BEZPIECZEŃSTWO INFORMACJI W WOJSKOWYCH SIECIACH TELEINFORMATYCZNYCH

Andrzej Wisz

ANALIZA ZAGROŻEŃ
Obszar sił zbrojnych

WYMAGANIA FIZYCZNE I ŚRODOWISKOWE
Obszar sił zbrojnych

WYMAGANIA PROCEDURALNE
Obszar sił zbrojnych

W dobie coraz gwałtowniejszego postępu technologicznego, zwłaszcza w dziedzinach teleinformatycznych, zabezpieczenie informacji oraz jej ochrona stają się aktualne i bardzo ważne. Informacja, która jest czynnikiem „przetwórczym" we współczesnym świecie jest zbyt cenna, aby można było sobie pozwolić na jej niekontrolowane ujawnianie.

Celem artykułu jest przedstawienie zarówno zagrożeń dla bezpieczeństwa informacji w wojskowych sieciach teleinformatycznych, jak i wymagań stawianych bezpieczeństwu informacji.

We współczesnym świecie informacja jest zasobem strategicznym, i to tylko ta, która niesie istotne treści, jest dostarczana terminowo, do właściwego adresata, w formie nienaruszonej (niemodyfikowana) i niezawodnie – po prostu bezpiecznie. Z tym strategicznym charakterem informacji zaczynają się oswajać państwa i różne narodowe oraz ekonomiczne instytucje. Można przy tym zauważyć, że obecnie ciężar gatunkowy ochrony i bezpieczeństwa informacji przesuwa się z sektora polityczno-militarnego do sektora gospodarczego.

Ze względu na rosnące zapotrzebowanie na informację stosuje się coraz nowsze i efektywniejsze metody oraz środki, które przyjmują formę całych systemów, wykorzystujących do pozyskania informacji najnowsze zdobycze elektroniki. Jednak bardzo zaawansowany proces automatyza-

cji środków rozpoznania nie wyeliminował i prawdopodobnie nie wyeliminuje tradycyjnego agenturalnego sposobu zdobywania informacji.

Biorąc pod uwagę znaczenie bezpieczeństwa informacji, można sformułować następującą tezę. W procesie planowania oraz budowania wojskowych sieci teleinformatycznych obligatoryjnie powinno się uwzględniać wszelkie możliwe scenariusze i warunki, w jakich sieć może być wykorzystywana, zarówno pod kątem realizowanych zadań, jak i wymagań bezpieczeństwa (jeżeli takowe są stawiane) informacji w niej przesyłanej.

Proces organizacji ochrony sieci teleinformatycznych i zapewnienie bezpieczeństwa przesyłanej informacji zgodnie z przyjętą polityką bezpieczeństwa resortu obrony narodowej muszą być realizowane równolegle na wszystkich etapach planowania, a następnie wdrażania systemu, nie wyłączając z tego procesu eksploatacji.

Jeśli zatem planowana wojskowa sieć telekomunikacyjna w swoim zamyśle ma zapewnić przesyłanie informacji klasyfikowanych (niejawnych), organizator sieci powinien przeprowadzić analizę ryzyka w odniesieniu do infrastruktury sieci oraz wszystkich elementów i urządzeń, w których może zaistnieć prawdopodobieństwo niekontrolowanego lub nieautoryzowanego „ulotu" informacji podlegającej ochronie. Jest to nic innego jak analiza zagrożeń dla bezpieczeństwa informacji wytwarzanych, przetwarzanych, przesyłanych i przechowywanych w wojskowych sieciach teleinformatycznych, która powinna uwzględniać wszelkie możliwe warunki eksploatacji sieci, począwszy od okresu pokoju, aż do warunków ekstremalnych – wojny i prowadzenia działań bojowych.

ZAGROŻENIA BEZPIECZEŃSTWA INFORMACJI W WOJSKOWYCH SIECIACH TELEINFORMATYCZNYCH

W literaturze przedmiotu możemy spotkać się z różną klasyfikacją zagrożeń, począwszy od najbardziej ogólnej, podziału na wewnętrzne i zewnętrzne zagrożenia, aż po bardzo szczegółową, odnoszącą się do konkretnej sieci, uwzględniając jej organizację, możliwości konfiguracji, wykorzystywanie środków telekomunikacyjnych (transmisyjnych, ko-

mutacyjnych, informatycznych) czy samych urządzeń końcowych. Przy opracowywaniu bardzo szczegółowej klasyfikacji zagrożeń, choć trudno takową spotkać, gdyż informacje o tym, jakie czynniki i jakie zagrożenia zostały uwzględnione w procesie organizacji systemu ochrony, są zazwyczaj niejawne, nie ma i raczej nie może być jednomyślności. Zależy to bowiem od przyjętych przez organizatora danego systemu lub sieci warunków brzegowych oraz przyjętego kryterium oceny możliwości wystąpienia zagrożenia lub grupy zagrożeń.

Warto zastanowić się, jakie elementy współczesnych wojskowych sieci teleinformatycznych mogą stanowić potencjalne źródło ujawnienia informacji. Z analizy literatury i przede wszystkim dokumentów normatywnych, regulujących tę materię, wynika, że zalicza się do nich:

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

Nie zawsze jednak elementy te są traktowane równorzędnie. Zależności w tym wypadku tworzy środowisko pracy oraz otoczenie bliższe i dalsze poszczególnych elementów sieci.

W polskojęzycznej wersji dokumentu sojuszniczego *Dyrektywa bezpieczeństwa AD-70-1-PL* oraz w *Metodyce opracowywania szczególnych wymagań bezpieczeństwa systemu lub sieci teleinformatycznej (SWB)* spotykamy się z wyróżnieniem następujących rodzajów zagrożeń:

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

Zagrożenia wewnętrzne w tym kontekście odnoszą się do:

- utraty lub uszkodzenia danych w wyniku celowego działania użytkownika,
- braku możliwości obsługi systemu lub sieci informatycznej z powodu nieprawidłowego funkcjonowania,

- straty lub uszkodzenia informacji spowodowanych nieautoryzowanym dostępem,
- zniszczenia danych z powodu błędów w aplikacjach użytkowych, oprogramowaniu systemowym bądź wprowadzenie tzw. oprogramowania złośliwego – wirusa.

O **zagrożeniu zewnętrznym** mówimy wówczas, gdy zachodzi możliwość lub doszło do utraty lub uszkodzenia danych, utrata możliwości obsługi sieci teleinformatycznej w wyniku celowego bądź przypadkowego działania osób nieuprawnionych w zewnętrznym otoczeniu sieci.

Pojecie **zagrożeń fizycznych** w kontekście sieci teleinformatycznych nieodłącznie może się kojarzyć ze zniszczeniem infrastruktury sieci, urządzeń bądź samych obiektów, w których poszczególne elementy sieci są zainstalowane. Ich zniszczenie może nastąpić wskutek celowego działania potencjalnego przeciwnika w trakcie przygotowań do walki (okres kryzysu) lub w czasie prowadzenia działań zbrojnych bądź też jako efekt zaistnienia klęski żywiołowej, takiej jak: pożar, powódź, trzęsienie ziemi itp. Ponadto do tej grupy należy zaliczyć zagrożenia ze strony organizacji terrorystycznych, które są związane głównie z koniecznością zdobycia informacji niezbędnych do wykonania zamierzonego działania terrorystycznego, zdobycia lokalizacji obiektu, planów obiektów, planów działania w sytuacjach zagrożenia, informacji na temat stanu i możliwości sił bezpieczeństwa itp.

Inne spojrzenie na problematykę zagrożenia informacji w nowoczesnych sieciach teleinformatycznych, wykorzystujących w znacznej mierze techniki informatyczne, przedstawili w opracowaniu *Społeczeństwo informacyjne: szanse, zagrożenia, wyzwania* profesorowie Tomasz Goban-Klaus i Piotr Sienkiewicz. Wyodrębnili oni dwie grupy zagrożeń:

- sabotaż i zagrożenia nieumyślne,
- infiltrację.

Do pierwszej grupy zaliczyli zagrożenia charakteryzujące się występowaniem strat bez bezpośredniego materialnego czy informacyjnego zysku. Jako przykłady podali:

- pożary i inne klęski żywiołowe,
- awarie zasilania (systemu energetycznego),

- dezintegrację lub destrukcję informatyczną (wirusy, bomby logiczne, konie trojańskie itp.),
- fizyczne czynniki destrukcyjne i swoiste oddziaływanie ludzi.

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

W tej grupie zagrożeń znajduje się też sabotaż. Jego zasadniczym celem jest dezorganizacja pracy, zniszczenie lub uszkodzenie sieci teleinformatycznej. I w tym wypadku głównym źródłem zagrożenia jest człowiek. Może to być sfrustrowany, niezadowolony lub nieobowiązkowy pracownik techniczny obsługujący system lub nawet jego użytkownik, posiadający stosowną wiedzę lub uprawnienia. Gdy tego typu działanie jest inspirowane przez czynniki (osoby) zewnętrzne – wywiad gospodarczy lub innego państwa – działanie takie nazywamy dywersją.

W przeciwieństwie do sabotażu infiltracja to takie działanie osób nieupoważnionych, które ma na celu dążenie do zapewnienia sobie dostępu do informacji lub jej pozyskanie z zasobów danej sieci teleinformatycznej. Infiltracja jest dokonywana różnymi metodami i środkami, szczególnie poprzez „przenikanie" do wybranych (najbardziej wrażliwych lub słabo chronionych) elementów sieci. Infiltrację można podzielić na:

- bierną – śledzenie informacji w zadanym miejscu jej obiegu lub śledzenie częstotliwości wymiany informacji (np. zajętość kanału transmisyjnego);
- czynną – planowe i świadome zdobywanie informacji dzięki uzyskaniu dostępu do zasobów sieci z możliwością ingerencji w najważniejsze jej elementy lub nawet strukturę.

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

Najczęściej spotykane i stosowane metody infiltracji biernej to:

- przechwyt elektromagnetyczny oraz analiza sygnału emitowanego lub odbitego od promieniującego urządzenia (elementu sieci);

- dołączanie się do linii teletransmisyjnej sieci teleinformatycznej lub przechwyt informacji przesyłanej za pomocą środków radiowych;
- zdobywanie informacji przekazywanej środkami łączności, kanałami telekomunikacyjnymi w formie jawnej (bez zabezpieczenia kryptograficznego);
- analiza makulatury (np. wydruki komputerowe lub telefaksowe) oraz analiza elektronicznych nośników informacji;
- stosowanie ukrytych nadajników.

Z kolei w wyniku **infiltracji aktywnej** przeciwnik bezpośrednio zagraża danym, ich autentyczności (integralności).

Stosując infiltrację aktywną informacje uzyskuje się poprzez:
- uzyskanie dostępu do sieci;
- uzyskanie potwierdzenia tożsamości lub hasła upoważnionego użytkownika;
- korzystanie z przyłączonych urządzeń końcowych, gdy uprawniony użytkownik zawiesza pracę;
- przechwytywanie informacji użytkownika i podstawienie innych informacji;
- nielegalne korzystanie z komputera lub sprzętu łączności w czasie prac konserwatorskich;
- nielegalny wydruk zawartości pamięci komputera po zakończeniu działania programu.

Zasadniczym celem infiltracji aktywnej jest:

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

Jak już wspomniano, podziału zagrożeń dla bezpieczeństwa informacji w sieciach teleinformatycznych można dokonywać w wielu aspektach i płaszczyznach. Może to być zatem, na zasadzie „lustrzanego odbicia", podział odpowiadający obszarom stosowanych w praktyce środków oraz przedsięwzięć organizacyjno-technicznych i eksploatacyjnych, podejmowanych w celu zapewnienia bezpieczeństwa informacji w sieciach tele-

informatycznych. Zarówno w środowisku cywilnym, jak i wojskowym doktrynalnie przyjmuje się następujące obszary przedsięwzięć zapewniających ochronę całej sieci lub wybranych elementów oraz samej informacji:

- organizacyjno-proceduralne,
- personalne,
- fizyczne,
- techniczne.

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

W dalszych rozważaniach, opierając się na obowiązujących dokumentach normatywnych oraz na podstawie praktyki i doświadczeń, przedstawiono próbę przyporządkowania najczęściej identyfikowanych i występujących zagrożeń dla bezpieczeństwa informacji w wymienionych obszarach, które są podstawą do określenia niezbędnych środków przeciwdziałania w celu sprostania wymaganiom stawianym wojskowym sieciom teleinformatycznym.

WYMAGANIA BEZPIECZEŃSTWA INFORMACJI STAWIANE WOJSKOWYM SIECIOM TELEINFORMATYCZNYM

Przystępując do określenia wymagań bezpieczeństwa informacji stawianych wojskowym sieciom teleinformatycznym, wyodrębniono następujące obszary:

- bezpieczeństwo personalne,
- bezpieczeństwo źródeł informacji,
- kontrola dostępu do zasobów sieci teleinformatycznej.

Bezpieczeństwo personalne jest nazywane także bezpieczeństwem osobowym. Zadaniem jego jest i będzie w przyszłości odsunięcie od dostępu do informacji i niedopuszczenie osób, które z różnych względów będą gotowe do ujawnienia informacji o szczególnym znaczeniu lub sposobów ich

przekazywania przez sieci teleinformatyczne. Może to dotyczyć wielu ludzi, którzy mogą mieć dostęp do urządzeń przekazujących informacje, w tym także poprzez ich obsługę lub serwis. Działania takie zmierzają w kierunku wyboru i sprawdzenia ich poprzez wyspecjalizowane organy zarządzania bezpieczeństwem, a właściwy dobór personelu do pracy powinien skutecznie eliminować ewentualne zagrożenia. Przede wszystkim niezbędne jest przeprowadzenie weryfikacji 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, na którym takie dane mogłyby się znajdować.

Wymagania w zakresie bezpieczeństwa personalnego będą się zmieniały wraz z postępującymi zmianami wyposażenia w techniczne środki łączności i informatyki, strukturalnymi jednostek oraz w konsekwencji zmian stanowisk dowodzenia różnych szczebli. W ślad za tym powinien się przeobrażać system ochrony zasobów sieci teleinformatycznej. Punktem wyjścia powinna być aktualizacja istniejącej dokumentacji dotyczącej ochrony informacji niejawnych w sieciach teleinformatycznych, a następnie, na jej podstawie, wdrożenie i egzekwowanie systemu ich bezpieczeństwa. Fundamentem działania powinno być określenie strefy administracyjnej oraz stref bezpieczeństwa, systemu przepustowego i identyfikacji oraz ograniczenie dostępu osób niepowołanych do miejsc, w których istnieje zagrożenie nieautoryzowanego dostępu do informacji mających szczególne znaczenie. Oczywiście stworzony system bezpieczeństwa powinien uwzględniać konieczność ochrony i obrony elementów sieci teleinformatycznej, które gromadzą, przetwarzają i przekazują wiadomości niejawne, a zastosowane środki techniczne powinny mieć zabezpieczenia uniemożliwiające celowe ich zdobycie przez osoby nieuprawnione.

Bezpieczeństwo źródeł informacji o charakterze niejawnym w wojskowych sieciach teleinformatycznych wymusza konieczność tworzenia systemu ich rejestrowania, ewidencji dostępu osób uprawnionych i kontroli zapobiegających ich przechwyceniu przez osoby nieuprawnione oraz próbom modyfikowania ich treści. Wiadomości w nich zawarte należy chronić od chwili ich powstania, aż do zmiany klauzuli informacji na „jawne" bądź jej zniszczenia zgodnie z obowiązującymi przepisami.

Mając na uwadze konieczność prowadzenia działań poza miejscami stałego pobytu jednostek, w rejonach rozmieszenia stanowisk dowodzenia

powinny być zorganizowane lub rozmieszczone specjalne pomieszczenia do ich przechowywania, ochraniane przez osoby do tego wyznaczone oraz środki techniczne. Są to kancelarie niejawne (zazwyczaj na pojazdach), w których należy gromadzić źródła informacji wrażliwych, zawierających ważne dane w różnej postaci (coraz częściej w postaci nośników elektromagnetycznych).Wymusza to konieczność stosowania barier utrudniających uzyskanie informacji z urządzeń je przekazujących, gromadzących i przetwarzających, a ewidencja dokumentów powinna umożliwiać uzyskanie danych o stanie ilościowym dokumentów, o tym, kto był i jest ich użytkownikiem.

Bezpieczeństwo źródeł informacji w wojskowych sieciach teleinformatycznych można zapewnić, wykonując następujące czynności:

- nadanie klauzuli tajności i odpowiedniego priorytetu ochrony źródła informacji;
- zabezpieczenie przed utratą lub ujawnieniem treści źródła informacji;
- każdorazowe potwierdzenie otrzymania wiadomości ze źródła informacji przez osobę użytkującą, która po zakończeniu korzystania z niej ma obowiązek przekazania jej do kancelarii niejawnej;
- przestrzeganie przepisów eksploatacyjnych podczas korzystania z technicznych środków łączności i informatyki;
- wykrywanie i eliminowanie naruszeń obowiązujących zasad bezpieczeństwa informacji w sieciach teleinformatycznych;
- przestrzeganie przepisów korespondencji oraz stosowanie dokumentów, które mogą to ułatwić (np. tabele sygnałowe);
- realizowanie przedsięwzięć zabezpieczenia bojowego elementów celu ochrony elementów sieci teleinformatycznej, a także ich bezpośrednia ochrona i obrona;
- określenie kontrolowanych stref bezpieczeństwa;
- zapewnienie ochrony danych o sprzęcie niejawnym.

Sieci teleinformatyczne, w których następuje przetwarzanie wiadomości stanowiących tajemnicę służbową i państwową, muszą posiadać mechanizmy kontroli dostępu, a za ich wdrożenie oraz prawidłowe funkcjonowanie odpowiada administrator takiej sieci, który określa warunki, a także sposób przydzielenia uprawnień dostępu, kont i haseł. W tym względzie powinien ściśle współpracować z pełnomocnikiem dowódcy do spraw ochrony

informacji niejawnych, pomimo że nie jest jego podwładnym. Wszystkie uzgodnienia, przydział kont, hasła, uprawnienia dla poszczególnych użytkowników, procedury bezpieczeństwa, powinny być zawarte w wytworzonym i dostosowanym do specyfiki danej jednostki dokumencie pod nazwą „szczegółowe wymagania bezpieczeństwa dla sieci teleinformatycznej".

Kontrola dostępu do zasobów sieci teleinformatycznej powinna polegać na przyznawaniu uprawnień jej użytkownikom oraz opracowywaniu metod do sprawdzania, kto, kiedy i z jakich zasobów korzystał, a także sposobu ochrony przed niewłaściwym działaniem personelu i użytkowników. Jest ściśle połączona z identyfikacją, wiarygodnością oraz upoważnieniami dostępu do informacji. Kontrolę dostępu organizuje dowódca danej jednostki organizacyjnej za pośrednictwem pełnomocnika do spraw ochrony informacji niejawnej. Jednakże, aby spełniała ona oczekiwania, powinna obejmować przedsięwzięcia mogące mieć wpływ na przekazywanie informacji w sieci teleinformatycznej. Do najważniejszych można zaliczyć zaliczyć:

- określenie klauzuli informacji niejawnych dostępnych dla poszczególnych użytkowników;
- zaopatrzenie osoby przeszkolonej (z poświadczeniem bezpieczeństwa) w identyfikatory uprawniające do wejścia do stref bezpieczeństwa i wyjścia z nich;
- przydzielenie indywidualnych kodów dostępu i haseł;
- udzielanie informacji niejawnych tylko w stopniu wymaganym na danym stanowisku pracy (tzw. zasada wiedzy koniecznej);
- ścisłą ewidencję wejść i wyjść z danej strefy bezpieczeństwa, a także korzystanie z określonych zasobów danych;
- szczegółową kontrolę osób mogących wnieść sprzęt do kopiowania oraz przekazywania informacji (poprzez wartowników, patrole, system identyfikatorów);
- skuteczną ochronę i obronę, a także kontrolę wszystkich osób mogących stanowić zagrożenie dla bezpieczeństwa wiadomości niejawnych;
- przechowywanie informacji zgodnie z przyjętymi wymaganiami (chronione źródła informacji, np. dyski twarde i inne nośniki elektromagnetyczne);
- przekazywanie informacji tylko zgodnie z wcześniej ustalonymi oraz sprawdzonymi sposobami, które mogą je uchronić przed osobami nieuprawnionymi.

PODSUMOWANIE

Podstawowym wnioskiem płynącym z analizy zagadnień poruszonych w tym artykule jest przekonanie, że projektowanie i organizowanie infrastruktury bezpieczeństwa wojskowych sieci teleinformatycznych musi być kompleksowe. Tylko wtedy będziemy mogli mówić o prawidłowej organizacji, jeżeli uda się zbudować nową jakość ponad sumę użytych elementów, a to można osiągnąć tylko dzięki umiejętnemu połączeniu przedsięwzięć z dziedziny organizacji, polityki kadrowej, zarządzania oraz szeroko rozumianych zabezpieczeń technicznych i programowych.

Konieczność budowy infrastruktury bezpieczeństwa jest zdeterminowana występowaniem szerokiego spektrum zagrożeń w odniesieniu do samych sieci teleinformatycznych oraz informacji w nich wytwarzanych, przetwarzanych, przechowywanych i przesyłanych.

Zapewnienie bezpieczeństwa informacji w wojskowych sieciach teleinformatycznych zależy od specyfiki każdej sieci, choćby z punktu widzenia jej struktury organizacyjnej, zastosowanych środków informatycznych, komutacyjnych, transmisyjnych czy końcowych. Istotne jest również środowisko oraz otoczenie bliższe i dalsze, w którym sieć teleinformatyczna ma działać.