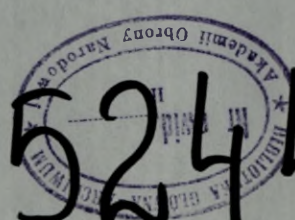
AKADEMIA OBRONY NARODOWEJ
WYDZIAŁ WOJSK LĄDOWYCH
KATEDRA DOWODZENIA I ŁĄCZNOŚCI

płk dr hab. inż. Józef MICHNIAK
kpt. dypl. inż. Andrzej WISZ

BEZPIECZEŃSTWO I OCHRONA INFORMACJI W WOJSKOWYCH SIECIACH TELEKOMUNIKACYJNYCH I ZAUTOMATYZOWANYCH SYSTEMACH DOWODZENIA

(Zasady ogólne)



WARSZAWA 2000 r.

SPIS TREŚCI

WSTĘP

Powodzenie działań taktycznych i operacyjnych zależy od wielu czynników w tym szczególnie od zachowania w tajemnicy celu ich podjęcia. Możliwość przechwytu przez przeciwnika informacji może utrudnić, a nawet zniweczyć osiągnięcie pożądanego stanu „szczelności informacyjnej". Dlatego, aby zachować w tajemnicy zamiary działań taktycznych (operacyjnych) oraz sposoby ich prowadzenia, należy podejmować szereg działań organizacyjno - technicznych zapewniających nie tylko terminowość, ciągłość i wierność łączności, ale także jej bezpieczne funkcjonowanie. Bezpieczeństwo łączności wojskowej jest rozumiane jako zdolność przeciwstawiania się jej rozpoznaniu przez przeciwnika oraz możliwościom wprowadzenia do systemu łączności wojskowej fałszywej informacji (dezinformacji). Spełnienie tego wymagania względem łączności jest bardzo trudnym zamierzeniem i zależy głównie od kategorii eksploatowanych systemów telekomunikacyjnych.

Proces planowania i organizowania systemów łączności różnych szczebli wojsk lądowych Sił Zbrojnych RP, przebiegał głównie w oparciu o doświadczenia, nawyki i niekiedy intuicję oficerów łączności. Jednak możliwości nowych środków walki, naukowo opracowane zasady prowadzenia działań taktycznych (operacyjnych) i kształt obecnej doktryny państwa stawia przed wojskowym systemem łączności znacznie większe wymagania. Projektowanie efektywnych, spełniających oczekiwania mobilnych organów dowodzenia, systemów łączności i informatyki jest procesem tworzenia różnych modeli posiadających określone cechy strukturalne, funkcjonalne i rozwojowe oraz weryfikowania ich użyteczności w praktycznym działaniu wojsk. W procesie projektowania wojskowych systemów łączności istotne miejsce zajmują przedsięwzięcia wpływające na zapewnienie wymaganego bezpieczeństwa łączności.

W treści opracowania zawarto podstawowe wiadomości z zakresu zapewnienia bezpieczeństwa wojskowych systemów łączności oraz ochrony informacji w sieciach komputerowych.

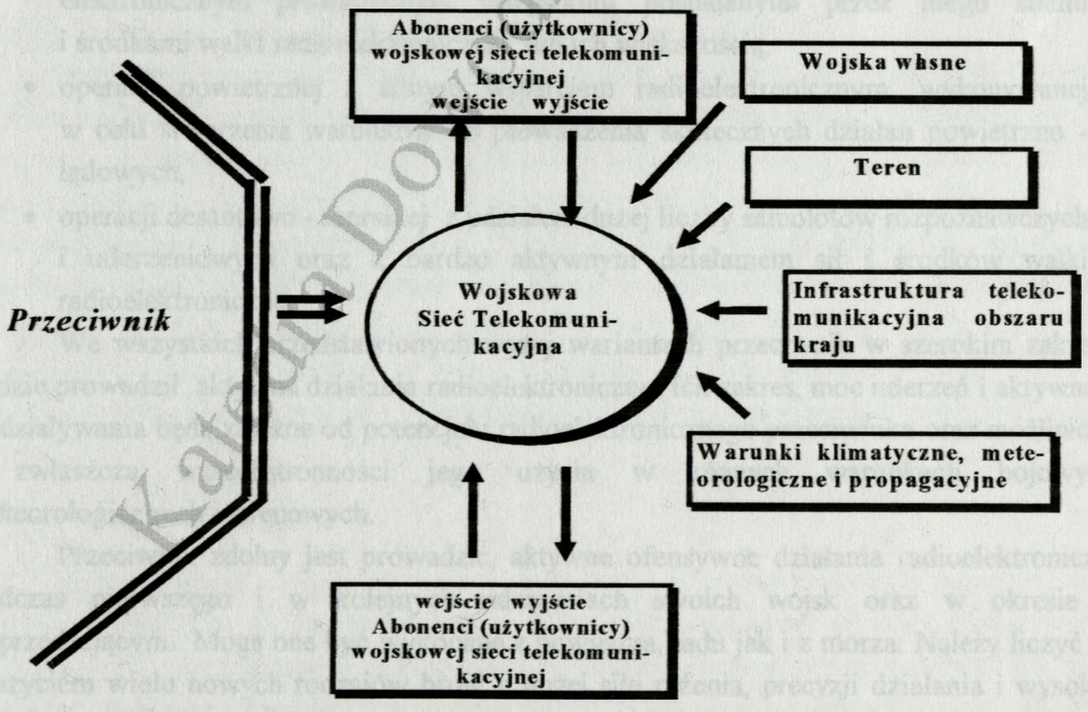
Opracowanie ma stanowić materiał uzupełniający dla słuchaczy kursów podyplomowych prowadzonych w AON interesujących się tą problematyką.

Autorzy

1. BEZPIECZEŃSTWO WOJSKOWEJ SIECI TELEKOMUNIKACYJNEJ

1.1. Otoczenie wojskowej sieci telekomunikacyjnej

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.1.1.



Rys.1.1. Otoczenie wojskowej sieci telekomunikacyjnej

1.2. 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 radioelektronicznego. 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 radioelektroniczne. Użyte mogą być elektroniczne środki prowadzenia wojny - broń precyzyjna i środki obezwładniania radioelektronicznego. 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 radioelektronicznego, będącego zmasowanym oddziaływaniem radioelektronicznym prowadzonym wszystkimi posiadanymi przez niego siłami i środkami walki radioelektronicznej, lub ich większością,
- operacji powietrznej z silnym wsparciem radioelektronicznym, 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 radioelektronicznej.

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

Przeciwnik zdolny jest prowadzić, aktywne ofensywne działania radioelektroniczne 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 radioelektronicznego 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 radioelektronicznych. 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 radioelektronicznej umożliwiają wykonanie różnego rodzaju zadań, szeroko rozumianego rozpoznania i obezwładniania. Zmasowane, aktywne działania radioelektroniczne 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 radioelektronicznej 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.

Przykłady:

Podczas wojny na Bliskim Wschodzie w 1967 roku, dzięki aktywnie prowadzonej dywersji radiowej wojska izraelskie uzyskały znaczne sukcesy w skali operacyjnej i taktycznej. Do wykonania zadań wojska izraelskie zawczasu przygotowały specjalne kadry z dobrą znajomością języka arabskiego. Zorganizowano wyspecjalizowane grupy dywersyjne, dla których opracowano szczegółowe plany działania i wyposażono je w odpowiednie środki łączności. Zadaniem ich była bieżąca analiza sytuacji radiowej, dokładne i ciągłe śledzenie pracy relacji radiowych wojsk arabskich, a w określonych

sytuacjach przekazywanie w nich fałszywych rozkazów, zarządzeń, komend i meldunków. Znany jest powszechnie fakt sprowadzenia na izraelskie lotniska sześciu libijskich samolotów MiG - 21 lecących do Kairu, którym w relacjach łączności radiowej naprowadzania podano w języku arabskim fałszywe kursy lotów. Podobna sytuacja zaistniała kiedy armia izraelska zdobyła przez zaskoczenie lotnisko w El Arish, przy czym wygląd lotniska pozostawiono bez zmian, a radiostację obsadzono przez operatora biegle władającego językiem arabskim. Dowództwo egipskie nie znając tego faktu kierowało posiłki przybywające samolotami z Algieru na to lotnisko, gdzie przejmowały je wojska izraelskie. Taka sytuacja trwała całą dobę. Wojskom izraelskim prowadzenie dywersji radiowej ułatwiał duży chaos, jaki panował w sieciach radiowych wojsk arabskich, gdzie nie przestrzegano podstawowych zasad korespondencji radiowej. Nie stosowano też sprawdzania tożsamości radiostacji oraz utajniania przekazywanych informacji. W początkowym okresie wojny w 1973 roku sukcesy w dywersji radiowej odnosiły wojska egipskie. Radiowe działania dywersyjne, w połączeniu z zakłóceniami dezorganizowały dowodzenie izraelskimi batalionami czołgów. Przykładem tego jest wprowadzenie izraelskiego batalionu czołgów, któremu przekazano drogą radiową fałszywe rozkazy, pod ogień własnych środków przeciwpancernych. Batalion stracił około 60% czołgów.

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 radioelektronicznych 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 radioelektroniczne 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 radioelektronicznego przeciwnika na relacje łączności systemów radiowych różnych szczebli dowodzenia i rodzajów wojsk. Stanowi element składowy obezwładniania radioelektronicznego - jednej z zasadniczych form walki radioelektronicznej.

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 radioelektronicznego, między innymi dywersję radiową, skoordynowaną z uderzeniami ogniowymi oraz z działaniem głównych zgrupowań uderzeniowych.

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

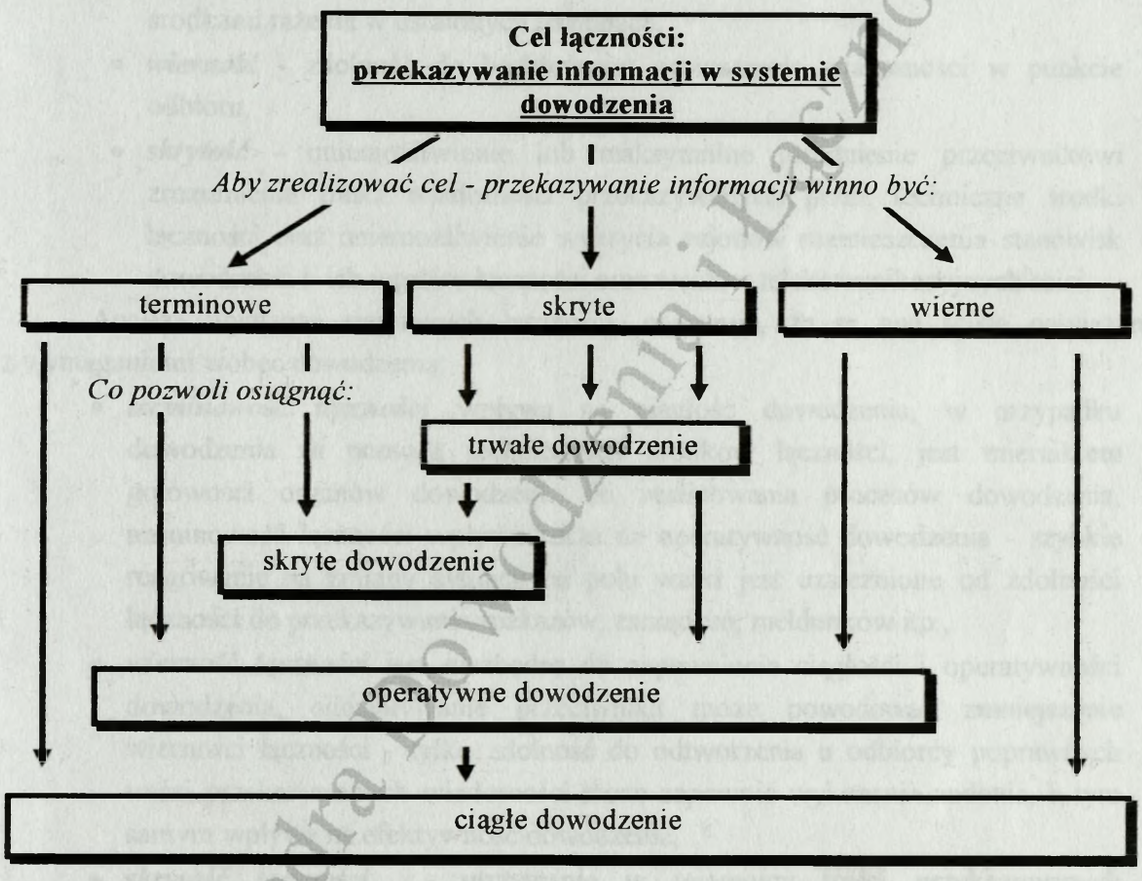
- przekazywanie dowódcom i sztabom, załogom samolotów, okrętów i wojskom informacji (mylnych meldunków, rozkazów, komunikatów itp.) oraz przedstawianie mylnego obrazu tego, co istnieje na polu walki lub tego, co już nie istnieje albo dopiero nastąpi,
- zajmowanie czasu w kanałach łączności i radionawigacyjnych, 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.

Jednym z zasadniczych elementów wchodzących w skład kompleksu przedsięwzięć z zakresu ochrony i obrony wojskowych systemów łączności, jest zapewnienie bezpieczeństwa łączności, którego ***celem jest ochrona treści przekazywanych wiadomości przez techniczne środki łączności przed rozpoznaniem radio-elektronicznym, penetracją pisemnych informacji przekazywanych środkami wojskowej poczty polowej, dywersją radiową oraz zabezpieczenie przed ucieczką informacji.***

1.3. Wymagania stawiane łączności wojskowej

Dla osiągnięcia celu bezpieczeństwa łączności należy zaplanować i zrealizować szereg zadań, których wykonanie zagwarantuje spełnienie wymagań jakie stawia się przed łącznością.

Łączność jest podstawowym środkiem zapewnienia dowodzenia wojskami i sterowania środkami rażenia.



Rys.1.2. Związek wymagań stawianych dowodzeniu i łączności

Z celu jaki stawia się łączności do osiągnięcia wynikają jej zadania:

- zapewnienie dowódcy i sztabowi dowodzenia wojskami oraz sterowania środkami rażenia,
- zapewnienie współdziałania pomiędzy związkami taktycznymi (oddziałami, pododdziałami) organicznymi, przydzielonymi i wspierającymi oraz z sąsiadami,

- zapewnienie przekazywania sygnałów powiadamiania, ostrzegania i alarmowania,
- zapewnienie wymiany wiadomości dla potrzeb kierowania organami regulacji ruchu, przekazywania i otrzymywania danych o sytuacji meteorologicznej, a także sygnałów wzajemnego rozpoznania i służby czasu.

Chcąc spełnić wymagania stawiane przez dowodzenie co do realizacji tych zadań, należy wyeksponować te cechy łączności, które w sposób najbardziej efektywny podnoszą jakość dowodzenia. Aby dowodzenie było ciągłe, trwałe, operatywne i skryte, łączność musi być przede wszystkim terminowa, wierna (wiarygodna) i skryta.

- ***terminowość*** - zdolność do zabezpieczenia dowodzenia wojskami i sterowania środkami rażenia w ustalonych terminach,
- ***wierność*** - zdolność do bezbłędnego odtwarzania wiadomości w punkcie odbioru,
- ***skrytość*** - uniemożliwienie lub maksymalne utrudnienie przeciwnikowi zrozumienia treści wiadomości przekazywanych przez techniczne środki łączności oraz uniemożliwienie wykrycia rejonów rozmieszczenia stanowisk dowodzenia i ich węzłów łączności oraz węzłów telekomunikacyjnych seici.

Analiza wymagań stawianych łączności, wykazuje, że są one ściśle powiązane z wymaganiami wobec dowodzenia:

- ***terminowość łączności*** wpływa na ciągłość dowodzenia, w przypadku dowodzenia za pomocą technicznych środków łączności, jest miernikiem gotowości organów dowodzenia do realizowania procesów dowodzenia, terminowość łączności wpływa także na operatywność dowodzenia - szybkie reagowanie na zmiany sytuacji na polu walki jest uzależnione od zdolności łączności do przekazywania rozkazów, zarządzeń, meldunków itp.,
- ***wierność łączności*** jest niezbędna do zapewnienia ciągłości i operatywności dowodzenia, oddziaływanie przeciwnika może powodować zmniejszenie wierności łączności - tylko zdolność do odtworzenia u odbiorcy poprawnych treści przekazywanych wiadomości może zapewnić wykonanie zadania, a tym samym wpływa na efektywność dowodzenia,
- ***skrytość łączności*** - utrzymanie w tajemnicy treści przekazywanych wiadomości oraz samego faktu i miejsca ich przekazywania, w dużym stopniu zapewnia osiąganie skrytości dowodzenia.

Żeby spełnić wymagania stawiane przez dowodzenie, łączność musi cechować się odpowiednią terminowością, wiernością oraz skrytością - cechy te nazywa się syntetycznie jakością łączności ($J_Ł$). Jakość łączności jest więc funkcją jej wierności ($W_Ł$), skrytości ($S_Ł$) oraz terminowości ($T_Ł$).

$$J_Ł = f(W_Ł, S_Ł, T_Ł)$$

Jakość łączności to właściwość, która charakteryzuje je zdolność do wykonywania zadań w zakresie zapewnienia terminowej, wiernej i skrytej łączności w procesie dowodzenia oraz kierowania środkami walki. Będąc charakterystyką jednej z podstawowych składowych

procesu dowodzenia, jakość łączności sama w sobie opisuje proces wzajemnej wymiany informacji. Należy zauważyć, że jakościowe cechy łączności są wzajemnie uzależnione i w konkretnych warunkach mogą być powiązane między sobą różnymi relacjami. Przykładowo: terminowość łączności jest podstawowym wskaźnikiem przy ocenie procesu przekazywania wiadomości - szczególnie o najwyższych kategoriach pilności. Jednakże wiadomości, które zostały odebrane z wiernością niższą niż zadana, nie mogą być zaliczone do obsłużonych (są tracone), co obniża wskaźnik terminowości łączności. Z drugiej strony, w celu osiągnięcia zadanego poziomu wierności, wiadomość może być przekazana z niższą prędkością transmisji, z większym nadmiarem informacyjnym lub kilkakrotnie. Może to doprowadzić do zwiększania czasu przekazywania wiadomości powyżej dopuszczalnej granicy (dezaktualizacja informacji) oraz do opóźnień innych wiadomości, oczekujących w kolejce, a w konsekwencji - do obniżenia wskaźnika terminowości łączności.

Skrytość łączności okazuje się „pośrednią" charakterystyką łączności, ponieważ zmniejszenie wskaźnika skrytości, w wyniku oddziaływania przeciwnika może doprowadzić do pogorszenia terminowości i wierności łączności. Oprócz tego, zastosowanie urządzeń utajniających może zmniejszyć ogólną szybkość eksploatacyjną transmisji wiadomości.

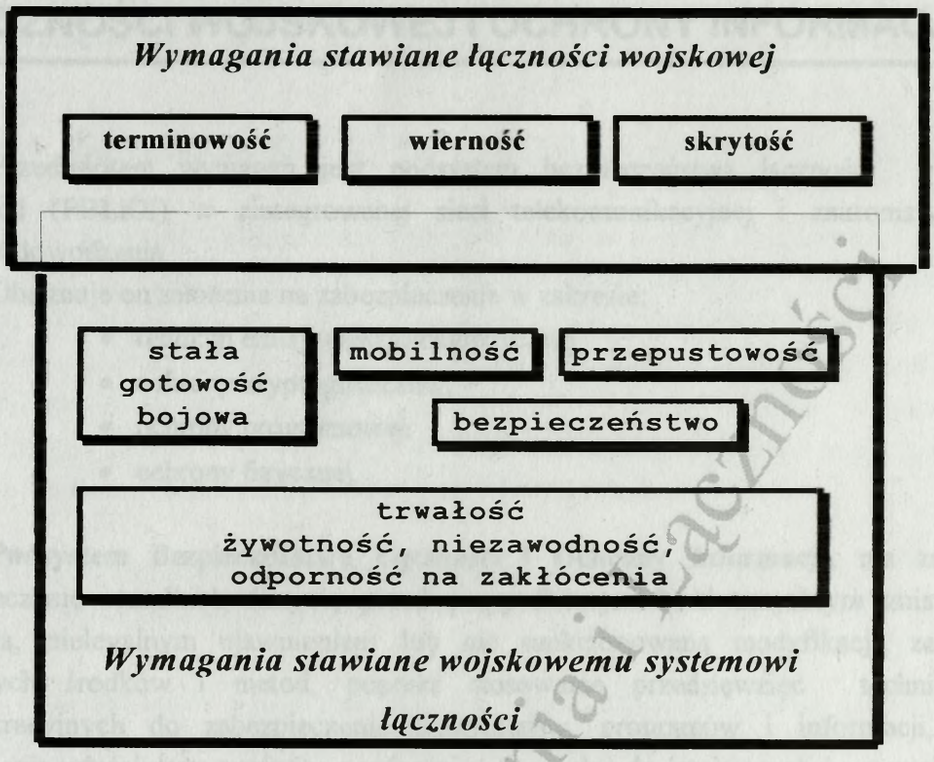
Jedną z podstawowych właściwości i wymaganiami, które stawia się łączności wojskowej jest zachowanie wysokiego stopnia bezpieczeństwa łączności.

Bezpieczeństwo łączności jest rozumiane jako zdolność przeciwstawiania się rozpoznaniu łączności przez przeciwnika, oraz zdolność przeciwstawienia się wprowadzaniu do systemu łączności fałszywych informacji (dezinformacji).

Wysoki stopień bezpieczeństwa łączności osiągnie się wtedy, kiedy uzyska się wysokie wskaźniki wszystkich trzech omówionych wyżej cech składających się na jakość łączności jednocześnie, ewentualnie dwóch lub jednej, ale z uwzględnieniem wpływu pozostałych.

1.4. Wymagania stawiane systemowi łączności

Terminowość, wierność i skrytość łączności (najbardziej uznawane wymagania stawiane łączności wojskowej) mają określone implikacje jeżeli idzie o oczekiwania. Przy uwzględnieniu wpływu otoczenia, można określić wymagania jakie musi spełniać *system łączności wojskowej* - przedstawia to rys. 1.3.



Rys. 1.3. Wymagania stawiane łączności wojskowej i wojskowemu systemowi łączności

- ***stała gotowość bojowa*** - zdolność przystąpienia do zapewnienia dowodzenia wojskami i sterowania środkami rażenia w czasie określonym przez dowództwo, po zmianie struktury systemu spowodowanej przejściem w wyższy stan gotowości bojowej lub wymuszonej sytuacją operacyjno - taktyczną,
- ***trwałość*** - zdolność do zapewnienia dowodzenia wojskami i sterowania środkami rażenia w warunkach intensywnego oddziaływania ogniowego i radioelektronicznego przeciwnika,
- ***mobilność*** - zdolność systemu do zmiany struktury oraz do rozwijania i przenoszenia elementów systemu, gwarantująca osiągnięcie gotowości całego systemu w nowych warunkach i w założonym czasie,
- ***przepustowość*** - zdolność do transmisji określonych strumieni wiadomości w wyznaczonym czasie,
- ***bezpieczeństwo*** - zdolność do poprawnego funkcjonowania w warunkach prowadzenia przez przeciwnika różnorodnych form walki radioelektronicznej.

2. WYMAGANIA ZAPEWNIENIA BEZPIECZEŃSTWA ŁĄCZNOŚCI WOJSKOWEJ I OCHRONY INFORMACJI

Przedmiotem wymagań jest podsystem bezpieczeństwa łączności i ochrony informacji (PBŁiOI) w zintegrowanej sieci telekomunikacyjnej i zautomatyzowanym systemie dowodzenia.

Obejmuje on założenia na zabezpieczenie w zakresie:

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

Podsystem Bezpieczeństwa Łączności i Ochrony Informacji, ma za zadanie zabezpieczenie wszelkich danych, przed przypadkowym bądź umyślnym zniszczeniem, kradzieżą, nielegalnym ujawnieniem lub nie sankcjonowaną modyfikacją za pomocą dostępnych środków i metod, poprzez stosowanie przedsięwzięć technicznych i administracyjnych do zabezpieczenia komputerów, programów i informacji, w celu zapewnienia właściwego poziomu poufności w stosunku do istniejących i prognozowanych zagrożeń stanowisk pracy bojowej (SPB) w warunkach bliskiej styczności ze środkami WRE potencjalnego przeciwnika.

Bazą techniczną zapewniającą funkcjonowanie ZSŁącz. są aparatownie komutacyjne i transmisyjne, a ZSyD zaś mobilne obiekty wyposażone w odpowiedni pokładowo-przenośny Zestaw Środków Technicznych (ZŚT) stanowiące różnego rodzaju Stanowiska Pracy Bojowej (SPB).

Zestaw Środków Technicznych (ZŚT) w podsystemie łączności stanowi, wyposażenie „lokalnych węzłów łączności" zapewniających osobom funkcyjnym wymianę informacji w relacjach zgodnych z powiązaniami informacyjnymi. System łączności powinien być budowany w oparciu o środki łączności cyfrowej posiadające odpowiednie zabezpieczenia niejawnej informacji, skuteczne zarówno w łączności radiowej, jak i radioliniowo-przewodowej oraz w sieciach informatycznych w ścisłym powiązaniu z ZSyD wojsk lądowych.

2.1. WYMAGANIA NA PODSYSTEM BEZPIECZEŃSTWA ŁĄCZNOŚCI I OCHRONY INFORMACJI

2.1.1. Założenia ogólne

Przy wyborze mechanizmów ochrony informacji w systemach łączności i informatyki należy przyjąć, że informacja powinna być chroniona od momentu jej powstania do momentu celowego zniszczenia po jej wykorzystaniu. A także każda informacja opracowywana, przechowywana oraz przesyłana w systemach łączności i informatyki powinna być zabezpieczona przed dekonspiracją i modyfikacją, ponieważ wyniku świadomego lub nieświadomego „ataku" ze strony użytkowników lub celowej ingerencji przez przeciwnika, może wystąpić zmiana stanu systemu lub sposobu jego działania.

2.1.2. Zagrożenia systemów teleinformatycznych i sieci telekomunikacyjnych

W celu uniknięcia ujawnienia ważnych informacji należy dążyć do eliminowania elementów systemu, które mogą stanowić źródło zagrożenia.

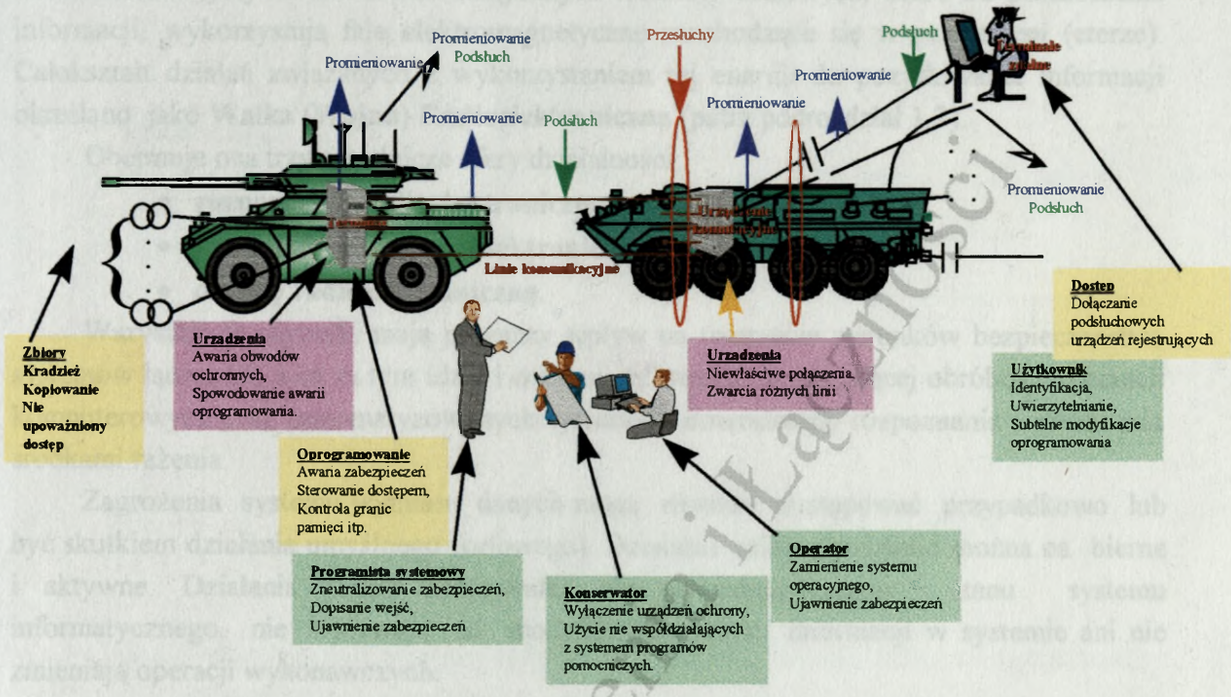
W związku z tym należy dokonać analizy i określić elementy systemów teleinformatycznych narażone na kompleksowe oddziaływanie przeciwnika w zakresie walki radioelektronicznej oraz ustalić możliwe sposoby i miejsca ujawniania (zdobywania) niezbędnych informacji.

Na podstawie dotychczasowych doświadczeń określono, że niezbędne informacje można pozyskać w wyniku:

1. Błędnego działania
   - systemu teleinformatycznego;
   - sprzętu łączności lub komputerów;
   - personelu.
2. Awarii
   - zasilania (brak zasilania, wahania napięcia, przepięcia, przebicia);
   - sieci transmisji (brak możliwości nawiązania połączenia, zerwanie połączenia, błędy komutacji, przesłuchy i zwarcia, błędy transmisji);
   - sprzętu łączności lub komputerów.
3. Klęsk żywiołowych
   - powódź;
   - pożar;
   - silne wyładowania atmosferyczne;
   - wstrząsy.

Podstawowymi zagrożeniami, jakie niesie za sobą zastosowanie informatyki procesach obróbki informacji, w tym głównie niejawnej, są wszelkiego typu emisje

elektromagnetyczne, w tym szczególnie emisje ujawniające: przewodzona i promieniowana. Szczegółowo zjawisko występowania ujawniającej emisji elektromagnetycznej ilustruje rys. 2.1.



Rys. 2.1. Występowanie ujawniającej emisji elektromagnetycznej

W urządzeniach takich jak elektroniczne centrale cyfrowe, urządzenia teletransmisyjne oraz terminale końcowe, promieniują praktycznie wszystkie elementy.

Wśród nich źródłem największego promieniowania ujawniającego systemów teleinformatycznych będą: środki komutacji, środki teletransmisyjne, źródła zasilania, uziomy, linie sieci abonenckiej i dalekosiężnej, urządzenia podsystemu zarządzania, terminale i ich wyposażenie.

W sieciach teleinformatycznych, urządzeniach i systemach łączności dodatkowe zagrożenie stanowią:

- przesłuchy pomiędzy obwodami abonenckimi i dalekosiężnymi liniami teletransmisyjnymi;
- niekontrolowany dostęp do zasobów terminali, który może doprowadzić do kradzieży, kopiowania i modyfikowania programów lub zabezpieczeń;
- ujawnienie osobom nie upoważnionym sposobu zabezpieczenia urządzeń, haseł, identyfikatorów dostępu itp.;
- niekontrolowany dostęp do urządzeń sterujących i zarządzających systemami łączności, co w konsekwencji może doprowadzić do okresowego lub całkowitego zablokowania funkcjonowania systemu.

Bardzo ważnym z punktu widzenia ciągłości funkcjonowania systemów teleinformatycznych, a w szczególności zautomatyzowanych systemów dowodzenia oraz

sterowania środkami rażenia, zagrożeniem jest elektromagnetyczne oddziaływanie potencjalnego przeciwnika.

Zagrożenie to wynika z powszechnego zastosowania do organizacji sieci telekomunikacyjnej na szczeblach taktycznych środków radiowych, które do przenoszenia informacji, wykorzystują fale elektromagnetyczne rozchodzące się w przestrzeni (eterze). Całokształt działań związanych z wykorzystaniem tej energii do pozyskiwania informacji określano jako **Walka (Wojna) Radioelektroniczna** (patrz podrozdział 1.2).

Obejmuje ona trzy zasadnicze sfery działalności;

- **rozpoznanie radioelektroniczne**;
- **obezwładnianie radioelektroniczne**;
- **obronę radioelektroniczną**.

Wszystkie te czynniki mają poważny wpływ na tworzenie warunków bezpieczeństwa systemów łączności, a co za tym idzie i ochrony informacji, podlegającej obróbce w sieciach komputerowych oraz zautomatyzowanych systemach dowodzenia, rozpoznania i sterowania środkami rażenia.

Zagrożenia systemu wymiany danych mogą również występować przypadkowo lub być skutkiem działania umyślnego (celowego). Działania celowe podzielić można na bierne i aktywne. Działania bierne przeciwnika nie powodują zmiany stanu systemu informatycznego, nie wpływają na modyfikacje żadnej informacji w systemie ani nie zmieniają operacji wykonawczych.

Najpowszechniej stosowane *działania bierne* to szeroko rozumiany **podsłuch i analiza ruchu sieci.** Działania bierne są najczęściej etapem przygotowawczym do *działań aktywnych* (wykonania ataku na system).

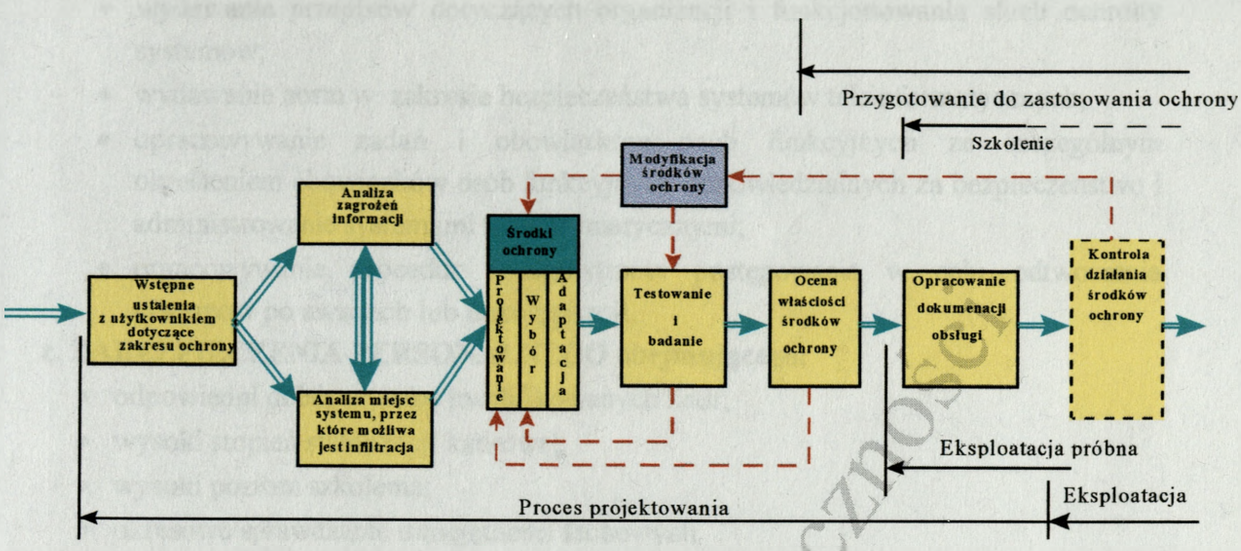
Systemy informatyczne bez odpowiednich zabezpieczeń, są szczególnie wrażliwe (podatne) na działania aktywne. Atak na system może być przeprowadzony ze strony użytkowników systemu lub z zewnątrz.

Aktualnie możliwe ataki na systemy informatyczne zostały w dużej mierze rozpoznane i poklasyfikowane. Nie oznacza to, że w tym zakresie skończyły się już możliwości i nie pojawiają się nowe zagrożenia.

Dla wojskowych systemów informatycznych szczególne zagrożenie stanowią:

- podsłuch przesyłanej informacji,
- obserwacja ruchu sieci,
- odbiór emisji ujawniającej (groźba nieuprawnionego ujawnienia informacji bez zmiany stanu w czasie oddziaływania na system);
- modyfikacja, powtórzenia, dezinformacja lub dywersja (możliwość preparowania nieautoryzowanych zmian systemu w czasie aktywnego oddziaływania na sieci lub ich elementy).

Na poniższym rysunku przedstawiony jest algorytm postępowania w czasie opracowywania metod ochrony sieci teleinformatycznych, który pozwala na wstępną analizę zagrożeń, uwzględnienie wymogów użytkowników oraz techniczno-programowych możliwości podsystemów i urządzeń, poparty badaniami oraz ewentualną modyfikacją i praktycznym sprawdzeniem skuteczności.



Rys. 2.2. Algorytm opracowywania metod ochrony sieci telekomunikacyjnych

2.1.3. Podstawowe zasady ochrony informacji w wojskowych systemach teleinformatycznych

W sieciach informatycznych z punktu widzenia zastosowania wyróżnia się: zautomatyzowane systemy dowodzenia (ZSyD), zautomatyzowany systemy rozpoznania (ZSyR) oraz zautomatyzowane systemy sterowania środkami rażenia (ZSySŚR).

Systemy te ze względu na swe przeznaczenie muszą być zabezpieczone w podstawowe moduły bezpieczeństwa elektronicznego przetwarzania i przesyłania danych, które zapewnia : **skrytość, integralność, dostępność informacji, pewność identyfikacji, łatwość w użyciu,** a ze względu na szerokie zastosowanie w systemach telekomunikacyjnych środków radiowych i radioliniowych, powinny być chronione przed kompleksowym, elektromagnetycznym oddziaływaniem potencjalnego przeciwnika.

Cele powyższe realizuje się poprzez stosowanie przedsięwzięć bezpieczeństwa łączności z zakresu :

a. ZABEZPIECZENIA TECHNICZNEGO obejmującego:

- ochronę kryptograficzną;
- ochronę danych;
- ochronę techniczną (fizyczną);
- redukcję emisji ujawniającej;
- ochronę przed czynnikami WRE.

b. ZABEZPIECZENIA ORGANIZACYJNEGO obejmującego:

- regulacje prawne w zakresie ochrony kryptograficznej;

- wydawanie przepisów dotyczących organizacji i funkcjonowania służb ochrony systemów;
- wydawanie norm w zakresie bezpieczeństwa systemów teleinformatycznych;
- opracowywanie zadań i obowiązków osób funkcyjnych ze szczególnym określeniem obowiązków osób funkcyjnych odpowiedzialnych za bezpieczeństwo i administrowanie systemami teleinformatycznymi;
- opracowywanie procedur i algorytmów postępowania w celu odtworzenia systemów po awariach lub dekonspiracji.

c. ZABEZPIECZENIA PERSONALNEGO obejmującego;

- odpowiedni dobór wysoko kwalifikowanych kadr;
- wysoki stopień stabilizacji kadrowej;
- wysoki poziom szkolenia;
- okresowe sprawdzanie umiejętności fachowych.

2.2. WYMAGANIA NA BEZPIECZEŃSTWO I OCHRONĘ INFORMACJI W WOJSKOWYCH SYSTEMACH TELEKOMUNIKACYJNYCH I ZAUTOMATYZOWANYCH SYSTEMACH DOWODZENIA

2.2.1. Założenia ogólne

W celu zapewnienia bezpieczeństwa informacji oraz właściwego i sprawnego funkcjonowania systemu, niezbędne jest stworzenie spójnego i szczelnego ***podsystemu bezpieczeństwa i ochrony informacji*** składającego się z:

- ♦ *modułu zarządzania urządzeniami łączności;*
- ♦ *modułu zarządzania bezpieczeństwem łączności;*
- ♦ *modułów ochrony kryptograficznej;*
- ♦ *przenośnej stacji dystrybucji danych kryptograficznych.*

Przy organizacji ***podsystemu bezpieczeństwa i ochrony informacji*** należy przyjąć, że informacje w systemie teleinformatycznym, w zależności od klauzuli tajności, powinny być chronione z gwarantowaną mocą poprzez:

1. ***Podsystem łączności utajnionej*** przeznaczony do zabezpieczenia informacji o klauzuli „TAJNE", oparty powinien być o cyfrowy system teleinformatyczny, wyposażony w urządzenia kryptograficzne zapewniające gwarantowaną moc kryptograficzną, umożliwiając:
   - automatycznie utajnianą łączność foniczną i telefaksową oraz transmisję danych;
   - wiarygodną identyfikację użytkowników systemu;
   - wiarygodną weryfikację uprawnień użytkowników systemu;

- wiarygodną identyfikację elementów składowych systemu (węzłów łączności SD),węzłów telekomunikacyjnych, wozów dowodzenia, aparatowni, radiostacji, terminali abonenckich itp.);
- integralność przesyłanym i przechowywanym informacjom;
- elastyczność i podatność na zmiany konfiguracji sieci telekomunikacyjnej;
- podatność na rozbudowę bez utraty spójności;
- archiwizację danych;
- maksymalną odporność na dekonspirację i dywersję.

A ponadto powinien :

a) posiadać terminale abonenckie (aparaty telefoniczne, telefaksy, komputery, serwery sieci, itp.) z atestem, potwierdzającym spełnienie wymagań w zakresie bezpieczeństwa łączności (dopuszczający do przetwarzania informacji niejawnych).

b) posiadać terminale abonenckie wyposażone w:
   - urządzenie utajniające (szyfrujące);
   - moduł bezpieczeństwa, spełniający rolę nośnika danych kryptograficznych oraz szereg innych niezbędnych dla ochrony funkcji.

Terminal, po wyjęciu z niego modułu bezpieczeństwa, powinien zawierać jedynie szczątkowe elementy kryptografii.

c) być wyposażony w urządzenia utajniające i moduły bezpieczeństwa z elementami programowej kontroli dostępu (hasła zabezpieczające).

d) posiadać dla każdego użytkownika indywidualny (osobisty) identyfikator (może nim być moduł bezpieczeństwa), zapewniający wiarygodną identyfikację oraz możliwość pracy z:
   - własnego terminala abonenckiego;
   - terminali abonenckich pracujących w systemie.

e) zapewnić stosowanie:
   - utajniania grupowego o przepływności 128 kitb/s ÷ 2048 kbit/s i większej;
   - utajniania indywidualnego - przeznaczonego do ochrony informacji fonicznej i transmisji danych (w tym w sieciach z komutacją pakietów), stosowanego w:
     ⇒ terminalach abonenckich;
     ⇒ radiotelefonach;
     ⇒ radiostacjach KF i UKF;
   - szyfrowania baz danych, plików w serwerach, stacjach roboczych do klauzuli TAJNE.

Utajnianie transmisji fonicznej i transmisji danych (w tym utajnianie indywidualne w sieci z komutacją pakietów) musi gwarantować identyfikację informacji, uwierzytelnianie informacji, integralność informacji.

2.2.2. Wymagania w zakresie redukcji elektromagnetycznej emisji ujawniającej

Każde urządzenie elektroniczne stanowi źródło ubocznej emisji elektromagnetycznej indukowanej w otaczającym je środowisku oraz we wszelkiego typu przewodach elektrycznych, liniach transmisyjnych i konstrukcjach metalowych.

Z punktu widzenia poprawności funkcjonowania innych urządzeń nazywana jest zakłóceniami elektromagnetycznymi, zaś z punktu widzenia możliwości wykorzystania jej do infiltracji elektronicznej obiektów - emisjami ujawniającymi. Promieniowanie to ma zasięg zróżnicowany uzależniony od typu ww. elementów

Niepożądane emisje elektromagnetyczne powinny być stłumione do wartości niższej od progowej, uznanej za dopuszczalną określonej zwykle stosownymi normami.

Problematyka redukcji niepożądanej emisji elektromagnetycznej jest jedną z dziedzin **KOMPATYBILNOŚCI ELEKTROMAGNETYCZNEJ *(KEM)*. Niepożądane emisje elektromagnetyczne ogranicza się dwiema głównymi metodami:**

1. **pasywną** - poprzez stosowanie odpowiednich przedsięwzięć technicznych w zakresie konstrukcji urządzeń;
2. **aktywną** - poprzez:
   a) stosowanie w wojskowych sieciach teleinformatycznych jedynie sprzętu atestowanego, a w warunkach mobilnych spełniającego wojskowe normy wytrzymałościowo-klimatyczne (w stosunku do sprzętu pochodzącego z importu oraz produkowanego w kraju);
   b) stosowanie urządzeń o obniżonym poziomie emisji ujawniającej;
   - osłony i kabiny ekranujące w warunkach stacjonarnych, natomiast w sprzęcie mobilnym nadwozia szczelne elektromagnetycznie (o odpowiedniej tłumienności, określanej przez Wojskowe Biuro Kryptograficzne);
   - ekranowanie pomieszczeń (tylko w warunkach stacjonarnego rozwijania SPB);
   - wykonanych w technice specjalnej, zapewniającej spełnienie norm na poziom emisji;

   c) stosowanie łączy światłowodowych;

Najskuteczniejszymi metodami zmniejszania niepożądanych emisji elektromagnetycznych jest ekranowanie i filtracja obwodów zewnętrznych urządzenia. Można również stosować separację za pomocą krótkich odcinków kabla światłowodowego, uzbrojonego w przetworniki optoelektryczne.

Ze względu na duże nakłady finansowe i czasochłonność związane z ekranowaniem i filtracją, a także odpowiednie wymagania estetyczne i ergonomiczne budowanych urządzeń, zagadnienia emisyjności rozwiązywać trzeba już na etapie projektowania poszczególnych bloków funkcjonalnych (modułów).

Uwzględnianie w procesie projektowania tych zasad (projektowanie obwodów drukowanych z punktu widzenia KEM, dobór parametrów sygnałów, uziemiania, symetryzacji, izolowania, separacji, kompensacji, doboru impedancji źródeł, odbiorników

i linii transmisyjnych itp.) pozwala na znaczne zmniejszenie EEM już u źródła, a tym samym na zmniejszenie wymagań dotyczących skuteczności ekranowania i filtracji.

2.2.3. Ochrona kryptograficzna

Metody kryptograficzne chronią przed przeglądaniem i podsłuchiwaniem czyniąc informację niezrozumiałą i w zasadzie są najskuteczniejszym sposobem ochrony informacji w systemach teleinformatycznych.

Odpowiednio zaprojektowany i wdrożony system kryptograficzny (z uwzględnieniem zagadnień sterowania szyfrowaniem) zdecydowanie ogranicza możliwości działania, nawet wyrafinowanego przeciwnika jednak nie eliminuje ich całkowicie.

Systemy ochrony kryptograficznej zapewniają:

1. Szyfrowanie informacji niejawnych przesyłanych w sieciach telekomunikacyjnych i teleinformatycznych w sposób zapewniający jej integralność. Postęp technologiczny umożliwił wysokiej jakości szyfrowanie informacji u źródła i odszyfrowywanie dopiero u jej ujścia. Jest to obecnie obowiązujący standard w nowoczesnych armiach świata.

   Zminiaturyzowane urządzenia elektroniczne realizujące odpowiednie algorytmy szyfrowania stanowią integralną część nowoczesnych abonenckich urządzeń łączności (cyfrowych aparatów telefonicznych, cyfrowych radiostacji, radiotelefonów) lub wyposażenia abonenckiego (np. telefaksów). Szyfrowanie i deszyfrowanie informacji odbywa się w czasie rzeczywistym.
2. Wiarygodną identyfikację stacji informatycznych i użytkowników oraz sprawdzanie ich uprawnień.
3. Maskowanie ruchu w sieci telekomunikacyjnej (tzw. "trafiku"). Uniemożliwia to identyfikację ważnych stanowisk dowodzenia i obiektów na podstawie przepływu (ruchu) informacji w sieci. Do maskowania ruchu (w tym sygnalizacji międzycentralowej) wykorzystywane są grupowe urządzenia utajniające.
4. Ochronę informacji gromadzonych w bazach danych systemów informatycznych.

2.2.3.1. Ogólne założenia na ochronę kryptograficzną transmisji informacji w podsystemach radiowych

Do przekazywania informacji w sieciach i kierunkach łączności radiowej wykorzystywane są:

- analogowe radiostacje KF i UKF (nie posiadające wewnętrznych modułów ochrony kryptograficznej);
- cyfrowe radiostacje UKF i KF (posiadające wewnętrzne moduły utajniające);
- cyfrowe radiostacje UKF (nie posiadające wewnętrznych modułów ochrony kryptograficznej);

Kryptograficzna ochrona informacji w kanałach radiowych powinna być realizowana poprzez:

a) w pierwszej kolejności - testowanie i adaptację algorytmów szyfrowych wewnętrznych urządzeń utajniających, stanowiących integralną część cyfrowej radiostacji UKF/KF, a następnie opracowanie i wdrożenie własnego modułu utajniającego, który powinien:
   - utajniać zarówno sygnały mowy jak i sygnały transmisji danych podawane na wejście cyfrowe radiostacji;
   - umożliwiać automatyczne przyporządkowanie różnych kluczy seansowych każdej sesji radiowej;
   - umożliwiać wprowadzanie kluczy szyfrowych za pośrednictwem urządzenia wprowadzania dokumentów kluczowych.

b) opracowanie utajniania do terminala taktycznego radiostacji cyfrowej UKF.

c) opracowanie wokoderowych urządzeń utajniających do prowadzenia rozmów niejawnych przez analogowe radiostacje KF. Wokoder powinien spełniać wymagania określone normami STANAG. Transmisja danych niejawnych przez analogowe radiostacje KF powinna odbywać się z wykorzystaniem wokoderowego modułu utajniającego. W przypadku braku modułu kryptograficznego należy zastosować kryptografię instalowaną w urządzeniu obsługującym radiostację.

d) zastosowanie automatycznego systemu uchylania się przed celowym rozpoznaniem i zakłócaniem w postaci F-H („skaczącej częstotliwości) posiadającego możliwość zastosowania kryptografii

2.2.3.2. Ogólne założenia na ochronę kryptograficzną w podsystemach radiodostępu

Do przekazywania informacji w podsystemach radiodostępu należy wykorzystywać cyfrowe radiostacje UKF i radiotelefony - radiodostęp simpleksowy oraz cyfrowe aparaty telefoniczne (cyfrowe punkty abonenckie) - radiodostęp dupleksowy. Kryptograficzna ochrona informacji w tych podsystemach powinna być realizowana poprzez zastosowanie radiowych urządzeń utajniających zgodnie z wymaganiami zawartymi w poprzednich punktach. Utajnianiu w tym systemie powinna podlegać transmisja foniczna i transmisja danych.

Szczegółowe wymagania na ochronę informacji przesyłanych i przekazywanych w podsystemach radiodostępu, powinny być określone w wymaganiach technicznych (WT) urządzeń kryptograficznych planowanych do wykorzystywania w tym podsystemie.

2.2.3.3. Ogólne założenia na ochronę kryptograficzną w podsystemie łączności wokoderowej

Należy przyjąć, że utajnianie w oparciu o metodę „wokoderową" w sieciach i kierunkach radiowych, powinno odbywać się z szybkością co najmniej 1,2 kbit/s (zarówno transmisja foniczna jak i transmisja danych).

Przy wykorzystaniu przewodowo-radioliniowych kanałów łączności, szybkość transmisji powinna wynosić 2400, 4800 i 9600 bit/s (wybór automatyczny i ręczny) -

transmisja foniczna i danych. Przy szybkości 4800 bit/s powinna istnieć możliwość równoczesnej transmisji fonicznej i transmisji danych.

Wokoder powinien spełniać wymagania określone normami STANAG (m.in. 4198, 4479).

Szczegółowe wymagania na ochronę informacji przetwarzanych i przesyłanych w tych podsystemach powinny być określone w WT urządzeń kryptograficznych planowanych do wykorzystywania w podsystemach radiowych i radioliniowo-przewodowych.

2.2.4. Ochrona programowa

Ochrona danych dotyczy zastosowania metod i środków programowych, zapewniających bezpieczeństwo informacjom przechowywanych, przetwarzanych w systemach komputerowych i przesyłanych w sieciach teleinformatycznych. Obejmuje ona cztery rodzaje sterowania, do których zaliczamy: sterowanie szyfrowaniem, sterowanie dostępem, sterowanie przepływu informacji, sterowanie wnioskowaniem.

2.2.4.1. Sterowanie szyfrowaniem

Programy zabezpieczające zawierają własne pliki danych sterujące procesem szyfrowania jak i przydzielania określonych kluczy, w zależności od przewidywanego poziomu zabezpieczeń i stopnia rozpowszechniania plików (np. tylko użytkownik, grupa użytkowników).

2.2.4.2. Sterowanie dostępem

Mechanizmy sterowania dostępem zapewniają, że wszystkie bezpośrednie dostępy do obiektów, danych systemu informatycznego, komunikacyjnego czy łączności **są legalne**.

Dzięki ustaleniu zasad czytania, zmieniania i kasowania danych oraz programów sterowanie dostępem zapobiegają przypadkowej lub zamierzonej utracie tajności, wiarygodności lub dostępności.

Skuteczność sterowania dostępem opiera się na dwóch przesłankach:

- poprawna identyfikacja użytkowników systemu (nikt z użytkowników nie powinien uzyskać cudzych praw dostępu do danych);
- informacje opisujące prawa dostępu każdego użytkownika lub programu są chronione przed nieuprawnioną modyfikacją.

2.2.4.3. Sterowanie przepływem informacji

Mechanizmy sterowania dostępem ustalają zasady dostępu do obiektów, lecz nie mają wpływu na to co podmioty mogą robić z informacjami zawartymi w obiektach. Wiele kłopotów związanych z „przeciekami" informacji nie wynika z błędnego sterowania dostępem lecz z braku polityki sterowania przepływem informacji.

Sterowanie przepływem informacji dotyczy **praw rozchodzenia się danych**, bez względu na to, jakie obiekty zawierają informacje. Sterowanie przepływem ustala legalne kanały, którymi informacje mogą przepływać.

2.2.4.4. Sterowanie „wnioskowaniem"

W przypadku, kiedy informacje czerpane z poufnych danych muszą być odtajnione i udostępnione w celu szerszej ich dystrybucji, wtedy mechanizmy kontroli przepływu nie wystarczają. Celem sterowania wnioskowaniem jest zapewnienie , by udostępnianie przez bazę danych statysty, nie doprowadziło do ujawniania danych poufnych.

2.2.4.5. Wymagania w zakresie ochrony programowej

Programowa ochrona danych związana jest z klasą stosowanych urządzeń oraz oprogramowania, a jako standard przyjęto klasyfikację opracowaną przez National Computer Security Center (NCSC) opublikowaną w opracowaniu pt. „Kryteria oceny bezpieczeństwa systemów komputerowych" zwanym także „**Pomarańczową książeczką"** *(Orange Book).*

Kryteria bezpieczeństwa podzielono na cztery kategorie: **D, C, B i A,** z których **C** została podzielona na dwie klasy **(C1 i C2)**, a następne w porządku wzrastających ograniczeń to **B (B1, B2, B3)** oraz **A1.**

Kategoria D: zapewnia minimalny poziom ochrony. Zawiera tylko jedną klasę, w której występują systemy oceniane, ale nie spełniające wymagań klas wyższych

Kategoria C: ochrona dyskrecjonalna, poprzez kontrolę zdarzeń.
W tej kategorii za poufność informacji odpowiada użytkownik.

C1 - Dyskrecjonalna ochrona. Zabezpieczenia indywidualnej identyfikacji użytkownika i zapewnienie niedostępności jego danych dla innych użytkowników systemu. Klasa ta przeznaczona jest dla użytkowników o jednakowym poziomie niejawności (POUFNE) danych.

C2 - Kontrolowana ochrona dostępu.
Klasa ta przeznaczona jest do wszystkich zastosowań komercyjnych administracji państwowej. Departament Obrony USA uznał tę klasę za wystarczającą dla danych nie wykraczających poza stopień POUFNE.

Kategoria B: Obowiązkowa ochrona. Wymogiem tej kategorii jest wymuszanie ustalonych zasad obowiązkowej kontroli dostępu.
Kategoria ta zapewnia wielopoziomowość zabezpieczeń.

B1 - Ochrona bazująca na etykietach bezpieczeństwa (musi spełniać wymagania C2). Najwyższy komercyjny poziom zabezpieczeń, polegający na hierarchii nadawania uprawnień (użytkownik nie może ich zmienić), a ponadto zapewniona jest także separacja pamięci operacyjnej przeznaczonej dla programów poszczególnych użytkowników.

B2 - Ochrona strukturalna. Poza cechami klasy B1 wymaga:

- ścisłej strukturalizacji części jądra systemu odpowiedzialnego za realizację funkcji zabezpieczających;
- kontroli kanałów komunikacyjnych systemu informatycznego, wraz ze śledzeniem ich adresów;
- sformalizowanej matematycznie dokumentacji zabezpieczeń;
- podziału roli głównego administratora systemu wśród kilku administratorów o mniejszych uprawnieniach.

Klasa ta zalecana jest do stosowania w systemach narażonych na dywersyjną penetrację.

B3 - Domeny ochrony. Posiada wszystkie cechy klasy B2 a ponadto posiada zminimalizowane jądro systemowe odpowiedzialne za realizację funkcji zabezpieczeń. System zabezpieczeń podzielony jest na małe strefy bezpieczeństwa pozwalające na łatwą analizę i testowanie, Wyposażony jest w funkcje administrowania bezpieczeństwem, śledzenia dostępu i procedury odtwarzania poawaryjnego.

Klasa ta zalecana jest do stosowania w systemach narażonych na dywersyjną penetrację.

Kategoria A: Ochrona weryfikowana. Charakteryzuje się zastosowaniem sformalizowanych metod weryfikacji wymagań ochrony.

A1 - Weryfikowane projektowanie. Składa się tylko z jednej klasy **A1,** jest to najwyższy poziom zabezpieczeń systemu komputerowego, który funkcjonalnie odpowiada klasie B3, z tą różnicą, że wszystkie testy systemu grupy A1 dają wynik co najmniej dostateczny.

Programowe metody ochrony zbiorów są na pewnych etapach procesu przetwarzania jedynymi metodami, które mogą skutecznie chronić zbiory informacji poprzez:

a) Kontrolę dostępu do sprzętu informatycznego, a w tym:

- identyfikacja i hasła dostępu (każdy użytkownik posiada przydzielony identyfikator wraz z hasłem bez którego nie może rozpocząć pracy w systemie);
- ograniczenie dostępu do danych (właściciel danych ogranicza dostęp do nich innym użytkownikom);
- monitorowanie pracy w czasie sesji użytkownika (pozwala na odtworzenie wszystkich poleceń dla systemu, a w tym wykrycie rozkazu niewłaściwie wydanego lub użytego), systemowe jądro ochrony - ewidencja zdarzeń w systemie;
- hierarchiczny dostęp do danych (ustalenie wielu szczebli uprawnień dostępu, z których użytkownicy o wyższym statusie uprawnień mają nieograniczoną możliwość ingerencji w dane użytkowników o niższym statusie);
- zabezpieczenie indywidualne (specjalistyczne oprogramowanie).

b) Ochronę danych w tym:

- zabezpieczenie przed modyfikacją danych;
- kontrola zmian dokonywanych w programie;
- kontrola ładowanie programów i danych;
- kontrola transmisji danych;
- przechowywanie danych w postaci zaszyfrowanej;

c) Kontrolę systemową w tym:

- kodowanie programów użytkowników;
- adresy przesyłane pomiędzy użytkownikami powinny być adresami logicznymi, rzeczywiste adresy nie mogą być akceptowane.

Szczegółowa architektura zabezpieczeń przedstawiona została w **polskiej normie PN-92 T-20001/02** pod tytułem *„Współdziałanie systemów otwartych (OSI) Podstawowy Model Odniesienia Architektura Zabezpieczeń"*

2.2.4.6. Ogólne założenia na ochronę informacji w sieciach transmisji danych i w komputerowych terminalach abonenckich

Terminal abonencki (stacja robocza), serwer sieci oraz instalacja sieciowa powinny spełniać ogólne wymagania na podsystem ochrony kryptograficznej, a ponadto:

a) w zakresie redukcji emisji ujawniającej;

b) *w zakresie ochrony programowej (dostępu)* - zapewnienie ochrony na poziomie klasy B3[1)] w zależności od klasy zastosowanego terminala (np. komputer typu IBM) tzn. sieć oraz terminal abonencki muszą posiadać:

- system indywidualnych (dla każdego użytkownika) identyfikatorów i haseł dostępu do terminala;
- możliwość ograniczenia przez użytkownika dostępu do swoich danych;
- system monitorowania w czasie pracy systemu oraz sesji poszczególnych użytkowników oraz system alarmowy i dziennik zdarzeń w systemie - pozwoli to na wykrycie rozkazów niewłaściwie wydanych i użytych, a także wykryje i powiadomi o próbie nielegalnego dostępu do systemu;
- hierarchiczny dostęp do danych - tzn. wieloszczeblowość uprawnień, ograniczone i zamknięte grupy użytkowników.

c) w zakresie ochrony kryptograficznej:

1) posiadać wbudowany, indywidualny dla terminala:

- moduł szyfrujący dane zawarte na nośnikach, zawierający elastyczny system kluczowy (czas obowiązywania klucza) i posiadający elementy zabezpieczeń przed dekonspiracją.
- moduł bezpieczeństwa terminala.

[1)] „Kryteria oceny bezpieczeństwa systemów informatycznych" - tzw. Orange Book Departament Obrony USA 1983 r.

2) transmitowane dane muszą być szyfrowane kluczem sesyjnym (każdorazowo innym) i powinny zawierać elementy podpisu cyfrowego w celu uwierzytelnienia informacji i korespondenta.

d) w zakresie ochrony fizycznej:

- terminal (serwer sieci) musi posiadać mechanizm pozwalający na (tam gdzie to jest możliwe) wyjęcie dysku „twardego" i modułu szyfrującego celem zabezpieczenia systemu przed dekonspiracją (w czasie pozostawienia terminala bez nadzoru, przechowywania, magazynowania itp.).

  W innym przypadku terminal musi być pod stałym nadzorem użytkownika;

  - w czasie pracy terminala muszą być wyznaczone strefy ochronne wokół pomieszczeń, aparatowni, wozów dowodzenia, itp., w których zainstalowane zostaną terminale[2)].

2.2.5. Ochrona techniczna (fizyczna)

W obszarze tym przyjmuje się założenie, że ograniczenie możliwości poruszania się osób nieuprawnionych po obiektach, w których rozwijane i instalowane są systemy komputerowe, osprzęt sieciowy i teletransmisyjny, a także kontrola ruchu osób uprawnionych, w zdecydowany sposób wpływa na poprawę stanu bezpieczeństwa systemów teleinformatycznych i sieci komputerowych.

Planowane rozwiązania powinny stwarzać szczelny system ochrony obiektów i sprzętu przed nieuprawnionym dostępem. Wybór zastosowanych środków powinien uwzględniać ważność informacji przetwarzanej i przechowywanej w systemie, specyfikę obiektu oraz koszty ochrony.

Ochronę fizyczną obiektów (kontrola dostępu) organizuje się z wykorzystaniem:

- rozwiązań tradycyjnych;

obejmujących - służby (dyżurne, ochronne), warty (wojskowe i cywilne lub wyspecjalizowane agencje ochrony), portierów, dozorców itp.;

- środków technicznych;

przede wszystkim - ogrodzenia, mechaniczne urządzenia zabezpieczające (zamki, blokady, kraty), techniczne urządzenia sygnalizacyjne i alarmowe, systemy obserwacji telewizyjnej, łączność dwustronna, oświetlenie, wieże obserwacyjne, strefy ochronne, umocnienia inżynieryjne.

- rozwiązań mieszanych;

obejmujących elementy rozwiązań tradycyjnych oraz środki techniczne.

[2)] wielkość strefy bezpieczeństwa zostanie określona po przebadaniu modelu terminala na poziom emisji ujawniającej.

2.2.5.1. Ogólne założenia na ochronę techniczną Zintegrowanej Sieci Telekomunikacyjnej i Zautomatyzowanego Systemu Dowodzenia

Ochrona techniczna powinna obejmować organizację i kontrolę:

- zabezpieczenia WD, WDSz i aparatowni łączności;
- okablowywania i wprowadzania łączy z punktu widzenia wymagań bezpieczeństwa i ochrony;
- systemu ochrony przez wartowników;
- stref ograniczonego dostępu;
- wytyczenie stref ochrony wokół wozów dowodzenia i aparatowni, w których przetwarzana jest informacja niejawna;
- zabezpieczanie instalacji przed klęskami żywiołowymi;
- zapewnianie niezawodności źródeł energii elektrycznej i klimatyzacji;
- stosowanie środków ochrony przed nieuprawnionym dostępem do sprzętu i programów (karty magnetyczne, "zworki programowe", itp.);

Ponadto urządzenia PBŁiOI powinny być instalowane przez operatora lub technika mających odpowiednie przygotowanie techniczne oraz stosowne zezwolenia, a przewóz ich musi być pod kontrolą upoważnionych pracowników na zasadach obowiązujących w „Przepisach o gospodarce materiałowej sprzętem łączności specjalnej i utajnionej w SZ RP".

X X X

Wydrukowano w 5 egz.
Egz. nr 1-4 – Bibl. Jawna AON
Egz. nr 5 – Archiwum AON
Druk. B.K. 6.03.2000 r.