne sieci łączności – album schematów, AON, Warszawa 2003

Zebrane w toku dotychczasowych rozważań wnioski w zakresie struktury i organizacji sieci teletransmisyjnej dywizji podczas prowadzenia przez nią działań taktycznych, a szczególnie jej zasadniczych elementów składowych stanowić będą podstawę dokonania przez autora w dalszej części niniejszej dysertacji wyboru jednego z rozpatrywanych wariantów sieci, który poddany zostanie ocenie pod względem spełniania przez niego podstawowych wymagań bezpieczeństwa informacji.

[95] Z. Fiołna, P. Daniluk, Koncepcja struktur organizacyjno-technicznych...., op. cit. s. 51

2.6. WYBÓR WARIANTU SIECI TELETRANSMISYJNEJ PODDANEGO OCENIE POD WZGLĘDEM BEZPIECZEŃSTWA PRZESYŁANEJ INFORMACJI

Mając na uwadze główny problem badawczy rozpatrywany w ramach niniejszej dysertacji zasadnym wydaje się dokonanie wyboru jednego z prezentowanych wariantów sieci, która stanowić będzie podstawę przeprowadzenia oceny stanu bezpieczeństwa informacji w sieci teletransmisyjnej dywizji zmechanizowanej. Sytuacja ta pozwoli na urealnienie i zbliżenie do rzeczywistości prowadzone badania w zakresie stanu bezpieczeństwa informacji w danej rzeczywistej sytuacji taktycznej.

Wychodząc z tego założenia do dalszych rozważań przyjęty zostanie jeden z omówionych narodowych wariantów sieci teletransmisyjnej. Decyzja o rozpatrywaniu narodowego wariantu sieci wynika z faktu, iż zarówno procedury bezpieczeństwa jak i rozwiązania organizacyjne czy techniczne w zakresie sposobów i środków ochrony stanowią informacje prawnie chronione, do których dostęp ograniczony jest tylko do niezbędnego personelu narodowego. Stąd też nie znając wszystkich rozwiązań i uwarunkowań trudno byłoby oceniać stan bezpieczeństwa informacji w sieci teletransmisyjnej związku taktycznego innego państwa przez pryzmat narodowych standardów czy nawet wymagań sojuszniczych.

Aby dokonać rzetelnie wyboru sieci teletransmisyjnej, należy przyjąć jasne i klarowne kryteria, które umożliwią realizację zamierzonego celu. Z dotychczasowej praktyki i doświadczeń zawodowych autora w dziedzinie ochrony informacji, które w pełni zgodne są z wyrażonymi opiniami ekspertów (załącznik nr 5) można stwierdzić, ***że każdy punkt, element lub zespół funkcjonalny systemu (sieci) łączności i informatyki traktowany jest przez specjalistów w dziedzinie bezpieczeństwa jako potencjalne miejsce nieplanowanego (nieautoryzowanego) wypływu lub dostępu do informacji podlegającej ochronie***. Stanowisko powyższe odnosi się do ogółu wojskowych systemów i sieci rozwijanych zarówno w warunkach stacjonarnych jak i polowych.

Przenosząc tak sprecyzowane stanowisko na grunt pojęciowy sieci teletransmisyjnej to wówczas można założyć, iż zdarzenie polegające na możliwości niekontrolowanego lub nieplanowanego ujawnienia informacji może wystąpić w każdym funk-

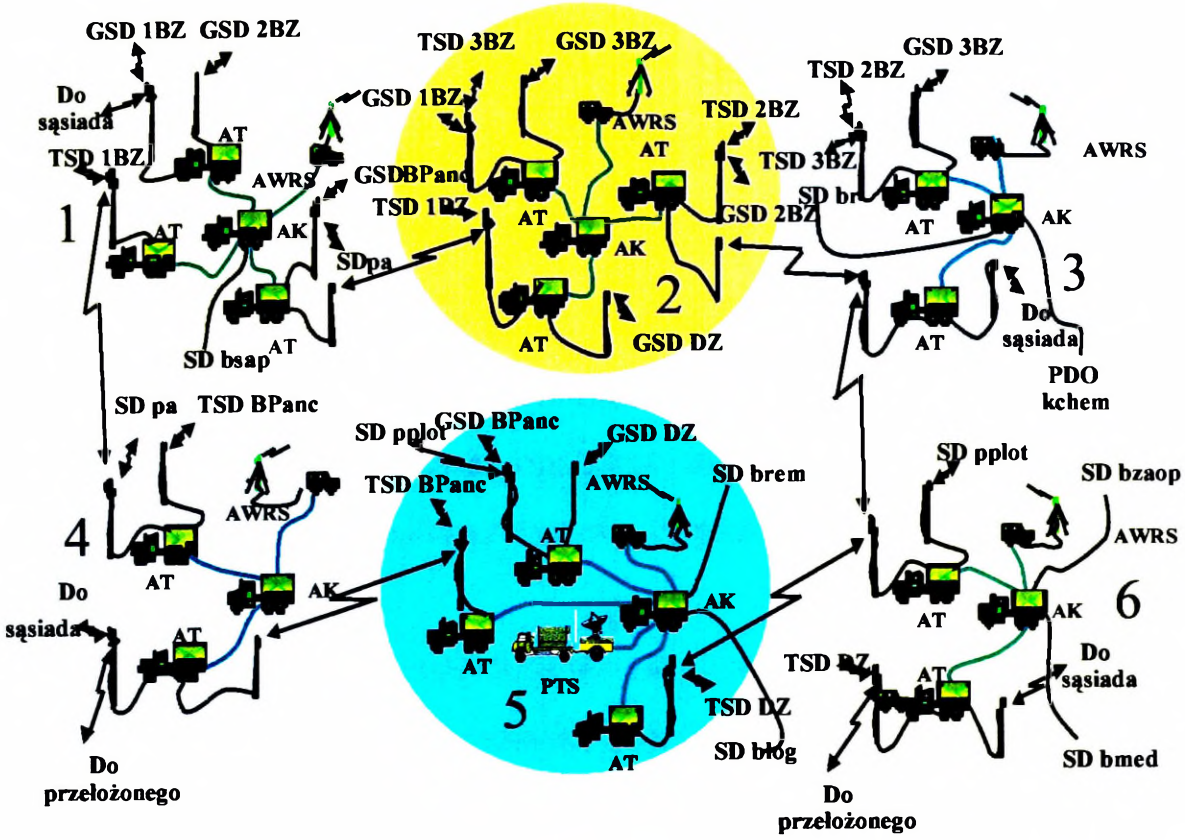
cjonalnym elemencie sieci teletransmisyjnej tj. zarówno w liniach telekomunikacyjnych (radiowa, radioliniowa, przewodowa, itd.) czy też na pomocniczych węzłach łączności lub nawet poszczególnych urządzeniach (aparatowniach) wchodzących w skład jego struktury organizacyjnej. Incydenty oraz zagrożenia sprzyjające wystąpieniu rozpatrywanego zdarzenia lub ciągu zdarzeń poddane zostaną analizie w jednym z kolejnych rozdziałów dysertacji.

Uogólnienie dotychczas prowadzonego rozważania sprowadza się do wniosku, że zasadniczym kryterium determinującym wybór sieci teletransmisyjnej podlegającej ocenie pod względem bezpieczeństwa przesyłanej w niej informacji powinien być czynnik ***„ilościowy”.***

Stąd też po przeprowadzeniu analizy struktur rozważanych sieci teletransmisyjnych zgodnie z przyjętym kryterium do dalszych rozważań w aspekcie bezpieczeństwa informacji przyjęta została sieć teletransmisyjna zaplanowana i zorganizowana w ramach ćwiczenia pk. „Donośna Surma 2003”.

W przyjętym wariancie sieci teletransmisyjnej zasadniczym środkiem teletransmisyjnym sieci są dalekosiężne linie radiowe, które fizycznie realizowane są za pomocą horyzontowych środków radioliniowych. Zapewniają one wzajemne połączenie poszczególnych pomocniczych węzłów łączności pomiędzy sobą (linie międzywęzłowe) oraz dołączenie do nich węzłów łączności głównych i tyłowych stanowisk dowodzenia związków taktycznych oraz oddziałów (linie dowiązania). Stanowiska dowodzenia samodzielnych pododdziałów dywizji dowiązywane są do sieci za pośrednictwem pomocniczych węzłów łączności przy użyciu dalekosiężnych linii kablowych.

Opierając się na tabelarycznym zestawieniu traktów radioliniowych i przewodowych (tabele 2.3.5 i 2.3.6) sieci teletransmisyjnej ćwiczenia pk. „Donośna Surma 2003” oraz przyjętych założeniach w zakresie organizacji i możliwościach technicznych aparatowni wchodzących w skład struktury pomocniczego węzła łączności na rysunku 2.6.1 przedstawiona została rozpatrywana sieć teletransmisyjna dywizji zmechanizowanej uwzględniająca indywidualne wyposażenie każdego pomocniczego węzła łączności.



Rys. 2.6.1 Organizacja badanej sieci teletransmisyjnej dywizji zmechanizowanej uwzględniająca indywidualną strukturę pomocniczych węzłów łączności.

Źródło: opracowanie własne na podstawie dokumentacji ćwiczenia dowódczo-sztabowego „Donośna Surma 2003"

Reasumując prowadzone dotychczas rozważania w aspekcie zasad organizacji oraz struktury organizacyjnej sieci teletransmisyjnej dywizji zmechanizowanej podczas prowadzenia przez nią działań taktycznych oraz uwzględniając uprzednio przyjęte założenia w zakresie ilości miejsc oraz punktów wrażliwych przedstawiona na rys. 2.6.1 szczegółowa struktura organizacyjna i funkcjonalna sieci teletransmisyjnej stanowić będzie materiał wyjściowy w zakresie oceny spełniania przez nią narodowych oraz sojuszniczych wymagań i standardów bezpieczeństwa przesyłanej w niej informacji.

3. WYMAGANIA NARODOWE I SOJUSZNICZE STAWIANE BEZPIECZNEJ SIECI TELETRANSMISYJNEJ DYWIZJI ZMECHANIZOWANEJ.

Zaczynając rozważania na temat określenia wymagań narodowych i sojuszniczych stawianych bezpiecznej sieci teletransmisyjnej dywizji zmechanizowanej należy w pierwszej kolejności zdefiniować ogólne wymagania stawiane łączności wojskowej, które pozwolą jednocześnie skonkretyzować wymagania dla wojskowego systemu telekomunikacyjnego.

Pozwoli to na wyjaśnienie podstawowych pojęć i terminologii używanej w ramach niniejszej dysertacji oraz umożliwi określenie roli i miejsca pojęcia bezpieczeństwa w strukturze wymagań stawianych wojskowemu systemowi telekomunikacyjnemu.

Zamierzonym efektem stanowiącym zakończenie rozdziału będzie zdefiniowanie pojęcia bezpieczeństwa informacji i określenie wymagań stawianych bezpiecznej sieci teletransmisyjnej związku taktycznego (dywizji zmechanizowanej) według poglądów narodowych oraz w myśl dokumentów normatywnych Organizacji Paktu Północnoatlantyckiego.

3.1 WYMAGANIA BEZPIECZEŃSTWA STAWIANE WOJSKOWEMU POLOWEMU SYSTEMOWI ŁĄCZNOŚCI

Gdy mówimy o wojskowym systemie telekomunikacyjnym to mamy na myśli zbiór złożonych oraz zespolonych ze sobą obiektów (urządzeń), które rozmieszczone są na określonym obszarze celem zapewnienia wymiany informacji dla potrzeb dowodzenia, kierowania i sterowania środkami rażenia.

System taki funkcjonuje w specyficznym otoczeniu, którego odzwierciedleniem zarówno w warunkach pokoju, kryzysu czy też konfliktu zbrojnego jest stała możliwość oddziaływania na niego przez potencjalnego przeciwnika.

Oddziaływanie takie ma wieloraki charakter i może być stosowane na wiele sposobów przy użyciu różnych sił i środków, których zasadniczym zadaniem jest uniemożliwienie realizacji podstawowego celu funkcjonującego systemu tj.

przekazywania informacji w systemie dowodzenia i sterowania środkami rażenia. Utrudnienie lub wręcz sparaliżowanie systemu dowodzenia wojskami można osiągnąć m.in. poprzez rażenie ogniowe we wszelkich dostępnych formach i metodach Stanowisk Dowodzenia (SD), ale także węzłów łączności SD, pomocniczych węzłów łączności (PWŁ) oraz innych wrażliwych elementów systemu telekomunikacyjnego, których zniszczenie bądź obezwładnienie radioelektroniczne będzie miało zasadniczy wpływ na wymagania stawiane łączności.

Dla osiągnięcia celu bezpieczeństwa łączności należy zaplanować i zrealizować szereg zadań, których wykonanie zagwarantuje spełnienie wymagań, jakie stawia się przed łącznością. Z celu jaki stawia się łączności do osiągnięcia, wynikają jej zadania[96]:

- zapewnienie dowódcy i sztabowi dowodzenia wojskami oraz sterowania środkami rażenia;
- zapewnienie współdziałania pomiędzy związkami taktycznymi (oddziałami, pododdziałami) organicznymi, przydzielonymi i wspierającymi oraz z sąsiadami;
- zapewnienie przekazywania sygnałów powiadamiania ostrzegania i alarmowania;
- zapewnienie wymiany wiadomości dla potrzeb kierowania organami regulacji ruchu, przekazywania i otrzymywania danych o sytuacji meteorologicznej, a także sygnałów wzajemnego rozpoznania i służby czasu.

Zadania powyższe realizowane są w następstwie wymagań stawianych przez dowodzenie, które winno być ciągłe, trwałe, operatywne i skryte.

Poprzez analizę przedstawionych powyżej wymagań w stosunku do systemu dowodzenia można wykazać, że są one ściśle związane z wymaganiami stojącymi przed łącznością, do których zalicza się[97]:

- ***terminowość łączności***, która wpływa na ciągłość dowodzenia; w przypadku dowodzenia za pomocą technicznych środków łączności, jest miernikiem gotowości organów dowodzenia do realizowania procesów dowodzenia; termi-

[96] J. Michniak, A. Wisz, Bezpieczeństwo i ochrona informacji w wojskowych sieciach telekomunikacyjnych i zautomatyzowanych systemach dowodzenia....op. cit., s. 9
[97] J. Michniak, Bezpieczeństwo i ochrona...., op. cit., s. 10

nowość łączności wpływa na operatywność dowodzenia tzn. szybkie reagowanie na zmiany sytuacji na polu walki jest uzależnione od zdolności łączności do przekazywania rozkazów, zarządzeń, meldunków itp.;

- ***wierność łączności*** jest niezbędna do zapewnienia ciągłości i operatywności dowodzenia, oddziaływanie przeciwnika może powodować zmniejszenie wierności łączności - tylko zdolność do odtworzenia u odbiorcy poprawnych treści przekazywanych wiadomości może zapewnić wykonanie zadania, a tym samym wpływa na efektywność dowodzenia;
- ***skrytość łączności*** - utrzymanie w tajemnicy treści przekazywanych wiadomości oraz samego faktu i miejsca ich przekazywania, w dużym stopniu zapewnia osiąganie skrytości dowodzenia.

Syntetyzując wszystkie trzy wymienione cechy łączności można przypisać im jedno wspólne pojęcie nazwane jakością łączności.



Rys. 3.1.1 Jakościowe cechy łączności wojskowej
Źródło: J. Michniak, A. Wisz, Bezpieczeństwo i ochrona informacji w wojskowych sieciach telekomunikacyjnych i zautomatyzowanych systemach dowodzenia, AON, Warszawa 2000

W takim ujęciu jakościowe cechy łączności są wzajemnie od siebie uzależnione, przy czym relacje te zależne są od konkretnych sytuacji i warunków.

Biorąc pod uwagę najbardziej uznawane wymagania łączności wojskowej oraz uwzględniając wpływ otoczenia, można określić wymagania jakie musi spełniać system łączności wojskowej.

Zgodnie z danymi przedstawionymi na rysunku 3.2 wymagania stawiane wojskowemu systemowi łączności to:

- ***stała gotowość bojowa*** jako zdolność przystąpienia do zapewnienia dowodzenia wojskami i sterowania środkami rażenia w czasie określonym przez do-

wództwo, po zmianie struktury systemu spowodowanej przejściem w wyższy stan gotowości bojowej lub wymuszonej sytuacją operacyjno – taktyczną;



Rys. 3.1.2 Wymagania stawiane wojskowemu systemowi łączności
Źródło: J. Michniak, A. Wisz, Bezpieczeństwo i ochrona informacji w wojskowych sieciach telekomunikacyjnych i zautomatyzowanych systemach dowodzenia, AON, Warszawa 2000.

- ***trwałość*** jako zdolność do zapewnienia dowodzenia wojskami i sterowania środkami rażenia w warunkach intensywnego oddziaływania ogniowego i radioelektronicznego przeciwnika;
- ***mobilność*** jako zdolność systemu do zmiany struktury oraz do rozwijania i przenoszenia elementów systemu, gwarantującą osiągnięcie gotowości całego systemu w nowych warunkach i w założonym czasie;
- ***przepustowość*** jako zdolność do transmisji określonych strumieni wiadomości w wyznaczonym czasie;
- ***bezpieczeństwo*** jako zdolność do poprawnego funkcjonowania w warunkach prowadzenia przez przeciwnika różnorodnych form walki radioelektronicznej.

Analizując wymienione wymagania stawiane wojskowemu systemowi łączności, można pozwolić sobie na stwierdzenie, że sumarycznie stanowią one jedną integralną całość w tym sensie, że występuje pomiędzy nimi określona korelacja. Przykładem potwierdzającym tę tezę może być choćby zależność między przepustowością a bezpieczeństwem. Jest bowiem ogólnie znanym faktem, że zastosowanie urządzeń ochrony kryptograficznej (bezpieczeństwo) ma bezpośrednie przełożenie na prędkość

transmisji (przepustowość). Zatem jednoczesna realizacja wszystkich cytowanych wymagań pozwala na spełnienie wymagań stawianych systemowi dowodzenia.

Dotychczasowe usystematyzowanie wiedzy w zakresie określenia wymagań stawianych zarówno łączności wojskowej jak i wojskowemu systemowi łączności pozwoliło na zidentyfikowanie miejsca i roli bezpieczeństwa w systemie dowodzenia poprzez techniczne środki łączności.

Wiedza ta jednocześnie stanowi podstawę dalszych rozważań, których oczekiwanym rezultatem będzie identyfikacja wymagań bezpieczeństwa informacji w systemie teletransmisyjnym dywizji zmechanizowanej w działaniach taktycznych.

3.2 WYMAGANIA BEZPIECZEŃSTWA STAWIANE SIECI TELETRANSMISYJNEJ DYWIZJI ZMECHANIZOWANEJ

Przed przystąpieniem do rozważań w zakresie określenia wymagań stawianych bezpiecznej sieci teletransmisyjnej dywizji zmechanizowanej w działaniach taktycznych należy zauważyć, że pojęcia występujące w temacie rozdziału, tzn. bezpieczeństwo, informacja oraz sieć teletransmisyjna są różnorako interpretowane. Dlatego też celowym jest przedstawienie na bazie dostępnych źródeł różnych definicji wymienionych pojęć, by wyodrębnić z nich te, które posłużą zdefiniowaniu podstawowego celu, którym jest określenie wymagań bezpieczeństwa informacji.

W literaturze poświęconej zagadnieniom ochrony systemów telekomunikacyjnych czy zapewnieniu bezpieczeństwa informacji w nich przetwarzanych i przesyłanych nie wydzielane jest z pojęcia wojskowego systemu telekomunikacyjnego pojęcie sieci teletransmisyjnej. Fakt ten jest bardzo łatwy do wytłumaczenia, gdyż sieć teletransmisyjna jest integralną częścią, elementem sieci telekomunikacyjnej, a z dotychczas zebranej i usystematyzowanej wiedzy wynika, że proces zapewnienia bezpieczeństwa systemowi musi być realizowany w sposób kompleksowy i obejmować wszystkie jego elementy funkcjonalne i organizacyjne. Podobnie rzecz ma się w odniesieniu do samego bezpieczeństwa systemu czy sieci, bowiem nie mają zasadniczego znaczenia miejsce i struktura organizacyjna systemu, w której powstał stan niepożądany polegający na ujawnieniu lub niekontrolowanym wypływie chronionej informacji. Zdarzenie to świadczy jedynie o tym, że zastosowane środki i metody ochrony nie spełniły sta-

wianych przed nimi wymagań i nie uwzględniały wszystkich czynników wpływających na zapewnienie wymaganego poziomu bezpieczeństwa.

Uogólniając tok powyższego rozumowania w trakcie dalszych rozważań będących tematem niniejszej dysertacji wymagania stawiane bezpieczeństwu wojskowego systemu łączności będą traktowane jako równoznaczne tym wymaganiom, które stawiane są sieci teletransmisyjnej dywizji zmechanizowanej.

W poprzednim rozdziale poświęconym identyfikacji struktury i organizacji sieci teletransmisyjnej dywizji zmechanizowanej zdefiniowano już pojęcie sieci teletransmisyjnej – stąd też zostanie ono celowo pominięte.

Pierwszym z wymienionych pojęć jest „bezpieczeństwo" (ang. Security[98]). Jest ono bardzo szerokim pojęciem, zawierającym w sobie wszystkie aspekty i pojęcia wchodzące w zakres ochrony informacji, do których zalicza się między innymi podatność, zagrożenia, ryzyko, aspekty zarządzania i zabezpieczenia. W Słowniku Języka Polskiego[99] jest definiowane jako „stan nie zagrożenia, spokoju, pewności". W ujęciu technicznym pojecie bezpieczeństwa określane jest jako stopień[100] pewności (wytrzymałości) konstrukcji na działania obciążające (niszczące) daną konstrukcję. Z jednej strony definicje te są bardzo proste i zwięzłe, ale jednocześnie ich zakres znaczeniowy jest bardzo szeroki. O wiele bardziej interesującą pod kątem naszych rozważań będzie definicja zawarta w Myśli Wojskowej[101] mówiąca, że bezpieczeństwo to jedna z podstawowych potrzeb człowieka i określa „stan, który daje poczucie pewności i gwarancję jego zachowania oraz szansę na doskonalenie. Sytuacja odznaczająca się brakiem ryzyka utraty czegoś, co człowiek szczególnie ceni, na przykład zdrowia, pracy, szacunku, uczuć, dóbr materialnych".

W odniesieniu do systemu telekomunikacyjnego bezpieczeństwo[102] pojmowane jest jako „stan osiągany, gdy określone informacje, materiały, personel czynności i obiekty zostają zabezpieczone przed szpiegostwem, sabotażem, dywersją i terroryzmem, a także przed utratą lub nieautoryzowanym dostępem".

---

[98] Dokument NATO serii AMSG 524 – „Słownik pojęć i definicji z zakresu bezpieczeństwa łączności i informatyki"
[99] „Słownik Języka Polskiego"- PWN, Warszawa 1978
[100] „Encyklopedia popularna PWN", Warszawa 1982
[101] „Myśl Wojskowa"- Bellona, Warszawa Listopad-Grudzień 2002, 6 (623)
[102] Systemy telekomunikacyjne i informatyczne – terminologia, Norma Obronna, NO-01-A003

Inaczej problem postrzegany jest i definiowany w odniesieniu do bezpieczeństwa łączności[103], gdzie traktowany jest on jako zdolność systemu do ochrony przesyłanych informacji oraz stacji (aparatowni), urządzeń i dokumentów kluczowych przed rozpoznaniem. Definicja powyższa w cytowanej już wcześniej „Normie Obronnej NO-01-A003 poszerzona jest o środki bezpieczeństwa mające na celu zapobieżenie nieautoryzowanemu dostępowi lub w celu zapewnienia ich autentyczności.

W dokumentach normatywnych[104] Paktu Północnoatlantyckiego pojęcie bezpieczeństwa łączności (ang. Communication Security – COMSEC[105]) traktowane jest jako zespół zabezpieczeń wynikających z używania środków ochrony kryptograficznej, środków zabezpieczenia transmisji i emisji na okres połączenia (sesji), a także z zastosowań fizycznych środków zabezpieczenia informacji. Podejmuje się je w celu ochrony przed dostępem osób nieautoryzowanych do informacji lub w celu zapewnienia autentyczności takiego połączenia

Poddając analizie cytowane definicje bezpieczeństwa łączności oraz opierając się na literaturze przedmiotu[106] można przyjąć, że bezpieczeństwo łączności osiąga się poprzez realizację następujących czynności:

- spełnienie wymagań technicznych w projektowaniu, rozmieszczanie i montaż urządzeń ochrony informacji, linii telekomunikacyjnych i abonenckich, urządzeń końcowych oraz wyposażenia pomocniczego;
- ścisłe przestrzeganie przepisów techniczno-eksploatacyjnych, zasad obsługiwania i wykorzystania urządzeń ochrony kryptograficznej;
- właściwe zgodne z obowiązującymi postępowanie z materiałami kryptograficznymi;
- zapewnienie odpowiedniej obsady stanowisk w organach bezpieczeństwa łączności i informatyki, specjalistyczne przygotowanie obsług oraz ich stabilizację na zajmowanych stanowiskach;

---

[103] Tymczasowe zasady organizacji, funkcjonowania i bezpieczeństwa łączności utajnionej w SZ RP – Szefostwo Wojsk Łączności sygn. Łączn. 988/88 s. 49

[104] Dyrektywa Bezpieczeństwa AD 70-1 PL, część V, § 13

[105] Dokument NATO serii AMSG 524 – „Słownik pojęć i definicji z zakresu bezpieczeństwa łączności i informatyki"

[106] m.in. Projektowanie, budowa oraz rozwijanie stacji łączności utajnionej stacjonarnych i polowych węzłów łączności – Szefostwo Wojsk Łączności sygn. Łączn. 624/76, s 26-27, Przepisy bezpieczeństwa łączności i eksploatacji oraz ochrony informacji w podsystemie cyfrowej łączności utajnionej SZ RP, s. 3-4.

- ograniczenie do niezbędnego minimum ilości osób zapoznawanych z zagadnieniami bezpieczeństwa łączności i informatyki a w tym ochrony kryptograficznej;
- systematyczne prowadzenie działalności kontrolnej w zakresie przestrzegania zasad ochrony tajemnicy;
- inne przedsięwzięcia organizacyjno-techniczne określone przepisami szczegółowymi oraz innymi obowiązującymi specjalistycznymi dokumentami normatywno-prawnymi.

Zestawienie i analiza wszystkich wymienionych powyżej czynności pozwalają zdefiniować bezpieczeństwo łączności jako ***całokształt działalności zmierzającej do uniemożliwienia przypadkowego lub celowego ujawnienia chronionej informacji, która jest przesyłana za pomocą technicznych środków łączności, poprzez zastosowanie w sposób kompleksowy technicznych, personalnych, fizycznych i organizacyjno-proceduralnych środków ochrony***.

Zobrazowaniem tego podejścia do pojęcia bezpieczeństwa łączności jest przedstawiona na rysunku 3.2.1 ogólna klasyfikacja lub podział obszarów, w których stosowanie adekwatnych środków ochrony zapewnia wymagany poziom bezpieczeństwa systemu lub sieci telekomunikacyjnej.

Stosowane środki ochrony w wojskowym systemie telekomunikacyjnym podzielone zostały na następujące grupy:

1. Bezpieczeństwo fizyczne;
2. Bezpieczeństwo personalne;
3. Bezpieczeństwo organizacyjno-proceduralne;
4. Bezpieczeństwo techniczne tj.:
   a) ochrona kryptograficzna,
   b) ochrona elektromagnetyczna,
   c) techniczne wsparcie ochrony fizycznej,
   d) ochrona programowa.



Rys. 3.2.1 Ogólny podział środków bezpieczeństwa w systemie telekomunikacyjnym

Źródło: J. Janczak, G. Świdzikowski, Bezpieczeństwo informacji w wojskowym systemie telekomunikacyjnym, AON, Warszawa 2004

Reasumując, zapewnienie bezpieczeństwa systemu telekomunikacyjnego ma na celu ochronę treści przekazywanych wiadomości przez techniczne środki łączności, przed rozpoznaniem radioelektronicznym, dywersją radiową oraz zabezpieczenie przed „niekontrolowaną" ucieczką informacji z systemu[107].

Mając zatem na uwadze stwierdzenie cytowane powyżej wszelkie przedsięwzięcia oraz obszary, w których stosowane są środki ochrony mające na celu zapewnienie bezpieczeństwa wojskowemu systemowi telekomunikacyjnemu sprowadzają się do zapewnienia ochrony:

a) informacji wprowadzanej, przesyłanej i wyprowadzanej z systemu;
b) technicznym środkom łączności zapewniającym przekazywanie informacji na odległość oraz infrastrukturze telekomunikacyjnej, w której ww. urządzenia są zainstalowane.

Wypływa z tego wniosek, że „informacja", a szczególnie ta podlegająca ochro-

[107] J. Michniak, A. Wisz, Bezpieczeństwo i ochrona informacji..., op. cit., s. 8

nie z mocy prawa w wojskowym systemie telekomunikacyjnym, jest tym zasadniczym elementem, który stanowi podstawę i cel organizacji całego szeregu przedsięwzięć zapewniających jej ochronę.

Czym w takim razie jest i jak należy rozumieć pojęcie informacji. Słownik Języka Polskiego[108] podaje, że informacja to: ***„powiadomienie o czymś, zakomunikowanie czegoś; wiadomość, wskazówka, pouczenie", ale także „każdy czynnik, dzięki któremu ludzie lub urządzenia automatyczne mogą bardziej sprawnie, celowo działać".***

Drugie ze znaczeń doprecyzowuje sens pierwszego, wskazuje na to, że poprzez bycie pewnego rodzaju wiadomością informacja nabiera stosownej dla niej wagi, pokazuje celowość jej przekazywania, przechowywania i przetwarzania jako czynnika usprawniającego pewne procesy. Innymi słowy treść informacji nabiera znaczenia dla konkretnego „użytkownika" do którego jest skierowana, na przykład procedury wykorzystywane przez aplikację zapisane w postaci pliku tekstowego mogą być zupełnie niezrozumiałe dla kogoś kto nie miał do czynienia z programowaniem, a dla osoby zorientowanej mogą one stanowić źródło wiedzy o idei działania tegoż programu.

W normie obronnej „Systemy telekomunikacyjne i informatyczne – terminologia" informacja traktowana jest jako *wiadomość lub elementy wiedzy, które mogą być przedstawione w postaci nadającej się do przekazania, zapisu lub przetwarzania*[109]. Informacja taka może być prezentowana przy użyciu np.: znaków, symboli, obrazków lub dźwięków[110].

Bardziej czytelną i praktyczną definicję przedstawia D. Mąka, według którego *informację stanowi każdy czynnik, dzięki któremu odbierający go obiekt (np. człowiek, organizm żywy, organizacja, urządzenie automatyczne, itp.) może polepszać swoją znajomość otoczenia i bardziej sprawnie przeprowadzać celowe działania*[111].

Przedstawiona różnorodność form, zastosowań i interpretacji pojęcia informacji pozwala zatem na jej zdefiniowanie dla konkretnych potrzeb stanowiących przedmiot

---

[108] „Słownik Języka Polskiego", op. cit., s. 124
[109] Polska norma - PN-93/E-50701
[110] norma europejska - IEC 701-01-01
[111] D. Mąka, „Ryzyko w systemie bezpieczeństwa informacyjnego państwa w aspekcie standardów NATO i Unii Europejskiej" – rozprawa doktorska, AON, Warszawa 2004, s. 73

zainteresowania niniejszej dysertacji. A zatem do dalszych rozważań przyjęta zostanie definicja informacji o następującym brzmieniu:

Informacja w wojskowym systemie telekomunikacyjnym są to wszelkie dane wypracowane w procesie dowodzenia dotyczące stanu i działania wojsk własnych i przeciwnika oraz mające wpływ na organizację i kierowanie wojskami w okresie pokoju, kryzysu czy wojny, które przekazywane są za pośrednictwem technicznych środków łączności.

Zadania realizowane przez siły zbrojne RP, dowództwa rodzajów wojsk (wydzielone z nich komponenty), czy w końcu związki taktyczne, oddziały i pododdziały z reguły nie mają charakteru jawnego, gdyż stanowią element polityki bezpieczeństwa państwa w dziedzinie obronności.

Stąd też w wymiarze militarnym pojęciu „informacji" nieodłącznie towarzyszy pojęcie „bezpieczeństwa"[112], które w rozważanym kontekście przyjmuje brzmienie – bezpieczeństwa informacji w sieci teletransmisyjnej.

Ochrona czyli zapewnienie bezpieczeństwa informacji w wojskowym systemie lub sieci telekomunikacyjnej nie jest przypisana lub zapewniana każdej informacji. Zgodnie z obowiązującymi dokumentami normatywnymi[113] obowiązek zapewnienia bezpieczeństwa odnosi się tylko do informacji klasyfikowanej, a przez klasyfikowanie[114] należy rozumieć czynność mającą na celu określenie stopnia ich tajności oraz zidentyfikowanie każdej informacji wymagającej ochrony poprzez oznaczenie jej stosowną klauzulą tajności (tajemnica państwowa lub służbowa). Klauzula przypisana danej informacji powinna zapewniać ciągłość jej niejawności od momentu jej wytworzenia do chwili jej celowego, kontrolowanego ujawnienia lub zniszczenia.

Warto w tym miejscu zastanowić się jak pojmowane jest ogólnie pojęcie bezpieczeństwa informacji i jak jest ono definiowane czy pojmowane w różnych wymiarach.

W wymiarze gospodarczym[115] bezpieczeństwo informacji to osiągnięcie uzasadnionych biznesowo poziomów poufności, integralności, dostępności, autentyczno-

---

[112] R. Wróblewski, „Podstawowe pojęcia z dziedziny polityki bezpieczeństwa, strategii i sztuki wojennej", AON, Warszawa 1999, s. 53

[113] m.in. Ustawa o ochronie informacji niejawnych – Dz. U. 1999 Nr 11, poz. 95

[114] Dyrektywa bezpieczeństwa.....op. cit. cz. II § 5

[115] A. Gałach, K. Szczypiorski, Bezpieczeństwo systemów teleinformatycznych, CITCOM PW, 2002, s. 47 -56

ści i rozliczalności informacji tworzonej, przechowywanej, przetwarzanej i przesyłanej. Bezpieczeństwo informacji nie powstaje na zewnątrz przedsiębiorstwa, musi ono wynikać z rzeczywistych potrzeb biznesowych i odpowiadać ryzyku związanemu z działalnością biznesową. Stworzenie, wdrożenie a następnie utrzymanie bezpieczeństwa informacji i systemów informacyjnych wspierających działalność przedsiębiorstwa jest zagadnieniem bardzo złożonym.

W kolejnej definicji bezpieczeństwa informacji[116] zasadniczy nacisk skierowano na ocenę miary stopnia skuteczności zastosowanych środków i metod ochrony w stosunku do istniejących i prognozowanych zagrożeń bezpieczeństwa informacji. Polegają one na zabezpieczeniu informacji przed przypadkowym bądź umyślnym zniszczeniem, kradzieżą, nielegalnym ujawnieniem lub nie sankcjonowaną modyfikacją. Przez środki ochrony rozumie się przedsięwzięcia technologiczne i administracyjne, do zabezpieczenia środków łączności i informatyki, oprogramowania strukturalnego i danych, w celu zapewnienia ochrony interesów instytucji i poufności. Do środków ochrony informacji zaliczane są również rozwiązania prawne, organizacyjno-administracyjne, mechanizmy programowe, urządzenia techniczne, ochrona fizyczna oraz kryptografia.

Zagrożenia bezpieczeństwa informacji to zdarzenia przypadkowe (losowe) lub działania celowe, które mogą spowodować przesłanki do legalnego lub nielegalnego ujawnienia informacji, jej modyfikację, zniszczenie lub kradzież.

Ochrona to wszelkie działania mające chronić przed zagrożeniami, działaniami szkodliwymi lub niebezpiecznymi, natomiast zabezpieczenia to środki i metody zabezpieczające.

Postać definicji zawartej w polskiej normie PN-ISO/IEC-17799/2003 jest bardzo krótka i zwięzła – odnosi się bowiem do zachowania poufności, integralności oraz dostępności informacji[117] w dowolnym typie, rodzaju systemu informacyjnego.

W odniesieniu do systemów teleinformatycznych bezpieczeństwo informacji[118] określane jest jako definiowanie, osiąganie i utrzymywanie sześciu podstawowych cech, do których zalicza się:

---

[116] Kryteria oceny bezpieczeństwa systemów łączności i informatyki, Praca zbiorowa, SWŁiI SG WP, Warszawa 1996 r., s. 15-19

[117] PN-ISO/IEC-17799/2003

- ***poufność*** – dostęp do informacji musi być ograniczony jedynie do kręgu uprawnionych użytkowników;
- ***integralność*** – informacja musi być zachowana w swojej oryginalnej postaci, z wyjątkiem przypadków, gdy jest ona legalnie aktualizowana lub usuwana przez uprawnione osoby;
- ***dostępność*** – informacja musi być dostępna dla uprawnionych użytkowników zawsze, kiedy mają taką potrzebę;
- ***rozliczalność*** – dostęp użytkownika do informacji może być przypisany w sposób jednoznaczny tylko temu użytkownikowi;
- ***autentyczność*** – tożsamość (pochodzenie) informacji lub podmiotu z nią związanego (np. osoba wysyłająca daną wiadomość) musi być zgodna z zadeklarowaną (osobą);
- ***niezawodność*** – zachowanie i skutki działania np. urządzeń zawierających informacje, które podlegają ochronie, które należy zapewnić i utrzymać jako podstawowe atrybuty bezpieczeństwa informacji.

Kolejna, chyba najbardziej zbliżona do rozważanego w ramach dysertacji obszaru zainteresowania definicja przyjmuje, że bezpieczeństwo informacji[119] to całokształt działalności zmierzającej do uniemożliwienia przypadkowego lub celowego ujawnienia informacji niejawnych (niezależnie od formy i sposobu ich wyrażenia), przechowywanych, przetwarzanych przy pomocy systemów informatycznych, systemów automatyzacji dowodzenia oraz przesyłanych za pomocą technicznych środków łączności, poprzez zastosowanie w sposób kompleksowy organizacyjnych, fizycznych, technicznych oraz personalnych metod ochrony.

Bezpieczeństwo informacji jest stanem pożądanym, którego osiągnięcie jest procesem złożonym. Zapewnienie pożądanego stanu osiągane jest poprzez wdrożenie całego szeregu środków i metod zabezpieczeń. Dotychczasowa praktyka i doświadczenia wykazują, że osiągnięcie tego stanu nie jest możliwe przy zastosowaniu tylko wybranych środków, czy metod zapewniających bezpieczeństwo. Zasadnym zatem wydaje

---

[118] J. Michniak i inni, Bezpieczeństwo i ochrona informacji w sieciach łączności i informatyki wojskowej w okresie pokoju, kryzysu i wojny – praca naukowo-badawcza pk. „OCHRONA", AON, Warszawa 2004, s. 41

[119] A. Dańczak, Bezpieczeństwo informacji w SZ RP. Aspekty strategiczne. Praca studyjna, Warszawa, AON 2002, s. 12

się stwierdzenie, że stosowanie zabezpieczeń musi mieć charakter kompleksowy, gdyż w przeciwnym przypadku może nastąpić utrata informacji niejawnej polegająca na tym, że treść informacji w całości lub części stanie się znana osobom nieupoważnionym, czyli nie sprawdzonym przez właściwe władze bezpieczeństwa i nie mającym zezwolenia na dostęp do takich informacji, lub gdy informacje niejawne zostały narażone na takie ryzyko[120].

Bezpieczeństwo każdego systemu informacyjnego, a w tym sieci teletransmisyjnej, nie jest kategorią absolutną. Z tej przyczyny celem organizacji bezpieczeństwa informacji jest stworzenie jednolitego, gwarantowanego systemu ochrony i nadzoru, a przez to zapewnienie tajności, skrytości przetwarzania i transmisji informacji niejawnej w sieciach telekomunikacyjnych SZ RP oraz zachowania jej integralności (zabezpieczenie przed dezinformacją), a także przywrócenie jej właściwej roli po awariach i dekonspiracji[121].

Z punktu widzenia prof. J. Michniaka i A. Wisza[122] przedmiotem wymagań stawianych bezpieczeństwu informacji jest podsystem bezpieczeństwa łączności i ochrony informacji (PBŁiOI) w zintegrowanej sieci telekomunikacyjnej i zautomatyzowanym systemie dowodzenia i obejmuje on założenia na zabezpieczenie w zakresie:

- redukcji emisji elektromagnetycznej,
- ochrony kryptograficznej,
- ochrony programowej,
- ochrony fizycznej.

Podsystem Bezpieczeństwa Łączności i Ochrony Informacji według powyżej cytowanych autorów, ma za zadanie zabezpieczenie wszelkich danych, przed przypadkowym bądź umyślnym zniszczeniem, kradzieżą, nielegalnym ujawnieniem lub niesankcjonowaną modyfikacją za pomocą dostępnych środków i metod, poprzez stosowanie przedsięwzięć technicznych i administracyjnych do zabezpieczenia komputerów, programów i informacji, w celu zapewnienia właściwego poziomu poufności

---

[120] D. Mąka, Elementy zagrożeń i zarządzania ryzykiem w świetle polityki bezpieczeństwa informacyjnego, IT Security Magazine nr 8-9, 2001

[121] Przepisy bezpieczeństwa łączności i eksploatacji oraz ochrony informacji w podsystemie cyfrowej łączności utajnionej SZ RP, SWŁiI, Warszawa 1996, s. 3

[122] J. Michniak, A. Wisz, Bezpieczeństwo i ochrona informacji w wojskowych sieciach...., op. cit., s. 12

w stosunku do istniejących i prognozowanych zagrożeń stanowisk pracy bojowej (SPB) w warunkach bliskiej styczności ze środkami WRE potencjalnego przeciwnika.

Wynikiem przeprowadzonej analizy cytowanych dotychczas definicji, wymagań oraz standardów towarzyszących pojęciu bezpieczeństwa jest przyjęcie następującej definicji bezpieczeństwa informacji w sieci teletransmisyjnej dywizji:

„Bezpieczeństwo informacji w sieci teletransmisyjnej dywizji zmechanizowanej w działaniach taktycznych to zespół działań i przedsięwzięć mających na celu zapewnienie spełnienia wszystkich atrybutów bezpieczeństwa informacji, które osiągane jest przez zastosowanie w sposób kompleksowy metod i środków ochrony w następujących obszarach:

- ***organizacyjnym,***
- ***fizycznym,***
- ***technicznym,***
- ***personalnym.***

Po przyjęciu za punkt wyjścia cytowanej powyżej definicji celowe jest rozważenie na tym etapie badań nad samej istoty bezpieczeństwa informacji oraz następstw jej celowego bądź przypadkowe jej ujawnienia.

W tym aspekcie zasadniczym problemem jest zdefiniowanie, jakie informacje powinny podlegać ochronie oraz jakie czynniki mogą wpływać na zagrożenie jej bezpieczeństwa w sieci teletransmisyjnej.

W pierwszej z wymienionych płaszczyzn w wojskowych systemach telekomunikacyjnych ochronie powinny podlegać te informacje, które w rozumieniu ustawy z dnia 22.01.1999 r. „ O ochronie informacji niejawnych" stanowią tajemnicę państwową lub służbową, gdzie informacją niejawną stanowiącą **tajemnicę państwową** jest informacja, której nieuprawnione ujawnienie może spowodować istotne zagrożenie dla interesów Rzeczypospolitej Polskiej, a w szczególności dla niepodległości lub nienaruszalności terytorium, interesów obronności, bezpieczeństwa państwa i obywateli, albo narazić te interesy na co najmniej znaczną szkodę. Wyżej wymieniona ustawa precyzuje, że **tajemnica służbowa** to informacja niejawna nie będąca tajemnicą państwową, uzyskana w związku z czynnościami służbowymi albo wykonywaniem prac zleconych, której nieuprawnione ujawnienie mogłoby narazić na szkodę interes

państwa, interes publiczny lub prawnie chroniony interes obywateli albo jednostki organizacyjnej.

Analizując drugą z wymienionych płaszczyzn można pokusić się o stwierdzenie, że następstwo bagatelizowania zagrożeń dla bezpieczeństwa informacji w systemie telekomunikacyjnym może doprowadzić do:

1. utraty poufności informacji, które należy rozumieć jako nieautoryzowane ujawnienie informacji przez nieuprawniony dostęp do systemu;
2. utraty integralności informacji, które należy rozumieć jako nieautoryzowaną modyfikację informacji oraz utratę prawidłowego i spójnego działania systemu;
3. utraty dostępności, które należy rozumieć jako odmowę autoryzowanego dostępu lub opóźnienie operacji krytycznych pod względem czasu i celu;
4. utraty autentyczności rozumianej jako weryfikację tożsamości podmiotów lub prawdziwość aktywów systemu telekomunikacyjnego,
5. utraty rozliczalności oznaczającej określenie i weryfikowanie odpowiedzialności za działania, usługi i funkcje realizowane za pośrednictwem systemu;
6. utraty niezawodności rozumianej jako gwarancje odpowiedniego zachowania się systemu telekomunikacyjnego i otrzymanych wyników.

Wymienione i bardzo pobieżnie scharakteryzowane czynniki, będące następstwem utraty bezpieczeństwa przez system telekomunikacyjny, a tym samym znajdującej się w nim informacji, można traktować na równi z wymaganiami stawianymi nowoczesnej sieci teletransmisyjnej w zakresie ochrony przesyłanej w niej informacji. Z ustawowego punktu widzenia bez znaczenia jest fakt, które z przedstawionych wymagań zawiodło i stało się przyczyną ujawnienia informacji osobom nieupoważnionym do zapoznawania się z treściami podlegającymi ochronie. Z tej perspektywy również pozostają bez znaczenia warunki i otoczenie funkcjonowania sieci, które nie zapewniając spełnienia choćby jednego z tak określonych wymagań w okresie pokoju może zawieść i raczej na pewno zawiedzie w okresie kryzysu, czy też wojny w aspekcie ochrony oraz bezpieczeństwa informacji.

Teza powyższa wynika z analizy obowiązujących dokumentów normatywnych, w których nie sprecyzowano ani w sposób ogólny, ani szczegółowo okresu „ważności" informacji opatrzonych klauzulą tajności wymienianych lub przesyłanych za pomocą

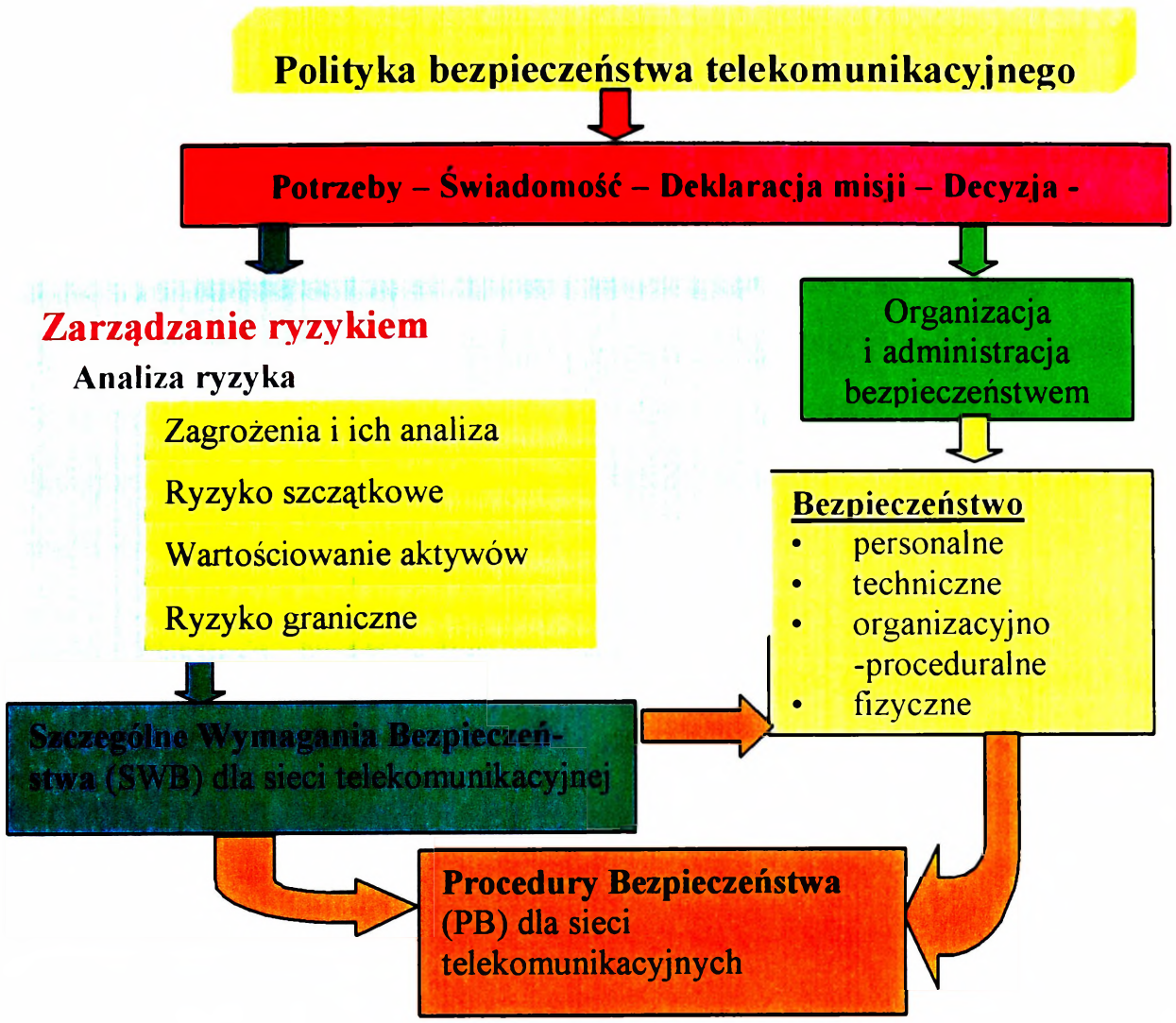
środków technicznych, a w tym w wojskowych systemach telekomunikacyjnych. Stąd też możemy wnioskować, że okres ten jest równoznaczny z czasem i zasadami obowiązującymi w zakresie archiwizacji niejawnych dokumentów w formie papierowej lub nośników elektronicznych.

Opierając się na przyjętych lub cytowanych dotychczas stwierdzeniach można sformułować następującą tezę:

W procesie planowania oraz budowania wojskowej sieci telekomunikacyjnej (sieci teletransmisyjnej) obligatoryjnie powinno uwzględniać się wszelkie możliwe scenariusze oraz warunki w jakich system może być eksploatowany zarówno w aspekcie realizowanych zadań, jak również w aspekcie wymagań bezpieczeństwa (jeżeli takowe są stawiane) informacji w nim przesyłanej.

Tak postawiona teza i wypływające z niej wnioski pozwalają na dokonanie uogólnienia, które można zawrzeć w następującym zdaniu – proces organizacji ochrony systemu telekomunikacyjnego i zapewnienie bezpieczeństwa informacji w nim przesyłanej zgodnie z przyjętą polityką bezpieczeństwa resortu Obrony Narodowej musi być realizowany równolegle na wszystkich etapach planowania, a następnie wdrażania systemu, nie wyłączając z tego procesu eksploatacji.

Jeśli zatem planowany wojskowy system telekomunikacyjny w swoim zamyśle ma zapewnić przesyłanie informacji klasyfikowanych (niejawnych) to wówczas organizator systemu winien przeprowadzić analizę ryzyka w odniesieniu do infrastruktury telekomunikacyjnej oraz wszystkich elementów i urządzeń systemu telekomunikacyjnego, w których może zaistnieć prawdopodobieństwo niekontrolowanego lub nieautoryzowanego „ulotu" informacji podlegającej ochronie. Jest to nic innego jak analiza zagrożeń dla bezpieczeństwa informacji wytwarzanych, przetwarzanych, przesyłanych i przechowywanych w wojskowym systemie telekomunikacyjnym (sieci teletransmisyjnej), która winna uwzględniać wszelkie możliwe warunki eksploatacji tego systemu począwszy od okresu pokoju aż do warunków ekstremalnych – wojny i prowadzenia działań bojowych.



Rys. 3.2.2 Rola i miejsce „Szczególnych wymagań bezpieczeństwa" w strukturze polityki bezpieczeństwa telekomunikacyjnego

Źródło: D. Mąka, wykład nt. „Bezpieczeństwo informacyjne", studia podyplomowe, AON

Biorąc za podstawę przyjętą definicję bezpieczeństwa informacji oraz dokonując analizy narodowych i sojuszniczych dokumentów normatywnych[123] w dziedzinie bezpieczeństwa można stwierdzić, że podstawowym wymaganiem dla każdego systemu lub sieci służącej do przechowywania, przetwarzania i przesyłania informacji klasyfikowanej (oznaczonej narodową lub sojuszniczą klauzulą tajności) jest opracowanie przez zespół pracowników odpowiedzialnych za przygotowanie i wdrożenie danego systemu (sieci) deklaracji nazywanej „Szczególne Wymagania Bezpieczeństwa" (*ang. Specyfic Security Reguirement Statement*[124]), którą następnie zatwierdza właściwa instytucja bezpieczeństwa ds. akredytacji[125]. Deklarację

[123] m.in. Ustawa o ochronie informacji niejawnych (Dz.U. 1999, Nr 11, poz. 95), „Security within NATO", Allied Command in Europe directive, SHAPE 1997

[124] Dokument NATO serii AMSG 524 – „Słownik pojęć i definicji z zakresu bezpieczeństwa łączności i informatyki"

[125] Dyrektywa bezpieczeństwa..., op. cit. cz. V § 6

powyższą należy sformułować we wstępnej fazie projektowania systemu, a następnie uzupełniać i poszerzać w miarę rozwoju prac nad projektem, w czasie jego wdrażania i po uruchomieniu systemu telekomunikacyjnego, czy sieci teletransmisyjnej w rozważanym przypadku. Omawiane „Szczególne wymagania bezpieczeństwa" stanowią pełną i jednoznaczną wykładnię obowiązujących zasad, które muszą być przestrzegane, oraz precyzyjnie opisanych wymagań szczegółowych bezpieczeństwa, którym system (sieć) musi sprostać. Podstawa ich opracowania opiera się na polityce bezpieczeństwa telekomunikacyjnego (rys. 3.2.2) – w tym ocenie stopnia ryzyka i możliwych zagrożeń.

Opracowany pełny dokument winien określać parametry bezpiecznego środowiska pracy systemu i sieci telekomunikacyjnej (teletransmisyjnej), jak najniższy (najbardziej powszechny) poziom dopuszczenia do tajemnicy, najwyższy stopień utajnienia informacji, poziom bezpieczeństwa pracy, wymagania użytkownika. Stanowi on jednocześnie integralną częścią dokumentacji systemu (sieci), przedstawianej właściwym władzom w celu zatwierdzenia proponowanych rozwiązań. W swej formie ostatecznej „Szczególne Wymagania Bezpieczeństwa" muszą zawierać stwierdzenie, że wdrożony system (sieć) jest w pełni bezpieczny, co jest poparte szczegółowym opisem środków zapewniających wymagany poziom ochrony przechowywanych informacji niejawnych.

Z analizy wymagań stawianych przez dokumenty normatywne oraz ujętych w „Szczególnych wymaganiach bezpieczeństwa" treści wynika, że ich istotą jest szczegółowy opis zastosowanych w danym systemie bądź sieci środków i metod zapewniających wymagany poziom bezpieczeństwa informacji.

Jednak zaproponowanie a następnie zastosowanie rzeczonych środków i metod zapewniających stosowny poziom bezpieczeństwa informacji musi posiadać logiczne i fizyczne uzasadnienie, które praktycznie realizowane poprzez analizę ryzyka oraz identyfikację zagrożeń dla planowanego systemu lub sieci telekomunikacyjnej.

Stąd też w kolejnym kroku rozważań prowadzonych w ramach dysertacji na temat bezpieczeństwa informacji w sieci teletransmisyjnej dywizji zmechanizowanej niezbędne jest zdefiniowanie pojęcia zagrożenia oraz identyfikacja typu i rodzaju za-

grożeń, które mogą wpływać na poziom bezpieczeństwa informacji w rozpatrywanej sieci teletransmisyjnej.

4. ZAGROŻENIA WPŁYWAJĄCE NA BEZPIECZEŃSTWO INFORMACJI W SIECI TELETRANSMISYJNEJ DYWIZJI ZMECHANIZOWANEJ

W toku dotychczasowych rozważań ustalono, że warunkiem uznania informacji za bezpieczną w sieci teletransmisyjnej jest spełnienie przez nią następujących kryteriów:

- poufności,
- integralności,
- dostępności,
- rozliczalności,
- autentyczności,
- niezawodności.

Ponadto jak wynika z narodowych i sojuszniczych dokumentów normatywnych podstawowym wymaganiem uznania danego konkretnego systemu lub sieci za bezpieczny jest opracowanie i wdrożenie „Szczególnych wymagań bezpieczeństwa".

Jednak opublikowanie w formie zwartej, w postaci dokumentu, jakim są „Szczególne wymagania bezpieczeństwa" np. sieci teletransmisyjnej dywizji zmechanizowanej jest następstwem procesu analitycznego wchodzącego w skład zarządzania ryzykiem, które z kolei stanowi integralna część polityki bezpieczeństwa teleinformacyjnego[126].

Podstawowym elementem tego procesu jest analiza ryzyka, w skład której wchodzi określenie oraz analiza wszelkich możliwych zagrożeń oraz ich analiza i na tej podstawie oszacowanie tzw. ryzyka granicznego. Przy czym pojęcie ryzyka granicznego należy traktować jako incydenty lub zdarzenia, do których może dojść w sieci lub systemie a ich wystąpienie nie ma zasadniczego wpływu na zachowanie określonego (wymaganego) poziomu bezpieczeństwa.

---

[126] Polityka bezpieczeństwa jest to szeroko rozumiany plan lub sposób działania, przyjęty w celu osiągnięcia wysokiego poziomu bezpieczeństwa systemu oraz ochrony danych, realizowany jako skutek podjętych decyzji administracyjnych – J. Stokłosa, Bezpieczeństwo danych w systemach informatycznych, Wydawnictwo Naukowe PWN, Warszawa – Poznań 2001, s. 16

Zasadne jest zatem w kolejnym etapie rozważań prowadzonych w ramach niniejszej dysertacji podjęcie próby zdefiniowania samego pojęcia „zagrożenia". Opierając się na obszarach i płaszczyznach, w których zagrożenia występują dokonany zostanie ich podział. Pozwoli to na ich scharakteryzowanie i określenie poziomu istotności (gradacji) w kontekście wpływu na bezpieczeństwo informacji w sieci teletransmisyjnej. Zamierzonym efektem końcowym stanowiącym podsumowanie rozdziału będzie określenie tych zagrożeń, które w sposób bezpośredni oddziaływają na poziom bezpieczeństwa informacji w rozpatrywanej sieci teletransmisyjnej dywizji zmechanizowanej.

4.1. PODZIAŁ I CHARAKTERYSTYKA ZAGROŻEŃ BEZPIECZEŃSTWA INFORMACJI W SIECI TELETRANSMISYJNEJ DYWIZJI ZMECHANIZOWANEJ

Podejmując próbę dokonania podziału oraz charakterystyki zagrożeń bezpieczeństwa informacji w sieci teletransmisyjnej należy scharakteryzować, a następnie zdefiniować, co rozumiemy pod pojęciem zagrożenia bezpieczeństwa informacji.

W myśl dokumentów sojuszniczych[127] ogólne pojecie zagrożenia bezpieczeństwa *(ang. breach of security*[128]*)* przyjmowane jest jako każde postępowanie sprzeczne z ogólnymi lub miejscowymi przepisami bezpieczeństwa bądź pomijanie tych przepisów, w wyniku czego rośnie ryzyko nieuprawnionego ujawnienia informacji niejawnych NATO i może dojść do ich utraty.

W ujęciu amerykańskim[129] zagrożeniem jest każdy „dokuczliwy" atak, który potencjalnie może wpłynąć na powstanie ryzyka utraty bezpieczeństwa narodowego.

Przedstawione definicje traktują omawiany problem w sposób ogólny, ale pozwalają na wyrobienie poglądu czym jest i jak rozumiane jest pojęcie zagrożenia bezpieczeństwa zarówno narodowego (USA) jak i sojuszniczego (NATO).

---

[127] CM-55(final), Polityka bezpieczeństwa NATO, cz.IX, § 4

[128] Dokument NATO serii AMSG 524 – „Słownik pojęć i definicji z zakresu bezpieczeństwa łączności i informatyki"

[129] R.H Anderson, Securing the U.S. Defense Information Infrastructure: A Proposed Approach, National Defense Research Institute, RAND 1999, s. 5

Zagadnienia związane z zagrożeniami bezpieczeństwa informacji w sieciach informatycznych, telekomunikacyjnych czy teletransmisyjnych w tym kontekście są pojęciem bardziej szczegółowym.

Ogólnie rzecz ujmując, z zagrożeniem systemów lub sieci mamy do czynienia wówczas, gdy istnieje możliwość narażenia na szwank ich bezpieczeństwa na skutek utraty poufności, utraty integralności bądź utraty dostępu do systemu lub sieci. Słabe punkty można określić jako brak kontroli lub niewystarczającą kontrolę, w wyniku czego zwiększa się ryzyko zagrożenia bezpieczeństwa zasobów informacyjnych systemu bądź sieci. Słaby punkt to np. pomijanie lub upraszczanie procedur kontroli. Słaby punkt może mieć charakter techniczny, proceduralny czy operacyjny.

Informacje niejawne NATO przechowywane w systemach i sieciach telekomunikacyjnych w sposób zintegrowany i w postaci gotowej do szybkiego przetworzenia, przekazania i użytku mogą stanowić słaby punkt ze względu na ryzyko ich nieuprawnionego ujawnienia bądź wykorzystania przez osoby nieupoważnione lub nie posiadające prawa dostępu. Ponadto gromadzone w ten sposób informacje są narażone na kradzież, zniekształcenie treści i zniszczenie. Co więcej, sprzęt łączności i informatyki, podatny na uszkodzenia i niekiedy bardzo skomplikowany technologicznie, jest kosztowny i często trudno go szybko naprawić czy wymienić. Dlatego takie systemy i sieci łączności i informatyki stanowią atrakcyjny cel działań potencjalnego przeciwnika[130].

W innym definicyjnym podejściu[131] szczególny nacisk położony jest na czynnik ludzki stwierdza się, że zagrożenia dla systemu telekomunikacyjnego lub teleinformatycznego mogą wynikać ze strony każdej osoby, która usiłuje uzyskać dostęp do informacji i posiada do tego wystarczającą wiedzę i doświadczenie.

Jednak najlepiej istotę problemu ujmuje definicja, która traktuje zagrożenia bezpieczeństwa informacji w sieciach telekomunikacyjnych jako zdarzenia przypadkowe (losowe) lub działania celowe mogące spowodować przesłanki do legalnego lub

---

[130] Dyrektywa bezpieczeństwa AD-70/PL, cz.5, § 1

[131] Metodyka opracowania Szczególnych Wymagań Bezpieczeństwa systemu lub sieci teleinformatycznej, Wojskowe Biuro Bezpieczeństwa Łączności i Informatyki, Warszawa 2000, s. 17

nielegalnego ujawnienia informacji, jej modyfikacji, zniszczenia czy ewentualnej kradzieży[132].

W literaturze przedmiotu[133] możemy spotkać się z różnymi płaszczyznami klasyfikacji zagrożeń, począwszy od najbardziej ogólnych, jak podział na wewnętrzne i zewnętrzne, aż po bardzo szczegółowe, które odnoszą się do konkretnego systemu uwzględniającego jego organizację, możliwości konfiguracyjne, wykorzystywanych środków telekomunikacyjnych (transmisyjnych, komutacyjnych) czy samych urządzeń końcowych. Brak jednomyślności w tej kwestii jest następstwem niejawności informacji zawierających zarówno czynniki jak i zagrożenia, które uwzględnione zostały w procesie organizacji systemu ochrony. Wynika to bowiem i zależy od przyjętych przez organizatora danego systemu lub sieci warunków brzegowych oraz przyjętego kryterium oceny możliwości wystąpienia pojedynczego zagrożenia lub ich grupy.

Warto w tym miejscu zastanowić się jakie elementy współczesnego wojskowego systemu lub sieci telekomunikacyjnej mogą stanowić potencjalne źródło ujawnienia informacji. Z analizy wspomnianej literatury i przede wszystkim dokumentów normatywnych (ustawa i rozporządzenia) regulujących tę materię wynika, że zalicza się do nich:

- infrastrukturę telekomunikacyjną;
- elementy (urządzenia) telekomunikacyjne;
- elementy (urządzenia) informatyczne;
- aplikacje (oprogramowanie) systemowe;
- personel techniczny i użytkownicy systemu.

Nie zawsze jednak poszczególne elementy wymienione powyżej traktowane są równorzędnie. Zależności w tym przypadku kreuje środowisko pracy oraz otoczenie bliższe i dalsze poszczególnych elementów sieci lub systemu telekomunikacyjnego.

W polskojęzycznej wersji dokumentu sojuszniczego Dyrektywa Bezpieczeństwa AD-70-1-PL oraz w „Metodyce opracowywania Szczególnych Wymagań Bez-

---

[132] A. Dańczak, Bezpieczeństwo informacji w SZ RP....,op. cit. s. 12

[133] m.in. Pipkin D. L., Bezpieczeństwo informacji: ochrona globalnego przedsiębiorstwa, Wydawnictwo Naukowo-Techniczne, Wraszawa 2002, s. 231; Kryteria oceny bezpieczeństwa systemów łączności i informatyki, Praca zbiorowa, SWŁiI SG WP, Warszawa 1996, s. 27

pieczeństwa systemu lub sieci teleinformatycznej" (SWB) spotykamy się z wyróżnieniem następujących rodzajów zagrożeń:

- zagrożenia zewnętrzne,
- zagrożenia wewnętrzne,
- zagrożenia fizyczne.

Zagrożenia wewnętrzne w tym kontekście odnoszą się do:

- utraty lub uszkodzenia danych w wyniku celowego działania użytkownika;
- braku możliwości obsługi systemu lub sieci informatycznej z powodu nieprawidłowego funkcjonowania;
- straty lub uszkodzenia informacji spowodowanej nieautoryzowanym dostępem;
- zniszczenia danych poprzez błędy w aplikacjach użytkowych, oprogramowaniu systemowym bądź wprowadzenie tzw. oprogramowania „złośliwego" – wirusa.

O **zagrożeniu zewnętrznym** mówimy wówczas, gdy zachodzi lub zaszła możliwość utraty lub uszkodzenia danych, utrata możliwości obsługi systemu (sieci informatycznej), w wyniku celowego bądź przypadkowego działania ze strony osób nieuprawnionych działających w zewnętrznym otoczeniu sieci lub systemu.

W odniesieniu do podziału zagrożeń zawarte w Dyrektywie AD-70-1-PL o zagrożeniu fizycznym mówimy wówczas, gdy istnieje możliwość utraty lub uszkodzenia danych, urządzeń lub całych elementów systemu w wyniku katastrofy, klęski żywiołowej, które mają pośredni lub bezpośredni wpływ na poprawne funkcjonowanie systemu.

Inne spojrzenie na problematykę zagrożenia informacji w nowoczesnym systemie telekomunikacyjnym wykorzystującym w znacznej mierze techniki informatyczne przedstawili w opracowaniu „Społeczeństwo informacyjne: szanse, zagrożenia, wyzwania" Tomasz Goban-Klaus i Piotr Sienkiewicz[134]. Autorzy ci w swojej publikacji wyodrębnili następujące grupy zagrożeń:

1. Sabotaż i zagrożenia nieumyślne,

---

[134] T. Globan-Klaus, P. Sienkiewicz, Społeczeństwo informacyjne: szanse, zagrożenia, wyzwania, Wydawnictwo Fundacji Postępu Telekomunikacji, Kraków 1999, s. 58

2. Infiltracja.

Do pierwszej z wymienionych grup zaliczono zagrożenia charakteryzujące się występowaniem strat bez bezpośredniego materialnego czy informacyjnego zysku. Jako ich przykłady przytoczono:

- pożary i inne klęski żywiołowe;
- awarie zasilania (systemu energetycznego);
- dezintegrację lub „destrukcję informatyczną" (wirusy, bomby logiczne, konie trojańskie, itp.)
- fizyczne czynniki destrukcyjne i swoiste oddziaływanie ludzi.

Za główną przyczynę tego rodzaju szkód autorzy uważają beztroskę, nonszalancję, a nawet „głupotę" zarówno personelu technicznego odpowiedzialnego za funkcjonowanie systemu jak również i uprawnionych użytkowników.

Inne zagrożenie wymieniane w tej grupie to **sabotaż**. Jego zasadniczym celem jest wprowadzenie dezorganizacji w pracy, zniszczenia lub uszkodzenia systemu telekomunikacyjnego. I w tym przypadku główne źródło zagrożenia pochodzi ze strony człowieka. Może być to sfrustrowany, niezadowolony lub nieobowiązkowy pracownik techniczny realizujący obsługę systemu lub nawet jego użytkownik posiadający stosowną wiedzę lub uprawnienia. W sytuacji, gdy tego typu działanie inspirowane jest przez czynniki (osoby) zewnętrzne – wywiad gospodarczy państwa – to działanie takie nazywamy dywersją.

W przeciwieństwie do sabotażu **infiltracja** to takie działanie osób nieupoważnionych, które ma na celu dążenie do zapewnienia sobie dostępu lub pozyskania informacji znajdującej się w zasobach danego systemu telekomunikacyjnego lub informatycznego. Infiltracja realizowana jest różnymi metodami i środkami, a szczególnie poprzez „przenikanie" do celowo wybranych (najbardziej wrażliwych lub słabo chronionych) elementów tego systemu.

Infiltrację możemy podzielić na:

- bierną – śledzenie informacji w zadanym miejscu jej obiegu lub śledzenie częstotliwości wymiany informacji (np. zajętość kanału transmisyjnego);

– czynną – planowe i świadome pozyskiwanie informacji wynikające z uzyskania dostępu do zasobów systemu z możliwością ingerencji w najważniejsze elementy lub nawet strukturę systemu.

W wyniku **infiltracji biernej** przeciwnik może zagrażać poufności (prywatności) informacji lub danych. Nie może on jednak wpływać na ich treść. Najczęściej spotykane i stosowane metody infiltracji biernej to:

– przechwyt elektromagnetyczny oraz analiza sygnału emitowanego lub odbitego od promieniującego urządzenia (elementu systemu);
– dołączanie się do linii teletransmisyjnej systemu telekomunikacyjnego lub przechwyt informacji przesyłanej za pomocą środków radiowych;
– zdobywanie informacji przekazywanej środkami łączności, kanałami telekomunikacyjnymi w formie jawnej (bez zabezpieczenia kryptograficznego);
– analiza makulatury (np. wydruki komputerowe lub telefaksowe) oraz analiza elektronicznych nośników informacji;
– stosowanie ukrytych nadajników.

Z kolei w wyniku **infiltracji aktywnej**[135] przeciwnik bezpośrednio zagraża danym. Zagraża mianowicie ich autentyczności (integralności). Stosując infiltrację aktywną, informacje uzyskuje się poprzez:

– uzyskanie dostępu do systemu;
– uzyskanie potwierdzenia tożsamości lub hasła upoważnionego użytkownika;
– korzystanie z przyłączonych urządzeń końcowych, gdy uprawniony użytkownik zawiesza pracę;
– przechwytywanie informacji użytkownika i podstawienie w jej miejsce innych informacji;
– nielegalne korzystanie z komputera lub sprzętu łączności w czasie nie rejestrowanych prac konserwatorskich;
– nielegalny wydruk zawartości pamięci komputera po zakończeniu działania programu.

[135] Kryteria oceny bezpieczeństwa, op.cit. s. 32

Zasadniczym celem infiltracji aktywnej jest:

- zamazywanie dotychczasowych danych przez zapisanie na nich bezużytecznych danych;
- zmiana w treści danych;
- wprowadzenie dodatkowych rekordów danych, komunikatów wpływających na treść całości informacji.

Rozwój nowoczesnych systemów dowodzenia i sieci telekomunikacyjnych nieodłącznie związany jest z ich powszechną elektronizacją, a także automatyzacją procesów przetwarzania, składowania i przesyłania informacji, która w znacznym stopniu przyjmuje postać cyfrową. Ich zastosowanie w praktyce wpłynęło na pojawienie się (a fizycznie uzmysłowienie sobie) kolejnego zagrożenia dla bezpieczeństwa informacji w systemie telekomunikacyjnym wykorzystującym w swojej strukturze urządzenia informatyczne. Zagrożenie to określane jest pojęciem bezpieczeństwa emisji systemów telekomunikacyjnych i informatycznych.

Problemy powyższe wynikają ze specyficznej i skomplikowanej budowy urządzeń łączności i informatyki, opartej na układach elektronicznych oraz z niepotrzebnej nadprodukcji przez każde urządzenie informatyczne czy telekomunikacyjne energii emitowanej dookólnie, w liniach i kablach, która stanowi źródło wytwarzania i promieniowania (oprócz głównej emisji) emisji elektromagnetycznej ubocznej, niosącej w sobie część lub całość informacji użytkowej. Oznacza to tworzenie realnych możliwości do penetrowania naszych systemów przez wysoce wyspecjalizowane i wykwalifikowane służby wywiadowcze i to ze znacznych odległości, dochodzących nawet do kilku kilometrów, mających w swojej dyspozycji najnowocześniejsze środki i metody rozpoznania.

Prowadzone badania związane z zapewnieniem bezpieczeństwa łączności informacjom wykorzystującym ten rodzaj nowoczesnej techniki zostały ukierunkowane na określenie przyczyn występowania emisji ujawniającej i metod ochrony przed jej negatywnymi skutkami. Jest to dziedzina określana jako bezpieczeństwo emisji urządzeń informatycznych i telekomunikacyjnych. Najgroźniejszymi źródłami emisji ubocznej (ujawniającej) są: urządzenia łączności zbudowane w oparciu o ETO (Elek-

troniczną Technikę Obliczeniową) i mikrokomputery (komputery) wykonane standardowo.

Zjawisko to stanowi bardzo poważne zagrożenie, ponieważ walory użytkowe urządzeń elektronicznych nowej generacji oraz ich możliwości usprawniające i wspomagające procesy planistyczne, kierowania oraz dowodzenia jednostkami organizacyjnymi resortu Obrony Narodowej różnego szczebla stworzyły modę, która zmusza do posiadania zestawu komputerowego często taniego i tandetnego, w tym i na własne życzenie niebezpiecznego „szpiega" .

Problemy bezpieczeństwa łączności, emisji i ochrony informacji wiążą się ściśle z bezpieczeństwem narodowym, dlatego w państwach wysokorozwiniętych celem uniknięcia niekontrolowanego wykorzystania skutków powszechnej automatyzacji objęto je specjalnymi programami rządowymi. Zajmują się one wyłącznie opracowywaniem i zastosowaniem nowoczesnych środków i metod ochrony informacji oraz zachowania jej w ścisłej tajemnicy (w Stanach Zjednoczonych program rządowy **"TEMPEST"**)[136].

Słowo TEMPEST stało się swego rodzaju "wytrychem" używanym dla określenia ogółu zagadnień związanych z problemem emisji ujawniającej. Daje się to szczególnie zauważyć w publikacjach angielskojęzycznych. Można tam spotkać się z wypowiedziami traktującymi słowo TEMPEST jako akronim od angielskiego określenia Transient ElectroMagnetic Pulse Emanation Standard. Jednak oficjalne źródła rządowe nie potwierdzają tej tezy.

Dokument normujący powyższe zagadnienie zawiera instrukcje dla agencji federalnych USA dotyczące zabezpieczania informacji przed emisją ujawniającą. Jest on klasyfikowany jako tajny i określa procedury dla różnych rządowych wydziałów oraz przedstawicielstw mające na celu określenie środków bezpieczeństwa wymaganych dla urządzeń przetwarzających dane mające wpływ na bezpieczeństwo narodowe Stanów Zjednoczonych.

---

[136] M. Swanson, B. Guttman, Generally Accepted Principles and Practices for Securing Information Technology Systems, NIST, SP 800-14, September 1996, s. 78

Praktycznie prawie każde urządzenie w nowoczesnym systemie telekomunikacyjnym jest źródłem promieniowania elektromagnetycznego. Promieniowanie to może przybrać jedną z trzech form propagacji:

- pola elektrycznego i pola magnetycznego oraz fal elektromagnetycznych;
- fal elektromagnetycznych (tzw. fal powierzchniowych) emitowanych z zewnętrznych powłok metalicznych kabli koncentrycznych;
- prądów i napięć interferencyjnych indukowanych w liniach zasilania.

Informacja skorelowana z niekontrolowaną emisją promieniowania jest łatwa do przechwycenia. Zwykły odbiornik telewizyjny może stać się odbiornikiem sygnału niekontrolowanej emisji z odległości sięgającej do 100 metrów od jej źródła. W przypadku zastosowania odbiorników o większej czułości możliwe jest przechwycenie informacji nawet z odległości ponad kilometra. W przypadku fal powierzchniowych oraz pól indukowanych w kablach zasilających odległości te wynoszą ok. 100 - 150 m.

Jak wcześniej wspomniano nie ma jednolitego podejścia do problematyki zagrożeń dla bezpieczeństwa informacji czy ich podziału w odniesieniu do systemów telekomunikacyjnych lub informatycznych. Problematykę te rozpatruje się w działaniach praktycznych w wielu aspektach i płaszczyznach. Jednak zawsze ich podstawę stanowiły kryteria, według których rozpatrywane były zagadnienia możliwości wystąpienia zagrożeń bezpieczeństwa informacji dla konkretnych systemów i sieci oraz warunków w jakich one funkcjonują. Z tej przyczyny można pokusić się o swoiste i niekonwencjonalne podejście do problemu. Znając obszary, w których stosowane są przedsięwzięcia związane z ochroną informacji w systemach telekomunikacyjnych i informatycznych, spróbujemy zidentyfikować te zagrożenia, którym one przeciwdziałają. Normatywne dokumenty narodowe i sojusznicze narzucają bez wskazywania konkretnych zagrożeń, czy też ich rodzajów, stosowanie przedsięwzięć zapewniających ochronę dla systemów i sieci jako całości lub wybranych ich elementów oraz samej informacji w następujących obszarach:

- organizacyjno-proceduralnym,
- personalnym,
- fizycznym,
- technicznym.

Przedstawione obszary należy traktować jako bardzo ogólne i dopiero ich rozpatrywanie w kontekście konkretnego systemu jest równoznaczne z identyfikacją zagrożeń jednostkowych czy też całych grup zagrożeń.

Jednak w trakcie dalszych rozważań opierając się na obowiązujących dokumentach normatywnych oraz na podstawie praktyki i doświadczeń, podjęta zostanie próba przyporządkowania najczęściej identyfikowanych i występujących zagrożeń dla bezpieczeństwa informacji w uprzednio wymienionych obszarach, które stanowią podstawę do określenia niezbędnych środków przeciwdziałania w celu spełnienia wymagań stawianych przed systemem ochrony.

Każda organizacja (instytucja) państwowa lub niepubliczna, a w tym kontekście szczególnie siły zbrojne, w procesie wymiany informacji za pomocą technicznych środków łączności i informatyki musi mieć na uwadze fakt, że dane te przekazywane w sposób chaotyczny i niezorganizowany mogą przynieść więcej szkody niż korzyści. Zasada powyższa nabiera głębszego znaczenia w kontekście informacji opatrzonej klauzulą niejawności (tajemnica państwowa i służbowa) lub dedykowanej (prywatność). Z tej przyczyny począwszy od kierownictwa organizacji czy instytucji poprzez jej poszczególne szczeble organizacyjne, a kończąc na poszczególnych użytkownikach terminali końcowych systemu telekomunikacyjnego lub informatycznego niezbędne jest zrozumienie istoty problemu i opracowanie, a następnie **wdrożenie organizacyjnych zasad (procedur)** posługiwania się środkami łączności i informatyki. W ramach ustalonych procedur kierownictwo organizacji winno przydzielić poszczególnym pracownikom stopnie uprawnień, które w zależności od zajmowanego stanowiska, zapewniają możliwość dostępu do informacji wrażliwej (chronionej) dla danej instytucji czy organizacji.

Ograniczenie zagrożeń w tym zakresie zapewnia przygotowanie i wdrożenie przez właściwe organa dla danej jednostki organizacyjnej polityki bezpieczeństwa, której celem jest stworzenie podstaw, procedur i wymagań niezbędnych dla zapewnienia właściwej ochrony wytwarzanym, przetwarzanym, przechowywanym lub przesyłanym w systemie informacjom.

Polityka bezpieczeństwa[137] powinna obejmować takie działy jak:

---

[137] A.Sadowski, „Czym jest polityka bezpieczeństwa organizacji" – www.bezpieczeństwoit.pl

- bezpieczeństwo środków łączności i informatyki;
- bezpieczeństwo osobowe, fizyczne, przemysłowe i emisji.

W każdym systemie informacyjnym, a tym samym w systemie telekomunikacyjnym czy informatycznym, największe zagrożenie dla bezpieczeństwa informacji **stanowi czynnik ludzki**. Ludzkie błędy mogą przyczynić się między innymi do:

- celowej lub niezamierzonej utraty poufności informacji (ujawnienie);
- utraty integralności danych na skutek zamierzonego działania lub błędu użytkownika;
- zniszczenia urządzenia lub danych na skutek niedbalstwa;
- czasowego lub całkowitego „zawieszenia" systemu (przerwa w działaniu).

Dosyć często zagrożenia są wynikiem braku dostatecznej wiedzy na temat wymagań bezpieczeństwa. Reguły w instytucji są, lecz pracownicy ich nie znają - nie wiedzą, co do nich należy ani jak się zachować w określonej sytuacji.

Pojęcie **zagrożeń fizycznych** w kontekście systemu telekomunikacyjnego i informatycznego nieodłącznie kojarzyć się może ze zniszczeniem infrastruktury telekomunikacyjnej, urządzeń bądź samych obiektów, w których poszczególne elementy systemu są zainstalowane. Ich zniszczenie może nastąpić wskutek celowego działania potencjalnego przeciwnika w trakcie przygotowań do walki (okres kryzysu) lub w czasie prowadzenia działań zbrojnych bądź też jako efekt zaistnienia klęski żywiołowej takiej jak:

- pożar,
- powódź,
- trzęsienie ziemi,
- itp.

Ponadto do tej grupy należy zaliczyć następujące zagrożenia w ramach, których może nastąpić:

- niekontrolowany (nieuprawniony) dostęp do infrastruktury lub urządzeń systemu telekomunikacyjnego, a tym samym do informacji znajdującej się w nim;

– możliwość podglądu, podsłuchu lub innej formy obserwacji zapewniającej nieautoryzowany dostęp do zasobów informacyjnych systemu.

Innym skojarzeniem, które może nasuwać się nam przy zagrożeniach fizycznych to prewencja - odpowiednie zamykanie i ochrona pomieszczeń, służby ochrony, system przepustek, szafy pancerne, itd.

Zgodnie z przedsięwzięciami zabezpieczającymi informację w systemie telekomunikacyjnym oraz informatycznym na **płaszczyźnie technicznej** możemy wyodrębnić następujące zagrożenia mające wpływ na:

– bezpieczeństwo kryptograficzne,
– bezpieczeństwo elektromagnetyczne (emisja ujawniająca),
– bezpieczeństwo transmisji informacji,
– bezpieczeństwo programowe,
– bezpieczeństwo wsparcia technicznego.

Ze względu na wcześniej omówione zagrożenia, będące wynikiem niepożądanej emisji ujawniającej (elektromagnetycznej), ten aspekt zagrożeń zostanie pominięty.

W codziennej działalności służbowej każdy z nas, choć być może nie w pełni tego świadom, korzysta ze stacjonarnego lub polowego systemu telekomunikacyjnego Sił Zbrojnych RP przy okazji każdorazowego podniesienia np. słuchawki aparatu telefonicznego. Wymiana informacji podczas rozmowy dotyczy szerokiej gamy obszarów czy też różnych spraw. Rzadko jednak użytkownicy uświadamiają sobie, że zarówno w warunkach stacjonarnych jak i polowych mają do czynienia z urządzeniami końcowymi systemu telekomunikacyjnego lub informatycznego, który zapewnia nam wymianę informacji jawnej lub klasyfikowanej.

Najczęściej spotykanym zagrożeniem jest przekazywanie informacji niejawnych za pośrednictwem jawnych linii telekomunikacyjnych lub systemów informatycznych. Należy przy tym pamiętać, że uzyskanie przez osoby niepowołane pełnego dostępu do zbioru informacji jawnych np. podsłuch rozmów czy odczyt danych z dysku twardego komputera daje obraz kompetencji służbowych, realizowanych zadań i podejmowanych decyzji co sumarycznie wcale nie musi oznaczać informacji jawnej. Stąd też biorą się zagrożenia wymagające ochrony kryptograficznej.

W przypadku informacji klasyfikowanych wymogiem jest stosowanie urządzeń utajniających lub szyfrujących zapewniających kryptograficzną ochronę informacji. Zasadniczym problemem w tej materii jest określenie maksymalnego poziomu niejawności informacji, która w systemie telekomunikacyjnym lub informatycznym bez względu na rodzaj urządzenia końcowego może być przekazywana. Zastosowanie urządzeń zapewniających niższe niż wymagane bezpieczeństwo informacji jest głównym zagrożeniem.

Innym zagrożeniem dla bezpieczeństwa informacji z punktu widzenia kryptografii jest stosowanie w systemie telekomunikacyjnym urządzeń i/lub dokumentów kluczowych niezgodnie z ich przeznaczeniem oraz bez wydanych przez Służby Ochrony Państwa certyfikatów uprawniających je do zabezpieczenia informacji na określonym poziomie poufności.

Systemy kryptograficzne wymagają ścisłego przestrzegania procedur oraz zasad, od których najmniejsze czasami odstępstwo może przyczynić się do jego całkowitego wycofania z eksploatacji w systemie telekomunikacyjnym. Może to nastąpić wskutek utraty urządzenia kryptograficznego, zagubienia lub kradzieży różnych edycji dokumentów kluczowych lub dokumentacji implementacyjnej samego algorytmu szyfrującego (kody źródłowe).

Jednym z zasadniczych zadań każdego systemu telekomunikacyjnego czy też informatycznego jest przekazywanie informacji z jednego punktu do drugiego. Odległość między nimi uzależniona jest od przyjętych założeń i celu funkcjonowania systemu. Transmisja, czyli przekaz informacji może odbywać przy użyciu różnych takich mediów jak:

- linia kablowa (w tym światłowód),
- linia radiowa (radioliniowa, satelitarna),
- inne systemy elektromagnetyczne.

Każda z przedstawionych powyżej form transmisji narażona jest na zagrożenia, które w myśl dokumentów normatywnych Organizacji Paktu Północnoatlantyckiego[138] można podzielić następująco:

[138] „Transmission security" - MC322, NATO HQ, Brussells 1992

- nieautoryzowany przechwyt (przejęcie) informacji,
- zakłócanie,
- interferencja,
- analiza ruchu telekomunikacyjnego,
- podszywanie się.

Nieautoryzowany przechwyt informacji należy traktować jako działanie w celu poszukiwania, podsłuchu lub nagrywania wymiany telekomunikacyjnej do celów wywiadowczych lub oszukania przeciwnika poprzez "spoofing"[139] lub podszywanie się pod użytkownika systemu. Poprzez „spoofing" należy rozumieć przejęcie, zamianę i retransmisję sygnału w celu wprowadzenia w błąd odbiorcy sygnału.

Podszywanie się pod uprawnionego użytkownika systemu telekomunikacyjnego ma na celu zdobycie informacji pochodzącej z wymiany danych, ale również możliwość dokonania jej modyfikacji lub powtórzenia transmisji celem oszukania, wprowadzenia zamieszania lub przeciążenia systemu telekomunikacyjnego.

Zakłócanie wymiany informacji w systemie telekomunikacyjnym ma na celu obniżenie efektywności funkcjonowania zastosowanych w systemie urządzeń i sprzętu elektronicznego, aż do całkowitego zablokowania możliwości nadawania lub odbioru danych.

Przykładem mogą być zakłócenia interferencyjne, które są efektem transmisji na tej samej lub pobliskiej częstotliwości, a ich wynikiem jest zazwyczaj zanik lub wariacja pożądanej amplitudy sygnału.

Głównym i zasadniczym celem analizy ruchu jest sprawdzanie charakterystyki wymiany telekomunikacyjnej dla celów wywiadowczych wynikających z natury ruchu telekomunikacyjnego.

W tradycyjnych analogowych systemach telekomunikacyjnych zagrożenia bezpieczeństwa programowego dla ochrony informacji nie występowały. Nowoczesna technika mikrokomputerowa, która na stałe zagościła w telekomunikacji ze wszelkimi niesionymi przez siebie dobrodziejstwami, dostarcza również i zagrożeń – w tym zagrożeń programowych. Wynika to z faktu, że np.: centrale telefoniczne oraz inne urzą-

---

[139] Dokument NATO serii AMSG 524 – „Słownik pojęć i definicji z zakresu bezpieczeństwa łączności i informatyki"

dzenia komutacyjne czy transmisyjne systemu telekomunikacyjnego zawierają w sobie specjalizowane komputery.

Nieautoryzowany dostęp do oprogramowania systemowego, a w tym do oprogramowania umożliwiającego zarządzanie nawet całym systemem telekomunikacyjnym może przyczynić się do zawieszenia lub zablokowania funkcjonowania tego systemu. Przyczyną takiego stanu rzeczy może być wprowadzenie przez osoby nieuprawnione do oprogramowania popularnie znanych wirusów, „koni trojańskich" lub innego oprogramowania szkodliwego.

Jako zagrożenie dla bezpieczeństwa programowego należy traktować również implementację oprogramowania użytkowego, które nie zostało zainstalowane przez uprawniony personel techniczny lub niezgodnie z zaleceniami oraz przeznaczeniem.

System telekomunikacyjny stacjonarny lub polowy jest rozwijany i funkcjonuje w otoczeniu określonej infrastruktury telekomunikacyjnej. **Wsparcie techniczne** ma za zadanie zapewnić sprawne techniczne funkcjonowanie systemu, a tam gdzie jest to wymagane również jego bezpieczeństwo.

W sytuacji, gdy w systemie znajdują się lub przekazywane są informacje podlegające ochronie jednym z zasadniczych zagrożeń jest brak kontroli dostępu do infrastruktury telekomunikacyjnej oraz elementów lub kluczowych urządzeń systemu decydujących o jego niezakłóconej bądź bezpiecznej pracy. Niewdrożenie przedsięwzięć wsparcia technicznego, takich jak np. montaż systemu kontroli wstępu (karty magnetyczne) do wydzielonych obiektów lub systemu antywłamaniowego o klasie adekwatnej do klauzuli przetwarzanych, przechowywanych lub przesyłanych w systemie informacji bądź innego systemu ograniczającego dostęp do obszarów (stref), gdzie wejście do nich umożliwia bezpośredni dostęp do chronionej informacji stanowi poważne zagrożenie, a nawet naruszenie bezpieczeństwa. Dotyczy to szczególnie obiektów, pomieszczeń lub stref infrastruktury telekomunikacyjnej, w których zamontowane są urządzenia bezobsługowe i nie jest wymagana obecność personelu technicznego.

4.2. GRADACJA ZAGROŻEŃ BEZPIECZEŃSTWA INFORMACJI W POLOWYCH WOJSKOWYCH SIECIACH TELEKOMUNIKACYJNYCH

Posiadając tak usystematyzowaną wiedzę w zakresie podziału i charakterystyki najważniejszych zagrożeń dla bezpieczeństwa informacji w sieci telekomunikacyjnej można podjąć próbę dokonania oceny, które z nich są najistotniejsze oraz najczęściej występują z punktu widzenia przedsięwzięć realizowanych w ramach ochrony sieci lub wojskowych systemów telekomunikacyjnych.

W literaturze przedmiotu oraz w różnych periodykach poświęconych bezpieczeństwu informacji ocena tego typu jest traktowana raczej marginalnie i bardzo powierzchownie. Wynika to prawdopodobnie z faktu, że znakomita większość „incydentów" oraz zdarzeń związanych z nieautoryzowanym ujawnieniem informacji jest skrzętnie skrywana przez różne organizacje, w których fakt ten miał miejsce. Niepodawanie do publicznej wiadomości omawianych zdarzeń w sektorze gospodarczym związane jest przede wszystkim z koniecznością zachowania dobrego wizerunku danej firmy bądź instytucji na rynku globalnym. Utrata wizerunku powoduje brak wiarygodności u potencjalnych kontrahentów i w efekcie może pośrednio przyczynić się do upadku firmy. W sektorze finansowym – bankowości, informacje na temat włamań np. do systemu określonego banku również mogą stać się podstawą do wycofania przez część lub ogół klientów zarówno indywidualnych jak i korporacyjnych, przetrzymywanych w nim aktywów w celu uniknięcia strat.

Dotarcie zatem do tego typu informacji wprost jest bardzo utrudnione, a jeżeli jest już możliwe, to zostaje zazwyczaj obwarowane całym szeregiem rygorów – w tym zakazem dalszego rozpowszechniania tych danych.

Tego typu stanowisko oraz szereg przedsięwzięć mających na celu ograniczenie do minimum kręgu osób praktykowana jest w odniesieniu do wszelkiego rodzaju zdarzeń i incydentów mających miejsce w wojskowych systemach i sieciach telekomunikacyjnych bądź informatycznych.

Przystępując zatem do analizy stopnia możliwości występowania różnego rodzaju zagrożeń czy incydentów wpływających na poziom bezpieczeństwa informacji w wojskowych systemach telekomunikacyjnych należy uwzględnić ich specyfikę odróżniającą je od zwykłych systemów komercyjnych czy nawet rządowych. Tylko bo-

wiem wojskowe systemy i sieci możemy rozpatrywać jako systemy wykorzystujące stacjonarną infrastrukturę telekomunikacyjną oraz jako polowe, które zapewniają wymianę informacji w systemie dowodzenia wojskami, począwszy od sytuacji kryzysowych aż po prowadzenie działań zbrojnych.

Prowadzenie analizy ryzyka w zakresie ochrony informacji w systemach stacjonarnych jest prostsze niż realizacja tego samego przedsięwzięcia w systemach polowych. Związane jest to z jasnym określeniem struktury organizacyjnej, dostępnym czasem na przeprowadzenie ewentualnych zmian konfiguracyjnych, czy też znajomością środowiska oraz otoczenia, w którym system będzie funkcjonował.

Takiego komfortu organizatorzy systemu w przypadku systemów polowych, nie posiadają choćby ze względu na ciągłe zmiany w ugrupowaniu bojowym (położenie i konfiguracja) oraz towarzyszące temu zmiany środowiska pracy, czy otoczenia funkcjonującego systemu, które nie zawsze można w pełni przewidzieć.

Z tej też przyczyny analiza w zakresie ochrony informacji zostanie ograniczona do polowego systemu telekomunikacyjnego wojsk lądowych, który poza spektrum zagrożeń identyfikowanych dla systemu stacjonarnego uwzględnia również oddziaływanie ogniowe i radioelektroniczne przeciwnika.

Poszukując źródeł informacji, która pozwalałaby przeprowadzić taką analizę, można dokonać przeglądu dokumentacji wybranych ćwiczeń, treningów sztabowych szczebla brygadowego i dywizyjnego czy korpuśnego, gdzie równolegle z planowaniem, a następnie organizacją sieci telekomunikacyjnej, organizowane były działania zapewniające ochronę informacji. Jednak dokumentacja zawiera suche fakty w zakresie organizacji i przedsięwzięć, które to bezpieczeństwo zapewniają. Nie wymieniane są ani potencjalne, ani faktyczne zagrożenia, które zaistniały w czasie pracy sieci czy systemu. Jednak ten stan rzeczy pozwala na wyciągnięcie wniosku, że jeśli została opracowana dokumentacja to jest również personel techniczny oraz osoby funkcyjne, które zarówno organizowały system ochrony jak i monitorowały jego funkcjonowanie. Wniosek ten sprowadza się do stwierdzenia, że podstawowym źródłem informacji w tym zakresie mogą być i są etatowi pracownicy organów bezpieczeństwa łączności i informatyki szczebla taktycznego, którzy w swojej codziennej działalności służbowej

rozwiązują problemy wynikające z potrzeby ochrony informacji w wojskowych systemach telekomunikacyjnych.

Do rozstrzygnięcia pozostaje jeszcze jeden problem - forma i metoda uzyskania danych od miarę licznego, bo kilkudziesięcioosobowego grona specjalistów bez intencjonalnego wchodzenia w sferę zastrzeżonych zasobów informacyjnych, które są wykorzystywane tylko w pewnym kręgu osób funkcyjnych na zasadzie tzw. wiedzy koniecznej. Prowadząc analizę różnych metod naukowych, które uwzględniałyby założone ograniczenia i pozwalały na osiągnięcie w miarę obiektywnych wyników wydaje się, że najlepsze w zaistniałej sytuacji jest przeprowadzenie anonimowego badania ankietowego, które jednocześnie nie będzie ograniczać się do konkretnego systemu (sieci) funkcjonującego w określonym czasie i przestrzeni.

W celu uwiarygodnienia uzyskanych wyników w stosunku do respondentów narzucono pewne ograniczenia, które winny umożliwić uzyskanie jak najbardziej zbliżonych do rzeczywistości ocen w zakresie zagrożeń bezpieczeństwa informacji w polowych systemach telekomunikacyjnych wojsk lądowych (załącznik nr 4).

Mając sformułowane ograniczenia w stosunku do przyszłej „populacji" poddawanej badaniu nadszedł czas, aby zastanowić się nad treścią i układem samej ankiety. Rozważania w tej materii dotyczyły dwóch wariantów. Pierwszy z nich zakładał, że w stosunku do każdej grupy zagrożeń bezpieczeństwa informacji (personalnym, fizycznym, organizacyjno-proceduralnym i technicznym)w polowym systemie telekomunikacyjnym zostanie sprecyzowane oddzielne pytanie oraz w formie pewnego rodzaju „naprowadzenia" przedstawione będą przykłady zagrożeń.

Po uwzględnieniu całościowego podejścia zarówno do wojskowego systemu (sieci) telekomunikacyjnego oraz zagrożeń z tym związanych przeważył wariant drugi, w którym zakładano przygotowanie jednego pytania obejmującego wszystkie poddawane ocenie obszary. Wzorem poprzedniego wariantu każdej z wymienionych grup przypisano określone i wcześniej omówione zagrożenia bezpieczeństwa informacji.

Wynikiem tak prowadzonej analizy problemu było opracowanie jednego pytania ankietowego, które ostatecznie przyjęło następujące brzmienie:

Jakie jest prawdopodobieństwo wystąpienia zagrożenia ujawnienia lub utraty bezpieczeństwa informacji w polowym systemie telekomunikacyjnym związku tak-

tycznego w kontekście implementowanych organizacyjno-technicznych i eksploatacyjnych środków ochrony informacji?

Badaniu ankietowemu poddano łącznie około 65% ogółu pracowników pionu bezpieczeństwa łączności i informatyki wojsk lądowych szczebla taktycznego, ale po uwzględnieniu nałożonych na wstępie ograniczeń wyniki opracowano w oparciu o odpowiedzi udzielone przez 71 respondentów.

Zgodnie z przyjętym podziałem pierwszą rozpatrywaną płaszczyzną były zagrożenia pochodzące ze strony człowieka – personalne. Wśród nich jako szczegółowe wyodrębniono zagrożenia pochodzące ze strony:

- personelu technicznego,
- użytkowników systemu,
- osób funkcyjnych – różnych szczebli dowodzenia,
- oraz innych osób, które nie posiadają stosownych uprawnień zarówno do dostępu do urządzeń, lecz także zasobów informacyjnych systemu.

Przed rozpoczęciem ankietowania, w krótkim instruktażu, uszczegółowiono pojęcie „inne osoby", które należy pojmować jako osoby prowadzące szeroko rozumianą działalność agenturalną i szpiegowską.

Poddając analizie uzyskane w ramach przeprowadzonego badania ankietowego wyniki, nie można bezpośrednio i jednoznacznie stwierdzić, że zagrożenia te mają zasadniczy wpływ na poziom bezpieczeństwa informacji w sieci telekomunikacyjnej, bowiem opinie rozłożyły się niemal równomiernie. Jednak najliczniejsza grupa respondentów oceniła zdarzenia i incydenty wpływające na poziom bezpieczeństwa informacji, które pochodzą ze strony człowieka na poziomie średnim (tabela 4.2.1). Szczególną uwagę w tym przypadku zwrócić należy na fakt, że ponad jedna trzecia (37,14 %) badanych wykazała, iż głównym źródłem ich powstania są sami użytkownicy lub osoby funkcyjne różnego szczebla. Poddając ogólnej ocenie tę grupę zagrożeń największa liczba ankietowanych (28,57%) stwierdziła, że ich istotność jest na poziomie średnim.

Tabela 4.2.1

Zagrożenia personalne

Zagrożenia dla bezpieczeństwa informacji	Stopień prawdopodobieństwa wystąpienia zagrożenia				
	Bliskie jedności	Duże	Średnie	Małe	Bliskie zeru
Personalne:					
- ze strony personelu	**2,86**	**11,43**	**25,71**	**37,14**	**22,86**
- ze strony użytkowników	**5,71**	**31,43**	**37,14**	**22,86**	**2,86**
- ze strony osób funkcyjnych	**8,57**	**22,86**	**37,14**	**25,71**	**5,71**
- ze strony innych nieuprawnionych osób	**11,43**	**28,57**	**14,29**	**22,86**	**22,86**

Źródło: opracowanie własne na podstawie wyników badań metodą sondażu diagnostycznego techniką ankiety – załącznik nr 4

Następnym obszarem rozpatrywanym i poddanym ocenie pracownikom organów bezpieczeństwa łączności i informatyki szczebla taktycznego były zagrożenia w płaszczyźnie fizycznej. Wśród tej grupy wyodrębniono następujące zagrożenia szczegółowe:

- źle zorganizowaną obroną lub zbyt słabo ochraniane elementy systemu (np. warta);
- nieadekwatne zabezpieczenia zapewniające dostęp do wrażliwych elementów infrastruktury telekomunikacyjnej;
- w wyniku celowego działania potencjalnego przeciwnika;
- w rezultacie zaistnienia klęski żywiołowej, itp.

Wyniki przeprowadzonego badania ilustruje tabela 4.2.2. Tak jak w poprzednim przypadku nie można jednoznacznie wywnioskować, które z przytoczonych zagrożeń jest najważniejsze, gdyż odpowiedzi respondentów kształtują się prawie równomiernie na poziomie około 1/3 przy stopniach prawdopodobieństwa między małym a dużym.

Tabela 4.2.2

Zagrożenia fizyczne

Zagrożenia dla bezpieczeństwa informacji	Stopień prawdopodobieństwa wystąpienia zagrożenia				
	Bliskie jedności	Duże	Średnie	Małe	Bliskie zeru
Fizyczne:					
- źle zorganizowanej lub zbyt słabej ochrony elementów systemu (np. warta)	8,57	31,43	34,29	17,14	8,57
- nieadekwatne zabezpieczenia zapewniające dostęp do wrażliwych elementów infrastruktury telekomunikacyjnej. urządzeń systemu tj. drzwi, okna, kraty, itp.	2,86	22,86	28,57	34,29	11,43
- w wyniku celowego działania potencjalnego przeciwnika	17,14	34,29	25,71	20,00	2,86
- w rezultacie zaistnienia klęski żywiołowej, itp.	2,86	20,00	31,43	31,43	14,29

Źródło: opracowanie własne na podstawie wyników badań metodą sondażu diagnostycznego techniką ankiety – załącznik nr 4

Jeśli jednak zostaną pominięte najwyżej oceniane zagrożenia (34,29 %) podane w poszczególnych przykładach i wyciągnięta będzie średnia dla przyjętych stopni prawdopodobieństwa wystąpienia zagrożeń fizycznych, to w tej sytuacji 40 % respondentów uznaje istotność zagrożeń na poziomie średnim.

Trzecim obszarem zagrożeń, który poddany został osądowi respondentów, była problematyka możliwości wystąpienia zagrożeń bezpieczeństwa informacji w polowej sieci telekomunikacyjnej w płaszczyźnie organizacyjno-proceduralnej. Wzorem poprzednio rozważanych grup wyróżniono w niej następujące potencjalne zagrożenia szczegółowe:

- niewłaściwy przydział uprawnień;
- brak lub niski poziom szkolenia;
- niezrozumiałe procedury postępowania w sytuacjach krytycznych;

– niewłaściwa struktura i/lub zakres kompetencji organów odpowiedzialnych za bezpieczeństwo w systemach telekomunikacyjnych.

Tabela 4.2.3.

Zagrożenia w obszarze organizacyjno-proceduralnym

Zagrożenia dla bezpieczeństwa informacji	Stopień prawdopodobieństwa wystąpienia zagrożenia				
	Bliskie jedności	Duże	Średnie	Małe	Bliskie zeru
Organizacyjno-proceduralne:					
- niewłaściwego przydziału uprawnień	11,43	48,57	22,86	17,14	0,00
- brak lub niski poziom szkolenia	11,43	45,71	28,57	14,29	0,00
- niezrozumiałe procedury postępowania w sytuacjach krytycznych	5,71	51,43	31,43	11,43	0,00
- niewłaściwa struktura i/lub zakres kompetencji organów odpowiedzialnych za bezpieczeństwo w systemach telekomunikacyjnych	11,43	34,29	34,29	17,14	2,86

Źródło: opracowanie własne na podstawie wyników badań metodą sondażu diagnostycznego techniką ankiety – załącznik nr 4

W tym konkretnym przypadku łatwo jest zwrócić uwagę na fakt, że uzyskane odpowiedzi na pierwsze trzy punkty wymieniające zagrożenia szczegółowe (tabela 4.2.3) w sposób znaczący wskazują, iż ten typ zagrożeń jest istotny dla bezpieczeństwa informacji w polowej sieci telekomunikacyjnej wojsk lądowych. Podstawą tak sformułowanej opinii są uzyskane wyniki badania, które wykazują duże prawdopodobieństwo ich wystąpienia bowiem zarówno niewłaściwy przydział uprawnień jak i brak lub niski poziom szkolenia oraz niezrozumiałe procedury postępowania w sytuacjach krytycznych oscylują na zbliżonym do siebie poziomie – około 50%. Pozostałe przyjęte stopnie prawdopodobieństwa zaistnienia wymienionych zagrożeń są traktowane marginalnie. Ostatnie z wymienionych zagrożeń szczegółowych w tym obszarze, jak niewłaściwa struktura i/lub zakres kompetencji organów odpowiedzialnych za bezpieczeństwo w systemach telekomunikacyjnych, były traktowane przez tę samą liczbę respondentów (34,29 %) jako zagrożenia, których wystąpienie jest możliwe

z dużym lub średnim prawdopodobieństwem. Uzyskane wyniki pozwalają zatem sądzić, że zagrożenia, które przypisane zostały płaszczyźnie organizacyjno proceduralnej stanowią istotny czynnik mający wpływ na poziom bezpieczeństwa informacji w polowych sieciach telekomunikacyjnych wojsk lądowych.

Ostatnim z rozpatrywanych obszarów, w którym mogą zaistnieć lub wystąpić zagrożenia dla bezpieczeństwa informacji był obszar techniczny. Jednak poddając go opinii i ocenie respondentów biorących udział w badaniu ankietowym trzeba uwzględniać jego złożoność i wieloaspektowość. Z tej też przyczyny w ramach tego obszaru wyróżniono zgodnie z uprzednio przyjętym podziałem zagrożeń następujące płaszczyzny:

- zagrożenia bezpieczeństwa kryptograficznego;
- zagrożenia związane z emisją ujawniającą;
- zagrożenia związane oprogramowaniem systemowym i aplikacjami użytkowymi;
- zagrożenia w czasie przekazu informacji za pomocą technicznych środków łączności (transmisyjne);
- zagrożenia dla systemów wspierających technicznie ochronę informacji.

Przyjęte płaszczyzny zagrożeń oraz ich odrębność i niezależność z punktu widzenia stosowanych rozwiązań technicznych skłaniają do tego, aby każdą z wymienionych płaszczyzn poddać oddzielnej ocenie przez ankietowanych.

Zgodnie z wymienionym wcześniej podziałem jako pierwsze ocenie poddane były zagrożenia bezpieczeństwa informacji związane z problematyką ochrony kryptograficznej.

W trakcie badania ankietowego wyodrębniono w tej płaszczyźnie następujące zagrożenia szczegółowe:

- odpowiednio dobrana moc algorytmów kryptograficznych;
- nieprzestrzeganie zasad w zakresie obiegu i dostępu do urządzeń kryptograficznych;
- nieprzestrzeganie zasad w zakresie obiegu i dostępu do materiałów kryptograficznych;
- stosowanie urządzeń i dokumentów bez świadectwa certyfikacyjnego.

Uzyskane wyniki (tabela 4.2.5), szczególnie w odniesieniu do trzech pierwszych przytoczonych zagrożeń, uważane są przez ankietowanych za ważne, a stopień prawdopodobieństwa ich wystąpienia jako duży.

Tabela 4.2.4

Zagrożenia bezpieczeństwa informacji w obszarze ochrony kryptograficznej

Zagrożenia dla bezpieczeństwa informacji	Stopień prawdopodobieństwa wystąpienia zagrożenia				
	Bliskie jedności	**Duże**	**Średnie**	**Małe**	**Bliskie zeru**
Techniczne - kryptografia:					
- odpowiednio dobrana moc algorytmów kryptograficznych	**8,57**	**40,00**	**17,14**	**22,86**	**11,43**
- nieprzestrzeganie zasad w zakresie obiegu i dostępu do urządzeń kryptograficznych	**8,57**	**57,14**	**20,00**	**8,57**	**5,71**
- nieprzestrzeganie zasad w zakresie obiegu i dostępu do materiałów kryptograficznych	**25,71**	**48,57**	**8,57**	**5,71**	**11,43**
- stosowanie urządzeń i dokumentów bez świadectwa certyfikacyjnego	**14,29**	**22,86**	**28,57**	**14,29**	**20,00**

Źródło: opracowanie własne na podstawie wyników badań metodą sondażu diagnostycznego techniką ankiety – załącznik nr 4

Zdaniem respondentów mniejszy wpływ (średni) na poziom bezpieczeństwa informacji w polowej sieci telekomunikacyjnej ma stosowanie zarówno urządzeń jak i dokumentów komercyjnych, czyli tych które nie posiadają wymaganego przez Służby Ochrony Państwa atestu – certyfikatu.

Dokonawszy uśrednienia otrzymanych rezultatów badania, można powiedzieć, że ponad 42 % biorących udział w ankiecie uważa, iż istnieje duże prawdopodobieństwo wystąpienia zagrożeń w płaszczyźnie ochrony kryptograficznej. Do ich wystąpienia na poziomie średnim przychyla się już tylko niecałe 19 % ankietowanych. Stąd też wniosek, że należy bardzo uważnie przestrzegać zasad w zakresie obiegu i dostępu do urządzeń i materiałów kryptograficznych. Zapewnienie bowiem hermetycznie za-

mkniętego ich obiegu, a także ograniczenie dostępności do niezbędnego minimum stanowi o bezpieczeństwie nie tylko samej informacji, lecz także całego systemu i to od momentu ich wytworzenia, aż do fizycznego zniszczenia po wycofaniu z eksploatacji.

Drugim elementem (płaszczyzną) składowym zagrożeń bezpieczeństwa informacji w polowej sieci telekomunikacyjnej znajdującym się w obszarze technicznym jest emisja ujawniająca. W jej ramach do zagrożeń szczegółowych można zaliczyć:

- stosowanie w systemie niezbadanych urządzeń komercyjnych,
- brak strefy (obszaru kontrolowanego),
- nie przestrzeganie zasad rozmieszczania urządzeń (odległości),
- nieprzestrzeganie zasad rozwijania linii kablowych (światłowodowych, itd.).

W tym przypadku zauważyć można (tabela 4.2.5) brak jednoznacznych rozstrzygnięć, które związane są z rozłożeniem opinii pomiędzy dużym a średnim poziomem zagrożenia (pomiędzy 30 a 40 % respondentów). Choć w opinii ekspertów i wielu specjalistów[140] zajmujących się problematyką niekontrolowanego ulotu informacji w polowych sieciach telekomunikacyjnych, które rozwijane są z reguły poza dużymi skupiskami ludzkimi (obszarach poza miejskich), ten czynnik nie odgrywa tak dużego znaczenia jak dla systemów stacjonarnych. Można w tym przypadku posiłkować się choćby przykładem dyslokacji obiektów Sztabu Generalnego, gdzie w gruncie rzeczy brak jest fizycznych możliwości zapewnienia stref bezpieczeństwa o niższych niż maksymalne rygorach.

[140] Patrz - załącznik nr 4

Tabela 4.2.5.

Zagrożenia bezpieczeństwa informacji w obszarze ochrony przed emisją ujawniającą

Zagrożenia dla bezpieczeństwa informacji	Stopień prawdopodobieństwa wystąpienia zagrożenia				
	Bliskie jedności	Duże	Średnie	Małe	Bliskie zeru
Techniczne – emisja ujawniająca:					
- stosowanie w systemie niezbadanych urządzeń komercyjnych	**8,57**	**37,14**	**31,43**	**17,14**	**5,71**
- brak strefy (obszaru kontrolowanego)	**8,57**	**37,14**	**37,14**	**11,43**	**5,71**
- nie przestrzeganie zasad rozmieszczania urządzeń (odległości)	**8,57**	**37,14**	**28,57**	**22,86**	**2,86**
- nieprzestrzeganie zasad rozwijania linii kablowych (światłowodowych, itd.)	**2,86**	**40,00**	**34,29**	**17,14**	**5,71**

Źródło: opracowanie własne na podstawie wyników badań metodą sondażu diagnostycznego techniką ankiety – załącznik nr 4

Następna płaszczyzna w obszarze technicznym, w ramach której może lub występuje potencjalne prawdopodobieństwo utraty bezpieczeństwa informacji, to zagrożenia programowe. W pierwszej chwili kojarzą się one raczej z bezpieczeństwem systemów informatycznych. Jednak tego typu skojarzenie jest mylne, bowiem współczesne urządzenia telekomunikacyjne w swojej strukturze wewnętrznej czy funkcjonalnej bazują na rozwiązaniach informatycznych. Nowoczesne centrale telefoniczne, urządzenia komutacyjne lub transmisyjne bez wątpienia można nazwać minikomputerami, w których prawidłowo funkcjonujące oprogramowanie stanowi o niezakłóconym działaniu centrali, czy innego urządzenia telekomunikacyjnego. W ramach tej płaszczyzny zagrożeń jako szczegółowe w tym obszarze w ankiecie zostały przyjęte:

- brak procedur uwierzytelniania;
- łatwość dostępu do zasobów systemu (uprawnienia);
- możliwość instalacji prywatnego oprogramowania;

– możliwość wprowadzania nieautoryzowanych zmian w treści informacji (konfiguracji systemu);
– nieszyfrowanie informacji na nośnikach elektronicznych;
– słabe zabezpieczenia przed oprogramowaniem złośliwym;
– błędy użytkowników (celowe i niecelowe);
– błędy personelu technicznego (celowe i niecelowe).

Opinie i zdania wyrażone przez respondentów przedstawione zostały w tabeli 4.2.6.

Tabela 4.2.6

Zagrożenia bezpieczeństwa informacji w obszarze ochrony przed złośliwym oprogramowaniem

Zagrożenia dla bezpieczeństwa informacji	Stopień prawdopodobieństwa wystąpienia zagrożenia				
	Bliskie jedności	Duże	Średnie	Małe	Bliskie zeru
Techniczne – programowe:					
- brak procedur uwierzytelniania	**14,29**	**45,71**	**31,43**	**8,57**	**0,00**
- łatwość dostępu do zasobów systemu (uprawnienia)	**5,71**	**60,00**	**25,71**	**8,57**	**0,00**
- możliwość instalacji prywatnego oprogramowania	**8,57**	**31,43**	**37,14**	**20,00**	**2,86**
- możliwość wprowadzania nieautoryzowanych zmian w treści informacji (konfiguracji systemu)	**11,43**	**42,86**	**37,14**	**8,57**	**0,00**
- nie szyfrowanie informacji na nośnikach elektronicznych	**5,71**	**34,29**	**37,14**	**20,00**	**2,86**
- słabe zabezpieczenia przed oprogramowaniem złośliwym	**14,29**	**51,43**	**28,57**	**5,71**	**0,00**
- błędy użytkowników (celowe i niecelowe)	**8,57**	**31,43**	**45,71**	**14,29**	**0,00**
- błędy personelu technicznego (celowe i niecelowe)	**2,86**	**37,14**	**45,71**	**14,29**	**0,00**

Źródło: opracowanie własne na podstawie wyników badań metodą sondażu diagnostycznego techniką ankiety – załącznik nr 4

Jak dotychczas po raz pierwszy tak znaczna liczba ankietowanych - 60% stwierdziła jednomyślnie, że najważniejszym zagrożeniem w tej płaszczyźnie jest łatwość dostępu do zasobów informacyjnych systemu.

Innymi słowy mowa tutaj jest o urządzeniach końcowych za pośrednictwem, których realizuje się wymianę informacji niejawnych oraz tych elementów urządzeń i infrastruktury telekomunikacyjnej umożliwiających dostęp do informacji podlegających ochronie. Problemu tego nie można jednak rozpatrywać samodzielnie i w oderwaniu od systemu nadawania uprawnień poszczególnym osobom funkcyjnym nazywanym „uprawnionymi użytkownikami systemu" oraz związanych z tym ściśle procedur uwierzytelniania, które zapewniają dostęp do zasobów systemu na zasadzie wiedzy koniecznej (*ang. need to know*).

Drugim, według respondentów, istotnym zagrożeniem w zakresie bezpieczeństwa oprogramowania (51,43 %) jest brak lub słabość zabezpieczeń przed implementacją tzw. oprogramowania złośliwego. Pod pojęciem należy rozumieć wirusy, robaki, bomby logiczne, konie trojańskie, itd., których wprowadzenie do oprogramowania systemowego lub użytkowego sieci z jednej strony może przyczynić się do odmowy dostępu do zasobów informacyjnych uprawnionym do nich użytkownikom, z drugiej zaś może wpłynąć na prawidłowość funkcjonowania całego systemu lub sieci. Ze względu na ogólną dużą wiedzę na tamat tego zagadnienia, dostępną w literaturze przedmiotu[141] nie będzie ono dalej rozwijane.

Kolejnym zagrożeniem, na które zwrócili uwagę respondenci w ankiecie był brak stosownych zabezpieczeń uniemożliwiających wprowadzanie nieautoryzowanych (nieuprawnionych) zmian w treści przekazywanych informacji lub oprogramowaniu systemowym pozwalającym nawet na zmianę konfiguracji systemu (42,86 %).

Na niższym bo średnim poziomie etatowy personel bezpieczeństwa łączności i informatyki ocenił prawdopodobieństwo wystąpienia zagrożeń, które są następstwem celowych i nie celowych błędów popełnianych przez użytkowników oraz personel techniczny (45,71 %).

---

[141] m.in.J. Stokłosa, Bezpieczeństwo danych w systemach informatycznych, PWN, Warszawa-Poznań 2001, s. 33-34, R. Anderson, Securing the US Defense Information Infrastructure, RAND, Washington 1999, s. 17-25

Kolejna płaszczyzna zagrożeń dla bezpieczeństwa informacji w obszarze technicznym, poddana pod rozwagę respondentów obejmowała zagrożenia związane z procesem przesyłania informacji, zwane inaczej zagrożeniami wpływającymi na bezpieczeństwo transmisji sygnału użytecznego. W płaszczyźnie tej do zagrożeń szczegółowych (tabela 4.2.7.) w ramach badania ankietowego zaliczono:

- nieautoryzowany przechwyt informacji realizowany przez siły i środki rozpoznania radioelektronicznego lub inne wyspecjalizowane agendy przeciwnika;
- celowe i niecelowe zakłócanie informacji, tzn. przedsięwzięcia wchodzące w skład walki radioelektronicznej, ale i zakłócanie wynikające z propagacji fal radiowych oraz innych źródeł np.: przemysłowych;
- interferencja jako nakładanie się fal radiowych przy złym doborze zakresów częstotliwości;
- możliwość prowadzenia analizy ruchu telekomunikacyjnego, ilości korespondentów, okresów nasilenia wymiany informacji, zajętości pasma, kanału, itd.;

Tabela 4.2.7.

Zagrożenia bezpieczeństwa informacji w obszarze transmisji informacji

Zagrożenia dla bezpieczeństwa informacji	Stopień prawdopodobieństwa wystąpienia zagrożenia				
	Bliskie jedności	Duże	Średnie	Małe	Bliskie zeru
Techniczne – transmisyjne:					
- nieautoryzowany przechwyt informacji	11,43	37,14	37,14	14,29	0,00
- celowe i niecelowe zakłócanie informacji	2,86	34,29	42,86	20,00	0,00
- interferencja	2,86	22,86	40,00	28,57	5,71
- możliwość prowadzenia analizy ruchu telekomunikacyjnego	5,71	31,43	28,57	31,43	2,86
- podszywanie się pod uprawnionego użytkownika	14,29	28,57	22,86	20,00	14,29

Źródło: opracowanie własne na podstawie wyników badań metodą sondażu diagnostycznego techniką ankiety – załącznik nr 4

– podszywanie się np.: jako użytkownicy celem pozyskania informacji lub ewentualnego wprowadzenia w błąd (dezinformacja).

Zagrożenia dla bezpieczeństwa informacji w procesie jej transmisji nabierają szczególnego znaczenia w wojskowych polowych systemach i sieciach telekomunikacyjnych ze względu na fakt, że podlegająca ochronie informacja, która po opuszczeniu źródła nadawania przyjmuje postać fali elektromagnetycznej (linia radiowa, radioliniowa, satelitarna), sygnału elektrycznego (linia kablowa) czy sygnału świetlnego (linia światłowodowa) narażona jest na oddziaływanie szeregu nieprzyjaznych czynników, na które my jako jej użytkownicy nie mamy fizycznego wpływu. Natomiast z punktu widzenia potencjalnego przeciwnika ten moment jest najdogodniejszy dla pozyskania informacji, ewentualnego jej zakłócenia czy też prowadzenia działań dezinformacyjnych.

Jednak uzyskane w tej materii wyniki, które zawarte są w tabeli 4.2.7, nie zdają się tego stanowiska potwierdzać. Brak jest bowiem jednoznacznego stanowiska wskazującego na duży poziom istotności i prawdopodobieństwa wystąpienia przytoczonych zagrożeń. Przeciętnie tylko około 1/3 respondentów uważa, że wymienione zagrożenia szczegółowe wpływają poważnie (w dużym stopniu) na bezpieczeństwo informacji w sieci telekomunikacyjnej. Podobna populacja ankietowanych traktuje je jako zagrożenia na poziomie średnim.

Ostatnią płaszczyzną poddaną osądowi pracowników organów bezpieczeństwa łączności i informatyki szczebla taktycznego w obszarze technicznym były zagrożenia wynikające z zastosowania lub braku urządzeń wchodzących w skład tzw. systemów wsparcia technicznego. W jej ramach dla celów badania ankietowego opracowano, a następnie przedstawiono pod rozwagę respondentów niżej wymienione zagrożenia szczegółowe (tabela 4.2.8):

– brak lub niewłaściwie zorganizowany system kontroli wejścia, wyjścia;
– brak lub nieadekwatny system antywłamaniowy, ppoż.;
– brak lub niewłaściwy system zasilania awaryjnego;
– inne systemy zabezpieczające funkcjonowanie systemu telekomunikacyjnego.

Tabela 4.2.8

Zagrożenia bezpieczeństwa informacji w obszarze wsparcia technicznego

Zagrożenia dla bezpieczeństwa informacji	Stopień prawdopodobieństwa wystąpienia zagrożenia				
	Bliskie jedności	Duże	Średnie	Małe	Bliskie zeru
Techniczne – wsparcie techniczne:					
- brak lub niewłaściwie zorganizowany system kontroli wejścia, wyjścia	**5,71**	**31,43**	**45,71**	**14,29**	**2,86**
- brak lub nieadekwatny system antywłamaniowy, ppoż.	**2,86**	**17,14**	**28,57**	**40,00**	**5,71**
- brak lub niewłaściwy system zasilania awaryjnego	**8,57**	**22,86**	**40,00**	**28,57**	**5,71**
- inne systemy zabezpieczające funkcjonowanie systemu telekomunikacyjnego	**2,86**	**11,43**	**42,86**	**40,00**	**2,86**

Źródło: opracowanie własne na podstawie wyników badań metodą sondażu diagnostycznego techniką ankiety – załącznik nr 4

Po analizie uzyskanych z przeprowadzonego badania ankietowego wyników, można stwierdzić, że prawdopodobieństwo zaistnienia zagrożeń w tej płaszczyźnie traktowane jest przez respondentów z większą pobłażliwością niż większość pozostałych i oceniana na poziomie małym lub średnim.

Podsumowując dotychczasowe rozważania w zakresie zagrożeń bezpieczeństwa informacji w wojskowych sieciach telekomunikacyjnych oraz weryfikując je z uzyskanymi w ramach sondażu diagnostycznego techniką ankiety wynikami, nie można jednoznacznie powiedzieć, że jedna lub druga grupa w przyjętych na potrzeby dysertacji obszarach zagrożeń jest w sposób ewidentny istotniejsza od pozostałych. Potwierdzeniem tej tezy są opinie wyrażone w ramach ankiety przez respondentów. Znakomita większość (blisko 70 %) pracowników pionów bezpieczeństwa łączności i informatyki szczebla taktycznego stwierdziła bowiem, że przytoczone w poszczególnych obszarach zagrożenia wpływają w dużym lub średnim stopniu na poziom bezpieczeństwa informacji w wojskowych polowych sieciach telekomunikacyjnych. Wniosek ten

wypływa z uśrednienia wyników (tabela 4.2.9) uzyskanych w ramach przeprowadzonego sondażu metodą ankiety.

Tabela 4.2.9

Uśrednione wyniki sondażu diagnostycznego techniką ankiety w rozpatrywanych obszarach zagrożeń

Zagrożenia dla bezpieczeństwa informacji	Stopień prawdopodobieństwa wystąpienia zagrożenia				
	Bliskie jedności	Duże	Średnie	Małe	Bliskie zeru
Typ (rodzaj) zagrożenia:					
Personalne	7,14	23,57	28,57	27,14	16,07
Fizyczne	7,86	26,40	30,00	25,72	9,29
Organizacyjno-proceduralne	10,00	45,00	29,29	15,00	0,71
Techniczne	8,56	34,67	30,22	19,22	5,34
- kryptograficzne	14,29	42,14	18,57	12,86	12,14
- emisja ujawniająca	7,14	37,86	32,86	17,14	5,00
- programowe	8,93	41,79	36,07	12,50	0,72
- transmisyjne	7,43	30,86	34,29	22,86	4,57
- wsparcie techniczne	5,00	20,72	39,29	30,72	4,29
Średnia arytmetyczna [%]	8,48	33,67	31,02	20,35	6,48

Źródło: opracowanie własne na podstawie wyników badań metodą sondażu diagnostycznego techniką ankiety – załącznik nr 4

Aby dokonać pełniejszej weryfikacji tak sformułowanej tezy, ponownie stosując metodę sondażu diagnostycznego, ale tym razem techniką wywiadu (arkusz wywiadu – załącznik nr 5), zwrócono się z identycznym pytaniem do pracowników organów bezpieczeństwa łączności i informatyki, którzy z racji wieloletnich doświadczeń w dziedzinie bezpieczeństwa łączności i informatyki oraz pełnionych funkcji uprawniających ich do posiadania w tej materii stosownej wiedzy można nazwać ekspertami. Mowa jest bowiem o Panach – płk. M. Sobczaku oraz płk. A. Dańczaku.

Obaj wymienieni eksperci potwierdzili, że czynnikami determinującymi poziom zagrożeń czy nawet możliwość ich wystąpienia są architektura i przeznaczenie samego systemu oraz warunki i otoczenie, w którym system ten funkcjonuje. Jednocześnie stwierdzili, że głównym czynnikiem stanowiącym o podjęciu działań, przedsięwzięć czy środków bezpieczeństwa w celu ochrony informacji w systemie są przyjmowane kryteria istotności zagrożeń, które w czasie funkcjonowania systemu mogą na niego wpływać. Odpowiadając na pytanie, które z zagrożeń dla bezpieczeństwa informacji w polowych systemach telekomunikacyjnych są ich zdaniem najważniejsze, bez wahania jednogłośnie stwierdzili, że najsłabszym ogniwem w całym systemie ochrony i bezpieczeństwa informacji bez względu na typ i przeznaczenie systemu lub sieci jest człowiek. Dopiero bezpośrednio po nim jako kolejne należy rozpatrywać wszelkiego
rodzaju zagrożenia wchodzące w skład szeroko rozumianych zagrożeń organizacyjno-proceduralnych, fizycznych czy technicznych, które wcześniej zostały omówione.

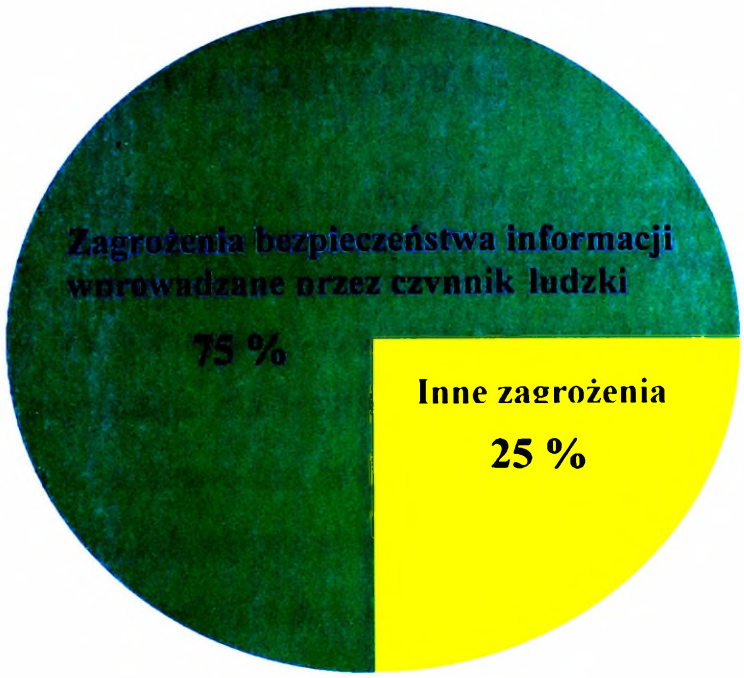
Stanowisko cytowanych oficerów potwierdzają badania przeprowadzone przez przedstawicieli amerykańskiego świata nauki[142], którzy stwierdzili, że zagrożenia związane bezpieczeństwa informacji i powstanie różnych problemów w systemach telekomunikacyjnych lub informatycznych stwarza nieuczciwy bądź niezadowolony personel (rys. 4.2.1).

Choć prowadzone przez nich badania obejmowały przede wszystkim systemy komercyjne (cywilne oraz rządowe) i dotyczyły raczej zdarzeń o podłożu kryminalnym nie zmienia znaczenia w kwestii zasadniczej fakt, że około 75% problemów i zagrożeń stanowi właśnie człowiek.

Po zebraniu dotychczasowych danych, które uzyskano w ramach prowadzonych badań oraz informacji będących wynikiem prac badawczych innych osób, można dokonać uogólnienia, dotyczącego przypisania poszczególnym rozważanym obszarom zagrożeń stopnia istotności (gradacji) w odniesieniu do ich wpływu na wymagany poziom bezpieczeństwa informacji w polowej sieci telekomunikacyjnej.

---

[142] D Icove., K Seger., von Storch, A Crimefighter Handbook, O'Reilly&Associates, Arkansas 1991, s. 123



Rys.4.2.1 Statystyka zagrożeń wg poglądów Icove D., Seger K., von Storch.
Źródło: A Crimefighter Handbook, O'Reilly&Associates, Arkansas 1991, s. 123

Wspomniane rezultaty badawcze pozwalają rozważanym obszarom zagrożeń przydzielić następującą kolejność:

1. Zagrożenia personalne,
2. Zagrożenia organizacyjno-proceduralne,
3. Zagrożenia techniczne,
4. Zagrożenia fizyczne.

Ze względu na występowanie szeregu płaszczyzn w obszarze zagrożeń technicznych zostanie, on podobnie jak w trakcie badań potraktowany indywidualnie i poszczególnym płaszczyznom przydzielona następująca kolejność:

1. Zagrożenia kryptograficzne;
2. Zagrożenia programowe;
3. Zagrożenia wynikające z emisji ujawniającej;
4. Zagrożenia transmisyjne;
5. Zagrożenia dla wsparcia technicznego.

Uzyskane wyniki będą stanowić również podstawę do określenia zagrożeń istotnych dla bezpieczeństwa informacji w rozpatrywanej sieci teletransmisyjnej dywizji zmechanizowanej.

4.3. IDENTYFIKACJA ZAGROŻEŃ DLA SIECI TELETRANSMISYJNEJ DYWIZJI ZMECHANIZOWANEJ

Z dotychczasowych rozważań na temat sieci teletransmisyjnej dywizji zmechanizowanej wiemy, że stanowi ona integralny element sieci telekomunikacyjnej związku taktycznego. Przy tak sformułowanym założeniu można wyprowadzić twierdzenie wprost, że każde zagrożenie dla bezpieczeństwa informacji w sieci teletransmisyjnej stanowi adekwatne zagrożenie dla bezpieczeństwa informacji w sieci telekomunikacyjnej i odwrotnie. Ten tok rozumowania, uprawnia ono do stwierdzenia, iż definiowane i omawiane do tej pory obszary i płaszczyzny zagrożeń odnoszą się również do sieci teletransmisyjnej.

W tej sytuacji identyfikacja zagrożeń w sieci teletransmisyjnej dywizji zmechanizowanej odbywać się będzie wśród obszarów już znanych i uprzednio omówionych w podrozdziałach 4.1 i 4.2.

Znając zatem problematykę zagrożeń i obszarów oraz płaszczyzn, w których z pewnym prawdopodobieństwem mogą one wystąpić stosowne wydaje się przypomnieć podstawowe informacje o poddawanej ocenie sieci teletransmisyjnej - jej strukturze i organizacji. W tym celu należy odnieść się do przyjętej struktury organizacyjnej rozpatrywanej sieci teletransmisyjnej przedstawionej na rysunku 2.3.3 lub bardziej szczegółowej uwzględniającej indywidualną strukturę pomocniczych węzłów łączności – rysunek 2.6.1.

Uzyskane na bazie dotychczasowych rozważań wnioski oraz przyjęte założenia pozwalają stwierdzić, że podstawowymi elementami struktury sieci teletransmisyjnej dywizji zmechanizowanej są linie telekomunikacyjne oraz pomocnicze węzły łączności, które stanowią jednocześnie z punktu widzenia bezpieczeństwa informacji miejsca ewentualnego niekontrolowanego czy nieautoryzowanego „wypływu" podlegającej ochronie informacji.

Pierwszy składnik sieci teletransmisyjnej dywizji zmechanizowanej to linie telekomunikacyjne. Informacja, w zależności od środka transmisyjnego, podczas jej przesyłania przyjmuje formę sygnału elektrycznego, świetlnego, czy fali elektromagnetycznej.

W tym konkretnym przypadku nasuwa się wniosek, że zasadniczym rodzajem zagrożeń dla informacji podczas jej przesyłania są zagrożenia transmisyjne. Zgodnie z wcześniejszymi ustaleniami (dokumenty normatywne NATO) zalicza się do nich:

- nieautoryzowany przechwyt informacji,
- celowe i niecelowe zakłócanie informacji,
- interferencja,
- możliwość prowadzenia analizy ruchu telekomunikacyjnego,
- podszywanie się pod uprawnionego użytkownika.

Jeśli poddamy każde z zagrożeń indywidualnie szczegółowej analizie stwierdzimy, że zarówno celowe bądź niecelowe zakłócanie informacji czy interferencja lub możliwość prowadzenia analizy ruchu telekomunikacyjnego przez potencjalnego przeciwnika, nie ma bezpośredniego przełożenia na bezpieczeństwo informacji. Odnoszą się one raczej do zagrożeń wchodzących w obszar zapewnienia bezpieczeństwa sieci teletransmisyjnej, choć z drugiej strony mają wpływ na spełnienie takich atrybutów bezpieczeństwa informacji, jak dostępność czy niezawodność.

Pozostałym atrybutom tj. poufności, integralności, rozliczalności czy też autentyczności można w tej sytuacji przypisać zagrożenia będące następstwem nieautoryzowanego przechwytu i podszywania się pod uprawnionego użytkownika.

Wszystkie z wymienionych zagrożeń są następstwem prowadzonych przez przeciwnika aktywnych działań radioelektronicznych. Wyjątek może stanowić interferencja, gdyż powstałe zakłócenia mogą pochodzić również od własnych środków transmisyjnych (problematyka propagacji fal elektromagnetycznych). Zakres, moc i aktywność oddziaływania zależna jest od potencjału radioelektronicznego przeciwnika oraz możliwości jego użycia w konkretnych warunkach bojowych, meteorologicznych czy terenowych. Siły i środki walki radioelektronicznej umożliwiają wykonanie różnego rodzaju zadań, szeroko rozumianego rozpoznania i obezwładniania.

Jednak zasadniczym elementem będącym w obszarze zainteresowania jest w tym przypadku możliwość nieautoryzowanego przechwytu informacji, która stanowi integralną część rozpoznania. Przechwyt transmitowanej i podlegającej ochronie informacji może przyczynić się do utraty jej poufności. Znajomość treści przekazywanych w określonych relacjach danych umożliwia przeciwnikowi prowadzenie innych dzia-

łań, do których zaliczyć możemy m.in. dywersję w sieci teletransmisyjnej. Dywersja[143] jest celowym działaniem przeciwnika na zorganizowane systemy radioelektroniczne łączności przewodowej i bezprzewodowej oraz systemy radionawigacyjne, zmierzającym do dezorganizowania dowodzenia wojskami i sterowania środkami rażenia, co zasadniczo wpływa na obniżenie wartości bojowych wojsk własnych. Stanowi szczególną formę celowego i aktywnego oddziaływania na systemy dowodzenia wojskami i kierowania środkami walki. Polega ona między innymi na ciągłym śledzeniu przez przeciwnika wymiany radiowej i włączaniu jego radiostacji w wybrane, ważniejsze relacje radiowe i przekazywaniu w nich rozkazów, zarządzeń, komend, meldunków, komunikatów w celu przekazywania w nich fałszywych treści. Te same możliwości uzyskuje się poprzez „wpięcie" się w dalekosiężną linie kablową. Nieco większe problemy sprawia ta sama czynność w odniesieniu do linii światłowodowych, ale aktualne możliwości techniczne pozwalają, a nawet wręcz wymuszają, uwzględnianie tego typu zagrożenia.

Tak rozumiane pojęcie dywersji wpływa na takie cechy bezpieczeństwa informacji jak integralność, rozliczalność czy w końcu autentyczność.

Drugi z rozpatrywanych składników sieci teletransmisyjnej dywizji zmechanizowanej – pomocniczy węzeł łączności – jest elementem bardziej złożonym niż poprzedni. Z tego powodu jego rozpatrywanie w aspekcie zagrożeń dla bezpieczeństwa informacji musi być dokonane wielopłaszczyznowo.

W składzie podlegającej ocenie sieci teletransmisyjnej występuje sześć pomocniczych węzłów, które choćby ze względu na rodzaj i ilość realizowanych przez nie linii międzywęzłowych oraz dowiązania mają różną strukturę wewnętrzną. W rozdziale drugim, gdzie nastąpiła identyfikacja sieci teletransmisyjnej przyjęto jednak, że podstawowy sprzęt w strukturze pomocniczych węzłów łączności, jak aparatownia transmisyjna i komutacyjna czy aparatownia radiodostępowa jest identyczny. Założenie to pozwala na dokonanie pewnych ograniczeń w procesie identyfikacji zagrożeń bezpieczeństwa informacji w sieci teletransmisyjnej dywizji zmechanizowanej w odniesieniu do pomocniczych węzłów łączności. Przyjmuje się bowiem, że możliwość lub występowanie zagrożenia dla bezpieczeństwa informacji w jednym z pomocniczych węzłów

[143] J. Janczak, „Współczesne koncepcje walki informacyjnej", AON, Warszawa 2002, s. 74

łączności jest odpowiednio adekwatne do prawdopodobieństwa jego zaistnienia w każdym z pozostałych pomocniczych węzłów łączności funkcjonujących w strukturze sieci teletransmisyjnej.

Stąd też podczas dalszej identyfikacji zagrożeń bezpieczeństwa informacji w sieci teletransmisyjnej rozpatrywany będzie jeden z pomocniczych węzłów łączności.

Zgodnie z przyjętym założeniem rozpatrywanie problematyki zagrożeń dla bezpieczeństwa informacji w ramach pomocniczych węzłów łączności sieci teletransmisyjnej dywizji zmechanizowanej przeprowadzone zostanie od identyfikacji zagrożeń personalnych.

W czasie prowadzenia działań taktycznych przez dywizję zmechanizowaną poza wcześniej (podrozdział 3.1, 3.2) wymienionymi zagrożeniami personalnymi należy liczyć się z możliwością dostania się do niewoli personelu technicznego obsługującego poszczególne aparatownie, stacje lub urządzenia pomocniczego węzła łączności, którego wiedza i doświadczenie przekazana przeciwnikowi może ułatwić ominięcie lub złamanie stosowanych zabezpieczeń, co w sposób pośredni przekłada się na bezpieczeństwo informacji podczas dalszej eksploatacji sieci teletransmisyjnej.

Jest to ściśle związane z zagrożeniami organizacyjno-proceduralnymi, gdyż każdy zaistniały incydent lub zdarzenie w czasie prowadzenia walki przez dywizję winien znaleźć swoje odzwierciedlenie we wszelakiego rodzaju procedurach postępowania, a głównie w sytuacjach innych niż standardowe definiując jednocześnie nowe przypadki lub uszczegółowiając obowiązujące dotychczas.

Omawiając obszar zagrożeń technicznych, należy brać pod uwagę, że zagadnienia środków i materiałów kryptograficznych będące przedmiotem pożądania właściwych służb wojsk przeciwnika w okresie pokoju jest tym bardziej obszarem eksploracji podczas konfliktu zbrojnego. Stąd też należy liczyć się ze zdwojonymi wysiłkami pozyskania lub złamania przez przeciwnika stosowanych nie tylko w urządzeniach ochrony kryptograficznej szyfrów i kodów. Zwiększa się tym bardziej możliwość utraty kontroli nad urządzeniami zapewniającymi bezpieczne przesyłanie informacji w sieci teletransmisyjnej lub dokumentów kluczowych, które zapewniają ich prawidłowe funkcjonowanie. Pod pojęciem „utraty kontroli" autor ma na myśli możliwość przejęcia przez wojska przeciwnika konkretnych urządzeń kryptograficznych lub co

gorsza eksploatowanych i dalej funkcjonujących aparatowni, stacji, czy nawet całych pomocniczych węzłów łączności.

Z dotychczasowych rozważań dotyczących problematyki zagrożeń wchodzących w skład emisji ujawniającej wiemy, że przedsięwzięcia eliminujące ten czynnik realizowane są tylko i wyłącznie w specjalistycznych laboratoriach. Niemniej jednak istotne jest, aby personel obsługujący w każdym momencie eksploatacji urządzeń na polu walki, które spełniają określone wymagania i normy w tym zakresie, mógł mieć możliwość potwierdzenia iż te normy dalej są spełniane.

Problematyka zagrożeń programowych ogranicza się tylko do wcześniej już omówionych, ponieważ rozpatrywana sieć teletransmisyjna traktowana jest jako sieć dedykowana, która nie posiada galwanicznych połączeń z innymi ogólnodostępnymi systemami i sieciami telekomunikacyjnymi. Stąd też autor, uważając za niecelowe ich powtarzanie odwołuje się do zagrożeń przedstawionych i omówionych w rozdziałach poprzednich.

Rozpatrując zagadnienia związane z zagrożeniami, które wchodzą w skład płaszczyzny wsparcia technicznego, autor w pełni zgadza się z wynikami uzyskanymi w procesie sondażu diagnostycznego metodą ankiety jak również wywiadu. W polowych warunkach rozwijania i funkcjonowania sieci teletransmisyjnej dywizji zmechanizowanej, a tym bardziej podczas prowadzenia działań taktycznych zdefiniowane w tym obszarze zagrożenia są traktowane marginalnie. Zmiana czynników wchodzących w ich skład, szczególnie uwzględniających uwarunkowania współczesnego pola walki winna podnieść ich rangę. Rozważania w tej materii prowadzone będą w następnym rozdziale niniejszej dysertacji.

Ostatnim z wyodrębnionych dotychczas obszarów, który ma wpływ na bezpieczeństwo informacji w strukturze pomocniczego węzła łączności sieci teletransmisyjnej są zagrożenia fizyczne.

Zagrożeń tych nie należy jednak pojmować w tradycyjny sposób i ograniczać ich do spełniających określone wymagania sejfów, drzwi czy też krat, jak ma to miejsce w systemach i sieciach stacjonarnych. Podstawowym elementem determinującym ich występowanie jest realny przeciwnik, określone uwarunkowania i czynniki sił przeciwnika, które wpływają lub mogą wpływać w sposób rzeczywisty na bezpieczeństwo

pomocniczych węzłów łączności sieci teletransmisyjnej dywizji zmechanizowanej i przesyłanej informacji.

Mając na uwadze przytoczone powyżej uwarunkowania należy uznać, że zasadniczym elementem zagrażającym bezpieczeństwu informacji jest bezpośredni celowy lub niezamierzony atak wydzielonych lub dedykowanych sił wojsk przeciwnika na pomocnicze węzły łączności, który z jednej strony może prowadzony być w celu wyeliminowania danego węzła z dalszej eksploatacji w sieci teletransmisyjnej lub jeśli okaże się to możliwe przejęcia części lub całości sprzętu stanowiącego wyposażenie danego pomocniczego węzła łączności. Problem ten jest ściśle związany z zagadnieniem ochrony i obrony wszystkich elementów struktury sieci teletransmisyjnej.

Reasumując prowadzone rozważania w zakresie identyfikacji zagrożeń dla bezpieczeństwa informacji w sieci teletransmisyjnej dywizji zmechanizowanej podczas prowadzenia przez nią działań taktycznych należy wnioskować, że główną ***uwagę zwrócić należy na siły, sposób działania i możliwości oddziaływania na sieć wojsk przeciwnika. Prawidłowe zdefiniowanie wymienionych powyżej czynników jest podstawą uzyskania przez wojska własne sukcesu zarówno w obszarze typowych działań taktycznych jak również przedsięwzięć zapewniających bezpieczeństwo informacji w sieci teletransmisyjnej.***

5. KONCEPCJA PRZEDSIĘWZIĘĆ ORGANIZACYJNO-EKSPLOATACYJNYCH ZAPEWNIAJĄCYCH SPEŁNIENIE WYMAGAŃ BEZPIECZEŃSTWA INFORMACJI W SIECI TELETRANSMISYJNEJ DYWIZJI ZMECHANIZOWANEJ

Zmierzając do osiągnięcia zasadniczego celu rozprawy jakim jest określenie aktualnego poziomu bezpieczeństwa informacji w sieci teletransmisyjnej dywizji zmechanizowanej w czasie prowadzenia działań taktycznych rozdział ten poświęcono szczególnemu działowi polityki bezpieczeństwa, który w następstwie analizy ryzyka pozwala dokonać identyfikacji metod i środków[144] ochrony informacji stosowanych w wojskowych systemach telekomunikacyjnych zarówno narodowych jak i sojuszniczych. Uzyskana w tym zakresie wiedza będzie stanowić podstawę umożliwiającą przeprowadzenie dokładnej analizy tych przedsięwzięć organizacyjno-eksploatacyjnych wchodzących w skład systemu ochrony[145] oraz elementów struktury organizacyjnej sieci, które mają wpływ na bezpieczeństwo informacji w sieci teletransmisyjnej.

Systematyczne i kompleksowe podejście do głównego przedmiotu rozważań przyczyni się do pozytywnej lub negatywnej weryfikacji hipotezy roboczej w kontekście ewentualnego wyeliminowania niekontrolowanego „wypływu" informacji z tej sieci i tym samym podniesienia poziomu ochrony informacji. Pozwoli ponadto stwierdzić, czy istnieje konieczność wprowadzenia nowych przedsięwzięć organizacyjno-eksploatacyjnych w celu utrzymania lub podniesienia poziomu bezpieczeństwa informacji w sieci teletransmisyjnej dywizji, czy też stosowane dotychczas są wystarczające.

Wymienione dotychczas czynności i przedsięwzięcia określone są wieloma dokumentami normatywnymi (m.in. Rozporządzeniem Prezesa Rady Ministrów z dnia 25 lutego 1999 r. w sprawie podstawowych wymagań bezpieczeństwa systemów i sieci teleinformatycznych - Dz.U.Nr 18, poz. 162), na podstawie których można wnio-

---

[144] Środki i metody ochrony to przedsięwzięcia technologiczne i administracyjne, do zabezpieczenia m.in. urządzeń telekomunikacyjnych i danych w celu zapewnienia interesów instytucji i poufności – A. Dańczak, Bezpieczeństwo informacji w SZ RP, op. cit. s. 12

[145] Ochrona to wszelkie działania mające chronić przed zagrożeniami, działaniami szkodliwymi lub niebezpiecznymi – Słownik języka polskiego, PWN, Warszawa 2000

skować, że zasadniczym celem bezpieczeństwa i ochrony informacji w sieciach teletransmisyjnych jest:

- ochrona danych przetwarzanych i przesyłanych w tych systemach;
- zabezpieczenie systemów przed blokowaniem oraz spowalnianiem ich pracy;
- zabezpieczenie przed dezinformacją;
- zabezpieczenie przed dekonspiracją:
  - urządzeń;
  - algorytmów;
  - kluczy i ich procedur zabezpieczających;
- odtwarzanie systemów po awariach i dekonspiracji.

5.1. ŚRODKI OCHRONY INFORMACJI W POLOWYCH WOJSKOWYCH SYSTEMACH TELEKOMUNIKACYJNYCH

W praktyce życia codziennego stosuje się dwa możliwe podejścia do ryzyka: wyprzedzające (nastawione na wczesną identyfikację zagrożeń i ich unikanie) oraz przeciwdziałające (nastawione na wykrywanie i naprawianie szkód).

W procesie planowania, a następnie eksploatacji systemu telekomunikacyjnego lub informatycznego, na etapie analizy ryzyka dla zapewnienia bezpieczeństwa informacji w tym systemie, stosuje się przede wszystkim podejście wyprzedzające.

Analiza ryzyka to systematyczny podział na kategorie zagrożeń danych i środków im przeciwdziałających oraz określenie planu działania, który większość zasobów (technicznych i pozatechnicznych) skieruje przeciw najbardziej prawdopodobnemu ryzyku. Istotną sprawą jest uwzględnianie priorytetów zagrożeń. Analiza ryzyka nie ma na celu stworzenia planu całkowitej ochrony; ma zapewnić stopień bezpieczeństwa proporcjonalny do wagi chronionej informacji.

Do elementów analizy ryzyka należą:

- założone cele,
- zagrożenia, częstość zagrożeń,
- odporność na zagrożenia, stosunek ryzyka do potencjalnych strat,
- ochrona, koszt ochrony,

- koszt analizy,
- implementacja mechanizmów ochrony.

Zasadniczym celem analizy ryzyka jest zatem identyfikacja wszelkich możliwych i mniej lub więcej prawdopodobnych zagrożeń dla informacji w systemie pochodzących ze środowiska wewnętrznego, jak i zewnętrznego. W stosunku do tych zagrożeń dobiera się stosowne środki lub metody ochrony, które umożliwią ich uniknięcie lub minimalizację.

W kolejnym kroku dokonuje się ponownej weryfikacji zagrożeń, gdyż należy mieć świadomość tego, że żadne z urządzeń technicznych lub najlepsze metody organizacyjne w zakresie bezpieczeństwa informacji w systemie telekomunikacyjnym nie zapewniają pełnej tzw. 100% gwarancji bezpieczeństwa systemu telekomunikacyjnego. Taka analiza pozwala na określenie ryzyka szczątkowego, o którym organizator systemu wie i musi się z nim liczyć.

Jednak zawsze na tym etapie dochodzi do swoistego konfliktu – szacowana wartość informacji oraz wymierna wartość nakładów na urządzenia (elementy) systemu telekomunikacyjnego w stosunku do środków finansowych, które planowane są na urządzenia ochrony informacji w systemie.

Stąd też w wielu przypadkach ryzyko graniczne wynika z określonych nakładów finansowych na bezpieczeństwo systemu telekomunikacyjnego, które odnosi się zarówno do strony technicznej (implementacja środków ochrony), jak również strony organizacyjnej (struktura i obsada etatowa organów bezpieczeństwa łączności i informatyki).

Po przeprowadzeniu identyfikacji zagrożeń oraz dokonaniu analizy ryzyka dla bezpieczeństwa informacji w systemie telekomunikacyjnym lub informatycznym jest przedstawienie metod oraz sposobów jej zabezpieczenia przy pomocy organizacyjnych i technicznych środków ochrony.

Zastosowanie metod, jak i środków ochrony informacji w systemie telekomunikacyjnym lub informatycznym, zależne jest od wielu czynników. Uwzględnić bowiem należy strukturę systemu, jego przeznaczenie, rodzaj świadczonych usług telekomunikacyjnych oraz klauzulę przesyłanych w nim informacji. Nie bez znaczenia jest również środowisko zewnętrzne jak i wewnętrzne, w którym dany system ma funkcjono-

wać. Wymienione czynniki mają podstawowe znaczenie przy doborze metod i środków ochrony informacji, co jednak nie oznacza, że w indywidualnych przypadkach nie jest wskazane uwzględnienie innych aspektów mających wpływ na bezpieczeństwo informacji w danym systemie telekomunikacyjnym czy informatycznym.

Zgodnie z przyjętym wcześniej założeniem stosowane środki bezpieczeństwa informacji w systemach telekomunikacyjnych można wyodrębnić i podzielić na następujące płaszczyzny:

- organizacyjno-proceduralne,
- personalne,
- fizyczne,
- techniczne.

Techniczne środki ochrony informacji, przy tak przyjętym podziale, obejmują wyszczególnione poniżej grupy, w skład których wchodzą:

- ochrona kryptograficzna,
- ochrona elektromagnetyczna,
- ochrona programowa,
- ochrona transmisji informacji,
- techniczne wsparcie ochrony fizycznej.

W ramach przedsięwzięć organizacyjno-proceduralnych oraz zgodnie z aktualnie obowiązującymi aktami normatywnymi (ustawa, rozporządzenia Prezesa Rady Ministrów, rozporządzenia Ministra Obrony Narodowej oraz inne) w strukturach sił zbrojnych w zakresie bezpieczeństwa organizacyjno - proceduralnego współdziałają dwa niezależne piony – pełnomocnika ochrony oraz organy bezpieczeństwa łączności i informatyki.

Rozkaz dzienny dowódcy lub kierownika jednostki organizacyjnej jest podstawą dla personelu bezpieczeństwa łączności i informatyki umożliwiającą określenie uprawnień dla poszczególnych użytkowników w zakresie dostępu do niejawnych zasobów informacyjnych systemu telekomunikacyjnego bądź informatycznego. Rozkaz taki powinien określać zakres wiedzy koniecznej (*ang. need to know*) dla danego stanowiska służbowego oraz maksymalną klauzulę informacji, z którą może być zapoznawana dana osoba funkcyjna. Umożliwia to bowiem zarówno w okresie planowania,

czy też eksploatacji systemu, określenie i przydział niezbędnej ilości niejawnych terminali (urządzeń) końcowych, które zabezpieczą zakładany dla systemu dowodzenia obieg informacji.

Innym przedsięwzięciem w zakresie bezpieczeństwa organizacyjno-proceduralnego jest określenie w ramach zajmowanej przez określoną jednostkę organizacyjną resortu Obrony Narodowej infrastruktury tzw. stref bezpieczeństwa i kontroli dostępu do nich. Mowa tutaj o różnego rodzaju systemach przepustkowych – począwszy od standardowych po elektroniczne, które umożliwiają osobom funkcyjnym poruszanie się tylko po tych obszarach lub budynkach, do których posiadają stosowne uprawnienia z racji wykonywanych zadań służbowych.

Aby zachować określone przez dowódcę lub kierownika jednostki organizacyjnej wymagania bezpieczeństwa informacji wspomniany uprzednio system przepustkowy musi stanowić integralną część systemu rejestracji zdarzeń i dostępu do wydzielonych obiektów, stref czy też pomieszczeń przeznaczonych na potrzeby przetwarzania, przechowywania lub przesyłania niejawnych zasobów informacyjnych systemu telekomunikacyjnego bądź informatycznego.

Jako strefę bezpieczeństwa należy traktować obszar, obiekt, fragment budynku, jedno lub kilka pomieszczeń, posiadające ściśle określone, oznaczone i strzeżone granice, w których przechowywane, przetwarzane lub wytwarzane są informacje niejawne o klauzuli „Poufne" lub wyższej. Wejście osób do strefy lub wyjście z niej może nastąpić wyłącznie po okazaniu przepustki, identyfikatora lub po akceptacji przez system kontroli dostępu.

W zależności od sposobu dostępu do informacji niejawnych rozróżnia się następujące strefy bezpieczeństwa:

Strefa bezpieczeństwa klasy I – obszar, w którym przetwarzane i przechowywane są informacje niejawne o klauzuli „Poufne" lub wyższej w taki sposób, że wejście do tego obszaru praktycznie oznacza dostęp do tych informacji.

Strefa bezpieczeństwa klasy II – obszar, w którym wytwarzane, przetwarzane i przechowywane są informacje o klauzuli „Poufne" lub wyższej w taki sposób, że wejście do niego nie jest równoznaczne z dostępem do tych informacji.

W bezpośrednim otoczeniu stref bezpieczeństwa klasy I oraz II , w którym zapewniona jest kontrola ruchu osób i pojazdów znajduje się strefa administracyjna. Przykładowe rozmieszczenie poszczególnych stref bezpieczeństwa z podziałem na klasy przedstawia rysunek nr 5.1.1.



Rys. 5.1.1. Przykładowe rozmieszczenie stref bezpieczeństwa

Źródło: J. Janczak, G. Świdzikowski, Bezpieczeństwo informacji w wojskowym systemie telekomunikacyjnym, AON, Warszawa 2004

W sytuacji, gdy mamy wyznaczone strefy bezpieczeństwa personel bezpieczeństwa łączności i informatyki we współpracy z pełnomocnikiem ochrony winien określić procedury i zasady korzystania z urządzeń końcowych niejawnych systemów telekomunikacyjnych, czy informatycznych rozmieszczonych w strefach bezpieczeństwa.

W strefie bezpieczeństwa klasy I mogą być zatrudnione wyłącznie osoby posiadające poświadczenie bezpieczeństwa osobowego, upoważniające do dostępu do informacji niejawnych o klauzuli odpowiadającej co najmniej klauzuli najwyższej sklasyfikowanej informacji wytwarzanej, przetwarzanej, przechowywanej lub przesyłanej za pomocą technicznych środków łączności bądź informatyki.

Wstęp osób nie będących żołnierzami albo pracownikami komórki organizacyjnej objętej strefą może nastąpić tylko i wyłącznie za zgodą kierownika komórki organizacyjnej (dowódcy) i pod nadzorem upoważnionego przez niego żołnierza lub pracownika wojska, pod warunkiem uprzedniego zabezpieczenia informacji niejawnych w sposób uniemożliwiający przypadkowe ujawnienie ich treści. Dla przykładu może

to być wyłączenie ekranu monitora, zasłonięcie (przykrycie) urządzeń ochrony kryptograficznej, itp. Warunek powyższy dotyczy nie tylko przybyłych interesantów, ale także (na co w praktyce mało zwraca się uwagę) personelu technicznego i sprzątającego.

Mniejsze obostrzenia należy stosować w odniesieniu do strefy bezpieczeństwa klasy II. Zatrudniony w tej strefie personel (żołnierze i pracownicy wojska) oraz personel techniczny i sprzątający zobowiązany jest do posiadania poświadczenia bezpieczeństwa osobowego upoważniającego co najmniej do dostępu do informacji niejawnych oznaczonych klauzulą „Poufne". Zasady wejścia w obręb strefy osób nie będących pracownikami winny być realizowane jak w strefie klasy I.

Kolejnym istotnym czynnikiem gwarantującym wymagany poziom bezpieczeństwa systemu telekomunikacyjnego jest określenie dla użytkowników i personelu technicznego procedur postępowania w przypadku zaistnienia choćby podejrzeń o możliwości ujawnienia informacji, włamania do systemu, podszywania pod uprawnionego użytkownika bądź utraty urządzeń ochrony kryptograficznej (dokumentów kluczowych). Ze względu na fakt, że w tym przypadku istotną rolę odgrywa czas, tryb zgłaszania i postępowania winien być jak najbardziej uproszczony.

Z organizacyjnego punktu widzenia dla bezpieczeństwa informacji w systemie telekomunikacyjnym bardzo ważną rzeczą jest zdefiniowanie sposobu postępowania w przypadkach ekstremalnego funkcjonowania systemu wynikającego z klęsk żywiołowych, ataku terrorystycznego czy zagrożeń będących następstwem prowadzenia walki zbrojnej. Procedury postępowania w tych sytuacjach powinny być jasne i precyzyjnie definiować krok po kroku wszystkie konieczne do zrealizowania przez różne osoby funkcyjne czynności.

Personel techniczny musi być również przygotowany na możliwość awarii poszczególnych urządzeń systemu telekomunikacyjnego (w tym urządzeń ochrony kryptograficznej) czy też awarii zasilania. Przygotowane w tej materii procedury muszą uwzględniać strukturę oraz realizowane przez system zadania (np. ciągłość).

Pojęcie bezpieczeństwa personalnego w potocznym rozumieniu kojarzy się nam z posiadaniem poświadczenia bezpieczeństwa osobowego o klauzuli wymaganej na zajmowanym stanowisku służbowym. Jednak dla bezpieczeństwa informacji w syste-

mie telekomunikacyjnym lub informatycznym jest to warunek konieczny, ale nie wystarczający.

Sam fakt wyznaczenia na dane stanowisko określa zgodnie z zasadą wiedzy koniecznej (*ang. need to know*) zakres lub obszar wiedzy, z którą dana osoba funkcyjna w ramach wykonywanych czynności służbowych winna być zapoznawana.

Podział obowiązków i odpowiedzialności w zakresie zabezpieczenia oraz zasada najniższego poziomu przywilejów powinny być podstawą definiowania stanowiska pracy w zakresie określania poziomu dostępu do niejawnych aktywów systemu telekomunikacyjnego. Zgodnie z zasadą podziału, pojedynczy użytkownik lub pracownik pionu technicznego nie może samodzielnie realizować krytycznych, z punktu widzenia systemu telekomunikacyjnego (informatycznego), procesów. Ponadto mając na uwadze zasadę najniższego poziomu przywilejów, użytkownik nie powinien mieć przywilejów większych niż niezbędne do wypełnienia swoich obowiązków.

Przy definiowaniu przywilejów należy zwrócić uwagę na efektywność pracy grup użytkowników (możliwości zastępowania nieobecnych) oraz możliwości działania w sytuacjach awaryjnych i katastrofalnych (np. warunkowe przydzielenie przywilejów). Na podstawie definicji stanowisk należy określić ich znaczenie dla bezpieczeństwa systemu oraz sklasyfikować je. W zależności od znaczenia stanowiska mogą być przyjęte specjalne wymagania w zakresie rekrutacji pracowników.

Procedura zakończenia użytkowania lub korzystania z niejawnych zasobów systemu telekomunikacyjnego i informatycznego powinna być częścią standardowego zestawu działań kończących zatrudnienie pracownika, jednakże charakter tego zwolnienia może w istotny sposób wpływać na bezpieczeństwo systemu informacyjnego.

W każdym przypadku zwalniany żołnierz lub pracownik wojska powinien przekazać wszelkie informacje o aktywach systemu będących w jego dyspozycji (np. w postaci dokumentacji elektronicznej, struktury katalogów, lokalizacji kopii bezpieczeństwa itp.). Ponadto, powinien udostępnić inne elementy systemu zabezpieczenia, takie jak hasła dostępowe, tokeny uwierzytelnienia czy klucze kryptograficzne.

Wraz ze zwolnieniem pracownika powinno być również zamknięte jego konto jako użytkownika systemu. Jeśli zachodzi uzasadnione podejrzenie, że zwalniany (np. dyscyplinarnie) żołnierz lub pracownik wojska dysponuje narzędziami lub informa-

cjami, które może wykorzystać w celu naruszenia zabezpieczenia systemu telekomunikacyjnego, to należy zminimalizować prawdopodobieństwo zaistnienia tego zagrożenia. Działania sprawdzające powinny obejmować wszystkie aktywa systemu (urządzenia, aplikacje, oprogramowanie, dane, kopie bezpieczeństwa itp.), do których osoba ta miała dostęp.

Korzystanie w ramach przysługujących kompetencji z zasobów informacyjnych systemu telekomunikacyjnego lub informatycznego wymaga zapoznania się z obowiązującymi w danej jednostce organizacyjnej przepisami, wytycznymi oraz przyjętymi procedurami, które opisano w poprzednim podrozdziale.

Organy bezpieczeństwa łączności i informatyki poszczególnych szczebli dowodzenia we współpracy z pełnomocnikiem ochrony zobowiązane są do prowadzenia w tym zakresie systematycznego szkolenia całego podległego stanu osobowego.

Użytkownicy systemu telekomunikacyjnego lub informatycznego powinni uzyskać odpowiednie informacje dotyczące jego zabezpieczenia. W zależności od zakresu oraz kategorii użytkowników, informacje te mogą być przekazywane na trzech poziomach:

- uświadamiania,
- szkolenia,
- edukacji.

Programy uświadamiania i szkolenia oraz edukacji użytkowników systemu powinny uwzględniać zróżnicowane potrzeby w zakresie znajomości zabezpieczenia użytkowanych systemów telekomunikacyjnych i informatycznych.

Uświadomienie pracowników w zakresie zabezpieczenia systemów obejmuje przede wszystkim przedstawienie celów polityki zabezpieczeń prowadzonej w instytucji oraz pokazanie, w jaki sposób przyczynia się ona do realizacji celów działalności i ochrony aktywów danej jednostki organizacyjnej resortu obrony narodowej oraz doprowadzenie do całkowitego zrozumienia wytycznych w zakresie zabezpieczenia funkcjonujących (eksploatowanych) systemów.

Celem szkolenia jest przekazanie pracownikom umiejętności, które sprawią, że będą oni wykonywali swe zadania zgodnie z procedurami określonymi w polityce zabezpieczenia systemu telekomunikacyjnego lub informatycznego. Aby szkolenie było

efektywne, powinno być zorientowane na poszczególne kategorie odbiorców. Podstawowymi kategoriami są użytkownicy wymagający szkolenia ogólnego oraz część personelu, która potrzebuje szkolenia specjalizowanego lub zaawansowanych umiejętności.

Celem szkolenia ogólnego jest wpojenie pracownikom zasad odpowiedniego postępowania z zasobami systemów łączności i informatyki, a w szczególności:

- zasad ochrony informacji stanowiącej tajemnicę państwową oraz służbową w myśl ustawy „O ochronie informacji niejawnych" i aktów wykonawczych do niej;
- fizycznego zabezpieczenia pomieszczeń oraz zasobów systemu (np. pomieszczenia urządzeń końcowych, stacji łączności kryptograficznej, itp.);
- ochrony haseł lub innych środków uwierzytelnienia (np. kart magnetycznych), umożliwiających dostęp do zasobów systemu;
- przekazywania informacji o dostrzeżonych anomaliach działania systemu, które mogą być efektem naruszenia systemu zabezpieczenia.

Szkolenie specjalistyczne może dotyczyć kierownictwa (obejmować np.: umiejętność szacowania ryzyka) lub administratorów, którzy muszą umieć instalować dane mechanizmy zabezpieczeń.

Edukacja sięga głębiej niż szkolenie i jest skierowana do osób funkcyjnych zawodowo zajmujących się zabezpieczeniami systemów telekomunikacyjnych oraz informatycznych. Ta działalność przeważnie nie znajduje się w zakresie programów szkoleniowo-uświadamiających, a jedynie stanowi element doskonalenia zawodowego personelu organów bezpieczeństwa łączności i informatyki. Procesy uświadamiania i szkolenia oraz edukacji w zakresie zabezpieczenia powinny mieć charakter ciągły.

Ogólnie rzecz ujmując wymagany poziom bezpieczeństwa personalnego można osiągnąć poprzez spełnienie następujących zasad:

1. Właściwy system doboru kadr zgodny z określoną procedurą, wymaganymi i posiadanymi kwalifikacjami, określonymi i posiadanymi cechami psychofizycznymi.
2. Stabilność kadr poprzez prowadzenie właściwej polityki kadrowej.

3. Wysoki poziom w ramach organizowanych centralnie w ośrodkach szkoleń oraz wewnętrznego szkolenia doskonalącego kadry i pracowników wojska, w oparciu o systematycznie aktualizowane programy szkolenia uwzględniające ciągły rozwój i postęp techniczny.
4. Okresowe sprawdzanie umiejętności i bieżące egzekwowanie wysokiego poziomu umiejętności fachowych kadry i pracowników wojska.

Każdy system telekomunikacyjny lub informatyczny, a szczególnie jego urządzenia transmisyjne, komutacyjne, końcowe czy ochrony informacji instalowane są w uprzednio przygotowanych obiektach, budynkach, pomieszczeniach lub pojazdach mechanicznych zwanych dalej infrastrukturą telekomunikacyjną.

Naturalnym przedsięwzięciem jest ich montaż, szczególnie tych elementów, które decydują o prawidłowym i niezakłóconym toku pracy (wrażliwych), w wydzielonych obszarach lub strefach. Miejsca te, szczególnie w odniesieniu do systemów wytwarzających, przetwarzających, przechowujących lub przesyłających informacje niejawne muszą być chronione za pomocą **środków zabezpieczenia fizycznego**.

Przy podejmowaniu decyzji w zakresie zastosowania odpowiedniego stopnia zabezpieczeń pochodzących z grupy środków ochrony fizycznej należy brać pod uwagę takie uwarunkowania, jak:

- stopień tajności i kategoria chronionych w systemie informacji;
- liczba informacji i ich forma (urządzenia końcowe, wydruki komputerowe, elektroniczne nośniki informacji);
- upoważnienia wydane personelowi przez stosowne władze bezpieczeństwa, zezwalające na dostęp do informacji niejawnych i powody, dla których osoby te powinny być dopuszczone do tajemnicy, zgodnie z nadrzędną zasadą wiedzy koniecznej;
- ocena zagrożeń ze strony służb wywiadowczych podejmujących działania wymierzone przeciwko siłom zbrojnym RP, aktów sabotażu i terroryzmu oraz innych działań o charakterze antypaństwowym lub kryminalnym.

Zasadniczym zadaniem i celem stosowania środków ochrony fizycznej jest zabezpieczenie urządzeń i niejawnych aktywów systemu telekomunikacyjnego lub informatycznego zarówno w godzinach służbowych jak i po pracy w zakresie:

- nieuprawnionego potajemnego lub z użyciem siły wejścia osób na teren objęty ochroną;
- odstraszenia nielojalnych członków personelu, w tym osób działających na zlecenie obcych wywiadów (szpieg „od wewnątrz"), ich wykrywanie i tym samym uniemożliwienie pozyskania informacji niejawnych;
- możliwości grupowania pracowników w celu wdrożenia zasady ograniczonego dostępu do informacji niejawnych, czyli udostępniania ich jedynie osobom, którym informacje te są niezbędne do wykonania powierzonej pracy i jedynie w takim zakresie, jaki jest konieczny do wypełnienia obowiązków służbowych.

Skala stosowanych środków bezpieczeństwa fizycznego jest zależna przede wszystkim od klauzuli tajności informacji, do której wytwarzania, przetwarzania, przechowywania lub przesyłania dany system telekomunikacyjny (informatyczny) jest przeznaczony.

W dedykowanych systemach telekomunikacyjnych i informatycznych przekazywane informacje na potrzeby dowodzenia i kierowania wojskami czy sterowania środkami rażenia opatrzone są klauzulami stanowiącymi tajemnicę państwową i służbową.

Z tej przyczyny ich instalacja i funkcjonowanie może być realizowane tylko i wyłącznie w infrastrukturze telekomunikacyjnej znajdującej się lub stanowiącej strefę bezpieczeństwa klasy I bądź II w zależności od różnych uwarunkowań (np. struktura budynku lub kontenera na pojeździe) oraz przeznaczenia i zadań systemu. Strefa bezpieczeństwa poszczególnych klas bezpieczeństwa wyznaczana jest rozkazem organizacyjnym określonego szczebla dowodzenia.

Strefy bezpieczeństwa przeznaczone do wytwarzania, przetwarzania, przechowywania lub przesyłania niejawnych informacji mogą być chronione następującymi środkami:

- służba wartownicza;
- sejfy, szafy pancerne i skarbce;
- drzwi i zamki;
- okna i kraty.

Stanowią one najlepszy sposób ochrony, a więc zapewniają przeciwdziałanie aktom sabotażu i stanowią środki ochrony przed szkodą wyrządzoną w sposób celowy i złośliwy. Środków tych nie zastąpią same procedury sprawdzania personelu.

Szczegółowe zasady i wymagania w zakresie implementacji poszczególnych środków bezpieczeństwa fizycznego w systemach teleinformacyjnych zawarte są w dyrektywie DBBT – 301A „Wytyczne w zakresie bezpieczeństwa fizycznego kancelarii kryptograficznych, stacji łączności kryptograficznej oraz pomieszczeń wydzielonych, przeznaczonych do przetwarzania informacji niejawnej", która dostępna jest w organach bezpieczeństwa łączności i informatyki sił zbrojnych RP.

Gdy do zapewnienia nienaruszalności stref bezpieczeństwa, chroniących przed dostępem do „wrażliwych" urządzeń systemu telekomunikacyjnego bądź bezpośrednio do informacji niejawnych wykorzystywana jest **służba wartownicza**, to osoby pełniące te obowiązki muszą być wcześniej sprawdzone w trybie stosownej procedury, a następnie odbyć przeszkolenie w celu zdobycia wymaganych kwalifikacji. Ochrona obiektów i stref realizowana przez służbę wartowniczą powinna być stale nadzorowana.

Strefy bezpieczeństwa klasy I i II należy patrolować poza ustawowymi godzinami pracy i w dni wolne, w odstępach czasu określonych w planie ochrony danej jednostki organizacyjnej, stosownie do poziomu możliwych do wystąpienia zagrożeń. Patrole muszą zapewnić, że niejawne systemy telekomunikacyjne lub informatyczne są właściwie chronione, i zapobiegać wszelkim incydentom, które mogłyby zagrozić ich bezpieczeństwu.

Aby usprawnić ochronę obiektu i zapewnić kontrolę miejsc najściślej strzeżonych, do których wartownicy nie są dopuszczani, w celu wykrycia prób wtargnięcia na chroniony obszar należy zainstalować kamery telewizji przemysłowej działającej w systemie zamkniętym, urządzenia alarmowe lub punkty nadzoru wizualnego. Pierwszy z wymienionych środków zabezpieczenia może być stosowany zamiast patrolowania strefy chronionej.

Ze składu warty lub pododdziału alarmowego należy wydzielić zespoły szybkiego reagowania. Wskazane jest, aby w razie alarmu możliwe było skierowanie co najmniej dwóch wartowników do miejsc, gdzie doszło do zagrożenia bezpieczeństwa.

Działanie zespołu nie może wpłynąć na osłabienie ochrony innych rejonów strzeżonego obszaru. Należy systematycznie sprawdzać czas reagowania służby wartowniczej (pododdziału alarmowego) na sygnały alarmowe i sytuacje zagrożenia. Ich reakcja musi być na tyle szybka, aby przeszkodzić każdemu potencjalnemu intruzowi w dotarciu i pozyskaniu chronionych urządzeń systemu i niejawnych informacji w nim znajdujących się.

Takie wyposażenie infrastruktury telekomunikacyjnej jak **sejfy, szafy pancerne** czy przygotowanie skarbców nie ma bezpośredniego wpływu na bezpieczeństwo informacji wytwarzanej, przetwarzanej lub przesyłanej w systemach telekomunikacyjnych czy informatycznych. Jednak mają one znaczenie dla informacji pochodzącej z wymiany za pośrednictwem technicznych środków łączności i informatyki, które przechowane są w postaci dokumentów papierowych lub na nośnikach elektronicznych. Drugim elementem systemu telekomunikacyjnego (informatycznego), który musi podlegać ochronie przy użyciu sejfów, szaf pancernych lub znajdować się w skarbcach, to nie wykorzystywane aktualnie (np. zapasowe lub tzw. „gorąca rezerwa") urządzenia ochrony kryptograficznej oraz materiały kryptograficzne zabezpieczające prawidłowy tryb niejawnej pracy tych urządzeń.

Zgodnie z pragmatyką Organizacji Paktu Północnoatlantyckiego zawartą w dokumencie CM - (55)15 (Final) – „Bezpieczeństwo w ramach Organizacji Paktu Północnoatlantyckiego" czy dyrektywie bezpieczeństwa ACE Directive AD-70-1 sejfy, szafy pancerne lub pojemniki zostały podzielone na klasy od A do C. Każda z klas po uzyskaniu stosownej akceptacji od organów pełniących funkcję krajowej władzy bezpieczeństwa wyznacza kategorię informacji, która może być w nich przechowywana. Powyższe dokumenty normatywne NATO określają ponadto ściśle i dokładnie miejsce, w którym można je stosować jako środki bezpieczeństwa fizycznego.

Elementem uzupełniającym tę gamę środków bezpieczeństwa fizycznego są skarbce. Są to pomieszczenia budowane w obszarze stref bezpieczeństwa klasy I oraz II, które posiadają wzmocnienia architektoniczne. Dzięki specjalnej konstrukcji w skarbcach możliwe jest przechowywanie materiałów kryptograficznych, czy niejawnych informacji na odkrytych półkach.

Przed oddaniem w użytkowanie krajowa władza bezpieczeństwa (służba ochrony państwa) ma obowiązek sprawdzenia, czy ściany, podłogi, sufity i drzwi tych pomieszczeń zapewniają ochronę na poziomie odpowiadającym klasie sejfu (szafy pancernej, pojemnika) zaakceptowanego do przechowywania materiałów niejawnych.

Dostęp do stref bezpieczeństwa lub do pomieszczeń, w których bezpośrednio wytwarzane, przetwarzane, przechowywane lub przesyłane są informacje niejawne musi być **chroniony drzwiami i zamkami** posiadającymi specjalną konstrukcję lub wykonanymi z materiału zapewniającego wymaganą wytrzymałość. Drzwi te powinny ponadto być wyposażone w certyfikowane zamki, które dodatkowo zabezpieczają strefę, pomieszczenie lub kompleks pomieszczeń przed nieautoryzowanym do nich wejściem.

Zarówno drzwi jak i zamki muszą uzyskać od Wojskowych Służb Informacyjnych pełniących w resorcie Obrony Narodowej funkcję Służby Ochrony Państwa stosowne świadectwo kwalifikujące je jako możliwe do zastosowania środki bezpieczeństwa fizycznego. Tak jak ma to miejsce w przypadku sejfów czy szaf pancernych zarówno drzwi jak i zamki zabezpieczające informacje niejawne podzielono na trzy klasy, które muszą spełniać różne kryteria w zależności od klauzuli zabezpieczanych informacji.

Przed opuszczeniem pomieszczeń, gdzie znajdują się informacje niejawne, osoby sprawujące nad nimi pieczę muszą upewnić się, czy dokumenty są bezpiecznie składowane w przeznaczonych do tego miejscach, chronionych przez urządzenia zamykające. Po zakończeniu pracy powinny być przeprowadzane niezależne inspekcje stanu zabezpieczenia informacji niejawnych i miejsc ich przechowywania.

Bardzo istotnym zagadnieniem w procesie korzystania z środków bezpieczeństwa fizycznego, które odnosi się zarówno do sejfów, szaf pancernych jak i drzwi z zamontowanymi specjalnymi zamkami jest kontrola i nadzór nad kluczami je zamykającymi. Klucze do tych urządzeń ochrony fizycznej nie powinny być wynoszone poza budynek, które zabezpieczają. Upoważnione osoby muszą zapamiętać kody umożliwiające otwarcie pojemników zabezpieczających.

Zapasowe klucze i zapisy kodów, którymi należy posługiwać się tylko w nagłych wypadkach, powinny być przechowywane w zapieczętowanej, nieprzezroczystej ko-

percie we właściwej komórce jednostki organizacyjnej. Klucze używane na co dzień oraz klucze zapasowe trzeba przechowywać w osobnych pojemnikach. Dane dotyczące każdego kodu szyfrowego powinny być przechowywane w oddzielnych kopertach. Klucze i koperty z zapisem kodów wymagają równie rygorystycznej ochrony jak materiały niejawne, do których umożliwiają dostęp. Znajomość kombinacji szyfrowych uruchamiających zamki sejfów (szaf pancernych, pojemników), w których przechowywane są informacje niejawne NATO, należy ograniczyć do jak najmniejszej liczby osób. Kod szyfrowy musi być zmieniony:

- po każdej zmianie personelu;
- gdy doszło do ujawnienia kodu lub też istnieje domniemanie, iż może to nastąpić;
- w ustalonych dokumentami normatywnymi odstępach czasu.

Przed opuszczeniem pomieszczeń, gdzie znajdują się informacje niejawne, osoby sprawujące nad nimi pieczę muszą upewnić się, czy wszelkie informacje oraz urządzenia są bezpiecznie składowane w przeznaczonych do tego celu miejscach, chronionych przez urządzenia zamykające. Po zakończeniu pracy powinny być przeprowadzane niezależne inspekcje stanu zabezpieczenia informacji niejawnych i miejsc ich przechowywania.

Okna infrastruktury telekomunikacyjnej stanowiące granicę strefy bezpieczeństwa, wydzielonego pomieszczenia lub ich kompleksu, w których wytwarza, przetwarza, przechowuje lub przesyła informacje niejawne muszą posiadać zabezpieczenia przed nieuprawnionym wejściem, podglądem.

Standardowym zabezpieczeniem okien jest **montaż krat**. Wymóg ten jest uzależniony od najbliższego otoczenia chronionego obszaru (strefy) lub obiektu oraz od usytuowania samego okna. Przede wszystkim należy uwzględnić wysokość, na której znajduje się okno lub okna obszaru chronionego, w stosunku do elewacji budynku – mierzona od jego podstawy, jak i od dachu. Szczegóły w tej materii zawarte są w dyrektywie DBBT – 301A „Wytyczne w zakresie bezpieczeństwa fizycznego kancelarii kryptograficznych, stacji łączności kryptograficznej oraz pomieszczeń wydzielonych przeznaczonych do przetwarzania informacji niejawnej". W dokumencie powyższym ponadto zdefiniowano w formie normatywu konstrukcje samych krat – grubość (śred-

nica) materiału, odległość pomiędzy np. prętami oraz sposób ich zamocowania w otworze okiennym.

W niektórych sytuacjach dodatkowym wymogiem może być założenie siatki o określonych wymiarach „oczka" na zamontowane kraty.

Przedsięwzięcia uniemożliwiające podgląd – dotyczy to przede wszystkim okien stanowiących granicę strefy kontrolowanej, do których istnieje możliwość bezpośredniego lub pośredniego wglądu (np. brak strefy administracyjnej) – ograniczają się do zastosowania jednego lub kombinacji następujących środków:

- założenie ciężkich kotar lub zasłon,
- naklejenie na szkła okien specjalnej folii odblaskowej,
- zastąpienie normalnych szyb szybami ornamentowymi lub matowymi,
- założenie rolet lub żaluzji.

Przy wyborze środków uniemożliwiających podgląd należy mieć na uwadze, że winny one spełniać stawiane przed nimi wymagania i być skuteczne zarówno w warunkach światła dziennego, jak i przy świetle sztucznym.

Struktura organizacyjna i funkcjonalna współczesnych systemów telekomunikacyjnych oraz informatycznych podlega ciągłym przeobrażeniom, które wynikają z systematycznej implementacji coraz to nowszej generacji urządzeń (oprogramowania) lub modyfikacji dotychczas wykorzystywanych celem poprawienia wydajności systemów czy poszerzeniu gamy usług telekomunikacyjnych oferowanych przez system. Z tej też przyczyny system telekomunikacyjny bądź informatyczny możemy traktować jak „żywy organizm".

Wszystkie zmiany, a szczególnie te, które związane są z wykorzystaniem zdobyczy nauki i techniki, poza wszelkim niesionym ze sobą dobrodziejstwem wprowadzają również pewne elementy niebezpieczeństwa dla informacji wytwarzanej, przetwarzanej, przechowywanej lub przesyłanej w systemie.

Jak wcześniej wspomniano „wrażliwe" urządzenia lub terminale użytkowników niejawnego systemu telekomunikacyjnego muszą znajdować się w strefie bezpieczeństwa. Z reguły wymogiem jest, aby strefa ta była również strefą technicznie bezpieczną.

Mówiąc o strefie bezpiecznej technicznie mamy na myśli środki podsłuchowe, które można szybko i niepostrzeżenie zainstalować na terenie strefy lub wprowadzić je wraz z montowanym tam sprzętem technicznym lub innym stanowiącym wyposażenie miejsc pracy. Z tego powodu konieczne jest zbadanie sprzętu telekomunikacyjnego oraz biurowych urządzeń elektrycznych i elektronicznych wszelkiego typu, aby wykluczyć możliwość przypadkowego bądź celowego przekazania za ich pomocą niezaszyfrowanych informacji poza granice strefy. Należy prowadzić rejestr mebli i urządzeń znajdujących się na tym obszarze, zawierający dane dotyczące ich typu, numeru seryjnego i numeru inwentaryzacyjnego. Nie użytkowane rejony stref technicznie bezpiecznych powinny być niedostępne dla osób postronnych, a klucze do znajdujących się tam pomieszczeń trzeba chronić w takim samym stopniu, jak klucze do zamków (drzwi i sejfów) zabezpieczających informacje niejawne.

Ponadto mając na uwadze **bezpieczeństwo techniczne** w trakcie instalacji wszystkich urządzeń niejawnego systemu telekomunikacyjnego lub informatycznego musimy zwracać uwagę na:

- odległość pomiędzy urządzeniami transmisyjnymi, komutacyjnymi, końcowymi, itd. systemu jawnego i niejawnego, jeśli instalowane są w pobliżu siebie;
- odległość pomiędzy urządzeniami transmisyjnymi, komutacyjnymi, końcowymi, itd. systemów niejawnych przetwarzających informacje opatrzone różnymi klauzulami tajności;
- odległości pomiędzy okablowaniem strukturalnym różnych systemów (jawny – niejawny, niejawne różnych klauzul);
- okablowanie sieci energetycznej (separacja zasilania systemów niejawnych od jawnych);
- miejsce znajdowania się źródła zasilania systemów niejawnych (strefa bezpieczeństwa, strefa administracyjna, poza kontrolą);
- instalacja wodno-kanalizacyjna (separacja);
- instalacja centralnego ogrzewania (separacja).

Przedstawione powyżej czynniki mające wpływ na bezpieczeństwo techniczne w sposób bardziej szczegółowy zostały zdefiniowane i opisane w dyrektywie BTPO –

701A „Wytyczne w zakresie instalacji urządzeń przeznaczonych do przetwarzania informacji niejawnych".

Zawarte w niej wymogi stanowią normatyw dla wszelkich urządzeń technicznych łączności i informatyki funkcjonujących, wdrażanych lub planowanych do wdrożenia systemów telekomunikacyjnych i informatycznych w siłach zbrojnych.

Z tej przyczyny organy odpowiedzialne za bezpieczeństwo łączności i informatyki muszą na bieżąco śledzić wszelkie zmiany lub modyfikacje wprowadzane do systemów i dokonywać analizy stanu bezpieczeństwa, co może wpływać na:

- bezpieczeństwo kryptograficzne,
- ochronę elektromagnetyczną,
- ochronę programową,
- ochronę transmisji informacji,
- techniczne wsparcie ochrony fizycznej.

Każdy wojskowy system telekomunikacyjny lub informatyczny, w którym wytwarza, przetwarza, przechowuje i przede wszystkim przysyła się informacje niejawne stanowiące tajemnicę państwową lub służbową, wykorzystuje do ochrony zasobów informacyjnych urządzenia ochrony kryptograficznej.

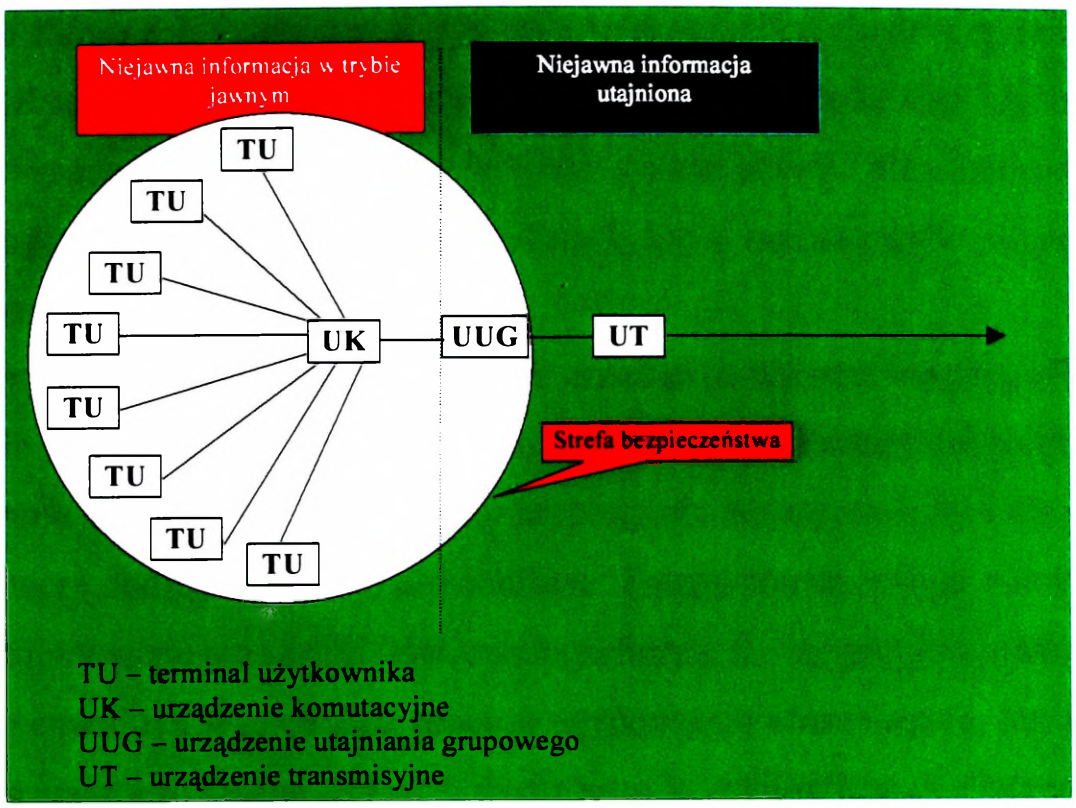
Ze względu na sposób i miejsce utajniania informacji w systemie urządzenia **ochrony kryptograficznej** możemy podzielić na:

- urządzenia utajniania grupowego;
- urządzenia utajniania indywidualnego.

Pierwsze z nich, przedstawione na rysunku nr 5.1.2, zazwyczaj stosujemy w sytuacji, gdy w pewnym rejonie lub obszarze mamy zgrupowane urządzenia końcowe (terminale) zabezpieczające dostęp uprawnionych użytkowników do niejawnych zasobów informacyjnych systemu.

Wszystkie urządzenia systemu telekomunikacyjnego bądź informatycznego znajdują się w obszarze strefy bezpieczeństwa lub rejonie chronionym zgodnie z zaleceniami oraz wytycznymi służb ochrony państwa. Niejawna informacja zmienia swoją postać i zostaje zaszyfrowana przez grupowe urządzenie utajniające dopiero w momencie, gdy ta opuszcza wyznaczony rejon lub strefę bezpieczeństwa. W zależności od rozwiązań strukturalnych systemu urządzenie transmisyjne może znajdować się

w strefie lub poza nią. Z punktu widzenia bezpieczeństwa dla już utajnionej informacji nie ma to większego znaczenia.



Rys.5.1.2. Przykład utajniania grupowego

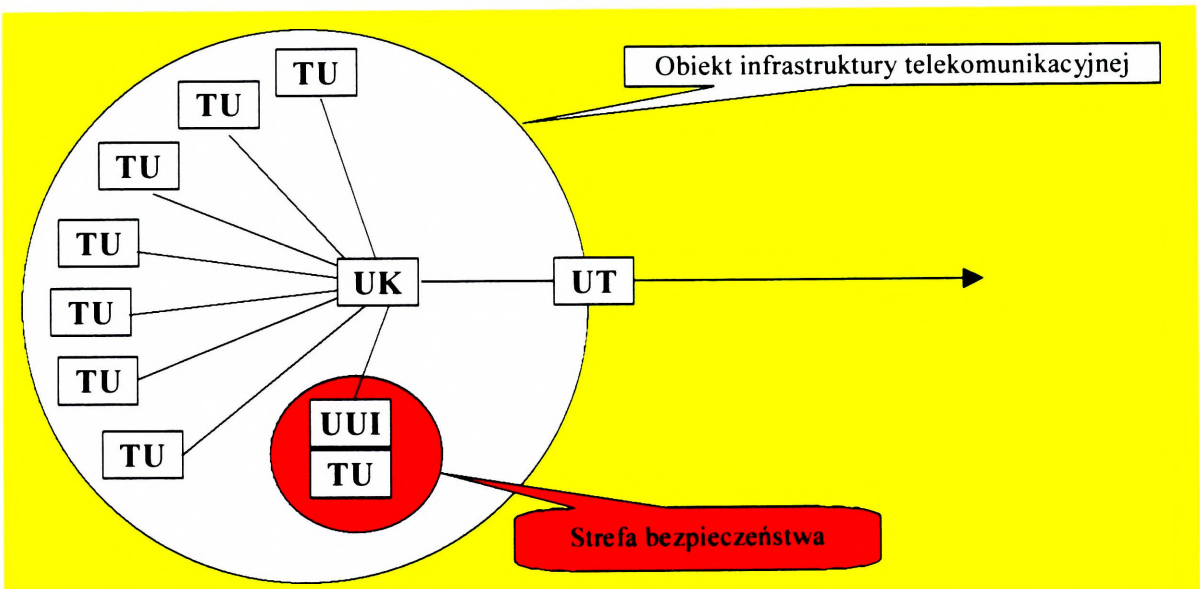
Źródło: J. Michniak i inni, „Bezpieczeństwo i ochrona informacji w sieciach łączności i informatyki wojskowej w okresie pokoju, kryzysu i wojny", Praca naukowo- badawcza pk. OCHRONA, AON, Warszawa 2004

Przedstawione powyżej rozwiązanie jest rozwiązaniem ekonomicznym, gdyż utajnia informacje na potrzeby pewnej grupy użytkowników systemu bez względu na rodzaj świadczonych przez niego usług telekomunikacyjnych. Jednak musimy pamiętać, że poza wymaganiami stawianymi dla strefy bezpieczeństwa klasy I lub II, obligatoryjnie każdy uprawniony użytkownik systemu musi posiadać poświadczenie bezpieczeństwa osobowego odpowiadające maksymalnej klauzuli informacji wytwarzanej, przetwarzanej, przechowywanej lub przesyłanej w danym systemie.

W przypadku stosowania urządzeń utajniania indywidualnego (rysunek 5.1.3), tak jak poprzednio, mamy grupę użytkowników z przydzielonymi terminalami jawnego systemu telekomunikacyjnego. Jednak tylko jeden lub kilku z nich posiada uprawnienia do wytwarzania, przetwarzania, przechowywania lub przesyłania informacji niejawnych. Z tej przyczyny tylko i wyłącznie te osoby funkcyjne jako użytkownicy systemu mają przydzielone urządzenia utajniania indywidualnego, które znajdują się w bezpośredniej bliskości terminala lub stanowią jego integralną część.

Przy utajnianiu grupowym cała opuszczająca chroniony rejon lub strefę bezpieczeństwa informacja była utajniona. W sytuacji stosowania urządzeń utajniania indywidualnego informacja utajniona w systemie telekomunikacyjnym czy informatycznym stanowi pewną określoną część wymienianych zasobów informacyjnych systemu. Z tej też przyczyny system traktowany jest jako system jawny i nie musi spełniać szeregu wymogów czy rygorystycznych obostrzeń, które normatywnie nałożone są na system niejawny.

Głównym zadaniem realizowanym przez urządzenia ochrony kryptograficznej jest zapewnienie poufności oraz integralności informacji. Aby założony cel mógł być spełniony zarówno urządzenia jak i materiały kryptograficzne zapewniające ich poprawne działanie muszą podlegać szczególnej ochronie. Polega ona na stałym monitorowaniu od momentu wytworzenia materiałów kryptograficznych, czy procesu produkcji urządzeń, aż do chwili ich wycofania z procesu użytkowania i zniszczenia. Ich zamknięty obieg zapewniają wydzielone „kanały" dystrybucji kryptograficznej, a liczba personelu musi być ograniczona do niezbędnego minimum.



Rys. 5.1.3 Przykład utajniania indywidualnego

Źródło: J. Michniak i inni, „Bezpieczeństwo i ochrona informacji w sieciach łączności i informatyki wojskowej w okresie pokoju, kryzysu i wojny", Praca naukowo- badawcza pk. OCHRONA, AON, Warszawa 2004

Szczegółowe informacje w tym zakresie zawiera dyrektywa BTPO – 601A „Wytyczne w zakresie postępowania z materiałami kryptograficznymi". Natomiast w stosunku do urządzeń i niejawnych systemów sojuszniczych obszar ten reguluje dyrektywa AD – 90-9 „Procedury w zakresie zabezpieczenia, ewidencji oraz zaopatrywania w środki i materiały kryptograficzne".

Cechą charakterystyczną emisji niekontrolowanej jest możliwość przechodzenia sygnału z jednej postaci w drugą. Na przykład fala elektromagnetyczna, natrafiając na przewodnik, może być propagowana dalej w postaci fali powierzchniowej. Dlatego **ochrona przed emisją ujawniającą** musi uwzględniać wszystkie typy propagacji oraz całą szerokość widma.

Problematyka zwalczania niekontrolowanej emisji jest w dużej mierze sprawą kompatybilności elektromagnetycznej. W pierwszym rzędzie należy zagwarantować spełnienie przez urządzenia elektryczne systemu telekomunikacyjnego bądź informatycznego krajowych norm dotyczących ograniczenia emisji elektromagnetycznej. Dodatkowe środki zabezpieczenia przed emisją ujawniającą można podzielić na trzy kategorie:

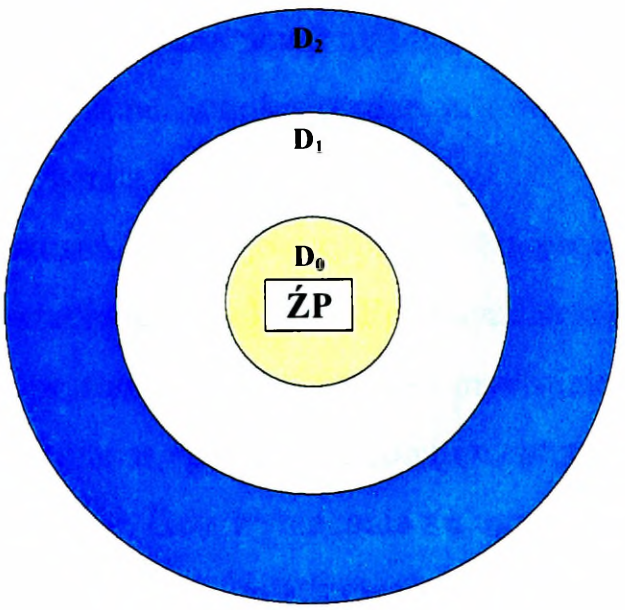
- modyfikacje urządzeń i przyrządów,
- stosowanie urządzeń maskujących,
- ekranowanie, blokowanie i filtrowanie.

Możliwości modyfikowania urządzeń przez zwykłego użytkownika systemu telekomunikacyjnego lub informatycznego są bardzo ograniczone z uwagi na brak specjalistycznej aparatury oraz groźbę utraty gwarancji producenta na posiadany sprzęt. Z kolei oferowane na rynku urządzenia o obniżonym poziomie emisji elektromagnetycznej są bardzo kosztowne. Stosowanie urządzeń maskujących (generatorów szumu elektromagnetycznego) jest prawnie zabronione, ponieważ są one źródłem zakłóceń dla wszystkich innych urządzeń elektrycznych i telekomunikacyjnych pracujących w najbliższym sąsiedztwie. Podstawowymi technikami dodatkowego ograniczania niekontrolowanej emisji dla większości systemów są zatem różne sposoby ekranowania. Można ekranować urządzenia, budynki i pomieszczenia oraz przenośne kabiny.

Zastosowanie poszczególnych rozwiązań uzależnione od wielu czynników, do których możemy przykładowo zaliczyć:

- przeznaczenie systemu,
- klauzula przekazywanych informacji,
- koszt planowanych do zastosowania urządzeń,
- wymagany poziom obniżenia emisji ujawniającej.

Ostatnie z wymienionych zadań określa się na podstawie przeprowadzonych przez specjalistyczne komórki sił zbrojnych pomiarów poziomu emisji ujawniającej, które popularnie zwane jest „strefowaniem". Jest to nic innego jak określanie poziomu emisji w danej odległości od źródła promieniowania, co zilustrowane zostało na rysunku 5.1.4.



ŹP – źródło promieniowania
D_0 ,D_1 ,D_2 – granica strefy

Rys. 5.1.4. Przykładowe zasady wyznaczania strefy
Źródło: J. Janczak, G. Świdzikowski, Bezpieczeństwo informacji w wojskowym systemie telekomunikacyjnym, AON, Warszawa 2004

Dopuszczalny poziom emisji ujawniającej dla urządzeń telekomunikacyjnych i informatycznych oraz wynikająca z przeprowadzonych pomiarów strefa określa wymogi zarówno w stosunku do samych urządzeń jak i samej infrastruktury, w której dany system ma funkcjonować. Po przeprowadzeniu analizy stref przedstawionych na rysunku zamieszczonym powyżej należy stwierdzić, że najwyższe wymagania w zakresie emisji ujawniającej, co do montażu urządzeń telekomunikacyjnych i informatycznych, dotyczą strefy D0. Wzrost numeracji strefy, a tym samym wzrost odległości,

gdzie jesteśmy w stanie kontrolować i monitorować dany obszar, wymagania te obniża.

Wymagania w zakresie strefowania oraz samych urządzeń przetwarzających, przechowujących czy przesyłających informacje niejawne określa każda narodowa służba ochrony państwa.

Do ochrony obudów urządzeń oraz ekranów monitorów stosuje się specjalne materiały ekranujące: folie metalizowane, plastyki z powłoką metalową, farby metalizowane, szkło metalizowane. Otwory wentylacyjne powinny być zabezpieczone specjalnymi siatkami.

Dla wszystkich połączeń w systemie należy stosować wyłącznie ekranowane kable i łączówki, gniazdka zasilania powinny mieć filtry elektromagnetyczne, a na kablach powinny być instalowane tłumiki (o rdzeniu toroidalnym). Długość wszystkich kabli połączeniowych powinna być minimalna.

Ochronę pomieszczeń uzyskuje się przez zbudowanie izolowanej konstrukcji metalowej znanej powszechnie jako klatka Faradaya. Ściany pomieszczeń można zabezpieczyć za pomocą płyt metalowych montowanych jako wewnętrzna warstwa betonowej konstrukcji. Płyty te są spawane ze sobą i elektrycznie izolowane, a następnie uziemione w jednym punkcie. Gdy wymagania na ograniczenie emisji nie są zbyt wygórowane, można zastosować folie metalizowane klejone na ściany. Podłogi chroni się materiałami izolacyjnymi, np. laminowanym papierem lub płytami PCV. Dostępne są metalizowane, podwieszane ekrany sufitowe.

W pomieszczeniach należy zabezpieczyć drzwi (za pomocą płyt metalowych) oraz okna (wypełnione ekranowanym szkłem). Dodatkowo, wszystkie nieelektryczne instalacje (np. rury instalacji wodno-kanalizacyjnej) powinny być dołączone do metalowych ekranów, a przewody wentylacyjne powinny być wyposażone w filtry elektromagnetyczne. W punktach wyjścia z pomieszczenia wszystkich przewodów zasilających, linii telefonicznych i kabli sieciowych również powinny być instalowane filtry.

Zasady ekranowania kabin są takie same, jak pomieszczeń. Zaletą przenośnych kabin jest brak ograniczeń występujących w budynkach (np. wynikających z obowiązku stosowania prawa budowlanego). W związku z tym koszt zabezpieczenia kabin jest niższy niż pomieszczeń.

Ważnym elementem bezpieczeństwa wojskowego systemu telekomunikacyjnego i informatycznego jest **ochrona programowa**. Wiąże się ona z identyfikacją, upoważnieniem lub uwierzytelnieniem zapewniającym uprawniony dostęp do systemu lub określonych zasobów informacyjnych znajdujących się w systemie. Zapewnia to między innymi oprogramowanie operacyjne systemu, którego rodzaj (typ) określają wojskowe dokumenty normatywne oraz sposób jego instalowania na potrzeby systemu niejawnego.

Metody programowe ochrony informacji praktycznie stosowane są we wszystkich cyfrowych wojskowych systemach telekomunikacyjnych oraz informatycznych przeznaczonych do wytwarzania, przetwarzania, przechowywania i przesyłania informacji niejawnych. Jest to bowiem jeden z wymogów umożliwiających dopuszczenie przez służby ochrony państwa systemu do eksploatacji w siłach zbrojnych.

Celem ochrony programowej jest logiczna kontrola dostępu i ochrona przed nieuprawnionym dostępem do zabezpieczanych zasobów informacyjnych systemu, a tym samym zapewnienie poufności informacji oraz rozliczalność działań i zdarzeń mających miejsce w systemie. Poza „intruzami" w systemie pozwala uchronić go przed nierozważnym, lekkomyślnym działaniem własnego personelu technicznego czy jego użytkowników.

Do głównych zalet metody ochrony programowej w zakresie kontroli dostępu możemy zaliczyć:

- możliwość samodzielnego bądź dedykowanego opracowania a następnie wdrożenia do systemu;
- brak wpływu na proces wytwarzania, przetwarzania, przechowywania lub przesyłania informacji w systemie;
- stosowanie niekonwencjonalnych rozwiązań podnoszących poziom bezpieczeństwa i tym samym prawdopodobieństwo ochrony systemu oraz jego zasobów informacyjnych.

Współczesne systemy telekomunikacyjne, szczególnie te, które wykorzystują w swojej strukturze technicznej urządzenia informatyczne są zmuszane do stosowania programowych metod ochrony informacji, które na pewnych etapach przetwarzania są

jedynymi skutecznie chroniącymi system oraz znajdujące się w nim zbiory niejawnych informacji.

Odpowiednio przygotowana i wdrożona ochrona programowa w systemie powinna spełniać następujące wymagania:

- posiadać możliwość każdorazowej identyfikacji uprawnionego użytkownika terminala końcowego bądź stacji roboczej;
- posiadać ściśle zdefiniowane zbiory chronionej informacji oraz uprawnienia przydzielane i posiadane przez poszczególnych jego użytkowników;
- posiadać zdolność monitorowania wszystkich zdarzeń występujących w systemie (np. uprawnione i nieuprawnione wejścia, wyjścia z systemu);
- uniemożliwiać wszelkie próby nieautoryzowanej modyfikacji lub niszczenia zbiorów informacji;
- monitorować transmisję informacji zarówno opuszczającą chronioną strefę jak i informację do niej wchodzącą;
- w uzasadnionych przypadkach zapewniać szyfrowanie przechowywanych w systemie danych.

Do podstawowych środków ochrony programowej zapewniających bezpieczeństwo dostępu do systemu i jego zasobów informacyjnych zaliczane są:

- hasła dostępowe oraz identyfikatory, które zapewniają dostęp do chronionych urządzeń systemu i umożliwiają rozpoczęcie pracy w systemie (np. po zalogowaniu się);
- definiowanie zasobów informacyjnych, do których ma dostęp pojedynczy (indywidualny) użytkownik;
- rejestracja zdarzeń w systemie do poziomu monitorowania pracy i poleceń realizowanych przez poszczególnych użytkowników;
- zastosowanie hierarchicznego systemu dostępu do urządzeń, usług i zasobów informacyjnych systemu zgodnie z zasadą wiedzy niezbędnej (np. użytkownicy o wyższym statusie (priorytecie) mają możliwość ingerencji w możliwości użytkowników o niższym statusie – przerywanie połączeń telefonicznych);
- zabezpieczenia indywidualne (np. dedykowane specjalistyczne oprogramowanie).

Do najbardziej znaczących, wymienionych powyżej, środków ochrony można zaliczyć rejestrację zdarzeń w systemie, które w postaci dziennika ewidencji pracy systemu stanowi zestaw chronologicznie uszeregowanych informacji o realizowanych przez sam system, jak i indywidualnych użytkowników, zadań. Szczególnie ważne jest zwracanie bacznej uwagi na wykonywane przez system zadania, które odbiegają od przyjętych standardów i procedur. Ponadto analiza dziennika pozwala na:

- zebranie informacji w zakresie upoważnień związanych z chronionymi zbiorami;
- ustalenie odpowiedzialności w zakresie dokonywanych modyfikacji;
- wykrycia prób dostępu do chronionych zasobów informacyjnych oraz przypadków odmowy udzielenia dostępu;
- wykrycia zmian w konfiguracji systemu zarówno z poziomu administratora jak i użytkownika;
- ustalenia grupy użytkowników najczęściej popełniających błędy;
- określenie czasu i zasobów niejawnych, do których udzielono tzw. upoważnień tymczasowych.

W wielu systemach telekomunikacyjnych wykorzystujących urządzenia komputerowe jako standard zapewniający identyfikację oraz uwierzytelnienie przyjęto dwuelementowy mechanizm – identyfikator oraz uzgodnione dwustronnie (podane przez użytkownika) hasło.

W stosunku do haseł istnieje szereg wymagań. Zaliczyć do nich możemy:

- długość hasła (ilość znaków);
- kombinacyjny układ haseł (np. litery i cyfry, znaki duże i małe);
- termin ważności hasła (cykliczność zmiany hasła).

Przedstawione powyżej środki i metody ochrony programowej w systemach nie stanowią pełnego oraz rzeczywistego obrazu przedsięwzięć stosowanych w tym zakresie. Ilość i rodzaj środków czy metod uzależniona jest od funkcji i przeznaczenia każdego systemu w zależności od indywidualnych potrzeb.

W myśl dokumentów normatywnych[146] Organizacji Paktu Północnoatlantyckiego **bezpieczeństwo transmisji** informacji (*ang. transmission security – TRANSEC*) jest

[146] MC-322, Transmission security, Military Committee, Brussels 1992

tym komponentem bezpieczeństwa łączności i informatyki, w którym stosuje się wszystkie rodzaje środków ochrony z wyjątkiem zabezpieczeń fizycznych. Zadaniem bezpieczeństwa transmisji jest ochrona informacji przed nieautoryzowanym przechwytem i wykorzystaniem przez środki inne niż analiza kryptograficzna.

Celem tej dziedziny jest zrozumienie jak zapewnić bezpieczeństwo wysyłanej oraz obieranej za pomocą technicznych środków łączności i informatyki informacji, która może przyjmować postać znaków, sygnałów, obrazów czy dźwięków – włączając w to wszelkie formy wymiany fonicznej, graficznej, telefaksowej, transmisji danych oraz innych wiadomości. Transmisja informacji może odbywać się za pomocą środków radiowych, radioliniowych, liniami (trasami) kablowymi, optycznymi lub przy użyciu innych systemów elektromagnetycznych.

Mechanizmy bezpieczeństwa transmisji muszą wspomagać cele polityki bezpieczeństwa w zakresie osiągalności i poufności informacji. Cel integralności uzyskiwany jest bezpośrednio jako funkcja całkowitej osiągalności zapewnionej przez zastosowane mechanizmy "TRANSEC" w celu uniemożliwienia potencjalnemu przeciwnikowi zakłócenia planowej transmisji.

W większości przypadków wymaganie to realizowane jest w aspekcie dostępności wymaganego np. pasma częstotliwości radiowej, które przeznaczone jest na potrzeby transmisji. W praktyce nowe mechanizmy bezpieczeństwa transmisji z tzw. skokową zmianą częstotliwości (*ang. frequency hopping - FH*) nadajników oraz odbiorników środków radiowych mogą przeciwdziałać planowym lub niezamierzonym zakłóceniom naszych systemów transmisyjnych przez przeciwnika. W uzasadnionych przypadkach może to wpływać na eliminację zakłóceń interferencyjnych pochodzących od własnych źródeł promieniowania przez własne systemy (kompatybilność elektromagnetyczna). Pod pojęciem FH należy rozumieć szybką (skaczącą), symultaniczną zmianę częstotliwości nadajnika i odbiornika w oparciu o pseudolosowy ciąg częstotliwości. Gdy natomiast mówimy o problemach kompatybilności elektromagnetycznej to jej zasadniczym efektem mającym wpływ na transmisję informacji są zakłócenia interferencyjne. Oznacza to bowiem, że równolegle prowadzona jest transmisja na tej samej lub pobliskiej częstotliwości, której wynikiem może być zanik lub wariacja pożądanej amplitudy sygnału. Nie zastosowanie tych przedsięwzięć może

umożliwić nieuprawnionemu użytkownikowi modyfikację informacji wyrażającą się w:

- dopisaniu jakiejś nowej treści do oryginalnej informacji,
- przekształceniu treści oryginalnej informacji,
- częściowym lub pełnym wykasowaniem oryginalnej informacji,
- celowym opóźnianiu przesłania informacji,
- powtarzaniu transmitowanych komunikatów.

Tego typu atak na system telekomunikacyjny lub informatyczny ma na celu spowodowanie utraty integralności lub niespełnienie wymogu terminowości w przekazywaniu informacji. Dość istotnym czynnikiem jest powtarzanie transmisji tych samych danych, informacji lub komunikatów, które przy znacznym nasileniu mogą przyczynić się do zablokowania (przeładowania) kanałów transmisyjnych.

Innym rozwiązaniem zapewnienia dostępności, które może spełniać uprzednio wymienione wymagania jest szerokość spektrum sygnałowego. Pod tym pojęciem należy rozumieć zastosowanie takich środków (urządzeń) techniki telekomunikacyjnej, w której modulowana informacja jest transmitowana w paśmie znacznie większym niż zajmowałaby to informacja oryginalna.

Aspekt poufności informacji należy rozpatrywać w sytuacji, gdy zachodzi możliwość wykrycia wykorzystywanej do transmisji informacji częstotliwości radiowej. W następstwie wykrycia częstotliwości może nastąpić przechwyt informacji rozumiany jako nieautoryzowane działanie w celu poszukiwania, podsłuchu lub nagrywania wymiany telekomunikacyjnej dla celów wywiadowczych lub oszukania przeciwnika poprzez „spoofing", czy naśladowanie podstępu.

Środkiem zapobiegającym ewentualnemu ujawnieniu przesyłanej informacji w wyniku przechwytu może być i zazwyczaj w praktyce jest stosowane utajnianie informacji. Przechwycenie informacji zabezpieczonej przy użyciu środków ochrony kryptograficznej przez osoby niepowołane nie jest równoznaczne z jej ujawnieniem, ponieważ przechwycone dane są w postaci zaszyfrowanej. Dlatego też wyspecjalizowane komórki rozpoznawcze i wywiadowcze potencjalnego przeciwnika działają dwutorowo:

- podejmują próby rozszyfrowania utajnionej informacji,

– przeprowadzają analizę transmisji (przesyłu informacji).

Złamanie zasad utajniania jest procesem bardzo złożonym i przede wszystkim wymagającym znacznego nakładu czasu oraz sił i środków, którego celem i efektem jest odczyt zaszyfrowanych wiadomości.

Drugie rozwiązanie jest prostsze. Zamiast zajmować się rozszyfrowaniem, bada się **strukturę budowy przesyłanych komunikatów**, ich długość i częstotliwość z jaką są wysyłane. Analiza przesyłu pozwala też na odkrycie lokalizacji i tożsamości wymieniających informacje urządzeń telekomunikacyjnych lub informatycznych. Tego typu dane mogą być równie ważne, jak treść przesyłanych informacji.

Z wojskowego punktu widzenia wykrycie samego ruchu w określonym kanale komunikacyjnym może dostarczyć przeciwnikowi informacji operacyjnej lub taktycznej o planach, realizowanych przedsięwzięciach wojsk własnych. Ujawnienie tych specyficznych informacji w odniesieniu do dyslokacji i ilości tych sił może być sprzeczne z interesem naszych wojsk i efektywnie przyczynić się do niepowodzenia planowanych lub toczących się działań zbrojnych.

W związku z powyższym w celu zapewnienia bezpieczeństwa natężenia przepływu informacji należy stosować urządzenia ochrony kryptograficznej, które bez względu na obecność informacji w kanale transmisyjnym będą zapewniały ten sam poziom natężenia przepływu informacji.

Kolejnym bardzo istotnym przedsięwzięciem zapewniającym bezpieczeństwo transmisji informacji w systemie telekomunikacyjnym i informatycznym jest wdrożenie systemu bądź środków zapewniających **uwierzytelnienie każdego użytkownika** uprawnionego do pracy w systemie. Zastosowanie odpowiednich mechanizmów w tej dziedzinie daje pewność autentyczności w zakresie wymiany informacji (transmisji), oraz że jest ona realizowana pomiędzy uprawnionymi użytkownikami systemu.

Najprostszym przykładem zastosowania tych mechanizmów w wojskowych sieciach radiowych jest procedura sprawdzenia tożsamości, która stanowi uzupełnienie danych radiowych, tabeli sygnałów rozpoznawczych, itp. oraz sumarycznie stanowi o bezpieczeństwie transmisji informacji w systemie.

Podszywanie się pod uprawnionego użytkownika systemu telekomunikacyjnego ma na celu zdobycie informacji pochodzącej z wymiany danych, ale również możli-

wość dokonania jej modyfikacji lub powtórzenia transmisji w celu oszukania, wprowadzenia zamieszania lub przeciążenia systemu telekomunikacyjnego.

Gdy mówimy o **technicznym wsparciu przedsięwzięć** realizowanych w ramach ochrony fizycznej niejawnych systemów telekomunikacyjnych lub informatycznych to mamy na myśli środki, w skład których wchodzą:

- instalacje alarmowe,
- instalacje przeciwpożarowe,
- systemy monitorujące,
- kołowroty,
- bezpieczeństwo środków bezpieczeństwa.

Zgodnie z ogólnie przyjętą w całym współczesnym świecie pragmatyką stosowanie samych środków ochrony fizycznej, które w języku potocznym nazywamy zabezpieczeniem antywłamaniowym, jest wymogiem podstawowym, ale nie dającym całkowitej pewności zapewnienia wymaganego poziomu bezpieczeństwa systemom łączności i informatyki.

Odnosi się to szczególnie do tych obiektów i pomieszczeń, w których nie ma wymogu pełnienia całodobowych dyżurów (np. bezobsługowe stacje łączności) lub niejawnych terminali końcowych wykorzystywanych tylko w godzinach pracy służbowej. Dodatkowo w tych obiektach czy pomieszczeniach winny być instalowane systemy alarmowe bądź systemy monitorujące telewizji przemysłowej (możliwa kombinacja), których zadaniem jest wykrycie nieuprawnionego wejścia po ewentualnym przełamaniu pozostałych środków bezpieczeństwa fizycznego. Wytyczne w zakresie zasad instalacji oraz klasy systemu alarmowego zawiera dyrektywa DBBT – 301A „Wytyczne w zakresie bezpieczeństwa fizycznego kancelarii kryptograficznych, stacji łączności kryptograficznej oraz pomieszczeń wydzielonych przeznaczonych do przetwarzania informacji niejawnej".

Wsparcie techniczne ochrony fizycznej musi ponadto uwzględniać stosowanie zabezpieczeń przeciw możliwym katastrofom takim, jak pożar, powódź, trzęsienie ziemi, itp.

Przedsięwzięcia realizowane w tym zakresie mogą obejmować przykładowo:

- założenie instalacji przeciwpożarowej;

- instalację dodatkowych bezpieczników przepięciowych dla sprzętu łączności i informatyki;
- zakup stabilizatorów i zasilaczy awaryjnych (UPS);
- instalację czujników wykrywających wodę w pomieszczeniach;
- instalację systemów powodujących automatyczne zamknięcie (wyłączenie) systemów operacyjnych (urządzeń telekomunikacyjnych) w przypadku ogłoszenia alarmu.

Za wsparcie techniczne należy ponadto uważać urządzenia lub systemy monitorujące czy kontrolujące wejścia i wyjścia do oraz ze stref bezpieczeństwa, obszarów chronionych, które zazwyczaj wspomagają elektroniczne systemy przepustkowe (np. karty magnetyczne), które coraz częściej stosowane w jednostkach organizacyjnych resortu Obrony Narodowej.

Umożliwiają bowiem praktycznie natychmiastowe stwierdzenie, w przypadku zaistnienia incydentu wpływającego na bezpieczeństwo informacji w systemie, kto może być za niego odpowiedzialny.

Zadaniem wsparcia technicznego jest ponadto zapewnienie określonego w dyrektywach i wytycznych poziomu bezpieczeństwa dla stosowanych w systemie telekomunikacyjnym bądź informatycznym środków bezpieczeństwa.

Wszystkie omówione dotychczas przedsięwzięcia mają na celu zapewnienie bezpieczeństwa informacji w systemach telekomunikacyjnych. Stopień oraz natężenie ich występowania w systemie ochrony np. sieci teletransmisyjnej, choć prawnie wymagane, wynika przede wszystkim z analizy ryzyka, ale również i pewnych ograniczeń, które wynikają między innymi z możliwości technologicznych i nakładów wyrażonych określoną kwotą środków finansowych.

Jednak w procesie oceny bezpieczeństwa informacji w sieci teletransmisyjnej dywizji zmechanizowanej, aby była ona pełna, zostanie uwzględniony ogół przytoczonych przedsięwzięć organizacyjno-eksploatacyjnych i technicznych, których zadaniem jest ochrona informacji.

5.2. OCENA BEZPIECZEŃSTWA INFORMACJI W SIECI TELETRANSMISYJNEJ DYWIZJI ZMECHANIZOWANEJ

Podejmując próbę dokonania oceny bezpieczeństwa informacji w sieci teletransmisyjnej dywizji zmechanizowanej musimy pamiętać, że zgodnie z obowiązującymi w Polsce przepisami warunkiem koniecznym oddania do eksploatacji każdego systemu lub sieci wytwarzającej, przetwarzającej, przechowującej lub przesyłającej informacje niejawne jest opracowanie oraz zatwierdzenie „Szczególnych wymagań bezpieczeństwa".

W związku z powyższym po uwzględnieniu powyższego wymogu ocena bezpieczeństwa informacji dokonana zostanie zgodnie z „Metodyką opracowania Szczególnych Wymagań Bezpieczeństwa systemu lub sieci teleinformatycznej", w której zalecany układ ma następujący kształt:

1.Charakterystyka sieci:

- określenie sieci,
- rola i zadania (przeznaczenie),
- kto użytkuje.

2. Dane o budowie:

- lokalizacja,
- architektura (konfiguracja sprzętowa, połączenia wewnętrzne, zewnętrzne, oprogramowanie systemowe i użytkowe).

3. Wymagania bezpieczeństwa

- zagrożenia,
- podatność na zagrożenia,
- minimalne standardy bezpieczeństwa.

4. Środowisko bezpieczeństwa:

- globalne,
- lokalne,
- środowisko bezpieczeństwa elektronicznego.

5. Środki bezpieczeństwa:

- przedsięwzięcia,
- środki ochrony.

6. Zarządzanie bezpieczeństwem:
   - struktura organów
   - zarządzanie ryzykiem,
   - procedury bezpieczeństwa,
   - kontrola konfiguracji,
   - utrzymanie,
   - dokumentacja,
   - szkolenia,
   - certyfikacja,
   - wycofanie,
7. Ogólne zasady instalacji urządzeń.
8. Zasady dowiązywania (łączenia) z innymi sieciami lub systemami.

Podążając zatem tak przyjętym tokiem rozumowania oraz dokonując analizy poszczególnych punktów „Szczególnych wymagań bezpieczeństwa", można przyjąć, że charakterystyka sieci, dane o jej budowie oraz wymagania bezpieczeństwa i środowisko pracy rozpatrywanej sieci teletransmisyjnej dywizji zmechanizowanej zawarte zostały w poprzednich rozdziałach niniejszej dysertacji.

Jeśli jednak zastanowić się głębiej nad wymienionymi aspektami organizacji i funkcjonowania omawianej sieci teletransmisyjnej, to zaczyna nasuwać się jedno zasadnicze pytanie – czy możliwe jest tak dokładne zaplanowanie i określenie wszystkich wymienionych przedsięwzięć, a następnie ujęcie ich w sformalizowany i zatwierdzony przez stosowne organy bezpieczeństwa dokument podczas prowadzenia przez dywizję działań taktycznych?

Aby udzielić rzeczowej odpowiedzi na tak postawione pytanie należy wziąć pod uwagę między innymi następujące czynniki:

- otrzymane przez dywizję zadanie oraz przyjętą w procesie dowodzenia koncepcję prowadzenia działań, która stanowi podstawę organizacji sieci teletransmisyjnej dywizji;
- dotychczasowe i przewidywane oddziaływanie sił i środków przeciwnika na sieć teletransmisyjną;
- obszar rozwinięcia i funkcjonowania sieci (m.in. terytorium własne czy obce).

Wymienione czynniki wskazują, ze podstawą organizacji sieci teletransmisyjnej jest decyzja dowódcy wyrażona w postaci rozkazu operacyjnego, w którym zawarte są wszelkie zalecenia i uwarunkowania dotyczące funkcjonowania systemu dowodzenia – w tym sieci teletransmisyjnej. Z tego punktu widzenia dla określonego czasu, miejsca i przestrzeni można określić lokalizację, architekturę oraz środowisko, w którym sieć teletransmisyjna pracuje. Jednak działania taktyczne prowadzone przez dywizję nie są statyczne. Cechują się one bowiem choćby manewrowością i zmiennością sytuacji, która wpływa na obraz pola walki i tym samym wymusza wprowadzanie korekt do przyjętej koncepcji działania. Nie pozostaje to bez wpływu na organizację i funkcjonowanie sieci teletransmisyjnej dywizji.

Analiza kolejnego piątego punktu, która obejmuje problematykę środków bezpieczeństwa pozwoli na dokonanie oceny bezpieczeństwa informacji w badanej sieci teletransmisyjnej dywizji zmechanizowanej. Przystępując do niej musimy mieć na uwadze z jednej strony przyjętą w rozdziale drugim strukturę sieci (rys. 2.5.2), z drugiej zaś pamiętać o zidentyfikowanych w rozdziale poprzednim zagrożeniach dla bezpieczeństwa informacji. Zestawienie tych dwóch czynników bowiem stanowi dopiero punkt wyjścia do określenia przedsięwzięć organizacyjno-eksploatacyjnych i technicznych, które wchodząc w skład systemu ochrony zapewniają bezpieczeństwo informacji w rozpatrywanej sieci teletransmisyjnej dywizji zmechanizowanej. Uwzględnienie przyjętej gradacji zagrożeń sprawia, że ocena bezpieczeństwa informacji w sieci teletransmisyjnej rozpoczęta zostanie od obszaru **bezpieczeństwa personalnego**.

Zgodnie z wymogami ustawowymi[147] dostęp do informacji niejawnych mogą posiadać tylko i wyłącznie osoby do tego upoważnione. Jako upoważnienie w tym kontekście należy rozumieć uzyskanie od właściwych organów państwa poświadczenia bezpieczeństwa (informacje narodowe) i/lub certyfikatu (informacje sojusznicze) uprawniającego do dostępu do informacji niejawnych o określonej klauzuli tajności. Poświadczenie stanowi zatem swego rodzaju rękojmię dającą zapewnienie, że każda osoba, której jej udzielono jest gwarantem zachowania i spełnienia atrybutów bezpieczeństwa informacji.

[147] Ustawa „O ochronie informacji niejawnych", op. cit. §12

Przy założeniu, że w podlegającej ocenie sieci teletransmisyjnej dywizji zmechanizowanej maksymalny poziom przesyłanych w niej informacji obwarowany jest klauzulą „Tajne", każda osoba, której nadaje się odpowiednie uprawnienia do pracy w niej musi posiadać poświadczenie o tej lub wyższej klauzuli.

Z przeprowadzonej w rozdziale drugim analizy oraz przyjętych założeń wynika, że w rozpatrywanej strukturze organizacyjnej (rys. 2.5.2) występuje jedynie personel techniczny oraz osoby funkcyjne sprawujące merytoryczny nadzór nad rozwijaniem oraz prawidłową eksploatacją sieci teletransmisyjnej. W tej sytuacji zgodnie z pragmatyką kadrową stosowaną w Siłach Zbrojnych RP można wnioskować, że obie wymienione grupy przy wyznaczaniu na konkretne stanowiska w sieci teletransmisyjnej, które związane są z dostępem do informacji niejawnych spełniały warunek konieczny jakim jest posiadanie poświadczenia bezpieczeństwa osobowego.

Stąd też, jeśli jako kryterium spełnienia wymagań bezpieczeństwa informacji w obszarze personalnym, przyjęty zostanie fakt posiadania przez cały personel adekwatnego do klauzuli przesyłanych w sieci teletransmisyjnej dywizji zmechanizowanej poświadczenia bezpieczeństwa osobowego, to wówczas możemy ocenić pozytywnie bezpieczeństwo informacji w sieci teletransmisyjnej w obszarze personalnym.

Drugim obszarem, zgodnie z przyjętymi założeniami, który podlega ocenie w zakresie bezpieczeństwa informacji w sieci teletransmisyjnej dywizji zmechanizowanej są **przedsięwzięcia organizacyjno-proceduralne**. Najistotniejszym problemem w tej materii, który podnoszony był zarówno przez pracowników pionów bezpieczeństwa łączności i informatyki (uwagi dodatkowe sondażu diagnostycznego techniką ankiety) oraz cytowanych w rozdziale poprzednim ekspertów (sondaż diagnostyczny techniką wywiadu) jest szkolenie. Jest ono bowiem ostatnim, ale chyba najważniejszym ogniwem w łańcuchu polityki bezpieczeństwa (rys. 3.2.2 *Potrzeby – Świadomość – Deklaracja misji – Decyzja – Szkolenie*). Zebrane opinie nie odnoszą się do braku problematyki bezpieczeństwa informacji w procesie szkolenia, ale do systematyczności i częstotliwości jej występowania podczas różnego rodzaju zajęć. Ponadto zwrócona została również uwaga na czytelność oraz zrozumiałość procedur, które między innymi dotyczą zasad postępowania personelu sieci teletransmisyjnej w sytuacjach krytycznych.

Problematyczne, i nie do końca zgodne z uregulowaniami NATO, są zasady przydziału uprawnień dostępu do informacji niejawnych w sieci teletransmisyjnej. Jak dotychczas w systemach narodowych podstawowym w tej materii kryterium jest zajmowane stanowisko i klauzula zawarta w poświadczeniu bezpieczeństwa osobowego. Jednak tego typu podejście kłóci się ze spełnieniem wymagania dostępu do informacji prawnie chronionych na zasadzie „wiedzy koniecznej" (*ang. need to know*), gdzie w myśl rozwiązań sojuszniczych podstawowym kryterium nie jest pełniona funkcja tylko zakres kompetencji i odpowiedzialności danej osoby funkcyjnej. Drugie z cytowanych podejść w aspekcie organizacyjnym sieci teletransmisyjnej nie tylko wydaje się rozsądniejsze, ale bardziej odzwierciedla wymagania wynikające z atrybutów bezpieczeństwa informacji.

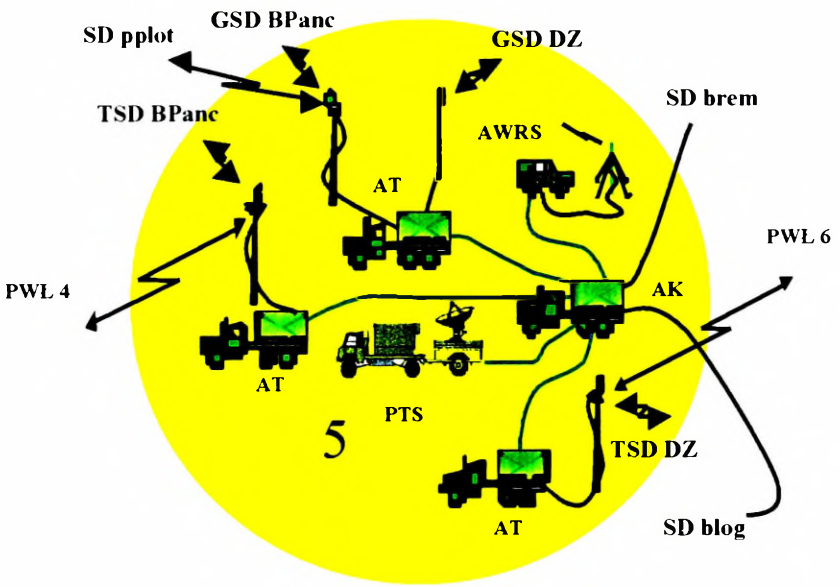
Kolejnym elementem wchodzącym w skład przedsięwzięć organizacyjno-proceduralnych mających zapewnić bezpieczeństwo informacji w sieci teletransmisyjnej jest wyznaczanie tzw. stref bezpieczeństwa, które są podstawą opracowania „planu ochrony i obrony pomocniczego węzła łączności". Jednak mówiąc o planie ochrony i obrony wchodzimy w zakres przedsięwzięć bezpieczeństwa fizycznego (warta, patrol), co jednoznacznie powinno uzmysławiać nam przenikanie się poszczególnych obszarów zapewnienia bezpieczeństwa, które dopiero w ujęciu globalnym i systemowym stanowią o systemie ochrony sieci teletransmisyjnej.

Studiując dokumentację różnych ćwiczeń i treningów sztabowych, w których następstwie nastąpiła między innymi identyfikacja rozpatrywanej aktualnej sieci, można spotkać dokładnie opracowane plany ochrony i obrony stanowisk dowodzenia i węzłów łączności je obsługujących. Marginalnie i w sposób uproszczony natomiast traktowane było, w każdej przywoływanej dokumentacji, zagadnienie ochrony pomocniczych węzłów łączności sieci teletransmisyjnej. Jeżeli już o tym problemie wspominano, to siły i środki zapewniające bezpieczeństwo sieci w rozumieniu przyjętym w ramach dysertacji pochodziły ze składu załóg aparatowni oraz urządzeń wchodzących w skład poszczególnych pomocniczych węzłów łączności.

W tej sytuacji, kiedy rozpatrujemy strukturę pojedynczego pomocniczego węzła łączności (rys. 5.2.1) ocenianej sieci teletransmisyjnej oraz uwzględniamy uwarunko-

wania techniczne i elektromagnetyczne (dyferencja) przestrzennego rozmieszczenia poszczególnych stacji nasuwa się pytanie – czy te skromne siły są wystarczające?

Analiza rozmieszczenia poszczególnych elementów węzła na określonym obszarze (około 1 km^2)[148] przy założeniu, że informacje prawnie chronione w wewnętrznej sieci strukturalnej pomocniczego węzła łączności są informacjami typu „black"[149], to pozwala stwierdzić, że cały obszar należy traktować jako strefę bezpieczeństwa klasy pierwszej.



Rys.5.2.1 Strefa bezpieczeństwa pomocniczego węzła łączności nr 5 ze struktury organizacyjnej sieci teletransmisyjnej treningu dowódczo-sztabowego pk. „Donośna Surma 2003"

Źródło: opracowanie własne na podstawie dokumentacji treningu dowódczo-sztabowego pk. „Donośna Surma 2003"

Analiza zagadnienia uwzględniająca zatem takie czynniki jak obszar, stan osobowy i uzbrojenie personelu mogącego stanowić ochronę węzła pozwala stwierdzić, że przy różnego rodzaju działaniach grup specjalnych, dywersyjnych czy nawet poddziałów rozpoznania sił przeciwnika nie jest on w stanie spełnić w pełni zadań związanych z ochroną węzła, a tym samym zapewnić bezpieczeństwa informacji w sieci teletransmisyjnej dywizji zmechanizowanej. U podstaw tak sformułowanego wniosku poza rozważaniami teoretycznymi leżą doświadczenia armii rosyjskiej[150] wyniesione z konfliktu w Afganistanie. Mowa jest tutaj o stałych przerwach w funkcjo-

[148] Materiały reklamowe firmy „TRANSBIT" nie uwzględniające standardów i wymogów aparatowni AWRS oraz PTS z rys. 5.2.1

[149] Informacje podlegające ochronie przekazywane w trybie jawnym – DBBT-701A

[150] M. Kuleba, Imperium na kolanach: wojna w Czeczenii 1994 – 1996, Bellona, Warszawa 1998, s. 117-123

nowaniu utrzymywanej przez siły rosyjskie osi radioliniowej, które były następstwem licznych ataków partyzantów afgańskich na osamotnione załogi stacji radioliniowych. Śmierć załóg i przejmowanie sprzętu łączności (w tym urządzeń ochrony kryptograficznej) przez siły afgańskie uzmysłowiło dopiero Rosjanom konieczność zmiany podejścia do problematyki ochrony poszczególnych elementów eksploatowanej osi. Wydzielenie dodatkowych sił i przydzielenie ich do ochrony stacji podniosło niezawodność funkcjonowania całej osi radioliniowej, a tym samym zapewniło spełnienie pozostałych czynników wchodzących w skład atrybutów bezpieczeństwa informacji.

Kolejnym elementem systemu ochrony, który należałoby uwzględniać w planie ochrony i obrony jest organizacja wejścia i wyjścia na obszar zdefiniowanej strefy bezpieczeństwa oraz dostęp do poszczególnych aparatowni (stacji) czy urządzeń telekomunikacyjnych węzła. W warunkach polowych, które są naturalnym środowiskiem rozwijania i eksploatacji sieci teletransmisyjnej dywizji zmechanizowanej trudno jest zorganizować system „przepustkowy" wspomagany rozwiązaniami technicznymi. Z tego można wnioskować, że podstawą uprawniającą do wejścia (wyjścia) na chroniony obszar mogą być identyfikatory (przepustki), które szeroko stosowane są podczas różnego rodzaju ćwiczeń i treningów. Jednak w czasie działań taktycznych ze względów bezpieczeństwa i nie tylko rozwiązanie to stanowi warunek konieczny, lecz nie wystarczający. Zasadniczym powodem tej konkluzji jest konieczność uwierzytelnienia (potwierdzenia) autentyczności danej osoby legitymującej się konkretnym identyfikatorem ze względu na działanie w obszarze odpowiedzialności dywizji, który można w znacznej mierze identyfikować jako zasięg i obszar działania omawianej sieci teletransmisyjnej, różnych macierzystych i nie macierzystych oddziałów oraz poddziałów dywizji czy grup wojsk przeciwnika. Sugerując pewne rozwiązania poza tymi, które wynikają z historycznych doświadczeń (hasło – odzew), weryfikacja osób pragnących mieć dostęp do elementów wrażliwych sieci teletransmisyjnej (np. urządzenia ochrony kryptograficznej) lub informacji podlegających ochronie realizowana powinna być w warunkach polowych, w oparciu o sformalizowany dokument upoważniający do wykonywania konkretnych czynności poparty potwierdzeniem tożsamości danej osoby funkcyjnej.

Reasumując prowadzone rozważania w zakresie ochrony takich elementów sieci teletransmisyjnej dywizji zmechanizowanej jak pomocnicze węzły łączności, należy stwierdzić, że problem ten nie jest właściwie doceniany zarówno przez organizatorów sieci jak i stosowne organy odpowiedzialne za bezpieczeństwo przesyłanej w niej informacji. Z tej perspektywy i w tym danym kontekście można negatywnie ocenić zespół przedsięwzięć organizacyjno-proceduralnych z elementami bezpieczeństwa fizycznego realizowanych w ramach sieci teletransmisyjnej dywizji zmechanizowanej.

Kolejnym krokiem zapewniającym kontynuację oceny sieci w odniesieniu do zagadnień związanych z bezpieczeństwem informacji, które realizowane są za pomocą **środków ochrony fizycznej** (poza omówionymi dotychczas) zasadnym jest rozpatrzenie miejsca instalacji urządzeń transmisyjnych i komutacyjnych oraz zasad ich rozmieszczenia wewnątrz tych obiektów.

Z analizy sieci teletransmisyjnej dywizji zmechanizowanej prowadzonej w rozdziale drugim, wynika między innymi konieczność zapewnienia mobilności poszczególnym elementom umożliwiającą tym samym ich okresowe przemieszczanie jak i rekonfigurację sieci zależnie od okoliczności czy warunków towarzyszących prowadzeniu przez dywizję działań bojowych. Stąd też wypływa wniosek, że każda ze stacji (AT, AK, AWRS, PTS) wchodzących w skład pomocniczego węzła łączności zamontowana jest na pojeździe kołowym lub gąsienicowym.

Przyjęcie założenia o mobilności poszczególnych typów stacji zezwala na porównanie wymagań w zakresie bezpieczeństwa fizycznego zawartych w dokumentach normatywnych[151] z praktyczną ich realizacją tzn. kontenerami, w których urządzenia są fizycznie instalowane. Prowadzona w oparciu o wymienione. dokumenty analiza wymagań poparta wynikami badań wykonanych przez właściwe komórki wojskowych służb ochrony państwa upoważnia do stwierdzenia, że obiekty (kontenery) telekomunikacyjne, w których zainstalowane są urządzenia transmisyjne, komutacyjne i inne funkcjonujące w ramach stacji lub aparatowni sieci teletransmisyjnej dywizji zmecha-

[151] Dyrektywa DBBT – 301A – Wytyczne w zakresie bezpieczeństwa fizycznego kancelarii kryptograficznych, stacji łączności kryptograficznej oraz pomieszczeń wydzielonych przeznaczonych do przetwarzania informacji niejawnej, WSI, Warszawa 2000, Decyzja nr 181 /MON Ministra Obrony Narodowej z dnia 6 października 2000 r. w sprawie organizacji szczególnej ochrony systemów i sieci teleinformatycznych w resorcie obrony narodowej

nizowanej spełniają wymagania bezpieczeństwa informacji w zakresie ochrony fizycznej.

W ramach oceny poszczególnych stacji i aparatowni wchodzących w skład pomocniczych węzłów łączności sieci teletransmisyjnej zostaną poddane ocenie przedsięwzięcia wchodzące w zakres tzw. **bezpieczeństwa technicznego**.

Pierwszą i chyba najistotniejszą płaszczyzną przedsięwzięć w tym obszarze jest **bezpieczeństwo kryptograficzne**. Procedury postępowania[152] ze środkami oraz materiałami kryptograficznymi są dziedziną najbardziej sformalizowaną pośród wszystkich dotychczas omawianych i dotyczą zarówno okresu eksploatacji jak i zasad ich przechowywania. Rygorystycznemu przestrzeganiu przepisów towarzyszy systematyczna kontrola realizowana przez organy nadrzędne.

Z tej przyczyny po analizie zaleceń zawartych w dokumentach narodowych i sojuszniczych w materii przedsięwzięć związanych z ochroną kryptograficzną można powiedzieć, że w rozpatrywanej sieci teletransmisyjnej dywizji zmechanizowanej są one wykonywane na poziomie co najmniej zadawalającym.

Opinia ta wynika z faktu, że wpływ personelu bezpieczeństwa łączności i informatyki oraz personelu technicznego szczebla dywizji ogranicza się do typowych czynności eksploatacyjnych, bowiem urządzenia utajniające stanowią integralne wyposażenie wymienionych wcześniej stacji i aparatowni. Ponadto zgodnie z przyjętym wcześniej założeniem w rozpatrywanej sieci teletransmisyjnej przesyłane są informacje do klauzuli „Tajne" włącznie i nie występuje problem połączeń systemów kryptograficznych zapewniających ochronę informacji na różnym poziomie utajniania. W przeciwnym przypadku znacznie wzrosłaby złożoność przedsięwzięć w zakresie ochrony kryptograficznej.

Zastosowane środki i metody ochrony przed zjawiskiem tzw. „**emisji ujawniającej**" w poddawanej ocenie sieci teletransmisyjnej są również zgodne i spełniają wymagania wynikające z narodowych i sojuszniczych dokumentów normatywnych. Wniosek ten można uzasadnić tym, że każdy „kontener" wraz z zainstalowanymi

---

[152] Dyrektywa BTPO – 601A – Wytyczne w zakresie postępowania z materiałami kryptograficznymi, WSI, Warszawa 2000, Dyrektywa NATO AD – 90 – 9 – Procedury w zakresie zabezpieczenia, ewidencji oraz zaopatrywania w środki i materiały kryptograficzne

w nim urządzeniami telekomunikacyjnymi pracującymi w sieci teletransmisyjnej poddawany jest badaniom kwalifikacyjnym, których celem jest określenie spełnienia wymaganych norm[153] w tym zakresie. Elementem wspomagającym ten sposób zapewnienia bezpieczeństwa informacji jest ponadto instalacja według określonych standardów oraz wymagań[154] poszczególnych urządzeń telekomunikacyjnych wewnątrz danego „kontenera" stanowiących wyposażenie aparatowni (stacji) przy uwzględnieniu jej okablowania strukturalnego i wyprowadzeń zewnętrznych. Czynności te realizowane są już na etapie produkcji tzn. jeszcze przed dopuszczeniem aparatowni do eksploatacji

w sieci teletransmisyjnej. Prowadzone już podczas pracy okresowe badania i kontrole pozwalają potwierdzić stopień spełniania określonych w stosownych dokumentach, norm i wymagań w zakresie ochrony przed niekontrolowanym „ulotem" informacji.

Następną płaszczyzną, która podlega ocenie, w ramach przedsięwzięć bezpieczeństwa technicznego jest **ochrona programowa**. Przeznaczenie, realizowane funkcje i zadania oraz struktura rozpatrywanej sieci teletransmisyjnej wskazują na znaczne ograniczenia w stosowaniu przedsięwzięć wchodzących w zakres ochrony programowej. Prezentowane stanowisko wynika bowiem z następujących przesłanek:

1. Sieć teletransmisyjna jest siecią zamkniętą tzn. liczba użytkowników ogranicza się tylko do uprawnionego personelu technicznego.
2. Sieć nie posiada galwanicznych połączeń z sieciami ogólnodostępnymi.
3. Zasadniczo oprogramowanie systemowe występuje przede wszystkim na stanowisku zarządzania, urządzeniach komutacyjnych i ochrony kryptograficznej.

Minimalna liczba osób posiadająca tzw. hasła administratora, wykonywanie określonych czynności tylko w obecności drugiego uprawnionego pracownika personelu ogranicza znacznie możliwości wprowadzania czy to oprogramowania złośliwego, czy też nieautoryzowanych zmian w oprogramowaniu systemowym i jednocześnie pozwala na szybkie zidentyfikowanie tego pracownika, który danego przedsięwzięcia

---

[153] AMSG-784, „Test procedures for tactical mobile platform", Military Committee, Brussels 1992

[154] BTPO – 701A „Wytyczne w zakresie instalacji urządzeń przeznaczonych do przetwarzania informacji niejawnych", WSI, Warszawa 2000

dokonał. Z tej też przyczyny sądzić można, że poziom zastosowanych środków i metod ochrony jest wystarczający, choć nie można jednoznacznie zanegować możliwości wystąpienia różnych incydentów w tej płaszczyźnie.

Jako kolejne ocenie poddane będą przedsięwzięcia w zakresie **technicznego wsparcia ochrony fizycznej.** Zarówno eksperci w sondażu diagnostycznym techniką wywiadu jak i wyniki uzyskane techniką ankiety zdają się potwierdzać ich marginalność w kontekście rozpatrywanej sieci teletransmisyjnej dywizji zmechanizowanej oraz w ujęciu szerszym - jak wojskowe polowe systemy telekomunikacyjne. Przytaczany już wcześniej brak możliwości lub może bardziej niecelowość budowy elektronicznego systemu przepustkowego w rejonie obszaru chronionego oraz instalowanie systemów antywłamaniowych czy przeciwpożarowych w poszczególnych aparatowniach i stacjach pomocniczych węzłów łączności wchodzących w skład sieci przy założeniu ciągłości ich pracy (tryb dyżurowy) stanowią żywy dowód, że tego typu myślenie czy rozwiązania odnoszą się i są stosowne dla systemów, sieci stacjonarnych – nie tylko wojskowych.

W sieci teletransmisyjnej rozwijanej na potrzeby walczącej dywizji przedsięwzięciem technicznym sprzyjającym utrzymaniu bezpieczeństwa przekazywanej informacji oraz po części wspierającym bezpieczeństwo fizyczne wydaje się być system sygnalizacyjny bądź ostrzegawczy. Jego istota polegałaby na natychmiastowym, równoległym przesłaniu sygnału alarmowego o zaistniałym zagrożeniu (np. atak wojsk nieprzyjaciela lub nawet możliwość przejęcia danej aparatowni czy stacji) do stanowiska zarządzania pomocniczym węzłem łączności jak i całej sieci teletransmisyjnej. Realizacja tego przedsięwzięcia musi być mało skomplikowana i przede wszystkim nie czasochłonna. Za przykład technicznego rozwiązania w tym wypadku posłużyć może sposób „zerowania" (kasowania pamięci) urządzeń ochrony kryptograficznej.

Oceniane do tej pory metody i środki oraz realizowane przedsięwzięcia w zakresie zapewnienia bezpieczeństwa informacji w sieci teletransmisyjnej dywizji zmechanizowanej skupiały się przede wszystkim na czynniku ludzkim i sprzętowym. Jeśli natomiast mówimy o bezpieczeństwie transmisji to odnosimy się do informacji, która w zależności od środka transmisyjnego przekazywana jest w postaci sygnału elektrycznego, świetlnego czy fali elektromagnetycznej.

Warunkiem umożliwiającym przeprowadzenie rzeczowej oceny bezpieczeństwa transmisji w rozpatrywanej sieci jest porównanie wymagań ze stosowanymi w tym zakresie środkami i metodami ochrony. Jednak w narodowych dokumentach normatywnych oraz wytycznych obowiązujących w dziedzinie bezpieczeństwa informacji takie wymagania nie zostały sprecyzowane. W dokumentach sojuszniczych[155] natomiast bezpieczeństwo transmisji traktowane jest jako zespół przedsięwzięć mających na celu ochronę informacji przed innymi niż kryptograficzne metodami i środkami jej pozyskania. Przy czym zwraca się jednocześnie uwagę, że odnosi się to tylko do przekazywania informacji za pomocą środków radiowych.

W oparciu o cytowany powyżej dokument oraz zakładając, że informacja nie chroniona środkami kryptograficznymi występuje w sieci teletransmisyjnej tylko w wydzielonych strefach bezpieczeństwa, gdzie stosowane są inne środki i metody jej ochrony, można stwierdzić, że utrata atrybutów bezpieczeństwa informacji i jej ewentualne pozyskanie przez potencjalnego przeciwnika jest niemożliwe. Założenie powyższe w tym przypadku rozciągnięte zostało na pozostałe środki transmisyjne występujące w omawianej sieci.

Poddając analizie zarządzanie bezpieczeństwem, które jest kolejnym punktem zawartości „Szczególnych wymagań bezpieczeństwa" sieci teletransmisyjnej, można stwierdzić, iż za ten obszar odpowiedzialny jest etatowy personel bezpieczeństwa łączności i informatyki szczebla dywizji zmechanizowanej. Prowadzone przez nich ciągłe monitorowanie systemu bezpieczeństwa eksploatowanej sieci teletransmisyjnej pozwala działać wyprzedzająco lub reagować natychmiast na wszelkie zaistniałe w systemie ochrony incydenty i zdarzenia, czego efektem jest utrzymanie wymaganego poziomu bezpieczeństwa. W ich gestii jest prowadzenie dokumentacji związanej z bezpieczeństwem sieci oraz opracowywanie i aktualizacja procedur postępowania w sytuacjach krytycznych.

Przeprowadzona analiza zawartości dokumentacji ćwiczenia pk. „Donośna Surma" pozwala na sformułowanie twierdzenia, że wszystkie wymienione czynności zostały rzetelnie i sumiennie zrealizowane i w tym konkretnym przypadku spełniły wymagania bezpieczeństwa informacji w sieci teletransmisyjnej ćwiczącej dywizji.

---

[155] MC-322, Transmission security, Military Committee, Brussels 1992

W treściach zawartych w części odnoszącej się do ogólnych zasad instalacji urządzeń pracujących w strukturze sieci teletransmisyjnej zawarty został wyciąg i odniesienie do wspomnianej już uprzednio dyrektywy „Wytyczne w zakresie instalacji urządzeń przeznaczonych do przetwarzania informacji niejawnych", których praktyczne stosowanie potwierdzone zostało w trakcie prowadzenia przez personel bezpieczeństwa kontroli konfiguracji sieci. Zezwala to na pozytywną jej ocenę w tym aspekcie bezpieczeństwa informacji w poddawanej ocenie sieci teletransmisyjnej dywizji zmechanizowanej.

W ostatnim punkcie „Szczególnych wymagań bezpieczeństwa" zawarte być powinny wymagania i zasady dowiązywania sieci teletransmisyjnej dywizji zmechanizowanej z innymi sieciami lub systemami łączności i informatyki. Wymaganie powyższe staje się rzeczowe w przypadku, gdy wymagane jest galwaniczne połączenie systemów lub sieci przesyłających informacje o różnych klauzulach tajności. W omawianym przypadku zgodnie z przyjętym założeniem problem dotyczy tylko jednego poziomu niejawności informacji oznaczonej klauzulą „Tajne". Założenie powyższe jest słuszne w przypadku, gdy dołączone sieci lub systemy spełniają te same przynajmniej na tym samym poziomie wymagania bezpieczeństwa co analizowana sieć teletransmisyjna dywizji zmechanizowanej.

Przeprowadzona analiza treści zawartych w „Szczególnych wymaganiach bezpieczeństwa" zdaje się potwierdzać praktyczną realizację przytaczanych punkt po punkcie przedsięwzięć wchodzących w skład systemu ochrony bezpieczeństwa informacji badanej sieci teletransmisyjnej. Przyjęte na tej podstawie stanowisko umożliwia jednoczesne wyprowadzenie wniosku, że zastosowane środki i metody ochrony informacji wspomagane rozwiązaniami organizacyjno-eksploatacyjnymi pozwalają uważać rozpatrywaną sieć teletransmisyjną dywizji zmechanizowanej w badanym obszarze za bezpieczną.

Opinia ta pokrywa się ze zdaniem wyrażonym przez ekspertów (załącznik nr 5), którzy na zadane pytanie – „Jak oceniają poziom bezpieczeństwa informacji w wojskowych polowych systemach telekomunikacyjnych?" stwierdzili, że bezpieczeństwo informacji wytwarzanej, przetwarzanej, przechowywanej lub przesyłanej w wojsko-

wych mobilnych systemach telekomunikacyjnych jest zapewnione na wysokim poziomie przy zachowaniu i spełnieniu standardów i wymogów NATO.

Jednak mimo pozytywnie sformułowanej i potwierdzonej przez ekspertów opinii podczas prowadzonej analizy i oceny bezpieczeństwa informacji można było zauważyć pewne elementy, których wdrożenie, zastosowanie czy zaniechanie w badanym systemie ochrony nasuwa pewne spostrzeżenia i uwagi. Pierwszą i chyba najbardziej zasadniczą jest sam wymóg opracowania i zatwierdzenia „Szczególnych wymagań bezpieczeństwa" jeszcze przed oddaniem sieci do eksploatacji. Z praktycznego punktu widzenia takie rozwiązanie zarówno w okresie kryzysu jak i prowadzenia walki zbrojnej na każdym szczeblu dowodzenia jest fizycznie niemożliwe. Odnosząc się bowiem tylko do obszaru rozważań niniejszej dysertacji można stwierdzić, że nie można w sposób jednoznaczny i zawczasu określić struktury, organizacji oraz uwarunkowań (środowiska) funkcjonowania sieci teletransmisyjnej dywizji zmechanizowanej podczas prowadzenia przez nią działań taktycznych, szczególnie jeśli nie jest to początkowy tylko kolejny etap walki. Zatem można przyjąć, że obszar pokrywany przez pierwsze cztery punkty „Szczególnych wymagań bezpieczeństwa" jest adekwatny i powinien odnosić się do systemów stacjonarnych, a nie mobilnych, gdzie występuje stała zmienność czynników determinujących ich funkcjonowanie.

Podobne jak nie identyczne sformułowanie można odnieść do drugiego z wymaganych dokumentów – „Procedur bezpieczeństwa". Nie sposób, w systemie polowym przypisać na stałe użytkowników sieci bądź systemu, gdyż coraz częściej spotykamy się z pojęciem struktur zadaniowych lub wzmocnieniem danego związku taktycznego na określony etap realizacji zadania. Ponadto w warunkach ciągłego oddziaływania przeciwnika (w tym ogniowego) poza usterkami eksploatacyjnymi należy liczyć się z tzw. stratami bezpowrotnymi zarówno w ludziach jak i sprzęcie. To stawia pod znakiem zapytania konieczność zapisu numerów seryjnych wykorzystywanego sprzętu, urządzeń, itd.

Dotychczasowe rozważania i wyciągnięte wnioski upoważniają do sprecyzowania uogólnienia, z którego wynika iż:

Obowiązywanie rygoru w czasie prowadzenia działań taktycznych (walki zbrojnej) opracowywania i zatwierdzania „Szczególnych wymagań bezpieczeństwa" dla

sieci teletransmisyjnej dywizji zmechanizowanej (polowego systemu telekomunikacyjnego sił zbrojnych RP) w przedstawionej formie czyni ten przepis „martwym".

Stąd też rozsądne wydaje się odstąpienie w stosunku do sieci telekomunikacyjnych rzeczywistego pola walki zarówno od wymogu czasowego jak i przyjętej oraz stosowanej dotychczas formy opracowywania „Szczególnych wymagań bezpieczeństwa".

Wniosek ten nie ma na celu proponowania całkowitego zaniechania działań w tym obszarze, lecz podjęcie próby urealnienia tego wymogu i przystosowania do warunków i przedsięwzięć realizowanych na szczeblu taktycznym.

Przeprowadzona dotychczas analiza w zakresie struktury oraz zasad organizacji sieci teletransmisyjnej pozwala na wyprowadzenie wniosku, że podstawą określającą cel, zadania oraz strukturę i organizację sieci teletransmisyjnej jest decyzja dowódcy dywizji wyrażona w postaci rozkazu operacyjnego, w którym zawarte są ponadto uwarunkowania lokalnego i globalnego środowiska obszaru działania dywizji.

W sformułowaniu tym można łatwo zauważyć dużą zbieżność, jak również niepełne pokrywanie się pewnych elementów wynikających ze struktury i układu „Szczególnych wymagań bezpieczeństwa".

W związku z powyższym sugerowanym rozwiązaniem omawianej sytuacji, które pozwoliłoby wyeliminować przytaczane wcześniej uwagi jest zawarcie „Szczególnych wymagań bezpieczeństwa" w strukturze rozkazu operacyjnego, a dokładniej w załączniku „Łączność i informatyka", gdzie występuje już problematyka związana z bezpieczeństwem informacji.

Kolejne uwagi i spostrzeżenia, które wynikają z przeprowadzonej przez autora analizy bezpieczeństwa informacji w sieci teletransmisyjnej dywizji zmechanizowanej, obejmujące zagadnienia szczegółowe, wchodzące w zakres przedsięwzięć bezpieczeństwa personalnego, organizacyjno-proceduralnego, fizycznego i technicznego można, zawrzeć w następujących wnioskach sugerujących jednocześnie określone ich rozwiązanie:

1. *Sama świadomość, jeśli nie jest podparta ustawicznym szkoleniem czy też jasnym i klarownym tłumaczeniem obowiązujących reguł i zasad, nie zapewnia ich przestrzegania.*

2. *Przydziałowi uprawnień dostępu do informacji klasyfikowanych w sieci teletransmisyjnej dywizji zmechanizowanej dla każdej osoby funkcyjnej przyświecać powinna zasada „wiedzy koniecznej". Celem uniknięcia różnorodności interpretacyjnej tego pojęcia maksymalna klauzula informacji, jak również obszar odpowiedzialności poszczególnych osób funkcyjnych i w szerszym niż rozpatrywany – użytkowników, może zostać zawarty w karcie opisu stanowiska.*
3. *Organizacyjnemu wyznaczeniu strefy bezpieczeństwa określonej klasy (pierwsza lub druga) w ramach danego pomocniczego węzła łączności sieci teletransmisyjnej musi towarzyszyć w warunkach polowych wydzielenie odpowiednich sił i środków sprawujących jego ochronę i obronę przed ewentualnym atakiem różnego przeznaczenia wydzielonych grup wojsk przeciwnika. Istotnym jest również precyzyjne określenie zasad dostępu do obszaru chronionego - szczególnie dla osób nie stanowiących personelu zapewniającego bieżące funkcjonowanie sieci czy jej elementów składowych. Uwzględnienie tych czynników zapewni bowiem spełnienie wymaganych atrybutów bezpieczeństwa informacji w sieci teletransmisyjnej każdego związku taktycznego.*
4. *W sieci teletransmisyjnej dywizji zmechanizowanej prowadzącej działania taktyczne modyfikacji powinno ulec podejście do przedsięwzięć wchodzących w zakres technicznego wsparcia bezpieczeństwa fizycznego. Zasadniczy wpływ na tak sformułowany wniosek ma specyfika i zasady funkcjonowania sieci oraz bardziej realne zagrożenia wynikające z działania wojsk przeciwnika.*
5. *Uregulowania w formie opracowania zarówno naukowego jak i doktrynalnego wymaga problematyka bezpieczeństwa transmisji, która przy uwzględnieniu wszystkich występujących w sieci teletransmisyjnej oraz innych wojskowych systemach i sieciach środkach transmisyjnych określałaby na wzór dokumentu NATO, narodowe wymagania w tym zakresie.*

Dokonując podsumowania prowadzonych rozważań w zakresie oceny systemu ochrony zapewniającego bezpieczeństwo informacji w sieci teletransmisyjnej dywizji zmechanizowanej, można stwierdzić, że tylko systemowe podejście do omawianego

problemu uwzględniające zastosowanie wszystkich wymienionych metod, środków czy przedsięwzięć organizacyjnych, technicznych oraz eksploatacyjnych pozwala uzyskać zamierzony efekt końcowy tj. spełnienie wymagań określonych atrybutami bezpieczeństwa informacji.

Jednak opracowany i wdrożony system zabezpieczeń jest efektywny tylko i wyłącznie w odniesieniu do konkretnych uwarunkowań wewnętrznych i zewnętrznych, w których funkcjonuje dana sieć teletransmisyjna lub inny system telekomunikacyjny bądź informatyczny. Każda zmiana determinantu określającego zastosowanie tego a nie innego środka lub metody ochrony (rodzaj oraz typ zagrożenia), wymusza przeprowadzenie weryfikacji w danym aspekcie całego systemu bezpieczeństwa informacji.

Stąd też cały proces dokonywania oceny odbywał się przy założeniu stabilności organizacyjnej oraz niezmienności warunków funkcjonowania badanej sieci teletransmisyjnej dywizji zmechanizowanej.

ZAKOŃCZENIE

Przeprowadzone badania, których przedmiotem naukowego zainteresowania była ocena aktualnego stanu bezpieczeństwa informacji w sieci teletransmisyjnej dywizji zmechanizowanej, stały się dla autora polem wzmożonej i intensywnej, ale jednocześnie przynoszącej satysfakcję pracy badawczej. Pozwoliła ona doskonalić warsztat naukowy i umożliwiła podniesienie poziomu wiedzy w zakresie działań taktycznych, polowych systemów łączności i informatyki oraz problematyki związanej z szeroko rozumianym pojęciem ochrony informacji niejawnych.

Eksploracją naukową w trakcie prowadzonych badań objęto dwa zasadnicze obszary: sieć telekomunikacyjną i bezpieczeństwo informacji. Uzyskane w procesie badań wyniki w obu wymienionych obszarach stanowiły dane wyjściowe umożliwiające osiągnięcie głównego celu niniejszej dysertacji, którym jest ocena aktualnego stanu bezpieczeństwa informacji w sieci teletransmisyjnej dywizji zmechanizowanej.

Prowadzenie badań w obszarze sieci telekomunikacyjnej rozpoczęto od określenia typu i rodzaju działań prowadzonych przez związki i oddziały szczebla taktycznego. Mając na uwadze ogólny podział działań taktycznych autor przystąpił do wyodrębnienia ze struktury sieci telekomunikacyjnej rozwijanej na potrzeby systemu dowodzenia dywizji zmechanizowanej tych jej elementów, które wchodzą w skład podstawowego obiektu badań, jaki stanowi sieć teletransmisyjna. Jako czynniki determinujące zdefiniowanie samego pojęcia sieci teletransmisyjnej przyjęte zostały: rola i zadania węzłów łączności różnego przeznaczenia oraz informacja, a konkretnie to co się z nią dzieje w poszczególnych elementach sieci telekomunikacyjnej. Określenia struktury oraz organizacji zdefiniowanej sieci teletransmisyjnej dokonano na podstawie analizy dokumentacji ćwiczeń, treningów sztabowych i dowódczo-sztabowych („Opal 99", „Donośna surma 2003", „Jantar 2004", „Odra 2004") realizowanych przez narodowe związki taktyczne szczebla dywizji oraz praktycznie funkcjonującej w rzeczywistym środowisku i otoczeniu sieci teletransmisyjnej dywizji wielonarodowej pełniącej misję stabilizacyjną w Iraku. Zasadniczą bazę informacyjną autora stanowił udział w sympozjach i konferencjach naukowych oraz studiowanie licznych pu-

blikacji z tej dziedziny. Jednocześnie uzupełnieniem wiedzy, które pozwalało na uogólnienie poglądów i zajęcie rzeczowego stanowiska w rozpatrywanym aspekcie, było przedstawienie struktury sieci teletransmisyjnej związku taktycznego Bundeswehry (AUTOKO 90).

Prowadzone rozważania w obszarze cząstkowego problemu badawczego, którego celem było określenie struktury sieci teletransmisyjnej, pozwoliły na wyprowadzenie następujących wniosków:

- podstawowymi elementami sieci teletransmisyjnej są pomocnicze węzły łączności i tory teletransmisyjne zapewniające dowiązanie się do niej węzłów łączności stanowisk dowodzenia oraz innych elementów ugrupowania bojowego dywizji;
- parametrami determinującymi strukturę sieci są: rodzaj prowadzonych działań taktycznych oraz typ realizowanego przez dywizję zadania;
- preferowanym sposobem organizacji sieci jest układ mieszany (kratowy);
- najbardziej rozbudowana struktura sieci występuje podczas prowadzenia rozstrzygających działań taktycznych (obrona) przez dywizję zmechanizowaną;
- struktura wewnętrzna podstawowego elementu sieci teletransmisyjnej – pomocniczego węzła łączności uzależniona jest od ilości realizowanych przez niego linii dowiązań (torów transmisyjnych);
- poza różnicą ilościową, podstawowy sprzęt komutacyjny i teletransmisyjny każdego pomocniczego węzła łączności można uznać za jednorodny.

Przeprowadzone badania w obszarze bezpieczeństwa informacji potwierdziły w pełni kompatybilność narodowych unormowań prawnych i doktrynalnych z sojuszniczymi w tym zakresie. Kontynuując zaprezentowaną powyżej myśl, można pokusić się nawet o twierdzenie idące dalej, że niektóre z nich stanowią lustrzane odbicie dokumentów normatywnych NATO. Studiowanie i analiza dostępnej literatury przedmiotu oraz dokumentów normatywnych umożliwiło określenie wymaganych cech bezpieczeństwa informacji (poufność, integralność, dostępność, rozliczalność, autentyczność i niezawodność). Ich zapewnienie i utrzymanie zarówno na etapie planowania jak i podczas eksploatacji sieci teletransmisyjnej dywizji zmechanizowanej jest

procesem złożonym i skomplikowanym. Autor podczas prowadzenia badań tej problematyki wyizolował trzy etapy:

1. Analiza zagrożeń i wyodrębnienie tych, które mają wpływ na bezpieczeństwo informacji w sieci teletransmisyjnej dywizji zmechanizowanej.
2. Wybór odpowiednich środków i metod ochrony informacji zapewniających eliminację zidentyfikowanych wcześniej zagrożeń.
3. Opracowanie i zatwierdzenie „Szczególnych wymagań bezpieczeństwa sieci teletransmisyjnej dywizji zmechanizowanej" oraz „Procedur bezpieczeństwa".

których realizacja stanowi o uznaniu danej sieci lub systemu za bezpieczny.

Podczas prowadzenia identyfikacji zagrożeń dla bezpieczeństwa informacji wyciągnięto następujące wnioski:

- największe zagrożenie dla bezpieczeństwa informacji, w każdym systemie lub sieci przesyłającej dane za pośrednictwem technicznych środków łączności i informatyki, stanowi celowa i niecelowa działalność człowieka;
- każdy element struktury sieci teletransmisyjnej (pomocniczy węzeł łączności i linie teletransmisyjne) stanowi potencjalne źródło zagrożenia dla bezpieczeństwa informacji w aspekcie niekontrolowanego (nieautoryzowanego) wypływu podlegającej ochronie informacji.

Dokonaniu wyboru środków i metod zapewniających ochronę informacji w obszarach:

- bezpieczeństwa personalnego,
- bezpieczeństwa organizacyjno-proceduralnego,
- bezpieczeństwa fizycznego,
- bezpieczeństwa technicznego,

towarzyszyć powinna świadomość, że nie wybiórcze, lecz kompleksowe i systemowe ich zastosowanie, zapewnia realizację celu ich użycia.

Ostatni trzeci etap stanowi usystematyzowane opracowanie w formie pisemnej wszystkich zebranych w poprzednich dwóch etapach informacji uzupełnionych o dane dotyczące między innymi przeznaczenia, struktury, organizacji oraz procedur postępowania w sytuacjach krytycznych dla sieci teletransmisyjnej. Przygotowane zwarte

dokumenty nazywane są „Szczególnymi wymaganiami bezpieczeństwa" i „Procedurami bezpieczeństwa".

Zestawiając omówiony powyżej proces z wymaganiami normatywnymi autor doszedł do następującej konkluzji:

Sieć teletransmisyjną w sensie prawnym uznać można za bezpieczną, jeśli opracowane „Szczególne wymagania bezpieczeństwa" i „Procedury bezpieczeństwa" zostaną zaakceptowane jeszcze przed jej oddaniem do eksploatacji przez stosowne organy akredytacyjne Służb Ochrony Państwa, a następnie organizatorzy tej sieci wdrożą je w praktyce.

Pogłębiona wiedza, wsparta doświadczeniami i wnioskami płynącymi z przeprowadzonych badań naukowych dała autorowi merytoryczne podstawy dokonania rzeczowej oceny aktualnego stanu bezpieczeństwa informacji w sieci teletransmisyjnej dywizji zmechanizowanej, która jest jednocześnie celem głównym niniejszej rozprawy doktorskiej.

Przeprowadzona punkt po punkcie, zgodnie z zaleceniami i wytycznymi[156] w zakresie opracowywania „Szczególnych Wymagań Bezpieczeństwa" ocena bezpieczeństwa informacji w sieci teletransmisyjnej pozwala na stwierdzenie, że zastosowane w niej przedsięwzięcia w obszarach bezpieczeństwa: personalnego, organizacyjno-proceduralnego, fizycznego oraz technicznego spełniają stawiane przed nimi zadania w zakresie ochrony informacji.

Jednak pomimo uzyskania pozytywnej oceny stanu bezpieczeństwa informacji w sieci teletransmisyjnej dywizji zmechanizowanej w trakcie jej prowadzenia nasunęły się pewne uwagi i spostrzeżenia, które stały się podstawą określenia i zaproponowania nowego lub zmodyfikowanego ujęcia i podejścia do rozpatrywanych rozwiązań w obszarach bezpieczeństwa personalnego, organizacyjno-proceduralnego, fizycznego oraz technicznego.

Na szczególną uwagę w tym aspekcie zasługuje propozycja rozpatrzenia możliwości ograniczenia zawieranych treści i formy, której następstwem może być umiejscowienie „Szczególnych wymagań bezpieczeństwa" w strukturze rozkazu operacyj-

---

[156] „Metodyka opracowywania Szczególnych Wymagań Bezpieczeństwa dla systemów i sieci teleinformatycznych", Wojskowe Biuro Bezpieczeństwa Łączności i Informatyki, Warszawa 2000

nego. Ponadto wykazano konieczność zajęcia się problematyką bezpieczeństwa transmisji, która nie znalazła, zdaniem autora, właściwego dla swojego znaczenia odzwierciedlenia zarówno pośród wymagań jak i narodowych normatywów zajmujących się problematyką bezpieczeństwa informacji przesyłanej za pomocą technicznych środków łączności i informatyki.

Jednocześnie wskazano pewne obszary bezpieczeństwa informacji w sieci teletransmisyjnej, w których zmiana podejścia systemowego lub zastosowanie proponowanych rozwiązań szczegółowych umożliwiałaby podniesienie poziomu ochrony informacji.

Przeprowadzone badania wykazały rozległość obszarów prowadzonych dociekań naukowych, która wynikała przede wszystkim z wielu płaszczyzn i różnego spektrum problematyki poddanej badaniom. Dlatego też, autor, zdając sobie sprawę ze swojej niedoskonałości, pozwala sobie na stwierdzenie, że w obrębie obszarów związanych z dysertacją istnieje jeszcze wiele problemów szczegółowych wymagających bardziej dogłębnego zbadania. Zaliczyć do nich można nie tylko informatyzację urządzeń i środków teletransmisyjnych, która jest nieodłącznym elementem współczesnego rozwoju technicznego, ale również stale rosnący „popyt" i zapotrzebowanie systemu dowodzenia w zakresie obiegu informacji, co wymusza zwiększenie przepustowości torów transmisyjnych lub zwiększenie ilości sprzętu zaangażowanego w proces przekazywania informacji na odległość.

Przedstawiona w rozprawie ocena bezpieczeństwa sieci teletransmisyjnej dywizji zmechanizowanej oraz zaproponowane nowe lub modyfikujące aktualne podejście do problematyki bezpieczeństwa informacji w polowych sieciach telekomunikacyjnych wojsk lądowych nie jest zapewne rozwiązaniem ostatecznym, którego nie można poprawiać lub uzupełniać o nowe elementy. Wskazują na to wyspecyfikowane w dysertacji obszary, w których mogą i powinny być prowadzone selektywne i specjalistyczne badania w ramach nakreślonej w rozprawie problematyki zapewnienia bezpieczeństwa informacji. Pozwala ona jednak stwierdzić, iż główny problem rozprawy rozwiązany został w stopniu zapewniającym jego wiarygodność naukową. Jeśli zaproponowane w dysertacji rozwiązania problemów wchodzących w skład przedsięwzięć związanych z ochroną informacji w wojskowych polowych sieciach telekomunikacyjnych stano-

wić będą materiał pobudzający do dalszych rozważań naukowych w tym obszarze, to świadomość tego stanowić będzie powód do satysfakcji dla autora.

BIBLIOGRAFIA

1. AMSG-784, *Test procedures for tactical mobile platform*, Military Committee, Brussels 1992.
2. Anderson R.H, *Securing the U.S. Defense Information Infrastructure: A Proposed Approach*, National Defense Research Institute, RAND 1999.
3. Andrukiewicz E., *Rola polityki bezpieczeństwa w systemach i sieciach teleinformatycznych przetwarzających informacje niejawne,* IT Security Magazine nr 1, 1999.
4. *AUTOKO 90* – materiał reklamowy firmy Siemens.
5. Barczak A. i inni, *Planowanie systemu łączności*, DW Bellona, Warszawa 1999.
6. Bogusz R., *Bezpieczeństwo przetwarzania informacji: aktywna ochrona przed emisją ujawniającą*, IT Security Magazine nr 1-2, 2000.
7. Bryczkowski M., *Bezpieczeństwo systemów sieciowych,* magazyn Postępy Kryminalistyki nr 1, 1997.
8. Cendrowski J., *Ochrona informacji niejawnych w systemach i sieciach teleinformatycznych*, IT Security Magazine, cz. 1 nr 1 1999, cz.3 nr 1-2 2000, cz. 4 nr 3 2000.
9. Chrobak R. i inni, *Działania bojowe dywizji*, AON, Warszawa 2003.
10. Cieślarczyk M., Krawczyk P., Korulczyk Z., *Poradnik Metodyczny Autorów Prac Kwalifikacyjnych*, WWLiOP AON, Warszawa 2002.
11. *Cyfrowa sieć telekomunikacyjna związku taktycznego wojsk lądowych „Storczyk"* – poradnik łącznościowca, Warszawa, Sztab Generalny WP, 2002.
12. Dańczak A., Sienkiewicz P., *Bezpieczeństwo informacji w SZ RP. Aspekty strategiczne* - praca studyjna, Warszawa, AON 2002
13. Dokument NATO serii AMSG 524 – *Słownik pojęć i definicji z zakresu bezpieczeństwa łączności i informatyki.*
14. Dokumentacja ćwiczenia dowódczo-sztabowego pk. „Jantar2004".
15. Dokumentacja ćwiczenia dowódczo-sztabowego „Opal 99".
16. Dyrektywa NATO AD – 90 – 9 – *Procedury w zakresie zabezpieczenia, ewidencji oraz zaopatrywania w środki i materiały kryptograficzne*.
17. Dokumentacja ćwiczenia pk. „Donośna surma 2003".
18. Dokumentacja treningu sztabowego pk. „Odra 2004".
19. *Dyrektywa bezpieczeństwa* AD-70-1-PL, WSI, Warszawa 1997.

20. *Encyklopedia popularna PWN*, Warszawa 1982.

21. Fiołna Z., Daniluk P. *Koncepcja sieci łączności wojsk lądowych w działaniach taktycznych perspektywicznego pola walki* – praca naukowo-badawcza pk. „KROS", AON, Warszawa 2001.

22. Fiołna Z., *Organizacja taktycznych sieci łączności* – materiały z sympozjum naukowego, AON, Warszawa 2001

23. Fiołna Z., Daniluk P., *Koncepcja struktur organizacyjno-technicznych taktycznych sieci łączności wojsk lądowych. Struktura organizacyjno-techniczna sieci łączności dywizji*, pk. „Kros-2.2", AON, Warszawa 2002.

24. Gałach A., Szczypiorski K., *Bezpieczeństwo systemów teleinformatycznych*, CITCOM PW, Warszawa 2002.

25. Globan-Klaus T., Sienkiewicz P., *Społeczeństwo informacyjne: szanse, zagrożenia, wyzwania*, Wydawnictwo Fundacji Postępu Telekomunikacji, Kraków 1999.

26. Griffith J., *C^4ISR Handbook for Integrated Planning*, Department of Defense, Washington 1998.

27. Huzarski M. i inni, *Aspekty narodowe i sojusznicze w teorii taktyki ogólnej wojsk lądowych* - pk. „Garda", AON, Warszawa 2000.

28. Huzarski M. i inni, *Taktyka ogólna wojsk lądowych,* AON, Warszawa 2001.

29. Huzarski M., *Zagadnienia taktyki wojsk lądowych*, A. Marszałek, Toruń 1999.

30. Icove D., Seger K., von Storch, *A Crimefighter Handbook*, O'Reilly&Associates, Arkansas 1991.

31. Janczak J., Daniluk P., Wisz A., *Kierowanie mobilnymi systemami łączności wojsk lądowych* – cz. 3, AON, Warszawa 2002.

32. Janczak J. i inni, *Mobilne sieci łączności – album schematów*, AON, Warszawa 2003.

33. Kopaliński W., *Słownik wyrazów obcych i zwrotów obcojęzycznych,* Wiedza Powszechna, Warszawa, 1983.

34. Kowalewski M., *System łączności dywizji* - rozprawa habilitacyjna, AON, Warszawa 1994.

35. Koziej S., *Teoria walki zbrojnej*, AON, Warszawa 1993.

36. Kręcikij J., *Współczesne kierowanie wojskami. Proces dowodzenia*, AON, Warszawa 2002.

37. *Kryteria oceny bezpieczeństwa systemów łączności i informatyki* - praca zbiorowa, SWŁiI SG WP, Warszawa 1996.

38. Kukawski A., *Zasady rozmieszczania, przemieszczania i obrona węzłów łączności*, ASG WP, Warszawa 1986.

39. Kuleba M., *Imperium na kolanach: wojna w Czeczenii 1994 – 1996*, Bellona, Warszawa 1998.

40. Kupisiewicz Cz., *Podstawy dydaktyki ogólnej*, PWN, Warszawa 1976.

41. Lidwa W., *Przemieszczanie wojsk*, AON, Warszawa 1995.

42. *Leksykon naukowo-techniczny*, WNT, Warszawa 1984.

43. Lenert M., Smakulski E., *Model systemu łączności korpusu wojsk lądowych*, AON, Warszawa 1993.

44. Majewski W., *Teletransmisyjne systemy cyfrowe*, Wydawnictwo Komunikacji i Łączności, Warszawa 1976

45. Mazurkiewicz J., Kulma W., *System dowodzenia i łączności związku taktycznego*, AON, Warszawa 1996.

46. Mazurkiewicz J., *Leksykon łączności*, AON, Warszawa 1994.

47. Mąka D., *Ryzyko w systemie bezpieczeństwa informacyjnego państwa w aspekcie standardów NATO i Unii Europejskiej* – rozprawa doktorska, AON, Warszawa 2004.

48. Mąka D., *Elementy zagrożeń i zarządzania ryzykiem w świetle polityki bezpieczeństwa informacyjnego*, IT Security Magazine nr 8-9, 2001.

49. *Metodyka opracowania Szczególnych Wymagań Bezpieczeństwa systemu lub sieci teleinformatycznej*, Wojskowe Biuro Bezpieczeństwa Łączności i Informatyki, Warszawa 2000.

50. Michniak J., *Kompendium łączności,* AON, Warszawa 1992.

51. Michniak J., Wisz A., *Bezpieczeństwo i ochrona informacji w wojskowych sieciach telekomunikacyjnych i zautomatyzowanych systemach dowodzenia*, AON, Warszawa 2000.

52. Michniak J., *Dowodzenie i łączność*, AON, Warszawa 2004.

53. Michniak J., *Kierowanie mobilnymi systemami łączności wojsk lądowych* - cz. 1, Główne problemy, AON, Warszawa 2003.

54. Michniak J., *Model organizacyjny polowej sieci łączności związku taktycznego w latach 1995-2005*, AON, Warszawa 1995.

55. Michniak J., *Koncepcja systemów łączności związku operacyjnego, związku taktycznego i oddziału* – praca naukowo-badawcza pk. „System", AON, Warszawa 1995.

56. Michniak J. i inni, *Bezpieczeństwo i ochrona informacji w sieciach łączności i informatyki wojskowej w okresie pokoju, kryzysu i wojny* – praca naukowo-badawcza pk. „OCHRONA", AON, Warszawa 2004.

57. *Multimedialna encyklopedia* PWN.

58. *Myśl Wojskowa* - Bellona, Warszawa, Listopad-Grudzień 2002, 6(623).

59. Nowicki W., *Glosarium telekomunikacji* - zalecane terminy, ich definicje, odpowiedniki obcojęzyczne, komentarze, zeszyt 2, Biuletyn informacyjny nr 2-3 (276-277) IŁ, Warszawa-Międzeszyn, 1990.

60. Nowicki W., *Glosarium Telekomunikacji*, Zeszyt 1, Instrytut Łączności, Warszawa 1991.

61. *Ochrona informacji niejawnych – zbiór dokumentów normatywnych*, Wojskowe Biuro Bezpieczeństwa Łączności i Informatyki, Łączn. Wewn. S4/2002, Warszawa 2002.

62. Piedziuk E., *Słownik pojęć z zakresu telekomunikacji*, AON, Warszawa 1997.

63. Pieter J., *Zarys metodologii pracy naukowej*, PWN, Warszawa 1975.

64. Piotrkiewicz E., *Leksykon wiedzy wojskowej*, ASG WP, Warszawa 1985.

65. Pipkin D., *Bezpieczeństwo informacji : ochrona globalnego przedsiębiorstwa*, WNT, Warszawa 2002.

66. Plewko K., *Biuletyn informacyjny* 2-3, Instytut Łączności, Warszawa 1990.

67. Pohorecki G., *Zarządzanie bezpieczeństwem systemów teleinformatycznych według Polskiej Normy PN-1-13335*, IT Security Magazine nr 1, 1999.

68. *Polowy system łączności cyfrowej „STORCZYK 2000"* - materiały reklamowe firmy „Transbit".

69. *Przepisy bezpieczeństwa łączności i eksploatacji oraz ochrony informacji w podsystemie cyfrowej łączności utajnionej SZ RP*, SWŁiI, Warszawa 1996.

70. *Projektowanie, budowa oraz rozwijanie stacji łączności utajnionej stacjonarnych i polowych węzłów łączności* – Szefostwo Wojsk Łączności sygn. Łączn. 624/76.

71. Prezentacja *Das Automatisierte Kommunikationsnetz* (derzeit: AUTOKO 90).

72. Regulamin DWLąd, Warszawa 1991.

73. Robling Denning D., *Kryptografia i ochrona danych*, WNT, Warszawa1993.

74. Sadowski A., *Czym jest polityka bezpieczeństwa organizacji,* www.bezpieczeństwoit.pl .

75. Security within NATO C-M(55) 15 (Final), NATO HQ, Brussels 1990.

76. *Słownik Języka Polskiego* - PWN, Warszawa 1978.

77. *Słownik języka polskiego*, PWN, Warszawa 2000.

78. Stachowiak Z., *Metodyka i metodologia pisania prac kwalifikacyjnych*, AON, Warszawa 2001.

79. Stokłosa J., *Bezpieczeństwo danych w systemach informatycznych*, Wydawnictwo Naukowe PWN, Warszawa – Poznań 2001.

80. *Strategia Bezpieczeństwa RP* – z dnia 04.01.2000.

81. *Strategia Obronności RP* – z dnia 23.05.2000.

82. Strzoda M., Prusiński N., *System dowodzenia. Terminologia* cz. 1, AON, Warszawa 2002.

83. *Systemy telekomunikacyjne i informatyczne* – terminologia, Norma Obronna, NO-01-A003.

84. Swanson M., Guttman B., *Generally Accepted Principles and Practices for Securing Information Technology Systems*, NIST, SP 800-14, September 1996.

85. Szeżyńska M., *Bezpieczeństwo informacji* - konspekt wykładu, Instytut Systemów Elektronicznych Politechniki Warszawskiej, Warszawa 2002.

86. Ścibiorek Z., O*brona związku taktycznego (oddziału)*, AON, Warszawa 1993.

87. Ścibiorek Z., *Główne problemy natarcia*, AON, Warszawa 1993.

88. Ścibiorek Z., *Działania opóźniające*, AON, Warszawa 1996.

89. Ścibiorek Z., Lidwa W., *Działania obronno-opóźniające w przygranicznym pasie przesłaniania*, AON, Warszawa 1999.

90. Świdzikowski G., *Bezpieczeństwo informacji w mobilnych systemach telekomunikacyjnych* - materiały pokonferencyjne – załącznik - prezentacje, AON, Warszawa 2004.

91. Topulos A., *Ilustrowany leksykon techniczny*, Wydawnictwo Naukowo-techniczne, Warszawa 1983.

92. *Tymczasowe zasady organizacji, funkcjonowania i bezpieczeństwa łączności utajnionej w SZ RP* – Szefostwo Wojsk Łączności sygn. Łączn. 988/88.

93. *Transmission security* – MC-322, NATO HQ, Brussells 1992.

94. Wiśniewski E., *Metodyka wojskowych badań naukowych*, ASG WP, Warszawa 1988.

95. Wróblewski R., *Podstawowe pojęcia z dziedziny polityki bezpieczeństwa, strategii i sztuki wojennej*, AON, Warszawa 1999.

96. Ura E., *Prawo telekomunikacyjne – komentarz*, Wydawnictwo Prawnicze, Warszawa 2001.

97. *Wytyczne w zakresie bezpieczeństwa fizycznego kancelarii kryptograficznych, stacji łączności kryptograficznej oraz pomieszczeń wydzielonych przeznaczonych do przetwarzania informacji niejawnej* - DBBT – 301A.

98. *Wytyczne w zakresie instalacji urządzeń przeznaczonych do przetwarzania informacji niejawnych* - BTPO – 701A.

99. *Wytyczne w zakresie postępowania z materiałami kryptograficznymi* - BTPO – 601A .

DOKUMENTY NORMATYWNE

100. Ustawa z dnia 22 stycznia 1999 roku o ochronie informacji niejawnych.- Dz. U. 1999. Nr 11, poz. 95.

101. Rozporządzenie Prezesa Rady Ministrów z dnia 25 lutego 1999 roku w sprawie podstawowych wymagań bezpieczeństwa systemów i sieci teleinformatycznych.- Dz. U. 1999 r. Nr 18, poz. 162.

102. Decyzja Ministra Obrony Narodowej Nr 10/MON z dnia 18 stycznia 1999 roku w sprawie wdrożenia w resorcie obrony narodowej zasad i przepisów regulujących problematykę bezpieczeństwa teleinformacyjnego w relacjach międzysojuszniczych.

103. Decyzja Ministra Obrony Narodowej Nr 181/MON z dnia6 października 2000 roku w sprawie organizacji szczególnej ochrony systemów i sieci teleinformatycznych w resorcie obrony narodowej.

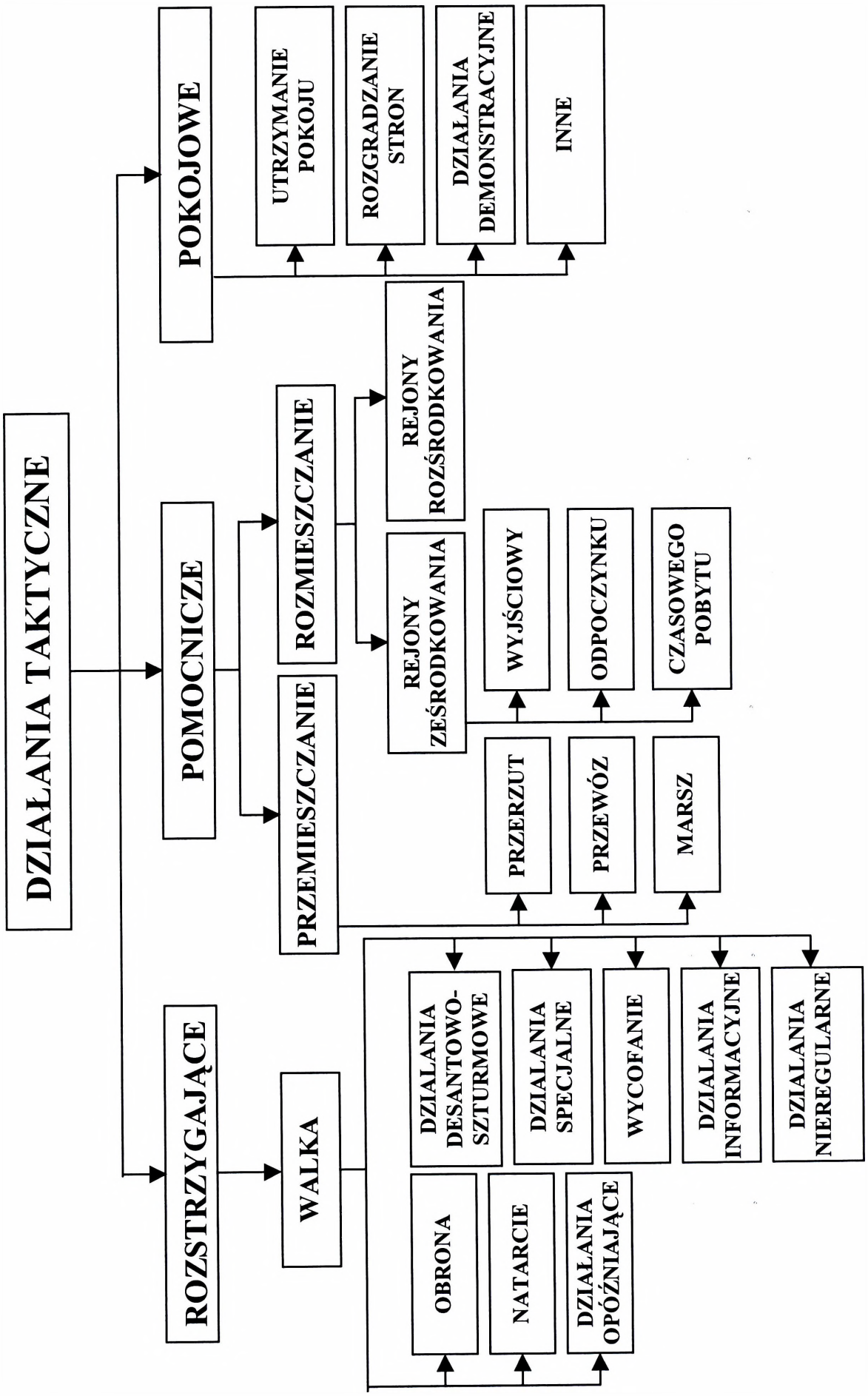
104. Decyzja Ministra Obrony Narodowej Nr 29/MON z dnia 22 lutego 2001 roku w sprawie trybu certyfikacji i kontroli kancelarii zagranicznych, kancelarii środków i materiałów kryptograficznych, punktów obsługi dokumentów zagranicznych, stacji łączności kryptograficznej oraz pomieszczeń wydzielonych (terminali) teleinformatycznych w jednostkach organizacyjnych resortu obrony narodowej.

105. Decyzja Ministra Obrony Narodowej Nr 80/MON z dnia 10 maja 2001 roku zmieniająca decyzją w sprawie powołania pełnomocników do spraw ochrony informacji niejawnych, administratorów systemów i sieci teleinformatycznych oraz utworzenia pionów ochrony w jednostkach organizacyjnych resortu obrony narodowej.

106. Zarządzenia Szefa Sztabu Generalnego z dnia 26 stycznia 2000 roku w sprawie opracowywania Szczególnych Wymagań Bezpieczeństwa dla systemów i sieci teleinformatycznych. Rozporządzenie Ministrów Spraw Wewnętrznych i Administracji oraz Obrony Narodowej z dnia 26 lutego 1999 roku w sprawie trybu i sposobu przyjmowania, przewożenia, wydawania i ochrony materiałów.- Dz. U. 1999 r. Nr 18, poz. 168.

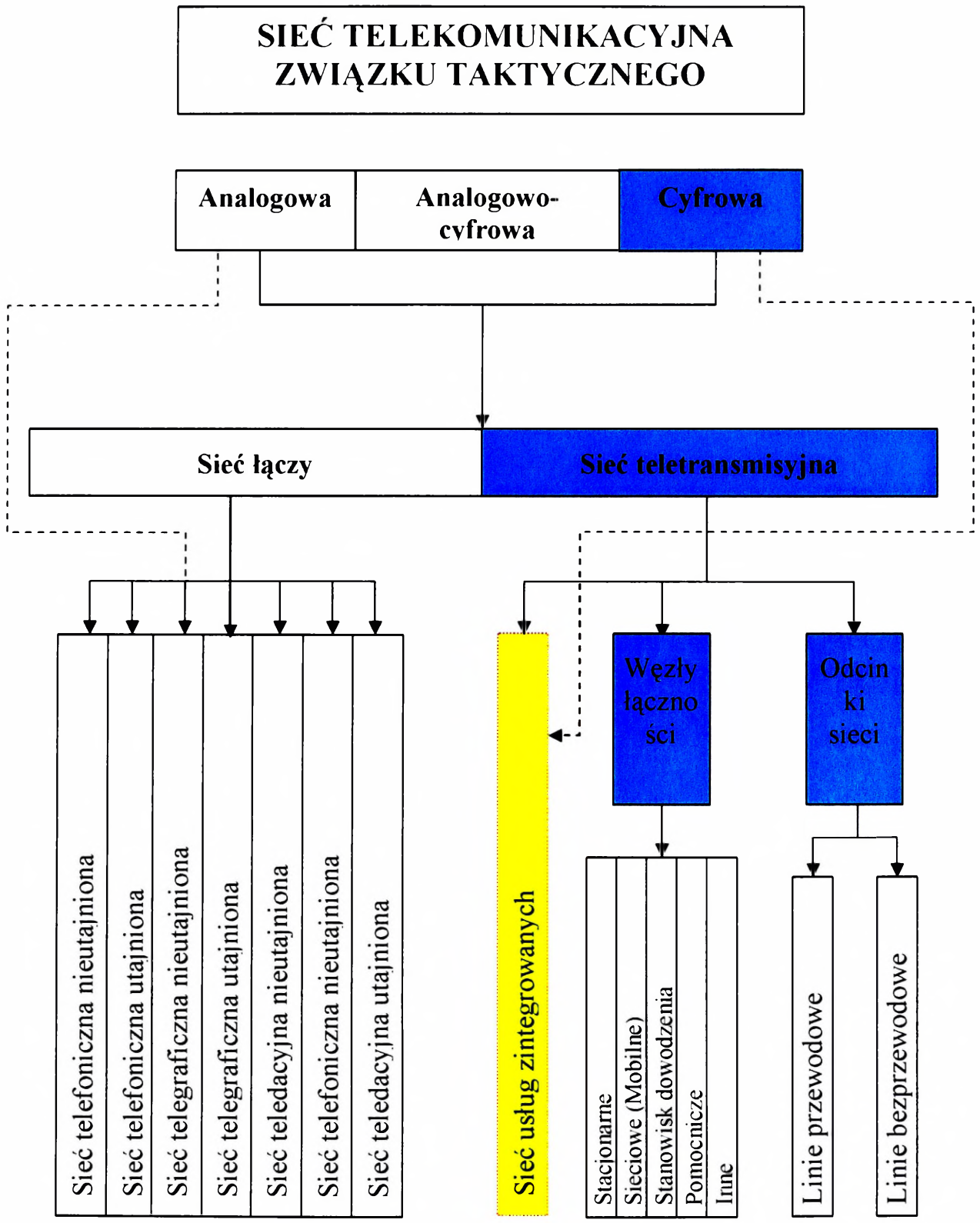
Załącznik nr 1

DZIAŁANIA TAKTYCZNE



Źródło: Huzarski M. i inni, „Taktyka ogólna wojsk lądowych", AON, Warszawa 2001.

SIEĆ TELEKOMUNIKACYJNA ZWIĄZKU TAKTYCZNEGO



Źródło: Mazurkiewicz J., Kulma W., *„System dowodzenia i łączności związku taktycznego"*, AON, Warszawa 1996.

AKADEMIA OBRONY NARODOWEJ

WYDZIAŁ WOJSK LĄDOWYCH

ARKUSZ OBSERWACJI

ĆWICZEŃ WOJSKOWYCH Z DOWÓDZTWAMI I WOJSKAMI W ASPEKCIE STRUKTURY I ORGANIZACJI SIECI TELETRANSMISYJNEJ DYWIZJI ZMECHANIZOWANEJ

Warszawa **2004**

1. TEMAT BADAŃ: Struktura i organizacja sieci teletransmisyjnej dywizji zmechanizowanej.
2. METODA BADAWCZA: Obserwacja niestandaryzowana zewnętrzna.
3. CEL BADAŃ: Określić strukturę i organizację sieci teletransmisyjnej dywizji zmechanizowanej oraz zidentyfikować przedsięwzięcia związane z ochroną informacji.
4. CZAS BADAŃ: Luty 2003 – grudzień 2004
5. OPIS PRZEBIEGU BADAŃ: Badanie przeprowadzono metodą obserwacji niestandaryzowanej zewnętrznej podczas ćwiczeń:
   - ❖ prowadzonych w Akademii Obrony Narodowej – dowódczo-sztabowego (szkieletowego);
   - ❖ prowadzonych w wojskach operacyjnych – dowódczo-sztabowego w 1, 11 i 12 Dywizji Zmechanizowanej.

Badaniami objęto działanie komórek organizacyjnych dywizji odpowiedzialnych za przygotowanie i organizację systemu łączności w czasie prowadzenia działań na szczeblu taktycznym. Badania prowadzono mając możliwość stałego kontaktu z ćwiczącymi na poszczególnych stanowiskach funkcyjnych określonych powyżej zespołów stanowiska dowodzenia. Pozwoliło to na wymianę poglądów z oficerami wykonującymi zadania w poszczególnych obszarach planowania, organizacji i nadzoru nad funkcjonowaniem systemu łączności oraz przedsięwzięć związanych z bezpieczeństwem przesyłanej informacji. Obserwacja niestandaryzowana jest szczególnie przydatna w badaniach eksploracyjnych (poszukujących) bowiem jej zasadniczym celem jest uzyskanie odpowiedzi w zakresie stanu aktualnego bez przyjmowania jakichkolwiek hipotez. Obserwator ma szeroki zakres pola badawczego. Brak karty obserwacji czy też innego środka standaryzacji daje większe możliwości na twórcze poszukiwanie rozwiązań szczegółowych.

W oparciu o wyniki prowadzonej obserwacji można sformułować w odniesieniu do problematyki organizacji i struktury sieci teletransmisyjnej oraz realizowanych przedsięwzięć związanych z ochroną informacji następujące wnioski:

1. Podstawowymi elementami sieci teletransmisyjnej szczebla dywizji zmechanizowanej są pomocnicze węzły łączności oraz linie telekomunikacyjne (międzywęzłowe oraz dowiązania).
2. Struktura sieci oraz ilość pomocniczych węzłów łączności uzależniona jest od:
   - zadania jakie ma realizować dana dywizja;
   - wytycznych i ograniczeń narzuconych przez przełożonego;
   - uwarunkowań terenu działania i zakładanych możliwości oddziaływania przeciwnika;
   - etatowego wyposażenia w środki teletransmisyjne.
3. Międzywęzłowe linie telekomunikacyjne realizowane są w oparciu o środki radioliniowe.
4. Linie telekomunikacyjne zapewniające dowiązanie się do sieci teletransmisyjnej poszczególnych elementów ugrupowania bojowego dywizji budowane są za pomocą środków radioliniowych oraz przewodowych.
5. Dla każdej organizowanej sieci teletransmisyjnej przeznaczonej do przesyłania informacji niejawnych opracowane i zatwierdzone zostały przed rozpoczęciem treningu lub ćwiczenia (30 dni) „Szczególne wymagania bezpieczeństwa" oraz „Procedury bezpieczeństwa", w ramach których zdefiniowane zostały wszelkie obszary i przedsięwzięcia związane z ochroną przekazywanych informacji.
6. Podejmowane przedsięwzięcia w zakresie zapewnienia bezpieczeństwa informacji obejmowały obszary:
   - bezpieczeństwa personalnego;
   - bezpieczeństwa fizycznego;
   - bezpieczeństwa technicznego;
   - bezpieczeństwa organizacyjno-proceduralnego.

sie Obserwację zewnętrzną zastosowano do badania wybranych problemów badawczych, szczególnie struktury organizacyjnej oraz funkcjonowania sieci teletransmisyjnej dywizji zmechanizowanej i procesu planowania przedsięwzięć związanych z ochroną informacji. Metoda obserwacji umożliwiła rozpoznanie,

wyróżnienie i ocenę sieci teletransmisyjnej dywizji oraz procesów w niej zachodzących. W jej ramach zbierano głównie wiadomości z zakresu funkcjonalności sieci, jej elementów składowych, które potencjalnie stanowią źródła niekontrolowanego (nieautoryzowanego) wypływu informacji podlegającej ochronie. Metoda ta pozwoliła również na:

- poznanie relacji i powiązań zachodzących między elementami badanego systemu a otoczeniem;
- kompleksowe ujęcie wszystkich elementów zachodzących procesów i występujących między nimi powiązań i zależności;
- ukierunkowanie działalności badawczej przy opracowywaniu oceny bezpieczeństwa informacji w sieci teletransmisyjnej dywizji zmechanizowanej.

Przedmiot obserwacji w kontekście rozważanych problemów stanowiły następujące ćwiczenia i treningi dowódczo-sztabowe (z udziałem i bez udziału wojsk), które opatrzone zostały kryptonimami: „Opal 99"; „Akademicki pierścień 2003"; oraz sieć teletransmisyjna dywizji wielonarodowej biorącej udział w misji stabilizacyjnej PKW w Iraku[1].

[1] Organizacja i funkcjonowanie sieci teletransmisyjnej rozwiniętej w Iraku były m.in. przedstawiane w ramach konferencji międzynarodowej zorganizowanej przez Instytut Zarządzania i Dowodzenia „Łączność w operacjach reagowania kryzysowego" w październiku 2003r.

AKADEMIA OBRONY NARODOWEJ

WYDZIAŁ WOJSK LĄDOWYCH

KWESTIONARIUSZ ANKIETY

Dla pracowników organów bezpieczeństwa łączności i informatyki jednostek wojskowych podległych Dowództwu Wojsk Lądowych oraz jednostek organizacyjnych szczebla centralnego Ministerstwa Obrony Narodowej

Wydział Wojsk Lądowych Akademii Obrony Narodowej prowadzi badania naukowe w zakresie problematyki bezpieczeństwa informacji w mobilnych systemach telekomunikacyjnych wojsk lądowych.

Celem badań jest ustalenie najbardziej wrażliwych elementów bądź struktury systemu telekomunikacyjnego szczebla taktycznego, które wnoszą największe zagrożenia utraty bezpieczeństwa informacji wytwarzanej, przetwarzanej, przechowywanej lub przesyłanej w tym systemie.

W związku z powyższym, zwracamy się do Pana z prośbą o udział w badaniach poprzez wypełnienie niniejszego kwestionariusza ankiety. Jej wypełnienie polega na uważnym przeczytaniu pytania zasadniczego oraz wybraniu i zaznaczeniu jednej odpowiedzi w każdym z poszczególnych zaproponowanych aspektów ochrony informacji w systemach telekomunikacyjnych. Proszę również o ewentualne wpisanie tych zagrożeń, które Pana zdaniem są istotne, a nie zostały uwzględnione w poszczególnych obszarach ochrony informacji.

Materiał uzyskany w toku badań będzie przedmiotem analiz naukowych, a po opracowaniu będzie podstawą doskonalenia procesu, wypracowania niezbędnych rozwiązań i wprowadzenia ewentualnych zmian organizacyjno-proceduralnych mających na celu zapewnienie wyższej efektywności bezpieczeństwa informacji w wojskowych systemach telekomunikacyjnych.

Gwarantujemy pełną anonimowość formułowanych przez Pana opinii i poglądów poprzez traktowanie uzyskanych odpowiedzi jako poufne.

**SERDECZNIE DZIĘKUJĘ PANU
ZA UDZIAŁ W BADANIACH
I
UDZIELENIE SZCZERYCH,
WARTOŚCIOWYCH ODPOWIEDZI**

ppłk mgr niż. Grzegorz ŚWIDZIKOWSKI

WARSZAWA **2004**

DANE SOCJODEMOGRAFICZNE

(Uprzejmie proszę, wyłącznie dla celów analitycznych, podanie kilku danych o sobie)

M1. Korpus kadry

(numer jednej z wybranych poniżej odpowiedzi proszę zakreślić „X")

1. **Oficer starszy** 2. **Oficer młodszy** 3. **Podoficer**

M2. Jaka jest Pana specjalność wojskowa?

(numer jednej z wybranych poniżej odpowiedzi proszę zakreślić „X")

1. **Ogólnowojskowa** 2. **Artyleria** 3. **Inżynieryjna**
4. **Logistyka** 5. **Łączność** 6. **Radiotechniczna**
7. **Inna (jaka?)**

M3. W jakim przedziale zawiera się Pana wiek?

(numer jednej z wybranych poniżej odpowiedzi proszę zakreślić „X")

1.	do 35 lat	**2.**	36 – 45 lat	**3.**	powyżej 45 lat

M4. Pana wykształcenie?
(numer jednej z wybranych poniżej odpowiedzi proszę zakreślić „X")

1.	Wyższe 2 stopnia	**2.**	Wyższe 1 stopnia	36 – 45 lat	**3.**	Średnie

M5. Staż Pana służby zawodowej
(numer jednej z wybranych poniżej odpowiedzi proszę zakreślić „X")

1.	do 5 lat	**2.**	6 – 9 lat	**3.**	10 - 14 lat
4.	15 – 19 lat	**5.**	20 – 24 lata	**6.**	powyżej 25 lat

M6. Staż Pana pracy w organach bezpieczeństwa łączności i informatyki
(numer jednej z wybranych poniżej odpowiedzi proszę zakreślić „X")

1.	do 1 roku	**2.**	2 – 3 lata	**3.**	4 - 5 lat
4.	6 – 7 lat	**5.**	8 – 9 lat	**6.**	10 i więcej lat

M7. Udział w ćwiczeniach i treningach dowódczo-sztabowych z udziałem wojsk (w kraju i za granicą) na obecnie zajmowanym stanowisku

(numer jednej z wybranych poniżej odpowiedzi proszę zakreślić „X")

1.	nie brałem udziału	**2.**	1 raz	**3.**	2 razy
4.	3 razy	**5.**	4 razy	**6.**	5 i więcej razy

Jakie jest prawdopodobieństwo wystąpienia zagrożenia ujawnienia lub utraty bezpieczeństwa informacji w polowej sieci telekomunikacyjnej związku taktycznego w kontekście implementowanych organizacyjno-technicznych i eksploatacyjnych środków ochrony informacji?

(proszę wybrać poziom prawdopodobieństwa poprzez postawienie symbolu X przy każdym rodzaju zagrożenia)

Opinie o zagrożeniach

Zagrożenia dla bezpieczeństwa informacji	**Stopień prawdopodobieństwa wystąpienia**				
	Bliskie jedności	**Duże**	**Średnie**	**Małe**	**Bliskie zeru**
Personalne:					
-ze strony personelu technicznego					
-ze strony użytkowników					
-ze strony osób funkcyjnych					
-ze strony innych nieuprawnionych osób					
Fizyczne:					
-źle zorganizowanej lub zbyt słabej ochrony elementów systemu (np. warta)					
-słabych lub nieadekwatnych zabezpieczeń zapewniających dostęp do wrażliwych elementów infrastruktury telekomunikacyjnej lub urządzeń systemu tj. drzwi, okna, kraty, itp.					
-w wyniku celowego działania potencjalnego przeciwnika					
-w rezultacie zaistnienia klęski żywiołowej, itp.					
Organizacyjno-proceduralne:					
-niewłaściwego przydziału uprawnień osobom funkcyjnym					
-braku lub niskiego poziomu szkolenia w zakresie bezpieczeństwa informacji					
-niejasno sformułowanych (niezrozumiałych) procedur postępowanie w sytuacjach krytycznych (nadzwyczajnych)					
-nieodpowiednio dobranej struktury oraz zakresu kompetencji organów odpowiedzialnych za organizację, nadzór i funkcjonowanie bezpieczeństwa w systemach łączności i informatyki					

Zagrożenia dla bezpieczeństwa informacji	Stopień prawdopodobieństwa wystąpienia				
	Bliskie jedności*	Duże*	Średnie*	Małe*	Bliskie zeru*
Techniczne: kryptografia					
-niewłaściwie dobranej mocy algorytmów kryptograficznych					
-nieprzestrzeganie zasad bezpieczeństwa w zakresie wytwarzania, obiegu i dostępu do urządzeń ochrony kryptograficznej					
-nieprzestrzeganie zasad bezpieczeństwa w zakresie wytwarzania, obiegu i dostępu do dokumentów kluczowych (szyfrowych)					
-stosowania urządzeń bez świadectwa certyfikacyjnego					
Techniczne: emisja ujawniająca					
-stosowania w systemie telekomunikacyjnym urządzeń komercyjnych nie posiadających stosownych świadectw certyfikacyjnych					
-brak strefy (obszaru kontrolowanego)					
-nie przestrzeganie zasad rozmieszczania urządzeń (odległości)					
-braku zabezpieczeń i nie spełnienie wymagań w zakresie rozwijania linii kablowych, światłowodowych, itp.					
Techniczne: transmisja					
-nieautoryzowany przechwyt informa-					
-celowe i niecelowe zakłócanie informacji					
-interferencja					
-prowadzenie przez osoby nieuprawnione analizy ruchu telekomunikacyjnego					
-podszywanie się pod użytkowników lub inne uprawnione osoby funkcyjne					
Techniczne: programowe					
-brak procedur uwierzytelniania (np. wejścia, wyjścia z systemu)					
-brak lub nieadekwatne programowe zabezpieczenie do dostępu do zasobów systemu (nadawanie uprawnień)					
-istnienie możliwości instalacji oprogramowania prywatnego - nie dedykowanego dla danego systemu i nie posiadającego wymaganego certyfikatu					

Zagrożenia dla bezpieczeństwa informacji	Stopień prawdopodobieństwa wystąpienia				
	Bliskie jedności*	Duże*	Średnie*	Małe*	Bliskie zeru*
-brak lub niewłaściwe wdrożenie zabezpieczeń uniemożliwiających nieautoryzowaną możliwość wprowadzania zmian – modyfikacji informacji, aplikacji systemowych					
-brak szyfrowania informacji na nośnikach elektronicznych					
-brak lub słabe zabezpieczenia przed oprogramowaniem złośliwym (np. wirusy, itp.)					
-błędy użytkowników (działania celowe i niezamierzone)					
-błędy personelu technicznego (działania celowe i niezamierzone)					
Techniczne: wsparcie techniczne					
-brak lub niewłaściwie zorganizowany system przepustkowy					
-brak lub nieadekwatny system antywłamaniowy i ppoż.					
-brak lub niewłaściwy system zasilania awaryjnego					
-inne systemy zabezpieczające funkcjonowanie systemu telekomunikacyjnego					
Inne nie ujęte powyżej:					

Własne uwagi i spostrzeżenia

.....

.....

.....

.....

.....

LEGENDA (stopień prawdopodobieństwa)	
Bliskie jedności	0,9 – 1
Duże	0,7 – 0,8
Średnie	0,4 – 0,6
Małe	0,2 – 0,3
Bliskie zeru	0 - 0,1

SPRAWOZDANIE Z BADANIA ANKIETOWEGO DOTYCZĄCEGO GRADACJI ZAGROŻEŃ DLA BEZPIECZECZEŃSTWA INFORMACJI W POLOWEJ SIECI TELEKOMUNIKACYJNEJ

1. TEMAT BADAŃ: Ocena poziomu istotności zagrożeń dla bezpieczeństwa informacji w polowej sieci telekomunikacyjnej związku taktycznego.
2. METODY BADAWCZE: Metoda sondażu diagnostycznego techniką ankiety.
3. CEL BADAŃ: Określenie stopnia istotności i prawdopodobieństwa wystąpienia zagrożeń dla bezpieczeństwa informacji w polowej sieci telekomunikacyjnej związku taktycznego szczebla dywizji.
4. CZAS BADAŃ: 26 luty 2004.
5. OPIS PRZEBIEGU BADAŃ: Badania przeprowadzono podczas dorocznego szkolenia personelu pionów bezpieczeństwa łączności i informatyki wojsk lądowych, które realizowane było na bazie obiektów Centrum Szkolenia Łączności i Informatyki w Zegrzu w dniach 24 – 26.02.2004 r. oraz w czasie szkoleń uzupełniających kadry Wojskowego Biura Bezpieczeństwa Łączności i Informatyki i Centrum Analiz Kryptograficznych i Bezpieczeństwa Teleinformacyjnego w miesiącu marcu 2004 r. Badaniami objęto oficerów i podoficerów, którzy spełniali założone i wyszczególnione poniżej przez autora kryteria:

a) respondent jest etatowym pracownikiem organów bezpieczeństwa łączności i informatyki lub jednostek organizacyjnych resortu Obrony Narodowej odpowiedzialnych za organizację ochrony informacji w wojskowych systemach, sieciach łączności i informatyki;

b) jego staż pracy w tych strukturach wynosi minimum3 lata;

c) posiada doświadczenia w zakresie zasad organizacji bezpiecznego systemu (sieci), które jest następstwem udziału w ćwiczeniach lub treningach sztabowych z udziałem i bez udziału wojsk - minimum 2-krotnie.

W procesie badań zastosowano metodę sondażu diagnostycznego, którą w praktyce zrealizowano techniką ankiety. Spośród 71 respondentów do dalszych badań uwzględniono tylko 44 ankiety, które wypełnione zostały przez personel spełniający założone przez autora wymagania.

AKADEMIA OBRONY NARODOWEJ

WYDZIAŁ WOJSK LĄDOWYCH

WYWIAD EKSPERCKI

Warszawa **2004**

Szanowny Panie

Członkostwo naszego państwa w strukturach organizacji Traktatu Północno-atlantyckiego przyczyniło się do wprowadzenia zmian prawnych i uregulowań normatywnych w zakresie zasad ochrony narodowych i sojuszniczych informacji niejawnych. Przywoływane dokumenty dotyczyły wszystkich dziedzin, w tym też bezpieczeństwa informacji w sieciach, systemach łączności i informatyki SZ RP.

Kilkuletni okres ich obowiązywania i diametralne zmiany, oczywiście nie we wszystkich obszarach, zarówno w podejściu systemowym jak i zalecanych środków i metod ochrony informacji w wojskowych sieciach telekomunikacyjnych pozwalają na sformułowanie pierwszych wniosków i uwag w tym zakresie.

Z tej przyczyny, przy założonym zawężeniu rozpatrywanego obszaru, przedmiotem zainteresowania prowadzącego badania ocena aktualnego stanu bezpieczeństwa informacji w sieci teletransmisyjnej dywizji zmechanizowanej.

Proszę o odpowiedź na następujące pytania:

1. Jak przebiegał proces wdrażania nowych standardów i wymagań w zakresie bezpieczeństwa informacji na szczeblach taktycznych?

Sprawnie		**Z problemami**		**Nie wiem**	

2. Które z wprowadzonych zmian są według Pana najistotniejsze?

1. **2.....**		**Nie mam zdania**		**Nie wiem**	

3. W jakich obszarach i w jakich aspektach powinno rozpatrywać się problematykę zagrożeń bezpieczeństwa informacji w sieciach polowych i jakie adekwatne stosować środki lub metody im zapobiegające?

1. **2.....**		**Nie mam zdania**		**Nie wiem**	

4. Czy w Pana opinii zakres realizowanych przedsięwzięć zapewnia wymagany poziom bezpieczeństwa w sieci teletransmisyjnej związku taktycznego (dywizji)?

Tak		**Nie**		**Nie mam zdania**	

5. Jakie jeszcze ewentualne kroki, czynności można przedsięwziąć aby zminimalizować ryzyko utraty wymaganych atrybutów bezpieczeństwa informacji w sieci teletransmisyjnej?

1. **2.....**		**Nie mam zdania**		**Nie wiem**	

SPRAWOZDANIE Z BADAŃ OPINII EKSPERTÓW DOTYCZĄCEGO OCENY BEZPIECZEŃSTWA INFORMACJI W SIECI TELETRANSMISYJNEJ DYWIZJI ZMECHANIZOWANEJ

1. TEMAT BADAŃ: Ocena stanu bezpieczeństwa informacji w sieci teletransmisyjnej dywizji zmechanizowanej.
2. METODY BADAWCZE: Metoda ocen ekspertów.
3. CEL BADAŃ: Uzyskanie danych niezbędnych do przeprowadzenia oceny aktualnego stanu bezpieczeństwa informacji w sieci teletransmisyjnej dywizji zmechanizowanej.
4. CZAS BADAŃ: Styczeń 2004 – Kwiecień 2004.
5. OPIS PRZEBIEGU BADAŃ: Badania przeprowadzono metodą ocen ekspertów, objęto nimi oficerów, którzy spełniali założone i wyszczególnione poniżej przez autora kryteria:

a) posiadali wieloletnie doświadczenie w zakresie zapewnienia bezpieczeństwa informacji w systemach łączności i informatyki umożliwiające im porównanie byłych i aktualnych wymagań w tym zakresie;

b) znają problematykę i posiadają wiedzę w zakresie standardów i wymagań bezpieczeństwa informacji NATO;

c) opracowywali lub wdrażali na różnych szczeblach dowodzenia obowiązujące dokumenty normatywne związane z ochroną informacji niejawnych w wojskowych sieciach telekomunikacyjnych;

d) czynnie uczestniczyli w przedsięwzięciach związanych z nadzorem lub kontrolą w obszarze spełnienia wymagań w zakresie bezpieczeństwa informacji.

Badania prowadzono techniką opartą na wzajemnym komunikowaniu się, ze względu na możliwość zdobywania dodatkowych informacji poza standardowo przygotowanymi i zawartymi w kwestionariuszu pytaniami.

Szczególnie przydatne okazały się wypowiedzi tych oficerów, którzy uczestniczyli w przedsięwzięciach związanych z ochroną informacji w różnych strukturach (dowództwach) NATO oraz brali czynny udział w procesie akcesyjnym i dostosowawczym sił zbrojnych RP do wymagań i standardów sojuszu w rozpatrywanym obszarze.

Praktyczne podejście do rozwiązywanych problemów poznano podczas wywiadu z oficerami Centrum Analiz Kryptograficznych i Bezpieczeństwa Teleinformacyjnego oraz Wojskowego Biura Bezpieczeństwa Łączności i Informatyki, których doświadczenie w tej materii jest najbogatsze.

W oparciu o uzyskane w trakcie prowadzenia wywiadów wypowiedzi i opinie można sformułować w odniesieniu do rozpatrywanych obszarów i problemów następujące generalne wnioski:

1. Pierwszy, początkowy etap wdrażania i dostosowania narodowych wymagań i przedsięwzięć w zakresie bezpieczeństwa informacji w wojskowych sieciach łączności i informatyki do standardów NATO był bardzo trudny. Wynikało to

bowiem z faktu, że czas uzyskania niezbędnych w tym obszarze dokumentów normatywnych od stosownych organów sojuszu pozwalał jedynie na przekazanie ich w oryginalnej formie do podległych jednostek organizacyjnych szczebla taktycznego, gdzie znajomość języka angielskiego w pionach odpowiedzialnych za organizacje bezpieczeństwa w sieciach telekomunikacyjnych była znikoma. Opracowaniu narodowych normatywów uwzględniających treści wymagań sojuszniczych towarzyszyły liczne pytania, kontrowersje oraz różnorodność interpretacyjna. Stan trwał jeszcze przez pewien okres po ich wdrożeniu i po części przeniósł się również na szczeble niższe, w tym taktyczne. Jednak liczne kontakty z przedstawicielami państw sojuszu oraz agend NATO pozwalały na systematyczne eliminowanie kwestii podlegających wyjaśnieniu. Towarzyszyły temu liczne szkolenia prowadzone z personelem bezpieczeństwa łączności i informatyki, które umożliwiają w chwili obecnej na stwierdzenie pełnej jasności i stabilizacji w tej materii.

2. Zmiana zapewniająca dostosowanie narodowych aktów prawnych i dokumentów wykonawczych do standardów i wymogów organizacji Traktatu Północnoatlantyckiego wprowadziła usystematyzowanie w proces organizacji bezpieczeństwa informacji w sieci telekomunikacyjnej polegającej na ścisłym określeniu obszarów na organizacyjno-proceduralne, personalne, fizyczne i techniczne, w których przedsięwzięcia winny być realizowane. Jednak chyba najbardziej istotna jest zasada lub dokładniej wymóg opracowania i zatwierdzenia przed rozpoczęciem eksploatacji „Szczególnych wymagań bezpieczeństwa" oraz „Procedur bezpieczeństwa" dla każdego systemu lub sieci, w której planowane jest wytwarzanie, przetwarzanie, przesyłaniu lub przechowywanie informacji stanowiących tajemnicę państwową i służbową.

3. Problematyka zagrożeń dla bezpieczeństwa informacji jest niezwykle ważna. Określenie wagi informacji (klauzuli), struktury i organizacji sytemu, w którym ma być przesyłana, dyslokacji (rozmieszczenia) poszczególnych jej elementów bądź urządzeń oraz czynniki wewnętrzne i zewnętrzne pochodzące

ze środowiska dalszego i bliższego stanowią podstawowe determinanty leżące u podstaw procesu identyfikacji zagrożeń dla bezpieczeństwa informacji w każdym systemie lub sieci. Jednak każdy z ekspertów podkreślał, że głównym czynnikiem mającym wpływ na bezpieczeństwo informacji jest celowa lub niezamierzona działalność człowieka. Sprecyzowanie i scharakteryzowanie zagrożeń umożliwia dopiero wybór tych środków oraz metod, których kompleksowe zastosowanie pozwoli na ich wyeliminowanie. Czynności te w warunkach polowych są jeszcze bardziej skomplikowane, gdyż muszą uwzględniać zmienność wymienionych czynników zarówno w czasie jak i przestrzeni. Stąd też identyfikacja zagrożeń oraz stosowania środków i metod ochrony informacji w sieciach polowych powinna być dokonywana przynajmniej na każdym etapie realizowanych zadań bojowych lub każdorazowo w następstwie zaistnienia istotnych zmian określonych wcześniej determinantów.

4. Jeśli jako determinant przy dokonywaniu oceny bezpieczeństwa informacji w wojskowych sieciach telekomunikacyjnych, w których przekazywane są informacje niejawne, wzięty zostanie ustawowy wymóg opracowania oraz zatwierdzenia „Szczególnych wymagań bezpieczeństwa" to można udzielić na tak przedstawione i sformułowane pytanie odpowiedzi twierdzącej. Podstawą tej opinii były wyniki prowadzonych kontroli potwierdzające zgodność treści zawartych w przytoczonym powyżej dokumencie z praktycznie zastosowanymi w systemach i sieciach rozwiązaniami w obszarach personalnym, organizacyjno-proceduralnym, fizycznymi i technicznymi zabezpieczeniami.

5. W systemach polowych zasadnicze rozwiązania powinny bazować na ochronie informacji „żywej" przekazywanej w czasie rzeczywistym i tutaj najbardziej istotnym elementem jest szybkość powiadomienia nadawcy, odbiorcy czy poszczególnych węzłów łączności – stanowisk dowodzenia, pomocniczych węzłów łączności – że coś się stało z którymś z ogniw pośredniczących w przekazywaniu tej informacji. Mowa jest o typowym dostaniu się aparatow-

ni w ręce przeciwnika. Teraz istotnym jest w jakim czasie my zdążymy zareagować na fakt, że ta aparatownia nie jest wiarygodna oraz jaki wpływ ma przejęcie jednego lub kilku urządzeń ochrony kryptograficznej z przejętej lub przejętych aparatowni na dalsze funkcjonowanie i konfigurację naszego systemu. Ile zatem czasu zajmie nam jego rekonfiguracja lub przejście na inny system. Powinniśmy dążyć to tego, że strata i dostanie się pojedynczych urządzeń ochrony kryptograficznej nie powinna załamywać nam dalszego funkcjonowania systemu wymiany informacji. Zabezpieczenie tego typu posiada np. radiostacja PRG-4, gdzie jesteśmy w stanie zidentyfikować czy obsługuje ją legalny, uprawniony użytkownik, czy ktoś pod niego się podszywa. Próba dostania się do wnętrza urządzenia odcina zasilanie i powoduje wykasowanie wszelkich zapisanych tam danych. „Wpadka" aparatowni może spowodować, że my dalej nieświadomie przesyłamy informacje, a jeśli stosujemy środki retranslacyjne, to tak naprawdę nie znamy drogi, którą informacja dociera do odbiorcy.

Akademii Obrony Narodowej
BIBLIOTEKA GŁÓWNA - ARCHIWUM
II
06989
68650