AKADEMIA
OBRONY
NARODOWEJ

AON 5598/2004

Józef JANCZAK
Grzegorz ŚWIDZIKOWSKI

BEZPIECZEŃSTWO INFORMACJI W WOJSKOWYM SYSTEMIE TELEKOMUNIKACYJNYM

WARSZAWA 2004

AKADEMIA OBRONY NARODOWEJ

WYDZIAŁ WOJSK LĄDOWYCH
INSTYTUT DOWODZENIA

AON 5598/04

Józef JANCZAK
Grzegorz ŚWIDZIKOWSKI

BEZPIECZEŃSTWO INFORMACJI W WOJSKOWYM SYSTEMIE TELEKOMUNIKACYJNYM

WARSZAWA 2004

Recenzent: płk dr hab. inż. Józef MICHNIAK – profesor nadzwyczajny AON

Praca zbiorowa pod kierownictwem i redakcją naukową
płk dr hab. inż. Józefa JANCZAKA

Skład komputerowy:
ppłk mgr inż. Grzegorz ŚWIDZIKOWSKI

Druk i oprawa:
Akademia Obrony Narodowej – Wydział Wydawniczy, zam. nr 1498/2003

Spis treści

Wstęp

płk dr hab. inż. Józef Janczak, ppłk mgr inż. Grzegorz Świdzikowski

Działalność i funkcjonowanie prawie każdej instytucji państwowej, gospodarczej czy społecznej związana jest z opracowywaniem, przechowywaniem i przesyłaniem informacji za pośrednictwem systemów telekomunikacyjnych i informatycznych.

Aktualnie, w epoce budowy społeczeństwa informacyjnego wzrasta bardzo szybko znaczenie informacji przesyłanej w postaci elektronicznej, która powoli, ale systematycznie wypiera tradycyjne formy przekazu wiadomości – w tym usługi głosowe oraz dokumenty papierowe.

Przewartościowania w zakresie technik przekazu informacji stały się możliwe dzięki postępowi w dziedzinie elektroniki. Jednak zastosowanie nowoczesnych cyfrowych środków technicznych w systemach telekomunikacyjnych czy też informatycznych niesie ze sobą wymierne zagrożenia, które wpływają na bezpieczeństwo procesów wytwarzania, przetwarzania, przesyłania oraz przechowywania w nich informacji.

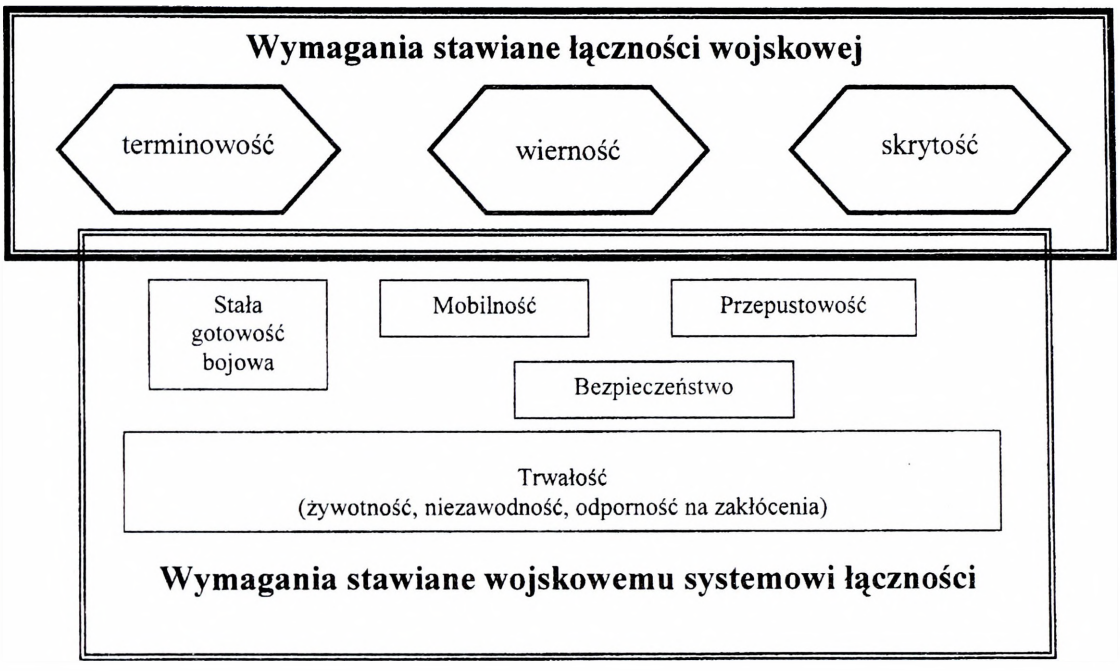
Ważność i aktualność tej problematyki ma szczególne znaczenie w Siłach Zbrojnych RP ze względu na fakt, że wymiana informacji za pośrednictwem technicznych środków łączności i informatyki dotyczy obronności kraju, a w szerszym ujęciu bezpieczeństwa państwa. Informacje te z reguły stanowią tajemnicę państwową lub służbową i z tego względu ustawowo podlegają ochronie.

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

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

Oddziaływanie takie ma wieloraki charakter i może być stosowane wieloma sposobami przy użyciu różnych sił i środków, których zasadniczym zadaniem jest uniemożliwienie realizacji podstawowego celu funkcjonującego systemu tj. obiegu informacji w systemie dowodzenia i sterowania środkami rażenia. Utrudnienie lub wręcz sparaliżowanie systemu dowodzenia wojskami osiąga się m.in. poprzez rażenie ogniowe we wszelkich dostępnych formach i metodach stanowisk dowodzenia (SD), ale także węzłów łączności SD, pomocniczych węzłów łączności (PWŁ) oraz innych wrażliwych elementów systemu

telekomunikacyjnego. Ich fizyczne zniszczenie bądź obezwładnienie radioelektroniczne, będzie zasadniczo wpływało na realizację wymagań przedstawionych na rysunku 1. stawianych zarówno łączności wojskowej jak i wojskowemu systemowi łączności.



Rys. 1. Wymagania stawiane łączności wojskowej i wojskowemu systemowi łączności

Dostępna z tej dziedziny literatura zawiera i szeroko opisuje zasady oraz skutki oddziaływania ogniowego bądź radioelektronicznego na wojskowy system telekomunikacyjny.

Z tej przyczyny opracowanie niniejsze poświęcone zostało zasadom organizacji ochrony informacji w wojskowym systemie telekomunikacyjnym, które wynikają z ustawy „O ochronie informacji niejawnych" z dnia 22 stycznia 1999 roku. W myśl tej ustawy zmianie uległy bowiem wymagania oraz wprowadzone zostały nowe płaszczyzny wymuszające zapewnienie w nich bezpieczeństwa informacjom stanowiącym tajemnicę państwową i służbową zarówno w wymiarze narodowym jak i sojuszniczym.

Problematyce powyższej poświęcono również uwagę w Strategii Bezpieczeństwa RP: *W związku z wejściem do Sojuszu Północnoatlantyckiego wzrosła odpowiedzialność Polski za ochronę informacji niejawnych nie tylko krajowych, ale i powierzonych nam przez sojuszników. Sprawność i bezpieczeństwo systemów przekazywania i przetwarzania*

informacji odgrywa coraz ważniejszą rolę w funkcjonowaniu struktur państwa i społeczeństwa.

Należy podkreślić, że w przeciwieństwie do okresu minionego, w którym ochrona informacji (bezpieczeństwo łączności i informatyki) dotyczyła niemal wyłącznie resortów obrony narodowej i spraw wewnętrznych oraz wybranych dziedzin gospodarki, to aktualnie obowiązujące akty prawne obejmują wszelkie dziedziny życia, w których występują lub mogą być wykorzystywane informacje o różnych klauzulach tajności.

Modyfikacji i przewartościowaniu uległo też samo pojęcie bezpieczeństwa systemów łączności i informatyki obowiązujące w Siłach Zbrojnych RP, które do niedawna obejmowało swoim zakresem takie obszary jak rozpoznanie radioelektroniczne czy działalność obcych służb wywiadowczych.

Intencją autorów niniejszego opracowania jest przedstawienie na kanwie zagrożeń dla informacji w wojskowych systemach telekomunikacyjnych zbioru odpowiednio uzasadnionych przedsięwzięć organizacyjno-eksploatacyjnych, które w myśl aktualnie obowiązujących aktów normatywnych będą przeciwdziałać tym zagrożeniom a zarazem zapewnią wymagany poziom bezpieczeństwa systemu.

Opracowanie składa się ze wstępu, pięciu rozdziałów merytorycznych, zakończenia oraz wykazu literatury i podstawowych dokumentów normatywnych obowiązujących w tym zakresie.

W **rozdziale pierwszym,** celem wprowadzenia do problematyki bezpieczeństwa w wojskowych systemach telekomunikacyjnych i informatycznych, zamieszczono podstawowe definicje i pojęcia, które obowiązują w dziedzinie ochrony informacji wytwarzanej, przetwarzanej, przechowywanej lub przesyłanej za pomocą technicznych środków łączności i informatyki.

Rozdział drugi poświęcony został identyfikacji oraz charakterystyce współczesnych zagrożeń dla bezpieczeństwa informacji w wojskowych systemach telekomunikacyjnych i informatycznych. Szczególną uwagę zwrócono na zagrożenia wewnętrzne, zewnętrzne oraz fizyczne. Uwzględniono ponadto problemy wynikające z niekontrolowanego (ubocznego) promieniowania elektromagnetycznego, które emituje każde urządzenie łączności i informatyki. W dalszej części rozdziału przedstawiono zagrożenia dla bezpieczeństwa informacji w świetle stosowanych środków ochrony. Rozważaniami objęto zagrożenia pochodzące ze strony rozwiązań organizacyjnych, personalnych, fizycznych i technicznych.

W **rozdziale trzecim** przedstawiono problematykę dotyczącą potrzeb opracowywania oraz wdrażania polityki bezpieczeństwa informacji w wojskowych systemach

telekomunikacyjnych i informatycznych. Przedstawiono w nim, a następnie scharakteryzowano, poszczególne elementy składowe polityki bezpieczeństwa.

Rozdział czwarty w całości poświęcono organizacji i administrowaniu bezpieczeństwem na przykładzie aktualnie występujących w strukturze Sił Zbrojnych RP organów bezpieczeństwa łączności i informatyki.

W **rozdziale piątym**, zdaniem autorów najważniejszym, zawarto metody i możliwe do zastosowania środki ochrony informacji w wojskowych systemach telekomunikacyjnych oraz informatycznych. Rozważaniami objęto, adekwatnie do zagrożeń zidentyfikowanych w rozdziale drugim, odpowiednio uzasadnione przedsięwzięcia organizacyjne, personalne, techniczne i fizyczne.

Treści opracowania kierowane są do studentów i słuchaczy kursów Akademii Obrony Narodowej oraz osób funkcyjnych pracujących w strukturach organów łączności i informatyki różnych szczebli dowodzenia, których przedmiotem zainteresowania jest problematyka bezpieczeństwa informacji w wojskowych systemach telekomunikacyjnych i informatycznych.

Zdaniem autorów wiedza zawarta w opracowaniu może być przydatna specjalistom różnych rodzajów wojsk i służb, a także poza sferą militarną, bowiem w warunkach pokojowych istnieje również potrzeba zapewnienia bezpieczeństwa informacji w systemach telekomunikacyjnych i informatycznych różnego przeznaczenia.

1. Podstawowe pojęcia z zakresu bezpieczeństwa wojskowych systemów łączności i informatyki

ppłk mgr inż. Grzegorz Świdzikowski

Każde państwo w dobie globalizacji oraz budowy społeczeństwa informacyjnego musi oprócz tradycyjnie znanej polityki bezpieczeństwa (np. bezpieczeństwo publiczne, obronność) posiadać politykę określającą sposoby i zasady wykorzystania informacji, łącznie z jej przetwarzaniem, przechowywaniem, dystrybucją i prezentacją, niezależnie od wymagań dotyczących jej bezpieczeństwa czy też bezpieczeństwa systemów telekomunikacyjnych i informatycznych.

Stąd też powstało i egzystuje pojęcie polityki bezpieczeństwa informacji, które definiowane jest różnie zarówno przez poszczególne państwa jak i instytucje. Przykładowo Unia Zachodnioeuropejska w „Przepisach bezpieczeństwa UZE – RS 100" (1996 r.) politykę bezpieczeństwa informacji definiuje jako przeciwdziałanie zagrożeniom przypadkowej lub celowej utraty poufności, integralności lub dostępu do informacji. Inna definicja zawarta w dokumentach normatywnych Departamentu Obrony USA przekazana na spotkaniu AFCEA Roma Symposium and Expositiom w 1994 r. określa politykę bezpieczeństwa informacji jako zestaw praw, reguł i zasad tworzenia, dystrybucji, użytkowania i przechowywania informacji niejawnych.

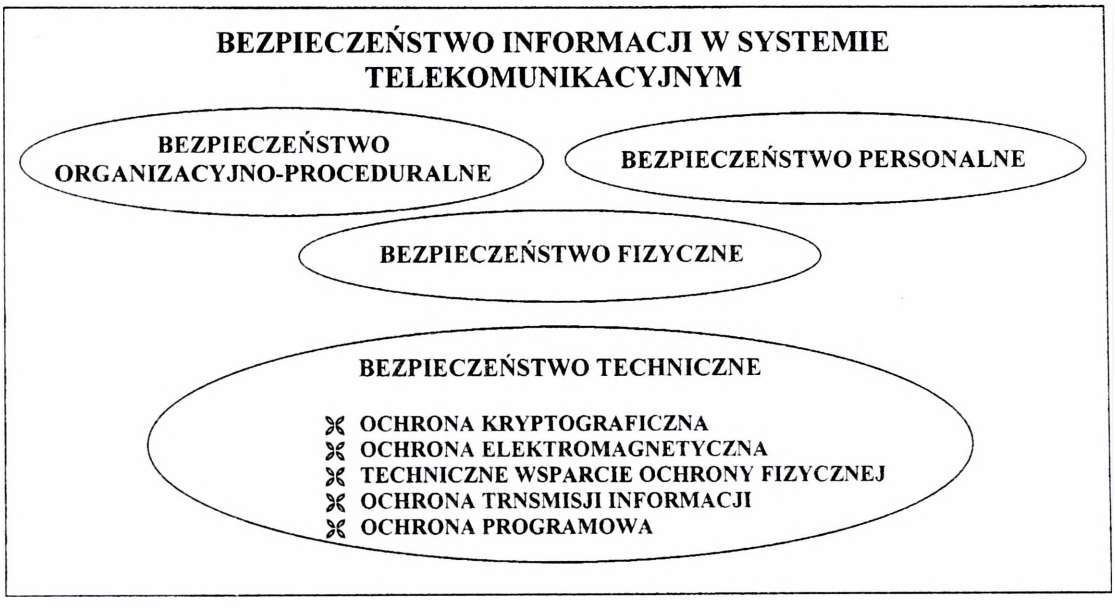
W niniejszym opracowaniu do dalszych rozważań autorzy przyjęli następującą definicję:

- polityka bezpieczeństwa informacji stanowi zestaw praw, reguł i praktycznych doświadczeń regulujących sposób zarządzania, ochrony i dystrybucji informacji niejawnej zarówno wewnątrz jak i na zewnątrz określonego organu dowodzenia, którego nieodłącznym elementem jest system łączności i informatyki.

Z uwagi na sposób przekazywania informacji system ten dzieli się na dwa zasadnicze elementy tj. podsystem telekomunikacyjny oraz podsystem wojskowej poczty polowej. Ze względu na ograniczenie nakreślone tematem, w dalszej części opracowania rozważane będą problemy dotyczące części telekomunikacyjnej i informatycznej, stanowiącej określoną całość - a więc system.

W Siłach Zbrojnych RP ochrona zasobów informacyjnych w systemie telekomunikacyjnym i informatycznym ma na celu zapewnienie bezpieczeństwa łączności

i informatyki. Pod tym pojęciem rozumie się całokształt działalności zmierzającej do uniemożliwienia przypadkowego lub celowego ujawnienia informacji niejawnej, wytwarzanej, przetwarzanej, przechowywanej lub przesyłanej w procesie dowodzenia za pomocą technicznych środków łączności i informatyki, poprzez zastosowanie w sposób kompleksowy technicznych, personalnych, fizycznych i organizacyjno-proceduralnych środków ochrony. Ogólny podział środków bezpieczeństwa stosowanych w systemie telekomunikacyjnym i informatycznym przedstawiono na rysunku 2.



Rys. 2. Ogólny podział środków bezpieczeństwa w systemie telekomunikacyjnym i informatycznym

Zasady i warunki stosowania poszczególnych środków bezpieczeństwa informacji w wojskowym systemie telekomunikacyjnym opisane zostaną w kolejnych rozdziałach niniejszego opracowania.

Środki i metody ochrony informacji w systemie telekomunikacyjnym lub informatycznym można zdefiniować jako przedsięwzięcia techniczne i administracyjne służące zabezpieczeniu poszczególnych elementów systemu, a w tym technicznych środków łączności oraz informatyki, w celu zapewnienia ochrony interesów instytucji oraz poufności danych.

Zagrożenia bezpieczeństwa informacji w systemie telekomunikacyjnym lub informatycznym definiuje się jako zdarzenia przypadkowe (losowe) lub działania celowe,

które mogą spowodować przesłanki do legalnego lub nielegalnego ujawnienia informacji, jej modyfikacji, zniszczenia lub kradzieży.

Mając na uwadze zagrożenia bezpieczeństwa informacji przekazywanej za pomocą technicznych środków łączności i informatyki Dyrektywa Bezpieczeństwa AD-70-1-PL definiuje je w sposób następujący:

Zagrożenia dla systemu telekomunikacyjnego lub informatycznego mogą wynikać ze strony każdej osoby, która usiłuje uzyskać dostęp do informacji i posiada do tego wystarczającą wiedzę i doświadczenie.

Z kolei ochrona informacji to wszelkie działania, które chronią przed zagrożeniami, działaniami szkodliwymi lub niebezpiecznymi.

Natomiast zabezpieczenia informacji to zastosowane środki i metody zabezpieczające.

Należy nadmienić, że pojęcie bezpieczeństwo informacji jest pojęciem bardzo szerokim obejmującym w sobie wszystkie aspekty z zakresu ochrony informacji, takie jak podatność, zagrożenia, ryzyko, zarządzanie i zabezpieczenia. W odniesieniu do systemów telekomunikacyjnych lub informatycznych bezpieczeństwo określane jest jako definiowanie, osiąganie i utrzymywanie sześciu podstawowych cech:

- **poufność** – dostęp do informacji musi być ograniczony jedynie do grona uprawnionych użytkowników;
- **integralność** – informacja musi być zachowana w swej oryginalnej postaci, jej legalne aktualizowanie bądź usuwanie może być realizowane jedynie przez upoważnione osoby;
- **dostępność** – informacja musi być dostępna na każde żądanie uprawnionego użytkownika;
- **rozliczalność** - fizyczny dostęp do informacji może być przypisany tylko temu uprawnionemu użytkownikowi, który z niej korzystał;
- **autentyczność** – tożsamość (pochodzenie) informacji lub podmiotu z nią związanego (np. wysyłającego informację) jest zgodna z zadeklarowaną;
- **niezawodność** – zachowanie i skutki działania (elementów lub urządzeń systemu zawierającego informacje ochraniane) są zgodne z zamierzonymi.

Z przedstawionych powyżej definicji wynika, że bezpieczeństwo informacji w wojskowym systemie telekomunikacyjnym lub informatycznym to miara stopnia skuteczności zastosowanych środków i metod ochrony w stosunku do istniejących

i prognozowanych zagrożeń jej bezpieczeństwa, które polega na zabezpieczeniu danych przed przypadkowym lub umyślnym zniszczeniem, kradzieżą, nielegalnym ujawnieniem a także nieuprawnioną modyfikacją.

Wojskowy system telekomunikacyjny lub informatyczny zapewnia wytwarzanie, przechowywanie oraz przekazywanie informacji na potrzeby systemu dowodzenia i kierowania środkami walki, które w większości opatrzone są określoną klauzulą tajności. Zgodnie z aktualnie obowiązującymi dokumentami normatywnymi informacje opatrzone nimi mogą stanowić tajemnicę państwową lub służbową.

Informacją niejawną stanowiącą tajemnicę państwową są dane, których 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. Wykaz rodzajów informacji niejawnych stanowiących tajemnicę państwową jest zawarty w ustawie „O ochronie informacji niejawnych" z dnia 22 stycznia 1999 r. Jest to katalog zamknięty, co oznacza, że tylko informacje zawierające dane ujęte w tym wykazie, mogą być oznaczone odpowiednio klauzulą „tajne" lub „ściśle tajne".

Różnica między klauzulami „ściśle tajne" a „tajne" została zdefiniowana przede wszystkim przez rozmiar szkód, jakie mogłoby spowodować nieuprawnione ujawnienie informacji. W przypadku informacji „ściśle tajne" jest to „istotne zagrożenie", „nieodwracalne lub wielkie straty" oraz „szkoda w wielkich rozmiarach". Natomiast w przypadku informacji opatrzonej klauzulą „tajne" – „zagrożenie" oraz „istotna szkoda".

Tajemnicą służbową objęte są informacje niejawne nie będące tajemnicą państwową, uzyskane w związku z czynnościami służbowymi albo wykonywaniem prac zleconych, których nieuprawnione ujawnienie mogłoby narazić na szkodę interes państwa, interes publiczny lub prawnie chroniony interes obywateli albo jednostki organizacyjnej. Kategoria ta obejmuje dwie klauzule: „poufne" i „zastrzeżone". Informacje niejawne oznacza się klauzulą „poufne" w przypadku, gdy ich nieuprawnione ujawnienie powodowałoby szkodę dla interesów państwa, interesu publicznego lub prawnie chronionego interesu obywateli. Natomiast klauzulę „zastrzeżone" stosuje się do informacji niejawnych, których nieuprawnione ujawnienie mogłoby spowodować szkodę dla prawnie chronionych interesów obywateli albo jednostki organizacyjnej.

Z punktu widzenia organizatora oraz osób funkcyjnych eksploatujących określony wojskowy system telekomunikacyjny lub informatyczny podstawowym determinantem wszelkich przedsięwzięć organizacyjnych i technicznych w zakresie zapewnienia

bezpieczeństwa informacji jest określenie maksymalnej klauzuli danych, które w tym konkretnym systemie będą wytwarzane, przetwarzane, przechowywane lub przesyłane. Stanowi bowiem podstawę do wstępnego określenia wymogów bezpieczeństwa zarówno w kontekście samego systemu jak i informacji, która może się w nim znajdować.

2. Zagrożenia bezpieczeństwa informacji w wojskowym systemie telekomunikacyjnym

ppłk mgr inż. Grzegorz Świdzikowski, płk dr hab. inż. Józef Janczak

Codzienne funkcjonowanie społeczności ludzkiej opiera się na komunikowaniu ludzi pomiędzy sobą lub przekazywaniu, odbiorze danych z otaczającej ich rzeczywistości. Wymiana jak i sam obieg informacji jest systematycznie udoskonalana przez człowieka. Temu służą systemy telekomunikacyjne, które w coraz większej mierze wykorzystują nowoczesne urządzenia łączności sprzęgnięte ze środkami informatycznymi. Dzięki nim między innymi uzyskano poprawę i możliwości wiernej i szybkiej transmisji różnych postaci danych.

Przebudowie narodowych sił zbrojnych towarzyszy wprowadzanie nowoczesnych systemów dowodzenia i kierowania środkami walki, które w znacznej mierze opierają się na cyfrowych systemach telekomunikacyjnych.

W codziennej działalności służbowej wykorzystuje się różne środki techniczne, które w ramach wojskowego systemu telekomunikacyjnego, obejmującego swoim zasięgiem całe państwo, zapewniają usługi wymiany lub przekazywania informacji. Informacje te przyjmują różną postać (np. foniczna, elektroniczna, dokument papierowy) i z reguły mając na uwadze charakter oraz obszar działalności sił zbrojnych opatrzone są odpowiednią klauzulą niejawności. Ich klasyfikacja obejmuje pełne spektrum klauzul zdefiniowanych w obowiązujących aktualnie dokumentach normatywnych.

Obecnie informacja stanowi istotny czynnik w ramach przygotowania i prowadzenia operacji oraz innych przedsięwzięć realizowanych przez siły zbrojne. Potencjalny przeciwnik stara się pozyskać informacje poprzez własne wyspecjalizowane jednostki rozpoznania radioelektronicznego oraz organa wywiadowcze, funkcjonujące w ramach każdego systemu obronnego państwa. Ich głównym zadaniem jest systematyczne zbieranie a następnie analiza wszelkiej informacji zarówno w okresie pokoju, kryzysu czy też wojny. Podczas prowadzenia walki zbrojnej wymienione uprzednio jednostki i organy wywiadu wspierane są przez jednostki rozpoznawcze wojsk operacyjnych.

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.

2.1. Charakterystyka i podział zagrożeń

We współczesnym wojskowym systemie telekomunikacyjnym elementami stanowiącymi potencjalne źródło ujawnienia informacji mogą być:

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

W dokumentach Dyrektywa Bezpieczeństwa AD-70-1-PL oraz „Metodyka opracowywania Szczególnych Wymagań Bezpieczeństwa systemu lub sieci teleinformatycznej" wyróżnia się następujące rodzaj zagrożeń:

- zagrożenia zewnętrzne;
- zagrożenia wewnętrzne;
- zagrożenia fizyczne.

Następstwem celowego bądź przypadkowego wystąpienia ww. rodzajów zagrożeń może być:

1. Utrata poufności informacji, którą należy rozumieć jako nieautoryzowane ujawnienie informacji przez nieuprawniony dostęp do systemu.
2. Utrata integralności informacji, którą należy rozumieć jako nieautoryzowaną modyfikację informacji oraz utratę prawidłowego i spójnego działania systemu.
3. Utrata dostępności, którą należy rozumieć jako odmowę autoryzowanego dostępu lub opóźnienie operacji krytycznych pod względem czasu i celu.

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 telekomunikacyjnego.

2.2. Sabotaż i zagrożenia nieumyślne

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:

1. Sabotaż i zagrożenia nieumyślne.
2. Infiltracja.

Do grupy tej 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);
– dezintegracji lub „destrukcji informatycznej" (wirusy, bomby logiczne, konie trojańskie, itp.)
– fizycznych czynników destrukcyjnych i swoistego oddziaływania ludzi.

Za główną przyczynę tego rodzaju powstałych szkód autorzy uznali 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 realizowana jest różnymi metodami i środkami, a szczególnie poprzez „przenikanie" do celowo wybranych (najbardziej wrażliwych lub słabo chronionych) elementów tego systemu.

Infiltrację możemy podzielić na:

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

b) 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.

Inne zagrożenie wymienione w tej grupie to sabotaż. Jego zasadniczym celem jest wywołanie 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 także nazywamy dywersją.

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

a) bierną – śledzenie informacji w zadanym celu jej zdobycia lub ustalenie częstotliwości wymiany informacji (np. zajętość kanału transmisyjnego);

b) czynną – planowe i świadome poszukiwanie [illegible] uzyskania dostępu do zasobów systemu, np. możliwości ingerencji w najważniejsze elementy struktury systemu.

W wyniku infiltracji biernej przeciwnik może zagrażać poufności (tajności) informacji lub danych. Nie może on jednak wpływać na ich treść.

Najczęściej spotykane i stosowane metody infiltracji biernej to:

– przechwyt elektromagnetyczny, czyli analiza sygnału emitowanego [illegible] 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 odpadów (np. wydruki komputerowe lub teledalekopisowe) oraz analiza elektronicznych nośników informacji;

– stosowanie ukrytych czujników.

programami szpiegującymi. Zajmują się one wyszukiwaniem, opracowywaniem i wykorzystaniem nowoczesnych środków i metod ochrony informacji oraz zachowania jej w ścisłej tajemnicy (w Stanach Zjednoczonych program o nazwie „TEMPEST").

Słowo TEMPEST stało się swego rodzaju kryptonimem używanym dla określenia ogółu zagadnień związanych z problemem emisji ujawniającej. Dało się to szczególnie zauważyć w publikacjach anglojęzycznych. 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 czy pól indukowanych w kablach zasilających odległość ta wynosi ok. 100 - 150 m.

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.

2.4. Zagrożenia informacji w świetle stosowanych środków bezpieczeństwa

Podziału zagrożeń dla bezpieczeństwa informacji w systemie telekomunikacyjnym czy informatycznym można dokonywać w wielu aspektach i płaszczyznach. Z tej przyczyny celowym, a nawet wskazanym jest dokonanie ich analizy z punktu widzenia możliwych lub stosowanych środków zapewniających bezpieczeństwo informacji. W problematyce tego tematu zarówno w środowisku cywilnym jak i wojskowym przyjmuje się następujące grupy środków bezpieczeństwa:

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

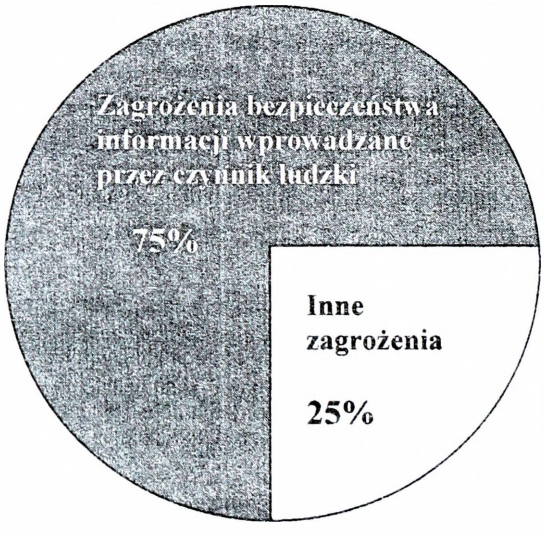
Każda organizacja (instytucja) państwowa lub prywatna, a w tym kontekście szczególnie siły zbrojne, w procesie wymiany informacji za pomocą technicznych środków łączności i informatyki musi mieć na uwadze fakt, że dane te przekazywane w sposób chaotyczny i niezorganizowany mogą przynieść więcej szkody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

Ograniczenie zagrożeń w tym zakresie zapewnia przygotowanie i wdrożenie przez właściwe organa dla danej jednostki organizacyjnej polityki bezpieczeństwa, której celem jest stworzenie podstaw, procedur i wymagań niezbędnych dla zapewnienia właściwej ochrony wytwarzanym, przetwarzanym, przechowywanym lub przesyłanym w systemie informacjom. Polityka bezpieczeństwa 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** (rysunek 3.). Opierając się na przykładowej statystyce zagrożeń opracowanej przez Icove D., Seger K., von Storch (A Crimefighter Handbook, O'Reilly&Associates) około 75% problemów stwarza nieuczciwy bądź niezadowolony personel. 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).



Rys. 3. Statystyka zagrożeń wg poglądów Icove D., Seger K., von Storch

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 **zagrożenia fizyczne** w kontekście systemu telekomunikacyjnego i informatycznego nieodłącznie kojarzyć się mogą ze zniszczeniem infrastruktury telekomunikacyjnej, urządzeń bądź samych obiektów, w których poszczególne elementy

systemu są zainstalowane. Ich zniszczenie może nastąpić wskutek celowego działania przeciwnika bądź klęsk żywiołowych takich jak:

- pożar;
- powódź;
- trzęsienie ziemi;
- itp.

Ponadto w tej grupie zagrożeń należy uwzględnić następujące elementy takie jak:

- 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 omówienie zagrożeń wynikających z niepożądanej emisji ujawniającej (elektromagnetycznej) w rozdziale 2.3. ten aspekt problemu zostanie pominięty.

W codziennej działalności służbowej każdy z nas, choć być może nie w pełni tego świadom, korzysta ze stacjonarnego lub mobilnego systemu telekomunikacyjnego Sił Zbrojnych RP przy okazji kazdorazowego podniesienia np. słuchawki aparatu telefonicznego. Wymiana informacji podczas rozmowy dotyczy szerokiej gamy obszarów czy też różnych spraw. Rzadko jednak użytkownicy uświadamiają sobie, że zarówno w warunkach

stacjonarnych jak i polowych mają do czynienia z urządzeniami końcowymi systemu telekomunikacyjnego lub informatycznego, który zapewnia nam wymianę informacji jawnej lub klasyfikowanej.

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

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

Innym zagrożeniem dla bezpieczeństwa informacji z punktu widzenia kryptografii jest stosowanie w systemie telekomunikacyjnym urządzeń i/lub dokumentów kluczowych niezgodnie z ich przeznaczeniem oraz 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:

1. Nieautoryzowany przechwyt (przejęcie) informacji.
2. Zakłócanie.
3. Interferencja.
4. Analiza ruchu telekomunikacyjnego.
5. 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 zarządzaniem 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 tego typu 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 mobilny 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.

3. Polityka bezpieczeństwa informacji w systemie telekomunikacyjnym

ppłk mgr inż. Grzegorz Świdzikowski

Polityka bezpieczeństwa informacji w Polsce opiera się o dokumenty normatywne – ustawy, rozporządzenia oraz szczegółowe wytyczne i instrukcje. Na ich podstawie można pokusić się o jej zdefiniowanie jako udokumentowany zbiór zasad, procedur i zarządzeń, który precyzyjnie charakteryzuje sposoby ochrony informacji w systemie telekomunikacyjnym lub informatycznym.

Polityka bezpieczeństwa informacji winna przyjmować sobie za cel stworzenie podstaw dla metod zarządzania, procedur i wymagań, które umożliwią zminimalizowanie zagrożenia niekontrolowanego ujawnienia informacji prawnie chronionych lub tych, które z punktu widzenia organizacji (instytucji) ochronie mają podlegać.

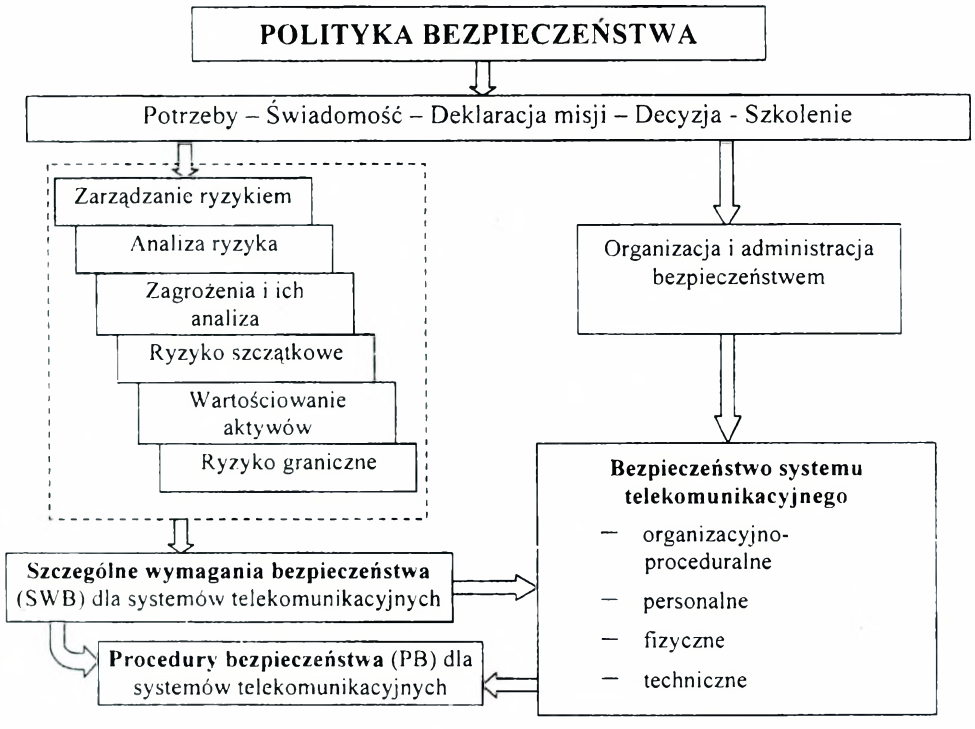
Bezpieczeństwo informacji nie odnosi się w tym miejscu tylko i wyłącznie do procesu przetwarzania, przechowywania lub przesyłania informacji w samym systemie telekomunikacyjnym czy informatycznym. Jej ochrona powinna obejmować kompleksowo poszczególne etapy „życia informacji" i trwać od momentu jej wytworzenia do całkowitego zniszczenia lub utraty znaczenia jako informacji podlegającej ochronie (np. przeklasyfikowanie lub dezaktualizacja).

Przy tworzeniu w Siłach Zbrojnych RP polityki bezpieczeństwa dla systemów telekomunikacyjnych czy innych systemów informacyjnych warto kierować się powszechnie akceptowanymi zasadami:

1. Bezpieczeństwo systemu telekomunikacyjnego (informatycznego) wspiera cel działania Sił Zbrojnych RP, a w tym poszczególnych jednostek organizacyjnych resortu obrony narodowej). Środki bezpieczeństwa są wprowadzane po to, aby chronić te zasoby systemu, które mają dla sił zbrojnych wartość lub objęte są klauzulą niejawności. W tym sensie stanowią istotny element działania Ministerstwa Obrony Narodowej.
2. Bezpieczeństwo systemu telekomunikacyjnego (informatycznego) jest integralnym elementem sprawnego kierowania . Ochrona systemu może być równie ważna, jak ochrona innych aktywów resortu obrony narodowej (uzbrojenie, finanse, itp.) i dlatego zasługuje na troskę ze strony kadry kierowniczej resortu lub dowództwa jednostki wojskowej.

3. Przy wyborze środków zabezpieczeń należy zawsze brać pod uwagę koszty i oczekiwane korzyści. Wyznaczony poziom bezpieczeństwa powinien odpowiadać wartości systemu oraz prawdopodobieństwu, powadze i zakresowi możliwych naruszeń tego bezpieczeństwa.
4. Organizator ponosi odpowiedzialność za bezpieczeństwo swego systemu. W przypadku świadczenia usług na zewnątrz klient takiego systemu musi mieć informacje o jego bezpieczeństwie oraz pewność, że system ten jest odpowiednio zabezpieczony.
5. Odpowiedzialność za bezpieczeństwo systemu oraz rozliczalność działań w systemie powinna być jasno i wyraźnie sprecyzowana.
6. Koncepcja bezpieczeństwa systemu lub systemów telekomunikacyjnych (informatycznych) powinna być całościowa i zintegrowana. Bardzo często efektywność funkcjonowania jednych mechanizmów zabezpieczenia zależy od prawidłowego wdrożenia innych mechanizmów. Zapewnienie odpowiedniego doboru procedur organizacyjnych i środków technicznych oraz właściwe zarządzanie nimi pozwala na uzyskanie efektu synergii. Efektywność zabezpieczeń zależy także od zarządzania systemem, uwarunkowań prawnych, zarządzania jakością. W bezpieczeństwo systemów telekomunikacyjnych muszą być wkomponowane i uwzględnione elementy tradycyjnego bezpieczeństwa i higieny pracy.
7. Poziom bezpieczeństwa systemu telekomunikacyjnego lub informatycznego powinien podlegać okresowej kontroli. System telekomunikacyjny czy informatyczny oraz środowisko, w którym działa zmienia się nieustannie. Wiele z tych zmian może w istotny sposób wpływać na zdefiniowany poziom bezpieczeństwa i funkcjonowanie tego systemu.
8. Czynnik ludzki jest jednym z podstawowych czynników wpływających na bezpieczeństwo systemu telekomunikacyjnego. Potrzeby bezpieczeństwa mogą w istotny sposób ograniczać prawo jednostki - użytkownika systemu - do prywatności lub inne prawa wynikające z zasad pełnienia służby w resorcie obrony narodowej. Dokonując wyboru środków bezpieczeństwa należy brać pod uwagę uwarunkowania społeczne, środowiskowe i kulturowe istniejące w danym zbiorowisku ludzkim i liczyć się z trudnościami w ich zaakceptowaniu.

Zasady powyższe stały się podstawą do wypracowania algorytmu zamieszczonego na rysunku 4., który przedstawia kolejne przedsięwzięcia (kroki) w procesie opracowywania polityki bezpieczeństwa informacji na potrzeby danej organizacji (instytucji).



Rys.4. Algorytm opracowywania polityki bezpieczeństwa

3.1. Co powinna uwzględniać polityka bezpieczeństwa

Zgodnie z opinią wyrażoną przez amerykański Narodowy Instytut Standardów i Technologii (NIST) poprawnie skonstruowana polityka bezpieczeństwa powinna uwzględniać następujące obszary związane z bezpieczeństwem systemów telekomunikacyjnych:

- identyfikacja i uwierzytelnianie;
- kontrola dostępu;
- śledzenie odpowiedzialności;
- badanie (audyt) stanu bezpieczeństwa;

- ochrona współdzielonych zasobów;
- dokładność ochrony;
- niezawodność ochrony;
- ochrona komunikacji.

Identyfikacja i uwierzytelnianie określają mechanizmy autoryzacji użytkowników w systemie. Mechanizmy te zaimplementowane są we wszystkich współczesnych sieciowych systemach operacyjnych oraz systemach dedykowanych na potrzeby Sił Zbrojnych RP, a ich działanie uwidacznia się żądaniem podania nazwy i/lub hasła użytkownika. Dla wzmocnienia niezawodności i siły uwierzytelniania osób podających się za prawowitych użytkowników skonstruowano wiele ciekawych rozwiązań technicznych opierających się na personalnych generatorach tymczasowych haseł bądź nawet bezpośrednim pomiarze danych antropometrycznych.

Kontrola dostępu sprowadza się do określenia praw poszczególnych osób do korzystania z zasobów systemu. Prawa te mogą zabraniać dostępu do określonych zasobów (plików, programów, urządzeń itp.) bądź ograniczać go tylko do podzbioru dozwolonych operacji, jakie użytkownik może na zasobach lub urządzeniach systemu wykonać. Mechanizmy zapewniające taką kontrolę mogą mieć różnorodną naturę, zależną od rodzaju chronionych zasobów. W grę wchodzą tu zarówno rozwiązania ograniczające fizyczny dostęp do nośników i urządzeń, jak również zabezpieczenia systemowe zaimplementowane w specjalistycznym lub dedykowanym oprogramowaniu.

Śledzenie odpowiedzialności polega na możliwości odtworzenia historii operacji wykonanych w systemie w powiązaniu z jednoznaczną identyfikacją użytkowników, którzy zainicjowali ich wykonanie oraz czasem wykonania. Również te operacje, które wykonano nielegalnie, omijając zabezpieczenia systemu, co uniemożliwia bezpośrednią identyfikację sprawcy muszą być śledzone w celu zbadania stopnia ich szkodliwości oraz przywrócenia pierwotnego stanu systemu.

Badanie stanu bezpieczeństwa systemu jest ważnym zadaniem, które winno być realizowane cyklicznie w celu utrzymywania zabezpieczeń systemu w stanie wysokiej gotowości. Ze względu na dynamicznie zmieniające się środowisko działania systemów,

wciąż wykrywane „dziury" w zabezpieczeniach oraz niesłabnącą pomysłowość włamywaczy – skuteczność wykorzystywanych zabezpieczeń powinna być ciągle monitorowana i poprawiana. Stąd rosnąca popularność systemów wykrywania włamań i testowania zabezpieczeń, które na zasadzie sprzężenia zwrotnego potrafią modyfikować ich konfigurację w celu uzyskania pewniejszej ochrony.

Ochrona współdzielonych zasobów stanowi rozwinięcie zagadnienia kontroli dostępu. Dotyczy zaś tej grupy zasobów, która z racji ich współdzielenia przez wielu użytkowników jest szczególnie wrażliwa na zachowania naruszające zasady dobrej współpracy i działania w dobrej wierze. Z tematem tym wiążą się dwa kolejne elementy podlegające kontroli polityki bezpieczeństwa: dokładność i niezawodność ochrony.

Dokładność i niezawodność ochrony powinny zapewnić systemowi odporność na wszelkie próby zmonopolizowania jego zasobów przez działającego nieudolnie bądź nierozważnie uprzywilejowanego użytkownika jak również oddalić groźbę przejęcia kontroli nad systemem przez osoby nieuprawnione w sytuacji kryzysowej lub udaremnić próbę infiltracji. Sytuacja taka może mieć miejsce w warunkach nietypowych, takich jak poważna awaria systemu zasilania bądź wystąpienie krytycznego błędu aplikacji użytkowej.

Ochrona transmisji jest problemem, który często mylnie utożsamiany jest z całokształtem bezpieczeństwa systemów telekomunikacyjnych. Rzeczywiście, jest to niezwykle ważny element każdej polityki bezpieczeństwa. Odnosi się bowiem do obszaru, w którym informacja opuszcza chroniony fizycznie obszar systemu po to, aby w sposób bezpieczny i niezawodny dotrzeć do odbiorcy. Zapewnienie poufności oraz integralności tych danych bądź informacji w dużej mierze zależne jest od doboru urządzeń ochrony stanowiących „granicę" systemu (ang. boundary protection devices). Różnorodność sprzętu technicznego lub aplikacji bezpieczeństwa, który można zastosować jako urządzenia wyjścia i wejścia z obszaru fizycznie chronionego systemu, daje szerokie pole manewru osobom funkcyjnym odpowiedzialnym za opracowanie a następnie wdrożenie polityki bezpieczeństwa w aspekcie ochrony transmisji danych lub informacji w systemie telekomunikacyjnym.

3.2. Zarządzanie ryzykiem

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,
- konsekwencje ataków,
- 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).

4. Organizacja i administracja bezpieczeństwem

ppłk mgr inż. Grzegorz Świdzikowski

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.

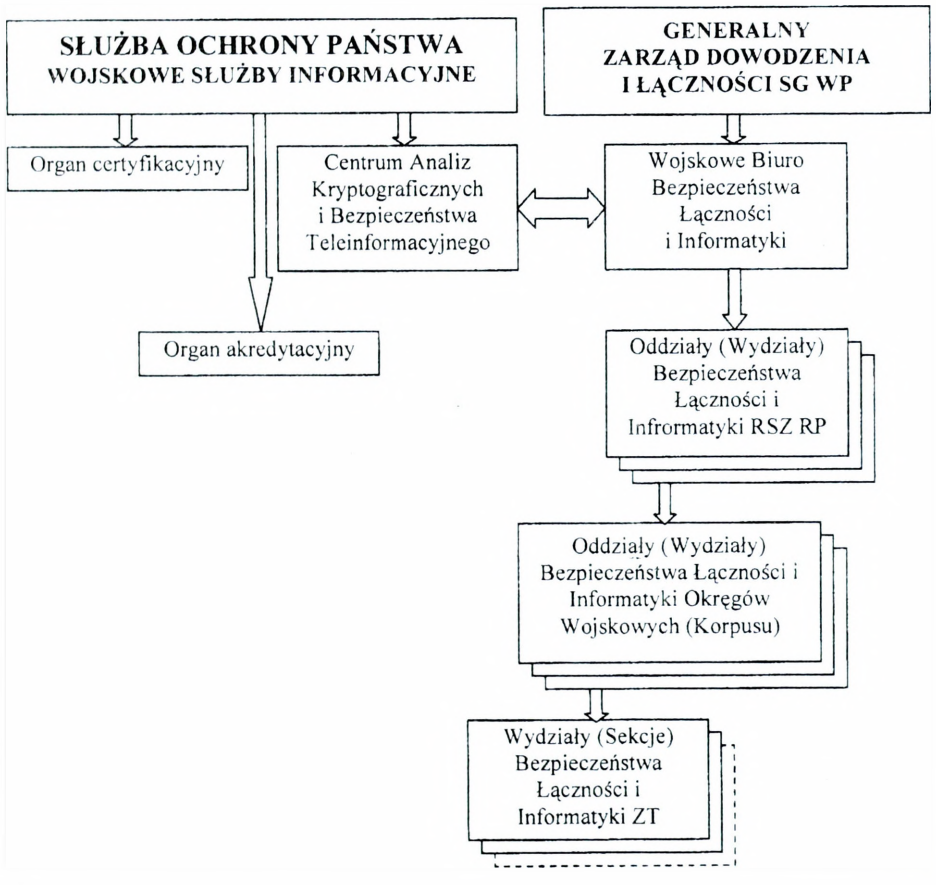
W tej strukturze organizacyjnej (jeśli nie występuje oddzielnie) znajduje się personel odpowiedzialny za prawidłowe i bezpieczne funkcjonowanie systemów telekomunikacyjnych (informatycznych). Do obowiązków tego personelu należy wdrażanie i bieżący merytoryczny nadzór nad procedurami i technicznymi środkami 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.

4.1. Struktura organizacyjna wojskowych organów bezpieczeństwa łączności i informatyki

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.



Rys.5 Struktura organizacyjna organów bezpieczeństwa informacji w wojskowych systemach telekomunikacyjnych i informatycznych.

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.

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.

5. Metody i środki ochrony informacji w wojskowych systemach telekomunikacyjnych

ppłk mgr inż. Grzegorz Świdzikowski, płk dr hab. inż. Józef Janczak

Kolejnym krokiem 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.

5.1. Bezpieczeństwo organizacyjno – proceduralne

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 6.

Rys. 6. 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 niejawnych o klauzuli odpowiadającej co najmniej klauzuli najwyższej sklasyfikowanej

informacji wytwarzanej, przetwarzanej, przechowywanej lub przesyłanej za pomocą technicznych środków łączności bądź informatyki.

Wstęp osób nie będących żołnierzami albo pracownikami komórki organizacyjnej objętej strefą może nastąpić tylko i wyłącznie za zgodą kierownika komórki organizacyjnej (dowódcy) i pod nadzorem upoważnionego przez niego żołnierza lub pracownika wojska, pod warunkiem uprzedniego zabezpieczenia informacji niejawnych w sposób uniemożliwiający przypadkowe ujawnienie ich treści. Dla przykładu może to być wyłączenie ekranu monitora, zasłonięcie (przykrycie) urządzeń ochrony kryptograficznej, itp. Warunek powyższy dotyczy nie tylko przybyłych interesantów, ale także (na co w praktyce mało zwraca się uwagę) personelu technicznego i sprzątającego.

Mniejsze obostrzenia należy stosować w odniesieniu do strefy bezpieczeństwa klasy II. Zatrudniony w tej strefie personel (żołnierze i pracownicy wojska) oraz personel techniczny i sprzątający 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).

5.2. Bezpieczeństwo personalne

Pojęcie bezpieczeństwo personalne 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 zminimalizować prawdopodobieństwo zaistnienia tego zagrożenia. Działania sprawdzające powinny obejmować wszystkie aktywa systemu (urządzenia, aplikacje, oprogramowanie, dane, kopie bezpieczeństwa itp.), do których osoba ta miała dostęp.

Korzystanie w ramach przysługujących kompetencji z zasobów informacyjnych systemu telekomunikacyjnego lub informatycznego wymaga zapoznania się z obowiązującymi w danej jednostce organizacyjnej przepisami, wytycznymi oraz przyjętymi procedurami, które opisano w poprzednim podrozdziale.

Organy bezpieczeństwa łączności i informatyki poszczególnych szczebli dowodzenia we współpracy z pełnomocnikiem ochrony zobowiązane są do prowadzenia w tym zakresie systematycznego szkolenia całego podległego stanu osobowego.

Użytkownicy systemu telekomunikacyjnego lub informatycznego powinni uzyskać odpowiednie informacje dotyczące jego zabezpieczenia. W zależności od zakresu oraz kategorii użytkowników, informacje te mogą być przekazywane na trzech poziomach:

- uświadamiania;
- szkolenia;
- edukacji.

Programy uświadamiania i szkolenia oraz edukacji użytkowników systemu powinny uwzględniać zróżnicowane potrzeby w zakresie znajomości zabezpieczenia użytkowanych systemów telekomunikacyjnych i informatycznych.

Uświadomienie pracowników w zakresie zabezpieczenia systemów obejmuje:

- 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.

5.3. Bezpieczeństwo fizyczne

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 co do koniecznego stopnia zabezpieczenia środkami 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, aktów sabotażu i terroryzmu oraz innych działań o charakterze antypaństwowym lub kryminalnym.

Zasadniczym zadaniem i celem stosowania środków bezpieczeństwa fizycznego 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 (telekomunikacyjne i informatyczne) 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 teleinformacyjnych. 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 teleinformacyjnego, 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.

5.4. Bezpieczeństwo techniczne

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 teleinformacyjnego 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;
- ochronę elektromagnetyczną;
- ochronę programową;
- ochronę transmisji informacji;
- techniczne wsparcie ochrony fizycznej.

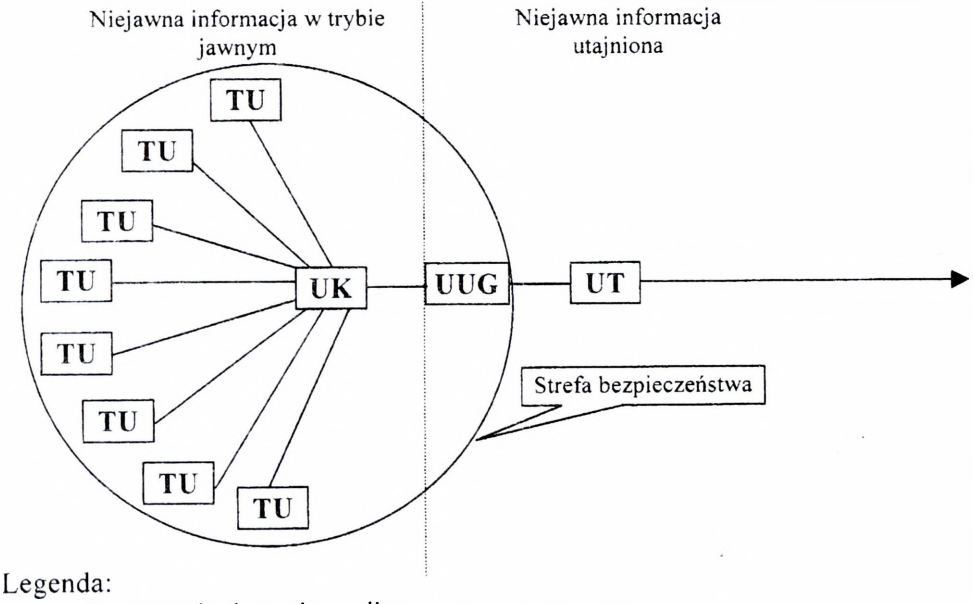
5.4.1. Bezpieczeństwo kryptograficzne

W każdym wojskowym systemie telekomunikacyjnym lub informatycznym, w którym wytwarza się, przetwarza, przechowuje i przede wszystkim przysyła 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 7., zazwyczaj stosujemy w sytuacji, gdy w pewnym rejonie lub obszarze mamy zgrupowane urządzenia końcowe (terminale) zabezpieczające dostęp uprawnionych użytkowników do niejawnych zasobów informacyjnych systemu.



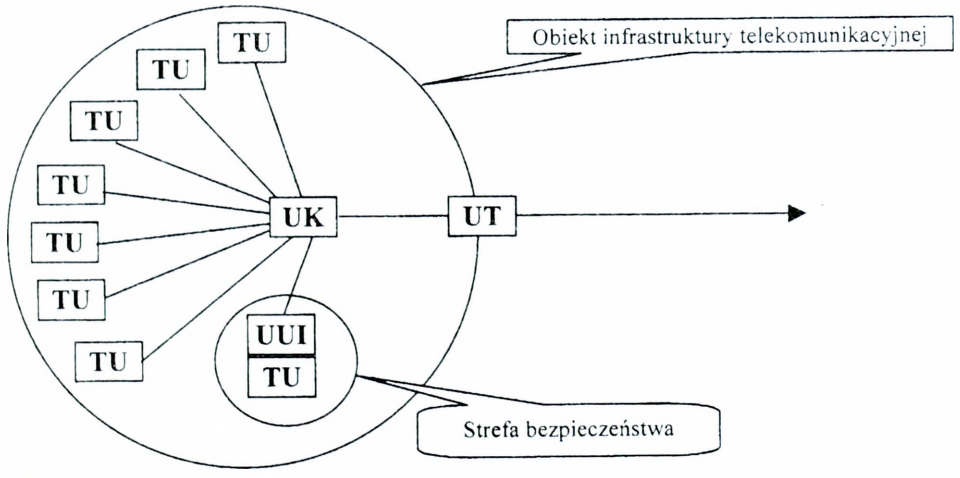
Legenda:
TU – terminal użytkownika
UK – urządzenie komutacyjne
UUG – urządzenie utajniania grupowego
UT – urządzenie transmisyjne

Rys. 7. Przykład utajniania grupowego

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.

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 8.) 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.



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

Rys. 8. Przykład utajniania indywidualnego

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.

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".

5.4.2. Ochrona elektromagnetyczna

Cechą charakterystyczną emisji niekontrolowanej jest możliwość przechodzenia sygnału z jednej postaci w drugą. Na przykład fala elektromagnetyczna, natrafiając na przewodnik, może być propagowana dalej w postaci fali powierzchniowej. Dlatego ochrona przed emisją ujawniającą musi uwzględniać wszystkie typy propagacji oraz całą szerokość widma.

Problematyka zwalczania niekontrolowanej emisji jest w dużej mierze sprawą kompatybilności elektromagnetycznej. W pierwszym rzędzie należy zagwarantować spełnienie przez urządzenia elektryczne systemu telekomunikacyjnego bądź informatycznego krajowych norm dotyczących ograniczenia emisji elektromagnetycznej.

Dodatkowe środki zabezpieczenia przed emisją ujawniającą można podzielić na trzy kategorie:

- modyfikacje urządzeń i przyrządów;
- stosowanie urządzeń maskujących;
- ekranowanie, blokowanie i filtrowanie.

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

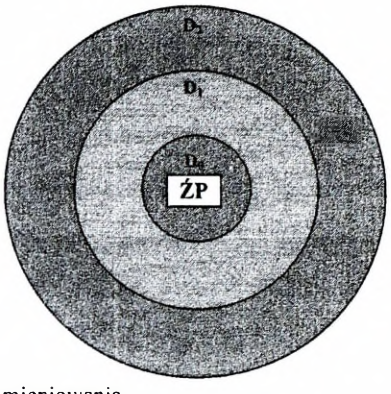
Z kolei oferowane na rynku urządzenia o obniżonym poziomie emisji elektromagnetycznej są bardzo kosztowne. Stosowanie urządzeń maskujących (generatorów szumu elektromagnetycznego) jest prawnie zabronione, ponieważ są one źródłem zakłóceń dla wszystkich innych urządzeń elektrycznych lub telekomunikacyjnych 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 9.



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

Rys. 9. 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 D_0. 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.

5.4.3. Ochrona programowa

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.

5.4.4. Bezpieczeństwo transmisji informacji

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[1] 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.

[1] Problemy te rozpatrywane są w ramach zapewnienia kompatybilności elektromagnetycznej.

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"[2] 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).

[2] Pojęcie wyjaśniono w rozdziale 2 str. 23.

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.

5.4.5. Techniczne wsparcie ochrony fizycznej

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.

Zakończenie

płk dr hab. inż. Józef Janczak, ppłk mgr inż. Grzegorz Świdzikowski

W opracowaniu przedstawiano najbardziej istotne problemy zapewnienia bezpieczeństwa informacji w procesie organizacji oraz eksploatacji wojskowych systemów telekomunikacyjnych i informatycznych zgodnie z wymaganiami aktualnie obowiązującej ustawy „O ochronie informacji niejawnych" z dnia 22 stycznia 1999 r. Zaprezentowane rozwiązania pozwalają uzmysłowić złożoność i szczegółowość wszelkich niezbędnych i koniecznych do zastosowania przedsięwzięć organizacyjnych oraz technicznych w celu zapewnienia wymaganego poziomu bezpieczeństwa, adekwatnie do pojawiających się zagrożeń.

Z tej przyczyny przedstawiono szerokie spektrum zagrożeń w odniesieniu do samych systemów jak również informacji w nich wytwarzanych, przetwarzanych, przechowywanych czy przesyłanych, które każdy organizator systemu musi mieć na uwadze i uwzględniać w procesie planowania[3], a następnie w czasie eksploatacji niejawnych wojskowych systemów telekomunikacyjnych i informatycznych. Zdaniem autorów opracowanie może stanowić bazę do dalszych rozważań w zakresie identyfikacji możliwych i potencjalnych zagrożeń dla bezpiecznego funkcjonowania wojskowego systemu telekomunikacyjnego lub informatycznego.

Inne przedstawione w opracowaniu uwarunkowania determinują natomiast zastosowanie środków ochrony, które zależne są przede wszystkim od najwyższej klauzuli informacji możliwej do wytwarzania, przetwarzania, przechowywania lub przesyłania w danym systemie.

Najlepiej obrazują to dokumenty takie jak „Szczególne warunki bezpieczeństwa" oraz „Procedury bezpieczeństwa", które w myśl obowiązujących dokumentów normatywnych muszą być opracowane przez organizatora niejawnego wojskowego systemu telekomunikacyjnego i informatycznego, przed oddaniem systemu do eksploatacji.

Należy nadmienić, że w dokumentach tych zawarta jest specyfika i indywidualność każdego systemu choćby z punktu widzenia jego struktury organizacyjnej, zastosowanych środków komutacyjnych, transmisyjnych czy końcowych. Uwzględniają one również środowisko oraz otoczenie to bliższe i dalsze, w którym system ma docelowo funkcjonować. Stanowią one zatem podstawę do przeprowadzenia analizy wszelkich możliwych zagrożeń

[3] Czynności te wykonuje się podczas oceny sytuacji.

dla bezpieczeństwa opisywanego systemu i tym samym leży u podstaw doboru niezbędnych narzędzi oraz środków ochrony w zależności od poziomu wymaganego bezpieczeństwa.

„Procedury bezpieczeństwa" uwzględniając uprzednio wymienione uwarunkowania definiują natomiast sposoby i uprawnienia dostępu personelu technicznego oraz użytkowników zarówno do podlegających ochronie urządzeń jak i niejawnych zasobów informacyjnych systemu. Określają ponadto procedury normujące sposoby zachowania oraz postępowania w sytuacjach zagrożenia będących następstwem ataku terrorystycznego, klęski żywiołowej takiej jak pożar, powódź, itp.

Tak opracowane dokumenty są wyrazem prowadzonej w siłach zbrojnych polityki bezpieczeństwa informacji oraz stanowią podstawę zgłoszenia służbom ochrony państwa o gotowości przygotowywanego niejawnego systemu do użytkowania w danej jednostce organizacyjnej bądź w całym resorcie obrony narodowej, a tym samym ubiegania się o uzyskanie przez system stosownej akredytacji.

Zdaniem autorów przedstawione w niniejszym opracowaniu problemy oraz podstawowe środki w zakresie zapewnienia bezpieczeństwa systemów telekomunikacyjnych i informatycznych nie wyczerpują w pełni zagadnienia ze względu na jego złożoność.

Postęp techniczny i technologiczny w dziedzinie środków łączności oraz informatyki otwiera coraz to nowe możliwości w świadczeniu usług telekomunikacyjnych, sprawności i wydajności systemu, ale także niesie ze sobą nowe zagrożenia dla bezpieczeństwa informacji, która w wojskowych systemach telekomunikacyjnych oraz informatycznych podlega prawnej ochronie.

Z tej przyczyny organy odpowiedzialne za wdrażanie i utrzymanie bezpieczeństwa w systemach telekomunikacyjnych oraz informatycznych muszą na bieżąco monitorować bezpieczeństwo samego systemu i znajdującej się w nim informacji oraz stan (efektywność) zastosowanych środków ochrony. Reagować natychmiast na wszystkie otrzymane zgłoszenia o możliwości utraty bezpieczeństwa lub ujawnienia informacji.

Temu też mają służyć zalecane przez służby ochrony państwa audyty (przeglądy) systemów telekomunikacyjnych i informatycznych oraz systemów ochrony zapewniających im bezpieczeństwo.

Podstawowym wnioskiem, który winien wypływać z lektury tego opracowania jest postulat, że poziom bezpieczeństwa systemu telekomunikacyjnego oraz informatycznego zależy w dużej mierze od świadomości samych użytkowników oraz od zastosowanych w nich środków bezpieczeństwa i stałego eliminowania nowych nie znanych dotychczas zagrożeń. Osiąga się to przez stałe monitorowanie systemu zabezpieczeń oraz jego modernizację wynikającą z potrzeb eksploatacyjnych oraz postępu technicznego.

Literatura

1. Aloksa W. Karpiński C. Mencel A. – *Rola inżynierii kompatybilności elektromagnetycznej w procesie budowy systemów elektronicznych, WAT, Warszawa 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. Bryczkowski Maciej - *Bezpieczeństwo systemów sieciowych, Postępy Kryminalistyki Nr 1/97.*
4. Goban-Klaus Tomasz, Sienkiewicz Piotr – *Społeczeństwo informacyjne: szanse, zagrozenia, wyzwania, Wydawnictwo Fundacji Postępu Telekomunikacji, Kraków 1999.*
5. Icove D. Seger K. von Storch - *A Crimefighter Handbook, O'Reilly&Associates 1999.*
6. Jakubski J.K. - *Polityka zabezpieczenia informacji - potrzeba czy wymóg. II Krajowa Konferencja Zastosowań Kryptografii - Enigma'98, Warszawa 26-28 maja 1998 r.*
7. Janczak J. – *Obrona informacyjna w działaniach wojsk lądowych, AON, Warszawa 2000.*
8. Janczak J. – *Obrona informacyjna w działaniach obronnych związku operacyjnego, AON, Warszawa 2002.*
9. Kwećka Roman – *Informacja w walce zbrojnej, AON, Warszawa 2001.*
10. Mąka Dobrosław – *Elementy zagrozeń i zarządzanie ryzykiem w świetle polityki bezpieczeństwa, IT Security Magazine, Nr 8-9, 2001.*
11. Michniak J. Wisz A. - *Bezpieczeństwo i ochrona informacji w wojskowych sieciach telekomunikacyjnych i zautomatyzowanych systemach: (zasady ogólne), AON, Warszawa 2000.*
12. Moller E. - *Protective Measures Against Compromising Electromagnetic Radiation Emitted by Video Display Terminals, InterPact Press, 1991.*
13. Sienkiewicz P. Dańczak A. – *Praca studyjna „Bezpieczeństwo informacji w Siłach Zbrojnych RP. Aspekty strategiczne", AON, Warszawa 2002.*
14. Stokłosa J. Bilski T. Pankowski T. – *Bezpieczeństwo danych w systemach informatycznych, Wydawnictwa Naukowe PWN Poznań 2001*
15. Swanson M., Guttman B. - *Generally Accepted Principles and Practices for Securing Information Technology Systems, NIST, SP 800-14, September 1996*
16. Wróblewski R. - *Podstawowe pojęcia z dziedziny polityki bezpieczeństwa, strategii i sztuki wojennej, AON, Warszawa 1999.*

Dokumenty normatywne

1. 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)
2. Rozporządzenie Rady Ministrów z dnia 9 lutego 1999 r. w sprawie organizacji kancelarii tajnych. (Dz.U.Nr 18, poz. 156)
3. 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)
4. 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)
5. Zarządzenie nr 49/MON Ministra Obrony Narodowej z dnia 7 sierpnia 2002 r. w sprawie szczególnych zasad organizacji kancelarii tajnych, stosowania środków ochrony fizycznej oraz obiegu informacji niejawnych.
6. Decyzja nr 181/MON Ministra Obrony Narodowej z dnia 6 października 200 r. w sprawie organizacji szczególnej ochrony systemów i sieci teleinformatycznych w resorcie obrony narodowej.
7. Dyrektywa bezpieczeństwa - *AD-70-1-PL, WSI, Warszawa 1997.*
8. Dyrektywa BTPO – 601A - *Wytyczne w zakresie postępowania z materiałami kryptograficznymi.*
9. Dyrektywa BTPO – 701A - *Wytyczne w zakresie instalacji urządzeń przeznaczonych do przetwarzania informacji niejawnych.*
10. CM - (55)15 (Final) – *„Bezpieczeństwo w ramach Organizacji Traktatu Północnoatlantyckiego"*
11. Dyrektywa DBBT – 301A - *Wytyczne w zakresie bezpieczeństwa fizycznego kancelarii kryptograficznych, stacji łączności kryptograficznej oraz pomieszczeń wydzielonych przeznaczonych do przetwarzania informacji niejawnej.*
12. Dyrektywa NATO AD – 90-9 - *Procedury w zakresie zabezpieczenia, ewidencji oraz zaopatrywania w środki i materiały kryptograficzne.*
13. *Metodyka opracowywania Szczególnych Wymagań Bezpieczeństwa dla systemów i sieci teleinformatycznych* – Wojskowe Biuro Bezpieczeństwa Łączności i Informatyki, Warszawa 2000.

Publikacje
Akademii Obrony Narodowej

do nabycia w Wydziale Wydawniczym AON
al. gen. A. Chruściela 103, bl. 2
00-910 Warszawa,
tel. 681 40 55, tel./faks 681 37 52

- S. Bartosiewicz, M. Mróz – Zaopatrywanie jednostek wojsk lotniczych i obrony powietrznej w techniczne środki materiałowe techniki naziemnej – 7,00 zł
- Bezpieczne niebo. Materiały z konferencji naukowej – 14,00 zł
- J. Bieńkowski, R. Stępień (red.) – Edukacja pedagogiczna w wyższej uczelni wojskowej – 16,00 zł
- H. Binkowski (red.) – OBWE w procesie umacniania bezpieczeństwa europejskiego – 16,00 zł
- A. Bujak – Praca w terenie na szczeblach taktycznych według standardów NATO – 10,00 zł
- W. Chojnacki – Socjologiczne aspekty tendencji instytucjonalno-organizacyjnego rozwoju wojska – 16,00 zł
- R. Chrobak i in. – Działania bojowe dywizji – 15 zł
- M. Cieślarczyk, P. Krawczyk, Z. Korulczyk – Poradnik metodyczny autorów prac kwalifikacyjnych – 8,00 zł
- M. Cieślarczyk, M. Chojnacki, A, Radomyski – Współpraca cywilno-wojskowa (CIMIC) w siłach zbrojnych (SP) RP – 13,00 zł
- M. Cieślarczyk (red.) – Metody, techniki i narzędzia badawcze oraz elementy statystyki – 13,00 zł
- A. Ciupiński, M. Zając (red.) – Wybrane problemy walki z terroryzmem międzynarodowym – 17 zł
- A. Ciupiński (red.) – Dyplomacja wielostronna – 25,00 zł
- A. Ciupiński – Podstawowe elementy polityki bezpieczeństwa i obrony RP – 15,00 zł
- A. Ciupiński, R. Białoskórski – Wczesne ostrzeganie i zapobieganie współczesnym konfliktom zbrojnym w strategii Sojuszu Północnoatlantyckiego – 7,00 zł
- A. Ciupiński, H. Binkowski, A. Legucka – Bezpieczeństwo w stosunkach międzynarodowych – 30,00 zł
- T. Compa – Zarządzanie przestrzenią powietrzną – 10,00 zł
- J. Czaja – Stolica apostolska wobec integracji europejskiej – 15,00 zł
- K. Czajka – Użycie artylerii w obronie oddziału – 8,00 zł
- P. Daniluk – Radiostacje pola walki – 10,00 zł
- A. Dawidczyk – Nowe wyzwania, zagrożenia i szanse dla bezpieczeństwa Polski u progu XXI w. – 9,00 zł
- P. Dela, J. Wołejszo – Wsparcie komputerowe ćwiczeń wojskowych 16 zł
- Dowodzenie lotnictwem sił powietrznych w działaniach wojsk lądowych (praca zbiorowa) – 15,00 zł
- W. Drążczyk – Logistyka sił powietrznych w działaniach wielonarodowych – 9,00 zł
- A. Fellner – Zautomatyzowane systemy kontroli ruchu lotniczego przestrzeni powietrznej – 20,00 zł
- M. Flemming – Międzynarodowe prawo humanitarne konfliktów zbrojnych – 45,00 zł
- P. Gawliczek, J. Pawłowski – Zagrożenia asymetryczne – 14,00 zł
- M. Gąska, A. Ciupiński – Międzynarodowe prawo humanitarne konfliktów zbrojnych – 21,00 zł
- A. Glen, W. Marud – Kontrola przestrzeni powietrznej w czasie kryzysu i wojny – 18,00 zł
- J. Gotowała – Lotnictwo XXI wieku – 11,00 zł
- J. Groskrejc – Antropologiczne i aksjologiczne aspekty edukacji oficerów – 10,00 zł
- J. Halik – Metodyka opracowania pracy magisterskiej i studyjnej – 15,00 zł
- J. Halik, J. Wołejszo – Ćwiczenia wojskowe sił zbrojnych RP w aspekcie interoperacyjności w ramach NATO – 14,00 zł
- M. Huzarski (red.) – Taktyka ogólna wojsk lądowych – 21,00 zł
- K. Jałoszyński – Terroryzm antyizraelski – 12,00 zł
- K. Jałoszyński – Terroryzm czy terror kryminalny w Polsce? – 12,00 zł
- K. Jałoszyński – Zagrożenie terroryzmem w wybranych krajach Europy Zachodniej oraz w Stanach Zjednoczonych – 12,00 zł
- J. Janczak – Zakłócanie informacyjne – 12,00 zł
- Cz. Jarecki – Użycie wojsk rakietowych i artylerii w operacji – 13,00 zł
- T. Jemioło – Globalizacja. Szanse i zagrożenia – 8,00 zł
- T. Jemioło, K. Malak (red.) – Bezpieczeństwo zewnętrzne Rzeczypospolitej Polskiej – 25,00 zł
- A. Jóźwiak, Cz. Marcinkowski – Wybrane problemy współczesnych operacji pokojowych – 18,00 zł
- M. Juszczyk – Wsparcie działań przez państwo gospodarza – 14 zł
- L. Kanarski, P. Gawliczek – Przywództwo w armiach NATO – 9,00 zł
- L. Kanarski, B. Rokicki (red.) – Teoria i praktyka przywództwa wobec wyzwań edukacyjnych – 24,00 zł
- J. Kardas, K. Loranty – Wybrane problemy bezpieczeństwa i obronności państwa w opiniach pracowników administracji publicznej – 12,00 zł
- J. Kardas, K. Loranty – Instytucjonalizacja przygotowania obronnego kadr administracji – 15,00 zł
- J. Karpowicz, Z. Chojnacki – Bezpieczeństwo lotów – 10,00 zł
- J. Karpowicz, E. Cieślak – Lotnictwo wsparcia w sojuszniczych działaniach powietrznych – 17 zł
- J. Karpowicz, K. Kozłowski – Bezzałogowe statki powietrzne i miniaturowe aparaty latające – 18 zł
- J. Karpowicz – Współczesne konstrukcje lotnicze – 20,00 zł

- Cz. Kącki – Siły wielonarodowe do misji pokojowych – 15 zł
- Cz. Kącki – Izrael. Jego wpływ na rozwój sytuacji w regionie Bliskiego Wschodu – 15,00 zł
- Kierowanie mobilnymi systemami łączności wojsk lądowych (praca zbiorowa) cz.I – 14 zł, cz.II – 8 zł, cz.III. – 12 zł
- W. Kitler (red.) – Obrona cywilna (niemilitarna) w obronie narodowej III RP – 25,00 zł
- W. Kitler – Obrona narodowa III RP. Pojęcie. Organizacja. System (rozprawa habilitacyjna) – 24,00 zł
- W. Kitler – Obrona narodowa w wybranych państwach demokratycznych – 14,00 zł
- Z. Klawitter – Rola i zadania zespołu wsparcia personalnego na stanowisku dowodzenia BZ/BPanc – 7,00 zł
- T. Kochański – Logistyka międzynarodowa – 12,00 zł
- T. Kochański – Logistyka jako koncepcja zintegrowanego zarządzania – 18,00 zł
- T. Kochański, S. Kurek – Konkurencyjność przedsiębiorstw – 15 zł
- M. Koziński – Umowa offsetowa i inne formy udziału państwa w międzynarodowym obrocie gospodarczym – 10,00 zł
- M. Kozub – Lotnictwo w operacjach połączonych – 7,00 zł
- M. Kozub – Lotnictwo wojsk lądowych w operacjach połączonych – 8,00 zł
- M. Kozub – Lotnictwo w bojowym poszukiwaniu i ratownictwie – 8,00 zł
- J. Kręcikij – Współczesne kierowanie wojskami. Proces dowodzenia – 12,00 zł
- J. Kręcikij – Metodyka pracy sekcji dowodzenia oddziału i związku taktycznego – 13,00 zł
- J. Kręcikij –Wybrane problemy kierowania zgrupowaniami wielonarodowych sił połączonych – 14,00 zł
- R. Kwećka, M. Gryga – Siły specjalne w kontekście współczesnych zagrożeń – 15,00 zł
- K. Kubiak – Transport wojsk i ładunków wojskowych drogą morską przy użyciu statków handlowych – 12,00 zł
- L. Łukaszuk – Międzynarodowe prawo pokoju i bezpieczeństwa – 20,00 zł
- L. Łukaszuk – Dyplomacja współczesna a problemy prawa i bezpieczeństwa międzynarodowego – 20,00 zł
- L. Łukaszuk – Europejskie prawo pokoju i bezpieczeństwa – 20,00 zł
- T. Majewski – Ankieta i wywiad w badaniach wojskowych – 9,00 zł
- T. Majewski – Kierownik – dowódca w organizacji – 12,00 zł
- T. Majewski – Miejsce celów, problemów i hipotez w procesie badań naukowych – 8 zł
- T. Majewski i in. – Planowanie w organizacji – 9 zł
- K. Malak – Polityka zagraniczna i bezpieczeństwa Białorusi – 18,00 zł
- J. Marczak (red.) – Samoorganizacja społeczeństwa na rzecz bezpie-czeństwa powszechnego. Samoobrona powszechna III RP – 20,00 zł
- M. Marszałek – Siły powietrzne w operacjach ewakuacyjnych (według poglądów amerykańskich) – 13 zł
- M. Marszałek, A. Radomyski – Metodyka pracy zespołów funkcjonalnych na stanowisku dowodzenia brygady rakietowej sił powietrznych – 25,00 zł
- Z. Maślak – Podstawy teorii informacji obrony powietrznej – 10,00 zł
- Z. Maślak (oprac.) – Informacje w obronie powietrznej – potrzeby, wymagania, zagrożenia. Materiały z sympozjum naukowego – 17,00 zł
- M. Michalec (oprac.) – Kierunki rozwoju rosyjskiej myśli teoretycznej i praktyki w zakresie użycia lotnictwa w walce – 14,00 zł
- J. Michniak (red.) – Projektowanie struktury organizacyjnej dowództwa brygady zmechanizowanej (pancernej) – 12,00 zł
- J. Michniak – Stanowiska dowodzenia w wojskach lądowych – 10 zł
- G. Nowacki – Informacja w walce zbrojnej. Materiały z sympozjum naukowego – 17,00 zł
- G. Nowacki – Strategiczne siły jądrowe wybranych państw – 14,00 zł
- G. Nowacki – Rozpoznanie satelitarne USA i Federacji Rosyjskiej – 8,00 zł
- G. Nowacki (red.) – Militaryzacja kosmosu – 17,00 zł
- A. Nowak – Działalność rozpoznawcza na szczeblach taktycznych – 12,00 zł
- E. Nowak – Gospodarowanie zasobami majątkowymi – 15,00 zł
- M. Obrusiewicz – Wielonarodowe połączone siły zadaniowe CJTF – 12,00 zł
- M. Obrusiewicz – Geneza i prognoza kooperatywnych stosunków wojskowych końca XX i początku XXI w. na tle bezpieczeństwa europejskiego – 15 zł
- J. Pawłowski, A. Ciupiński (red.) – Umiędzynarodowiony konflikt wewnętrzny – 20,00 zł
- M. Pelc, M. Juszczyk – Matematyka – 25 zł
- J. Płaczek – Ewolucja polskiej myśli obronno-ekonomicznej w latach 1976–2000 – 20,00 zł
- J. Płaczek (red.) – Gospodarka obronna Polski w końcu lat dziewięćdziesiątych. Szanse i zagrożenia – 25,00 zł
- Podróż studyjna w systemie edukacji oficerów w AON. Materiały z sympozjum naukowego – 17,00 zł
- A. Polak – Wybrane zagadnienia obrony wybrzeża w Polsce (1920–2002) – 16,00 zł
- A. Polak – Teoria grup operacyjnych w polskiej sztuce wojennej okresu międzywojennego – 30,00 zł
- Prawo w stosunkach międzynarodowych. Wybór dokumentów (praca zbiorowa) – 35,00 zł (dwa tomy)
- K. Przeworski – Ewakuacja jako sposób ochrony ludności – 7,00 zł
- Pułk przeciwlotniczy w działaniach operacyjnych (praca zbiorowa) – 20,00 zł
- A. Radomyski – Metody i treść pracy zespołu OPL na stanowisku dowodzenia dywizji zmechanizowanej – 18,00 zł
- A. Skrabacz – Kobiety w obronie narodowej Polski u progu XXI w. – 15,00 zł
- J. Skrzyp (red.) – Informator geograficzny o państwach kandydujących do Sojuszu Północnoatlantyckiego – 14,00 zł

- J. Skrzyp, Z. Lach – Informator geograficzny. Państwa członkowskie NATO – 20,00 zł
- Z. Skwarek – Powietrzne systemy wczesnego wykrywania i powiadamiania – 13,00 zł
- K. Słaboń – Sytuacja jeńców wojennych w konflikcie iracko-irańskim (1980-1988) – 10,00 zł
- Słownik terminów z zakresu bezpieczeństwa narodowego (praca zbiorowa) – 15,00 zł
- Słownik terminów z zakresu psychologii (praca zbiorowa) – 10,00 zł
- Słownik pojęć sojuszniczej obrony powietrznej (praca zbiorowa) – 12,00 zł
- H. Spustek – Wybrane zagadnienia badań operacyjnych i modelowania liniowego – 8,00 zł
- Z. Stachowiak – Metodyka i metodologia pisania prac kwalifikacyjnych (licencjackich, magisterskich i podyplomowych) – 9,00 zł
- Z. Stachowiak, J. Płaczek (red.) – Wybrane problemy ekonomiki bezpieczeństwa – 30,00 zł
- R. Stępień (red.) – Edukacja w wyższych szkołach wojskowych – 21,00 zł
- M. Strzoda (red.) – Wybrane terminy z zakresu dowodzenia i zarządzania – 7,00 zł
- M. Strzoda – Słownik nazw, skrótów i akronimów państw, instytucji, dowództw, jednostek organizacyjnych i osób funkcyjnych – 8 zł
- J. Suwart – Zarys obrony cywilnej w Polsce w latach 1920–1996 – 30,00 zł
- R. Szpyra – Powietrzna sztuka operacyjna wybranych państw – 15,00 zł
- Środki dowodzenia (praca zbiorowa) – 12 zł
- E.A. Wesołowska, A. Szerauc (red.) – Patriotyzm – Obronność – Bezpieczeństwo – 20,00 zł
- J. Wołejszo – Wybrane problemy procesu planowania i rozliczania działalności szkoleniowej na szczeblach taktycznych w SZ RP – 16 zł
- J. Wołejszo – Trening sztabowy dowództw szczebla taktycznego SZ RP – 17,00 zł
- J. Wołejszo – Wybrane aspekty projektowania struktury organizacyjnej zespołu dowodzenia stanowiska dowodzenia brygady zmechanizowanej – 11,00 zł
- J. Wołejszo – Wybrane problemy przygotowania i realizacji ćwiczeń sojuszniczych NATO – 16 zł
- J. Wołejszo, Z. Fiołna – Dowodzenie brygadą zmechanizowaną (pancerną) w obronie – 12,00 zł
- J. Wołejszo, Z. Fiołna – Dowodzenie brygadą zmechanizowaną (pancerną) w marszu – 15,00 zł
- Wojskowe wsparcie władz cywilnych i społeczeństwa. Materiały z seminarium – 20,00 zł
- Wojsko wobec polskiego października'56. Rezolucje, uchwały, listy (wybór, wstęp i opracowanie: E. J. Nalepa) – 30,00 zł
- J. Wojtasik (red.) – Studia z dziejów polskiej techniki wojskowej od XVI do XX wieku – 27,00 zł
- J. Wojtasik (red.) – Od Żółkiewskiego i Kosińskiego do Piłsudskiego i Petlury. Z dziejów stosunków polsko-ukraińskich od XVI do XX wieku – 20,00 zł
- M. Wrzosek – Działania rozpoznawcze na obszarze kraju – 10 zł
- M. Wrzosek – Organizacja pracy taktycznej komórki rozpoznania – 17 zł
- Wsparcie informacyjne obrony powietrznej. Materiały z sympozjum naukowego – 18 zł
- Wydział Lotnictwa i Obrony Powietrznej AON – Ewolucja dla postępu. Materiały z konferencji – 18 zł
- E. Zabłocki – Współczesne siły powietrzne – 13,00 zł
- S. Zalewski – Służby specjalne w państwie demokratycznym – 11,00 zł
- Założenia operacyjne do doktryny zasadniczej sił powietrznych (praca zbiorowa) – 10,00 zł
- L. Zapała – W rembertowskiej Alma Mater. Wspomnienia – 18,00 zł
- B. Zdrodowski, M. Marszałek – Operacje pozawojenne sił powietrznych – 16,00 zł
- J. Zieliński (red.) – Podstawowe założenia dydaktyki sztuki operacyjnej – 14,00 zł
- J. Zieliński – Wojska lądowe jako rodzaj sił zbrojnych – 14 zł
- J. Zuziak – Dzieje Instytutu Józefa Piłsudskiego w Londynie 1947–1997 – 25,00 zł

Zamówienia przyjmujemy telefonicznie lub pisemnie