AKADEMIA
OBRONY
NARODOWEJ

Egz. Nr 1

Po odłączeniu załącznika nr 2
JAWNE

BEZPIECZEŃSTWO INFORMACJI W MOBILNYCH SYSTEMACH TELEKOMUNIKACYJNYCH WOJSK LĄDOWYCH

Materiały z sympozjum naukowego

WARSZAWA 2004

AKADEMIA OBRONY NARODOWEJ

WYDZIAŁ WOJSK LĄDOWYCH
INSTYTUT ZARZĄDZANIA I DOWODZENIA

BEZPIECZEŃSTWO INFORMACJI W MOBILNYCH SYSTEMACH TELEKOMUNIKACYJNYCH WOJSK LĄDOWYCH

Materiały z sympozjum naukowego

Opracowane pod redakcją naukową

ppłk mgr inż. Grzegorza Świdzikowskiego

WARSZAWA **2004**

Opracowanie zawiera materiały wygłoszone i prezentowane podczas sympozjum
Forma przedstawienia zawartych materiałów odpowiada wersji przekazanej przez prelegentów

SPIS TREŚCI:

Wstęp

W dniu 06 maja 2004 r. w Instytucie Zarządzania i Dowodzenia odbyło się sympozjum naukowe nt.: „Bezpieczeństwo informacji w mobilnych systemach telekomunikacyjnych wojsk lądowych".

Bezpośrednim organizatorem sympozjum był Zakład Systemów Łączności i Informatyki kierowany przez płk. dr. hab. inż. Józefa Janczaka. Patronat naukowy nad przeprowadzonym sympozjum sprawował płk dr hab. inż. Józef Michniak.

Zasadniczym celem jaki przyświecał organizatorom tego spotkania naukowego była wymiana poglądów oraz zaprezentowanie osiągnięć, doświadczeń i wniosków wynikających z wdrażania w Siłach Zbrojnych RP postanowień ustawy "O ochronie informacji niejawnych" z dnia 22.01.1999 r. w aspekcie ochrony informacji w polowych systemach telekomunikacyjnych wojsk lądowych.

Obowiązki obejmujące przygotowanie, prowadzenie i redakcję naukowa sprawował ppłk mgr inż. Grzegorz Świdzikowski. W czasie sympozjum referaty naukowe wygłosili: kpt. dypl. inż. Piotr Waniek, płk mgr inż. Włodzimierz Nowak, płk mgr inż. Andrzej Dańczak, ppłk mgr inż. Grzegorz Świdzikowski, ppłk mgr Bogdan Rembacz oraz kpt. mgr inż. Mariusz Frączek. Jednak ze względu na przyczyny obiektywne, niezależne od organizatorów, nie wszystkie referaty zawarte zostały w niniejszej publikacji.

W sympozjum aktywnie uczestniczyli przedstawiciele Wydziału Wojsk Lądowych AON, Sztabu Generalnego WP, Wojskowych Służb Informacyjnych, Wojskowego Instytutu Łączności, Wojskowych Zakładów Łączności w Zegrzu, Centrum Szkolenia Łączności i Informatyki oraz Dowództwa Wojsk Lądowych wraz z przedstawicielami podległych im związków taktycznych.

Zaprezentowane w czasie sympozjum różne stanowiska oraz punkty widzenia w sferze rozpatrywanej problematyki pozwoliły na bardzo interesującą wymianę poglądów, które umożliwiły dokonanie pewnego rodzaju podsumowania wynikającego z dotychczasowych doświadczeń oraz zarysowały pewne obszary problematyki bezpieczeństwa informacji wymagające udoskonalenia.

płk mgr inż. Andrzej DAŃCZAK
Wojskowe Biuro
Bezpieczeństwa Łączności i Informatyki
Sztabu Generalnego WP

Charakterystyka zagrożeń bezpieczeństwa informacji w polowych systemach telekomunikacyjnych

Szanowni Państwo moje wystąpienie podczas dzisiejszego sympozjum nt. „Charakterystyka zagrożeń bezpieczeństwa informacji w polowych systemach telekomunikacyjnych" składać się będzie z następujących paneli problemowych:

1. Elementy składowe bezpieczeństwa systemów łączności i informatyki
2. Klasyfikacja zagrożeń polowych systemów telekomunikacyjnych
3. Zagrożenia a atrybuty bezpieczeństwa informacji
4. Wnioski

Omawiając pierwsze z wymienionych zagadnień posłużę się ogólnie znaną strukturą elementarną bezpieczeństwa łączności i informatyki przedstawioną na prezentowanym slajdzie, która przyjęła postać „puzli". Przyjmuje się, że w skład bezpieczeństwa wojskowych systemów telekomunikacyjnych wchodzą następujące obszary, do których zalicza się:

1. Bezpieczeństwo personalne i przemysłowe
2. Bezpieczeństwo urządzeń systemów łączności i informatyki
3. Ochrona kryptograficzna
4. Bezpieczeństwo oprogramowania
5. Bezpieczeństwo organizacyjne, dokumentacja akredytacyjna i szkolenie
6. Certyfikacja urządzeń i systemów (sieci)
7. Bezpieczeństwo fizyczne (techniczne)
8. Odpowiedzialność użytkownika
9. Bezpieczeństwo dokumentów niejawnych i ich nośników

W kontekście pierwszego z wymienionych zagadnień należy stwierdzić, że zarówno cały personel techniczny jak i wszyscy użytkownicy systemu przetwarzającego informacje niejawne powinni posiadać uprawnienia (poświadczenia

bezpieczeństwa osobowego) zgodne z maksymalną klauzulą informacji jaka w danym systemie może być wytwarzana, przetwarzana, przesyłana lub przechowywana.

Odnosząc się do bezpieczeństwa przemysłowego należy mieć na uwadze, że każdy sprzęt techniczny planowany do eksploatacji w niejawnym wojskowym systemie telekomunikacyjnym obligatoryjnie musi pochodzić ze „sprawdzonego źródła" – producenta, który jest wiarygodny i sprawdzony przez odpowiednie służby ochrony państwa i daje tym samym gwarancję bezpieczeństwa urządzeniom i przez to systemom na rzecz których one pracują.

Zapewnienie bezpieczeństwa urządzeń systemów łączności i informatyki jest przedsięwzięciem złożonym i obejmuje szereg czynności, do których między innymi można zaliczyć bezpieczeństwo w miejscu instalacji czy przechowywania określonych urządzeń.

Zasadniczym celem stosowania ochrony kryptograficznej jest zapewnienie bezpieczeństwa informacjom, które opuszczają obszar (strefę) technicznie oraz organizacyjnie bezpieczną. Problematyka powyższa dotyczy bezpieczeństwa zarówno urządzeń ochrony kryptograficznej jak i dokumentów kluczowych, szyfrowych, itd.

Problematyka bezpieczeństwa programowego wraz z rozwojem technik informatycznych i szerszego stosowania oraz wykorzystywania ich w nowoczesnych urządzeniach telekomunikacyjnych podnosi systematycznie rangę przedsięwzięć, które są niezbędne w celu zapewnienia bezpieczeństwa informacjom, a tym samym całym systemom łączności i informatyki.

Kolejną płaszczyzną bezpieczeństwa wojskowych systemów telekomunikacyjnych , która nie zawsze jest postrzegana z właściwą sobie uwagą są przedsięwzięcia organizacyjne, dokumenty akredytacyjne oraz szkolenie personelu i użytkowników systemów telekomunikacyjnych. Przedsięwzięcia wymienione powyżej powinny być elementem polityki bezpieczeństwa organizacji, która po jej przygotowaniu i zatwierdzeniu przez właściwe gremia kierownicze w celu jej wdrożenia w życie musi być szeroko propagowana i znana przez każdego członka danej organizacji – w naszym przypadku każdego żołnierza i pracownika wojska.

Zgodnie z pragmatyką i dokumentami normatywnymi każdy system telekomunikacyjny, który przetwarza informacje niejawne powinien być budowany w oparciu o urządzenia łączności i informatyki, które posiadają stosowne certyfikaty

uprawniające je do pracy w systemach niejawnych – wraz z określeniem maksymalnej klauzuli informacji do której dane urządzenie ochrony kryptograficznej zapewnia właściwy poziom bezpieczeństwa. Certyfikacji ponadto podlega cały system telekomunikacyjny przed oddaniem go do fizycznej eksploatacji. Podstawą certyfikacji jest opracowanie Szczególnych Wymagań Bezpieczeństwa dla danego systemu telekomunikacyjnego, które stanowią dla zespołu opiniującego informację określającą zgodność wymagań stawianych systemowi z wymaganiami normatywnymi. Sam proces certyfikacji po uzyskaniu pozytywnej opinii polega na stwierdzeniu zgodności stanu faktycznego z zapisami w zawartymi szczególnych wymaganiach bezpieczeństwa i procedurach bezpieczeństwa.

Kolejnym elementem zapewniającym bezpieczeństwo systemów łączności i informatyki są zabezpieczenia fizyczne i techniczne. Standardy oraz wymagania w tym zakresie zdefiniowane są w dokumencie „Wytyczne w zakresie bezpieczeństwa fizycznego kancelarii kryptograficznych, stacji łączności kryptograficznej oraz pomieszczeń wydzielonych przeznaczonych do przetwarzania informacji niejawnej". Jednak analiza tej dyrektywy skłania do refleksji, że większość zawartych w niej wymagań odnosi się do systemów stacjonarnych, a wojskowe systemy mobilne (taktyczne), które funkcjonują w zgoła odmiennych warunkach i środowisku, zostały w niej potraktowane marginalnie.

Jednym z istotniejszych czynników, które wpływają na bezpieczeństwo informacji w systemach łączności i informatyki to odpowiedzialność uprawnionego użytkownika tego systemu. Żaden środek techniczny, choćby najlepszy, nie jest w stanie zapewnić właściwego poziomu bezpieczeństwa informacji i całego systemu jeśli jego użytkownicy oraz personel techniczny celowo czy też nieumyślnie nie będą przestrzegać w sposób odpowiedzialny przewidzianych dla danego systemu procedur bezpieczeństwa.

Ostatnim elementem w łańcuchu bezpieczeństwa systemów łączności i informatyki są informacje wyprowadzane z tych systemów w postaci dokumentów papierowych i elektronicznej na różnego rodzaju nośnikach (dyskietki, dyski twarde, płyty CD, itd.). W stosunku do tych przedsięwzięć obowiązują szczegółowe dokumenty normatywne regulujące sposób postępowania i ewidencjonowania tego typu informacji. Z tej przyczyny nie będę tego tematu podejmował i dalej go rozwijał.

Przechodząc do omawiania kolejnego zagrożenia za stosowne uważam zwrócenie uwagi na specyfikę funkcjonowania polowych systemów telekomunikacyjnych, która w znacznym stopniu różni się od atrybutów działania systemów stacjonarnych. Mobilne wojskowe systemy telekomunikacyjne charakteryzują się bowiem:

- dynamiką zmian lokalizacji i konfiguracji systemu wynikająca z dynamiki pola walki;
- wysoką elastycznością;
- wpływem uwarunkowań topograficznych na funkcjonowanie (konfigurację) systemu;
- różnorodnością stosowanych dróg komunikacji (przewodowe, światłowodowe, radiowe KF i UKF, satelitarne);
- specyficznym sprzętem łączności i informatyki.

Analizując podatność polowych systemów telekomunikacyjnych na zagrożenia w zakresie bezpieczeństwa informacji możemy stwierdzić, że jest ona większa niż w systemach tradycyjnych rozumianych jako stacjonarne.

Do głównych czynników, które mają wpływ na zagrożenie polowych systemów telekomunikacyjnych możemy zaliczyć:

- możliwość pominięcia niektórych aspektów bezpieczeństwa informacji przy dużej dynamice działań w systemie;
- mnogość potencjalnych kanałów nieautoryzowanego dostępu do informacji (kanały przewodowe, światłowodowe, radiowe, satelitarne);
- możliwość wykorzystania specyficznych warunków środowiskowych do przeprowadzenia ataku zagrażającego bezpieczeństwu informacji.

Zastanawiając się natomiast nad sposobami niekontrolowanego (nieuprawnionego) ulotu informacji chronionych w taktycznych systemach telekomunikacyjnych można stwierdzić, że do ważniejszych dróg utraty danych zalicza się:

- podsłuch elektroniczny
- podgląd (podsłuch) bezpośredni
- zakłócenia radioelektroniczne
- przechwycenie fizyczne

W literaturze fachowej oraz w podejściu naukowym do problemu klasyfikacji zagrożeń bezpieczeństwa informacji w systemach telekomunikacyjnych nie spotykamy jednolitego ich podziału. Zagrożenia są pogrupowane i podzielone na wiele sposobów. Zaproponowany przeze mnie podział zagrożeń ogranicza się do dwóch podstawowych grup, wśród których można wyróżnić:

- losowe
- intencjonalne (zamierzone).

Obie wymienione powyżej grupy możemy podzielić na podgrupy: zewnętrzne i wewnętrzne – każda z nich odnosi się do obiektów systemów łączności i informatyki.

Zagrożenia losowe zewnętrzne uwzględniają takie czynniki jak temperaturę, wilgotność, zanieczyszczenie powietrza, zakłócenia zasilania, zakłócenia w komunikacji, wyładowania atmosferyczne, klęski żywiołowe itp.

Zagrożenia losowe wewnętrzne to niezamierzone błędy ludzi, błędy i pomyłki operatorów, administratorów (konfiguracja sprzętu i oprogramowania), zaniedbania użytkowników oraz defekty sprzętu i oprogramowania.

Zagrożenia intencjonalne (zamierzone) wynikają przede wszystkim z działania własnego personelu powodowanego chęcią zysku, chęcią rewanżu itp. W tej grupie zagrożeń są także działania użytkowników wykraczające poza ich obowiązki, działania przestępców komputerowych podejmowane z chęci z zysku, działania przedstawicieli prasy i innych mediów szukających dostępu do informacji, szpiegostwo gospodarcze i wojskowe, wandalizm chuligaństwo i terroryzm.

Wśród zagrożeń zamierzonych pozwolę sobie wyróżnić ich występowanie w różnych postaciach:

- ataki pasywne;
- ataki aktywne

Zamierzone ataki pasywne to przede wszystkim:

- wyparcie się nadania (odbioru) wiadomości przez rzeczywistego nadawcę;

- podgląd transmitowanych danych przez przyłączenie się do linii lub monitorowanie zmian pola elektromagnetycznego wokół przewodów, monitorowanie fal radiowych, optycznych itp.;
- obserwacja i analiza ruchu komunikatów(wiadomości, meldunków) w sieci – nawet gdy informacja jest zaszyfrowana (analiza ruchu w sieci, w wielu przypadkach może ujawnić konkretne i istotne informacje np. liczba, rozmiar, częstość, źródło i miejsce przeznaczenia wysyłanych informacji może wskazywać na zaangażowanie się organizacji we współpracę z identyfikowalnym partnerem.

Intencjonalne ataki aktywne, nazywane też „hakerskimi" są groźne w każdej swojej postaci. Są to:

- modyfikacja – zmiana przesyłanej informacji;
- wprowadzenie własnego, fałszywej go wiadomości, meldunku;
- usuwanie komunikatów lub opóźnianie ich przesyłania;
- przekierowanie – informacja jest kierowana do innego odbiorcy;
- powtarzanie – intruz powoduje powtórzenie poprzednio przesyłanej wiadomości;
- maskarada – intruz podaje się za innego użytkownika, w celu wymiany informacji w jego imieniu;
- pośrednictwo – włączenie się w dialog dwóch i symulowanie przed każdym z nich drugiego;
- odcięcie lub inne uszkodzenie kanału komunikacyjnego.

Zaprezentowane szczegółowe podgrupy zagrożeń można zilustrować zamieszczonym poniżej wykazem tylko wybranych zagrożeń, z którymi najczęściej spotykamy się w praktyce ochrony informacji:

- podsłuch bierny i aktywny;
- użycie programów typu „koń trojański";
- przełamanie haseł dostępu do systemu;
- przełamanie zabezpieczeń kryptograficznych;
- fałszowanie i kasowanie zbiorów w części lub w całości;

- destrukcja zbiorów i programów zewnętrznym impulsem elektromagnetycznym;
- użycie wirusów komputerowych lub tzw. „bomb logicznych";
- wyłudzenie, kradzież i fałszowanie dokumentów-nośników kluczy (haseł) dostępu) np. PIN;
- błędy organizacyjne i techniczne właściciela (administratora) systemu;
- inne.

Zagrożenie dla bezpieczeństwa informacji w systemie – ze strony każdego, kto usiłuje uzyskać dostęp do informacji i posiada do tego wystarczającą wiedzę oraz doświadczenie (legalny personel obiektów łączności, stacji kryptograficznych, osoby konserwujące sprzęt, goście lub różnego rodzaju organizacje zainteresowane informacjami znajdującymi się w zasobach systemu).

Stąd też można powiedzieć, że największe zagrożenie dla bezpieczeństwa informacji w każdym systemie łączności i informatyki stanowi – CZŁOWIEK, którego należy rozumieć jako:

- nieautoryzowany użytkownik, posiadający odpowiednią wiedzę, ale nie posiadający dostępu do systemu, może posłużyć się nieświadomym pracownikiem stacji lub organu bezpieczeństwa do osiągnięcia swojego celu.
- użytkownicy terminali abonenckich nie mają dostępu do urządzeń komutacyjnych i ochrony kryptograficznej oraz oprogramowania systemowego i użytkowego tych urządzeń; mogą jednak - celowo lub przypadkowo - udostępniać osobom nieuprawnionym pozyskane (np. w czasie rozmowy telefonicznej) informacje.
- zagrożeniem dla informacji w systemie może być personel stacji kryptograficznej, który celowo lub nieświadomie (np. z powodu słabego przeszkolenia) może doprowadzić do zablokowania pracy poszczególnych urządzeń zainstalowanych na stacji lub błędnego ich działania.

Następnym zagadnieniem, które chciałbym poruszyć w trakcie swojego wystąpienia, są atrybuty bezpieczeństwa informacji w systemach teleinformacyjnych. Zaliczamy do nich:

- poufność;
- integralność;
- dostępność.

Utrata POUFNOŚCI

Jest to nieautoryzowane ujawnienie informacji przez nieuprawniony dostęp do urządzeń zainstalowanych w pomieszczeniu stacji lub terminali abonenckich.

Czynniki mogące spowodować utratę poufności:

- pokonanie zabezpieczeń fizycznych lub programowych;
- brak kontroli nad osobami przebywającymi w obszarze chronionym (PWŁ, aparatowni, SD);
- naprawy i konserwacje urządzeń przez osoby nieuprawnione;
- podsłuch lub podgląd;
- elektromagnetyczna emisja ujawniająca (AMSG-784);
- nieprzestrzeganie zasad instalacji urządzeń – nie zachowywanie odpowiednich odległości pomiędzy urządzeniami;
- nieprzestrzeganie zasad rozwijania aparatowni, (uziemienia bezpieczeństwa, strefy wokół aparatowni, kontrola dostępu)
- nieprzestrzeganie zasad bezpieczeństwa przy korzystaniu z technicznych środków łączności np.:
  - w czasie prowadzenia rozmów telefonicznych, - równoczesne prowadzenie rozmów z aparatów telefonicznych jawnego i niejawnego;
  - przesyłanie informacji klasyfikowanych za pośrednictwem urządzeń podsystemu jawnego (np. urządzeń telefaksowych).

Utrata INTEGRALNOŚCI

Jest to nieautoryzowana modyfikacja informacji oraz utrata prawidłowego i spójnego działania zasobów systemu.

Czynniki mogące spowodować utratę integralności:

- uszkodzenie, celowe lub przypadkowe, oprogramowania systemowego lub urządzeń systemu;
- celowe lub przypadkowe uszkodzenie, zniszczenie przekazywanych danych, będące wynikiem błędnego działania urządzeń komutacyjnych lub kryptograficznych;

- uszkodzenie, celowe lub przypadkowe, oprogramowania aplikacyjnego i użytkowego urządzeń komutacyjnych, kryptograficznych i zarządzających;
- infekcje wirusowe oprogramowania systemowego lub użytkowego. (CIRC)

Utrata DOSTĘPNOŚCI

Jest to odmowa autoryzowanego dostępu lub opóźnienie operacji krytycznych pod względem czasu lub celu.

Czynniki mogące spowodować utratę dostępności:

- wadliwie działające urządzenia lub oprogramowanie urządzeń;
- infekcje wirusowe oprogramowania systemowego lub użytkowego;
- utrata narzędzi dostępowych (klucze, hasła itp.);
- awarie zasilania – zaniki, brak zasilania;
- klęski żywiołowe – pożar, powódź.

Reasumując moje dotychczasowe wystąpienie pozwolę sobie na pewne uogólnienia i wnioski, które w sposób zwarty odniosą się do problematyki bezpieczeństwa informacji w mobilnych systemach telekomunikacyjnych eksploatowanych między innymi w jednostkach wojsk lądowych. Są to:

1. Polowe systemy telekomunikacyjne są podatne na różnego rodzaju zagrożenia dla bezpieczeństwa informacji.
2. Niezbędna jest ocena zagrożeń dla bezpieczeństwa informacji w systemie – *analiza ryzyka (Co chronić? Przed czym? W jaki sposób?). – adekwatność zastosowanych środków do zagrożeń;*
3. Największe zagrożenie dla systemu – *CZŁOWIEK*.
4. Konieczne jest zastosowanie dostępnych środków ochrony fizycznej, technicznej oraz organizacyjno-proceduralnych jako efekt przeprowadzonej analizy ryzyka.

Celem spełnienia tak sformułowanych wniosków należy stosować środki ochrony w następujących obszarach jak:

- fizyczne;
- techniczne;
- organizacyjno-proceduralne (m.in. SWB, Plan ochrony i obrony elementów węzła łączności).

LITERATURA:

KONOPKA L.: *Walka sieciocentryczna sposobem działania sił zbrojnych w przyszłości.* Myśl Wojskowa nr 2/2004, Warszawa.

MICHNIAK J.: *Kierowanie mobilnymi systemami łączności wojsk lądowych, Cz.I – Główne problemy*. AON, Warszawa 2002.

KUSINA B.: *Zarządzanie bezpieczeństwem teleinformatycznym.* Materiały edukacyjne EDUSOFT, Warszawa 2002.

DAŃCZAK A.: *Bezpieczeństwo informacji w SZ RP. Aspekty strategiczne*. Praca studyjna, AON, Warszawa 2002

ppłk mgr inż. Grzegorz Świdzikowski
Zakład Systemów łączności i Informatyki
Instytut Zarządzania i Dowodzenia
WWLąd AON

GRADACJA ZAGROŻEŃ DLA BEZPIECZEŃSTWA INFORMACJI W SYSTEMACH TELEKOMUNIKACYJNYCH

Moje wystąpienie podczas dzisiejszej konferencji będzie poświęcone określeniu gradacji, czyli innymi słowy stopnia ważności różnego rodzaju zagrożeń dla bezpieczeństwa informacji w systemach telekomunikacyjnych ze szczególnym uwzględnieniem systemów mobilnych, które w nomenklaturze wojskowej bardziej znane są jako systemy taktyczne.

Pozwolicie Państwo, że w pierwszej kolejności przedstawię ogólnie układ swojego wystąpienia, na które składa się:

- określenie i zdefiniowanie pojęcia zagrożenia dla bezpieczeństwa informacji;
- przyjęcie podziału zagrożeń – niezbędnego dla dalszych rozważań w moim wystąpieniu;
- sposobu dojścia do zawartej w temacie wystąpienia gradacji zagrożeń dla bezpieczeństwa informacji w polowych systemach telekomunikacyjnych (metody badawczej i związanych, a raczej przyjętych w procesie badań ograniczeń);
- przedstawienie wyników przeprowadzonego badania ankietowego;
- zapoznanie z opinią ekspertów, którzy wypowiedzieli się na ten sam temat co badani respondenci (płk dypl. Marek SOBCZAK, płk mgr inż. Andrzej DAŃCZAK);
- podsumowanie oraz wnioski.

Przechodząc do części zasadniczej, pozwolę sobie przedstawić przyjętą przeze mnie definicję zagrożeń dla bezpieczeństwa informacji w systemach telekomunikacyjnych oraz systemach teleinformatycznych. W wyniku przeprowadzonej analizy literatury fachowej z dziedziny bezpieczeństwa systemów telekomunikacyjnych i teleinformatycznych zdecydowałem się przyjąć do dalszych rozważań definicję zaczerpniętą z dokumentu sojuszniczego sygnowanego przez Komitet Wojskowy NATO MC-315/2 „Bezpieczeństwo informacji w systemach C3 NATO". U podstaw jej wyboru legł fakt, że odnosi się ona zarówno do zagrożeń, które można powiedzieć są efektem działania celowego, jak również obejmuje te zagrożenia, jak gdyby niezależne, niezamierzone, spowodowane czasami lekkomyślnością, brakiem wyszkolenia człowieka, pochodzą od sił przyrody. Jest to moim zdaniem definicja oddająca w pełni problem wynikający z zagrożeń, którego następstwem może być nieuprawnione lub nieplanowany dostęp, utrata lub ewentualnie modyfikacja prawnie chronionej informacji.

Drugim zasadniczym elementem, który jest nieodzowny przy określaniu gradacji zagrożeń jest ich podział. Tutaj również spotkałem się, zarówno w literaturze fachowej jak i w opinii ekspertów z różnym podejściem i z różnymi zdaniami co do podziału zagrożeń, szczególnie mając na uwadze aspekt bezpiecznej organizacji i funkcjonowania polowego systemu telekomunikacyjnego. W literaturze fachowej podziały tam dokonywane przez znawców tego zagadnienia miały charakter od najbardziej ogólnych (zewnętrzne, wewnętrzne) po szczegółowe, ale odnosiły się przede wszystkim do systemów stacjonarnych. Nowsze wydawnictwa natomiast skupiają się na bezpieczeństwie informacji w systemach teleinformatycznych, zapominając moim zdaniem o warstwie transmisyjnej, która realizowana jest w dalszym ciągu przez systemy telekomunikacyjne. Również w pracy studyjnej Pana płk Andrzeja Dańczaka przedstawiany podział odnosi się raczej do systemów szczebla strategicznego, które ze swojej natury mają charakter bardziej stacjonarny niż polowy.

Z tej przyczyny wyszedłem z założenia, że podziału zagrożeń można dokonać, opierając się na płaszczyznach, w których realizowane są normatywne przedsięwzięcia z zakresu bezpieczeństwa łączności i informatyki. Przedsięwzięcia te bowiem służą przecież ochronie zarówno samej informacji jak i całego systemu, czyli ich zadaniem jest eliminacja potencjalnych zagrożeń przed nieautoryzowanym

dostępem do systemu telekomunikacyjnego jak i jego zasobów informacyjnych, które pragniemy chronić.

Z tak usystematyzowaną wiedzą przystąpiłem do wypracowania metody, która pozwoliłaby na określenie gradacji, ważności poszczególnych zagrożeń w wojskowym, polowym systemie telekomunikacyjnym. Początkowo planowałem dokonać analizy dokumentacji kilku wybranych ćwiczeń, treningów sztabowych szczebla dywizyjnego, gdzie równolegle z planowaniem a następnie organizacją systemu łączności i informatyki, prowadzone były działania zapewniające ochronę informacji w tym systemie. Jednak dokumentacja zawiera suche fakty w zakresie organizacji i przedsięwzięć, które to bezpieczeństwo zapewniają. Nie wymieniane są ani potencjalne zagrożenia, ani faktyczne, które miały miejsce w czasie pracy systemu. Ten stan rzeczy uświadomił mi, że najlepszą metodą uzyskania potrzebnych danych mogę uzyskać w formie ankiety od etatowych pracowników organów bezpieczeństwa łączności i informatyki, którzy w swojej codziennej działalności służbowej spotykają się z problemami wynikającymi z potrzeby ochrony informacji w wojskowych systemach telekomunikacyjnych.

Jednocześnie narzuciłem w stosunku do respondentów pewne ograniczenia, które moim zdaniem mogą uwiarygodnić uzyskane wyniki z przeprowadzonych badań. Do ograniczeń powyższych zaliczyłem:

1. Etatowy pracownik organów bezpieczeństwa łączności i informatyki
2. Staż pracy - minimum 3 lata
3. Udział w ćwiczeniach, treningach sztabowych z udziałem wojsk - minimum 2-krotnie.

Sformułowałem zatem jedno pytanie, które przyjęło brzmienie: **Jakie jest prawdopodobieństwo wystąpienia zagrożenia ujawnienia lub utraty bezpieczeństwa informacji w polowym systemie telekomunikacyjnym związku taktycznego w kontekście implementowanych organizacyjno-technicznych i eksploatacyjnych środków ochrony informacji?**

Mając przyjęty już uprzednio podział zagrożeń, wybraną metodę badawczą, sformułowane pytanie oraz ograniczenia w stosunku do respondentów przystąpiłem do budowy formy i kształtu ankiety. Ostatecznie przyjęła ona kształt jaki

przedstawiony jest na slajdzie. Tzn. przyjąłem 5 stopni prawdopodobieństwa wystąpienia zagrożeń – od bardzo mało prawdopodobnego, bliskiego zeru, aż po prawie pewne wystąpienie danego zagrożenia – czyli prawdopodobieństwo jego wystąpienia jest bliskie jedności. W poszczególnych obszarach wynikających z przyjętego podziału wyodrębniłem zagrożenia szczegółowe – ich źródła, do których respondenci winni się ustosunkować.

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

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

Respondenci ogólnie ocenili, że zagrożenia pochodzące ze strony człowieka nazwane w kwestionariuszu ankiety personalnymi zagrożeniami na poziomie średnim (Średnie 28,57%, Małe 27,14%) – średnia arytmetyczna.

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

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

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

Wśród zagrożeń organizacyjno-proceduralnych wyróżniłem:

- niewłaściwy przydział uprawnień;
- brak lub niski poziom szkolenia;

- niezrozumiałe procedury postępowania w sytuacjach krytycznych;
- niewłaściwa struktura i/lub zakres kompetencji organów odpowiedzialnych za bezpieczeństwo w systemach telekomunikacyjnych.

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

Kolejny obszar zagrożeń rozpatrywany przez respondentów to zagrożenia techniczne. Jako pierwsze ocenie poddane były zagrożenia związane ochroną kryptograficzną.

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

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

Drugi czynnik składowy zagrożeń w obszarze technicznym stanowi emisja ujawniająca, do których szczególnie zaliczyłem:

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

W tym przypadku zauważyć można rozłożenie się opinii pomiędzy dużym a średnim poziomem zagrożenia, choć moim zdaniem w systemach polowych, które rozwijane są z reguły poza dużymi skupiskami ludzkimi (obszarach pozamiejskich) ten czynnik nie odgrywa tak dużego znaczenia jak dla systemów stacjonarnych - można posiłkować się choćby przykładem obiektów Sztabu Generalnego ich dyslokacji i tym samym zapewnienia stref bezpieczeństwa.

Następnym elementem w obszarze technicznym są zagrożenia programowe, które w pierwszej chwili kojarzą się raczej z systemami informatycznymi. Jednak skojarzenie to jest mylne bowiem współczesne urządzenia telekomunikacyjne w swojej strukturze wewnętrznej czy funkcjonalnej bazują na rozwiązaniach informatycznych.

Nowoczesne centrale telefoniczne można nazwać przecież minikomputerem, w którym prawidłowo funkcjonujące oprogramowanie stanowi o działaniu samej centrali. Jako szczegółowe zagrożenia w tym obszarze przyjąłem:

- brak procedur uwierzytelniania;
- łatwość dostępu do zasobów systemu (uprawnienia);
- możliwość instalacji prywatnego oprogramowania;
- możliwość wprowadzania nieautoryzowanych zmian w treści informacji (konfiguracji systemu);
- nie szyfrowanie informacji na nośnikach elektronicznych;
- słabe zabezpieczenia przed oprogramowaniem złośliwym;
- błędy użytkowników (celowe i niecelowe);
- błędy personelu technicznego (celowe i niecelowe).

60% respondentów stwierdziło, że najważniejszym zagrożeniem jest łatwość dostępu do zasobów informacyjnych systemu, czyli innymi słowy do urządzeń końcowych zapewniających wymianę informacji w trybie niejawnym. Jest to ściśle związane z nadawaniem uprawnień poszczególnym osobom funkcyjnym będących jednocześnie użytkownikami systemu w oparciu o zasadę wiedzy koniecznej (ang. need to know).

Drugim istotnym zagrożeniem w tym obszarze jest można powiedzieć słabość zabezpieczeń przed implementacją tzw. oprogramowania złośliwego. Chodzi tu o wirusy, bomby logiczne, konie trojańskie, itd. Temat jest chyba znany i nie ma konieczności jego rozwijania. Kolejne zagrożenia na które zwrócili uwagę respondenci to procedury uwierzytelniania oraz możliwość wprowadzania zmian w treści informacji czy nawet konfiguracji systemu.

Jako kolejne zagrożenia w obszarze technicznym to zagrożenia, związane z procesem przesyłania informacji – transmisyjne. Jako zagrożenia szczegółowe wymieniono:

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

Zagrożenia dla bezpieczeństwa informacji w procesie jej transmisji nabierają szczególnego znaczenia w mobilnych systemach telekomunikacyjnych ze względu, że informacja jest przesyłana przede wszystkim drogą radiową lub radioliniową. Jednak uzyskane wyniki nie zdają się tego potwierdzać.

Ostatnim elementem w obszarze technicznym są zagrożenia wynikające z zastosowania lub braku urządzeń lub systemów wsparcia technicznego. Jak wynika z przeprowadzonego badania ten element nie ma zasadniczego wpływu na poziom bezpieczeństwa informacji w polowym systemie telekomunikacyjnym – zagrożenia z tego wypływające mają małe lub średnie znaczenie w ocenie respondentów.

Podsumowując uzyskane wyniki, nie można powiedzieć o jednym, drugim, czy też kilku zagrożeniach, które w sposób ewidentny były faworyzowane przez badanych. Po uśrednieniu wyników większość z nich oscyluje na poziomie 30 - 40 % przy uwzględnieniu stopnia prawdopodobieństwa jego wystąpienia na poziomie dużym lub średnim.

Na tej podstawie można wysunąć hipotezę, że nie ma zagrożeń ważnych, ważniejszych lub mniej istotnych. Zagrożenia bowiem można odnosić do konkretnego żywego systemu, o określonej architekturze, działającego w określonym

środowisku tzn. otoczeniu bliższym i dalszym systemu, jak również uwarunkowań wewnętrznych i zewnętrznych, które wpływają na jego funkcjonowanie. Ponadto zagrożenia zależne są od szczegółowości polityki bezpieczeństwa, która określa przedsięwzięcia oraz środki zapobiegające nieplanowanym czy niezamierzonym ujawnieniom chronionej informacji.

W tej materii zasadniczą rolę odgrywa dobrze skonstruowane czytelne i zwarte prawo. Tego typu sformułowania przedstawione przeze mnie powyżej są odzwierciedleniem myśli respondentów, którzy w krótki sposób uzasadniali dokonany przez siebie wybór poziomu zagrożeń.

W celu skonfrontowania i potwierdzenia uzyskanych wyników z ankiety przeprowadziłem wywiady z ekspertami tak jak wcześniej wspomniałem Panem płk Markiem Sobczakiem oraz płk Andrzejem Dańczakiem. Potwierdzili obaj, że czynnikami determinującymi poziom zagrożeń czy nawet możliwość ich wystąpienia jest architektura i przeznaczenie samego systemu oraz warunki i otoczenie, w którym system ten funkcjonuje. Jednocześnie stwierdzili, że głównym czynnikiem stanowiącym o podjęciu działań, przedsięwzięć czy środków bezpieczeństwa w celu ochrony informacji w systemie są przyjmowane kryteria istotności zagrożeń, które w czasie funkcjonowania systemu mogą na niego wpływać.

Odpowiadając na pytanie, które z zagrożeń dla bezpieczeństwa informacji w polowych systemach telekomunikacyjnych są ich zdaniem najważniejsze bez wahania stwierdzili – człowiek, a zaraz po nim wymieniono zagrożenia nazwane przeze mnie wcześniej technicznymi.

Zmierzając już ku końcowi i przystępując do podsumowania nasuwa się jeden podstawowy wniosek. Zagrożenia dla bezpieczeństwa informacji w systemach telekomunikacyjnych nie są jednakowe dla każdego systemu. Zależą bowiem od jego organizacji, architektury, środowiska funkcjonowania oraz stosowanych środków ochrony. Inaczej planuje się i organizuje system telekomunikacyjny w działaniach obronnych. Architektura systemu inaczej wygląda przykładowo w działaniach zaczepnych – system jest mniej rozbudowany. Mając na uwadze środowisko funkcjonowania systemu to w tym aspekcie przede wszystkim rozpatrywałbym potencjalnego przeciwnika – jego zdolności i możliwości bojowe (rażenie ogniowe z powietrza i ziemi), taktykę działania (grupy dywersyjne, dywersyjno-rozpoznawcze) czy też posiadane przez niego siły i środki walki radioelektronicznej, które mogą i raczej będą oddziaływać na nasze systemy.

Zarówno cytowani przeze mnie eksperci jak i inni znawcy problemu uważają, że najsłabszym ogniwem w systemie bezpieczeństwa był, jest i będzie człowiek. Nikt nie urodził się przecież szpiegiem, szpiegiem zostaje się poprzez ludzkie ułomności czy też chęć zysku. Również brawura, roztargnienie, nie przestrzeganie lub lekceważenie procedur i przepisów leży u podstaw zagrożeń w wojskowym systemie telekomunikacyjnym.

Stosowane zabezpieczenia techniczne w obszarze kryptografii, emisji ujawniającej, transmisji, wsparcia technicznego czy programowe bądź inne wcześniej już omawiane nie spełnią zadania przed nimi stawianego jeśli zawiedzie człowiek.

Mówiąc już o zagrożeniach technicznych to wśród wymienionych za najbardziej ważne w odniesieniu do polowego systemu telekomunikacyjnego są zagrożenia dla kryptografii i transmisyjne – dlatego, że gro informacji przysyłana jest w warunkach technicznych środkami radiowymi i radioliniowymi. Emisja ujawniająca ma większe znaczenie w systemach stacjonarnych ze względu na ich usytuowanie. Tak samo możemy odnieść się do wsparcia technicznego, gdzie raczej w aparatowniach nie będzie stosowało się systemów antywłamaniowych i ppoż.

Zagrożenia programowe należy traktować jednolicie bez względu na rodzaj i miejsce w systemie.

Dobrze przygotowana polityka bezpieczeństwa, której zasadniczym elementem jest system bezpieczeństwa wymaga ustawicznego szkolenia kadry i pracowników, aby użytkownicy systemu oraz personel techniczny był na bieżąco zapoznawany z przyjętymi rozwiązaniami organizacyjnymi oraz procedurami bezpieczeństwa. Najlepiej byłoby, aby pewne procedury przeobrazić w podświadome nawyki – tak jak gaszenie światła przy wyjściu z oświetlonego pomieszczenia. Zdaję sobie sprawę, że jest to ideał, ale do niego winniśmy dążyć.

Jeśli natomiast mówimy o zagrożeniach fizycznych to większość z nich ma wpływ ale na systemy stacjonarne. Tutaj a mam na myśli systemy polowe nikt nie będzie przecież sprawdzał grubości ścian, krat w oknach itd. Również w przypadku klęski żywiołowej jak pożar lub powódź system bazuje na pojazdach kołowych i w każdej chwili ma możliwość oddalenia od zagrożonego rejonu.

Kończąc swoje wystąpienie chciałbym wspomnieć o jeszcze jednym aspekcie – dobre prawo, czytelne i przede wszystkim spójne dla każdego organizatora systemu telekomunikacyjnego, a szczególnie w odniesieniu do systemu bezpieczeństwa jest podstawą eliminacji potencjalnych zagrożeń. Nie może jednak ono pozwalać na

dowolną interpretację. Implementacja do systemu telekomunikacyjnego danego rozwiązania organizacyjnego lub technicznego winna być jednakowo rozumiana w całych siłach zbrojnych.

Wybaczcie Państwo na swego rodzaju uwagę, ale moim zdaniem bardzo ważną. Nie spotkałem się do tej pory z dedykowaną, zwartą publikacją naukową czy też normatywną, która poświęcona by była właśnie bezpieczeństwu w systemach mobilnych lub jak kto woli taktycznych. Z tej przyczyny dziedzina ta powinna stać się obszarem dociekań naukowych umożliwiających skonkretyzowanie wymagań i określenie standardów dla sieci i systemów szczebla taktycznego.

Dziękuję serdecznie za uwagę

LITERATURA:

1. Anderson R. H., Feldman P. M. – *Securing the U.S. Defense Information Infrastracture: A Proposed Approach, National Defense Research Institute 1999*
2. Bryczkowski Maciej - *Bezpieczeństwo systemów sieciowych, Postępy Kryminalistyki Nr 1/97.*
3. Goban-Klaus Tomasz, Sienkiewicz Piotr – *Społeczeństwo informacyjne: szanse, zagrożenia, wyzwania, Wydawnictwo Fundacji Postępu Telekomunikacji, Kraków 1999.*
4. Icove D. Seger K. von Storch - *A Crimefighter Handbook, O'Reilly&Associates 1999.*
5. Jakubski J.K. - *Polityka zabezpieczenia informacji - potrzeba czy wymóg. II Krajowa Konferencja Zastosowań Kryptografii - Enigma'98, Warszawa 26-28 maja 1998 r.*
6. Janczak J. – *Obrona informacyjna w działaniach obronnych związku operacyjnego, AON, Warszawa 2002.*
7. Kwećka R. – *Informacja w walce zbrojnej, AON, Warszawa 2001.*
8. Mąka D. – *Elementy zagrożeń i zarządzanie ryzykiem w świetle polityki bezpieczeństwa, IT Security Magazine, Nr 8-9, 2001.*
9. Michniak J. Wisz A. - *Bezpieczeństwo i ochrona informacji w wojskowych sieciach telekomunikacyjnych i zautomatyzowanych systemach: (zasady ogólne), AON, Warszawa 2000.*
10. Sienkiewicz P. Dańczak A. – *Praca studyjna „Bezpieczeństwo informacji w Siłach Zbrojnych RP. Aspekty strategiczne", AON, Warszawa 2002.*
11. Stokłosa J. Bilski T. Pankowski T. – *Bezpieczeństwo danych w systemach informatycznych, Wydawnictwa Naukowe PWN Poznań 2001*
12. Swanson M., Guttman B. - *Generally Accepted Principles and Practices for Securing Information Technology Systems, NIST, SP 800-14, September 1996*
13. 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.

ppłk Bogdan Rembacz
Wojskowe Służby Informacyjne
CAKiBT

BEZPIECZEŃSTWO INFORMACJI W MOBILNYCH SYSTEMACH TELEKOMUNIKACYJNYCH

UWARUNKOWANIA PRAWNE, ORGANIZACYJNE I TECHNICZNE

Problematyka bezpieczeństwa łączności i informatyki jest zagadnieniem obszernym obejmującym swoim zasięgiem zarówno przedsięwzięcia organizacyjne jak i techniczne. Przedsięwzięcia te regulują dokumenty normatywne w formie ustawy, rozporządzeń i dyrektyw.

Do aktualnie obowiązujących normatywów zalicza się:

- Ustawa z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych *(Dz.U. z 1999 r. Nr 11, poz. 95; z 2000 r. Nr 12, poz. 136, Nr 39, poz. 462; z 2001 r. Nr 22, poz. 247, Nr 27, poz. 298, Nr 56, poz. 580)*;

- Rozporządzenie Prezesa Rady Ministrów z dnia 25 lutego 1999 r. w sprawie podstawowych wymagań bezpieczeństwa systemów i sieci teleinformatycznych *(Dz.U. z 1999 r., Nr 18, poz. 162)*;

- Rozporządzenie Ministrów Spraw Wewnętrznych i Administracji oraz Obrony Narodowej z dnia 26 lutego 1999 r. w sprawie trybu i sposobu przyjmowania, przewożenia, wydawania i ochrony materiałów *(Dz. U. z 1999 r., Nr 18, poz. 168)*;

- Decyzja Nr 181/MON Ministra Obrony Narodowej z dnia 6 października 2000r. w sprawie organizacji szczególnej ochrony systemów i sieci teleinformatycznych w resorcie obrony narodowej;

- Decyzja Nr 182/MON Ministra Obrony Narodowej z dnia 6 października 2000r. w sprawie sprawowania nadzoru nad ochroną informacji niejawnych w resorcie obrony narodowej;

- 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;

- Polska norma obronna NO – 06 – A201.

Ponadto akty powyższe są uszczegółowione poprzez regulacje prawne wprowadzone do użytku w resorcie obrony narodowej Rozkazem Szefa Wojskowych Służb Informacyjnych:

- nr Pf-46 z dnia 26 czerwca 2000 r.;
- nr Pf-8 z dnia 07 lutego 2002 r.;
- nr Pf-92 z dnia 13 grudnia 2002 r.

Zaliczamy do nich między innymi:

- Dyrektywa AD 70 – 1PL Dowództwa Połączonych Sił Zbrojnych;

- ,,Wytyczne w sprawie instalacji urządzeń przeznaczonych do przetwarzania informacji niejawnych. BTPO-701A";

- ,,Wytyczne w zakresie bezpieczeństwa fizycznego kancelarii kryptograficznych, stacji łączności kryptograficznych oraz pomieszczeń wydzielonych przeznaczonych do przetwarzania informacji niejawnych. DBBT-301A";

- ,,Bezpieczeństwo systemów i sieci teleinformatycznych. Wskazówki i zalecenia. DBBT-801A";

- „Wytyczne w zakresie postępowania z materiałami kryptograficznymi. BTPO – 601A".

Wojskowe systemy telekomunikacyjne przeznaczone do wykorzystywania w warunkach polowych są systemami specyficznymi. Ich specyfika w kontekście choćby warunków i miejsca ich rozwinięcia wymaga zastosowania stosownych rozwiązań organizacyjnych ale i sprzętowych. Jednym z rozwiązań sprzętowych są kontenery polowe.

Kontenery polowe przeznaczone są do kompleksowej ochrony informacji niejawnych w warunkach polowych, uniemożliwiając jej przechwycenie we wszystkich fazach jej wytwarzania, przetwarzania, przesyłania i przechowywania.

Rozwiązania techniczne zastosowane w kontenerach winny zapewnić minimalne warunki ochronno-funkcjonalne adekwatne do klauzuli przetwarzanych informacji niejawnych i przeznaczenia kontenera.

Każdy kontener polowy, na którym planowana jest instalacja urządzeń łączności i informatyki przeznaczonych do funkcjonowania w ramach niejawnego systemu telekomunikacyjnego winien spełniać następujące ogólne wymagania:

- kontener powinien posiadać stosunkowo niewielki ciężar, umożliwiający w sposób łatwy załadunek *(rozładunek)* na podwozie transportowe dźwigiem *(wózkiem widłowym)* lub własnym mechanizmem załadowawczym.

- kontener winien spełniać następujące wymagania:
  - zapewniać minimalne warunki ochronno-funkcjonalne stosowane w stacjonarnych kancelariach kryptograficznych, stacjach łączności kryptograficznej, pomieszczeniach wydzielonych, adekwatne do klauzuli przetwarzanych informacji niejawnych i przeznaczenia kontenera;
  - być wykonany z płyt warstwowych, składających się z dwóch warstw blach *(stopów aluminiowych lub stali)* każda o grubości co najmniej 1 mm wzajemnie połączonych, przedzielonych co najmniej 50 mm warstwą twardego i niepalnego poliuretanu;
  - płyty warstwowe na narożach winny być zespawane i wyposażone w zaczepy transportowe umożliwiające mocowanie w czasie transportu:
    - lądowego *(na samochodach ciężarowych, lawetach kołowych i kolejowych)*;
    - powietrznego *(na samolotach transportowych, śmigłowcach)*;

♦ wodnego *(na statkach lub okrętach transportowych)*;

– posiadać jedne drzwi wejściowe, które muszą być:
  - blokowane na czterech krawędziach, zawiasy powinny być umieszczone po wewnętrznej stronie drzwi i zabezpieczone przed wyważeniem. W przypadku zawiasów umieszczonych na zewnątrz, ich sworznie powinny być zalutowane mosiądzem lub zaspawane w celu uniemożliwienia prób nieuprawnionego zdjęcia drzwi;
  - wyposażone w dwa zamki, w tym jeden mechaniczny, drugi szyfrowy *(pkt 6.2. „DBBT 301A")*;
  - ryglowane od wewnątrz i wyposażone w mechanizm uniemożliwiający ich zablokowanie od zewnątrz przez osoby nieupoważnione;
  - wyposażone w mechanizm samozamykający.

– posiadać właz ewakuacyjny otwierany od wewnątrz, który powinien być zabezpieczony systemem alarmowym;

– nie może posiadać otworów okiennych;

– system oświetlenia musi być tak zaprojektowany, aby umożliwił 24 godzinną pracę personelu przy zamkniętych drzwiach wejściowych *(zgodnie z odpowiednimi wymaganiami bhp)*;

– kontener powinien być przystosowany do funkcjonowania w różnych warunkach atmosferycznych i klimatycznych.

– kontener musi być wyposażony w system klimatyzacji oraz urządzenia filtrowentylacji *(otwory wentylacyjne muszą być zabezpieczone siatką stalową o średnicy oczka 10 mm oraz wyposażone od wewnątrz w otwory rewizyjne umożliwiające kontrolę przewodów wentylacyjnych)*.

– instalacje zasilające i telekomunikacyjne winny być zabezpieczone dodatkowymi obwodami celem zapewnienia ciągłości pracy w sytuacjach awaryjnych.

Znając ogólne wymagania możemy zastanowić się jakim kryteriom bezpieczeństwa winien odpowiadać kontener. Stąd też wynika że wyposażenie kontenera polowego w środki bezpieczeństwa winno być adekwatne do:

- klauzuli tajności wytwarzanych, przetwarzanych, przechowywanych lub przesyłanych informacji niejawnych.

- łączność dla potrzeb personelu *(obsługi)* kontenera polowego *(aparatowni)* powinna być zapewniona poprzez zewnętrzne i wewnętrzne przyłącza abonenckie:
  - w ogólnym systemie telefonicznym stanowiska dowodzenia;
  - w systemach łączności niejawnej *(np. PCŁU);*
  - w sieciach teleinformatycznych *(np. LAN, WAN, SEC-WAN itp.)*.

- kontener polowy musi być wyposażony w przeciwpożarowy system alarmowy, systemy sygnalizujące próby siłowego otwarcia drzwi wejściowych oraz wykrywające ruch po zamknięciu.

- systemy i urządzenia alarmowe powinny odpowiadać następującym klasom:
  - **SA4** w przypadku przechowywania dokumentów zawierających informacje stanowiące tajemnicę państwową;
  - **SA3** w przypadku przechowywania dokumentów zawierających informacje stanowiące tajemnicę służbową. *(wymagania dotyczące ww. systemów zawarte są w „...DBBT 301A").*

- urządzenia i instalacje teletechniczne *(alarmowe, sygnałowe i energetyczne)* winny być wykonane zgodnie z „BTPO-701A".

- tłumienność sygnałów w zakresie emisji elektromagnetycznej kontenera powinna zapewniać bezpieczne zainstalowanie w kontenerze polowym urządzeń o **poziomie zabezpieczenia urządzenia 1** ***(PZU-1)*** zgodnie z „BTPO-701A" *(wg. AMSG-788A)*.

- niezależne zasilanie wprowadzane poprzez system filtrów – ~220V i pokładowe 27V *(oddzielne zasilanie dla obwodów typu **BLACK** i **RED**)* spełniające wymagania zawarte w „BTPO-701A" dla obiektów mobilnych.

- kontener polowy winien posiadać przyłącza i obwody telekomunikacyjne dla jawnych i niejawnych systemów łączności i informatyki spełniające wymagania zawarte w „BTPO-701A".

- kontener polowy winien posiadać uziemienie wykonane zgodnie z „BTPO-701A" dla obiektów mobilnych.

- sygnalizacja alarmowa *(akustyczna i świetlna)* powinna być wyprowadzona do wartowni *(dowódcy warty)*.

- kontener polowy winien być wyposażony w słupki i taśmę do oznakowania granic strefy bezpieczeństwa.

- kontener polowy winien posiadać akustyczną możliwość wywołania personelu *(obsługi)* oraz umożliwiać identyfikację osób wywołujących *(np. dzwonek, videofon, domofon. itp.)*.

- w dokumentacji eksploatacyjnej kontenera polowego winny być określone szczegółowe warunki zapewnienia bezpieczeństwa systemom łączności i informatyki, ochrony informacji niejawnych i określania stref bezpieczeństwa, a także zasady bezpieczeństwa w czasie przechowywania, użytkowania, transportowania kontenera jak i prowadzenia okresowych testów i sprawdzeń.

- w kontenerze powinno być wydzielone miejsce przeznaczone do zapoznawania upoważnionych osób funkcyjnych z dokumentami niejawnymi, w taki sposób, aby personel *(obsługa)* miał nad nimi stałą kontrolę.

- kontener polowy należy wyposażyć w sprzęt wymagany przepisami „DBBT 301A" i stosownie do przeznaczenia kontenera.

Celem dopuszczenia takiego kontenera do eksploatacji w niejawnych systemach telekomunikacyjnych musi on posiadać dokumentację techniczną, którą należy wykonać zgodnie z DUTW-73 z uwzględnieniem zmian wynikających z WPN-84/N-01001 załącznik informacyjny 4 i nowych lub znowelizowanych Polskich Norm oraz innych aktualnie obowiązujących przepisów ogólnych jak i wojskowych, która powinna zawierać:

- dokumentację techniczną, w tym:
  - warunki techniczne *(WT)*;
  - dokumentację konstrukcyjną *(DK)*;
  - opis techniczny *(OT)*.

- instrukcje eksploatacji, opis i ukompletowanie.

W zależności od wyposażenia i zastosowanych zabezpieczeń kontenery mogą być wykorzystywane jako:

- Kancelarie kryptograficzne;
- Stacje łączności kryptograficznej;
- Kancelarie tajne;
- Pomieszczenia wydzielone.

Polowe kontenerowe kancelarie kryptograficzne, stacje łączności kryptograficznej oraz pomieszczenia wydzielone winny posiadać akceptację Wojskowych Służb Informacyjnych.

DOWÓDZTWO WOJSK LĄDOWYCH
ZARZĄD DOWODZENIA I ŁĄCZNOŚCI
ODDZIAŁ BEZPIECZEŃSTWA
SYSTEMÓW ŁĄCZNOŚCI I INFORMATYKI

PRZEDSIĘWZIĘCIA ORGANIZACYJNO-TECHNICZNE ZAPEWNIAJĄCE BEZPIECZEŃSTWO INFORMACJI W POLOWYCH SYSTEMACH TELEKOMUNIKACYJNYCH WOJSK LĄDOWYCH.

kpt. mgr inż. Mariusz Frączek

W A R S Z A W A 2004

WSTĘP

Sieć telekomunikacyjna jest zespołem środków organizacyjno-technicznych pozwalających na wykorzystanie urządzeń i linii telekomunikacyjnych w celu zorganizowania i zapewnienia sprawnego obiegu informacji zgodnie z potrzebami jej użytkowników (informacji w postaci sygnałów). Jest systemem o złożonej strukturze, zmiennej w czasie i przestrzeni. Świadczy usługi przekazywania informacji w sposób szybki i niezawodny.[1]

Sieć telekomunikacyjna jest elementem systemu telekomunikacyjnego państwa, który tworzą urządzenia i linie telekomunikacyjne zorganizowane według określonych zasad oraz współpracujące ze sobą i służące do nadawania, przenoszenia i odbioru mowy, dźwięków, znaków pisma, obrazów oraz wszelkich, innych postaci informacji. Może być użytku publicznego (oferuje usługi telekomunikacyjne o charakterze powszechnym) lub wewnętrzna (oferuje usługi dla wybranego grona użytkowników –np.: dla SZ RP, Straży Granicznej, Policji, energetyki, PKP). Istnieją różne podziały sieci telekomunikacyjnych rozpatrywane w zależności od charakteru przyjętych kryteriów (postać sygnałów, sposób przekazywania informacji, na dostępność dla abonentów znajdujących się w ruchu i w ściśle określonych miejscach).

Polowy system telekomunikacyjny jest częścią systemu telekomunikacyjnego państwa przeznaczonym do zapewnienia obiegu informacji dla potrzeb sił zbrojnych w okresie ćwiczeń i szkoleń, a przede wszystkim do kierowania obronnością państwa w okresie zagrożenia wojennego i wojny. Jest samodzielnym zespołem sił oraz środków łączności i informatyki, rozwiniętym i połączonym w sposób odpowiadający organizacji dowodzenia, charakterowi prowadzonych działań i wykonywanym zadaniom. Dzięki niemu może funkcjonować dowodzenie siłami zbrojnymi, a także może być zapewniona łączność z siłami układu pozamilitarnego. W wojskach lądowych wyróżnia się dwa podstawowe systemy informacyjnego wsparcia dowodzenia: KOLORADO (dla szczebla operacyjnego) oraz SZAFRAN (dla szczebla związku taktycznego). Należy również wspomnieć, że w obszarze odpowiedzialności wojsk lądowych będą funkcjonowały systemy kierowania środkami walki takie jak:

---

[1] Definicja własna opracowana na podstawie: J.Mazurkiewicz, Leksykon łączności wojskowej, Warszawa AON, 1996, s.180 oraz J.Michniak, Z.Fiołna, Sieć łączności państwa, Warszawa AON, 2001, s.12.

TOPAZ i RODON w WRiA oraz ŻBIK w rozpoznaniu.[2] Użytkowanym polowym systemom telekomunikacyjnym należy zapewnić bezpieczeństwo ich działania oraz bezpieczeństwo przekazywanych w nich informacji.

Bezpieczeństwo można rozumieć jako stan, który daje poczucie pewności i gwarancje jego zachowania oraz szansę jego doskonalenia, oznacza brak ryzyka utraty czegoś, co człowiek szczególnie ceni. Określić tym terminem można stan uzyskany w wyniku zorganizowanej ochrony (przedsięwzięć organizacyjno-technicznych) przed możliwymi zagrożeniami, wyrażony stosunkiem posiadanego potencjału przeznaczonego do zapewnienia ochrony, planów i możliwości wykorzystania sił i środków odpowiednio do skali zagrożeń.[3]

Warto przypomnieć, że problematyka bezpiecznego przekazywania informacji narodziła się wraz z rozwojem technik umożliwiających komunikowanie się ludzi i związana jest z potrzebą przesyłania wiadomości w sposób utrudniający do niej dostęp osób nieuprawnionych. Zawsze istniała potrzeba ochrony ważnych informacji oraz istniały powody dla których ktoś pragnął je zdobyć.

PRZEDSIĘWZIĘCIA OCHRONY TECHNICZNEJ POLOWYCH SYSTEMÓW TELEKOMUNIKACYJNYCH WOJSK LĄDOWYCH.

Niezależnie od czasu funkcjonowania (okres pokoju lub wojny) urządzeniom technicznym przekazującym informacje w polowych systemach telekomunikacyjnych stawiane są wymagania dotyczące zabezpieczenia przekazywanych za ich pomocą wiadomości. Zastosowane urządzenia powinny posiadać zabezpieczenia uniemożliwiające zdobycie tych wiadomości przez osoby nieuprawnione. Odpowiedni sposób przekazywania informacji, identyfikacji urządzeń i połączeń oraz zabezpieczenie techniczne użytkowanego sprzętu powoduje stworzenie przeszkód (barier) dla osób nieuprawnionych skutecznie ochraniające informacje. W odniesieniu do takiego wymogu, gdy jest skomplikowany sposób wykorzystania,

[2] L. Stypik, Co nieco na temat systemów dowodzenia, PWL nr 2 (536) luty 2004, s. 75.
[3] Definicję bezpieczeństwa sformułowano na podstawie: B.Balcerowicz, Słownik terminów bezpieczeństwa narodowego, Warszawa AON 2002,s. 13-17, oraz J.Mazurkiewicz, Leksykon łączności wojskowej, Warszawa AON 1996, s.22.

identyfikacji urządzeń przekazujących, połączeń oraz ich zabezpieczenia, tym lepiej wiadomości są chronione. Ochronę techniczną w polowych systemach można podzielić na pięć zasadniczych grup:

- **zabezpieczenie sprzętowe polowych systemów telekomunikacyjnych;**
- **ochronę elektromagnetyczną;**
- **ochronę oprogramowania;**
- **ochronę fizyczną urządzeń;**
- **ochronę kryptograficzną.**

Zabezpieczenie sprzętowe polowych systemów telekomunikacyjnych.

Urządzenia pracujące w polowych systemach telekomunikacyjnych wojsk lądowych powinny zapewniać trwałość i ciągłość pracy oraz, w zależności od umiejscowienia, pożądany poziom zabezpieczenia przekazywanych wiadomości. Najlepiej by było, aby użytkowany sprzęt posiadał możliwość identyfikacji innych urządzeń z nim współpracujących za zasadzie swój-obcy. Wskazana jest również opcja pozwalająca na monitorowanie i stwierdzanie prób dostania się lub ingerencji w treści wiadomości. To spostrzeżenie pozwala także przypuszczać, iż zasadnym jest tworzenie i używanie różnego rodzaju kodów i znaków zabezpieczających, których zainstalowanie uniemożliwia niezauważone ich pominięcie. Nad takim rozwiązaniem zawsze pracuje wydzielona i ściśle sprawdzona grupa ekspertów, których wysiłki zmierzają do stworzenia skutecznego systemu ochrony dla przekazywanych informacji.

Podczas pracy urządzenia z innymi, nie może być również sposobu jego podmiany na inne bez naruszenia zabezpieczeń[4]. Zewnętrzne wejścia-wyjścia do urządzenia należałoby maksymalnie wykorzystać. Utrudni to niezauważone i nieuprawnione próby podłączenia. W wypadku niewykorzystywania do pracy wszystkich wejść-wyjść należy je zablokować (zatkać, oplombować) w sposób, w którym nie będzie możliwości ominięcia takich odpowiednio wykonanych zabezpieczeń.

[4] J.Plewa. Techniczne i organizacyjne środki ochrony systemów łączności, AON Warszawa 2001, s.18.

Urządzenia powinny spełniać wymagania odporności na zakłócenia i możliwości usunięcia danych, które ze względu na swój niejawny charakter nie powinny być ujawnione[5] podczas ich pracy jak i ewentualnych serwisów (napraw) oraz mieć zabezpieczenia utrudniające podsłuch, możliwość zabezpieczenia kodami dostępu do odpowiednich poziomów informacji. Ważne jest aby od zakupu sprzętu spełniającego wymagania bezpiecznego przekazywania informacji w polowych systemach telekomunikacyjnych prowadzić w nieprzerwany sposób jego ewidencję pracy, użytkowników oraz kontroli i remontów.

Z bezpieczeństwem systemów telekomunikacyjnych nieodzownie wiążą się spore nakłady finansowe na zgodne z potrzebami ochrony zabezpieczenie linii i urządzeń znajdujących się w strefach bezpieczeństwa oraz poza nimi. Wymaga to także wzrostu wymagalności w stosunku do procedur identyfikacji naruszeń systemu telekomunikacyjnego. W związku zaistnieniem powyższych faktów za optymalne uznano stosowanie linii światłowodowych, które gwarantują wysokie bezpieczeństwo przekazywania informacji i utrudniają bez ich fizycznego uszkodzenia, podsłuchiwania przesyłanych wiadomości (za wyjątkiem zastosowania trójnika światłowodowego, założenia sondy lub wygięcia włókna światłowodowego w kablu, ale można wykonać to posiadając wysokiej jakości sprzęt do detekcji sygnału).

Na zabezpieczenie sprzętowe systemów telekomunikacyjnych duży wpływ ma również utrzymanie stałego zasilania pracy urządzeń przekazujących informacje, jak również przestrzeganie wymogów bezpieczeństwa określonych w instrukcjach obsługi urządzeń czy też instrukcjach przeciwpożarowych.

Ochrona elektromagnetyczna.

Bezpieczeństwo elektromagnetyczne ma służyć ochronie technicznej polowych systemów telekomunikacyjnych i może stanowić poważną barierę w uzyskiwaniu informacji przez osoby chcące je zdobyć. Często lokalizacja urządzeń przekazujących (gromadzących i przetwarzających) w miejscach trudnodostępnych (np. pod ziemią, w specjalnie zabezpieczonych pomieszczeniach lub rejonach rozmieszczenia) może być najlepsza dla bezpieczeństwa przesyłania informacji. W połączeniu z ochroną

[5] J.Plewa, Techniczne i organizacyjne środki ochrony systemów łączności, AON Warszawa 2001,s.19

fizyczną, a także dostępem do stref bezpieczeństwa daje to możliwość skutecznej ochrony technicznej zgodnie z ustawą o „Ochronie informacji niejawnych" (DZ.U. nr 11, poz.95).

Od strony technicznej zapewnienie bezpieczeństwa przed emisją elektromagnetyczną polowych systemów telekomunikacyjnych można realizować w wyniku:

1. ekranowania komputerów, urządzeń przekazujących i ich okablowania, pomieszczeń, gdzie one pracują oraz stosowanie kabin ekranujących;
2. wprowadzania urządzeń o bardzo małej mocy, a tym samym niskiej emisji ujawniającej.

Przepisy o ochronie elektromagnetycznej zawarte są w 10 rozdziale „Ustawy ochronie informacji niejawnych" oraz wytycznych w art.7 Rozporządzenia Prezesa Rady Ministrów z 25 lutego 1999 roku w sprawie podstawowych wymagań bezpieczeństwa systemów i sieci teleinformatycznych:

- „ochronę elektromagnetyczną systemu lub sieci zapewnia się przez umieszczenie urządzeń, połączeń i linii w strefach bezpieczeństwa gwarantujących spełnienie wymogów zabezpieczenia elektromagnetycznego lub stosowanie urządzeń, połączeń i linii o obniżonym poziomie emisji lub ich ekranowanie i filtrowanie zewnętrznych linii zasilających i sygnałowych".[6]

Jest to wyzwanie przed którym stoi wielu projektujących rozmieszczenie urządzeń elektromagnetycznych mogących gromadzić, przetwarzać oraz przekazywać różnego typu wiadomości niejawne. Obniżenie poziomu promieniowania ujawniającego sieci telekomunikacyjne mogą uzyskać poprzez wykorzystanie sprzętu komputerowego klasy TEMPEST, wcześniej wspomnianych łączy światłowodowych,[7] transmisji sygnałów specjalnie przygotowanymi i zabezpieczonymi liniami telekomunikacyjnymi, stosowanie kodowania informacji, czy też urządzeń o zmniejszonej emisji elektromagnetycznej.

W tym miejscu należy jeszcze zwrócić uwagę na kilka istotnych informacji o ochronie elektromagnetycznej zawartych w literaturze[8]:

---

[6] Rozporządzenie Rady Ministrów z 23.02.1999 (Dz.U. 99.18.166), s.28
[7] M. Szaliłow, Organizacyjno-prawne aspekty ochrony systemów łączności i informacji w nich przesyłanej, AON Warszawa 2001, s.29
[8] A. Dańczak Bezpieczeństwo informacji w SZ. Aspekty strategiczne, Warszawa 2002, s. 42, s.46-47.

1. Bezpieczeństwo emisji *(EMSEC - Emanation Security),* to przedsięwzięcia techniczne utrudniające przejęcie informacji zawartej w ubocznym promieniowaniu elektromagnetycznym urządzeń przetwarzających i przesyłających nieutajnione informacje niejawne.
2. Ochronę elektromagnetyczną urządzeń elektronicznych, zapewnia się poprzez separację przestrzenną urządzeń, filtrowanie zewnętrznych linii zasilających i sygnałowych oraz wybór jednego z poniższych wariantów:
   - umieszczenie urządzeń, połączeń i linii w strefach bezpieczeństwa gwarantujących spełnienie wymogów zabezpieczenia elektromagnetycznego;
   - zastosowanie urządzeń, połączeń i linii o obniżonym poziomie emisji;
   - ekranowanie urządzeń, połączeń i linii.
3. Podstawowe działania w dziedzinie technicznych metod ochrony informacji niejawnych przed ulotem, opierają się na dążeniu do ograniczenia poziomu emisji ujawniającej, z wykorzystaniem właściwości i zjawisk fizycznych[9]:

   - tłumienia fali elektromagnetycznej, jej odbicia i pochłaniania;

   - uziemiania, ekranowania i filtrowania;

   - doboru parametrów czasowo-częstotliwościowych sygnałów użytecznych.

W „Szczególnych Wymaganiach Bezpieczeństwa dla MPCŁU z wykorzystaniem aparatowni łączności typu RWŁC" oraz „Szczególnych Wymaganiach Bezpieczeństwa Procedury Bezpieczeństwa dla MPCŁU z wykorzystaniem aparatowni łączności typu RWŁC" poruszany jest problem zdefiniowania i określenia takich środowisk dla danego SD jak:

- Globalne Środowisko Bezpieczeństwa (GŚB) - cały obszar danego stanowiska dowodzenia (PWŁ), w którym rozwinięte są sieci abonenckie i lokalne sieci komputerowe. Obejmuje wszystko, co znajduje się poza bezpośrednią, fizyczną kontrolą dowódcy aparatowni i to co może mieć związek z bezpieczeństwem tej sieci. Wejście do GŚB odbywa się na podstawie aktualnych dokumentów wystawionych przez komendanta SD.

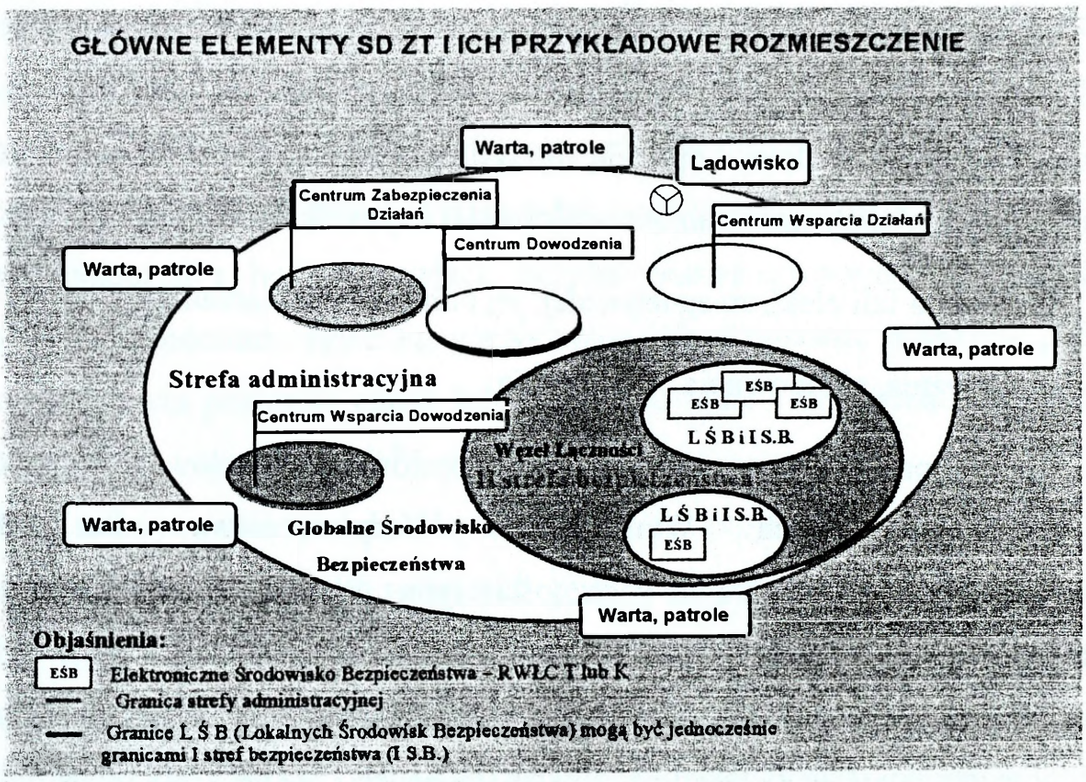
---

[9] A. Dańczak Bezpieczeństwo informacji w SZ. Aspekty strategiczne, Warszawa 2002, s. 42, s.46-47.

Znajduje się pod bezpośrednim nadzorem pełnomocnika dowódcy ds. ochrony informacji niejawnych.

- Lokalne Środowiska Bezpieczeństwa (LŚB) - rejony (oraz wyznaczony obszar) węzłów łączności na SD, gdzie są rozmieszczone aparatownie typu RWŁC, za które odpowiadają dowódcy RWŁC.
- Elektroniczne Środowisko Bezpieczeństwa (EŚB) – aparatownie RWŁC typu T lub K.

Wszystkie powyższe informacje są istotne z punktu szczebla stanowiska dowodzenia oraz rzeczywistych warunków na danym stanowisku dowodzenia (patrz rysunek 1).



Rysunek 1 – Główne elementy SD ZT i ich przykładowe rozmieszczenie[10]

[10] źródło – zmodyfikowany slajd prezentacji płk Józefa Michniaka – Szefa Instytutu Dowodzenia i Łączności AON.

Oprogramowanie, a bezpieczeństwo polowych systemów telekomunikacyjnych.

Oprogramowanie umożliwia działanie urządzeń wykorzystując ustalone mechanizmy zarządzania oraz kolejność realizacji poszczególnych zadań (np.: SZAŁ-99). Jego właściwości pozwalają również na prawidłowe funkcjonowanie systemów telekomunikacyjnych. Zawiera procesy umożliwiające gromadzenie, przetwarzanie i przekazywanie informacji, a od zastosowania określonego oprogramowania mogą wyniknąć określone działania. Zgodnie z „Ustawą o ochronie informacji niejawnych" (rozdział 10, art. 60), wszelkie oprogramowanie w sieciach (systemach) telekomunikacyjnych powinno pochodzić z legalnego źródła i posiadać certyfikat.

Stosowane w wojskach lądowych polowe systemy telekomunikacyjne również wykorzystują zaprogramowane mechanizmy sterowania oraz bezpieczeństwa. Powoduje to określenie wymagań do oprogramowania przez jego użytkowników warunkujące bezpieczeństwo informacji także podczas jej przekazywania. Z tego też względu dopuszcza się do użytku tylko zakupione oprogramowanie. Następnie dokonuje się badań przydatności do skutecznego zapewnienia ochrony informacji niejawnych oraz przeprowadza się kontrole mogące ujawnić jego wady i urządzeń w nie wyposażonych.

W moim przekonaniu, uwzględniając istniejące współcześnie potrzeby, bezpieczne oprogramowanie powinno umożliwiać:

1. realizację połączeń;
2. stworzenie bariery lub dużego utrudnienia we wprowadzeniu zainfekowanego oprogramowania – mogącego mieć trwałe skutki w postaci niesprawności systemu;
3. kontrole dostępu do informacji niejawnych przekazywanych w danym systemie telekomunikacyjnym (identyfikacja swój-obcy);
4. zmianę kodów dostępu przez osoby uprawnione – zdalne sterowanie sieciami;
5. identyfikację oprogramowania, profesjonalnej pomocy serwisowej, dostosowywanie do nowych oczekiwań;

6. spełnienie narzuconych norm bezpieczeństwa (barierę powyżej której dostęp do oprogramowania nie występuje), a jednocześnie pozwala na prace przy nim w zakresie jego modernizacji, kontroli, sporządzania sprawozdań z pracy.

Wskazuje to na fakt, że samo oprogramowanie nie będzie spełniać swojej roli bez powiązania go z innymi elementami ochrony technicznej sieci telekomunikacyjnych. Zapewnienie większego bezpieczeństwa przekazywania informacji oraz minimalizacja (wykluczenie) ilości błędów w przekazie jest ściśle związanez wykorzystaniem sprawdzonego oprogramowania.

Ochrona fizyczna.

Ochrona fizyczna jest jednym z fundamentów mających wpływ na ochronę stosowanych polowych systemów telekomunikacyjnych. Ochrona fizyczna zapewniona jest w wyniku zabezpieczenia rejonów rozmieszczenia stanowisk dowodzenia oraz elementów węzłów łączności (zgodnie z obowiązującymi przepisami oraz nadanymi numerami stref bezpieczeństwa). Wyznacza się i trwale oddziela strefy z ograniczeniem możliwości wejścia i wyjścia w zależności od klauzuli tajności informacji, a także charakteru zagrożeń w zakresie ich ujawnienia. Ma to zapewnić ochronę tych wiadomości z jednoczesnym pozwoleniem na korzystanie z ich zasobów przez osoby uprawnione. Za bezpieczeństwo informacji odpowiada przede wszystkim dowódca, który powinien to realizować poprzez pełnomocnika dowódcy ds. ochrony informacji niejawnych ściśle współpracującego z szefem wydziału (sekcji wsparcia) dowodzenia i łączności.[11]

Przyjmuje się, że właściwy poziom ochrony fizycznej poszczególnych wiadomości może być zapewniony, gdy zostaną spełnione następujące wymagania dla rejonów rozwinięcia elementów polowego systemu telekomunikacyjnego, w których znajdują się źródła informacji:

1. właściwie opracowany „Plan ochrony i obrony SD" danego szczebla uwzględniający możliwości poszczególnej jednostki wojskowej;

[11] Jednakże obowiązująca jeszcze literatura (Tymczasowe zasady organizacji, funkcjonowania i bezpieczeństwa łączności utajnionej w SZ PRL, W-wa 1988, sygn. Łączn. 928/88.) podaje również szefa sztabu danego szczebla.

2. przestrzeganie zaleceń oraz norm dotyczących ochrony i obrony elementów węzłów łączności zapewniających łączność niejawną:

a) strefa bezpieczeństwa od aparatowni typu RWŁC najmniej 3 metry, wyznaczony wartownik, rejon rozmieszczenia ogrodzony czerwoną taśmą na wysokości od 60 do 120 cm nad ziemią, odległość pomiędzy aparatowniami do 100 metrów;[12]

b) odległość minimalna pomiędzy aparatowniami RWŁC powinna wynosić 100 metrów, odległość aparatowni od radiostacji KF/UKF średniej mocy - nie mniej niż 1000 metrów, odległość aparatowni nie mniej niż 500 metrów od linii wysokiego napięcia, kable abonenckie - nie mniej niż 1 m od innych kabli;[13]

c) cały obszar danego stanowiska dowodzenia (pomocniczego węzła łączności) stanowi Globalne Środowisko Bezpieczeństwa pod nadzorem pełnomocnika ds. ochrony informacji niejawnych (warunki czasu „P"), a rejon węzła łączności na SD, a zwłaszcza miejsce rozmieszczenia aparatowni typu RWŁC, powinno być wyznaczone jako Lokalne Środowisko Bezpieczeństwa – najmniej 20 metrów od aparatowni, taśma ogrodzeniowa, wartownik, każdorazowy wpis w dziennik aparatowni o wejściu do I strefy (kontenera aparatowni). W II strefie bezpieczeństwa należy stworzyć system przepustek, system przechowywania kluczy, warty, posterunki i patrole, ochronę linii abonenckich MPCŁU.[14]

d) należy wyznaczyć strefy ochronne od użytkowanych aparatów typu AC-16MK-16, AP-92/ATS-2p lub 2c;

e) należy pamiętać o możliwościach technicznych kabla TKM10x2, kabla światłowodowego (przepływność 64-2048 kbit/s, dwa odcinki po 800 m), kabla PKD 1x4 (odcinek 750 m – do 8196 kbit/s), że dla R-432A wysokość anteny do pracy wynosi 24-28 metrów (maksymalnie 35 metrów, przepływność 256-2048 kbit/s);[15]

---

[12] Wytyczne w sprawie instalacji urządzeń przeznaczonych do przetwarzania informacji niejawnych. BTPO- 701A ,str.20.

[13] Szczególne Wymagania Bezpieczeństwa dla MPCŁU z wykorzystaniem aparatowni łączności typu RWŁC oraz Szczególne Wymagania Bezpieczeństwa Procedury Bezpieczeństwa dla MPCŁU z wykorzystaniem aparatowni łączności typu RWŁC. Przy czym stosowanie tego wymogu wiąże się z zaopatrzeniem aparatowni typu RWŁC w taśmę o długości najmniej 630 metrów (dla obwodu koła o promieniu r=100 m).

[14] tamże

[15] tamże

f) iż zapewnienie bezpieczeństwa, to nie tylko zadania lokalnego administratora MPCŁU, lecz także dowódcy RWŁC oraz personelu technicznego - starszego operatora RWŁC.[16]

g) konserwacja i naprawy w warunkach polowych tylko w obecności załogi – odnotować w dokumentacji aparatowni;[17]

h) meldowanie o naruszeniu bezpieczeństwa do Wojskowych Służb Informacyjnych drogą służbową i przez Wojskowe Biuro Bezpieczeństwa Łączności i Informatyki – odnotować w dokumentacji czego dotyczy: osoby, sprzęt, oprogramowanie, komunikacja, dokumenty.[18]

3. wyposażenie w sejfy dla dokumentów, które nie są bezpośrednio przekazywane przez system telekomunikacyjny (np. instrukcje, opisy urządzeń), ale stanowią źródła informacji niejawnych;
4. zorganizowanie systemu ochrony i obrony przed dostępem do aparatowni typu RWŁC (kancelarii kryptograficznych i tajnych), alarmowania o wejściu osoby nieuprawnionej do wyznaczonej strefy oraz uruchomienie alarmu do czasu przybycia osób odpowiedzialnych za ochronę (wartownicy, patrol);[19]
5. zorganizowanie systemu przeciwpożarowego;
6. być uodpornione na oddziaływanie z zewnątrz (zwłaszcza pomieszczenia aparatowni z urządzeniami służącymi do łączności niejawnej lub ułatwiające dostęp do danego systemu telekomunikacyjnego);
7. gwarantować stałe warunki pracy (wentylacja, klimatyzacja, poziom wilgoci, temperatura, stabilne napięcie zasilania urządzeń - brak przepięć).

Wymienione powyżej wymagania są realizowane na poziomach odpowiadających konieczności ochrony informacji. Podlegają wciąż analizie oraz dostosowaniu do potrzeb.

Dopiero wówczas można twierdzić, że tak realizowana ochrona fizyczna może być efektywna. Powinna skutecznie zapobiegać niszczeniu elementów polowego

---

[16] tamże

[17] Tymczasowe zasady organizacji, funkcjonowania i bezpieczeństwa łączności utajnionej w SZ PRL, W-wa 1988, sygn. Łączn. 928/88, rozdział IV str.24-29, rozdział IX str. 49-53, załącznik 6 – Dziennik ewidencji naruszeń bezpieczeństwa łączności i kontroli organów, pododdziałów (stacji) łączności utajonej, załącznik 7 – Dziennik ewidencji osób przebywających w stacjach (aparatowniach) łączności utajnionej.

[18] tamże

[19] Może to być osoba zupełnie przypadkowa w okresie pokoju, lecz również może być to osoba lub grupa ludzi celowo starająca się dostać do ochranianego LŚB.

systemu telekomunikacyjnego na WŁ SD (PWŁ) poprzez celowe akty dywersji, sabotażu, a nawet terroryzmu, jak również próbom penetracji przez obce służby specjalne, kradzieżami i włamaniami (wtargnięciem) osób nieuprawnionych.

Realizowanie ochrony fizycznej w rejonach rozwinięcia na stanowiskach dowodzenia nie jest proste, ale zdecydowanie więcej zagrożeń istnieje poza strefami bezpieczeństwa. Systemy telekomunikacyjne starają się sprostać wymaganiom ochrony informacji podczas jej przekazywania między innymi poprzez stosowanie światłowodów, a także takiego budowania i możliwości konfigurowania sieci, aby można było zawsze wykorzystać drogi zapasowe dla przekazania informacji. Stosuje się również programy pozwalające na szybką, zdalną zmianę przyjętej konfiguracji sieci oraz wykrywania wszelkiego rodzaju jej naruszeń, nieprawidłowości w jej pracy oraz zapewniające ochronę w sytuacjach awaryjnych. Natomiast zakres ochrony musi być zgodny z obowiązującymi aktami prawnymi.[20]

Ochrona kryptograficzna:

Kryptograficzne metody ochrony informacji niejawnych w systemach telekomunikacyjnych są kosztownym, ale skutecznym sposobem zapewniającym przekazywanie ich dla wybranego grona osób. Zastosowanie środków o gwarantowanej mocy kryptograficznej wraz z wszystkimi innymi dostępnymi metodami organizacyjno-technicznymi zabezpieczenia danej informacji powinno stanowić skuteczną barierę dla niepowołanych osób i instytucji chcących je zdobyć.
Ochrona kryptograficzna w systemach polowych realizowana jest poprzez:

- generację dokumentów kryptograficznych (kluczy), haseł zabezpieczających i dostępu;
- dystrybucję dokumentów kryptograficznych (kluczy), haseł zabezpieczających i dostępu;
- wprowadzanie dokumentów kryptograficznych (kluczy), haseł zabezpieczających i dostępu;

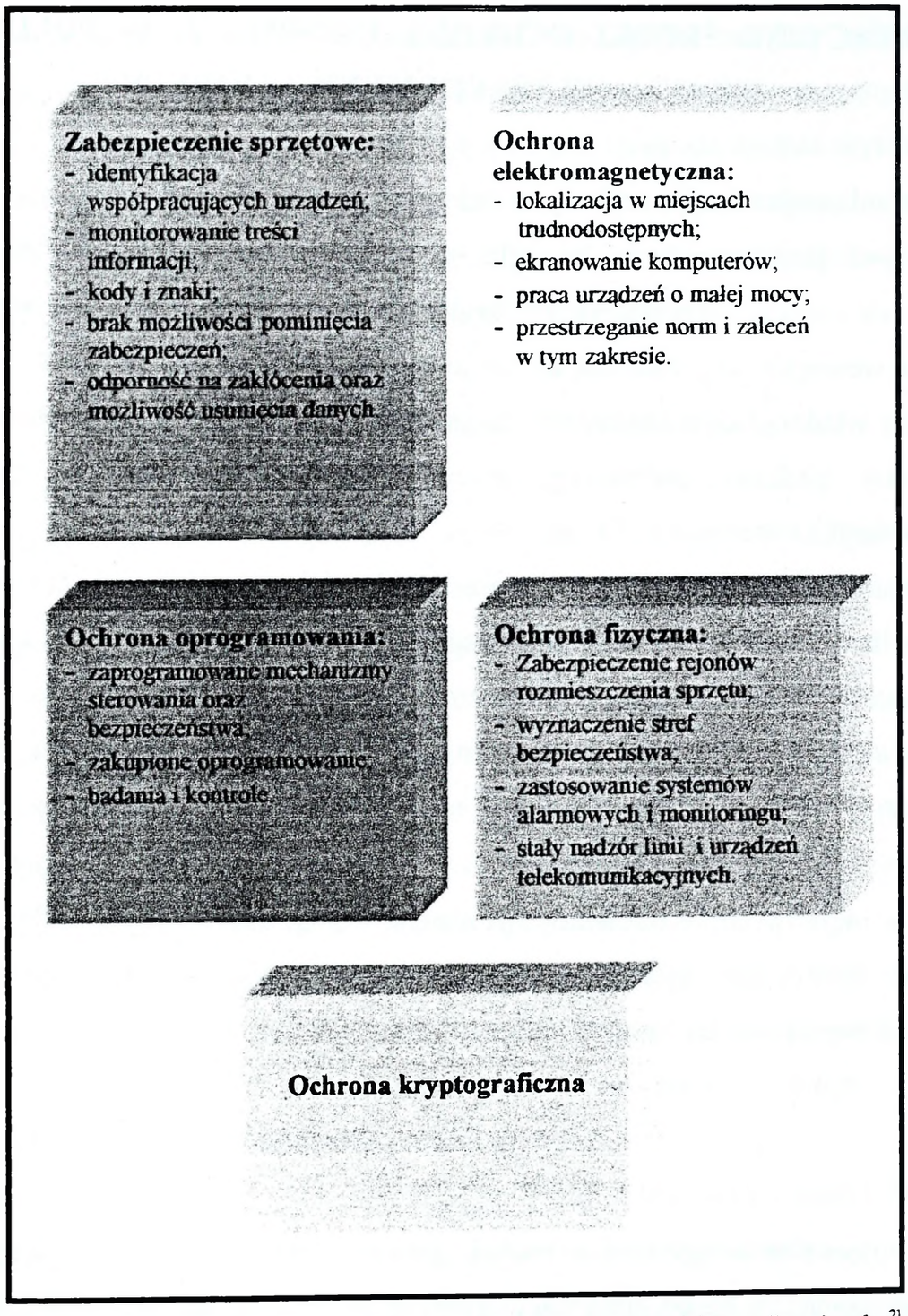
[20] Ustawa „O ochronie informacji niejawnych" z dnia 22.01.1999 roku.(Dz.U. Nr 11, poz.95), Rozdział X, art.56, pkt.2

- przechowywanie dokumentów kryptograficznych (kluczy), haseł zabezpieczających i dostępu;
- niszczenie dokumentów kryptograficznych (kluczy), haseł zabezpieczających i dostępu.

Wszystkie powyższe przedsięwzięcia są realizowane w celu właściwego jej zabezpieczenia i ich suma oraz ścisłe przestrzeganie daje pożądany efekt końcowy.

Aby przekazywane informacje w polowych systemach telekomunikacyjnych były bezpieczne, celowym jest umiejętne połączenie stworzonych barier technicznych w jeden sprawny system, który skutecznie przyczyni się do wzrostu poziomu ochrony informacji. Stosowanie zaprogramowanych mechanizmów sterowania oraz bezpieczeństwa pozwoli na skuteczną ochronę oprogramowania wykorzystywanego przez systemy telekomunikacyjne. Natomiast dbałość o odpowiednie rozmieszczenie i zabezpieczenie poszczególnych aparatowni powinno stanowić właściwą ochronę fizyczną urządzeń.

Wydaje się, że ochrona techniczna (rysunek 2) może stanowić skuteczną zaporę przed utartą lub ujawnieniem informacji niejawnych. Jednak by mogła spełnić pokładane w niej nadzieje należy powiązać jej strukturę i funkcjonowanie z organizacyjnymi środkami ochrony w polowych systemach telekomunikacyjnych.



Rysunek 2 – Składniki ochrony technicznej polowych systemów telekomunikacyjnych. [21]

[21] Źródło: opracowanie własne

ORGANIZACYJNE ŚRODKI OCHRONY INFORMACJI W POLOWYCH SYSTEMACH TELEKOMUNIKACYJNYCH

Organizacyjne środki ochrony w polowych systemach telekomunikacyjnych są czynnościami podejmowanymi w celu zapewnienia bezpieczeństwa informacji, a sposób ich realizacji wynika z obowiązujących aktów normatywno-prawnych oraz przepisów wewnętrznych. Znaczną uwagę poświęca się ludziom spełniającym kryteria dostępu do wiadomości o charakterze niejawnym. Weryfikuje się kandydatów i ich szkoli, aby podczas późniejszej pracy i służby korzystali z informacji klasyfikowanych.

Organizacyjne środki ochrony mają za cel wspomóc ochronę techniczną sieci telekomunikacyjnych oraz istniejący sposób przekazywania informacji niejawnych przez środki łączności oraz powodować wzrost ich bezpieczeństwa.

Za ochronę informacji informacji niejawnych odpowiada dowódca jednostki organizacyjnej, w której następuje jej gromadzenie, wytwarzanie, przetwarzanie i przekazywanie.[22] Powinien on wyznaczyć pełnomocnika dowódcy do spraw ochrony informacji niejawnych. Kierownicy jednostek organizacyjnych (dowódcy) mogą dodatkowo sprecyzować wymagania dotyczące ochrony informacji, a w szczególności ich bezpiecznego przekazywania.

Bezpieczeństwo personalne.

Bezpieczeństwo personalne można nazwać również osobowym. Jego istota sprowadza się do ochrony informacji poprzez odsunięcie od niej osób, które ze względu na swoje poglądy, sympatie, czasem układy towarzyskie czy też kłopoty finansowe i chęć zysku, gotowe będą do ujawnienia danych niejawnych lub sposobów ich przekazywania. Taka sytuacja tyczy się wielu osób, które mogą mieć dostęp do urządzeń przekazujących informacje poprzez ich obsługę lub serwis. Odpowiedni

[22] Ustawa o ochronie informacji niejawnych z dnia 22.01.1999 roku.(Dz.U. Nr 11, poz.95), Rozdział III art.18. To samo zagadnienie poruszono we wcześniejszych dokumentach.

dobór personelu do pracy powinien skutecznie eliminować problemy związane z wydostaniem się informacji niejawnych poza dany system telekomunikacyjny. W tym zakresie podstawowym warunkiem do spełnienia jest odpowiednie przeprowadzenie weryfikacji w stosunku do wszystkich osób mogących mieć styczność z informacjami niejawnymi. Żadna osoba, która nie spełnia wymagań nie powinna uzyskać poświadczenia bezpieczeństwa i być dopuszczona do pracy na stanowisku, gdzie takie dane mogłyby się znajdować. Należy również ograniczyć możliwość pracy z dokumentami innymi niż jest to konieczne.

Bezpieczeństwo źródeł informacji.

Czynnikiem, który może mieć wpływ na bezpieczeństwo przekazywania informacji w polowych systemach telekomunikacyjnych jest bezpieczeństwo źródeł informacji. Pod pojęciem „źródło informacji”[23] należy rozumieć wszelkie wiadomości gromadzone i przetwarzane w urządzeniach technicznych oraz zapisane przy pomocy umownych znaków (np. rysunków, obrazów, dźwięków, liczb lub przedstawione wskazania przyrządów pomiarowych) oraz wydrukowane dokumenty. Nie muszą być one przekazywane w postaci sygnałów w systemach telekomunikacyjnych, ale ich treść może zawierać wiadomości, jakich ujawnienie może spowodować wzrost zagrożeń dla bezpieczeństwa przekazywania informacji (np. opis sposobów kodowania informacji, dane dotyczące parametrów technicznych użytkowanego sprzętu, informacje o rozmieszczeniu i sposobach ochrony urządzeń telekomunikacyjnych).

Szczególnego zatem znaczenia nabiera ochrona wszystkich źródeł informacji o charakterze niejawnym, która wymusza konieczność zorganizowania systemu ich rejestrowania, ewidencji dostępu osób uprawnionych i kontroli zapobiegających ich przechwyceniu przez osoby nieuprawnione oraz próbom modyfikowania ich treści. Wiadomości zawarte w źródłach informacji (dokumentach niejawnych) należy zabezpieczyć od chwili ich powstania, aż do zmiany klauzuli źródła informacji na „JAWNE”, bądź jego zniszczenia zgodnie z obowiązującymi przepisami. Jednostki

organizacyjne wprowadzają powyższe wymagania, a twórca źródła informacji nadaje (kwalifikuje) go do odpowiedniej klauzuli niejawności. [23]

Nasuwa się zatem pytanie, jak należałoby właściwie zabezpieczyć źródła informacji (wytworzone dokumenty o charakterze niejawnym)?

W rejonach rozmieszenia SD powinny być zorganizowane specjalne pomieszczenia do ich przechowywania, ochraniane przez osoby do tego wyznaczone oraz środki techniczne. Są to kancelarie niejawne (zazwyczaj na pojazdach) gdzie można gromadzić źródła informacji (dokumenty) zawierające ważne wiadomości w różnej formie (notatki, rysunki, grafika, nośniki elektromagnetyczne, fotografie, taśmy video i magnetofonowe, filmy, obrazy itd.). W polowych systemach telekomunikacyjnych szczególnego znaczenia nabiera forma elektroniczna oraz dokumenty wydrukowane. Stwarza to potrzebę stosowania barier utrudniających uzyskanie informacji z urządzeń je przekazujących, gromadzących i przetwarzających, a ewidencja dokumentów powinna umożliwiać uzyskanie danych o stanie ilościowym dokumentu, kto był i jest aktualnie jego użytkownikiem.

W systemach telekomunikacyjnych funkcjonują i są zorganizowane komórki podlegające pełnomocnikowi ds. ochrony odpowiedzialne za rejestrowanie, przechowywanie, obieg i przekazywanie źródeł informacji zawierających treści niejawne. Te dane same już stanowią tajemnicę, która nie powinna być ujawniona. Ich praca realizowana jest na podobnych zasadach i odnosi się do następujących wspólnych elementów:

1. stworzenie pomieszczeń (kancelarii), w których gromadzi się, przechowuje, ewidencjonuje oraz z nich się przekazuje ważne źródła informacji (dokumenty) o różnym charakterze;
2. kancelarie są obsługiwane przez osoby o najwyższych stopniach poświadczeń bezpieczeństwa, sprawdzonych i weryfikowanych zgodnie z wymaganiami;[24]
3. kancelarie prowadzą rejestry ewidencji źródeł informacji (dokumentów);[25]
4. zabezpieczenie pomieszczeń kancelarii poprzez systemy alarmowe;

---

[23] J.Plewa, Techniczne i organizacyjne środki ochrony systemów łączności, AON Warszawa 2001. s.27.
[24] Ustawa o ochronie informacji niejawnych z dnia 22.01.1999 roku.(Dz.U. Nr 11, poz.95), rozdział VII, art.50
[25] Rozporządzenie Rady Ministrów z dnia 9 lutego 1999 roku w sprawie organizacji kancelarii tajnych. (Dz.U. Nr 18, poz.156)

5. organizowanie w danej jednostce organizacyjnej osobnych kancelarii dotyczących źródeł informacji (dokumentów) niejawnych narodowych oraz zagranicznych.[26]
6. źródła informacji (dokumenty) oznaczone klauzulami: „ściśle tajne" i „tajne" mogą być wydawane poza wyznaczone pomieszczenie (kancelarię tajną) jedynie w przypadku, gdy ich odbiorca zapewnia warunki ochrony takich źródeł informacji przed nieuprawnionym ujawnieniem. W razie wątpliwości co do zapewnienia warunków ochrony, źródło informacji (dokument) może być udostępniony wyłącznie w wyznaczonym i nadzorowanym pomieszczeniu (kancelarii tajnej).[27]

Rozpatrując bezpieczeństwo źródeł informacji dla potrzeb systemów telekomunikacyjnych należy zwrócić uwagę, że można je zapewnić poprzez realizację następujących czynności:

a) nadanie klauzuli tajności i odpowiedniego priorytetu ochrony źródła informacji (dokumentu);
b) zabezpieczenie przed utratą lub ujawnieniem treści źródła informacji;
c) dokładnego podania weryfikacji osób, które mogą korzystać z źródła informacji;
d) każdorazowe potwierdzenie otrzymania źródła informacji przez osobę użytkującą oraz zwrotu do wyznaczonej kancelarii niejawnej.

Niszczenie źródeł informacji (dokumentów) powinno się odbywać w sposób uniemożliwiający ich jakiekolwiek odtworzenie, komisyjnie, po sprawdzeniu ich zgodności z wykazem protokołów zniszczenia, a bezpośrednio po tych czynnościach źródło informacji (dany dokument) należy zdjąć z ewidencji.

Kontrola dostępu

Kontrola dostępu do informacji w polowych systemach telekomunikacyjnych powinna skupiać się na przyznawaniu uprawnień użytkownikom systemu oraz

[26] Rozporządzenie MSWiA oraz Obrony Narodowej z dnia 26 lutego 1999 roku „W sprawie trybu i sposobu przyjmowania, przewożenia, wydawania i ochrony materiałów" (Dz.U. z 1999 roku, nr 18, poz. 168).
[27] Ustawa o ochronie informacji niejawnych z dnia 22.01.1999 roku (Dz.U. Nr 11, poz.95), Rozdział VII art.52, pkt 2)

opracowywaniu metod do sprawdzania kto, kiedy i z jakich zasobów korzystał.[28] W tym celu wyznacza się strefy bezpieczeństwa i nadaje klauzule tajności wiadomości, a także sposobu ochrony przed niewłaściwym działaniem personelu i użytkowników. Organizacyjnie połączona jest z identyfikacją, wiarygodnością oraz upoważnieniami dostępu do informacji.

Kontrolę dostępu powinien zorganizować kierownik danej jednostki organizacyjnej za pośrednictwem pełnomocnika ds. ochrony informacji niejawnej.[29] Będzie ona spełniała swoją rolę po ujęciu przedsięwzięć mogących mieć wpływ na przekazywanie informacji w systemach telekomunikacyjnych. Do najważniejszych mogę zaliczyć:

1. określenie sposobu dopuszczenia do informacji niejawnych;
2. postępowania sprawdzające kandydatów do pracy z dostępem do wiadomości niejawnych oraz ich szkolenia z zakresu ochrony i bezpieczeństwa informacji;
3. zaopatrzenia osoby przeszkolonej (z poświadczeniem bezpieczeństwa) w identyfikatory uprawniające do wejścia-wyjścia z stref bezpieczeństwa;
4. przydzielenie indywidualnych kodów dostępu i haseł;
5. udzielania informacji niejawnych tylko w stopniu wymaganym na danym stanowisku pracy („Zasada wiedzy koniecznej");
6. ścisłą ewidencję wejść i wyjść z danej strefy bezpieczeństwa, jak również korzystanie z określonych zasobów danych;
7. wprowadzenie kontroli elektronicznej poprzez założenie systemów alarmowych oraz kamer;
8. szczegółową kontrolę osób mogących wnieść sprzęt do kopiowania oraz przekazywania informacji (poprzez wartowników, patrole, system identyfikatorów);
9. kontrolę wszystkich osób mogących stanowić zagrożenie dla bezpieczeństwa wiadomości niejawnych (zgodnie z rozdziałem I niniejszej pracy);

---

[28] M. Szaliłow. Organizacyjno-prawne aspekty ochrony systemów łączności i informacji w nich przesyłanej, AON Warszawa 2001,s.35.

[29] Ustawa o ochronie informacji niejawnych z dnia 22.01.1999 roku (Dz.U. Nr 11, poz.95) Rozdział III art.18, Rozdział IX art. 57, Rozdział X art. 64

10. możliwość wprowadzenia własnych zmian skutecznie zwiększających ochronę ważnych treści z posiadanych zasobów w przypadku, gdy zostaną zauważone błędy w funkcjonowaniu kontroli dostępu;
11. przechowywanie informacji zgodnie z przyjętymi wymaganiami (chronione źródła informacji np. dyski twarde komputerów, sejfy dla dokumentów, itp.);
12. przekazywanie informacji tylko zgodnie z wcześniej ustalonymi oraz sprawdzonymi sposobami, które mogą je uchronić przed osobami nieuprawnionymi.[30]

Należy podkreślić, że zakres działań organizacyjnych środków ochrony nie jest wyczerpany. W zależności od poziomu bezpieczeństwa może obejmować w mniejszym lub większym stopniu wszystkie powyższe przedsięwzięcia. Jeżeli kontrola dostępu funkcjonuje w sposób prawidłowy, to następuje wyeliminowanie przypadkowej lub celowej utraty informacji. Dokładne zbadanie w jaki sposób wiadomość o charakterze niejawnym mogłaby być utracona, może doprowadzić do zatrzymania osoby, która naruszyła obowiązujące przepisy ochrony.

Zarządzanie bezpieczeństwem w polowych systemach telekomunikacyjnych

Zarządzanie bezpieczeństwem jest połączeniem elementów organizacji i zarządzania, informatyki oraz różnorodnych zabezpieczeń technicznych i organizacyjnych. Jest to złożony i ciągły proces zachodzący w zmieniających się warunkach otoczenia i funkcjonowania informacji oraz rozwijających się nowych zagrożeń i w warunkach postępu technicznego. W zarządzaniu bezpieczeństwem dąży się do identyfikacji zagrożeń i eliminowania ich poprzez utrzymanie ustalonego poziomu ochrony, a zależy od personelu chroniącego informacje oraz kierownika jednostki organizacyjnej. Im wyższy stopień poufności wiadomości, tym większa ilość osób powinna pełnić zadania związane z jej bezpieczeństwem.

[30] Rozporządzenie Rady Ministrów Spraw Wewnętrznych i Administracji oraz Obrony Narodowej z dnia 26 lutego 1999 roku „W sprawie trybu i sposobu przyjmowania, przewożenia, wydawania i ochrony materiałów" (Dz.U. z 1999 roku, nr 18, poz. 168).

Zgodnie z obowiązującym prawem telekomunikacyjnym[31] tajemnica komunikowania się (zwana „tajemnicą telekomunikacyjną") obejmuje informacje przekazywane w systemach telekomunikacyjnych, dane dotyczące użytkowników, a także dane dotyczące faktu, okoliczności i rodzaju połączenia, prób uzyskania połączenia między określonymi zakończeniami sieci, jak również identyfikacji lub lokalizacji zakończenia sieci pomiędzy którymi wykonano połączenie.

Aby można było zachować wiarygodność należy ochronić wszystkie powyższe informacje. W odniesieniu do tego problemu szczególnego znaczenia nabiera zarządzanie bezpieczeństwem w systemach telekomunikacyjnych. W mojej ocenie powinno posiadać następujące właściwości:

1. dopuszczenie do pracy przy zarządzaniu tylko sprawdzonych, zaufanych osób;
2. być realizowane przez wykwalifikowaną obsługę i administratora;[32]
3. personel powinien znać strukturę eksploatowanej sieci telekomunikacyjnej oraz sieci współpracujących;
4. stała kontrola pomieszczeń podlegających ochronie;
5. przestrzeganie zasad obiegu informacji, ich wytwarzania, przechowywania i niszczenia;
6. zabezpieczenie techniczne, personalne i źródeł informacji (dokumentów);
7. alarmowanie o wszelkich naruszeniach bezpieczeństwa personelu ochrony oraz kierownika jednostki organizacyjnej;
8. pełnomocnik ds. ochrony informacji niejawnych (szef ochrony) powinien posiadać dostęp do wszystkich informacji mających wpływ na bezpieczeństwo systemu telekomunikacyjnego.

Zarządzanie bezpieczeństwem powinno być ściśle związane z profesjonalnie przygotowanym i wyszkolonym personelem, działającymi systemami alarmowymi, wszystkimi zabezpieczeniami technicznymi i organizacyjnymi. Jednak nawet wówczas należy mieć świadomość, że to do końca nie gwarantuje bezpieczeństwa chronionym informacjom i należy jeszcze posiadać plany działania w sytuacjach awaryjnych, które należy przewidzieć. Zaliczyć do nich należy:

---

[31] Prawo telekomunikacyjne, Ustawa z 21 lipca 2000 roku (Dz.U. z 6 września 2000 roku) Rozdział 5, dział 5, art. od 67 do 71;

[32] J.Plewa, Techniczne i organizacyjne środki ochrony systemów łączności, AON Warszawa 2001, s.28.

1. działanie na wypadek prób włamania się do zasobów systemu telekomunikacyjnego;
2. awarie systemu (zasilanie lub brak możliwości zarządzania);
3. procedury awaryjne na wypadek różnych zdarzeń (np. braku dostępu do kluczowych pomieszczeń);
4. możliwość zapisu informacji niejawnych w urządzeniach trudnych do penetracji przez osoby nieuprawnione, a wypadku zniszczenia sprzętu - odtworzenia informacji.

Kontrole bezpieczeństwa przekazywania i obiegu informacji w polowych systemach telekomunikacyjnych

Problemu kontroli bezpieczeństwa przekazywania informacji nie można traktować marginalnie. Wszystkie ujęte w poprzednio formy i sposoby jej ochrony są ważne, ale wszystkie one muszą podlegać kontroli. Tak rozumiane zapewnienie wymaganego poziomu bezpieczeństwa może stanowić o rzetelnej ochronie wszelkich treści o charakterze niejawnym.

W tym celu ważnym jest aby dowódca na SD, oprócz ochrony technicznej, bezpieczeństwa personalnego, źródeł informacji (dokumentów), kontroli dostępu i właściwego zarządzania systemem telekomunikacyjnym, nakazywał przeprowadzanie kontroli i porównywania stanu pożądanego z faktyczną realizacją zleconych środków ochrony. W ten sposób otrzymamy kolejny mechanizm organizacyjny, który pozwoli za zapewnienie przyjętego stanu bezpieczeństwa w systemie telekomunikacyjnym - kontrolę. Kontrola musi umożliwiać ocenę wysiłków podejmowanych działań zmierzających do utrudnienia i stworzenia barier przed jakąkolwiek utratą informacji o szczególnym znaczeniu.

W każdym systemie telekomunikacyjnym administrator sieci wraz z pełnomocnikiem ds. ochrony (szefem ochrony) powinien wdrożyć do realizacji stały i zaplanowany proces kontroli związany z utrzymaniem wysokiego poziomu bezpieczeństwa.[33] Jednakże przeprowadzane kontrole nie mogą stresować osób pracujących przy przekazywaniu informacji, lecz uświadomić im dodatkową formę

[33] J.Plewa, Techniczne i organizacyjne środki ochrony systemów łączności, AON Warszawa 2001,s.31.

nadzoru mającą wpływ na ochronę wiadomości. Podstawowe cele kontroli bezpieczeństwa i obiegu informacji w polowych systemach telekomunikacyjnych można by ująć w następujących punktach:

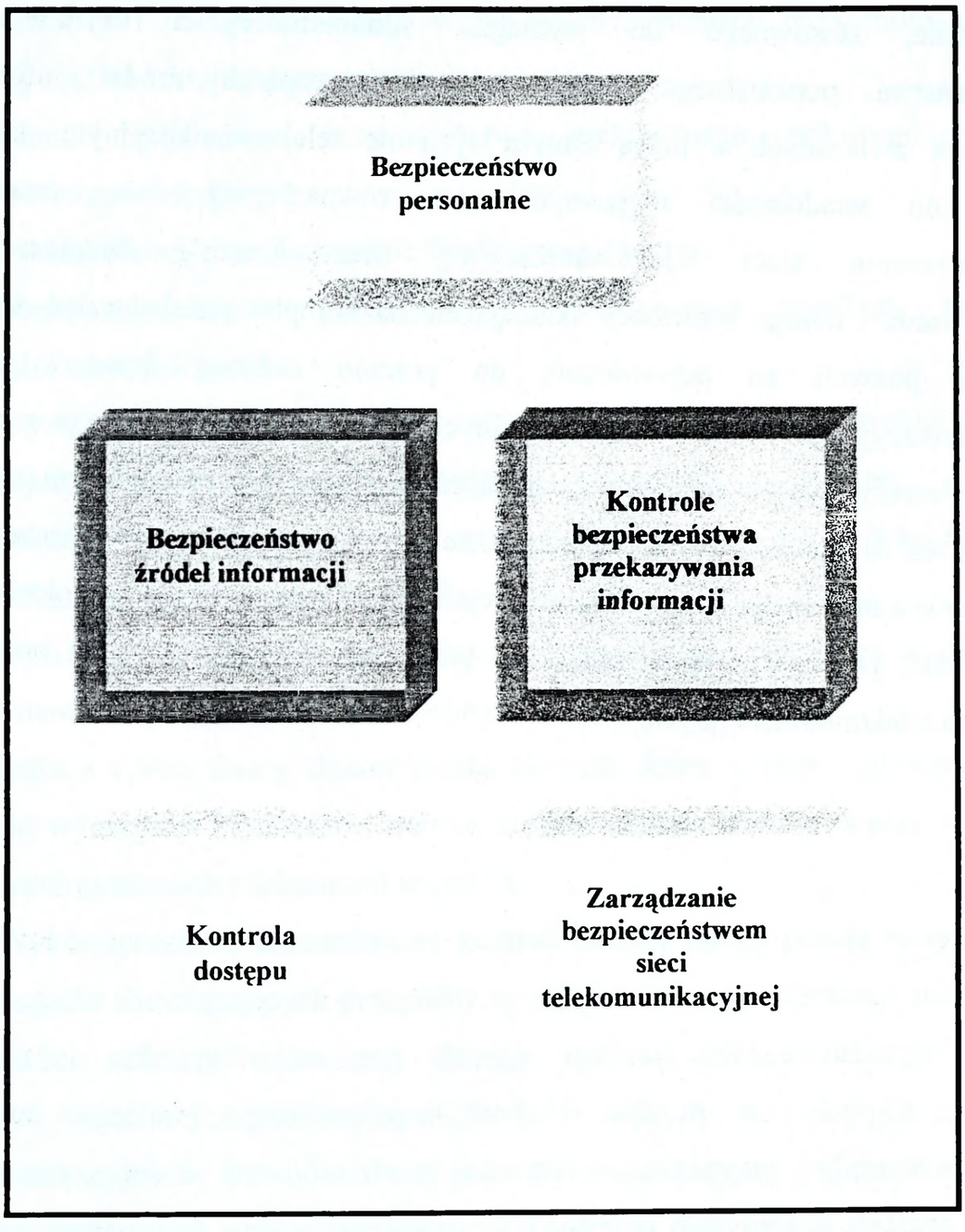
1. ocena faktycznego bezpieczeństwa technicznego polowego systemu telekomunikacyjnego;
2. ocena ochrony przez wszystkie środki organizacyjne;
3. porównanie stanu ewidencyjnego z faktycznym urządzeń, nośników i dokumentów;
4. czy sposób destrukcji nośników informacji, urządzeń i dokumentów oraz ich wyznaczenie do zniszczenia jest zgodne z przyjętymi procedurami;
5. zebranie wniosków mogących służyć do polepszenia stanu bezpieczeństwa informacji systemu telekomunikacyjnego;
6. wyciągnięcie wniosków dyscyplinarnych w stosunku do winnych zaniedbań i naruszeń przyjętego systemu ochrony.

Istnieją różne formy dokonywania kontroli, które można wykorzystać aby zapewnić wymagany i pożądany stopień bezpieczeństwa przekazywania informacji w polowych systemach telekomunikacyjnych.

Wybór sposobu i częstotliwości kontroli zależał będzie przede wszystkim od przestrzegania obowiązujących przepisów w zakresie ochrony informacji niejawnych, skuteczności ochrony technicznej danego systemu telekomunikacyjnego oraz opisanych wcześniej organizacyjnych środków ochrony w polowych systemach telekomunikacyjnych. Dowódca danej jednostki organizacyjnej (administrator sieci) powinien zaplanować stałe przedsięwzięcia kontrolne realizowane podczas bieżącej pracy systemu telekomunikacyjnego, które mogą wpłynąć na poprawę bezpieczeństwa przekazywanych informacji oraz zorganizować i przeprowadzić poprzez zaufaną grupę ludzi kontrole o charakterze doraźnym, okresowym lub kompleksowym.

Organizacyjne środki ochrony polowego systemu telekomunikacyjnego (rysunek 3), pomimo zapewnienia bezpieczeństwa przekazywania informacji poprzez zastosowanie środków technicznych, odgrywają nadal znaczną rolę. Ich właściwe i przemyślane zaplanowanie oraz wdrożenie do realizacji powinno gwarantować wymagany poziom ochrony nie tylko informacji niejawnych, ale wszystkich

wiadomości, które zamierzamy przekazać w danym systemie telekomunikacyjnym. Zapewnienie, stosownego do wymagań administratora i użytkowników, bezpieczeństwa personalnego, bezpieczeństwa wszystkich źródeł informacji niejawnych związanych z pracą danym systemie telekomunikacyjnym, kontroli dostępu do wiadomości niejawnych, jak również właściwe zarządzanie bezpieczeństwem sieci telekomunikacyjnej oraz kontrole bezpieczeństwa przekazywania i obiegu informacji składają się na komplet przedsięwzięć, których realizacja pozwoli na odpowiednią do potrzeb ochronę danego systemu telekomunikacyjnego. Środków organizacyjnych ochrony, których realizacja mogłaby w zdecydowany sposób poprawić bezpieczeństwo przekazywania informacji, jest wiele. Są one równie kosztowne jak techniczne sposoby zapewnienia bezpieczeństwa, ale wspólnie z nimi mogą eliminować potencjalne źródła zagrożeń dla funkcjonowania gromadzenia, przetwarzania, a zwłaszcza przekazywania informacji w polowych systemach telekomunikacyjnych.



Rysunek 3. Czynniki warunkujące organizacyjne środki ochrony polowego systemu telekomunikacyjnego[34]

ZAKOŃCZENIE

Wzrost zagrożeń wobec informacji wymusza ciągłe poszukiwanie i stosowanie nowych, trudniejszych do pominięcia lub przełamania sposobów ochrony wiadomości. W zależności od kategorii ważności informacji podejmowane są stosowne działania jej ochrony organizacyjno-technicznej poparte obowiązującym

[34] Źródło: opracowanie własne

prawem. Zaprojektowany i wprowadzony system bezpieczeństwa powinien chronić przed wszystkimi potencjalnymi zagrożeniami. Pominięcie lub zbyt duża ilość zabezpieczeń może mieć negatywny wpływ na ochronę przekazywanych informacji z powodu ich słabej ochrony lub trudnej do uniknięcia niewłaściwej realizacji i upraszczania wypracowanych procedur.

Zagrożenia dla bezpieczeństwa przekazywania informacji oraz potrzeba zapewnienia im odpowiedniej ochrony wskazuje, że najlepsze rezultaty uzyskać można poprzez:

1. powołanie i przeszkolenie ludzi, którzy będą dbali o bezpieczeństwo przekazywania informacji (a także jej gromadzenia i przetwarzania) tworząc personel bezpieczeństwa;
2. zastosowanie:

a. obowiązującego prawa do skutecznej ochrony informacji;
b. możliwych do użycia środków ochrony technicznej w polowych systemach telekomunikacyjnych;
c. wypracowanych organizacyjnych środków ochrony.

Personel bezpieczeństwa oraz kompleksowa ochrona organizacyjno-techniczna powinny skutecznie zapewniać bezpieczeństwo przekazywania informacji. Przy czym należy zwrócić uwagę, że im głębsza jest świadomość konieczności zapewnienia ochrony informacji (także gromadzonych i przetwarzanych) przez ludzi mających do niej dostęp, a także wzajemna dobra współpraca wszystkich jej użytkowników, tym zapewnienie bezpieczeństwa przekazywania informacji może być dużo lepsze. Przestrzeganie przyjętych zasad, procedur i tym samym ustalonego poziomu zapewniającego ochronę, nie może być traktowane jako zło konieczne, ale wynikać z przyjętej przez wszystkich konieczności takiego postępowania.[35] Należy ograniczać możliwości utraty, przechwycenia, podmiany lub modyfikacji przekazywanych wiadomości, jak również by przyjęte zasady jej ochrony nie zostały ujawnione.

Zapewnienie bezpieczeństwa przekazywania informacji w systemach telekomunikacyjnych realizuje się przy uwzględnieniu stworzenia warunków, w których jest ona chroniona poprzez:

a. użycie sprawdzonego sprzętu i oprogramowania;

[35] J.Plewa, Techniczne i organizacyjne środki ochrony systemów łączności, AON Warszawa 2001, s. 34.

b. właściwie przeszkolony personel;
c. zapewnienie ochrony źródeł informacji;
d. właściwe zarządzanie bezpieczeństwem;
e. ograniczenie dostępu osób nieuprawnionych lub osób, którym dana wiadomość nie jest potrzebna do wykonywania obowiązków służbowych;
f. system kontroli przekazywania i obiegu informacji.

Tylko sprawne połączenie powyższych komponentów może pozwolić na uzyskanie oczekiwanych rezultatów, natomiast powierzchowne potraktowanie jednej z metod lub zastosowanych środków prowadzi do niskiego poziomu ochrony informacji. Jednocześnie należy mieć na uwadze, że bardzo trudno jest zapewnić 100% bezpieczeństwa przekazywania informacji. W tym przypadku wskazane jest minimalizowanie prawdopodobieństwa przechwycenia (utraty) informacji oraz uczynić je nieopłacalnym z punktu widzenia czasu lub ekonomii[36] mając przekonanie, iż może znaleźć się ktoś, kogo będą interesowały przekazywane (gromadzone, przetwarzane) wiadomości.

Po dogłębnej analizie istniejących możliwości zapewnienia bezpieczeństwa przekazywania informacji nasuwają się następujące wnioski końcowe:

1. Najsłabszym elementem systemu bezpieczeństwa przekazywania informacji jest człowiek, ponieważ najwięcej zależy od niego (użytkowanie informacji, chęć zysku, dążenie do władzy, projektowanie systemu czy też popełnianie przestępstw związanych z włamaniem do zasobów informacji).
2. Postęp techniczny powoduje rozwój sposobów zabezpieczeń systemów telekomunikacyjnych, jak również doskonalenie środków umożliwiających zdobycie informacji.
3. Zawsze należy dążyć do stworzenia jak najbardziej optymalnego systemu zapewniającego bezpieczeństwo poprzez umiejętne połączenie prawa oraz zastosowanych środków organizacyjno-technicznych (należy stosować tylko sprawdzone i posiadające certyfikat urządzenia, oprogramowanie do sprzętu komputerowego) .
4. Poniesione koszty na bezpieczeństwo przekazywania informacji powinny dawać efekt w postaci ochrony wiadomości zgodnie z hierarchią ich ważności.

[36] Tamże, s. 35

5. Stosowanie systemu monitoringu powinno zapewniać sprawne wykrywanie zagrożeń oraz słabych punktów stosowanego systemu bezpieczeństwa, a projektowanie, organizacja i wprowadzenie do użycia środków bezpieczeństwa powinno zmierzać w kierunku stworzenia bezpiecznego środowiska pracy.

LITERATURA:

Literaturę przedmiotu pogrupowano w cztery główne grupy:

1. BIBLIOGRAFIA:

1. A. Dańczak, Bezpieczeństwo informacji w SZ. Aspekty strategiczne, Warszawa AON 2002,
2. Balcerowicz Bolesław, Słownik terminów z zakresu bezpieczeństwa narodowego, AON Warszawa 2002.
3. Mazurkiewicz Jerzy, Leksykon łączności wojskowej, AON Warszawa 1996.
4. Michniak Józef, Fiołna Zbigniew, Sieć łączności państwa, AON Warszawa 2000.
5. Plewa Jerzy, Techniczne i organizacyjne środki ochrony systemów łączności, AON Warszawa 2001;
6. Stypik L., Co nieco na temat systemów dowodzenia, PWL nr 2 (536) luty 2004
7. Szaliłow Marcin, Organizacyjno-prawne aspekty ochrony systemów łączności i informacji w nich przesyłanej, AON Warszawa 2001.
8. Szczególne Wymagania Bezpieczeństwa dla MPCŁU z wykorzystaniem aparatowni łączności typu RWŁC.
9. Szczególne Wymagania Bezpieczeństwa - Procedury Bezpieczeństwa dla MPCŁU z wykorzystaniem aparatowni łączności typu RWŁC.
10. Tymczasowe zasady organizacji, funkcjonowania i bezpieczeństwa łączności utajnionej w SZ PRL, W-wa 1988, sygn. Łączn. 928/88.

2. USTAWY

1. USTAWA z dnia 22 stycznia 1999 roku o ochronie informacji niejawnych. Dz. U. Nr 11, poz. 95) wraz z późniejszymi zmianami (2001 - Dz. U. Nr 22, poz. 247).
2. USTAWA z dnia 3 lutego 2001 roku o zmianie ustawy o ochronie informacji niejawnych (Dz. U. Nr 22, poz. 247).
3. USTAWA z dnia 21 lipca 2000 r. Prawo telekomunikacyjne. (Dz. U.00.73. 852 z dnia 6 września 2000 r.) – tekst ujednolicony po zmianie 30 sierpnia 2002 roku. Stan prawny na 1 stycznia 2003 roku.

3. ROZPORZĄDZENIA

1.ROZPORZĄDZENIE RADY MINISTRÓW z dnia 9 lutego 1999 roku w sprawie organizacji kancelarii tajnych. (Dz. U. Nr 18, poz. 156).

2.ROZPORZĄDZENIE MINISTRÓW SPRAW WEWNĘTRZNYCH I ADMINISTRACJI ORAZ OBRONY NARODOWEJ z dnia 26 lutego 1999 roku w sprawie trybu i sposobu przyjmowania, przewożenia, wydawania i ochrony materiałów. (Dz. U. Nr 18, poz. 168).

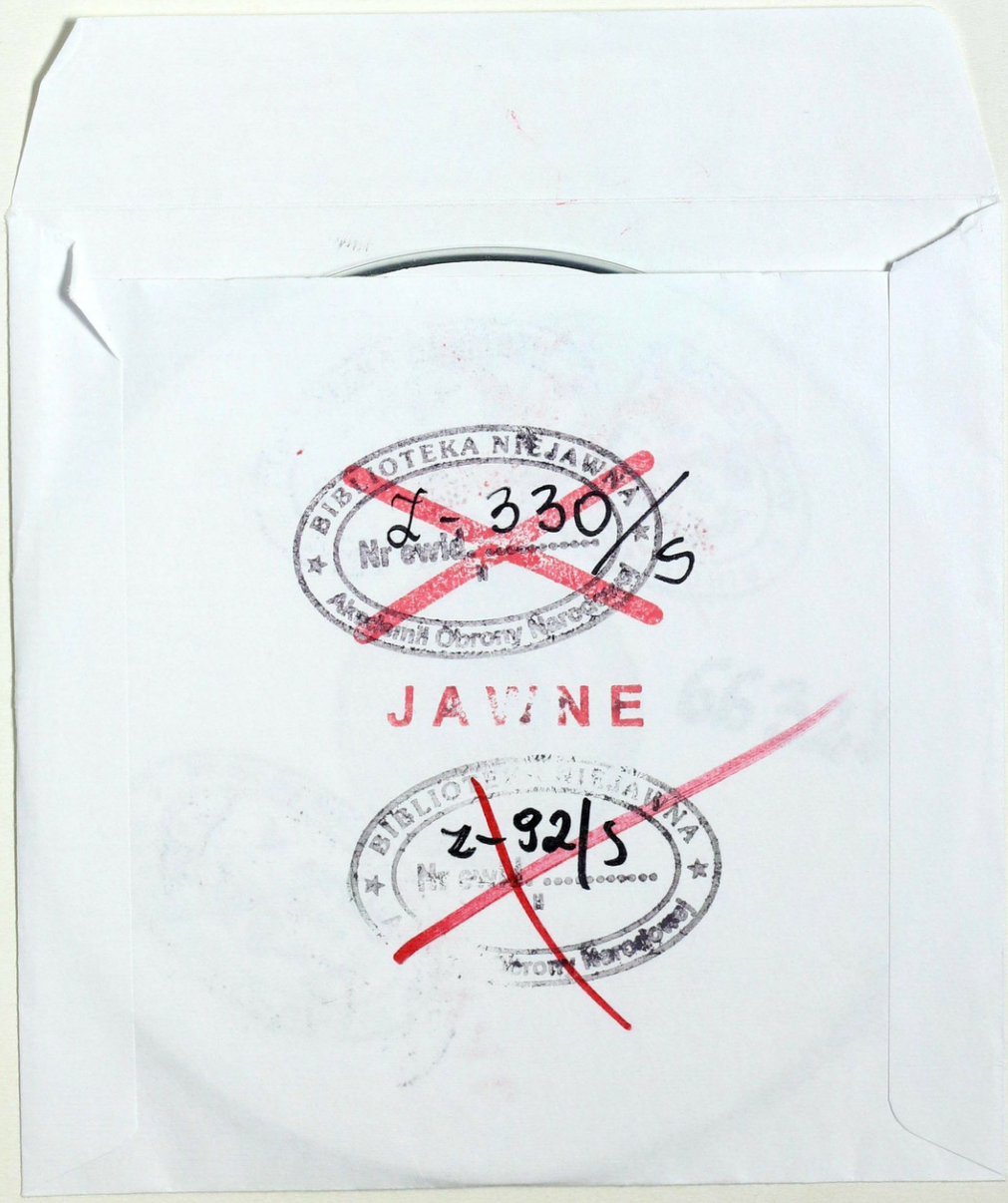
4. ROZKAZY, ZARZĄDZENIA

1. Instrukcje obowiązujące w SZ RP na podstawie Rozkazu Szefa Wojskowych Służb Informacyjnych z dnia 26 czerwca 2000 roku:

- „Wytyczne w sprawie instalacji urządzeń przeznaczonych do przetwarzania informacji niejawnych. BTPO-701A";

Wykonano w 2 egz.
Egz. nr 1 – OBSŁiI ZDiŁ G-6 DWLąd
Egz. nr 2 – Akademia Obrony Narodowej
Sporządził: kpt. Frączek
Wykonał: kpt. Frączek /878-202/

dodatkowo powielono w 5 egz. w Wydziale Wydawniczym AON dnia 6.12.04 r.
Nr RWD 191/Z-1/Z-189/WW/04
Chmielewska
Egz. nr 1-5 bibl. niejawna


BIBLIOTEKA NIEJAWNA
Nr ewid. 2-330/S
JAWNE
BIBLIOTEKA NIEJAWNA
Nr ewid. 2-92/S