AKADEMIA OBRONY NARODOWEJ

WYDZIAŁ WOJSK LĄDOWYCH
INSTYTUT ZARZĄDZANIA I DOWODZENIA

BEZPIECZEŃSTWO I OCHRONA INFORMACJI W SIECIACH ŁĄCZNOŚCI I INFORMATYKI WOJSKOWEJ W OKRESIE POKOJU, KRYZYSU I WOJNY

pk. „OCHRONA”

WARSZAWA 2004

AKADEMIA OBRONY NARODOWEJ

WYDZIAŁ WOJSK LĄDOWYCH
INSTYTUT ZARZĄDZANIA I DOWODZENIA

BEZPIECZEŃSTWO I OCHRONA INFORMACJI W SIECIACH ŁĄCZNOŚCI I INFORMATYKI WOJSKOWEJ W OKRESIE POKOJU, KRYZYSU I WOJNY

pk.: „OCHRONA"

Praca naukowo - badawcza

Warszawa **2004 r.**

Recenzent:

płk rez. prof. dr hab. Stanisław ŚLADKOWSKI

Opracował zespół autorski:

1. ***Kierownik : płk dr hab. inż. Józef MICHNIAK***

   - kierownictwo naukowe,
   - opracowanie: wstępu, rozdziału: 2, 3, 4 i zakończenia.

2. ***Członkowie:***

   - ***ppłk dr inż. Zbigniew FIOŁNA***

     - opracowanie rozdziału 1,

   - ***ppłk mgr inż. Grzegorz ŚWIDZIKOWSKI***

     - opracowanie rozdziału 4,

   - ***sierż. szt. mgr Dariusz GOŁAWSKI***

     - sekretarz zespołu,
     - korekta, redakcja techniczna, skład komputerowy, druk.

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

SPIS TREŚCI

WSTĘP *(płk dr hab. inż. Józef Michniak)* **5**

1. WOJSKOWE SIECI TELEKOMUNIKACYJNE I INFORMATYCZNE W OKRESIE POKOJU, KRYZYSU I WOJNY *(ppłk dr inż. Zbigniew Fiołna)* **11**

1.1. Charakterystyka sieci telekomunikacyjnych i informatycznych SZ RP 11

1.1.1. Charakterystyka stacjonarnego systemu łączności i informatyki SZ RP..... 13

1.1.2. Charakterystyka polowych sieci telekomunikacyjnych i informatycznych..... 19

1.2. Wykorzystanie wojskowych sieci telekomunikacyjnych i informatycznych w czasie pokoju... 28

1.2.1. Łączność wewnętrzna resortu Obrony Narodowej i dowodzenie jednostkami wojskowymi 28

1.3. Wykorzystanie wojskowych sieci telekomunikacyjnych i informatycznych w sytuacjach szczególnych 33

1.3.1. Wykorzystanie wojskowych sieci telekomunikacyjnych i informatycznych w sytuacjach kryzysowych 33

1.3.2. Wykorzystanie wojskowych sieci telekomunikacyjnych i informatycznych w czasie wojny 37

2. BEZPIECZEŃSTWO I OCHRONA INFORMACJI – PODSTAWOWA TERMINOLOGIA *(płk dr hab. inż. Józef Michniak)* **40**

2.1. Bezpieczeństwo 40

2.2. Informacja 42

2.3. Wojskowe sieci telekomunikacyjne..... 43

2.4. Wojskowe sieci komputerowe (informatyki) 43

2.5. Otoczenie wojskowej sieci telekomunikacyjnej i informatycznej 44

3. ZAGROŻENIA BEZPIECZEŃSTWA WOJSKOWYCH SIECI TELEKOMUNIKACYJNYCH I INFORMATYCZNYCH *(płk dr hab. inż. Józef Michniak)* **46**

3.1. Zagrożenia bezpieczeństwa łączności wojskowej 46

3.1.1. Zagrożenia sieci telekomunikacyjnych 47

3.1.2. Zagrożenia sieci komputerowych (informatycznych) 50

4. WYMAGANIA STAWIANE BEZPIECZNYM SIECIOM KOMPUTEROWYM *(płk dr hab. inż. Józef Michniak)* **57**

4.1. Aspekty bezpieczeństwa informacji..... 58

4.1.1. Bezpieczeństwo fizyczne..... 59

4.1.2. Bezpieczeństwo elektromagnetyczne..... 65

4.1.3. Bezpieczeństwo programowe 68

4.1.4. Zarządzanie prawami dostępu..... 72

4.1.5. Dzienniki systemowe 73

4.1.6. Profilaktyka antywirusowa 74
4.1.7. Archiwizacja danych 75
4.2. Polityka bezpieczeństwa 79

5. BEZPIECZEŃSTWO I OCHRONA INFORMACJI W SIECIACH TELEKOMUNIKACYJNYCH *(ppłk mgr inż. Grzegorz Świdzikowski)* 82

5.1. Podział i charakterystyka zagrożeń bezpieczeństwa informacji w wojskowych sieciach telekomunikacyjnych 85
5.2. Gradacja zagrożeń bezpieczeństwa informacji w wojskowych sieciach telekomunikacyjnych 96
5.3. Metody i środki ochrony informacji w wojskowych systemach telekomunikacyjnych 111
5.4. Struktura organizacyjna wojskowych organów bezpieczeństwa łączności i informatyki 138

ZAKOŃCZENIE *(płk dr hab. inż. Józef Michniak)* 143

BIBLIOGRAFIA 144

WSTĘP

płk dr hab. inż. Józef MICHNIAK

Od początku lat 80-tych XX wieku obserwujemy nowy sposób przechowywana i przetwarzania informacji mianowicie komputery. Stają się one narzędziem pracy coraz większej liczby ludzi, ze względu na wygodę ich stosowania i możliwości. Ewolucja, postęp technologiczny ale i zapotrzebowanie na przesyłanie informacji pomiędzy użytkownikami doprowadziły do powstania sieci telekomunikacyjnych i komputerowych zarówno małych, lokalnych jak i sieci o zasięgu globalnym jaką jest na przykład Internet. Wszyscy coraz chętniej korzystamy z dobrodziejstw jakie oferują nam komputery, sieci i aplikacje w nich pracujące. Coraz więcej informacji gromadzimy w zasobach komputerów. Komputery i sieci w których one pracują coraz częściej pojawiają się w naszym codziennym życiu, czasami nawet sobie nie zdajemy z tego sprawy. Jednym z takich przykładów mogą być chociażby automatyczne stacje benzynowe, gdzie jeden komputer najpierw inkasuje od nas gotówkę, a następnie wydziela nam odpowiednią ilość paliwa. Obserwowane do niedawna nasze opory w korzystaniu z komputerów zaczynają powoli zanikać. W ten sposób rozliczne sieci komputerowe zbierają różne informacje, o numerach kart kredytowych, dane osobowe, czy inne informacje istotne dla danej organizacji i przesyłają je liniami telekomunikacyjnymi do innych organizacji. Coraz częściej informacje te są dla nas szczególnie cenne, czy to ze względu na interes organizacji czy z powodu aktów normatywnych, które nakładają takie wymagania, jak to ma miejsce w przypadku danych osobowych. Dlatego też problematykę tę postanowiliśmy zbadać i wyniki przedstawić w niniejszej pracy.

Celem pracy jest omówienie zagrożeń i przedsięwzięć mających na celu zapewnienia bezpieczeństwa informacji w sieciach telekomunikacyjnych i komputerowych.

Na etapie określania celu pracy przyjęto, iż obszarem zainteresowań będą wydzielone wojskowe sieci telekomunikacyjne i komputerowe, które nie są połączone z siecią Internet. Związane jest to z koniecznością zapewnienia odpowiednio wysokiego poziomu bezpieczeństwa, poprzez ograniczenie dostępu osób trzecich.

Aby osiągnąć zamierzony cel pracy posłużono się następującymi pytaniami:

- Co to jest bezpieczeństwo, informacja i sieć telekomunikacyjna oraz komputerowa?
- Jakie są zagrożenia i ich źródła?
- Jakie są aspekty bezpieczeństwa?

- Co to jest i jak skonstruować politykę bezpieczeństwa?
- Jak najefektywniej chronić informację w tych sieciach ?

Niniejsza praca składa się z pięciu rozdziałów. Pierwszy z nich określa strukturę organizacyjno-techniczną sieci telekomunikacyjnej i informatycznej MON na obszarze kraju oraz wykorzystanie sieci stacjonarnej i polowej w okresie pokoju kryzysu i wojny. Rozdział drugi zawiera określenia podstawowych pojęć z badanego obszaru. Rozdział trzeci zawiera treści obrazujące poszczególne rodzaje zagrożeń bezpieczeństwa wojskowych sieci telekomunikacyjnych i informatycznych oraz wskazuje na ich źródła. Rozdział czwarty omawiane są wymagania stawiane bezpiecznym sieciom komputerowym, ich aspekty bezpieczeństwa i sposoby zabezpieczenia informacji. Opisano politykę bezpieczeństwa, będącą strategią organizacji w zapewnianiu bezpieczeństwa informacji w sieciach komputerowych.

W ostatnim rozdziale, piątym przedstawiono aspekty bezpieczeństwa i sposoby zabezpieczenia informacji w sieciach telekomunikacyjnych.

Podstawową wykorzystaną w pracy metodą badawczą jest analiza dokumentów, która została oparta na następujących materiałach źródłowych:

- akty prawne,
- dokumenty normatywne,
- publikacje z tematu bezpieczeństwa informacji, sieci komputerowych i telekomunikacyjnych,
- materiały z konferencji i sympozjów,
- materiały reklamowe producentów sprzętu i oprogramowania.

Ponadto w pracy zostały wykorzystane doświadczenia autorów z zakresu tematu pracy. Należy jednak zaznaczyć, że celem pracy nie jest przedstawianie konkretnych rozwiązań przywiązanych do urządzeń czy oprogramowania, a jedynie wskazanie ogólnych metod zabezpieczania sieci i informacji w nich zawartych. Wynika to z faktu, iż bardzo szybki rozwój technologiczny sprzętowy i programowy wymusza ciągłą aktualizację takich informacji co przyczyniło by się do szybkiej dezaktualizacji zawartej treści.

Koncepcja metodologiczna niniejszej pracy ma charakter złożony. Zakres problemowy pracy obejmuje uwarunkowania funkcjonowania sieci telekomunikacyjnych i informatycznych w warstwie stacjonarnej i polowej resortu obrony narodowej. We współczesnej dobie problem ten jest dosyć złożony ze względu na dynamiczny charakter rozwoju technologii

teleinformatycznych.. Kierowanie (dowodzenie, zarządzanie), aby mogło być realizowane musi oprócz innych składników, posiadać określoną bazę materialną. Dlatego w tym celu dla potrzeb sił zbrojnych organizuje się system łączności i informatyki, który musi zapewnić bezpieczeństwo przebywającej w nim informacji. Przedmiotem badań musiał być zatem obecny stan zorganizowania tego systemu, uwarunkowania bezpieczeństwa i obowiązujące nasze wymagania narodowe i wynikające z zobowiązań sojuszniczych oraz zadania realizowane w tych systemach.

Dlatego w odniesieniu do będącego przedmiotem zainteresowania naukowego bezpieczeństwa i ochrony informacji w wojskowych sieciach łączności i informatyki zaistniała potrzeba uporządkowania wiedzy o możliwościach zapewnienia bezpieczeństwa i ochrony informacji w funkcjonujących w okresie pokoju, kryzysu i wojny sieciach łączności i informatyki.

Założono, że opracowanie pisarskie pracy ma stanowić sumę wniosków uzyskanych w wyniku zastosowania różnorodnych metod badawczych. Już początkowe prace wykazały istnienie szeregu luk w istniejącej wiedzy w zakresie stanowiącym obszar zainteresowania zespołu autorskiego. W konsekwencji ujawniła się sytuacja problemowa, dając początek pierwszemu dosyć ograniczonemu etapowi procesu badań naukowych ze względu na szczupłość zespołu i ograniczone środki finansowe oraz czas.

Bazując na wytycznych zawartych w treści zadania, dotychczasowej wiedzy oraz wynikach badań wstępnych za **cel główny pracy** przyjęto:

1. ***Identyfikację struktury organizacyjno-technicznej sieci łączności i informatyki MON oraz zagrożeń bezpieczeństwa informacji w nich przesyłanych, przetwarzanych i gromadzonych.***
2. ***Określenie wymagań stawianych bezpiecznym sieciom komputerowym i telekomunikacyjnym oraz przedsięwzięć mających spełnić te wymagania.***

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

3. ***Zidentyfikować treść pojęcia „Bezpieczeństwo informacji" i pojęć pokrewnych.***
4. ***Określić strukturę organizacyjno-techniczną wojskowej sieci telekomunikacyjnej i informatycznej w warstwie stacjonarnej i polowej.***
5. ***Zidentyfikować zagrożenia bezpieczeństwa wojskowych sieci telekomunikacyjnych i informatycznych.***

6. ***Dokonać identyfikacji wymagań stawianych bezpiecznym sieciom komputerowym i telekomunikacyjnym.***
7. ***Wypracować koncepcję przedsięwzięć, które należy przedsięwziąć aby zapewnić bezpieczeństwo i ochronę informacji w sieciach telekomunikacyjnych.***

Już w trakcie badań wstępnych (zgodnie z przyjętą procedurą badawczą[1]) autorzy pracy określili strukturę organizacyjno-techniczną wojskowej sieci telekomunikacyjnej i informatycznej wraz z podstawową terminologią z zakresu bezpieczeństwa i ochrony informacji.

W toku dalszej pracy, dążąc do osiągnięcia zakreślonych wcześniej celów, autorzy sformułowali problem badawczy w postaci dwóch pytań:

1. ***Jakie zagrożenia bezpieczeństwa wojskowych sieci telekomunikacyjnych i informatycznych mogą występować?***
2. ***Jakie wymagania i w jaki sposób spełnić aby zapewnić bezpieczeństwo informacji w sieciach komputerowych i telekomunikacyjnych?***

Kolejny, drugi etap badań, będący w swej istocie etapem badań porównawczych, stanowił w głównej mierze ciąg analiz, porównań i analogii oraz dalsze, dogłębne studiowanie dostępnej literatury przedmiotu. W konsekwencji tych badań autorzy utwierdzili się w przekonaniu o konieczności podziału głównego problemu naukowego na kilka mniejszych, ograniczonych w zakresie rozpatrywanych zagadnień. W ten sposób zostały zidentyfikowane i wyodrębnione następujące problemy szczegółowe:

1. ***Jaką rolę odgrywają zagrożenia bezpieczeństwa informacji w sieciach komputerowych, a jaką w sieciach telekomunikacyjnych?***
2. ***Jaki muszą być spełnione wymagania aby sieci telekomunikacyjne i informatyczne były bezpieczne?***
3. ***Co należy robić aby zapewnić bezpieczeństwo informacji w tych sieciach?***

Rezultaty dalszych studiów literatury przedmiotu oraz wnioski z wywiadów i ankiet stanowiły podstawę sformułowania **hipotezy**.

Bazując na posiadanej wiedzy oraz wynikach poprzedniego etapu badań, autorzy założyli, że: ***„Do zapewnienia bezpieczeństwa informacji w wojskowych sieciach łączności i informatyki należy najsampierw zidentyfikować wszelkie możliwe zagrożenia dla tych sie-***

---

[1] **Procedura** to „(...) unormowany przepisami, zwyczajami sposób prowadzenia, załatwienia jakiejś sprawy, tok, tryb, przebieg czegoś", Słownik języka polskiego, Warszawa, PWN 1993, s. 65.

ci, a następnie przedsięwziąć takie czynności które te zagrożenia zredukowały by do minimum.

W trzecim etapie badań autorzy zastosowali szereg metod badawczych prowadzących do rozwiązania określonych uprzednio problemów szczegółowych.

Specyfika zidentyfikowanych problemów badawczych rzutowała bezpośrednio na fakt, iż wśród użytych metod znalazły się zarówno metody teoretyczne, jak i empiryczne.

Zastosowane metody teoretyczne to: analiza, synteza, wnioskowanie, porównanie, analogia oraz uogólnienie.

Analiza zastosowana została w głównej mierze do badań literatury dotyczącej problematyki identyfikacji struktury sieci i występujących dla nich zagrożeń , a także wymagań stawianych bezpiecznym sieciom.

Syntezie poddane zostały wnioski z badań teoretycznych i empirycznych, porównywane następnie z przyjętymi założeniami.

W wydobywaniu podobieństw i różnic w rozwiązaniach z zakresu organizacji bezpiecznych sieci łączności i informatyki w różnych konfiguracjach szczególnie pomocne było **porównanie**.

Poszukiwanie podobieństw badanych uwarunkowań bezpieczeństwa informacji w sieciach telekomunikacyjnych i informatycznych ułatwione zostało przez zastosowanie metody **wnioskowania**. Specyfika materiału badawczego jednoznacznie wskazywała na konieczność stosowania takiego schematu wnioskowania, w którym prawdziwość przesłanek nie przesądzała o prawdziwości wniosku. Z kolei, biorąc pod uwagę kryteria rodzaju zdań stanowiących przesłanki oraz zdań będących konkluzjami, wnioskowanie realizowane było głównie przez **analogię**.

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

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

Piąty, ostatni etap prac obejmował podsumowanie wyników badań, ich uogólnienie i syntezę. Przyjęto określoną, wiarygodną interpretację rozwiązania problemu badawczego, która zawarta została w pisarskim opracowaniu wyników badań.

Przedstawiona w niniejszym opracowaniu koncepcja zapewnienia bezpieczeństwa informacji w wojskowych sieciach łączności i informatyki stanowi w swej istocie logiczny ciąg twórczej pracy skromnego ilościowo zespołu badawczego w krótkim okresie czasu.

Struktura niniejszej pracy obejmuje wstęp, pięć rozdziałów oraz zakończenie.

We **wstępie** zawarto wprowadzenie w problematykę pracy i uzasadnienie wyboru tematu oraz metodologiczne aspekty badań wraz z konstrukcją opracowania pisarskiego pracy i przyjętą procedurę badawczą.

Rozdział pierwszy zawiera prezentację wyników badań dotyczących identyfikacji struktury organizacyjno-technicznej wojskowych sieci telekomunikacyjnych i informatycznych w okresie pokoju, kryzysu i wojny wraz z ich charakterystyką.

W rozdziale drugim zawarto podstawową terminologię z zakresu bezpieczeństwa i ochrony informacji.

Rozdział trzeci zawiera prezentację możliwych zagrożeń bezpieczeństwa wojskowych sieci telekomunikacyjnych i informatycznych.

W **rozdziale czwartym** ujęto wyniki badań dotyczące identyfikacji wymagań stawianych bezpiecznym sieciom komputerowym i sprecyzowano założenia polityki bezpieczeństwa w tym zakresie.

W **rozdziale piątym** przedstawiono koncepcję zapewnienia bezpieczeństwa i ochrony informacji w sieciach telekomunikacyjnych.

W **zakończeniu** ujęto wnioski z przeprowadzonych badań.

1. WOJSKOWE SIECI TELEKOMUNIKACYJNE I INFORMATYCZNE W OKRESIE POKOJU, KRYZYSU I WOJNY

ppłk dr inż. Zbigniew FIOŁNA

1.1 Charakterystyka sieci telekomunikacyjnych i informatycznych SZ RP

Analizując działanie wojskowych sieci telekomunikacyjnych i informatycznych w różnych stanach, w których przewidziane są do wykorzystywania, tj.: w okresie pokoju, kryzysu i wojny, należy skonstatować, że są one elementem systemu wyższego rzędu – wojskowego systemu łączności, a ten z kolei jest jednym z wielu, współdziałających (w pewnym zakresie) systemów łączności w kraju i jednocześnie jest podsystemem w systemie kierowania obronnością i w systemie dowodzenia siłami zbrojnymi. Stąd też jego struktura organizacyjna i techniczna uwarunkowana jest potrzebami tak systemu kierowania jak i systemu dowodzenia oraz możliwościami funkcjonowania samodzielnie jak i w otoczeniu telekomunikacyjnym (innych sieci).

Jako element systemu łączności i informatyki[2] Sił Zbrojnych RP sieci telekomunikacyjne i informatyczne są przeznaczone do:

- zapewnienia ciągłej, bezpiecznej, terminowej i niezawodnej wymiany informacji pomiędzy kierownictwem MON i organami dowodzenia Siłami Zbrojnymi RP, zarówno w czasie pokoju, sytuacjach kryzysowych, zagrożenia bezpieczeństwa państwa jak i w czasie wojny;
- zapewnienia współdziałania organów dowodzenia i kierowania Sił Zbrojnych RP z naczelnymi organami kierowania obronnością państwa, jednostkami układu pozamilitarnego oraz organami dowodzenia Sojuszu Północnoatlantyckiego.

Struktura sieci, stosownie do wymagań zhierarchizowanego systemu dowodzenia i kierowania Siłami Zbrojnymi, jest wielopoziomowa i obejmuje:

---

[2] Niejednokrotnie uwzględnia się wykorzystywanie w tym systemie usług teleinformatycznych i określa się go jako system łączności i informatyki, bądź też (co przy obecnym rozwoju usług telekomunikacyjnych jest oczywiste) pozostawia się nazwę „system łączności", traktując oferowane w nim usługi teleinformatyczne jako współczesny standard, natomiast określenie „system informatyczny" pozostawia się dla technicznie wyodrębnionych systemów – sieci komputerowych (także mogących świadczyć identyczne usługi jak systemy telekomunikacyjne) oraz systemów – programów komputerowych (operacyjnych lub aplikacji użytkowych).

- **szczebel strategiczny** – oparty jest głównie na stacjonarnych elementach sieci telekomunikacyjnej kraju (publicznej sieci telekomunikacyjnej współdziałającej ze stacjonarnym systemem łączności SZ RP). Dla zapewnienia wymaganego stopnia trwałości najważniejsze stacjonarne węzły i linie telekomunikacyjne będą wzmacniane lub dublowane mobilnymi urządzeniami i środkami telekomunikacyjnymi a sieć wg potrzeb uzupełniana mobilnymi węzłami telekomunikacyjnymi tworząc „bazową sieć telekomunikacyjną" na okresy kryzysów lub wojny (podrozdział 1.3). Na szczeblu strategicznym wykorzystywane są także sieci informatyczne rozległe (organizowane w ramach Sojuszu Północnoatlantyckiego jak i narodowe) oraz sieci lokalne;
- **szczebel operacyjno-taktyczny** – oparty jest na elementach bazowej sieci telekomunikacyjnej SZ RP wzmocnionej w obszarze działania związku operacyjnego (korpusu zmechanizowanego[3]) liniami i węzłami telekomunikacyjnymi rozwijanymi potencjałem sił i środków oddziałów dowodzenia tego związku operacyjnego (korpusu) co prowadzi do utworzenia „operacyjno-taktycznej sieci telekomunikacyjnej"[4] szczebla operacyjnego. Ponadto na szczeblu operacyjno-taktycznym wykorzystywane są autonomiczne sieci radiowe wykorzystywane do zapewnienia wymiany informacji w więziach informacyjnych systemu dowodzenia (sieci dowodzenia, współdziałania, zabezpieczenia logistycznego, rozpoznania i inne[5]). Wykorzystywane są także lokalne sieci informatyczne stanowisk dowodzenia współdziałające ze sobą (tworząc w ten sposób sieć rozległą) poprzez sieć telekomunikacyjną;
- **szczebel taktyczny** – oparty jest praktycznie w całości na bazie mobilnych środków łączności, z których części na szczeblu związku taktycznego tworzy się tzw. „pomocniczą sieć łączności"[6] (wykorzystujący poprzez dowiązanie liniami telekomunikacyjnymi także potencjał systemu telekomunikacyjnego szczebla operacyjno-taktycznego). Drugim komponentem sieci telekomunikacyjnych szczebla taktycznego są sieci radiowe, tzw. sieci radiowe pola walki, zbudowane z mobilnych i przenośnych środków radiowych. Spełniają one bardzo ważną funkcję w systemie dowodzenia na niższych

---

[3] Pomimo stopniowej redukcji sił zbrojnych w całej Europie (w tym także likwidacji występujących w strukturze Wojska Polskiego narodowych korpusów zmechanizowanych) należy przewidywać, w przypadku zaistnienia pogłębiającej się sytuacji kryzysowej mogącej z dużym prawdopodobieństwem doprowadzić do konfliktu zbrojnego, możliwość rozwinięcia sił zbrojnych do szczebla korpusu.

[4] Sieć ta jest także nazywana „podstawową siecią łączności".

5 Analizę rodzajów i struktur sieci, w tym sieci radiowych, na szczeblu operacyjno-taktycznym i szczeblach taktycznych przeprowadzono w „Podstawowe relacje dowodzenia oddziału, związku taktycznego i związku operacyjnego w działaniach wojsk lądowych, część II - album schematów", AON, Warszawa 2001.

[6] Jest to sieć radioliniowo-kablowa związku taktycznego. Nazywana jest także „siecią teletransmisyjną" lub „siecią bazową" (nazwa potoczna przyjęta w wielu jednostkach, co prowadzi do niewłaściwego utożsamiania z „bazową siecią telekomunikacyjną" szczebla strategicznego).

szczeblach (na najniższych szczeblach są praktycznie jedynym technicznym środkiem łączności) a także wykorzystywane są w systemach sterowania środkami rażenia. Podobnie jak na wyższych szczeblach tworzone są lokalne sieci informatyczne stanowisk dowodzenia.

Analizując funkcjonowanie systemu łączności i informatyki na wszystkich szczeblach kierowania i dowodzenia można wyodrębnić dwa jego składniki:

- **podsystem stacjonarny** - funkcjonujący w sposób ciągły i zapewniający wymianę informacji w trakcie działania Sił Zbrojnych w czasie pokoju oraz przewidziany do wykorzystywania także w czasie kryzysu i wojny;
- **podsystem polowy** (mobilny) - przygotowany i gotowy do działania ale przeznaczony przede wszystkim do zapewnienia wymiany informacji w systemie dowodzenia w trakcie działań wojennych[7] (możliwe jest także jego użycie w trakcie działań antykryzysowych ale ma to miejsce jedynie w ograniczonym zakresie, w uzasadnionych przypadkach i specyficznych warunkach.

1.1.1. Charakterystyka stacjonarnego systemu łączności i informatyki SZ RP

Stacjonarny system łączności i informatyki Sił Zbrojnych jest w strukturze systemu łączności państwa jedną z sieci wewnętrznych, tzn. świadczących usługi „dla własnych potrzeb" Ministerstwa Obrony Narodowej oraz jednostek mu podległych. Takie przyporządkowanie prawne oddziela system łączności i informatyki SZ RP od systemów publicznych, co zawęża możliwości świadczenia usług powszechnych, ale jednocześnie, ze względu na wyszczególnione powyżej zadania, gwarantuje systemowi łączności i informatyki SZ RP pewną uprzywilejowaną pozycję, zapewniającą możliwość wykorzystywania innych systemów łączności a także ukierunkowanie jego rozwoju przede wszystkim do realizacji zadań związanych z obronnością i bezpieczeństwem państwa.

Charakteryzując stacjonarny system łączności i informatyki SZ RP można w nim wyodrębnić:

- *podsystem kierowania*, w którym wyróżnia się organa kierowania systemem łączności i informatyki na szczeblu centralnym Sił Zbrojnych (Zarząd Łączności i Informatyki w Generalnym Zarządzie Dowodzenia i Łączności Sztabu Generalnego WP), na szczeblach

[7] Wykorzystywany jest także w trakcie ćwiczeń. Można to uznać za wykorzystywanie w czasie pokoju, jednakże ćwiczenia są przygotowaniem do wykonywania zadań bojowych, stąd też autorzy stwierdzają, że są to de facto „treningi wojny" a zatem przeznaczenie i wykorzystanie systemów mobilnych jest określone jako wojenne.

dowództw Rodzajów Sił Zbrojnych i okręgów wojskowych (odpowiednie zarządy) oraz garnizonów (dowództwa/szefowie garnizonowych węzłów łączności)

- *podsystem telekomunikacyjny* (sieci telekomunikacyjnej), którego głównymi składnikami są węzły telekomunikacyjne i łączące je linie teletransmisyjne,
- *podsystem informatyczny*, w tym zautomatyzowane systemy wspomagania dowodzenia, zautomatyzowane systemy dowodzenia, dowodzenia i kierowania środkami walki oraz specjalistyczne systemy informatyczne (np.: logistyczne),
- *podsystem pocztowy* – tworzony w oparciu o elementy pocztowe garnizonowych węzłów łączności oraz sieci kursów pocztowych.[8]

W zależności od przeznaczenia poszczególnych (wyodrębnionych[9]) makroskładników systemu łączności i informatyki wyróżnia się:

- ✓ podsystem łączności i informatyki Ministra Obrony Narodowej,
- ✓ podsystem łączności i informatyki Wojsk Lądowych,
- ✓ podsystem łączności i informatyki Sił Powietrznych,
- ✓ podsystem łączności i informatyki Marynarki Wojennej.

Każdy z tych podsystemów – makroskładników różni się od pozostałych charakterem wykonywanych zadań, jednakże tzw. platforma sprzętowa (rodzaje stosowanych urządzeń) oraz struktura jest wspólna dla całego systemu. Stąd też, przy analizie możliwości wykorzystania stacjonarnego systemu łączności i informatyki, celowe jest zbadanie i scharakteryzowanie przede wszystkim podsystemu telekomunikacyjnego i pocztowego jako tych elementów systemu, które w głównej mierze decydują o możliwościach całego systemu łączności i informatyki.

Garnizonowe węzły łączności

Podstawowymi elementami stacjonarnego systemu łączności SZ RP są garnizonowe węzły łączności (GWŁ). Są one samodzielnymi jednostkami organizacyjnymi, posiadającymi etatowe wyposażenie w środki i urządzenia łączności. Odpowiednio do ilości i rodzaju komórek organizacyjnych: sztabów, instytucji, jednostek wojskowych, a także charakteru wykony-

---

[8] Podsystem pocztowy jako element zapewniający fizyczny transport przesyłek pomiędzy nadawcą i adresatem nie jest przedmiotem badań.

[9] Obecna struktura stacjonarnego systemu łączności SZ RP, pomimo działań zmierzających do stworzenia jednolitego, zintegrowanego systemu łączności i informatyki dla całych Sił Zbrojnych charakteryzuje się wyraźnym rozdziałem na podsystemy „dedykowane" poszczególnych rodzajów wojsk.

wanych przez nie zadań poszczególne garnizonowe węzły łączności różnią się wyposażeniem, możliwościami usługowymi oraz etatem[10].

Głównym węzłem w stacjonarnym systemie łączności jest Centralny Węzeł Łączności MON. Przeznaczony jest do zapewnienia centralnym organom władzy państwowej odpowiedzialnym za bezpieczeństwo i obronę państwa (w tym także Ministrowi Obrony Narodowej), Sztabowi Generalnemu WP oraz wszystkim jednostkom stacjonującym na terenie Warszawy łączności wewnętrznej (w garnizonie) oraz dalekosiężnej łączności z dowództwami rodzajów wojsk, okręgów wojskowych, dowództwami jednostek wojskowych, organami kierowniczymi władzy państwowej, jednostkami układu pozamilitarnego oraz łączności międzynarodowej z państwami NATO.

W skład wyposażenia Centralnego Węzła Łączności MON wchodzą:

- centrala automatyczna międzymiastowa,
- grupa automatycznych central miejscowych[11],
- urządzenia telefonicznego systemu alarmowania (różnych typów),
- grupa urządzeń teletransmisyjnych[12] (kablowych i radioliniowych),
- grupa urządzeń telefaksowych,
- grupa urządzeń łączności utajnionej,
- grupa urządzeń łączności specjalnej,
- radiowe centrum nadawcze (RCN),
- radiowe centrum odbiorcze (RCO),
- grupa urządzeń radiotelefonicznych,
- urządzenia automatycznego systemu alarmowania przez radio,
- urządzenia telekonferencyjne.

Ponadto w strukturze węzła występują: stacja pocztowa oraz zespoły funkcjonalne zapewniające prawidłową pracę węzła (stacja zasilania, grupa eksploatacji i konserwacji, warsztat sprzętu łączności, biuro instalacji i remontów i inne).

---

[10] Do roku 2002 wyróżniane były kategorie garnizonowych węzłów łączności, zależne od szczebla jednostki lub instytucji w garnizonie. Obecnie, również w podobnej zależności, występuje etat garnizonowego węzła łączności. Odpowiada mu stopień szefa GWŁ.

[11] W ramach CWŁ MON funkcjonuje kilkanaście central telefonicznych o łącznej pojemności powyżej 10 000 NN.

[12] W poszczególnych obiektach – centralach CWŁ urządzenia wyodrębnionych grup tworzą tzw. stacje (stacja teletransmisji, stacja telefoniczna, stacja łączności specjalnej, itp.)

Garnizonowe węzły łączności niższego szczebla (np. w garnizonach z siedzibami dowództw okręgów – etat pułkownik, dowództw dywizji – ppłk /2 garnizony/ lub mjr), w zależności od liczby i wielkości jednostek stacjonujących w garnizonie, mają wyposażenie adekwatne do potrzeb. Stąd też można stwierdzić, że w stacjonarnym systemie łączności SZ RP nie występują (jak poprzednio) GWŁ-y o standardowym (zależnym od kategorii-etatu) wyposażeniu. Analiza wyposażenia GWŁ-ów pozwala jednak na stwierdzenie, że w większości z nich znajduje się:

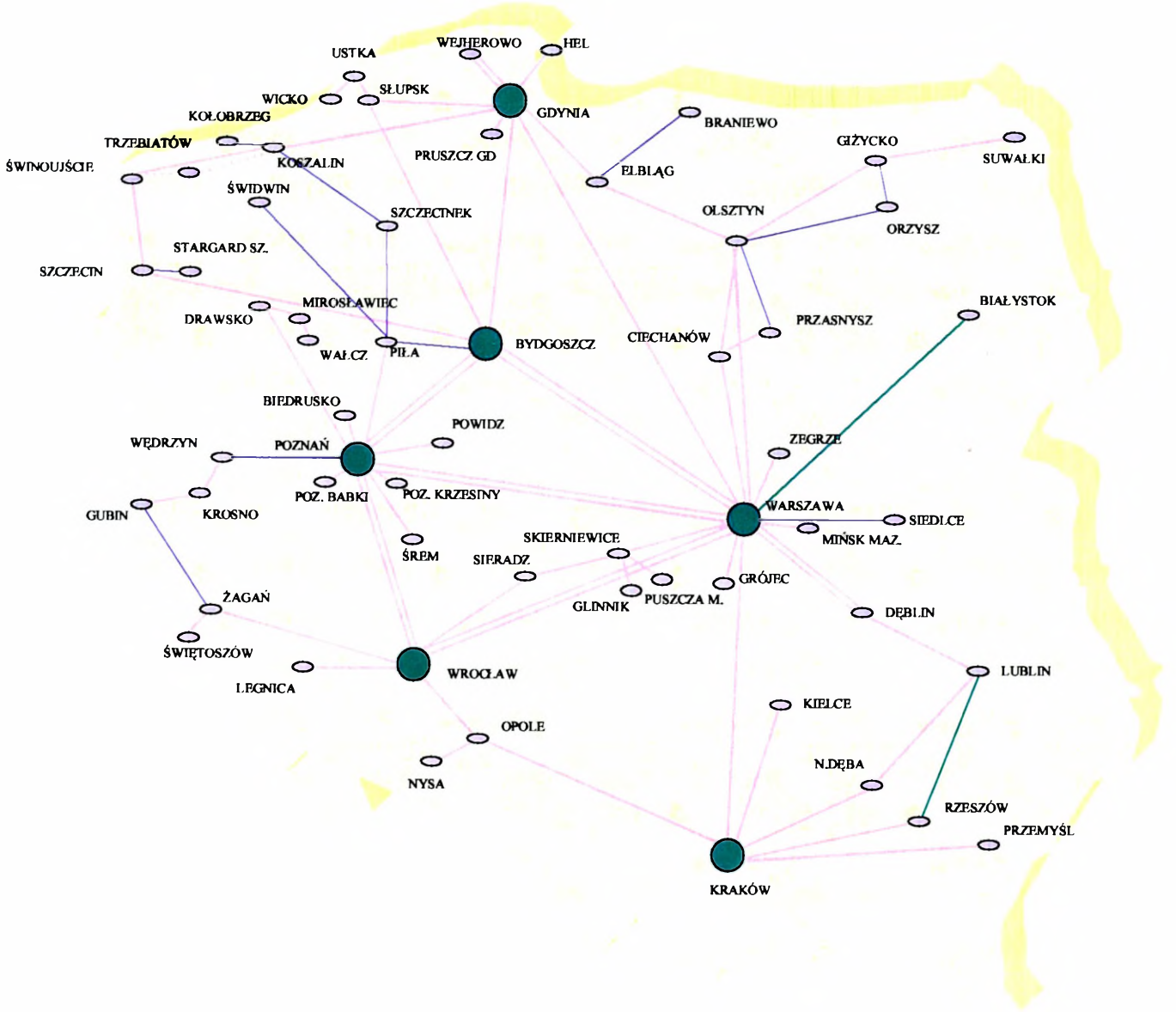
- automatyczna elektroniczna centrala miejscowo/międzymiastowa,
- urządzenie telefonicznego systemu alarmowania,
- stacja teletransmisji (w części z nich z urządzeniami radioliniowymi),
- urządzenia telefaksowe,
- stacja łączności utajnionej,
- stacja łączności specjalnej (w części),
- stacja radiowa (w większości i wyposażone w systemy alarmowania przez radio),
- stacja zasilania i inne zespoły pomocnicze.

Garnizonowe węzły łączności każdego szczebla są stosownie do potrzeb sprzężone z elementami łączności sieci publicznej (centralą miejską) i sieci wewnętrznych (np. resortu wewnętrznych i administracji) rozmieszczonymi na terenie danego garnizonu. Garnizonowe węzły łączności świadczą usługi, zgodnie ze swoim przeznaczeniem, w dwóch kategoriach: przekazu technicznymi środkami telekomunikacyjnymi (w podsystemie radioliniowo-kablowym lub radiowym) oraz poprzez transport i doręczanie przesyłek (w podsystemie poczty polowej).

Podsystem radioliniowo-kablowy

Podsystem radioliniowo-kablowy składa się z central telefonicznych garnizonowych węzłów łączności i sieci linii dalekosiężnych łączących je ze sobą. Sieć linii dalekosiężnych składa się z łączy (lub ich części) dzierżawionych z sieci publicznej (sieci telekomunikacyjnej TP S.A. – przeważająca większość łączy), łączy resortu obrony narodowej (kilka) oraz sporadycznie innych operatorów (np.: „Tel-energo" S.A.). Dzierżawa łączy od innych operatorów odbywa się na mocy ustawy „Prawo telekomunikacyjne" (art. 76, 77 i 78) oraz umów dwustronnych z operatorami. Liczba i rodzaj dzierżawionych łączy pozwala na zachowanie od-

powiedniego potencjału sieci, zapewniającego wykonywanie zadań i dużą niezawodność. Topologię węzłów garnizonowych i linii teletransmisyjnych przedstawia rys 1.1.1.1.



Rys.1.1.1.1. Topologia sieci radioliniowo-kablowej stacjonarnego systemu łączności SZ RP (rysunek poglądowy)[13]

Jak można zaobserwować, w sieci radioliniowo-kablowej przyjęta została zasada istnienia tzw. „drogi obejścia". Praktycznie każdy GWŁ o większym znaczeniu ma co najmniej dwie drogi połączeniowe do dowolnego innego węzła (topologia wieloboku). Zapewnia to zachowanie sprawności poszczególnych relacji nawet przy znacznych uszkodzeniach sieci. Ponadto, w przypadku awarii, możliwe jest zastosowanie w sieci publicznej alternatywnego

[13] Ze względu na klauzulę dokumentu rysunek został zmodyfikowany, aby oddawał istotę budowy sieci bez odzwierciedlenia rzeczywistości.

połączenia (poszukiwania innej, kolejnej drogi[14]), co zapewnia stosowanie w systemie nowoczesnych central elektronicznych[15] i cyfrowych łączy, lub przekazanie informacji w podsystemie radiowym, który może być sprzężony w ramach GWŁ z siecią radioliniowo-kablową. Istnieje także możliwość zestawienia połączenia za pomocą radiolinii, jeżeli znajdują się one w wyposażeniu węzłów.

Stacjonarna sieć radioliniowo-kablowa wykorzystywana jest przede wszystkim, jako sieć podstawowa, w bieżącej działalności wojsk i komórek funkcjonalnych resortu obrony. Przekazywane w niej są informacje jawne i utajnione w postaci fonicznej, telefaksowej bądź transmisji danych. W sieci radioliniowo-kablowej funkcjonują także systemy alarmowania.

Podsystem radiowy

W podsystemie radiowym organizuje się sieci i kierunki radiowe. Są one organizowane wyłącznie na bazie środków radiowych ze składu garnizonowych węzłów łączności. Wykorzystuje się je przede wszystkim w przypadku zaistnienia przerw w łączności kablowej oraz do przekazywania sygnałów powiadamiania i alarmowania wojsk.

Za pomocą środków radiowych może być utrzymywana łączność telefoniczna i transmisja danych jawna i utajniona oraz w zależności od relacji i potrzeb wiadomości mogą być szyfrowane i kodowane. Łączność radiową utrzymuje się w sieciach i kierunkach radiowych zorganizowanych przez Sztab Generalny WP i dowództwa rodzajów wojsk (także dowództwa okręgów). Sieci radiowe organizowane przez Sztab Generalny WP są czynne całą dobę i radiostacje obsługują pracownicy etatowi GWŁ-ów. Pozostałe sieci radiowe najczęściej uruchamiane są w miarę potrzeb. W sieciach radiowych funkcjonują także systemy automatycznego alarmowania.

W ramach systemu radiowego wykorzystywane są przede wszystkim radiostacje KF średniej mocy i (w mniejszych garnizonach) radiostacje UKF. System łączności radiowej jest uzupełniany systemem łączności radiotelefonicznej zbudowanym w oparciu o radiotelefony różnych typów (stare K-1M i R-1433 lub nowe radiotelefony o „cywilnej" konstrukcji a także radiostacje wyposażone w bloki sprzężenia radiowego) zainstalowane w garnizonowych węzłach łączności. System łączności radiotelefonicznej współpracuje z systemem łączności ra-

---

[14] Jest to możliwe tylko w przypadku transmisji jawnej.
[15] Praktycznie ostatnie egzemplarze central analogowych są obecnie wycofywane w stacjonarnym systemie łączności SZ RP z użytku.

dioliniowo-kablowej i umożliwia połączenia abonentów radiotelefonicznych znajdujących się w ruchu lub na postoju z abonentami sieci telefonicznej.

Podsystem informatyczny

W ramach podsystemu informatycznego funkcjonuje rozległa sieć teleinformatyczna NATO, której terminale znajdują się na stanowiskach dowodzenia (kierowania) szczebla strategicznego i operacyjno-taktycznego[16]. Funkcjonuje także sieć rozległa MIL-WAN – wewnętrzna sieć internetowa (intranet) Sił Zbrojnych RP oraz wykorzystywane są w sieci publicznej usługi internetowe (w zakresie przewidzianym dla korespondencji jawnej). Lokalne sieci informatyczne reprezentowane są przez wiele komercyjnych (ogólnodostępnych) aplikacji w sieciach wewnętrznych jednostek wojskowych i instytucji MON. Są to sieci albo sprzężone z siecią telekomunikacyjną (a więc i z sieciami publicznymi) i odpowiednio zabezpieczone, albo sieci całkowicie odizolowane od innych (rozdzielone fizycznie a nie tylko programowo). W sieciach sprzężonych z innymi sieciami (z możliwością jakiegokolwiek połączenia z siecią publiczną) wykorzystuje się systemy (aplikacje) zapewniające przetwarzanie danych i komunikację w zakresie jawnego obiegu informacji.[17] W systemach izolowanych wykorzystywane są aplikacje niezbędne do funkcjonowania jednostek i instytucji (np.: aplikacje finansowe, ewidencyjne, bazy danych) oraz ćwiczeń i treningów (np.: symulatory).

1.1.2. Charakterystyka polowych sieci telekomunikacyjnych i informatycznych

Polowe sieci telekomunikacyjne i informatyczne są, obok sieci stacjonarnych, drugim istotnym komponentem podsystemu przekazywania informacji. Są rozwijane siłami jednostek wsparcia dowodzenia i mogą realizować swoje funkcje praktycznie w każdych warunkach, w jakich mogą działać jednostki wojskowe. Ponieważ bieżąca działalność instytucji i jednostek wojskowych odbywa się w miejscach stałej dyslokacji czyli w miejscach o rozbudowanej infrastrukturze telekomunikacyjnej i informatycznej, więc polowe sieci telekomunikacyjne i informatyczne z zasady wykorzystywane są tylko wtedy, gdy są niezbędne, a więc w działaniach bojowych wojsk.

Polowe sieci telekomunikacyjne i informatyczne są więc takim składnikiem systemu dowodzenia, który zapewnia dowódcy (i organom dowodzenia rozmieszczonym w komór-

---

[16] Ze względu na przeznaczenie i sposób wykorzystania tej sieci nie jest ona przedmiotem badań.
[17] Lub odpowiednio zabezpieczone (kodowane) sposoby transmisji.

kach funkcjonalnych stanowisk dowodzenia) każdego szczebla dowodzenia, łączność z wojskami w warunkach zagrożenia lub prowadzenia działań zbrojnych, w każdych możliwych warunkach terenowych pogodowych i przy destrukcyjnym oddziaływaniu przeciwnika.

Wzrost znaczenia informacji w działaniach (nie tylko bojowych) i jej decydujący wpływ na wyniki procesu dowodzenia powodują, że cechą charakterystyczną współczesnych działań jest pozyskiwanie, przetwarzanie i dystrybucja coraz większych ilości informacji. Powoduje to wzrost wymagań w stosunku do systemów przekazywania i przetwarzania informacji. Powoduje to jednocześnie stawanie się tych systemów obiektem ataku o największym znaczeniu[18]. Stąd też wymagania stawiane polowym systemom łączności (terminowość, wierność i skrytość) określają ich przydatność w działaniach. Ponieważ polowe systemy łączności stały się priorytetowym obiektem rozpoznania i rażenia przez przeciwnika a jednocześnie (do tego są przewidziane z zasady) powinny funkcjonować w każdych warunkach otoczenia, więc ich struktura, zakres rozwinięcia, taktyka użycia, są zależne od wielu czynników, wśród których wymienić należy:

- czas przygotowania i wykonania zadania;
- odległości przemieszczeń;
- obszar prowadzenia działań;
- siła i sposób prowadzenia działań przeciwnika;
- prędkość przemieszczenia i prowadzenia działań;
- częstotliwość i wielkość zmian sytuacji taktycznej (operacyjnej);
- złożoność struktury ugrupowania oraz gęstość jego elementów;
- zależność od różnego rodzaju okoliczności, otoczenia i uwarunkowań (pora doby, oddziaływanie radioelektroniczne otoczenia, itp.).

Sprostanie wymaganiom systemu dowodzenia i uwzględnienie pozostałych czynników otoczenia determinuje wieloskładnikowość polowej sieci telekomunikacyjnej, w której, w zależności od szczebla, można wyróżnić następujące elementy składowe:

- podsystem radioliniowo-kablowy – sieci radioliniowo-kablowe,
- podsystem radiowy – sieci radiowe KF i sieci radiowe UKF.

---

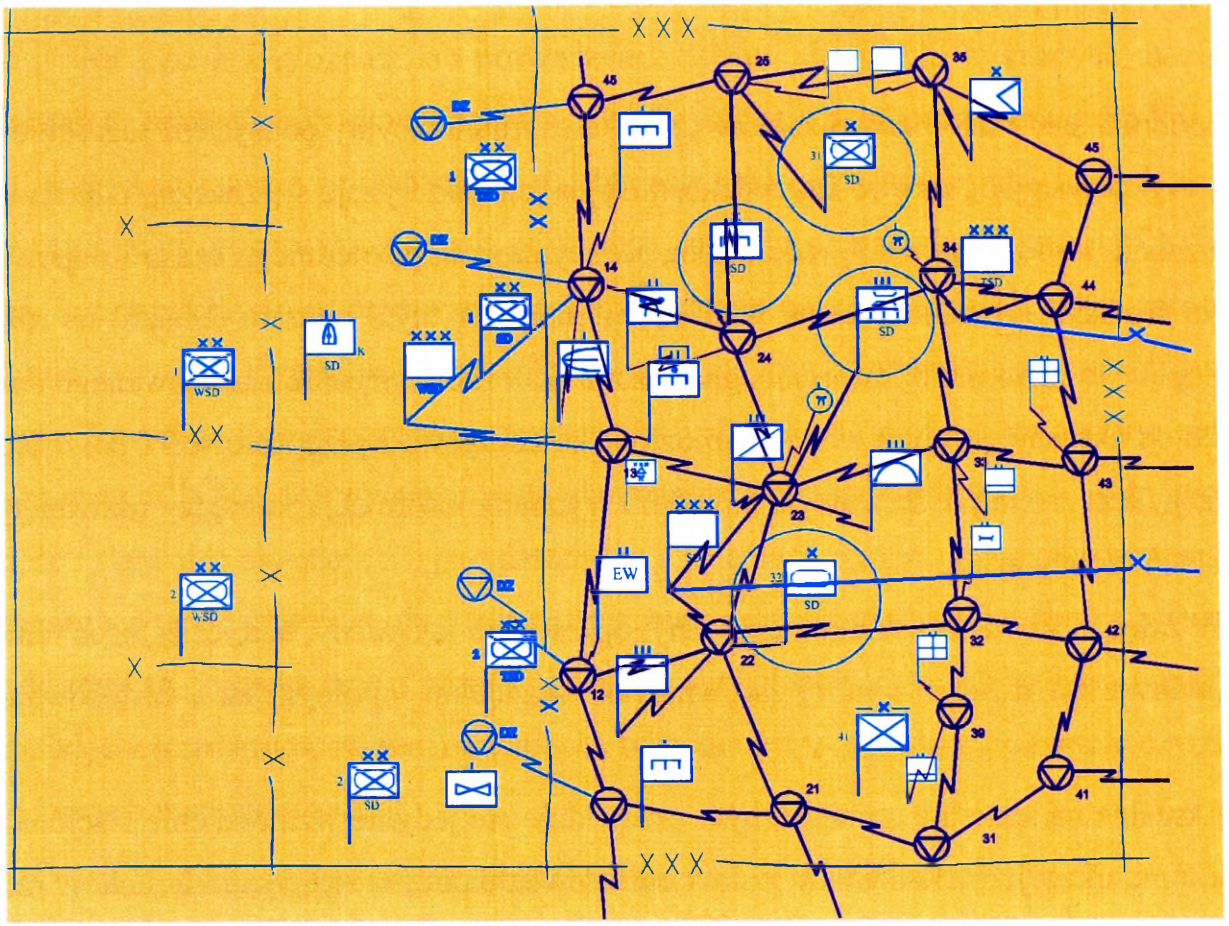
[18] „Atak na informację" jest praktycznie cechą charakterystyczną nie tylko współczesnych konfliktów zbrojnych – jest także „normalnym" elementem np. konkurencji rynkowej.

Podsystem radioliniowo-kablowy

Mobilna sieć radioliniowo-kablowa jako telekomunikacyjny podsystem radioliniowo-kablowy wykorzystujący torowe środki transmisyjne, charakteryzuje się znaczną odpornością na rozpoznanie i oddziaływanie przeciwnika, ale wymaga odpowiedniego czasu i odpowiedniej ilości środków (w zależności od wielkości i charakterystyki obszaru działań) na rozwinięcie. Zapewnia za to praktycznie nieograniczone (zależne wyłącznie zastosowanego sprzętu, a więc od aktualnego stanu techniki) możliwości usługowe i przepustowości poszczególnych relacji. Jest zatem podstawowym środkiem wymiany informacji pomiędzy rozwiniętymi stanowiskami dowodzenia.

W zależności od szczebla (strategiczny, operacyjno-taktyczny, taktyczny) sieć radioliniowo-kablowa ma różną strukturę, zarówno pod względem topologii jak i zastosowanego sprzętu.

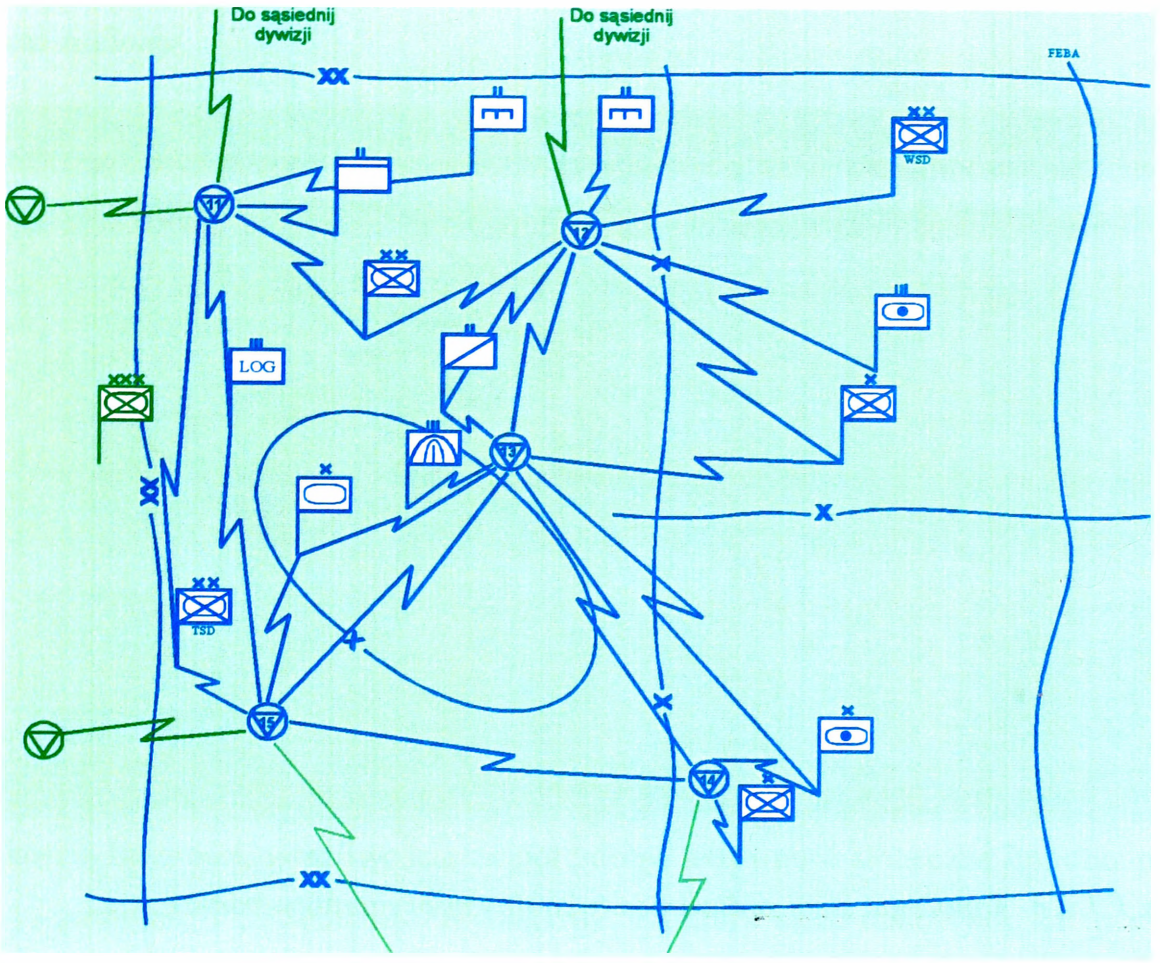
Aktualna na szczeblu strategicznym przewiduje się jedynie wzmocnienie stacjonarnej sieci telekomunikacyjnej elementami polowymi i (ewentualne) rozwinięcie kierunków radioliniowych do bezpośrednio podległych dowództw związków operacyjnych (taktycznych). Na szczeblu związku operacyjnego sieć radioliniowo-kablowa jest najbardziej rozbudowaną siecią telekomunikacyjną. Składa się z wielu (16÷25 a w szczególnych warunkach nawet więcej) węzłów połączonych ze sobą kierunkami radioliniowymi o dużej przepustowości. Do węzłów tych liniami radiowymi lub (w uzasadnionych przypadkach) kablowymi podłączone są węzły łączności stanowisk dowodzenia. Wieloboczna (tzw. kratowa) topologia sieci i dołączanie węzłów łączności stanowisk dowodzenia do 2 (szczebel związku operacyjnego i związku taktycznego) lub 1 (szczebel oddziału) węzłów sieciowych gwarantuje wysokie prawdopodobieństwo zapewnienia połączenia i utworzenie go na praktycznie dowolną odległość na obszarze pokrytym siecią (rys.1.1.2.1.).



Rys.1.1.2.1. Topologia sieci radioliniowo-kablowej (ciemne linie) związku operacyjnego (wariant)

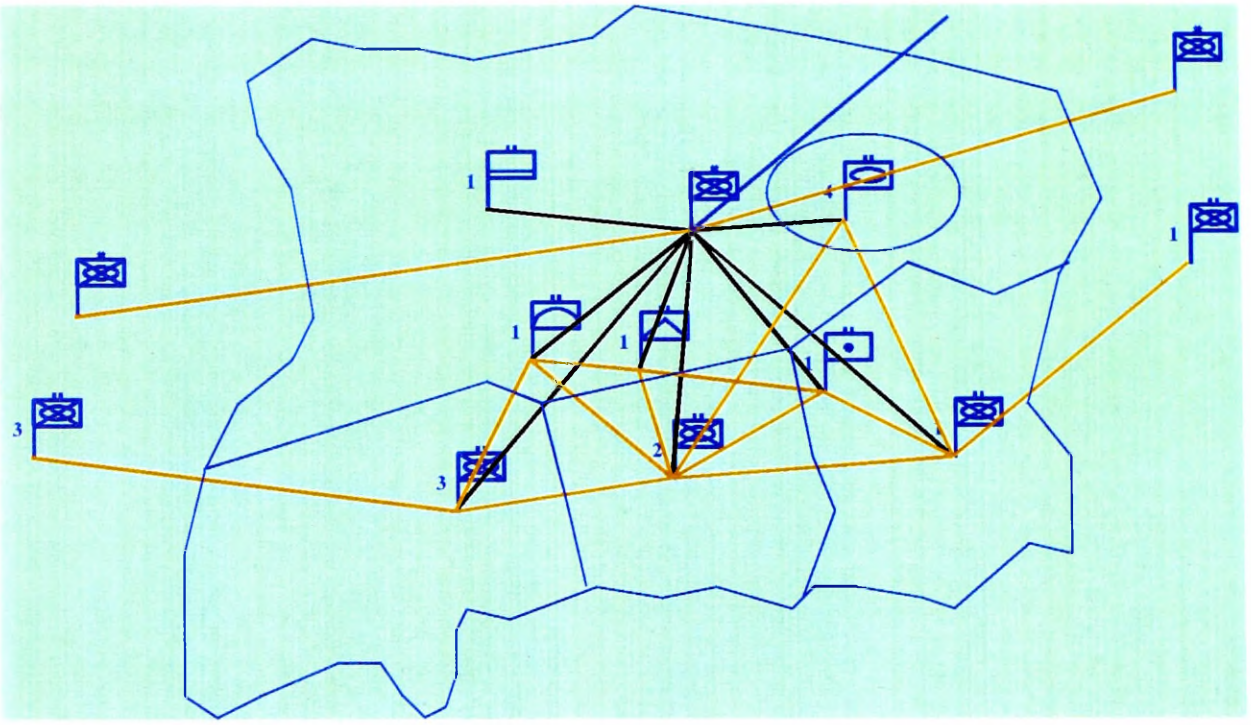
Struktura sieci radioliniowo-kablowej związku taktycznego jest w zasadzie dostosowana do wymogów współczesnego pola walki. Konstrukcja sieci oparta jest na 2÷6 pomocniczych węzłach łączności (PWŁ) połączonych między sobą i z węzłami sieci sąsiadów oraz przełożonego radiowymi liniami dalekosiężnymi (rys.1.1.2.2.).

Do takiej sieci dołączone są węzły łączności stanowisk dowodzenia związku taktycznego, oddziałów i samodzielnych pododdziałów (kablowo). co zapewnia możliwość wykorzystywania alternatywnych dróg połączeniowych np.: przez sieć przełożonego lub sąsiada, możliwość wykorzystywania systemu radiodostępu, zwiększenie efektywności wykorzystywania sieci, mobilności i podatności na rekonfiguracje całej sieci ze względu na wykorzystywanie w większości połączeń linii radiowych.



Rys.1.1.2.2. Topologia sieci radioliniowo-kablowej związku taktycznego (wariant)

Inaczej wygląda struktura sieci radioliniowo-kablowej brygady (rys.1.1.2.3.). Konstrukcja sieci oparta jest w zasadzie na węźle łączności stanowiska dowodzenia brygady, dołączonym poprzez radiolinie do PWŁ sieci radioliniowo-kablowej przełożonego i, ewentualnie (w ramach organizacji łączności współdziałania), do węzłów łączności stanowisk dowodzenia sąsiednich brygad. Pozostałe relacje – pomiędzy WŁ SD brygady a węzłami łączności podległych pododdziałów oraz, w ramach łączności współdziałania, pomiędzy podległymi pododdziałami, budowane są liniami kablowymi. Taka struktura sieci radioliniowo-kablowej jest efektem niewielkich obecnie możliwości sprzętowych batalionu dowodzenia brygady i podległych pododdziałów.



Rys. 1.1.2.3. Topologia sieci radioliniowo-kablowej brygady (wariant)

Podstawowymi urządzeniami transmisyjnymi w polowych sieciach radioliniowo-kablowych są radiolinie horyzontowe, umożliwiające tworzenie traktów cyfrowych o przepustowości do 2 Mbit/s i zapewniające zasięg łączności do ok. 25 km (maksymalnie, w sprzyjających warunkach do 40 km). Ich zaletą, w porównaniu do linii kablowych jest krótki czas rozwijania. Drugim środkiem transmisyjnym jest kabel. Budowane przy wykorzystaniu kabli linie łączności zapewniają transmisję sygnałów z szybkością (zależnie od długości linii) do 512 kbit/s.

Zaletami polowych sieci radioliniowo-kablowych są: duża przepustowość łączy, możliwość obsługi ruchu o dużym natężeniu, duża skrytość, duża odporność na działanie przeciwnika (stosowanie dróg obejściowych, możliwość rekonfiguracji), możliwość dowiązania do stacjonarnego systemu łączności Sił Zbrojnych a także publicznych systemów telekomunikacyjnych, świadczenie usług teleinformatycznych. Wadami natomiast są: brak możliwości pracy w ruchu i dość długi czas budowy sieci (węzeł – około 1 godziny, cała sieć – kilka godzin).

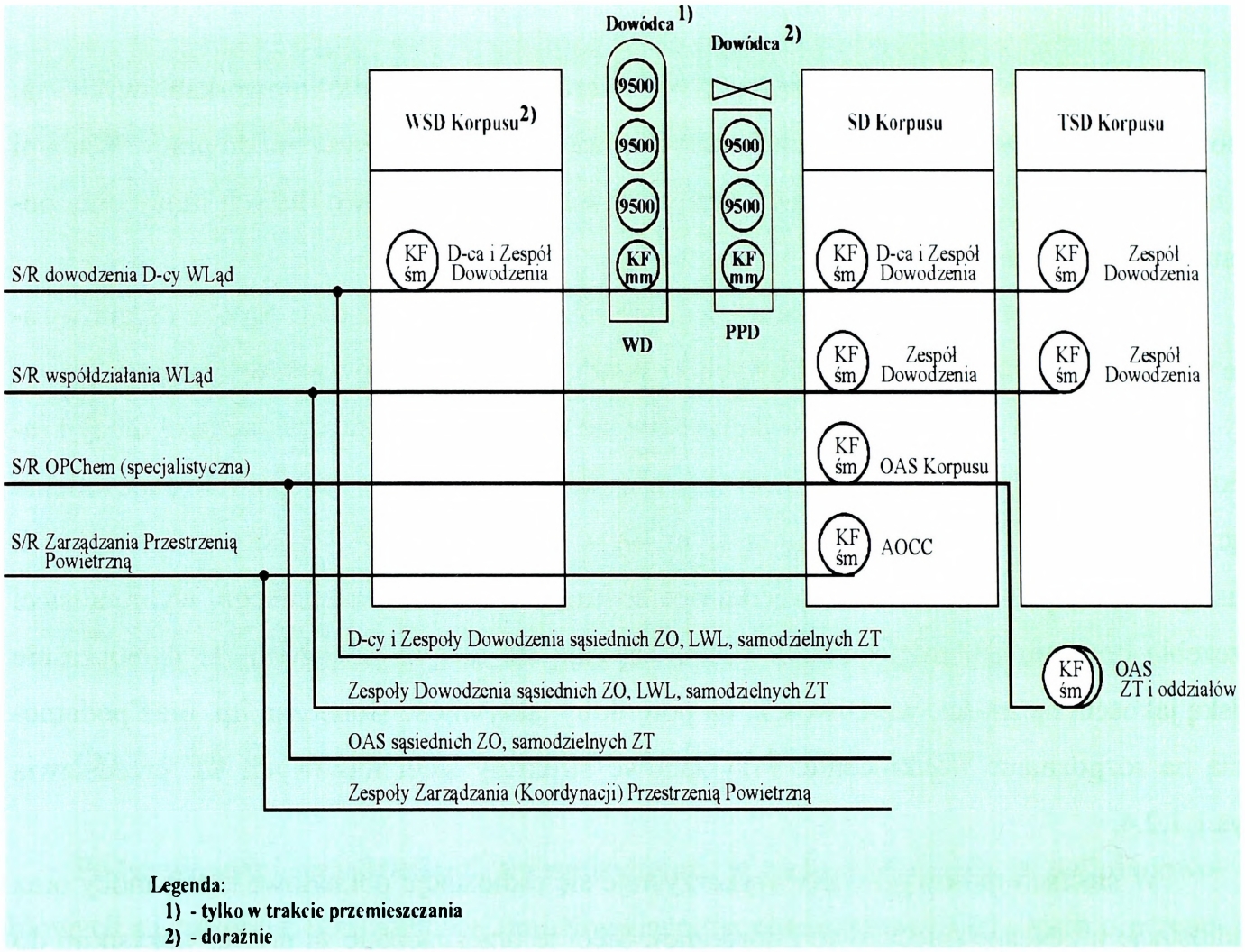
Podsystem radiowy

Zaletami podsystemu radiowego, w stosunku do sieci radioliniowo-kablowych, są: możliwość pracy w ruchu i praktycznie natychmiastowa gotowość systemu do pracy. Wadami – mała skrytość sieci radiowych związana z używaniem stosunkowo dużych mocy oraz podatność na zakłócanie przez przeciwnika.

W podsystemie radiowym organizuje się sieci i kierunki radiowe. Są one organizowane wyłącznie na bazie środków radiowych ze składu garnizonowych węzłów łączności.

W sieciach radiowych KF wykorzystuje się radiostacje przewoźne średniej mocy i radiostacje pokładowe małej mocy. Sieci te przeznaczone są przede wszystkim do zapewnienia łączności osobom funkcyjnym znajdującym się w ruchu na odległościach przekraczających zasięg środków UKF (szczebel związku operacyjnego i związku taktycznego, wybrane sieci szczebla oddziału np. rozpoznania). Charakteryzują się dużym zasięgiem ale jednocześnie niską jakością łączności, wrażliwością na porę doby, aktywność słoneczną itp. oraz podatnością na rozpoznanie i zakłócenie. Przykładowe struktury sieci radiowych KF przedstawia rys.1.1.2.4.

W sieciach radiowych UKF wykorzystuje się radiostacje pokładowe małej mocy oraz radiostacje przenośne (plecakowe i doręczne). Sieci te przeznaczone są przede wszystkim do zapewnienia łączności osobom funkcyjnym znajdującym się w ruchu (lub gdy przynajmniej jedna z nich przemieszcza się i nie może wykorzystywać sieci radioliniowo-kablowej) oraz do zapewnienia łączności w systemach sterowania środkami rażenia (ze względu na konieczną szybkość wymiany informacji i częstą zmianę stanowisk ogniowych środków rażenia). Zapewniają one łączność w zakresie od kilku do około 20÷30 km (zależnie od warunków terenowych i mocy radiostacji). Wykorzystywane są jako podstawowy środek łączności na najniższych szczeblach dowodzenia (do brygady włącznie). Zapewniają dobrą jakość łączności ale o ich stosowaniu decyduje niewielki zasięg.



Rys.1.1.2.4. Struktura sieci radiowych KF (wybrane elementy, wariant)

W strukturze sieci radiowych wyodrębnia się, w zależności od przeznaczenia sieci i uczestniczących w niej korespondentów:

- sieci dowodzenia –stanowią zasadniczy rodzaj łączności radiowej z podległymi oddziałami (pododdziałami) lub elementami ugrupowania, służą przede wszystkim do przekazywania krótkich informacji fonicznych. Jako praca uzupełniającą może być w nich realizowana transmisja danych.
- sieci specjalistyczne – stanowią radiowe sieci zintegrowanych, zautomatyzowanych systemów radiokomunikacyjnych: obrony przeciwlotniczej, artylerii, rozpoznania, obrony przeciwchemicznej, (w perspektywie także zarządzania siecią łączności). Zadaniem tych sieci jest przede wszystkim przesyłanie informacji (sygnałów, komend) w systemach sterowania środkami rażenia lub zautomatyzowanych systemach zbierania i przetwarzania informacji. Powinny one także posiadać odpowied-

nie interfejsy pozwalające na wymianę informacji z innymi sieciami radiowymi oraz w sieci radioliniowo-kablowej.[19]

- sieci radiodostępu – powinny funkcjonować jako sieci wielokanałowe (obecnie trwają zaawansowane badania dostępu jednokanałowego i wstępne - wielokanałowego), pozwalając przede wszystkim na przesyłanie informacji fonicznych oraz danych abonentom ruchomym znajdującym się w danym obszarze objętym zasięgiem stacji radiodostępu.
- sieci współdziałania – są sieciami doraźnie organizowanymi (zgodnie z zasadami organizowania współdziałania). W perspektywie możliwe będzie także wykorzystywanie sieci radiodostępu jako sieci współdziałania.
- sieci logistyki (oraz inne sieci, które funkcjonują jako sieci specjalistyczne w niezautomatyzowanych systemach).

Podsystem informatyczny

W ramach podsystemu informatycznego, na stanowiskach dowodzenia funkcjonują lokalne sieci komputerowe zbudowane w oparciu o aparatownie RWŁC-10/K lub RWŁC-10/T (węzeł pakietowy jako router), elementy informatyczne wozów dowodzenia i wozów dowódczo-sztabowych oraz elementy informatyczne zautomatyzowanych wozów dowódczo-sztabowych „Szafran" (perspektywa). W ramach lokalnych sieci komputerowych funkcjonują programy wspomagające proces dowodzenia, programy specjalistyczne (np.: kalkulacyjne logistyki, opchem, diagnostyczne systemu łączności), programy użytkowe niespecjalistyczne (edytory teksty, grafiki) oraz programy komunikacyjne (poczta itp.). Wykorzystanie węzła pakietowego aparatowni transmisyjnej lub komutacyjnej zapewnia wykorzystanie sieci radioliniowo-kablowej jako podsystemu transmisyjnego i utworzenie rozległej sieci teleinformatycznej.

[19] Obecnie takie sieci są dopiero tworzone w zautomatyzowanych systemach sterowania środkami rażenia.

1.2. Wykorzystanie wojskowych sieci telekomunikacyjnych i informatycznych w czasie pokoju

W czasie pokoju system telekomunikacyjny i informatyczny działa w oparciu o stacjonarny system łączności i informatyki Sił Zbrojnych RP. Jest to podyktowane dwoma względami:

1) ekonomicznym, gdyż zastosowanie mobilnego sprzętu jest wielokrotnie droższe (nawet ćwiczenia i treningi odbywające się w czasie pokoju pozwalają na sprawdzenie skuteczności polowego systemu łączności w zasadzie jedynie fragmentaryczne).

2) bezpieczeństwa systemu dowodzenia – zastosowanie w czasie pokoju systemów łączności przeznaczonych do skrytego dowodzenia wojskami w czasie wojny prowadzi do ich wcześniejszego rozpoznania i przygotowania do obezwładnienia, przez co stają się praktycznie bezwartościowe w czasie, na który są przeznaczone. Stąd też, pomijając, co było wcześniej argumentowane, wykorzystywanie polowych sieci telekomunikacyjnych w czasie ćwiczeń, w okresie pokoju „użytkowany" jest jedynie system telekomunikacyjny i informatyczny w ramach stacjonarnego systemu łączności Sił Zbrojnych.

Również ze względów ekonomicznych, w okresie pokoju stacjonarny system łączności i informatyki rozwinięty jest w ograniczonym zakresie, tzn., że zabezpiecza on głównie potrzeby kierowania działalnością wojsk podczas ich pobytu w garnizonach (miejscach stałej dyslokacji) i w rejonach ćwiczeń. Zapewnia (częściowo) także łączność na potrzeby prywatne żołnierzy zawodowych.

1.2.1. Łączność wewnętrzna resortu Obrony Narodowej i dowodzenie jednostkami wojskowymi

W czasie pokoju utrzymywana jest w systemie stacjonarnym:

- łączność jawna w relacjach międzynarodowych z organami dowodzenia Sojuszu Północnoatlantyckiego, dostępność tej usługi jest częściowo ograniczona,
- łączność utajniona w relacjach międzynarodowych z organami dowodzenia Sojuszu Północnoatlantyckiego, dostępność do tego rodzaju łączności jest ściśle określona

(szczebel dowodzenia i kierowania, zakres wykorzystania) i odbywa się poprzez urządzenia wspólne dla państw-członków Sojuszu,

- łączność jawna w relacjach krajowych, dostępność do tego rodzaju łączności nie jest ograniczona (z wyjątkiem taryfikowanych połączeń poza sieć wewnętrzną MON),
- łączność utajniona w podsystemie cyfrowej łączności utajnionej (PCŁU), dostępność, szczebel wykorzystania i przeznaczenie ściśle określone,
- podsystem szybkiej łączności alarmowania – dostępność, szczebel wykorzystania i przeznaczenie ściśle określone,
- podsystem łączności dyżurnych służb operacyjnych – dostępność, szczebel wykorzystania i przeznaczenie ściśle określone,
- podsystem łączności radiowej (w tym radiowe systemy alarmowania), – dostępność, szczebel wykorzystania i przeznaczenie ściśle określone,
- podsystem poczty polowej, – dostępność ograniczona do przesyłek służbowych, praktycznie w ramach resortu obrony narodowej,
- łączność jawna i utajniona w relacjach organizowanych wewnątrz stacjonarnego systemu łączności SZ, sprzężonego z polowymi systemami wojsk lub przy zewnętrznym wsparciu publicznych podmiotów telekomunikacyjnych w celu przeprowadzenia ćwiczeń z wykorzystaniem stacjonarnego systemu łączności (np. Canon Cloud) – organizowana sporadycznie w związku z ćwiczeniami, dostępność ściśle określona i kontrolowana,
- łączność radiowa jawna i utajniona związana z bezpieczeństwem lotów, nawigacją i łącznością z jednostkami pływającymi – dostępność ściśle określona i kontrolowana.

1.2.2. Przygotowanie systemu łączności i informatyki SZ RP na potrzeby obronne państwa

Podstawowym zadaniem stacjonarnego systemu łączności jest zapewnienie wymiany informacji dla celów dowodzenia, współdziałania, powiadamiania i ostrzegania w okresie pokoju, kryzysu i wojny. Ponieważ to stan kryzysu i stan wojny stwarzają dla systemu dowodzenia (kierowania) jak i dla systemu łączności warunki ekstremalne, więc w czasie pokoju systemy te powinny być przygotowywane do działania w potencjalnie prawdopodobnych warunkach, jakie mogą nastąpić w czasie kryzysu lub wojny.

Podstawy prawne przygotowywania systemów łączności (telekomunikacyjnych jak i pocztowych) stanowią akty prawne (ustawy i rozporządzenia Rady Ministrów) nakazujące

i precyzujące zakres wykonywanych przedsięwzięć w systemach telekomunikacyjnych w czasie pokoju w celu przygotowania i przystosowania ich do wykonywania zadań i prawidłowego funkcjonowania w trakcie kryzysu lub wojny.

W ramach działalności operatorów telekomunikacyjnych, w tym także resortu Obrony Narodowej, wymagane jest przygotowanie systemu łączności do działania w warunkach szczególnych. W tym celu nakazane jest przygotowanie systemów łączności „na potrzeby obronne państwa”[20]. Systemy takie powinny charakteryzować się:

- niezawodnością,
- odpornością na zakłócenia,
- zdolnością zapewnienia użytkownikom specjalnym (np. organom władzy publicznej, siłom zbrojnym) bezpiecznego przekazywania informacji,
- zdolnością zachowania ciągłości łączności podczas zmian miejsc pracy, w ramach stanowisk kierowania,
- zdolnością do elastycznej rekonfiguracji systemu,
- zdolnością do preferencyjnej obsługi użytkowników specjalnych.

Przygotowanie i wykorzystanie obronnych systemów łączności obejmuje planowanie, organizowanie i realizację przedsięwzięć umożliwiających kierowanie państwem w warunkach zagrożenia bezpieczeństwa państwa i w czasie wojny lub dowodzenie Siłami Zbrojnymi RP. Przygotowanie obronnych systemów łączności realizuje się w szczególności przez:

- precyzowanie potrzeb w zakresie łączności,
- analizę możliwości przedsiębiorców telekomunikacyjnych i pocztowych w zakresie ich wykorzystania na potrzeby obronne,
- planowanie wykorzystania istniejących systemów łączności na potrzeby obronne państwa[21],
- wytypowanie osób odpowiedzialnych za planowanie, wdrażanie, zarządzanie i eksploatację obronnych systemów łączności,
- precyzowanie standardów wyposażenia stanowisk kierowania,

---

[20] Rozporządzenie Rady Ministrów z dnia 3 sierpnia 2004 r. w sprawie przygotowania i wykorzystania systemów łączności na potrzeby obronne państwa. Rozporządzenie to jest spójne z wcześniejszymi zapisami w ustawie „prawo telekomunikacyjne” dotyczącymi przygotowania systemów telekomunikacyjnych do działania w warunkach szczególnych.

[21] Podobnie precyzowane są w ustawie „Prawo telekomunikacyjne” obowiązki operatorów telekomunikacyjnych w ramach przygotowania systemów łączności do działania w warunkach kryzysu.

- wykonywanie inwestycji.

Przygotowanie obronnych systemów łączności w zakresie telekomunikacji realizuje się w szczególności przez:

- opracowanie zasad współpracy sieci przedsiębiorców telekomunikacyjnych z resortowymi sieciami telekomunikacyjnymi,
- dostosowywanie obiektów i infrastruktury telekomunikacyjnej do współpracy z ruchomymi urządzeniami telekomunikacyjnymi zgodnie z potrzebami określanymi w szczególności przez Ministra Obrony Narodowej lub ministra właściwego do spraw wewnętrznych.

Przygotowanie obronnych systemów łączności dokonuje się w czasie pokoju, przy uwzględnieniu konieczności ich rozwinięcia, rozbudowy i rekonfiguracji w czasie zagrożenia bezpieczeństwa państwa i w czasie wojny.

Obronne systemy łączności wykorzystywane są na potrzeby:

- systemu kierowania bezpieczeństwem narodowym,
- zapewnienia funkcjonowania państwa w razie zagrożenia bezpieczeństwa i w czasie wojny,
- dowodzenia Siłami Zbrojnymi RP,
- współpracy z systemami łączności państw sojuszniczych.

Obronne systemy łączności mogą być wykorzystywane także w czasie pokoju, w tym w razie wystąpienia działań terrorystycznych lub innych szczególnych zdarzeń.

Na Ministrze Obrony Narodowej ciąży ponadto obowiązek wskazywania potrzeb Sił Zbrojnych RP w zakresie telekomunikacji i poczty oraz opracowania warunków wykonywania działalności telekomunikacyjnej i pocztowej w czasie zagrożenia bezpieczeństwa państwa i w czasie wojny przez komórki i jednostki organizacyjne resortu obrony narodowej oraz przez jednostki sił zbrojnych państw sojuszniczych przebywających czasowo na terenie Polski.

Opracowanie planów i wykonawstwo postulowanych inwestycji realizuje minister właściwy do spraw łączności.

Z przedstawionych regulacji prawnych wynika, że w ramach systemu łączności kraju, w warunkach szczególnych, dominującą rolę będzie odgrywał obronny system łączności a w

nim skoordynowane elementy stacjonarnego systemu łączności Sił Zbrojnych, systemów publicznych i innych sieci resortowych, wzmocnione w razie potrzeby mobilnymi wojskowymi systemami łączności.

Rozważając powyższe stwierdzenia w aspekcie przygotowań wojskowych sieci telekomunikacyjnych i informatycznych, zarówno stacjonarnych jak i mobilnych (polowych) należy stwierdzić, co potwierdzone zostało wieloma eksperymentami (także w ramach systematycznych ćwiczeń oddziałów i pododdziałów wsparcia dowodzenia), że współczesne wyposażenie stacjonarnego (centrale) jak i polowego (aparatownie „Storczyk") systemu telekomunikacyjnego pozwala na zapewnienie kompatybilności w niezbędnym zakresie do wzajemnego wykorzystywania zasobów technicznych i usługowych sieci wojskowych i publicznych. Odrębnym problemem jest natomiast gromadzenie danych pozwalających na formułowanie potrzeb w stosunku do sieci telekomunikacyjnych, które mogą być wykorzystywane w sytuacjach reagowania kryzysowego czy wojny. Przepisy stwierdzające, że komórki odpowiedzialne za zapewnienie łączności dla jednostek Sił Zbrojnych RP uczestniczących w działaniach antykryzysowych powinny przekazywać informacje dotyczące zapotrzebowania na zasoby infrastruktury telekomunikacyjnej państwa do komórek dyspozytorskich Stanowiska Kierowania Reagowaniem Kryzysowym MON (SK RK MON), natomiast jednostki operatorów telekomunikacyjnych, powinny gromadzić dane pochodzące z nadzoru własnych sieci oraz przekazywać je do systemu CK KSŁ, nie rozwiązują problemu oceny zagrożeń, podatności/odporności stacjonarnego systemu łączności na te zagrożenia, zakresu możliwego użycia wojsk i wielu innych czynników, które decydują o procesie (długotrwałym i kosztownym) przygotowania wojskowych i cywilnych sieci telekomunikacyjnych do działania w sytuacjach kryzysowych.

1.3. Wykorzystanie wojskowych sieci telekomunikacyjnych i informatycznych w sytuacjach szczególnych

1.3.1. Wykorzystanie wojskowych sieci telekomunikacyjnych i informatycznych w sytuacjach kryzysowych

Definiując sytuacje kryzysowe najczęściej podkreśla się utratę możliwości sprawnego kierowania normalnym działaniem kraju, regionu, miasta. Kryzys zatem cechuje się wzrostem chaosu działania, brakiem (lub opóźnieniem) informacji niezbędnych do prawidłowego podejmowania decyzji, a więc także niedowładem systemu informacyjnego. Zapewnienie sprawnego kierowania reagowaniem kryzysowym wymaga zatem innych – ponad standardowych środków przekazywania informacji pomiędzy poszczególnymi organami władzy, administracji i służb publicznych na każdym szczeblu. Analiza sytuacji kryzysowych, które zaistniały w ostatnich latach na obszarze kraju (np.: powodzie na Śląsku, w Trójmieście, na Podkarpaciu) jak i kryzysów w innych państwach (konflikty etniczne na Bałkanach, zamachy terrorystyczne we Francji i Hiszpanii, powódź w Czechach) potwierdza praktycznie najistotniejsze czynniki w walce z kryzysem – informację i jej terminową dystrybucję do organów decyzyjnych oraz wykonawczych. Niezbędne jest utrzymywanie łączności pomiędzy ośrodkami centralnymi administracji państwowej, wojewódzkimi, powiatowymi i gminnymi zespołami reagowania kryzysowego (tymi, których bezpośrednio lub pośrednio dotyczą działania antykryzysowe), zespołami kierującymi służbami publicznymi oraz grupami zadaniowymi w terenie objętym kryzysem. Istotnym zatem elementem systemu reagowania kryzysowego jest podsystem łączności.

Jednocześnie należy zauważyć, że normalnie funkcjonujące i spełniające swoje zadania systemy łączności, na obszarze objętym kryzysem są często niszczone przez antagonistyczne strony (Bałkany) lub przez żywioł (Śląsk, Czechy), przy czym wielkość tych zniszczeń lub uszkodzeń jest trudna do przewidzenia i może obejmować nawet większość istotnych dla funkcjonowania systemu łączności obiektów na całym, objętym kryzysem obszarze.

Celowe zatem jest tworzenie i utrzymywanie w ciągłej gotowości przedstawionego w poprzednim podrozdziale (i wymaganego odpowiednimi przepisami) obronnego systemu łączności.

Analizując skutki wymienionych kryzysów można skonstatować szybką utratę możliwości transmisyjnych systemów telekomunikacyjnych na każdym obszarze dotkniętym kryzysem. Stąd też należy założyć, a nawet przyjąć za aksjomat, że tylko zintegrowany system

łączności, złożony z dużej ilości technicznie różnych podsystemów, a więc wzajemnie się uzupełniających, może zapewnić wyższe (być może wystarczające) prawdopodobieństwo zapewnienia łączności w sytuacji kryzysowej.

Należy zatem uznać, iż występowanie w systemie łączności Sił Zbrojnych różnych podsystemów telekomunikacyjnych (stacjonarny funkcjonujący w oparciu o własne węzły i dzierżawione linie telekomunikacyjne, mobilny radioliniowo-kablowy, mobilny radiowy) dostosowanych do współpracy z elementami publicznej infrastruktury telekomunikacyjnej powinno umożliwić zachowanie ciągłości funkcjonowania systemu łączności lub szybkie jego rekonfigurowanie i odtworzenie części możliwości na obszarze objętym kryzysem.

Należy również zauważyć, że stacjonarny system łączności SZ RP (w części „przewodowej") jest tak silnie uzależniony od funkcjonowania publicznej sieci telekomunikacyjnej, że praktycznie sprawne działanie sieci publicznej implikuje jego sprawność. Można zatem założyć, że w przypadku gdy prowadzone będą działania antykryzysowe na terenie kraju (lub regionu kraju) i sprawny będzie system telekomunikacyjny kraju, wojskowy system telekomunikacyjny wykorzystywany w operacji reagowania kryzysowego nie ulegnie zmianie. Poza wykorzystywanymi w czasie pokoju sieciami mogą być uruchomione dodatkowe sieci, szczególnie sieci radiowe, zapewniające utrzymanie łączności pomiędzy ośrodkiem kierowania reagowaniem kryzysowym a dowództwami jednostek biorących udział w działaniach oraz sieci zapewniające dowodzenie (i współdziałanie) w ramach komponentu wojskowego. Konieczne jest jednak w tym miejscu podkreślenie, że sieci te nie będą odzwierciedlały systemu dowodzenia, jaki ma zastosowanie w warunkach bojowych lecz będą dostosowane strukturą, rodzajem środków, wykorzystywanymi danymi roboczymi, liczbą i rodzajem korespondentów do rodzaju i warunków prowadzenia działań antykryzysowych.

Większym zmianom ulega sieć łączności w przypadku udziału kontyngentu wojskowego w operacji reagowania kryzysowego za granicą. Operacje takie są z reguły wielonarodowe, stąd też zasady organizacji łączności mogą być (w wielu przypadkach, szczególnie gdy operacja prowadzona jest z wyłącznym lub większościowym udziałem wojsk państw członkowskich NATO) tożsame z ogólnymi zasadami łączności w operacjach wielonarodowych.

Zapewnienie łączności pomiędzy krajem, którego wojska biorą udział w misji i jego sztabem funkcjonującym w strukturze CJTF leży w gestii narodowej i kraj ten ustala sposób wymiany informacji. W gestii koordynatora operacji natomiast leży zapewnienie łączności w systemie stacjonarnym z najwyższymi narodowymi lub wielonarodowymi szczeblami dowodzenia.

Łączność organizowana jest centralnie pomiędzy kwaterą główną misji i poszczególnymi kontyngentami, narodowe kontyngenty wojskowe organizują dla siebie łączność wewnętrzną (a więc system łączności mógłby pozostać bez zmian, gdyby nie czynniki, które charakteryzują większość takich operacji – niewielkie siły na dużym obszarze, brak „przeciwnika", trudny teren o zniszczonej infrastrukturze, duża odległość od kraju i zaplecza logistycznego).

Wszystkie szczeble dowodzenia muszą być zdolne do zapewnienia łączności z narodowym dowództwem państwa-gospodarza, na terenie którego prowadzona jest operacja (co stanowi dodatkowe relacje łączności). Do zapewnienia wymiany informacji pomiędzy sztabem danego kraju i instytucjami państwa, na terenie którego funkcjonuje ten sztab, jako podstawową zasadę przyjęto wykorzystywanie narodowych publicznych sieci telekomunikacyjnych wszędzie tam, gdzie będzie to możliwe (a więc konieczność zapewnienia, przynajmniej w minimalnym zakresie, kompatybilności systemów).

Do zapewnienia wymiany informacji pomiędzy dowództwami sąsiadujących jednostek tego samego szczebla dwóch różnych państw przyjęto wykorzystywanie sieci radiowych i radioliniowych, a w przypadku wspólnego wykonywania zadań - także radiotelefonicznych (co w przypadku polskich jednostek niższych szczebli – np.: batalionu, powoduje konieczność nietypowego wyposażenia).

Wszystkie jednostki biorące udział w operacji powinny stosować możliwie najlepsze środki bezpieczeństwa łączności (co zazwyczaj sprowadza się do wykorzystywania odrębnych środków w każdym kontyngencie narodowym i odrębnych do współdziałania).

W przypadkach, w których nie można zapewnić odpowiedniego poziomu interoperacyjności łączności, mogą być adaptowane procedury narodowe (czyli także organizacyjne trudności z utrzymaniem łączności).

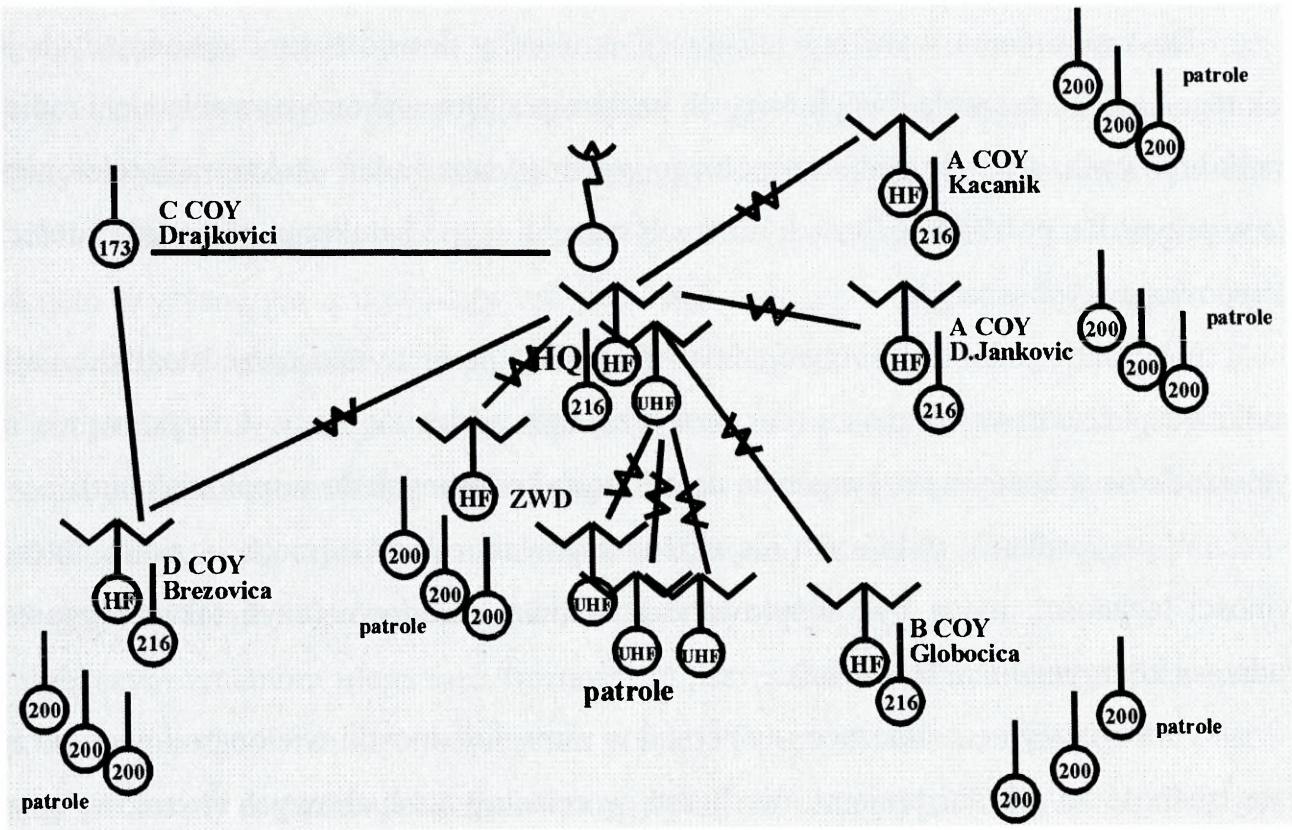
Pododdziały uczestniczące w operacji w ramach jednostki wielonarodowej, utrzymują stałą łączność ze swoimi krajami, niezbędną w celach pozasłużbowych (rozmowy prywatne a więc dodatkowe relacje w sieciach telekomunikacyjnych i informatycznych) oraz służbowych.

Państwa zarządzające danym terytorium powinny zapewnić dostęp do najbliższego węzła łączności, zapewniającego warunki dowiązania do systemów łączności ale to rozwijające się siły są odpowiedzialne za doprowadzenie łącza do węzła łączności, (jeżeli w danym państwie nie obowiązują inne zasady).

Przykładem może być sieć łączności w operacji reagowania kryzysowego z udziałem Polskiego Kontyngentu Wojskowego na Bałkanach, gdzie dla potrzeb sprawnego działania batalionu uruchomione zostały:

- stacjonarna sieć telekomunikacyjna,
- mobilne sieci radioliniowe: horyzontowe, troposferyczne i satelitarne,
- sieci radiowe KF,
- sieci radiowe UKF,
- lokalne sieci telefoniczne i informatyczne na stanowiskach dowodzenia.

Przykład sieci radiowej (mieszanej KF/UKF) polskiego batalionu przedstawia rys.1.3.1.1.



Rys.1.3.1.1. Organizacja sieci radiowej w operacji reagowania kryzysowego (przykład)

Uzasadnione jest zatem stwierdzenie, że celowym jest maksymalne wykorzystywanie na potrzeby łączności jednostek wojskowych wykonujących zadania w ramach operacji reagowania kryzysowego stacjonarnego komponentu systemu łączności a w dalszej kolejności

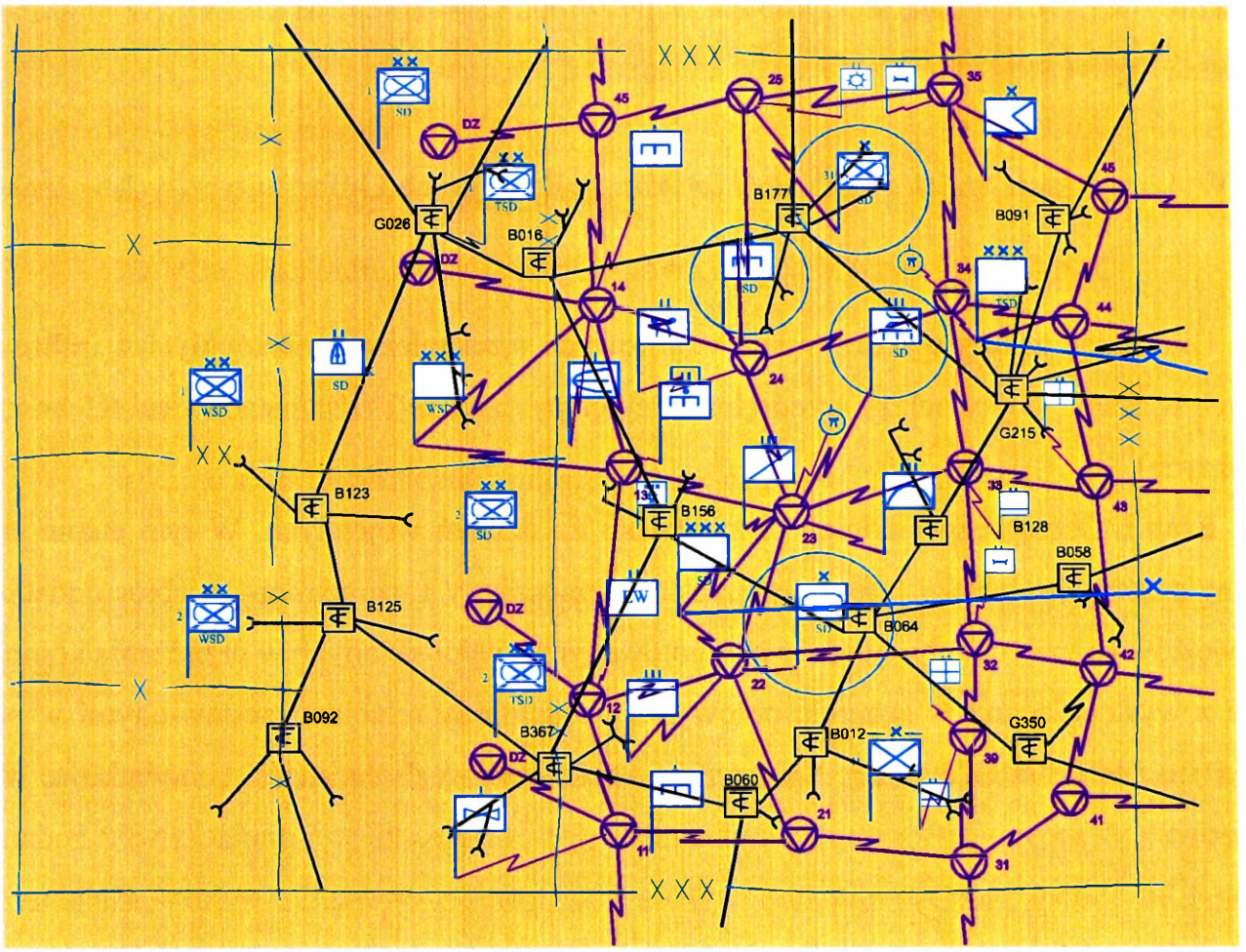
stworzenie indywidualnego, adekwatnego do potrzeb i wymagań systemu dowodzenia, podsystemu łączności polowej.

1.3.2. Wykorzystanie wojskowych sieci telekomunikacyjnych i informatycznych w czasie wojny

Określając zakres wykorzystania wojskowych sieci telekomunikacyjnych i informatycznych w czasie wojny należy wyodrębnić trzy etapy działań (i eksploatacji sieci telekomunikacyjnych):

Etap I. Okres bezpośrednich przygotowań do działań wojennych. W tym etapie stacjonarny system łączności i informatyki został wzmocniony i uzupełniony o zbiór dodatkowych węzłów bazowych odpowiednio przygotowanych i wyposażonych w urządzenia kompatybilne z występującymi w sprzęcie polowymi, uzupełniony relacjami zestawionymi w publicznej sieci telekomunikacyjnej, łączącymi garnizonowe węzły łączności (i dodatkowe węzły bazowe) w sposób zwiększający żywotność sieci. Jednostki wykonując swoje zadania (szkolenie, mobilizacyjne rozwinięcie) wykorzystują przede wszystkim system stacjonarny (w szczególności jego część radioliniowo-kablową) mając zorganizowane i pracujące na odbiór sieci radiowe (część). W tym też okresie może zachodzić konieczność zapewnienia łączności w stacjonarnym systemie łączności dla potrzeb jednostek wojskowych państw sprzymierzonych (w ramach HNS) wchodzących na teren Polski oraz zapewnienie z nimi łączności współdziałania w mobilnych systemach łączności.

Etap II. Okres działań wojennych, w czasie których możliwe jest wykorzystanie stacjonarnego systemu łączności. W tym etapie funkcjonuje w pełni rozwinięty polowy system łączności i informatyki i jednocześnie w maksymalnym stopniu wykorzystywany jest system stacjonarny (przykład rys.1.3.2.1..). Zapewnia to możliwość zachowania odwodów, zwiększenia żywotności systemu, jego mobilności i uzupełniania strat.



Rys.1.3.2.1. Organizacja sieci radioliniowo-kablowej korpusu w operacji obronnej z wykorzystaniem elementów bazowej sieci łączności (przykład)

Organizacja łączności w systemie polowym jest zgodna z wymogami wojennego systemu dowodzenia, struktury poszczególnych sieci radiowych, radioliniowo-kablowych i informatycznych odpowiadają wymaganiom stawianym przez system dowodzenia[22].

Etap III. Okres działań wojennych, w czasie którego nie funkcjonuje stacjonarny system łączności a dowodzenie działaniami odbywa się z przekazywaniem informacji wyłącznie w polowych systemach łączności. W tym okresie najprawdopodobniej wszystkie dostępne środki będą wykorzystane w systemie łączności. Oddziaływanie przeciwnika (mając na uwadze prawdopodobnego przeciwnika a więc posiadającego armię na co najmniej średnim europejskim poziomie) spowoduje częściowe straty fragmentaryczne rozpoznanie i lokalne obezwładnienia systemu, co wpłynie na zwiększone zużycie sił i środków łączności i prawdopodobną częściową utratę zdolności systemu do realizacji zadań. Okres ten charakteryzował się

[22] Analiza możliwości realizacji sieci telekomunikacyjnych i informatycznych oraz ich przykłady zostały przedstawione w: Z. Fiołna i zespół: Podstawowe relacje dowodzenia oddziału, związku taktycznego i związku operacyjnego w działaniach wojsk lądowych, część II - album schematów, AON Warszawa 2001 oraz J. Janczak i inni: Mobilne sieci łączności, AON Warszawa 2003

prawdopodobnie będzie znacznym pogorszeniem się możliwości działania systemów łączności (szczególnie telekomunikacyjnych) obu walczących stron, co z jednej strony pogorszy sprawność systemu dowodzenia a z drugiej (w konsekwencji) zmniejszy potencjalne możliwości oddziaływania przeciwnika na system łączności, a więc prawdopodobnie (autorzy nie mają możliwości przeprowadzenia badań w tym zakresie) może nastąpić stabilizacja parametrów systemu (procent zniszczenia, sprawności, możliwości świadczenia usług, tempo odtwarzania zdolności do działania) na pewnym, być może niskim poziomie, umożliwiając działanie systemu dowodzenia na poziomie wystarczającym do wykonywania dalszych zadań.

2. BEZPIECZEŃSTWO I OCHRONA INFORMACJI – PODSTAWOWA TERMINOLOGIA

płk dr hab. inż. Józef MICHNIAK

Zaczynając rozważania na temat bezpieczeństwa informacji w sieciach łączności i informatyki wojskowej należy zaznaczyć, iż wszystkie pojęcia występujące w temacie pracy, tzn. bezpieczeństwo, informacja oraz sieci łączności i informatyki mogą budzić wiele skojarzeń, powodując tym samym różnorakie interpretacje powyższego zagadnienia. Dlatego też zespół autorski przedstawia na bazie różnych źródeł definicje wymienionych pojęć, by wydobyć te z nich, które posłużą do zdefiniowania podstawowego zakresu tematyki, w obrębie której będziemy się poruszać w niniejszej pracy.

2.1. Bezpieczeństwo

Pierwszym z wymienionych pojęć jest „bezpieczeństwo". Pojęcie bezpieczeństwa (ang. Security) jest bardzo szerokim pojęciem, zawierającym w sobie wszystkie aspekty i pojęcia z zakresu ochrony informacji, takie jak podatności, zagrożenia, ryzyka, aspekty zarządzania i zabezpieczenia. Zgodnie ze Słownikiem Języka Polskiego[23] jest to „stan nie zagrożenia, spokoju, pewności". Z jednej strony jest to definicja bardzo prosta i zwięzła, ale jednocześnie jej zakres jest bardzo szeroki. O wiele bardziej interesującą pod kątem naszych rozważań będzie definicja zawarta w Myśli Wojskowej[24] mówiąca, że bezpieczeństwo to ***„stan, który daje poczucie pewności i gwarancję jego zachowania oraz szansę na doskonalenie. Jedna z podstawowych potrzeb człowieka. Sytuacja odznaczająca się brakiem ryzyka utraty czegoś, co człowiek szczególnie ceni, na przykład zdrowia, pracy, szacunku, uczuć, dóbr materialnych"***.

W odniesieniu do systemów teleinformatycznych bezpieczeństwo określane jest jako ***definiowanie, osiąganie i utrzymywanie*** sześciu podstawowych cech, (poufność, integralność,

---

[23] „Słownik Języka Polskiego"- PWN, Warszawa 1978;
[2] „Myśl Wojskowa"- Bellona, Warszawa Listopad-Grudzień 2002, 6(623);

dostępność, rozliczalność, autentyczność, niezawodność), którymi powinien charakteryzować się bezpieczny system teleinformatyczny[25].

Bezpieczeństwo informacji[26] to miara stopnia skuteczności zastosowanych środków i metod ochrony w stosunku do istniejących i prognozowanych zagrożeń bezpieczeństwa informacji, które polega na jej zabezpieczeniu przed przypadkowym bądź umyślnym zniszczeniem, kradzieżą, nielegalnym ujawnieniem lub nie sankcjonowaną modyfikacją, gdzie:

- środki i metody ochrony to przedsięwzięcia technologiczne i administracyjne, do zabezpieczenia komputerów, programów i danych, w celu zapewnienia ochrony interesów instytucji i poufności. Do środków ochrony informacji zaliczane są 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.

W związku z przedstawionymi powyżej definicjami, można przyjąć na potrzeby niniejszej pracy, że: BEZPIECZEŃSTWO INFORMACJI 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 i personalnych metod ochrony.

Bezpieczeństwo informatyki (ang. Computer Security) – COMPUSEC – to zasady bezpieczeństwa wymagane dla sprzętu i oprogramowania systemu komputerowego, w celu zapobieżenia lub zabezpieczenia przed nieautoryzowanym ujawnieniem, manipulacją, modyfikacją, usunięciem informacji lub odmową usługi[27].

---

[25] Raport techniczny Normalizacyjnej Komisji Problemowej nr 182 ds. Zabezpieczenia Systemów i Ochrony Danych – ISO/TRC 13335 – Grzegorz Podhorecki, Zarządzanie bezpieczeństwem systemów teleinformatycznych według Polskiej Normy PN-I-13335, IT Security Magazine, nr 1, 1999 r., s.7.
[26] Kryteria oceny bezpieczeństwa systemów łączności i informatyki, Praca zbiorowa, SWŁiI SG WP, Warszawa 1996 r., s. 15-19.
[27] Dyrektywa Bezpieczeństwa AD 70-1 PL, część V, § 13.

Bezpieczeństwo łączności (ang. Communication Security) – COMSEC – to zabezpieczenia wynikające 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[28]

2.2. Informacja

Kolejnym pojęciem występującym w temacie jest ***„informacja"***. Aby je przybliżyć powołam się ponownie na Słownik Języka Polskiego[29], który 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. Definicja encyklopedyczna[30] z kolei określa informację jako ***„obiekt abstrakcyjny, który w postaci zakodowanej (→ dane) może być przechowywany (na→ nośniku danych), przesyłany (np.: głosem, falą elektromagnetyczną, prądem elektrycznym), przetwarzany (w trakcie wykonywania → algorytmu) i użyty do sterowania (np.: komputerem steruje program będący zakodowaną informacją)"***. Tym razem mamy nie tylko określoną celowość informacji ale także próbę przedstawienia jej postaci, bo bez względu na to czy komunikujemy się głosem, listem tradycyjnym czy elektronicznym to zawarta w nich treść, a co za tym idzie i informacja, będzie ta sama, co więcej, jej znaczenie dla odbiorcy, użytkownika będzie takie samo.

---

[28] Tamże, część V, §14.
[29] „Słownik Języka Polskiego": op. cit.
[30] „Encyklopedia Powszechna"- PWN, Warszawa 1984;

Informacja wg Encyklopedii PWN – „Informacja [łac.], pojęcie (w zasadzie niedefiniowalne) występujące w teorii informacji[31]. Bardziej praktyczną definicję podaje prof. Piotr Sienkiewicz określając informację jako ***zbiór faktów, zdarzeń, cech obiektów itp. Zawarty w określonej wiadomości, tak ujęty i podany w takiej formie, że pozwala odbiorcy ustosunkować się do zaistniałej sytuacji i podjąć odpowiednie działania umysłowe lub fizyczne***[32].

Ze względu na różnorodność form i zastosowań informacji ostatnia z definicji wydaje się być najwłaściwszą do dalszych rozważań.

2.3. Wojskowe sieci telekomunikacyjne

Sieć telekomunikacyjna w ogóle to zespół aparatów przetwórczych, linii i stacji teletransmisyjnych, central :komutacyjnych, telefonicznych, telegraficznych, pakietowych, radiostacji oraz innych urządzeń telekomunikacyjnych znajdujących się na określonym obszarze, powiązanych ze sobą technicznie i przeznaczonych do świadczenia usług telekomunikacyjnych.

Wojskowa sieć telekomunikacyjna jest zbiorem złożonych i zespolonych ze sobą obiektów telekomunikacyjnych na stałe lub czasowo oddanych pod jurysdykcję wojskowych, rozmieszczonych przestrzennie i działających na dużym obszarze, przeznaczonym do zapewnienia wymiany informacji, tj. świadczenia usług telekomunikacyjnych dla potrzeb dowodzenia wojskami i sterowania środkami rażenia.

2.4. Wojskowe sieci komputerowe (informatyki)

Ostatnim pojęciem które postaram się przybliżyć będą ***„sieci komputerowe”***. Otóż zgodnie z Wielką Encyklopedią Sieci Komputerowych[33] pod tym pojęciem kryje się system komunikacyjny służący przesyłaniu danych, łączący dwa lub więcej komputerów i urządzeń peryferyjnych. Wynika z tego, że sieć jest jedynie fizycznym elementem spinającym komputery lub inne urządzenia, taka była bowiem idea tworzenia sieci komputerowych. W dobie wszechobecnych komputerów osobistych pojawiło się bowiem zapotrzebowanie na przesyłanie różnych informacji pomiędzy komputerami, a z czasem także i innymi urządzeniami podłączonymi do sieci. Kolejnym etapem rozwoju sieci było zróżnicowanie usług świadczonych

---

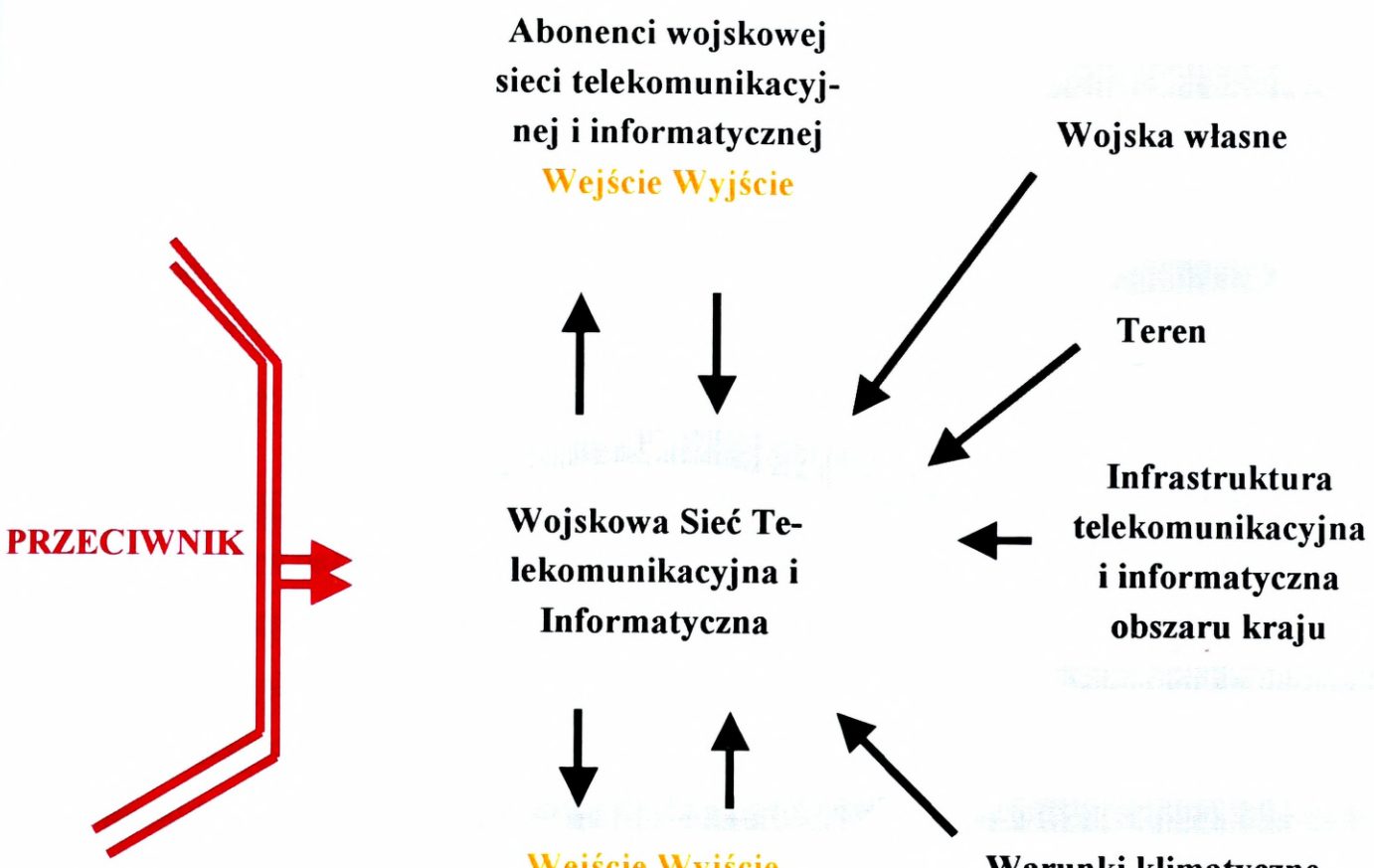
[31] TEORIA INFORMACJI, teoria przekazywania wiadomości ze źródła wiadomości do ich odbiorcy (ujścia); Multimedialna Encyklopedia PWN.
[32] Piotr Sienkiewicz *Inżynieria systemów*, MON, Warszawa 1993, s.61
[33] „Wielka Encyklopedia Sieci Komputerowych”- Wydawnictwo Robomatic, Wrocław 1995;

przez różne urządzenia, począwszy od tych podstawowych czyli stron WWW, poczty elektronicznej, czatów, aż do połączeń głosowych a w ostatnich latach nawet rozproszonego przetwarzania danych. Za każdą z tych usług kryją się innego rodzaju oczekiwania ze strony użytkownika, a co za tym idzie rozwiązania funkcjonalne, czy to typowo sprzętowe czy programowe. Tak więc pod pojęciem sieci komputerowej będziemy rozumieli system komunikacyjny łączący zarówno komputery jak i inne urządzenia sieciowe i świadczący określone rodzaje usług dla użytkownika. Należy jednak dodać, iż obiektem naszych zainteresowań nie będzie Internet tylko wydzielone sieci komputerowe mające określone przeznaczenie i nie będące ogólnodostępne,

2.5. Otoczenie wojskowej sieci telekomunikacyjnej i informatycznej

Jak już wcześniej określiliśmy, wojskowa sieć telekomunikacyjna jest zbiorem złożonych i zespolonych ze sobą obiektów telekomunikacyjnych, rozmieszczonych przestrzennie i działających na dużym obszarze, przeznaczonym do zapewnienia wymiany informacji, tj. świadczenia usług telekomunikacyjnych dla potrzeb dowodzenia i sterowania środkami rażenia.

Sieć telekomunikacyjna jest przygotowywana do działania i funkcjonowania w specyficznym otoczeniu, które jest zbiorem elementów do niego nie należących. Elementy te oddziaływają na sieć telekomunikacyjną, a jednocześnie ulegają zmianom pod wpływem jego działania. Specyficznymi i charakterystycznymi jedynie dla wojskowej sieci telekomunikacyjnej elementami otoczenia (środowiska w którym działa) są: przeciwnik, obszar działania, warunki klimatyczne, meteorologiczne oraz propagacyjne, a także własne systemy walki (zwane wojskami własnymi), w ramach których sieć telekomunikacyjna działa. Otoczenie wojskowego systemu łączności przedstawiono na rys.2.5.1.



Rys. 2.5.1. Otoczenie wojskowej sieci teleinformatycznej

3. ZAGROŻENIA BEZPIECZEŃSTWA WOJSKOWYCH SIECI TELEKOMUNIKACYJNYCH I INFORMATYCZNYCH

płk dr hab. inż. Józef MICHNIAK

3.1. Zagrożenia bezpieczeństwa łączności wojskowej

Przeciwnik jest tym elementem otoczenia wojskowych sieci telekomunikacyjnych, który w warunkach zagrożenia i wojny, a także w czasie pokoju może wywierać wpływ na ich poprawną pracę przez prowadzenie rozpoznania, oddziaływania ogniowego i elektronicznego. Niecelowo może wprowadzać zakłócenia swoimi pracującymi środkami łączności. Jeśli dojdzie do konfliktu to należy się spodziewać, że pierwsze uderzenia przeciwnika zostaną wykonane na wojska oraz na rozpoznane i obserwowane przez przeciwnika obiekty systemów dowodzenia tych wojsk - na ważne obiekty elektroniczne. Użyte mogą być elektroniczne środki prowadzenia wojny - broń precyzyjna i środki obezwładniania elektronicznego. Ich moc i precyzja oddziaływania jest tak wielka, że stanowią one duże zagrożenie dla systemów dowodzenia oraz łączności i informatyki.

Bez względu na rodzaj prowadzonych walk, agresywne działania bojowe wojsk przeciwnika będą realizowane w wymiarze powietrzno - lądowym. Należy więc mieć na uwadze powietrzno - lądowy charakter prowadzonych działań, co oznacza możliwość wykonywania przez przeciwnika równoczesnych uderzeń na różne obiekty i elementy ugrupowania bojowego (operacyjnego) wojsk dyslokowane na różnych głębokościach.

W trakcie walki działania przeciwnika mogą przyjąć różne formy, które mogą być realizowane w ramach :

- natarcia elektronicznego, będącego zmasowanym oddziaływaniem elektronicznym prowadzonym wszystkimi posiadanymi przez niego siłami i środkami walki elektronicznej, lub ich większością,
- operacji powietrznej z silnym wsparciem elektronicznym, wykonywanej w celu stworzenia warunków do prowadzenia skutecznych działań powietrzno - lądowych,

- operacji desantowo - morskiej z udziałem dużej liczby samolotów rozpoznawczych i uderzeniowych oraz z bardzo aktywnym działaniem sił i środków walki elektronicznej.

We wszystkich przedstawionych wyżej wariantach przeciwnik w szerokim zakresie będzie prowadził aktywne działania elektroniczne. Ich zakres, moc uderzeń i aktywność oddziaływania będą zależne od potencjału elektronicznego przeciwnika oraz możliwości - zwłaszcza wszechstronności jego użycia w różnych warunkach bojowych, meteorologicznych i terenowych.

3.1.1. Zagrożenia sieci telekomunikacyjnych

Przeciwnik zdolny jest prowadzić, aktywne ofensywne działania elektroniczne podczas pierwszego i w kolejnych uderzeniach swoich wojsk oraz w okresie je poprzedzającym. Mogą one być wykonane z powietrza, lądu jak i z morza. Należy liczyć się z użyciem wielu nowych rodzajów broni o dużej sile rażenia, precyzji działania i wysokiej celności oraz aktywnych środków prowadzenia rozpoznania i obezwładniania elektronicznego o nieznanych jeszcze parametrach technicznych i możliwościach bojowych. Nowoczesne środki umieszczane będą nie tylko w naziemnych środkach transportowych wojsk lądowych - lecz przede wszystkim na samolotach, śmigłowcach i okrętach.

Doświadczenia wojenne i symulacje komputerowe prowadzone w czasie ćwiczeń wykazują, że rażenie ogniowe oraz uderzenia wojsk przeciwnika będą wykonywane pod osłoną intensywnych zakłóceń elektronicznych. W zależności od stopnia rozpoznania systemu dowodzenia, uderzenia mogą rozpocząć się w skali masowej, lub ze zwiększonym nasileniem, z kilkunastu lub kilkuminutowym wyprzedzeniem przed uderzeniem wojsk. Siły i środki walki elektronicznej umożliwiają wykonanie różnego rodzaju zadań, szeroko rozumianego rozpoznania i obezwładniania. Zmasowane, aktywne działania elektroniczne przeciwnika prowadzone będą przeciwko rozpoznanym środkom, systemowi dowodzenia, a zwłaszcza przeciwko pracującym na jego potrzeby systemowi łączności i informatyki. Można przyjąć, że prognozowany średni czas rozpoznania przez przeciwnika elementów sieci telekomunikacyjnej w strefie taktycznej wyniesie podczas natarcia od 1,2 do 3 godzin dla linii radioliniowych, oraz do 3 godzin podczas obrony. Średni czas rozpoznania linii radiowych w czasie natarcia wyniesie od 2 do 2,5 godzin dla linii KF i od 1 do 1,5 godziny dla linii UKF. W czasie obrony średni czas rozpoznania może wynosić od 0,5 do 1 godziny dla linii KF i od 0,3 do 0,5 dla linii UKF. Szacuje się, że przeciwnik dysponujący nowoczesnym potencjałem sił i środków

do prowadzenia walki elektronicznej może obezwładnić około 60÷80% ważniejszych relacji łączności radiowej krótkofalowej, około 50÷60% ważniejszych relacji łączności radiowej ultrakrótkofalowej i radioliniowej, w wyniku czego może wystąpić łączne zmniejszenie możliwości przesyłanych wiadomości średnio o 40÷50%. Odtwarzanie łączności na zasadniczych kierunkach może trwać od 4 do 8 godzin.

Przeciwnik może stosować również w szerokim zakresie dywersję radiową. Dywersja radiowa jest celowym działaniem przeciwnika na zorganizowane systemy radioelektroniczne łączności bezprzewodowej oraz systemy radionawigacyjne, zmierzającym do dezorganizowania dowodzenia wojskami i sterowania środkami rażenia. Wpływa to na obniżenie wartości bojowych naszych wojsk. Stanowi szczególną formę celowego i aktywnego oddziaływania na systemy dowodzenia wojskami i kierowania środkami walki. Polega 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.

We współczesnej walce znaczenie prowadzenia dywersji radiowej wzrośnie głównie ze względu na rozmach prowadzonych działań, w których dowodzenie wojskami i sterowanie środkami rażenia realizowane będzie na dużych przestrzeniach przede wszystkim za pomocą środków radiowych takich jak: radiostacje, radiolinie, radiotelefony, satelity. Wysoka dynamika i manewrowość działań taktycznych i operacyjnych stwarzać będzie często trudne sytuacje, w których dowództwa nie będą miały ciągłej łączności lub jej utrzymanie będzie utrudnione. Ponadto duże możliwości rażenia i niszczenia przez lotnictwo, wojska rakietowe i artylerię, desanty i grupy dywersyjno-rozpoznawcze środków i obiektów elektronicznych będą przyczyną częstego „wypadania" korespondentów z poszczególnych relacji łączności bez wiedzy dowództw oraz węzłów łączności głównych stanowisk dowodzenia. Stworzy to bardzo korzystne warunki do prowadzenia dywersji radiowej - przez podszywanie się pod nie istniejące już środki łączności. Zakłócenia elektroniczne oraz dywersja radiowa będą pogłębiać i zwiększać chaos, utrudniając odtworzenie dowodzenia i gotowości bojowej wojsk, a także mogą stworzyć mylny obraz, tego co pozostało po uderzeniach.

Przekazywanie informacji nieprawdziwych może być przyczyną nieporozumień, niepewności, nieskoordynowanych działań i w konsekwencji przyniesie większe efekty niż zakłócenia. We współczesnej walce czy operacji dywersja radiowa będzie więc spełniała szczególnie ważną rolę i zadania. Traktować ją należy jako aktywną formę oddziaływania elektronicznego przeciwnika na relacje łączności systemów radiowych różnych szczebli dowodzenia

i rodzajów wojsk. Stanowi element składowy obezwładniania elektronicznego - jednej z zasadniczych form walki elektronicznej.

Prowadzenie dywersji radiowej przez przeciwnika może wynikać również z innych przyczyn. Bardzo często w walce mimo stosowania różnorakich środków, niekiedy z przyczyn obiektywnych, przeciwnik nie będzie mógł zdezorganizować zakłóceniami pracy w niektórych relacjach łączności. Często mimo stosowania manewru i przybliżania środków zakłócających nie będzie możliwe uzyskanie odpowiedniego stosunku sygnału zakłócającego do użytecznego naszych radiostacji. W takich warunkach przeciwnik będzie stosował inne sposoby oddziaływania elektronicznego, między innymi dywersję radiową, skoordynowaną z uderzeniami ogniowymi oraz z działaniem głównych zgrupowań uderzeniowych.

Radiowe działania dywersyjne traktować należy na równi z zakłóceniami elektronicznym. W swej istocie mają one bowiem charakter zakłóceń dywersyjnych. Tak samo jak klasyczne zakłócenia elektroniczne prowadzą w końcowym efekcie do dezorganizacji systemu dowodzenia wojskami. Do zasadniczych zadań dywersji radiowej stosowanej przez przeciwnika zalicza się:

- przekazywanie dowódcom i sztabom, załogom samolotów, okrętów i wojskom informacji (mylnych meldunków, rozkazów, komunikatów itp.) oraz przedstawianie mylnego obrazu tego, co istnieje na polu walki lub tego, co już nie istnieje albo dopiero nastąpi,
- zajmowanie czasu w kanałach łączności i radionawigacyjnych, tzn. blokowanie kanałów fałszywą lub całkowicie zbędną informacją,
- utrzymywanie dowództw w niepewności co do wiarygodności informacji oraz zmuszanie ich do stałego upewniania się co do prawdziwości przekazywanych danych, stałego potwierdzania otrzymanych informacji w kilku kanałach łączności oraz ciągłego sprawdzania tożsamości korespondenta itp., co łączy się ze stratą czasu i blokowaniem kanałów łączności i radionawigacyjnych,
- wprowadzenie chaosu i zamieszania w skoordynowane dowodzenie wojskami i kierowanie środkami rażenia poprzez przekazywanie fałszywych informacji lub też częste powtarzanie prawdziwych, wcześniej przekazywanych informacji.

3.1.2. Zagrożenia sieci komputerowych (informatycznych)

Zjawiskiem naturalnym jest fakt, iż w miarę rozwoju sieci komputerowych zwiększa się liczba zagrożeń. W zależności od przyjętego kryterium można dokonać różnorodnych ich podziałów.

Zgodnie z „Bezpieczeństwem danych w systemach informatycznych" zagrożenia możemy podzielić na dwie grupy. „Po pierwsze zagrożenia wynikające z celowego działania nieuprawnionego użytkownika. Po drugie, takie, które nie są skutkiem celowego działania"[34].

Z kolei autorzy Molski i Opala[35], proponują kilka innych podziałów, otóż dzielą oni zagrożenia na bierne i aktywne (czynne), wewnętrzne i zewnętrzne, sprzętowe i programowe oraz przypadkowe i celowe. Należy zauważyć, że podział zagrożeń na celowe i przypadkowe występuje w obu źródłach i wydaje się być najlepszy, gdyż powstaje samoistnie w momencie określenia ważniejszego z atrybutów dla danej sieci. Jeżeli mianowicie zależy nam przede wszystkim na poufności, to zabezpieczymy się przed zagrożeniami celowymi, jeżeli natomiast istotne są integralność i dostępność, to skupimy się na zagrożeniach przypadkowych.

Przyjąwszy za kryterium źródło zagrożeń możemy dokonać następującego podziału:

- zagrożenia ze strony użytkowników,
- ataki na systemy informatyczne,
- programy złośliwe,
- awarie sprzętu,
- emisja ujawniająca.

Każde z wymienionych zagrożeń może naruszyć co najmniej jeden aspekt bezpieczeństwa informacji w sieciach komputerowych.

Użytkownicy

Okazuje się, iż to właśnie człowiek stanowi najczęstszą przyczynę zagrożeń bezpieczeństwa sieci teleinformatycznych. To ludzie włamują się do sieci, wprowadzają programy złośliwe i zaniedbują swoje obowiązki, co w konsekwencji może przyczynić się do zmniejszenia bezpieczeństwa. Działalność ludzką możemy podzielić na dwie grupy: zewnętrzną i wewnętrzną. Działalność zewnętrzna ma miejsce kiedy osoby z zewnątrz dążą do wykradnięcia, modyfikacji bądź zniszczenia informacji lub zasobów sieci teleinformatycznej. Wewnętrznymi natomiast są wszystkie czynności osób związanych z samą siecią, takich jak ad-

---

[34] „Bezpieczeństwem danych w systemach informatycznych"- op. cit.
[35] „Elementarz bezpieczeństwa systemów informatycznych" – M. Molski, S. Opala, Mikom, Warszawa, 2002;

ministratorzy, użytkownicy, dostawcy czy klienci, powodujące obniżenie poziomu bezpieczeństwa.

Zgodnie z „Bezpieczeństwem danych w systemach informatycznych”[36] do zagrożeń wewnętrznych zaliczamy:

- akty wewnętrznego sabotażu,
- kradzież informacji,
- kradzież usług,
- błędy użytkowników,
- niedbalstwo,
- nieprawidłowe stosowanie mechanizmów bezpieczeństwa.

Akty wewnętrznego sabotażu polegają na celowym zmniejszaniu bezpieczeństwa sieci przez personel. Polegać mogą np.: na celowym wprowadzeniu programu złośliwego, czy doprowadzeniu do niesprawności urządzeń bądź procesów funkcjonujących w sieci.

Kradzież informacji ma miejsce w przypadku celowego udostępnienia osobom niepowołanym znajdujących się w sieci informacji, albo informacji o samej sieci.

Kradzież usług jest obecnie zjawiskiem nagminnym i polega na wykorzystywaniu przez pracowników istniejącej sieci do celów nie związanych z jej faktycznym przeznaczeniem. Może to być np.: odwiedzanie stron WWW niezwiązanych z wykonywanym zajęciem, czy instalowanie dodatkowego oprogramowania czy np. gier. Wszystkie te działania obniżają wydajność sieci, obciążają niepotrzebnie urządzenia sieciowe i zajmują pasmo w łączach.

Błędy użytkowników polegają na nieprawidłowym użytkowaniu sieci, programów, błędnym wprowadzaniu informacji, przypadkowych zmianach w konfiguracji oprogramowania.

Niedbalstwo jest bardzo poważnym problemem, ponieważ w sposób bezpośredni może prowadzić do powstania luki w całym systemie bezpieczeństwa sieci. Pod pojęciem tym kryją się między innymi brak zabezpieczeń antywirusowych, ich nieaktualność, bądź opóźnienia w wykonywaniu zmian w uprawnieniach użytkowników (np. przy odejściu pracownika z firmy). Poważnym zaniedbaniem jest też nierzetelne wykonywanie kopii bezpieczeństwa, umożliwiających odtworzenie informacji w przypadku ich utraty.

Pod pojęciem ***nieprawidłowego stosowania mechanizmów bezpieczeństwa*** kryją się między innymi wszystkie nieprawidłowości związane z korzystaniem z haseł dostępowych,

---

[36] „Bezpieczeństwem danych w systemach informatycznych”- op. cit.

udostępnianie ich osobom trzecim, zapisywanie w miejscach ogólnodostępnych, tworzenie haseł prostych do złamania (imiona, daty urodzin, itp.).

Ataki na systemy informatyczne

Według Lidermana[37] wyróżnić możemy następujące rodzaje ataków na systemy komputerowe:

- lokalne- kiedy intruz posiada fizyczny dostęp do atakowanego komputera;
- wewnętrzne- kiedy ataki przeprowadzane są z innego komputera tej samej sieci;
- zewnętrzne (zdalne)- kiedy ataki przeprowadzane są z sieci zewnętrznej.

Charakterystyczna cechą wszystkich ataków jest to, że intruz uzyskał dostęp do sieci, wszedł w posiadanie haseł dostępowych, bądź ominął zabezpieczenia i dostał się do systemu.

Najniebezpieczniejszym jest atak lokalny, ponieważ posiadając dostęp do komputera, intruz ma dostęp do całej jego zawartości, wszystkich zgromadzonych w nim informacji. Dokonanie takiego ataku poprzedzone jest odpowiednimi przygotowaniami. Napastnik zazwyczaj zbiera informacje na temat potencjalnego celu przy użyciu rozmaitych metod - od wypytywania użytkowników, aż po analizę ruchu i krążących w sieci pakietów. W taki sposób intruz może zdobyć informacje mówiące o wykorzystywanym systemie operacyjnym, zabezpieczeniach antywirusowych, rozmieszczeniu poszczególnych elementów sieci, lokalizacji ważniejszych urządzeń, sposobie monitorowania zdarzeń w sieci. Posiadając takie dane może on przygotować się dokładnie do obejścia odpowiednich zabezpieczeń i osiągnięcia zamierzonego celu.

Innym bardzo niebezpiecznym rodzajem ataku na sieć jest atak przy wykorzystaniu koni trojańskich, które zostaną scharakteryzowane poniżej.

Programy złośliwe

Programy złośliwe są to programy których celem jest przeprowadzenie nieuprawnionych i szkodliwych działań w zainfekowanym środowisku. Zgodnie z systematyką podaną przez „Bezpieczeństwo danych ..." dzielimy je na:

- wirusy komputerowe,
- bakterie,
- robaki,

---

[37] „Bezpieczeństwo teleinformatyczne"- op. cit.

- bomby logiczne,
- konie trojańskie.

Wirusy komputerowe są najczęściej spotykanymi programami złośliwymi. Pod pojęciem tym kryją się programy posiadające zdolność do rozmnażania się, dopisywania i modyfikowania plików wykonywalnych bądź ukrywania się w sektorach systemowych dysków twardych. W przypadku wirusów umieszczonych w plikach, uruchamiają one się w momencie uruchomienia pliku i infekują inne działające pliki. Natomiast wirusy znajdujące się w sektorach systemowych, uaktywniają się w momencie uruchamiania systemu, infekując przy tym wszystkie dostępne dyski logiczne. Wirusy mogą wywoływać zakłócenia w pracy systemu operacyjnego.

W przeciwieństwie do wirusów ***bakterie*** nie infekują innych plików ani sektorów systemowych, tylko są samodzielnymi programami, które posiadają umiejętność bardzo szybkiego rozmnażania się. Efektem ich działania jest zużywanie zasobów komputera (pamięć operacyjna, dyski logiczne, moc procesora).

Kolejnym rodzajem programów złośliwych są ***robaki***. W sposobie działania są zbliżone do bakterii, jednak obiektem ich zainteresowań nie są pojedyncze stacje robocze, ale sieci komputerowe. Infekują serwery, zmniejszają ich wydajność, aż do zablokowania.

Bomby logiczne są ukrytym i nieudokumentowanym fragmentem programu, który przy spełnieniu określonego warunku uruchamia szkodliwe dla systemu akcje. Warunkiem aktywacji mogą być takie parametry jak czas, data, zapisana objętość twardego dysku, ilość uruchomień programu nosiciela, itp.

Ostatnim z rodzajów programów złośliwych są ***konie trojańskie***. Są to programy, także te wykonujące pożyteczne zadania, we wnętrzu których ukryte są nieudokumentowane procedury, zadaniem których jest stworzyć nieuprawnionemu użytkownikowi możliwość dostania się do systemu operacyjnego i wykonywanie określonych czynności.

Coraz częściej możemy spotkać programy złośliwe łączące cechy kilku z wyżej wymienionych rodzajów.

Awarie sprzętu

W miarę rozwoju technologicznego urządzeń aktywnych sieci komputerowych (komputerów, ruterów, przełączników, itp.) zmniejsza się ich awaryjność, jednocześnie zwiększa się trwałość wykorzystywanych nośników informacji. Przy zachowaniu odpowiednich warunków możliwe jest zmniejszanie ilości awarii, jednak tylko w ramach okresu użyteczności

urządzenia. Niemożliwe jest jednak stworzenie urządzenia wolnego od awarii. Przyczyny niesprawności sprzętu możemy podzielić na[38]:

- błędy projektowe,
- wady produkcyjne,
- błędy instalacyjne,
- awarie.

Błędy projektowe powstają na etapie tworzenia projektu urządzenia i mogą być związane zarówno z wadami konstrukcyjnymi jak i jakościowymi, wynikającymi na przykład z użycia niewłaściwego materiału. Błędami tymi obarczone są wszystkie urządzenia zbudowane w oparciu o ten projekt.

Wady produkcyjne powstają na etapie fizycznego wykonywania urządzeń. Przykładowo mogą one wynikać z wykorzystania partii wadliwych podzespołów, wówczas wada ta występuje we wszystkich egzemplarzach w których wykorzystany został element z niej pochodzący.

Obie scharakteryzowane powyżej grupy tj. błędy projektowe i wady produkcyjne związane są z winą producenta, natomiast kolejne dwie czyli ***błędy instalacyjne i awarie*** są efektem niewłaściwego działania czy to instalatora, czy użytkownika. O ile producenci starają się zapobiegać powstawaniu wad produkcyjnych i projektowych, o tyle błędy będące wina użytkowników i instalatorów są trudne do wyeliminowania. Wynika to z faktu, iż ich wiedza i umiejętności oparte są na zdobytym doświadczeniu, które często okazuje się niewystarczające by zapobiec awariom.

Po pierwsze, instalator/użytkownik może popełnić *błędy instalacyjne*, przez które rozumieć należy efekty niewłaściwego zainstalowania, stosowania niewłaściwych materiałów instalacyjnych, nieprawidłowe obchodzenie się ze sprzętem podczas jego montażu i uruchamiania. Przykładem takiego niewłaściwego instalowania sprzętu może być źle wykonana instalacja elektryczna, co może doprowadzić w niej do przepięcia i w efekcie końcowym do spalenia zasilacza urządzenia.

Po drugie, na każdym etapie użytkowania mogą wystąpić *awarie*, które są najczęstszym problemem ze sprzętem. Wynika to z faktu, iż na funkcjonowanie sprzętu składa się najwięcej czynników. Użytkownik musi zatroszczyć się o stworzenie urządzeniom właściwych warunków do pracy, a pod tym pojęciem kryje się wiele zagadnień. Urządzenia wymagają odpowiedniej temperatury i wilgotności. Ponadto należy umieścić je w miejscu, gdzie

---

[38] „Bezpieczeństwem danych w systemach informatycznych"- op. cit.

nie będą narażone na oddziaływanie silnych pól elektromagnetycznych, które mogłyby negatywnie wpłynąć na poprawność ich pracy. Należy zapewnić im właściwe (stabilne) i bezpieczne zasilanie. Nawet wyposażenie pomieszczenia może okazać się punktem newralgicznym, który spowoduje uszkodzenie sprzętu, chodzi tu na przykład o wykładziny i inne materiały powodujące powstawanie ładunków elektrostatycznych.

Znaczący wpływ na awaryjność urządzeń ma również sposób ich eksploatacji, kultura pracy użytkownika. Sprzęt sieciowy należy podzielić na dwie grupy jeżeli chodzi o sposób pracy, mianowicie sprzęt pracujący średnio przez kilka godzin dziennie, taki jak stacje robocze czy drukarki, i na sprzęt pracujący w trybie ciągłym, serwery, rutery. W przypadku tej drugiej grupy istotne jest na przykład unikanie nadmiernego eksploatowania elementów niewykorzystywanych bezpośrednio do obsługi sieci, takich jak na przykład monitory.

W ramach awarii sprzętu należy też wspomnieć o nośnikach informacji wykorzystywanych w sieciach komputerowych. Należy wyszczególnić dwa rodzaje nośników: po pierwsze nośniki stałe sieci, takie jak dyski twarde komputerów czy macierze dyskowe, po drugie nośniki przenośne, czyli dyskietki, płyty CD, tasiemki do streamerów, itp. Podstawowymi parametrami, które są uwzględniane przy wyborze nośników, jest ich pojemność, czas dostępu i szybkość transmisji. Rzadko kiedy brany jest pod uwagę taki parametr jak trwałość nośnika i jego niezawodność. W przypadku pamięci stałych istotny jest nie tyle rodzaj nośnika, co organizacja pamięci masowej, która ma umożliwić w sytuacji krytycznej (uszkodzenie jednego z dysków) odtworzenie informacji na nich zapisanych, o czym będzie mowa w dalszej części pracy. Zagadnienie trwałości jest jednak bardzo istotne w przypadku nośników zewnętrznych. Narażone są one na różne czynniki zewnętrzne (światło, temperaturę, pola elektromagnetyczne, itp.) zmniejszające ich żywotność. Decydując się na konkretny rodzaj nośnika uwzględnić należy także takie uwarunkowania jak częstość korzystania z nośnika, częstość wykonywania na nim zmian mających także bezpośredni wpływ na jego żywotność.

Emisja ujawniająca

Ostatnim zagrożeniem które omówimy będzie emisja ujawniająca (promieniowanie ujawniające). Możemy podzielić ją na dwa rodzaje[39]:

- propagowaną,
- przewodzoną.

---

[39] „Elementarz bezpieczeństwa systemów informatycznych"- op. cit.

Emisja propagowana polega na indukowaniu pola elektromagnetycznego w przestrzeni otaczającej urządzenie. Źródłem tej emisji może być każdy element aktywny urządzenia, czyli element, w którym pojawiają się sygnały elektryczne. Może to być zarówno płyta główna, monitor, jak też klawiatura. W przypadku jednostek centralnych głównym źródłem ulotu informacji staje się magistrala i wszelkie interfejsy na których pojawiają się sygnały. Jednak największym zagrożeniem informacji są właśnie monitory i inne urządzenia peryferyjne, ponieważ sygnały sterujące przesyłane są wiązkami kabli miedzianych, które działają nie tylko jako przewodnik, ale także jako antena i emitują ten sam sygnał w „eter". Wystarczy odbiornik o podwyższonej czułości i odpowiednio skonfigurowany układ zawierający procesor sygnałowy aby odtworzyć informację znajdującą się takiej wiązce. Przykładem takiego urządzenia może być monitor van Ecka, który potrafi odtworzyć obraz wyświetlany na monitorze na podstawie sygnałów emitowanych przez jego kabel sygnałowy.

Drugim z rodzajów emisji jest emisja przewodzona. Polega ona na rozchodzeniu się sygnałów w instalacjach bezpośrednio podpiętych do urządzenia, takich jak zasilanie czy uziemienie. W taki sposób informacja może zostać wyemitowana poza strefę chronioną, gdzie przy pomocy odpowiednich urządzeń jest możliwe odtworzenie niektórych informacji znajdujących się w sieci.

W praktyce występuje również emisja będąca połączeniem dwóch wymienionych powyżej emisji – tzw. emisja mieszana. Polega ona na wyemitowaniu przez urządzenie sygnału w postaci pola elektromagnetycznego a następnie zaindukowaniu takiego sygnału w innym elemencie przewodzącym ładunki elektryczne. Doskonałym przykładem takiego zjawiska będzie np.: telefon lub instalacja CO zlokalizowane w niewielkiej odległości od urządzenia emitującego pole elektromagnetyczne. Metalowe elementy takich instalacji będą działać jak antena i pod wpływem pola zaindukuje się w nich sygnał, który może posłużyć do przechwycenia informacji emitowanych przez urządzenie sieciowe.

4. WYMAGANIA STAWIANE BEZPIECZNYM SIECIOM KOMPUTEROWYM

płk dr hab. inż. Józef MICHNIAK

W miarę ewolucji sieci komputerowych i świadczonych przez nie usług, zmieniają się wymagania, które się przed nimi stawia. W wielu przypadkach połączenie między sobą kilku komputerów przestaje być wystarczające, wymagany jest szereg zabezpieczeń i przedsięwzięć mających na celu sprostanie oczekiwaniom użytkowników co do bezpieczeństwa danej sieci.

Jednolite zasady tworzenia bezpiecznej sieci komputerowej są trudne do określenia. Ze względu na przeznaczenie sieci wymogi z tym związane mogą się zmieniać, a kiedy dodamy do tego jeszcze uwarunkowania środowiska, w którym ma ona być wykorzystywana, to okazuje się, że każdą sieć należy rozpatrywać indywidualnie.

Niemniej jednak możemy wyróżnić trzy podstawowe wymogi bezpieczeństwa informacji, określane jako aspekty bądź atrybuty informacji związane z jej bezpieczeństwem. Są to:

- poufność (*ang. confidentiality*),
- integralność (*ang. integrity*),
- dostępność (*ang. availability*).

Poufność określana także jako *tajność* oznacza niedostępność informacji dla osób nieuprawnionych. W zależności od wagi informacji można nadawać im określone klauzule (poufne, tajne, ściśle tajne) i przyporządkowywać im mniej lub bardziej restrykcyjne procedury dostępu.

Integralność jest atrybutem oznaczającym zachowanie przez informację stanu zgodnego z pierwotnym, czyli niezmienianie bądź nie wykasowanie w wyniku nieautoryzowanego dostępu. Jednak brak integralności nie koniecznie musi być związany z utratą przez informację poufności, może on wynikać z zaburzeń w pracy urządzeń pracujących w sieci, zakłóceń w transmisji, błędów w oprogramowaniu czy działania programów złośliwych. Integralność informacji można zapewniać wykorzystując kody wykrywające i korygujące błędy bądź też funkcje skrótu.

Dostępność związana jest z niczym nieograniczoną możliwością korzystania z informacji, aplikacji czy procesów na każde żądanie uprawnionego użytkownika.

Poza tymi trzema podstawowymi aspektami w niektórych wyspecjalizowanych sieciach istnieje konieczność ich rozszerzenia o kolejne atrybuty, ściśle zależne od przeznaczenia danej sieci. Jednym z takich atrybutów może być spójność danych, która w książce „Bezpieczeństwo danych w systemach informatycznych"[40] opisana jest jako „konieczność spełnienia przez każdy stan bazy danych zbioru warunków sformułowanych w definicji bazy danych. Warunki te, zwane *warunkami spójności*, dzielą się na warunki *statyczne* (określają zależności między danymi w każdym danym poszczególnym stanie bazy danych) i *dynamiczne* (definiują zależności między danymi z różnych stanów bazy danych , a więc tym samym określają reguły zmiany stanów). Zachodzenie spójności jest warunkiem koniecznym poprawności (niesprzeczalności) bazy danych. Innym z dodatkowych atrybutów może być wspomniana w „Bezpieczeństwie teleinformatycznym"[41] rozliczalność (ang. *accountability*) oznaczająca możliwość identyfikacji użytkowników i wykorzystywanych przez nich usług. Jednak znaczna większość wymagań stawianych sieciom komputerowym zawiera się we wspomnianych trzech atrybutach głównych.

4.1. Aspekty bezpieczeństwa informacji

W miarę rozwoju techniki pojawiają się coraz bardziej wyszukane sposoby zagrożenia bezpieczeństwa informacji w sieciach komputerowych. W związku z tym ciężko jest powiedzieć, że sieć jest bezpieczna. Zgodnie ze wspomnianym wcześniej już podziałem zagrożeń możemy wyróżnić trzy zasadnicze aspekty bezpieczeństwa, a mianowicie:

- bezpieczeństwo fizyczne;
- bezpieczeństwo elektromagnetyczne;
- bezpieczeństwo programowe (*ang. softwearowe*).

Niektóre źródła[42] podają jeszcze inne aspekty, takie jak bezpieczeństwo personelu czy zabezpieczenia organizacyjno-administracyjne, ale my skupimy się na wspomnianych trzech, przyjmując, że są one uniwersalnymi obszarami, które trzeba uwzględnić przy tworzeniu bezpiecznej sieci komputerowej. Natomiast wszystkie inne rodzaje zabezpieczeń można określić w ramach polityki bezpieczeństwa całej organizacji.

---

[40] „Bezpieczeństwo danych w systemach informatycznych" -J. Stokłosa, T. Bilski, T. Pankowski, PWN, Warszawa-Poznań, 2001;
[41] „Bezpieczeństwo teleinformatyczne"- K. Liderman, Warszawa, 2001;
[42] „Bezpieczeństwo teleinformatyczne"- op. cit.

4.1.1. Bezpieczeństwo fizyczne

Zgodnie z Dyrektywą Bezpieczeństwa AD 70-1 PL[43] głównym celem bezpieczeństwa fizycznego jest zabezpieczenie przed dostępem osób nieuprawnionych do informacji niejawnych. Według Krzysztofa Lidermana[44] w ramach bezpieczeństwa fizycznego wyszczególniamy następujące zagadnienia:

- organizacja i systemy kontroli dostępu,
- zabezpieczenia przeciw włamaniom (konstrukcje antywłamaniowe, urządzenia alarmowe),
- systemy i procedury zapewniające ciągłość pracy urządzeń składowych sieci,
- instalacje i utrzymywanie systemów zabezpieczeń przeciwpożarowych.

W ramach ostatniego punktu można jeszcze zawrzeć systemy wykrywające zagrożenia inne niżeli ogień, chociażby systemy wykrywające obecność wody w pomieszczeniu.

Dodatkowo Liderman porusza zagadnienie zapewnienia ciągłości i odpowiedniej jakości zasilania, co jest bardzo istotne, zważywszy na fakt, iż urządzenia są coraz precyzyjniejsze, a przez to bardziej wrażliwe na wszelkie anormalne zachowania sieci energetycznej. Do zagadnienia tego wrócimy jeszcze w dalszej części pracy.

Kontrola dostępu

Jak już wcześniej wspomnieliśmy, bezpieczeństwo fizyczne polega na zabezpieczeniu informacji przed dostępem osób nieuprawnionych. Pierwszym z aspektów tegoż bezpieczeństwa jest kontrola dostępu.

Pierwszym krokiem w tworzeniu kontroli dostępu powinno być określenie stref w których będzie się znajdować informacja niejawna. Tworzymy w ten sposób tzw. strefy bezpieczeństwa. Najczęściej określane są trzy rodzaje stref, są to:

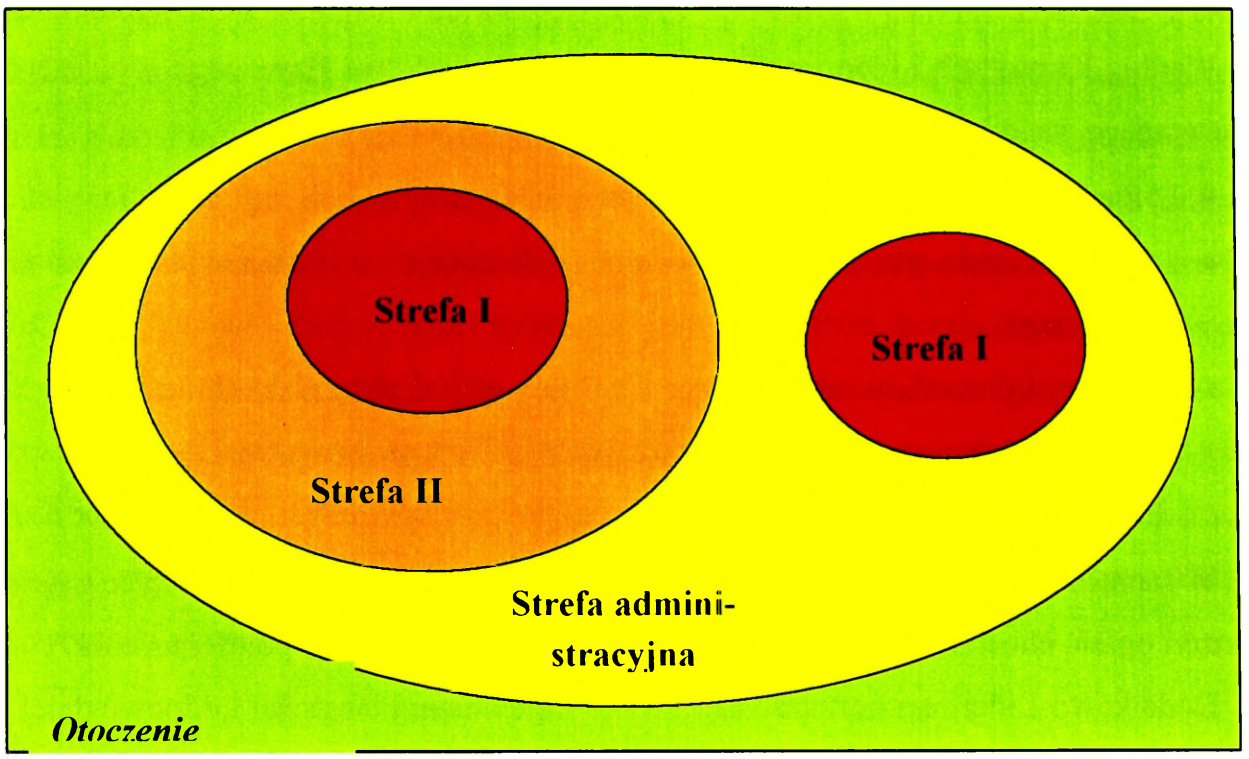
- strefa administracyjna,
- strefa II,
- strefa I.

Gradacja zabezpieczeń przebiega od zabezpieczeń najniższych w strefie administracyjnej do ścisłej kontroli dostępu w strefie I. I tak Strefa administracyjna jest to obszar chroniony, o najmniejszym stopniu zabezpieczeń, w ramach którego odbywa się już kontrola ruchu

---

[43] „Dyrektywa bezpieczeństwa- AD 70-1 PL"
[44] Bezpieczeństwo teleinformatyczne"- op. cit.

osób i pojazdów. Obszar ten przylega bezpośrednio do obszarów klasy I i II (rys. 4.1.1). Granice tych obszarów muszą być zaznaczone w sposób wyraźny.



Rys. 4.1.1. Koncepcja stref bezpieczeństwa

Strefy I i II są strefami, w których znajduje się informacja niejawna i w związku z tym muszą one zapewnić wspomnianą wcześniej rozliczalność, czyli kontrolować w sposób osobowy (imienny) wstęp do tych stref. Niezbędne są dodatkowe urządzenia kontroli dostępu, które mogą identyfikować osoby. Wszystkie osoby poruszające się po tych strefach muszą posiadać odpowiednie poświadczenia bezpieczeństwa, umożliwiające im kontakt z informacją znajdującą się w tym obszarze. Oczywiście należy przewidzieć sytuacje w których osoby inne niż stały personel będą musiały znaleźć się w strefie bezpieczeństwa. W tym celu należy określić osoby, które są uprawnione do wydawania zgody na takie wejście i osoby, które będą bezpośrednio odpowiedzialne za nadzór nad zakresem dostępu przez osoby trzecie do informacji niejawnych, z zachowaniem zasady wiedzy niezbędnej (ang. *need to know*).

Przejście pomiędzy obszarami musi być możliwe tylko w określonych miejscach, wyposażonych w odpowiednie systemy dostępu.

Kontrolę dostępu można realizować zarówno przy pomocy specjalnego personelu (wartownika, strażnika) jak i odpowiedniego sprzętu w postaci bramek wyposażonych w czytniki przepustek identyfikacyjnych. Niektóre przepisy, na przykład Dyrektywa

AD 70-1 PL traktują bramki jako urządzenia wspomagające ochronę a nie jej ekwiwalent, innymi słowy minimalnym zabezpieczeniem jest wartownik. Oczywiście są to przepisy obowiązujące w instytucjach NATO, więc w innych organizacjach rozwiązania mogą być odmienne, w zależności od chronionej informacji. Zaletą tego rozwiązania jest fakt iż występowanie tych dwóch środków równolegle prowadzi do zdublowania ról, co zwiększa poziom bezpieczeństwa obiektu, a co za tym idzie, znajdującej się w nim sieci komputerowej.

Zabezpieczenia konstrukcyjne i systemy alarmowe

Przez zabezpieczenia konstrukcyjne należy rozumieć wszelkie instalacje budowlane i inne, których zadaniem jest uniemożliwić ich sforsowanie. Przykładem takich zabezpieczeń może być zarówno ściana z cegły o grubości 30 cm ale również są to kraty na oknach, posiadające oczka o średnicy nie przekraczającej 20 mm. Na początek przyjrzyjmy się zabezpieczeniu pomieszczenia znajdującego się w budynku.

Po pierwsze musimy ocenić jakie jest bezpośrednie otoczenie naszego pomieszczenia, należy przez to rozumieć zarówno korytarz, pomieszczenia sąsiednie jak i otoczenie znajdujące się za oknem. Odpowiednio niższe będą wymogi na strukturę ściany oddzielającej pomieszczenia będące strefami o tej samej klauzuli niżeli na ścianę będącą granicą strefy. W przypadku kiedy mamy do czynienia z granica strefy I, gdzie znajdują się informacje stanowiące tajemnicę państwową ściana powinna posiadać taką grubość aby jej wytrzymałość odpowiadała ścianie betonowej o grubości 15cm. Ponadto ściana taka powinna posiadać zabezpieczenia elektroniczne w postaci czujek sejsmicznych, które zostaną omówione w dalszej części tego rozdziału.

Kolejnym elementem zabezpieczającym pomieszczenia są drzwi. Tutaj sytuacja jest podobna do powyższej, tzn. inne drzwi zastosujemy w przypadku przejścia pomiędzy pomieszczeniami w ramach tej samej strefy, a inne w przypadku granicy strefy. Drzwi stanowiące granicę strefy również powinny posiadać odpowiednią wytrzymałość, ryglować się we wszystkich krawędziach i być wyposażone w atestowane zamki, posiadające klasę bezpieczeństwa A, B lub C w zależności od klauzuli informacji którą mają zabezpieczać. Zamek klasy A (zgodnie z nomenklaturą NATO) jest to zamek w którym do zmiany szyfru niezbędny jest klucz i można tą operację przeprowadzić wyłącznie od wewnętrznej strony drzwi. Z kolei zamki klasy B są to zamki które także wymagają do zmiany kombinacji klucza, ale nie muszą posiadać innych cech zamka klasy A. Zamki klasy C są to zamki certyfikowane do użycia w meblach biurowych i zabezpieczonych sejfach.

Co do zawiasów drzwi zabezpieczających pomieszczenia, powinny być one umieszczone od wewnątrz, albo sworznie zawiasów powinny być lutowane mosiądzem lub spawane, w celu uniemożliwienia prób nieuprawnionego zdjęcia. Rama i mocowania drzwi powinny być co najmniej równie wytrzymałe jak same drzwi. Ściany w których osadzone są drzwi wraz z górnym ryglem nie powinny być słabsze niż drzwi.

Kolejnym elementem który należy zabezpieczyć w chronionym pomieszczeniu są okna. I tu znowu musimy najpierw zweryfikować otoczenie. Jeżeli nasze pomieszczenie znajduje się powyżej wysokości 5,5 metra i okna nie sąsiadują na przykład z ogólnodostępną ulicą to możemy poprzestać na wzmocnionych oknach , które dodatkowo wyposażone są w czujnik stłuczenia szyby. Niezbędne oczywiście jest także wykonanie szyb ze szkła nieprzeźroczystego, bądź wyposażenie w inne elementy umożliwiające ich zasłonięcie (żaluzje, zasłony, lustro weneckie), co ma na celu uniemożliwić ewentualne wizualne penetrowanie obszaru chronionego. Natomiast jeżeli nasze okno jest poniżej 5,5 metra nad terenem niekontrolowanym dachów, parapetów, itp., niezbędne jest zastosowanie okien z zabezpieczeniami antywłamaniowymi, wyposażonymi w szyby o podwyższonej wytrzymałości lub zbrojone, ale także dodatkowe wyposażenie ich w kraty, których rozmiar oczek jest określony przez odpowiednie przepisy, i które są wystarczająco solidnie osadzone w ścianie.

Okna nie są jednak jedynymi otworami w ścianach, pamiętać należy o pozostałych, takich jak chociażby wentylacja. Otwory wentylacyjne również powinny być zabezpieczone. W tym przypadku należy sobie zdawać sprawę z kilku zagrożeń. Pierwszym z nich jest oczywiście przedostanie się osób bądź innych stworzeń, które mogą zagrozić bezpieczeństwu informacji. Drugim z niebezpieczeństw jest podsłuch zarówno pośredni w postaci tzw. „pluskiew", jak również i ten akustyczny, kiedy to głos rozchodzi się kanałami wentylacyjnymi po sąsiednich pomieszczeniach. Można się oczywiście przed tym zabezpieczyć, montując odpowiednie kratki, które po pierwsze będą stanowiły barierę dla intruzów próbujących się dostać do chronionego pomieszczenia, a po drugie mogą dodatkowo stanowić tłumik akustyczny.

Zabezpieczone w ten sposób pomieszczenie należy dodatkowo wyposażyć w system alarmowy. Spełnia on funkcję aktywnego zabezpieczenia pomieszczeń, przed niepowołanym dostępem. W ramach systemu alarmowego powinien się znajdować szereg czujek rozmieszczonych w różnych miejscach pomieszczenia i działających na różnego rodzaju bodźce. Tak jak już wspominaliśmy przy okazji zabezpieczania okien, instaluje się czujki reagujące na stłuczenie szyby, innymi czujkami o tym samym zadaniu, czyli kontrolującymi dostęp do pomieszczenia, są czujniki otwarcia drzwi i wspomniane czujki sejsmiczne umieszczone na ścianach. Ponadto w pomieszczeniu powinny się znajdować czujki wykrywające ruch, po-

krywające całą przestrzeń, której nie możemy kontrolować wzrokowo, chodzi tu przede wszystkim o różnego rodzaju sufity podwieszane czy otwory wentylacyjne. Pomieszczenie można wyposażyć w przycisk antynapadowy, który w zależności od przeznaczenia pomieszczenia może być przytwierdzony na stałe, bądź występować w postaci pilota. Całość systemu powinna być nadzorowana przez 24 godziny na dobę przez ochronę obiektu. Wskazane jest, aby system był rozbrajany i uzbrajany jednocześnie przez uprawnionego użytkownika i ochronę, a informacje o wszystkich zdarzeniach w systemie były zapisywane i co jakiś czas weryfikowane przez osobę odpowiedzialną za ochronę. W ramach kodów rozbrajających system można określić także tzw. kod wejścia pod przymusem, kiedy to uprawniona osoba zostaje zmuszona do otworzenia pomieszczenia i w ten sposób może powiadomić ochronę o zaistniałej sytuacji.

Systemy alarmowe są obszarem, w którym określone zostały standardy i normy, w Polsce jest to chociażby PN-EN 50131-1:2002(U). Często przepisy powołują się na konkretne standardy, w przypadku systemów wojskowych wymagany jest na przykład standard SA4 dla całego systemu.

Ciągłość pracy urządzeń

Poprzednio omawiany powyżej wymóg bezpieczeństwa, a mianowicie dostępność, nakłada na nas kolejny istotny wymóg w postaci zapewnienia ciągłości pracy urządzeń. Zagadnienie to obejmuje kwestie dotyczące zarówno sprawności urządzeń jak i zapewnienia im warunków do pracy w postaci na przykład ciągłego i posiadającego właściwe parametry zasilania.

Bardzo często użytkownik oczekuje od sieci komputerowej, że jej zasoby będą dostępne w każdej chwili (ang. *on demand*), w związku z tym trzeba się zastanowić jak rozwiązać sprawę serwisowania urządzeń i procedur z tym związanych. Bardzo istotne jest wyselekcjonowanie kompetentnej firmy, która przede wszystkim zapewni nam odpowiedni poziom bezpieczeństwa (posiadanie przemysłowego poświadczenia bezpieczeństwa przez firmę i poświadczeń indywidualnych przez wszystkich pracowników obsługujących urządzenia) przy zachowaniu wymogów związanych z jakością obsługi sprzętu. W przypadku bardziej rozbudowanej sieci należy dokładnie przeanalizować jej zasoby pod kątem istotności poszczególnych urządzeń dla funkcjonowania całej sieci i dopiero z taką wiedzą określanie dla nich warunków serwisowania. Jeżeli chodzi o urządzenia istotne dla funkcjonowanie sieci, takie jak rutery i serwery warte rozważenia jest stworzenie gorącej rezerwy sprzętowej, co umożliwi awaryjnie bezzwłoczne przywrócenie sieci do pracy. Ciekawym przykładem mogą być banki

i ich sieci tranzakcyjne, w których normą stało się tworzenie zapasowych centrów obsługujących operacje sieciowe, które niemalże natychmiastowo przejmują funkcje centrum głównego. Pozostałe urządzenia możemy rozpatrywać w kategoriach naprawy w kolejnych dniach roboczych (*ang.* Next Bussiness Day-NBD), użytkownik jest w stanie korzystać z drukarki czy nawet komputera sąsiada (o ile dopuszcza to polityka bezpieczeństwa danej sieci) przez jeden czy dwa dni. Doświadczenie ostatnich miesięcy pokazuje jak bardzo ważne są procedury wycofywania zużytych elementów takiej sieci. Jeżeli komputer wykorzystywany był w sieci niejawnej to nie wszystkie z jego elementów zalecane są do powtórnego wykorzystania. Nośniki danych w postaci twardych dysków w zależności od stopnia niejawności należy albo zniszczyć albo wielokrotnie zapisać, gdyż istnieją metody odtworzenia zawartości dysków, które były raz czy dwa razy nadpisane. Odbywa się to przy pomocy głębszej analizy struktury magnetycznej nośnika, analizując brzegowe części ścieżek które tracą swój potencjał dopiero po dłuższym czasie. Podobnie dzieje się z dyskietkami, tyle, że w związku z niskimi kosztami tych nośników zaleca się ich niszczenie. Nieco inaczej sprawa przedstawia się w przypadku pamięci operacyjnych (*ang.* RAM- Random Access Memory), gdzie wystarczy kilkudniowy okres wyłączenia i zgromadzone w nich potencjały (informacje) tracone są bezpowrotnie.

Porównywalne, a może nawet większe znaczenie dla sprawności sieci ma jej zasilanie. W miarę rozwoju technologii komputery i inne urządzenia sieciowe stają się coraz bardziej wrażliwe na wahania sieci energetycznej. W związku z tym należy się zabezpieczyć przed różnego rodzaju zaburzeniami zasilania. Jeżeli natomiast mowa o ciągłości zasilania, to należy wymienić trzy zasadnicze sposoby zapobiegania zanikom napięcia, a mianowicie:

- przyłączenie do obiektu dwóch niezależnych linii energetycznych;
- stosowanie siłowni (agregatów);
- stosowanie zasilaczy awaryjnych (*ang.* UPS-Uninterruptable Power Supply).

Głównym zadaniem zasilaczy awaryjnych jest podtrzymanie zasilania, w przypadku krótkotrwałych zaników napięcia, ewentualnie do czasu uruchomienia siłowni zastępczych. Zasilacze awaryjne są niezbędnymi urządzeniami w sieciach komputerowych, jednak ich właściwa praca zależy w dużym stopniu od sposobu eksploatacji i obsługi, uwagę należy zwrócić na częstą kontrolę stanu baterii i regularne wykonywanie ich kalibracji. Nowoczesne UPS-y umożliwiają podłączenie ich do zasilanych urządzeń i przy ich pomocy zarządzanie parametrami zasilaczy. Poza tym istnieje jeszcze jedno bardzo ważne zastosowanie takiego połączenia, otóż można skonfigurować aplikację w taki sposób, aby przy krańcowym rozładowaniu

baterii zasilających urządzenia wydała systemowi operacyjnemu komendę do zamknięcia się, przez co można zapobiec utracie nie zapisanych danych.

Kolejnym zagrożeniem dla sprawności urządzeń jest wysoka temperatura. Okazuje się, iż nie tylko ludzie mają problemy z funkcjonowaniem w podwyższonych temperaturach, ale także urządzenia informatyczne wymagają utrzymania stałej temperatury na poziomie 18-22°C. Długotrwała praca w wyższych temperaturach zmniejsza żywotność i zwiększa awaryjność urządzeń.

Systemy przeciwpożarowe i ostrzegania o innych zagrożeniach

Bardzo istotne z punktu widzenia ciągłości pracy sieci komputerowej są wszelkie systemy ostrzegające i zapobiegające rozprzestrzenianiu się ognia i wody. Te dwa żywioły stanowią poważne zagrożenie dla sprawności urządzeń, ponieważ mogą uczynić je trwale niezdolnymi do pracy, co więcej zagrażają także nośnikom, na których zapisane są informacje.

Często spotykać można rozwiązania integrujące systemy ochrony, które integrują w sobie następujące podsystemy:

- sygnalizacji włamań i napadu,
- sygnalizacji pożaru i zalania,
- telewizji przemysłowej,
- monitorowania podejść do chronionego obiektu i jego wnętrza,
- kontroli dostępu,
- kontroli służb ochrony.

Jest to rozwiązanie praktyczne i ekonomiczne, ponieważ zmniejsza ilość specjalistycznego osprzętu w postaci central alarmowych i daje możliwość zcentralizowanego zarządzania.

4.1.2. Bezpieczeństwo elektromagnetyczne

Ten aspekt bezpieczeństwa związany jest ze wspomnianą wcześniej emisją ujawniającą urządzeń sieci komputerowych. Jest wiele sposobów zabezpieczania się przed ulotem informacji. Po pierwsze można stworzyć pomieszczenie, które stanowi klatkę Farraday'a. Osiąga się to przez powleczenie całej powierzchni pomieszczenia, podłogi, sufitu, ścian okien i drzwi drobną siatką wykonaną z materiału posiadającego dobre właściwości przewodzące (np. miedź), a następnie uziemienie całości do punktu o bardzo niskim potencjale i rezystancji. Istotne jest aby całe pomieszczenie było szczelnie wyścielane, żeby nie występowały

przerwy w ciągłości siatki, wszelkie elementy ruchome (drzwi, okna) powinny być wyposażone w specjalne uszczelki posiadające analogiczne właściwości jak siatka. Należy jednak pamiętać, że rozwiązanie to tłumi emisję propagowaną, tak zabezpieczone pomieszczenie należy więc doposażyć w tzw. separatory zainstalowane na wszystkich elementach metalowych wychodzących poza strefę, takich jak instalacje CO, wentylacyjne czy klimatyzacyjne, wstawiając je na granicy strefy, eliminując w ten sam sposób emisję przewodzoną.

Kolejnym sposobem zabezpieczenia urządzeń przed emisją ujawniającą jest stworzenie tzw. BSK (Bezpiecznego Stanowiska Komputerowego) czyli również rodzaju klatki Farraday'a, tylko na mniejszą skalę, ponieważ nie obejmuje ona całego pomieszczenia tylko samo stanowisko komputerowe.

Ostatnim sposobem zabezpieczania się przed elektromagnetycznym ulotem informacji jest stosowanie urządzeń o zmniejszonej emisji elektromagnetycznej. Bardzo często urządzenia te określane są jako urządzenia TEMPEST-owe. Nazwa ta pochodzi od zapoczątkowanego pod koniec lat 50-tych w Stanach Zjednoczonych specjalnego programu badawczego którego celem było rozwinięcie metod ograniczania emisji ujawniającej[45]. Efektem prowadzonych do dnia dzisiejszego prac są coraz to nowsze standardy zabezpieczeń urządzeń. Komputery wykonane w tej technologii posiadają specjalną obudowę, która pełni rolę klatki Farraday'a, dodatkowo są one wyposażone w specjalne filtry, które eliminują ulot informacji przez okablowanie bezpośrednio podłączone do komputera. W tej samej technologii wykonane są wszystkie elementy takiego zestawu, zarówno jednostka centralna, monitor, drukarka, klawiatura, a nawet mysz. Specjalnie ekranowane i uziemione są wszystkie kable sygnałowe tych urządzeń. Konstrukcje te mają dwie zasadnicze wady. Po pierwsze, masywna konstrukcja nie gwarantuje wydajnego chłodzenia poszczególnych elementów komputera, co zwiększa ich awaryjność, co z kolei wiąże się z drugim słabym punktem tych konstrukcji, a mianowicie koniecznością powtórnej certyfikacji po wymianie jakiegokolwiek elementu, co stanowi wydatek rzędu nowego komputera komercyjnego (około 2-3 tysięcy złotych). W nowych rozwiązaniach zmienione zostało podejście do emisji. Wyszczególniono niepożądane częstotliwości niosące informację i częstotliwości od nich wolne. Zadaniem konstrukcji jest ograniczenie emisji związanej z ulotem informacji. Nie ma natomiast potrzeby eliminowania częstotliwości generowanych przez zegar taktujący procesor czy płytę. Zmierza się także do zwiększenia niezawodności tych urządzeń przez poprawienie ich chłodzenia.

---

[45] „Kryptograficzne i elektromagnetyczne aspekty bezpieczeństwa sieci teleinformatycznych"- Marek Suchański, Biuletyn WIŁ, Zegrze 2000;

Często jednak przepisy wymuszają na nas konkretne rozwiązania, ponieważ tzw. PZU (poziom zabezpieczenia urządzenia) zdeterminowany jest przez PZM (poziom zabezpieczenia miejsca). Jeżeli chronione pomieszczenie znajduję się w obszarze o dużym zurbanizowaniu i w jego sąsiedztwie znajdują się budynki niekontrolowane to będziemy musieli zastosować urządzenia TEMPEST-owe. Koszt takiego zestawu produkcji zagranicznej to około 100 tys. złotych, krajowy wyrób to wydatek 75 tys. złotych, przy czym trzeba uważać, by zestaw zawierał dokumentację związaną z certyfikacją. Jest to warunkiem uznania jego klasy bezpieczeństwa, a polskie firmy produkujące ten sprzęt są dopiero w trakcie uzyskiwania takich dokumentów. Korzystniej jest więc zainwestować w prace budowlane i mieć możliwość późniejszej wymiany urządzeń, przy stosunkowo niewielkich kosztach, niżeli być związanym z przestarzałymi i niekoniecznie funkcjonalnymi ale na pewno kosztownymi urządzeniami.

Wróćmy jeszcze na chwilę do emisji przewodzonej. Omówione przy okazji urządzeń TEMPEST-owych zabezpieczenia nie wystarczą aby zupełnie ją wyeliminować. Musimy pamiętać, że obiektem naszych rozważań są sieci, a więc komputery muszą być ze sobą połączone okablowaniem sieciowym i właśnie tu napotykamy kolejne miejsce gdzie istnieje zagrożenie ujawnienia informacji. Kanały kablowe powinny być zabezpieczone przed niekontrolowanym dostępem, ponadto należy pamiętać o zjawisku przesłuchów (sprzężeń kabli-pojemnościowych lub indukcyjnych). Polega ono na indukowaniu się pochodnej sygnału pierwotnego w kablu biegnącym równolegle do naszego sygnału. Zjawisko to można wyeliminować na dwa sposoby. Po pierwsze zachowywać odpowiednie odległości pomiędzy przewodami sygnałowymi a innym okablowaniem, bądź zastosować okablowanie światłowodowe. Jest ono wprawdzie droższe, ale wymogi na przebieg tras kablowych są znacznie łagodniejsze, a w zasadzie należy skupić się przede wszystkim na ich fizycznym zabezpieczeniu przed nieuprawnioną ingerencją.

Zabezpieczenia wymagają także inne instalacje podłączone do naszych urządzeń, takie jak zasilanie czy uziemienie. W przypadku instalacji zasilających problem rozwiązywany jest przez zastosowanie zasilaczy awaryjnych wyposażonych w transformatory izolacyjne. Uziemienia natomiast muszą być wydzielonym obwodem, nie podłączonym do innych urządzeń (jawnych), co więcej powinny być zakończone w obszarze będącym strefą bezpieczeństwa. Powinny one także spełniać wymogi co do poziomu maksymalnej rezystancji i tak krajowe przepisy mówią o wartości nie przekraczającej 5Ω, przepisy NATO są bardziej rygorystyczne i mówią o wartości maksymalnej 1Ω. Często wymaga to zastosowania odpowiednio długich szpilek, w różnych ilościach, w zależności od właściwości gruntu.

4.1.3. Bezpieczeństwo programowe

Ostatnim aspektem bezpieczeństwa który omówimy będzie bezpieczeństwo programowe. Pod tym pojęciem kryją się zagadnienia związane z zasobami informacyjnymi komputerów znajdujących się w sieci. Korzystając z podziałów przedstawionych przez Stokłosę[46] zagadnienia te podzielimy na następujące grupy:

- uwierzytelnianie użytkowników;
- zarządzanie prawami dostępu;
- dzienniki zdarzeń;
- profilaktyka antywirusowa;
- archiwizacja informacji.

Należy zaznaczyć, że dziedzina oprogramowania komputerowego jest bardzo prężną i szybko rozwijającą się. W sprzedaży pojawiają się coraz to nowsze systemy operacyjne, posiadające nowsze i lepsze zabezpieczenia, jednak, jak pokazuje doświadczenie, nie są one wolne od wad. Równolegle z legalnym oprogramowaniem pojawiają się wciąż nowe i coraz groźniejsze programy złośliwe. W związku z tym należy na bieżąco śledzić wydarzenia w tej dziedzinie.

Uwierzytelnianie użytkowników

Podstawowym narzędziem administratora w zapewnianiu bezpieczeństwa informacji w sieci komputerowej jest zarządzanie użytkownikami. Jest to kolejny etap kontroli dostępu do informacji. Zgodnie z „Elementarzem bezpieczeństwa systemów informatycznych" możemy wyróżnić następujące sposoby uwierzytelniania użytkowników:

- **SYK** (*ang.* by Something You Know) – na podstawie wiedzy użytkownika,
- **SYH** (*ang.* by Something You Have) – na podstawie identyfikatorów materialnych,
- **SYA** (*ang.* by Something You Are) – na podstawie metod biometrycznych,
- **SYĐ** (*ang.* by Something You Do) – na podstawie czynności wykonywanych przez użytkownika.

---

[46] „Bezpieczeństwo danych w systemach informatycznych" – op. cit.

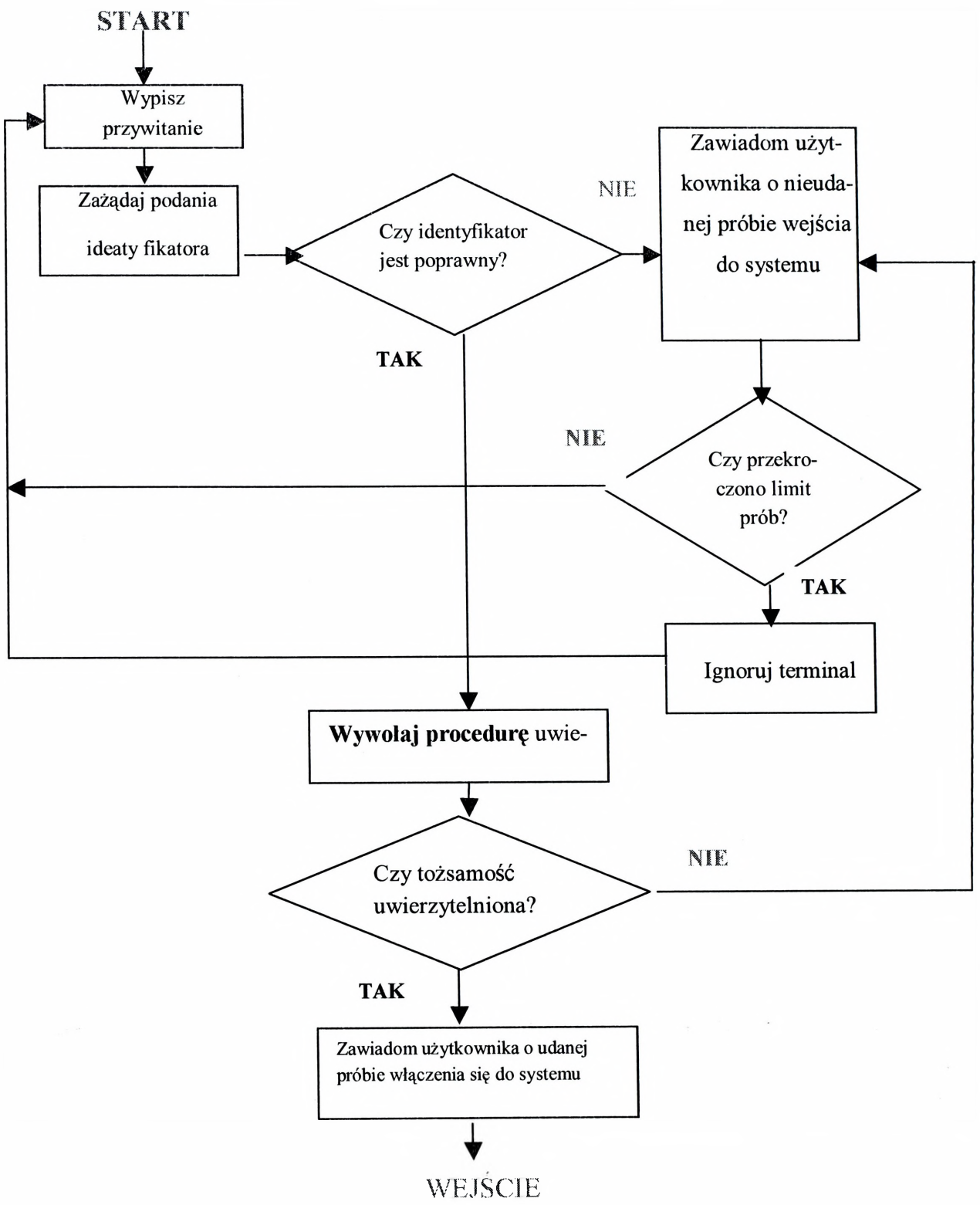
Pierwszy ze sposobów identyfikacji polega na sprawdzaniu przez system znajomości przez potencjalnego użytkownika danych dotyczących konta na które chce się zalogować, w postaci hasła albo nazwy użytkownika i hasła. Na tym poziomie możliwe jest określenie przez administratora systemu ilości niepoprawnych prób, które powodują zablokowanie konta.

Ponieważ jednak programy służące do łamania haseł stają się ogólnie dostępne, należy utrudnić łamanie haseł, czyniąc je nieopłacalnym, co można osiągnąć poprzez przestrzeganie kilku podstawowych zasad wyboru haseł[47]:

1. **Nie wybieraj:**
   - nazwiska (imienia, pseudonimu, przezwiska) twojego lub twoich bliskich,
   - nazw używanego oprogramowania, sprzętu,
   - numerów telefonów,
   - danych twojego samochodu,
   - danych identyfikacyjnych (nr DO, PESEL, NIP, ubezpieczenia, itp.),
   - łatwych do ustalenia informacji o tobie,
   - dat urodzenia,
   - nazw własnych,
   - słów ze słownika,
   - ciągu składającego się z identycznych znaków (np.: 11111111),
   - ciągu kolejnych znaków na klawiaturze (np.: qwerty, asdfgh),
   - ciągów liczących mniej niż 8 znaków,
   - wszystkich dotychczas wymienionych kombinacji w innych formach (np. wspak, dublowanie liter),
   - przekleństw, wulgaryzmów.
2. **Wybieraj hasła, które:**
   - zawierają małe i duże litery,
   - zawierają cyfry, znaki specjalne, znaki interpunkcyjne, symbole, itp.,
   - składają się z minimum 8 znaków,
   - są łatwe do zapamiętania przez użytkownika, ale trudne do odgadnięcia przez intruza,
   - są łatwe i szybkie we wprowadzaniu z klawiatury,
   - są dwoma wyrazami połączonymi znakiem specjalnym (np.: król-lew),

[47] „Elementarz bezpieczeństwa systemów informatycznych" – op. cit.

- są generowane losowo i podpowiadane przez system.



Rys.4.1.3.1. Typowa procedura identyfikacji i uwierzytelniania[48]

„Elementarz bezpieczeństwa systemów informatycznych" podaje także zestaw zaleceń praktycznych, które zwiększają skuteczność stosowania haseł. Są one następujące:

- hasła należy często zmieniać,

[48] „Elementarz bezpieczeństwa systemów teleinformatycznych"- op. cit.

- nie należy haseł nigdzie zapisywać,
- podczas wpisywania haseł na ekranie nie powinno być ich echa,
- po zwolnieniu pracownika, hasła w firmie powinny być natychmiastowo zmienione,
- ilość błędnych prób wpisywania hasła powinna być limitowana, po przekroczeniu limitu konto powinno zostać zablokowane,
- zmiana haseł powinna być wymuszana przez system po upływie określonego czasu jego „życia",
- wzorce haseł powinny być przechowywane w szyfrowanym pliku systemowym,
- hasła powinny być generowane losowo,
- administrator może zmienić hasło użytkownika, lecz nie może poznać hasła wprowadzonego przez użytkownika,
- system powinien wyświetlać ostatnie czasy logowania (udanego i nieudanego) tak aby użytkownik mógł wychwycić nielegalne próby logowania,
- w szczególnych zabezpieczeniach hasła mogą być dwuczęściowe i wymagać obecności dwóch osób,
- mogą być stosowane specyficzne formy kontroli dostępu do systemu tj.:
  - jednorazowe hasła według listy,
  - hasła uwarunkowane zegarem procesora,
  - kontrola typu *hasło-odzew*,
  - kontrola typu dialogowego.

Kolejnym sposobem uwierzytelniania jest SYH, czyli weryfikowanie na podstawie identyfikatorów materialnych, którymi mogą być różnego rodzaju karty magnetyczne, elektroniczne, klucze elektroniczne). Zaletą tej metody jest skomplikowanie pod względem sfałszowania, ponieważ wymaga zaangażowania nietypowych urządzeń i wiedzy na temat systemu i użytkowników. Zdecydowanymi wadami tego rozwiązania są wrażliwość na czynniki zewnętrzne i niebezpieczeństwo występujące w przypadku zagubienia bądź kradzieży, o ile nie ma dodatkowego zabezpieczenia w postaci haseł potwierdzających.

Trzecią metodą uwierzytelniania jest SYA, polegające na sprawdzaniu charakterystycznych dla człowieka cech fizycznych, w postaci siatkówki oka, linii papilarnych czy głosu. Rozwiązanie to posiada niewątpliwą przewagę nad poprzednikami, ponieważ jest ciężkie, praktycznie niemożliwe do sfałszowania, nie można tego zgubić ani zapomnieć i wiąże się

z ogromną wygodą w użytkowaniu. Niewątpliwym minusem tej technologii jest jej kosztowność. Jednak wszystko wskazuje na to, że w niedalekiej przyszłości rozwiązania takie staną się powszechne.

Ostatnim z wymienionych rodzajów uwierzytelniania jest SYD, będące pochodną SYA i SYK, w celu potwierdzenia tożsamości i hasła. Może się ono odbywać zarówno przy pomocy pisma jak i mowy. Rozwiązanie to jest dopiero w fazie testów i badań.

4.1.4. Zarządzanie prawami dostępu

Dostęp do informacji na poziomie sieci komputerowej jest dwuetapowy. Pierwszy etap, czyli uzyskanie dostępu do systemu już został omówiony. Drugim etapem jest uzyskanie dostępu do wybranych zasobów, co związane jest z uprawnieniami jakie dany użytkownik posiada.

Wyróżniamy następujące rodzaje kontroli dostępu do informacji:

- swobodna (*ang. discretionary access control*),
- obowiązkowa (*ang. mandatory access control*),
- zależna od zadań (*ang. role-based access control*).

Pierwszy ze sposobów polega na każdorazowym sprawdzeniu, czy użytkownik posiada uprawnienia do danej informacji. Mankamentem tej metody jest konieczność określania i weryfikowania dla każdego użytkownika praw dostępu do danego zasobu.

Kolejną metodą jest obowiązkowa kontrola dostępu. Polega to na określeniu klauzuli dla każdego zasobu i określeniu maksymalnych uprawnień dla każdego użytkownika. System sprawdza, czy poziom klasyfikacji informacji jest mniejszy bądź równy poziomowi posiadanemu przez użytkownika. Jeżeli tak, zezwala na jego wykorzystanie, w przeciwnym zaś razie odmawia dostępu. Mankamentem tego rozwiązania jest brak możliwości wprowadzenia zasady wiedzy niezbędnej (*ang. need to know*), księgowy nie musi, a czasem nawet nie może posiadać informacji związanych na przykład ze szczegółami technicznymi kontraktów organizacji.

Ostatnim z wymienionych rodzajów kontroli dostępu do zasobów jest kontrola dostępu zależna od wykonywanych zadań. Metoda ta składa się z dwóch elementów po pierwsze zadań wykonywanych przez wybranych użytkowników, a po drugie z obiektów które są niezbędne do ich realizacji.

Kontrolą dostępu do zasobów można zarządzać na kilka sposobów, wśród których wyróżniamy:

- ***sposób scentralizowany*** – uprawnienia przyznaje jeden (główny) administrator,
- ***sposób hierarchiczny*** – występują szczeble administrowania i każdy z nich zarządza uprawnieniami w ramach swojego obszaru odpowiedzialności,
- ***sposób zdecentralizowany*** – (samodzielny) właściciel obiektu upoważnia innych użytkowników do swojego obiektu,
- ***sposób dzielony*** – następuje wspólne korzystanie z jednego zasobu przez kilku użytkowników, za zgodą wszystkich zainteresowanych.

Wszystkie dostępne obecnie na rynku sieciowe systemy operacyjne oferują możliwość zarządzania prawami dostępu do zasobów. Zazwyczaj wykorzystują one zasadę swobodnego dostępu, w systemach Windows opartych na technologii NT tworzy się profil użytkownika posiadający określone uprawnienia, a następnie przypisuje się go do użytkowników. Dodatkowo każdy zasób ma możliwość określenia użytkowników którzy mogą z niego korzystać, bądź określić hasła uprawniające do tego.

4.1.5. Dzienniki systemowe

Pod pojęciem dziennika należy rozumieć *logi systemowe*, czyli pliki zawierające informacje na temat pracy zarówno pojedynczego komputera, jak też domeny. Przy pomocy dziennika osoba odpowiedzialna za bezpieczeństwo może uzyskać wiele cennych informacji związanych z pracą sieci, takich jak:

- daty ostatnich logowań,
- próby logowania zakończone niepowodzeniem,
- czas pracy konkretnych użytkowników w sieci,
- ważniejsze operacje wykonywane przez użytkowników.

W oparciu o takie dane można nie tylko wykrywać włamania lub ich próby, ale także zmieniać konfigurację sieci w celu usprawnienia jej pracy, wykrywać najsłabsze elementy

systemu, analizować skuteczność poszczególnych zabezpieczeń oraz wiele innych czynności pomagających bezpiecznie administrować siecią.

Dzienniki zdarzeń są coraz częściej wykorzystywane przez specjalne aplikacje, które analizują ich zawartość i podają w sposób czytelny interesujące nas dane. Na rynku rozpowszechniły się oprogramowania służące wykrywaniu włamań określane jako IDS/IRS (*ang. Intrusion Detection System/Intrusion Response System*). Programy te w sposób dynamiczny analizują dzienniki zdarzeń w podległych im systemach i wykrywają niepożądane zjawiska, a najnowsze potrafią nawet kojarzyć ze sobą pewne fakty świadczące o bardziej złożonych procesach zagrażających systemom. Istnieje możliwość określenia reakcji takiego programu na konkretne sytuacje, na przykład można mu zadać, że w przypadku wykrycia włamania ma/może samodzielnie zapobiegać ich postępowaniu, na przykład wyłączając podejrzaną stację roboczą.

4.1.6. Profilaktyka antywirusowa

Drugą bardzo istotną z punktu widzenia bezpieczeństwa informacji funkcją systemów IDS/IRS jest działanie antywirusowe. Jak pokazują wydarzenia ostatnich tygodni i miesięcy programy złośliwe są bardzo dużym zagrożeniem dla sieci komputerowych, a co za tym idzie informacji w nich zawartych. Na przykładzie robaka SASSER można zaobserwować jak programy złośliwe potrafią zaburzyć pracę dużych i - wydawać by się mogło - dobrze zabezpieczonych sieci. Są to tylko niektóre z powodów, dla których ochrona antywirusowa jest tak ważna.

Na rynku jest bardzo dużo różnego rodzaju programów antywirusowych. W zależności od zastosowań możemy sobie wybierać odpowiednie produkty, przy pomocy których można zabezpieczać sam system operacyjny, kontrolery domeny, serwery pocztowe a nawet konkretne procesy wykonywane przez komputery.

Zainstalowanie oprogramowania antywirusowego musi być poparte wieloma innymi przedsięwzięciami profilaktycznymi, które zapobiegają zainfekowaniu sieci. Podstawową czynnością jest wykonywanie regularnych aktualizacji bazy wirusów skanera antywirusowego. Ponadto należy pamiętać o tym, co powiedziane zostało już wcześniej, a mianowicie, iż nowe oprogramowanie nie jest wolne od wad i w miarę upływu czasu producenci wypuszczają tzw. Patch-e (łatki, uaktualnienia), które mają za zadanie eliminować kolejne wykryte luki w zabezpieczeniach programów.

Bardzo ważnym elementem obrony przed programami złośliwymi jest ograniczanie dróg infekcji. Większość obecnie występujących wirusów rozprzestrzenia się poprzez Internet, wykorzystując do tego celu pocztę, bądź - jak to miało miejsce ostatnio - samodzielnie odwołując się do konkretnego portu komputerów znajdujących się w otoczeniu i instalując się w nich. Jednakże, w przypadku sieci przeznaczonej do przetwarzania informacji niejawnych wykluczone jest jej połączenie z ogólnodostępnym Internetem. Możliwymi zaś drogami infekcji są wszelkie stacje pamięci zewnętrznych (stacje dyskietek, CD-ROM, PenDrive, itp.), należy więc ograniczyć ich wykorzystanie do niezbędnego minimum. Sytuacje, w których pamięci zewnętrzne muszą być wykorzystywane, powinny być monitorowane przez osoby odpowiadające za bezpieczeństwo sieci, a nośnik powinien zostać sprawdzony skanerem antywirusowym.

4.1.7. Archiwizacja danych

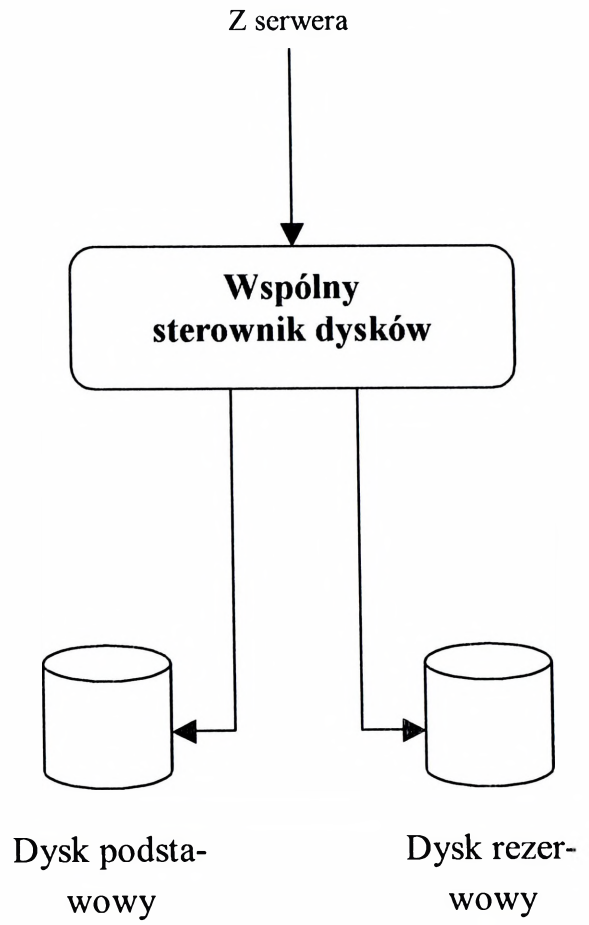
Użytkując sieć komputerową należy liczyć się z możliwością awarii sprzętowej bądź innego zdarzenia, które doprowadzi do utraty zawartych w serwerze bądź pojedynczym dysku informacji. W tym celu stosuje się dwa rodzaje zabiegów, pierwszy typowo sprzętowy polegający na organizacji zapisu danych na dyskach w taki sposób, aby po awarii jednego z nich możliwe było odtworzenie jego zawartości w oparciu o pozostałe. Drugą metodą jest wykonywanie tzw. Backup-ów czyli kopii bezpieczeństwa, polegających na zapisywaniu najistotniejszych informacji na nośnikach zewnętrznych.

W ramach pierwszej metody określanej jako FTS (*ang. Fault Tolerant System*) postaramy się przytoczyć najpopularniejsze z rozwiązań RAID (*ang. Redundant Array of Inexpensive Disks*), bazujące na zapisie danych w nadmiarowej macierzy dysków.

- **RAID_1** – metoda ta polega na dublowaniu dysków, gdzie każdy dysk główny posiada swój odpowiednik rezerwowy. W ramach tej metody wyróżniamy *mirro ring* kiedy to obydwa dyski podłączone są do tego samego sterownika i *duplexing* kiedy każdy z nich posiada swój niezależny sterownik sprzętowy. Zasadę działania obydwu metod przedstawiono na rys. 4.1.7.1.a i b.
- **RAID_2** – każdy bajt danych zapisywany jest na 8 dyskach po jednym bicie na każdym z nich i dodatkowo na 3 kolejnych dyskach zapisywane są trzy bity nadmiarowe.
- **RAID_3** – kolejne bajty informacji zapisywane są na kolejnych dyskach (2 do 4 dysków), na piątym dysku zapisywana jest wartość funkcji XOR zapisywanej informacji.

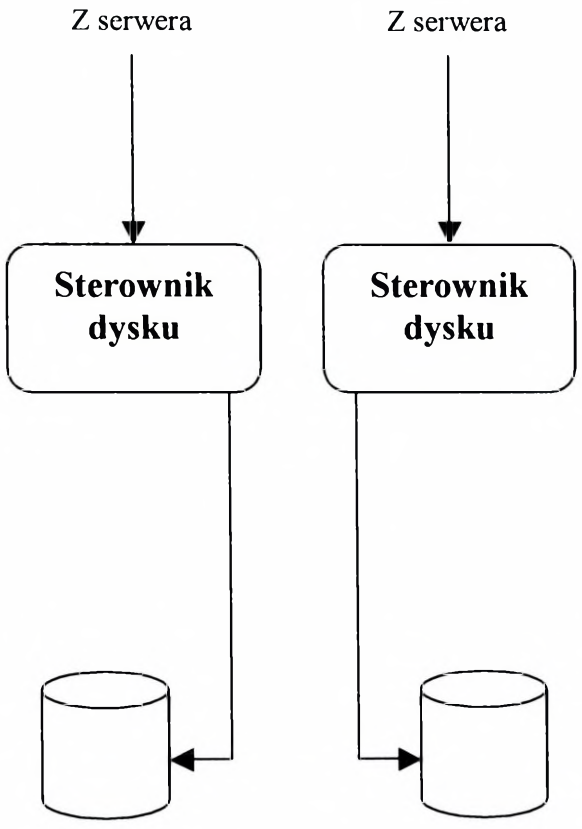
- **RAID_4** – zapis zbliżony jak w RAID_3, z tą różnicą, że na dysku piątym znajduje się suma modulo 2 zapisywanej informacji.
- **RAID_5** – metoda podobna do RAID_4, jednak informacja kontrolna jest zapisywana kolejno na wszystkich dyskach, brak jednego wyodrębnionego dysku zawierającego tylko i wyłącznie te dane.

a)



Rys.4.1.7.1.a. Dyski lustrzane

b)



Rys.4.1.7.1. b. Dyski zdublowane[49]

W sytuacjach kiedy uszkodzeniu ulegnie jeden z dysków macierzy redundancja dysków pozwala na odtworzenie zapisanych informacji z pozostałych dysków. Sposób odzyskiwania danych po awarii przedstawia rys. 4.1.7.2. a, b.

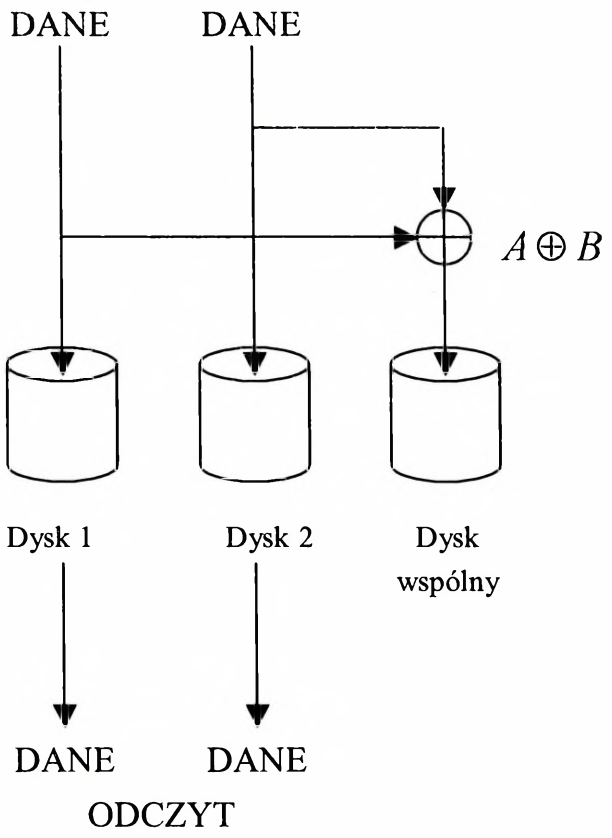
W praktyce spotkać można również inne wersje tej technologii, należą one jednak do rzadkości.

Drugim sposobem zabezpieczania się przed utratą informacji są kopie bezpieczeństwa. Powinny one obejmować zarówno informacje niejawne, które znajdują się w sieci, jak i dane konfiguracyjne sieci. I tak na przykład serwery pocztowe powinny zapisywać konfigurację kont użytkowników, ale także zawartość skrzynek. Kontrolery domeny natomiast zawierają informacje o samej sieci (przyłączone do sieci stacje robocze, konta użytkowników, adresacja sieci, itp.), a często również katalogi domowe użytkowników, w których umieszczone są ich pliki.

---

[49] „Elementarz bezpieczeństwa systemów teleinformatycznych" – op. cit.

a)

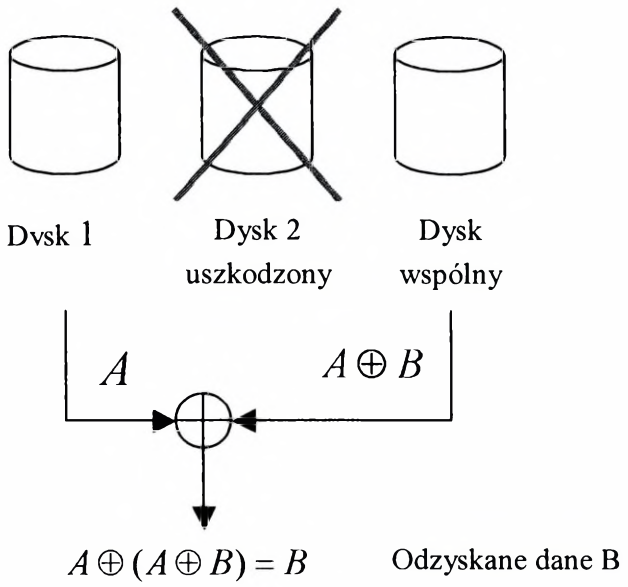


Rys. 4.1.7.2. a) Schemat działania macierzy dyskowych - zapis danych

W dostępnych na rynku rozwiązaniach programowych możemy się spotkać z następującymi sposobami wykonywania kopii bezpieczeństwa:

- *archiwizacja prosta (kompletna)* - regularne (np. codzienne) zapisywanie wszystkich danych zawartych w komputerze;
- *archiwizacja przyrostowa* - wykonywanie pełnej kopii wyłącznie w określone dni (np. każdy piątek), a w pozostałe dni zapisuje się wyłącznie dane przyrostowe, czyli te które pojawiły się od ostatniego wykonanego backup'u (poprzedniego dnia);
- *archiwizacja różnicowa* - wykonywanie pełnej kopii wyłącznie w określone dni (np. każdy piątek), a w pozostałe dni zapisuje się dane które zostały dopisane od ostatniego pełnego backup'u (ostatniego piątku).

b)



Rys. 4.1.6.2. b. Schemat działania macierzy dyskowych - odzyskiwanie danych z uszkodzonego dysku[50]

Nie bez znaczenia jest rodzaj nośnika którego będziemy wykorzystywać do wykonywania kopii bezpieczeństwa. W zależności od wielkości systemu, a co za tym idzie ilości danych wymagających archiwizacji, będziemy potrzebowali nośników o większych pojemnościach. Ponadto trzeba zastanowić się nad okresem i miejscem przechowywania tych nośników, ponieważ każdy z dostępnych rodzajów nośników (optyczne, magnetyczne, magnetooptyczne) ma inne właściwości i jest wrażliwy na inne czynniki. Nie wskazane jest używanie nośników magnetycznych w obszarach narażonych na silne pole magnetyczne, ponieważ może to doprowadzić do uszkodzenia ich struktury magnetycznej. Nośniki optyczne z kolei są wrażliwe na działanie promieni słonecznych.

4.2. Polityka bezpieczeństwa

Wszystkie dotychczas omówione metody zabezpieczania informacji w sieci komputerowej są przedsięwzięciami technicznymi. Aby zapewnić bezpieczeństwo informacji w sieci komputerowej należy również określić politykę bezpieczeństwa dla konkretnej sieci. W przypadku sieci komputerowych, zawierających dane osobowe istnienie dokumentu określającego politykę bezpieczeństwa zostało narzucone rozporządzeniem Ministra Spraw Wewnętrznych

[50] „Elementarz bezpieczeństwa systemów teleinformatycznych" – op. cit.

i Administracji[51]. Wiele źródeł mówi o formie tego dokumentu, m.in. zajął się tym zagadnieniem Polski Komitet Normalizacji ustanawiając normę PN-I-13335[52], w której zapisano, że polityka bezpieczeństwa to „zasady, zarządzania i procedury, które określają jak zasoby - włącznie z informacjami wrażliwymi- są zarządzane, chronione i dystrybuowane w instytucji i jej systemach informatycznych".

Opracowaniem polityki bezpieczeństwa powinny zajmować się osoby odpowiedzialne za bezpieczeństwo informacji i administratorzy danej sieci komputerowej, natomiast zatwierdzić ją powinno kierownictwo organizacji, tym samym wprowadzając ją w życie.

Polityka bezpieczeństwa, jako dokument powinna być znana wszystkim użytkownikom sieci komputerowej, której dotyczy. Każdy nowy użytkownik powinien mieć obowiązek zapoznania się z nią. W związku z tym ważne jest, aby dokument był napisany językiem prostym, zrozumiałym nawet dla tych użytkowników, którzy nie mieli wcześniej kontaktu zagadnieniami tego typu.

Dokument ten powinien obejmować całokształt działań i zachowań mających na celu zapewnienie jak najwyższego poziomu bezpieczeństwa sieci wraz z informacją w niej zawartą.

Autorzy Molski i Opala[53] podają następujące charakterystyczne elementy polityki bezpieczeństwa:

- określenie osób odpowiedzialnych za bezpieczeństwo systemu; określenie osób administrujących systemem (o ile nie jest to ta sama osoba),
- określenie celu tworzenia i zabezpieczania sieci; rodzaju dozwolonych operacji (poczta, strony www, współużytkowanie baz danych, itp.); rodzaj informacji znajdujących się w niej,
- określenie, kto może mieć konto w systemie; czy mogą istnieć konta typu „gość", na jakich kontach mogą pracować serwisanci firm które dostarczyły oprogramowanie,
- określenie, czy wiele osób może korzystać z jednego konta (na przykład przedstawiciele firm serwisujących oprogramowanie),
- określenie, w jakich sytuacjach odbierane jest prawo do korzystania z konta; co dzieje się z kontami użytkowników czasowo bądź na stałe odsuniętych od użytkowania systemu,

---

[51] Rozporządzenie MSWiA z dnia 3.06.1998 r. w sprawie określenia podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy służące do przetwarzania danych osobowych.
[52] PN-I-13335-1 *„IT security policy"*
[53] „Elementarz bezpieczeństwa systemów informatycznych" – op. cit.

- zdefiniowanie wymagań dotyczących haseł; na ile powinny być zawikłane; określenie okresu ich ważności i czy mogą się powtarzać,
- określenie metod sporządzania i przechowywania wydruków informacji zawartych w sieci,
- określenie warunków dostępu osób trzecich do sieci,
- określenie metod ochrony przed wirusami,
- sposób serwisowania urządzeń sieci; firmy prowadzące serwis; sposób zgłaszania usterek,
- postępowanie w przypadkach zagrożenia bezpieczeństwa informacji (rozpatrzenie jak największej liczy zagrożeń).

Wymienione elementy są tylko propozycjami, ponieważ dokument ten powinien być dostosowany do realiów każdej organizacji.

Bardzo ważne jest aby osoba odpowiedzialna za bezpieczeństwo na bieżąco dokonywała aktualizacji polityki bezpieczeństwa, dbając jednocześnie o to aby wszyscy użytkownicy byli na bieżąco ze stanem faktycznym.

5. BEZPIECZEŃSTWO I OCHRONA INFORMACJI W SIECIACH TELEKOMUNIKACYJNYCH

ppłk mgr inż. Grzegorz ŚWIDZIKOWSKI

Ludzkość od początku swojej egzystencji w codziennym funkcjonowaniu opierała i opiera się na przekazywaniu i odbiorze danych z otaczającej ją rzeczywistości. Sposób wymiany jak i sam obieg informacji jest systematycznie udoskonalany przez kolejne generacje społeczności ludzkiej. Współcześnie jednym z jej podstawowych elementów są nowoczesne systemy telekomunikacyjne, które zapewniają zarówno przekaz jak i odbiór informacji (danych) w skali globalnej. W dużej mierze możliwość dostępu do różnego rodzaju usług telekomunikacyjnych w dowolnym zakątku świata jest zasługą nowoczesnych urządzeń łączności sprzęgniętych w jeden system ze środkami informatycznymi. Dzięki temu, między innymi, uzyskano poprawę jakości oraz możliwość wiernej i szybkiej transmisji danych.

Przebudowywane narodowe siły zbrojne poza wdrażaniem nowych systemów uzbrojenia i sprzętu bojowego wprowadzają również nowoczesne systemy dowodzenia i kierowania środkami walki, które stanowią istotny element podniesienia walorów bojowych pododdziałów i oddziałów wojsk własnych.

Jednak powinniśmy zdawać sobie sprawę, że we współczesnym świecie informacja jest i staje się coraz bardziej zasobem strategicznym i to nie tylko ta, która niesie w sobie istotne treści, jest dostarczana terminowo, do właściwego adresata, w formie nienaruszonej (nie modyfikowana) i niezawodnie - po prostu bezpiecznie. Z tym strategicznym charakterem informacji zaczynają się oswajać państwa i różne narodowe oraz ekonomiczne instytucje. Można przy tym zauważyć, że obecnie ciężar gatunkowy ochrony i bezpieczeństwa informacji, który dominował do niedawna w sektorze polityczno – militarnym systematycznie przesuwa się i zmierza do sektora gospodarczego.

Dające się zauważyć wzrastające zapotrzebowanie na informację jest przyczyną stosowania coraz to nowszych i efektywniejszych metod oraz środków, które przyjmują formę całych systemów wykorzystujących do pozyskania informacji najnowsze zdobycze elektroniki. Jednak daleko posunięty proces automatyzacji środków rozpoznania nie wyeliminował i prawdopodobnie nie wyeliminuje tradycyjnego agenturalnego sposobu zdobywania informacji.

Jednak poziom wiedzy oraz świadomość w sektorze ekonomicznym nie idzie w parze z ciągle zwiększającym problemem bezpieczeństwa i rosnącymi zagrożeniami w zakresie ochrony informacji „wrażliwej" – z punktu widzenia ekonomicznego oraz prawnie chronionej, która ma wpływ na ogólnie rozumiane pojęcie bezpieczeństwa państwowego i narodowego.

Sytuacja ta może ulec znaczącej poprawie tylko i wyłącznie wówczas, gdy osoby odpowiedzialne za ochronę informacji oraz organizację i bezpieczne funkcjonowanie systemów telekomunikacyjnych będą zdawały sobie w pełni sprawę z faktu na jakie zagrożenia narażona jest informacja od momentu jej wytworzenia (powstania) do momentu utraty przez nią materialnego znaczenia oraz jakie następstwa niesie ze sobą utrata informacji lub utrata jej poufności.

Stąd też celowym jest zastanowienie się nad samą istotą bezpieczeństwa informacji oraz następstwem celowego bądź przypadkowego jej ujawnienia.

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

W pierwszej z wymienionych płaszczyzn w wojskowych systemach telekomunikacyjnych ochronie powinny podlegać te informacje, które w rozumieniu ustawy z dnia 22.01.1999r. „ 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. Cytując dalej za ww. ustawą **tajemnicą służbową** jest 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 nowoczesnemu systemowi telekomunikacyjnemu w zakresie ochrony przesyłanej w nim 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 systemu telekomunikacyjnego, który nie zapewniając spełnienia choćby jednego z tak określonych wymagań w okresie pokoju może zawieść i raczej 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 wojskowego systemu telekomunikacyjnego 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, która winna uwzględniać wszelkie możliwe warunki eksploatacji tego systemu począwszy od okresu pokoju aż do warunków ekstremalnych – wojny i prowadzenia działań bojowych.

5.1. Podział i charakterystyka zagrożeń bezpieczeństwa informacji w wojskowych sieciach telekomunikacyjnych

W literaturze przedmiotu 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 środkach telekomunikacyjnych (transmisyjnych, komutacyjnych) czy samych urządzeń końcowych. Przy drugim z wymienionych podziałów, choć trudno takowe spotkać, gdyż informacje te jakie czynniki i jakie zagrożenia zostały uwzględnione w procesie organizacji systemu ochrony są zazwyczaj niejawne, nie ma i raczej nie może być jednomyślności. Wynika to bowiem i zależy od przyjętych przez organizatora danego systemu lub sieci warunków brzegowych oraz przyjętego kryterium oceny możliwości wystąpienia pojedynczego lub grupy zagrożeń.

Warto w tym miejscu zastanowić się jakie elementy współczesnego wojskowego systemu lub sieci telekomunikacyjnej mogą stanowić potencjalne źródło ujawnienia informacji. Z analizy literatury i przede wszystkim dokumentów normatywnych 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 Bezpieczeństwa 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.

Zagrożenia fizyczne, w kontekście podziału zagrożeń przedstawionego 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. Profesorowie, autorzy powyższej publikacji wyodrębnili dwie grupy zagrożeń:

- sabotaż i zagrożenia nieumyślne;
- infiltracja.

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

- pożarów i innych klęsk żywiołowych;
- awarii zasilania (systemu energetycznego);
- dezintegracja lub „destrukcja informatyczna" (wirusy, bomby logiczne, konie trojańskie, itp.)
- fizyczne czynniki destrukcyjne i swoiste oddziaływanie ludzi.

Za główną przyczynę tego rodzaju powstałych 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 lub innego państwa – to działanie takie nazywamy dywersją.

W przeciwieństwie do sabotażu **infiltracja** to takie działanie osób nieupoważnionych, które ma na celu dążenie do zapewnienie sobie dostępu lub pozyskanie informacji znajdującej się w zasobach danego systemu telekomunikacyjnego lub informatycznego. Infiltracja reali-

zowana 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** przeciwnik bezpośrednio zagraża danym. Mianowicie zagraża 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.

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 i 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 (Elektroniczną 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 prowadzą do mody, 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")**.

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 dla bezpieczeństwa narodowego Stanów Zjednoczonych.

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 jest możliwe przechwycenie informacji nawet z odległości ponad kilometra. W przypadku fal powierzchniowych oraz pól indukowanych w kablach zasilających odległości te wynoszą ok. 100 - 150 m.

Podziału zagrożeń dla bezpieczeństwa informacji w systemie telekomunikacyjnym czy informatycznym jak już wcześniej wspomniano można dokonywać w wielu aspektach i płaszczyznach. Jedną z nich stanowić zatem może, na zasadzie „lustrzanego odbicia", podział odpowiadający obszarom stosowanych w praktyce środków oraz przedsięwzięć organizacyjno-technicznych i eksploatacyjnych w zakresie zapewnienia bezpieczeństwa informacji w systemie telekomunikacyjnym. W problematyce tego tematu zarówno w środowisku cywilnym jak i wojskowym doktrynalnie przyjmuje się następujące grupy przedsięwzięć zapewniających ochronę systemu jako całości lub wybranych jego elementów oraz samej informacji:

- organizacyjno-proceduralne;
- personalne;
- fizyczne;
- techniczne.

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 podejmę próbę 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 kierow-

nictwa 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 powinna obejmować takie działy jak:

- 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, nie wiedzą 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 telekomunika-

cyjnego 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 gdy nie posiadają 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 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);
- inne systemy elektromagnetyczne.

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

- 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 dla celów wywiadowczych lub oszukania przeciwnika poprzez "spoofing" lub podszywanie się pod użytkownika systemu.

Poprzez „spoofing" należy rozumieć przejęcie, zamiana i retransmisja sygnału celem 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 urządzenia 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. Nie wdrożenie 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.

5.2. Gradacja zagrożeń bezpieczeństwa informacji w wojskowych sieciach telekomunikacyjnych

Posiadając tak usystematyzowaną wiedzę w zakresie podziału i charakterystyki najważniejszych zagrożeń dla bezpieczeństwa informacji w sieci telekomunikacyjnej można spróbować dokonać oceny, które z nich są najistotniejsze i 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" i zdarzeń związanych z nieautoryzowanym ujawnieniem informacji jest skrzętnie skrywana przez różne organizacje, w których fakt ten miał miejsce. Nie podawanie do publicznej wiadomości omawianych zdarzeń w sektorze gospodarczym związany jest przede wszystkim z zachowaniem dobrego wizerunku danej firmy bądź instytucji na rynku globalnym, która mogłaby przez takowe ujawnienie stać się niewiarygodną dla potencjalnych kontrahentów i w efekcie końcowym pośrednio przyczynić nawet do jej upadku. 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.

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

fikowanych dla systemu stacjonarnego uwzględnia również oddziaływanie ogniowe i radioelektroniczne przeciwnika.

Poszukując źródeł informacji, która pozwalałaby przeprowadzić taka analizę można dokonać przeglądu dokumentacji wybranych ćwiczeń, treningów sztabowych szczebla brygadowego i dywizyjnego, 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 rozwiązania pozostaje jeszcze jeden problem - forma i metoda uzyskania danych od miarę licznego bo kilkudziesięcioosobowego grona specjalistów bez intencjonalnego wchodzenia w tę sferę informacji, które zastrzeżone są i do korzystania tylko w pewnym kręgu osób funkcyjnych na zasadzie tzw. wiedzy koniecznej. Najlepszą metodą w tej sytuacji jest anonimowe badanie ankietowe, które nie będzie jednocześnie ograniczać się do konkretnego systemu funkcjonującego w określonym czasie i przestrzeni.

W celu uwiarygodnienia uzyskanych wyników w stosunku do respondentów narzucono pewne ograniczenia, które pozwoliły na uzyskanie jak najbardziej zbliżonych do rzeczywistości ocen 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
- brał udział i posiada doświadczenia z ćwiczeń lub treningów sztabowych z udziałem wojsk - minimum 2-krotnie.

W ankiecie sformułowano tylko jedno pytanie, które przyjęło brzmienie:

Jakie jest prawdopodobieństwo wystąpienia zagrożenia ujawnienia lub utraty bezpieczeństwa informacji w polowym systemie telekomunikacyjnym związku taktycznego w kontekście implementowanych organizacyjno-technicznych i eksploatacyjnych środków ochrony informacji?

Badaniu ankietowemu poddano około 70% ogółu pracowników pionu bezpieczeństwa łączności i informatyki wojsk lądowych, ale po uwzględnieniu nałożonych na wstępie ograniczeń wyniki opracowano w oparciu o odpowiedzi udzielone przez 41 ankietowanych.

Przy tak zadanym respondentom pytaniu ankieta przyjęła kształt i formę przedstawioną w tabeli 5.2.1, gdzie w poszczególnych płaszczyznach zidentyfikowano zagrożenia szczegółowe przydzielając jednocześnie pięciostopniową skalę możliwości ich zaistnienia w systemie telekomunikacyjnym – począwszy od bardzo mało prawdopodobnych (bliskie zeru) aż po niemal pewne (bliskie jedności).

Tabela 5.2.1.

Struktura i kształt ankiety

Zagrożenia dla bezpieczeństwa informacji	**Stopień prawdopodobieństwa wystąpienia zagrożenia**				
	Bliskie jedności	**Duże**	**Średnie**	**Małe**	**Bliskie zeru**
Typ (rodzaj) zagrożenia					
- pochodzenie zagrożenia					

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 jak i zasobów informacyjnych systemu.

Respondenci ogólnie ocenili na poziomie średnim (tabela 5.2.2) zdarzenia pochodzące ze strony człowieka nazwane w kwestionariuszu ankiety zagrożeniami personalnymi (średnia arytmetyczna - 28,57%).

Tabela 5.2.2.

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**

Drugą płaszczyzną poddaną ocenie pracowników organów bezpieczeństwa łączności i informatyki były zagrożenia fizyczne, wśród których wyodrębniono:

- źle zorganizowaną 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.

W tym przypadku tylko 30 % respondentów stwierdziło, że tego typu zagrożenie wpływa średnio na możliwość wystąpienia zagrożenia fizycznego, a jako zagrożenie duże uważało tylko 27,15 % respondentów (tabela 5.2.3.).

Tabela 5.2.3.

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**

Kolejny obszar zagrożeń poddany osądowi respondentów to płaszczyzna organizacyjno-proceduralna wśród której wyróżniono 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.

Odpowiedzi na pierwsze trzy wymienione zagrożenia (tabela 5.2.4.) oscylują na zbliżonym do siebie poziomie – blisko 50% - co pozwala stwierdzić, że zagrożenia w płaszczyźnie organizacyjno-proceduralnej mają duży, istotny wpływ na bezpieczeństwo informacji w wojskowym polowym systemie telekomunikacyjnym.

Tabela 5.2.4.

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**

Kolejny obszar zagrożeń rozpatrywany przez respondentów w ankiecie to zagrożenia techniczne w ramach, których 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.

Jako pierwsze ocenie poddane były zagrożenia związane ochroną kryptograficzną.

Najistotniejszym elementem, jak widać z uzyskanych w procesie badań wyników w tym obszarze (tabela 5.2.5.), są zagrożenia związane z ochroną środków i materiałów kryptograficznych – od momentu ich wytworzenia, aż do fizycznego zniszczenia po wycofaniu z eksploatacji.

Tabela 5.2.5.

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

Zapewnienie bowiem hermetycznie zamkniętego ich obiegu, a także ograniczenie dostępności do niezbędnego minimum stanowi o bezpieczeństwie nie tylko samej informacji ale i całego systemu.

Drugą płaszczyzna składową zagrożeń znajdujących się w obszarze technicznym stanowi emisja ujawniająca. W jej ramach do zagrożeń szczegółowych szczególnie można zaliczyć (tabela 5.2.6.):

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

Tabela 5.2.6.

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**

W tym przypadku zauważyć można rozłożenie się opinii pomiędzy dużym a średnim poziomem zagrożenia, choć zdaniem wielu specjalistów 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 obiektów Sztabu Generalnego ich dyslokacji, gdzie w gruncie rzeczy brak jest fizycznych możliwości zapewnienia stref bezpieczeństwa o niższych niż maksymalne rygorach.

Kolejną rozpatrywaną w obszarze technicznym płaszczyzną są zagrożenia programowe (tabela 5.2.7), które w pierwszej chwili kojarzą się 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 minikomputerem, w którym prawidłowo funkcjonujące oprogramowanie stanowi o niezakłóconym działaniu tej 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);
- nie szyfrowanie informacji na nośnikach elektronicznych;
- słabe zabezpieczenia przed oprogramowaniem złośliwym;
- błędy użytkowników (celowe i niecelowe);
- błędy personelu technicznego (celowe i niecelowe).

Tabela 5.2.7.

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**

Jak dotychczas po raz pierwszy tak znaczna liczba respondentów - 60% stwierdziła jednomyślnie, że najważniejszym zagrożeniem w tej płaszczyźnie jest łatwość dostępu do zasobów informacyjnych systemu, czyli innymi słowy do urządzeń końcowych zapewniających wymianę informacji w trybie niejawnym. Problem ten nie istnieje samodzielnie bez systemu nadawania uprawnień poszczególnym osobom funkcyjnym będącym jednocześnie 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 jest brak lub słabość zabezpieczeń przed implementacją tzw. oprogramowania złośliwego. Pod pojęciem należy rozumieć wirusy, robaki, bomby logiczne, konie trojańskie, itd.

Ze względu na ogólną znajomość tego zagadnienia, któremu poświęca się dużo uwagi w literaturze przedmiotu nie będzie on dalej rozwijany. Kolejnym zagrożeniem, na które zwrócili uwagę respondenci to brak stosownych zabezpieczeń uniemożliwiających wprowadzanie nieautoryzowanych (nieuprawnionych) zmian w treści przekazywanych informacji lub oprogramowaniu systemowym pozwalającym nawet na zmianę konfiguracji systemu.

Jako kolejne zagrożenia w obszarze technicznym poddane pod rozwagę respondentów zostały zagrożenia związane z procesem przesyłania informacji zwane inaczej zagrożeniami wpływającymi na bezpieczeństwo transmisji sygnału użytecznego. W płaszczyźnie tej do zagrożeń szczegółowych (tabela 5.2.8.) 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, gdzie można wyróżnić 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.;
- podszywanie się np.: jako użytkownicy celem pozyskania informacji lub ewentualnego wprowadzenia w błąd (dezinformacja).

Tabela 5.2.8.

Zagrożenia bezpieczeństwa informacji w obszarze transmisji sygnału

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**

Zagrożenia dla bezpieczeństwa informacji w procesie jej transmisji nabierają szczególnego znaczenia w mobilnych systemach telekomunikacyjnych ze względu, że informacja jest przesyłana przede wszystkim drogą radiową lub radioliniową. Jednak uzyskane wyniki nie zdają się tego stanowiska potwierdzać. Przeciętnie tylko około 1/3 respondentów uważa, że zagrożenia mogące wpływać na bezpieczeństwo informacji są poważne.

Ostatnim elementem w obszarze technicznym są zagrożenia wynikające z zastosowania lub braku urządzeń, systemów wsparcia technicznego (tabela 5.2.9.). W ramach tej płaszczyzny zagrożeń w badaniu ankietowym respondentom przedstawiono do wyboru niżej wymienione zagrożenia szczegółowe:

- 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 5.2.9.

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	<u>45,71</u>	14,29	2,86
- brak lub nieadekwatny system antywłamaniowy, ppoż.	2,86	17,14	28,57	<u>40,00</u>	5,71
- brak lub niewłaściwy system zasilania awaryjnego	8,57	22,86	<u>40,00</u>	28,57	5,71
- inne systemy zabezpieczające funkcjonowanie systemu telekomunikacyjnego	2,86	11,43	<u>42,86</u>	40,00	2,86

Jak wynika z przeprowadzonego badania ten element nie ma zasadniczego wpływu na poziom bezpieczeństwa informacji w polowym systemie telekomunikacyjnym – zagrożenia z tego wypływające mają małe lub średnie znaczenie w ocenie respondentów.

Podsumowując uzyskane wyniki badania ankietowego, nie można jednoznacznie powiedzieć o jednym, drugim, czy też kilku zagrożeniach, które w sposób ewidentny byłyby faworyzowane przez respondentów. Po ich uśrednieniu większość z uzyskanych odpowiedzi oscyluje na poziomie 30 – 40% (tabela 5.2.10.) przy uwzględnieniu stopnia prawdopodobieństwa jego wystąpienia na poziomie dużym lub średnim.

Tabela 5.2.10.

Uśrednione wyniki badania ankietowego w poszczególnych 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

Podstawowym wnioskiem, który nasuwa się po przeprowadzeniu wnikliwej analizy rezultatów przeprowadzonego badania ankietowego jest stwierdzenie, że nie ma zagrożeń dla bezpieczeństwa informacji w wojskowych systemach telekomunikacyjnych mniej lub bardziej istotnych. Następstwem ich pojawienia się i potencjalnego zlekceważenia przez personel techniczny lub stosowne osoby funkcyjne może przyczynić się do ujawnienia informacji dla zabezpieczenia, której zbudowany został cały system ochrony.

Nie mając jednak pełnego przekonania do tak sformułowanego stwierdzenia, poszukując dalej najczęściej pojawiającego się w wojskowych sieciach telekomunikacyjnych, z identycznym pytaniem zwrócono się do dwóch ekspertów - płk M. Sobczak oraz płk A. Dańczak, którzy tę tezę mogliby potwierdzić.

Obaj w/w eksperci potwierdzili, że czynnikami determinującymi poziom zagrożeń czy nawet możliwość ich wystąpienia jest 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 jest człowiek. Dopiero bezpośrednio po nim jako kolejne należy rozpatrywać wszelkiego rodzaju zagrożenia wchodzące w skład szeroko rozumianych zagrożeń technicznych, które wcześniej zostały omówione.

Słowa cytowanych wyżej ekspertów zdają się potwierdzać badania prowadzone przez przedstawicieli amerykańskiego świata nauki. Fakt, że badania te dotyczą raczej systemów komercyjnych i zdarzeń o podłożu kryminalnym, jednak nie zmienia to znaczenia w zasadniczej kwestii – ujawnienia informacji i powstania problemów w systemach telekomunikacyjnych lub informatycznych stwarza nieuczciwy bądź niezadowolony personel. Opierając się na swoich badaniach panowie Icove D., Seger K., von Storch opracowali i przedstawili w „A Crimefighter Handbook" (wydawnictwo O'Reilly&Associates, 1991) przykładową statystykę (rys. 5.2.1.) zagrożeń, w której około 75% problemów i zagrożeń stanowi właśnie człowiek.

Rys.5.2.1. Statystyka zagrożeń wg poglądów Icove D., Seger K., von Storch.

5.3. Metody i środki ochrony informacji w 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 stworzenie planu całkowitej ochrony; ma zapewnić stopień bezpieczeństwa proporcjonalny do wagi chronionej informacji.

Do elementów analizy ryzyka należą:

- zagrożenia, częstość zagrożeń;
- cele;
- 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 nam 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 nam 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 funkcjonować. Wymienione czynniki mają podstawowe znaczenie przy doborze metod i środków ochrony informacji, co jednak nie oznacza, że w indywidualnych przypadkach nie jest wskazanym 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.

Podstawą dla personelu bezpieczeństwa łączności i informatyki umożliwiającą określenie uprawnień dla poszczególnych użytkowników w zakresie dostępu do niejawnych zasobów informacyjnych systemu telekomunikacyjnego bądź informatycznego jest rozkaz dzienny dowódcy lub kierownika jednostki organizacyjnej, w którym określony jest zakres wiedzy koniecznej (*ang. need to know*) dla danego stanowiska służbowego oraz maksymalna klauzula 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.

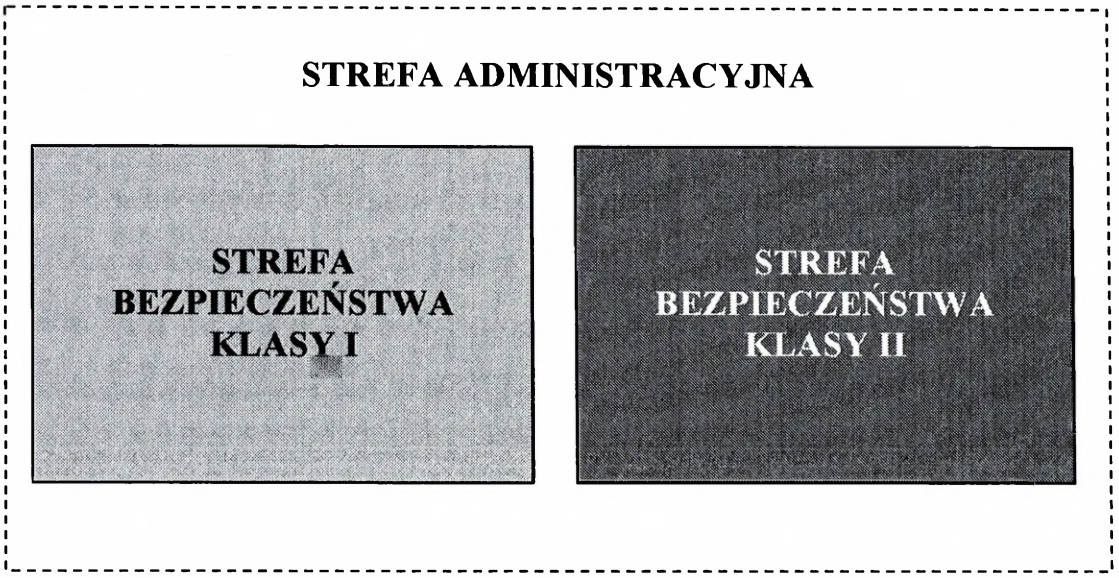
Jako strefę bezpieczeństwa należy traktować obszar, obiekt, fragment budynku, jedno lub kilka pomieszczeń, posiadające ściśle określone, oznaczone i strzeżone granice, w których przechowywane, przetwarzane lub wytwarzane są informacje niejawne o klauzuli „Poufne"

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:

1. Strefa bezpieczeństwa klasy I – obszar, w którym przetwarzane i przechowywane informacje niejawne o klauzuli „Poufne" lub wyższej w taki sposób, że wejście do tego obszaru praktycznie oznacza dostęp do tych informacji.
2. Strefa bezpieczeństwa klasy II – obszar, w którym wytwarzane, przetwarzane i przechowywane 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 5.3.1.



Rys. 5.3.1. Przykładowe rozmieszczenie stref bezpieczeństwa

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 niejaw-

nych 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 zobowiązani są do posiadania poświadczenia bezpieczeństwa osobowego upoważniające 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 systemie 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 informacjami, które może wykorzystać w celu naruszenia zabezpieczenia systemu telekomunikacyjnego, to należy zmi-

nimalizować 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:

- 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;
- całkowite zrozumienie 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 różnych uwarunkowań (np. struktura budynku lub kontenera na pojeździe) oraz przeznaczenia i zadań systemu.

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 i zapewniają tym samym 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. Wskazanym 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 Traktatu Północnoatlantyckiego zawartą w dokumencie CM - (55)15 (Final) – „Bezpieczeństwo w ramach Organizacji Traktatu 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 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 w zależności od klauzuli zabezpieczanych informacji muszą spełniać różne kryteria.

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 kopercie 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 (średnica) 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 funkcjonujących, wdrażanych lub planowanych do wdrożenia systemów telekomunikacyjnych i informatycznych w siłach zbrojnych w zakresie zasad instalacji urządzeń technicznych oraz sprzętu łączności i informatyki

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, które może wpływać na:

- bezpieczeństwo kryptograficzne;
- ochrona elektromagnetyczna;
- ochrona programowa;
- ochrona transmisji informacji;
- techniczne wsparcie ochrony fizycznej.

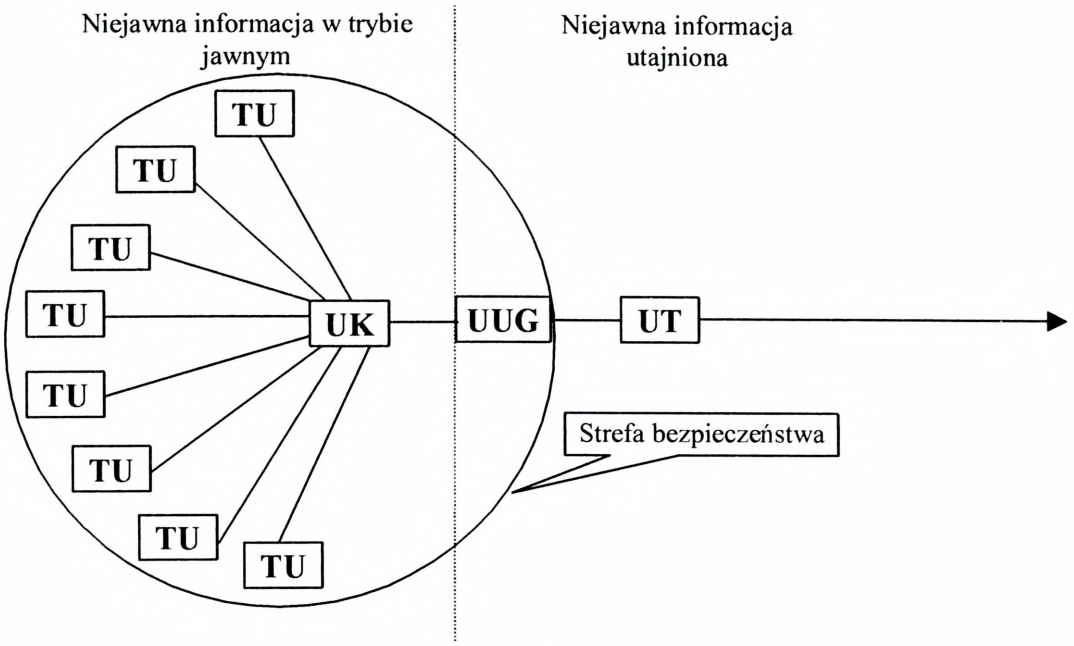
Każdy wojskowy system telekomunikacyjny lub informatyczny, w którym wytwarza, przetwarza, przechowuje i przede wszystkim przysyła się informacje niejawne stanowiące tajemnicę państwową lub służbową wykorzystuje do ochrony zasobów informacyjnych urządzenia ochrony kryptograficznej.

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 5.3.2, 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 w strefie lub poza nią. Z punktu widzenia bezpieczeństwa dla już utajnionej informacji nie ma to większego znaczenia.



TU – terminal użytkownika
UK – urządzenie komutacyjne
UUG – urządzenie utajniania grupowego
UT – urządzenie transmisyjne

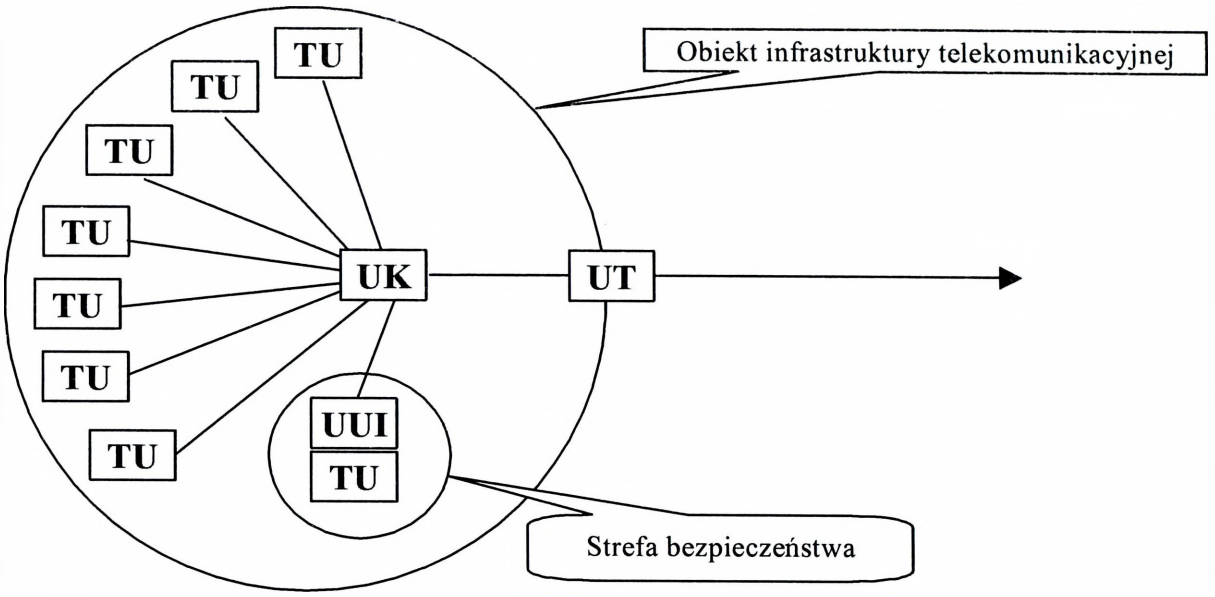
Rys.5.3.2. Przykład utajniania grupowego

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 5.3.3.) 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.



TU – terminal użytkownika
UK – urządzenie komutacyjne
UUI – urządzenie utajniania indywidualnego
UT – urządzenie transmisyjne

Rys. 5.3.3. Przykład utajniania indywidualnego

Główny 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.

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 przewod-

nik, 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.

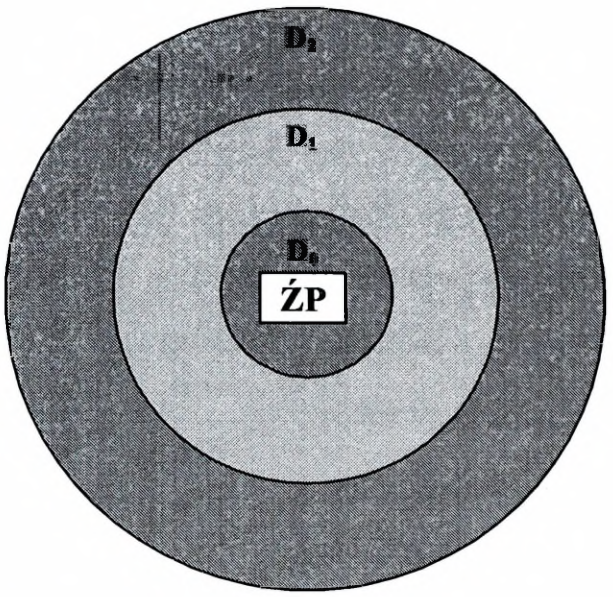
Możliwości modyfikowania urządzeń przez zwykłego użytkownika systemu telekomunikacyjnego lub informatycznego są bardzo ograniczone z uwagi na brak specjalistycznej aparatury oraz groźbę utraty gwarancji producenta na posiadany sprzęt.

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 lub telekomunikacyjnych pracujących w pobliżu. 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 przeprowadzonego 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 5.3.4.



ŹP – źródło promieniowania
D_0 ,D_1 ,D_2 – granica strefy

Rys. 5.3.4. Przykładowe zasady wyznaczania strefy

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. Prowadząc analizę 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 Organizacji Traktatu Północnoatlantyckiego **bezpieczeństwo transmisji** informacji (*ang. transmission security – TRANSEC*) jest tym komponentem bezpieczeństwa łączności i informatyki, w którym stosuje się wszystkie rodzaje środków ochrony za 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 nie spełnieniu 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 ewentualne ujawnienie 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. i 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 możliwość dokonania jej modyfikacji lub powtórzenia transmisji celem 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;
- instalacja dodatkowych bezpieczników przepięciowych dla sprzętu łączności i informatyki;
- zakup stabilizatorów i zasilaczy awaryjnych (UPS);
- instalację czujników wykrywających wodę w pomieszczeniach;

– instalacja 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 są 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.

5.4. Struktura organizacyjna wojskowych organów bezpieczeństwa łączności i informatyki

Każda organizacja lub instytucja, w której zasobach znajdują się informacje prawnie chroniona (tajemnica państwowa, służbowa) lub informacje podlegające ochronie zgodnie z przyjętymi założeniami organizacyjnymi (tajemnica związana z działalnością gospodarczą firmy, technologia wytwarzania produktu, itp.) w przypadku rozbudowanego systemu informacyjnego wykorzystującego środki techniczne do przesyłania informacji na odległość (telekomunikacja) winna w swoich strukturach organizacyjnych posiadać organy odpowiedzialne za organizację oraz administrowanie bezpieczeństwem własnych lub otrzymanych informacji.

W przypadku informacji niejawnych, które stanowią w świetle aktualnie obowiązującej ustawy „O ochronie informacji niejawnych" tajemnicę państwową i służbową wymóg ten jest obligatoryjny. W myśl ustawy organizacje (instytucje) przetwarzające, przechowujące lub przesyłające informacje (bez względu na ich formę – dokumenty papierowe, nośniki elektroniczne) opatrzone klauzulami: ściśle tajne, tajne, poufne, zastrzeżone zobligowane są do powołania osoby pełniącej funkcję „pełnomocnika ochrony informacji niejawnych". W zależności od wielkości danej jednostki organizacyjnej i ilości klasyfikowanych zasobów informacyjnych stanowisko to może być jednoosobowe lub powołuje się „pion ochrony informacji niejawnych", na czele którego znajduje się pełnomocnik.

W tej strukturze organizacyjnej (jeśli nie występuje oddzielnie) znajduje się personel odpowiedzialny za prawidłowe i bezpieczne funkcjonowanie systemów telekomunikacyjnych (informatycznych). Do obowiązków tego personelu należy wdrażanie i bieżący merytoryczny nadzór nad procedurami i technicznymi środkami ochrony informacji w systemie telekomunikacyjnym, których realizacja wynika z przyjętych w polityce bezpieczeństwa założeń.

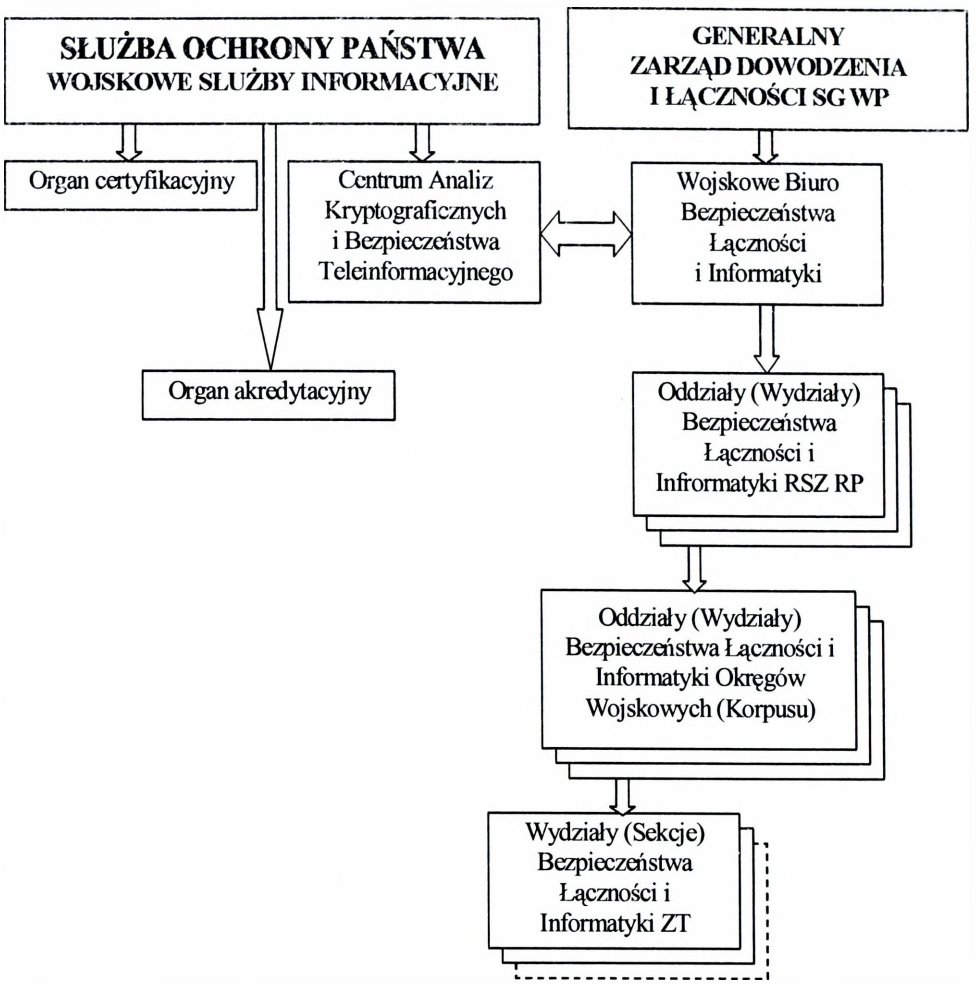
W jednostkach organizacyjnych lub instytucjach, w których nie przetwarza się informacji prawnie chronionych, decyzje w zakresie powołania personelu bezpieczeństwa systemu telekomunikacyjnego lub informatycznego podejmuje kierownictwo w zależności od charakteru prowadzonej działalności lub przyjętej strategii w dziedzinie bezpieczeństwa i ochrony informacji.

Siły Zbrojne Rzeczypospolitej Polskiej są organem realizującym politykę bezpieczeństwa w sferze obronności państwa. Obronny charakter doktryny narodowej nie zmienia faktu, że realizowane przez resort obrony narodowej przedsięwzięcia w wielu dziedzinach funkcjonowania armii mają charakter niejawny. Z tej też przyczyny, praktycznie w każdym wojskowym systemie telekomunikacyjnym czy informatycznym realizowana jest wymiana informacji objętych tajemnicą państwową lub służbową.

Organ taki jak siły zbrojne ustawowo w swoich strukturach organizacyjnych musi posiadać komórki odpowiedzialne za organizację i administrowanie bezpieczeństwem informacji. Strukturę organizacyjną organów bezpieczeństwa informacji w wojskowych systemach telekomunikacyjnych i informatycznych przedstawia rysunek 5.4.1.

Ze względu na różnorodność w resorcie obrony narodowej systemów zapewniających obieg klasyfikowanej informacji za pomocą środków technicznych łączności i informatyki, oprócz pionu pełnomocnika ochrony, powołano samodzielne komórki organizacyjne, których zadaniem jest planowanie, wdrażanie oraz nadzór nad bezpieczną eksploatacją systemów informatycznych i telekomunikacyjnych.

Dla resortu obrony narodowej naczelnym organem odpowiedzialnym za realizację przedsięwzięć i polityki w zakresie bezpieczeństwa informacji, w myśl ustawy „O ochronie informacji niejawnych", jest krajowa władza bezpieczeństwa (KWB), którą pełnią Wojskowe Służby Informacyjne.



Rys. 5.4.1. Struktura organizacyjna organów bezpieczeństwa informacji w wojskowych systemach telekomunikacyjnych i informatycznych

W ramach działalności służbowej wyspecjalizowany organ KWB udziela akredytacji, czyli innymi słowy wydaje zezwolenia na wdrożenie i eksploatację systemu telekomunikacyjnego lub informatycznego, w którym wytwarzane, przetwarzane, przechowywane lub przesyłane są informacje niejawne na potrzeby armii. Pełni on zarazem funkcje kontrolne w stosunku do systemów telekomunikacyjnych lub informatycznych, które taką akredytację uprzednio uzyskały – audyt.

Głównym zadaniem organu certyfikacyjnego jest badanie i ocena środków oraz narzędzi zapewniających wymagany poziom bezpieczeństwa informacji w wojskowych systemach telekomunikacyjnych i informatycznych. Uzyskanie od tego organu certyfikatu na zgłoszone przez różne podmioty gospodarcze urządzenia lub narzędzia jest równoznaczne z możliwością ich zastosowania jako środka ochrony bezpieczeństwa informacji – a tylko takie środki i narzędzia można implementować do bezpiecznych systemów telekomunikacyjnych i informatycznych eksploatowanych w resorcie obrony narodowej. Uzyskanie opinii negatywnej jest

automatycznym wykluczeniem danego produktu lub narzędzia z możliwości jego zastosowania w niejawnych wojskowych systemach łączności i informatyki.

Natomiast Centrum Analiz Kryptograficznych i Bezpieczeństwa Teleinformacyjnego jest tym organem krajowej władzy bezpieczeństwa, który kreuje w oparciu o akty normatywne politykę bezpieczeństwa w wojskowych systemach telekomunikacyjnych i informatycznych. Utrzymuje ponadto stałą i ścisłą kontrolę nad ilością i wykorzystaniem środków i narzędzi ochrony kryptograficznej oraz zabezpiecza je w materiały eksploatacyjne zapewniające ich prawidłowe funkcjonowanie w systemach telekomunikacyjnych oraz informatycznych funkcjonujących na potrzeby sił zbrojnych i w relacjach sojuszniczych.

Drugim filarem zapewniającym bezpieczeństwo informacji w wojskowych systemach telekomunikacyjnych są struktury organizacyjne wspierające bezpośrednio organy łączności i informatyki poszczególnych szczebli dowodzenia.

Na szczeblu centralnym w strukturach Generalnego Zarządu Dowodzenia i Łączności SG WP funkcjonuje Wojskowe Biuro Bezpieczeństwa Łączności i Informatyki. Biuro sprawuje merytoryczny nadzór nad eksploatowanymi w resorcie obrony narodowej systemami telekomunikacyjnymi i informatycznymi, w których wytwarzane, przetwarzane, przechowywane lub przesyłane są informacje niejawne. Opracowuje i wdraża dyrektywy oraz zalecenia operacyjnego wykorzystania środków ochrony informacji w wojskowych systemach telekomunikacyjnych i informatycznych. Uczestniczy ponadto w procesie planowania oraz wdrażania nowych systemów telekomunikacyjnych oraz informatycznych w aspekcie ochrony informacji.

Na szczeblu dowództw poszczególnych rodzajów sił zbrojnych za ochronę informacji przekazywanych przy użyciu technicznych środków łączności i informatyki odpowiedzialne są oddziały lub wydziały bezpieczeństwa łączności i informatyki, których zasadniczym zadaniem jest merytoryczny nadzór nad prawidłową implementacją i funkcjonowaniem środków ochrony informacji w systemach telekomunikacyjnych oraz informatycznych zabezpieczających proces dowodzenia (wymiany danych) i kierowania środkami walki w samym dowództwie oraz w podległych związkach operacyjnych i taktycznych. Zadania te realizowane są zarówno w stosunku do systemów pracujących w okresie pokoju, kryzysu czy też wojny. Pełnią one jednocześnie funkcje kontrolne w stosunku do podległych jednostek organizacyjnych.

W związkach operacyjnych i taktycznych poszczególnych rodzajów sił zbrojnych za bezpieczeństwo informacji w systemach telekomunikacyjnych i informatycznych odpowiadają wydziały lub sekcje bezpieczeństwa łączności i informatyki. Ich zasadniczym zadaniem jest zabezpieczenie prawidłowego funkcjonowania środków i narzędzi ochrony informacji

w rozwiniętych stacjonarnych lub rozwijanych polowych systemach telekomunikacyjnych i informatycznych wspomagających proces dowodzenia danego szczebla organizacyjnego.

Jednostki organizacyjne resortu obrony narodowej, w których bezpieczeństwo klasyfikowanej informacji realizowane jest przy użyciu technicznych środków ochrony kryptograficznej zobligowane są do powołania w swoich strukturach kancelarii kryptograficznych. Kierownik kancelarii (*ang. Crypto Custodian*) prowadzi na bieżąco ewidencję całego sprzętu ochrony kryptograficznej znajdującego się na wyposażeniu jednostki organizacyjnej oraz dokumentów kluczowych bądź szyfrowych, które zabezpieczają ich pracę w trybie niejawnym.

Merytoryczny nadzór nad pracą kierownika kancelarii sprawuje oficer bezpieczeństwa łączności (*ang. COMSEC officer – communication security officer*) danego szczebla organizacyjnego, który odpowiedzialny jest za prawidłowe funkcjonowanie oraz inspekcje środków oraz narzędzi ochrony informacji w eksploatowanych niejawnych systemach telekomunikacyjnych i informatycznych.

ZAKOŃCZENIE

płk dr hab. inż. Józef MICHNIAK

W obecnych czasach, kiedy mamy do czynienia z dynamicznym rozwojem technologii informatycznych większość organizacji w tym i wojsko, zmuszona jest do przedsięwzięcia odpowiednich kroków w celu zapewnienia bezpieczeństwa informacji znajdujących się w użytkowanych przez nią sieciach telekomunikacyjnych i komputerowych. Podyktowane może to być zarówno przepisami prawa jak i szeroko rozumianym dobrem organizacji.

Analiza zebranych materiałów i powyższych rozważań pozwala stwierdzić, iż w celu zapewnienia wymaganego poziomu bezpieczeństwa informacji w sieciach telekomunikacyjnych i komputerowych należy przedsięwziąć następujące kroki:

- określić oczekiwania (wymagania bezpieczeństwa) jakim ma sprostać przyszła sieć, określając m.in. akceptowalny poziom ryzyka,
- przeprowadzić analizę zagrożeń dla tak sformułowanych wymagań, w realiach organizacji,
- określić na podstawie analizy ryzyka szczegółowe wymagania bezpieczeństwa dla tworzonej sieci telekomunikacyjnej czy komputerowej, zawierające wytyczne z zakresu omówionych aspektów bezpieczeństwa,
- opracowanie i wdrożenie polityki bezpieczeństwa obejmującej całokształt przedsięwzięć związanych z bezpieczeństwem informacji w danej sieci telekomunikacyjnej czy komputerowej.

Wszystkie te przedsięwzięcia wymagają wsparcia ze strony organu zarządzającego organizacją, co związane jest z faktem kosztowności tego przedsięwzięcia.

Istotnym jest aby zdać sobie sprawę z jednej zasadniczej rzeczy mianowicie, że bezpieczeństwo nie jest stanem stałym. Raz osiągnięte nie pozostaje na zawsze. Zapewnianie bezpieczeństwa jest procesem ciągłym i wymaga nieustannej aktualizacji zarówno stanu wiedzy jak i metod zabezpieczenia.

Na zakończenie przytoczmy pewien bardzo znany slogan, który może być mottem dla osób odpowiedzialnych za szeroko rozumiane bezpieczeństwo:

„... najwyższym poziomem zaufania jest kontrola ...”

BIBLIOGRAFIA

1) Aloksa W., Karpiński C., Mencel A.: „Rola inżynierii kompatybilności elektromagnetycznej w procesie budowy systemów elektronicznych", WAT, Nr 1A.
2) Anderson R. H., Feldman P. M.: „Securing the U.S. Defense Information Infrastracture: A Proposed Approach", National Defense Research Institute, 1999.
3) Andrukiewicz E.: „Zarządzanie bezpieczeństwem systemu informatycznego, materiały szkoleniowe", 1999.
4) Bęczkowski J.: „Podstawowe zasady organizacji zabezpieczenia systemów teleinformatycznych", Materiały z seminarium CPiST Apexim S.A., 1999.
5) Boboli A.: „Bezpieczeństwo Systemów Informatycznych". Opracowanie Ministerstwa Sprawiedliwości, 1998.
6) Bryczkowski Maciej „Bezpieczeństwo systemów sieciowych, Postępy Kryminalistyki", Nr 1/97.
7) Bujnowski A., Mączyński A.: „Bezpieczeństwo w systemach komputerowych".
8) Dudek A.: „Nie tylko wirusy", Helion, 1998.
9) Gaj K. Kossowski R.: „Ochrona informacji w systemach informatycznych", CIT-COM-PW, 1993.
10) Gałach A.: „Ochrona baz danych", CITCOM-PW, 1998.
11) Goban-Klaus T., Sienkiewicz P.: „Społeczeństwo informacyjne: szanse, zagrożenia, wyzwania", Wydawnictwo Fundacji Postępu Telekomunikacji, 1999.
12) Hoffman L. J.: „Poufność w systemach informatycznych", 1982.
13) Icove D., Seger K. von Storch: „A Crimefighter Handbook, O'Reilly&Associates", 1999.
14) Jakubski J. K.: „Polityka zabezpieczenia informacji - potrzeba czy wymóg. II Krajowa Konferencja Zastosowań Kryptografii - Enigma'98", Warszawa 26-28.05.1998.
15) Jakubski K. J.: „Właściwe zabezpieczenie systemu informatycznego podstawą jego bezpieczeństwa", Materiały z seminarium, CPiST Apexim S.A., 1997.
16) Janczak J.; „Obrona informacyjna w działaniach obronnych związku operacyjnego", AON, 2002.
17) Janczak J.: „Obrona informacyjna w działaniach wojsk lądowych", AON, 2000.
18) Kifner T.: „Polityka bezpieczeństwa i ochrony informacji", Helion, 1999.

19) Klandel L.: „Haker Proof", Mikom, 1998.
20) Kwećka R.: „Informacja w walce zbrojnej", AON, 2001.
21) Liderman K.: „Bezpieczeństwo teleinformatyczne", BEL Studio, 2001.
22) Mąka D.: „Elementy zagrożeń i zarządzanie ryzykiem w świetle polityki bezpieczeństwa", IT Security Magazine, Nr 8-9, 2001.
23) Michniak J., Wisz A.: „Bezpieczeństwo i ochrona informacji w wojskowych sieciach telekomunikacyjnych i zautomatyzowanych systemach (zasady ogólne)", AON, 2000.
24) Moller E.: „Protective Measures Against Compromising Electromagnetic Radiation Emitted by Video Display Terminals", Inter Pact Press, 1991.
25) Molski M., Opala S.: „Elementarz bezpieczeństwa systemów informatycznych", Mikom, 2002.
26) Molski M.: „Podstawy Bezpieczeństwa Systemów Informatycznych", MSG-Media,
27) Molski. M.: „Bezpieczeństwo systemów informatycznych", Materiały szkoleniowe, 1997.
28) Nowiecki Z.T.: „Alarm o przestępstwie", TNOiK, 1997.
29) Rączkiewicz M.: „Bezpieczeństwo sieci komputerowych", FPT, 1995.
30) Sienkiewicz P., Dańczak A.: Praca studyjna „Bezpieczeństwo informacji w Siłach Zbrojnych RP. Aspekty strategiczne", AON, 2002.
31) Stawowski M.: „Badanie zabezpieczeń sieci komputerowych", ArsKom, 1999.
32) Stawowski M.: „Ochrona informacji w sieciach komputerowych", ArsKom, 1998.
33) Stokłosa J., Bilski T., Pankowski T.: „Bezpieczeństwo danych w systemach informatycznych", PWN, 2001.
34) Stokłosa J.: „Ochrona danych i zabezpieczenia w systemach teleinformatycznych", Wydawnictwo Politechniki Poznańskiej, 2003.
35) Suchański M.: „Kryptograficzne i elektromagnetyczne aspekty bezpieczeństwa sieci teleinformatycznych", Biuletyn WIŁ, 2000.
36) Swanson M., Guttman B.: „Generally Accepted Principles and Practices for Securing Information Technology Systems", NIST SP 800-14, 1996.
37) Wróblewski R.: „Podstawowe pojęcia z dziedziny polityki bezpieczeństwa, strategii i sztuki wojennej", AON, 1999.

Dokumenty normatywne

1) BS 7799-1:1999: Part 1: „Code of practice for Information Security Management Systems" British Standard Institute.
2) CM - (55)15 (Final) – „Bezpieczeństwo w ramach Organizacji Traktatu Północno-atlantyckiego"
3) 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.
4) Dyrektywa bezpieczeństwa – AD-70-1-PL, WSI, 1997.
5) Dyrektywa BTPO – 601A – Wytyczne w zakresie postępowania z materiałami kryptograficznymi.
6) Dyrektywa BTPO – 701A – Wytyczne w zakresie instalacji urządzeń przeznaczonych do przetwarzania informacji niejawnych.
7) Dyrektywa DBBT – 301A – Wytyczne w zakresie bezpieczeństwa fizycznego kancelarii kryptograficznych, stacji łączności kryptograficznej oraz pomieszczeń wydzielonych przeznaczonych do przetwarzania informacji niejawnej.
8) Dyrektywa NATO AD – 90 – 9 – Procedury w zakresie zabezpieczenia, ewidencji oraz zaopatrywania w środki i materiały kryptograficzne.
9) PN-I-02000: Technika informatyczna. Zabezpieczenia w systemach informatycznych. 1998.
10) PN-ISO-13335-1: Technika informatyczna. Wytyczne do zarządzania bezpieczeństwem systemów informatycznych. Pojęcia i modele bezpieczeństwa systemów informatycznych. 1999.
11) Rozporządzenie Prezesa Rady Ministrów z dnia 25 lutego 1999 r. w sprawie szczegółowego trybu prowadzenia przez służby ochrony państwa kontroli w zakresie ochrony informacji niejawnych stanowiących tajemnicę państwową (Dz.U.Nr 18, poz. 160).
12) Rozporządzenie Prezesa Rady Ministrów z dnia 25 lutego 1999 r. w sprawie podstawowych wymagań bezpieczeństwa systemów i sieci teleinformatycznych (Dz.U.Nr 18, poz. 162).
13) Rozporządzenie Prezesa Rady Ministrów z dnia 9 lutego 1999 r. w sprawie organizacji kancelarii tajnych (Dz.U.Nr 18, poz. 156).

14) Ustawa z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych (Dz.U.Nr 11, poz.95) wraz z późniejszymi zmianami. (2001 – Dz.U.Nr 22, poz. 247)
15) Ustawa z dnia 29.08.1997 r. o ochronie danych osobowych Dz. U. 133 poz. 883.
16) Zarządzenie Ministra Obrony Narodowej z dnia 7 sierpnia 2002 r. (nr 49/MON) w sprawie szczególnych zasad organizacji kancelarii tajnych, stosowania środków ochrony fizycznej oraz obiegu informacji niejawnych.