Ewa Chojnacka

Bezpieczeństwo usług teleinformatycznych resortu obrony narodowej

Obronność - Zeszyty Naukowe Wydziału Zarządzania i Dowodzenia Akademii Obrony Narodowej nr 4, 36-44

2012

AUTOR
mgr Ewa Chojnacka

RECENZENT
dr hab. inż. Józef Janczak

BEZPIECZEŃSTWO USŁUG TELEINFORMATYCZNYCH RESORTU OBRONY NARODOWEJ

Jakość usług teleinformatycznych w perspektywie postępu technologicznego wymusiła zwiększenie wymagań dotyczących zapewnienia odpowiedniego poziomu bezpieczeństwa usług teleinformatycznych, a co za tym idzie spełnienia szeregu wymogów na poziomie informatycznym i telekomunikacyjnym.

Z historycznego punktu widzenia bardzo bliskie są nam urządzenia telegrafu i telefonu, zważywszy na fakt, że już w roku 1839 oddano do użytku pierwszy komercyjny elektryczny telegraf, a w roku 1896 tradycyjny niezależny telefon. Oba te urządzenia przez wiele lat cieszyły się swoją świetnością i stały się początkiem ery transmisji danych i głosu. Tak zwana telekomunikacja stała się więc dziedziną techniki i nauki zajmującą się transmisją wszelkiego rodzaju informacji na odległość. Pojęcie to obejmuje również *sposoby przetwarzania informacji, kodowanie, sprzęt telekomunikacyjny, teorie propagacji, sieci telekomunikacyjne i wiele innych zagadnień*[1]. Dlatego też podczas I wojny światowej pozyskanie informacji wroga w trakcie działań wojennych miało strategiczne znaczenie. Nieprzypadkowo więc na początku XX wieku skonstruowano Enigmę – pierwszą maszynę szyfrującą, będącą skutecznym narzędziem do zabezpieczenia informacji przesyłanej między innymi dla Wehrmachtu. Kolejny etap transformacji przekazu informacji nastąpił w erze komputeryzacji, która poprzedziła informatyzację. Czym zatem jest teleinformatyka? Nazwa sama w sobie składa się z dwóch części: słowa informatyka i przedrostka tele – od telekomunikacja. Zatem teleinformatyka to przede wszystkim *dział telekomunikacji i informatyki, zajmujący się technologią przesyłu informacji oraz narzędziami logicznymi do sterowania przepływem oraz transmisją danych za pomocą różnych medium*[2].

Po dzień dzisiejszy dostęp do szeregu informacji jest ściśle zabezpieczany przed przedostaniem się w niepowołane ręce, chociażby w sferze bezpieczeństwa państwa, czy też bezpieczeństwa usług teleinformatycznych, których przykładem jest bezpieczeństwo bankowości elektronicznej.

[1] http://pl.wikipedia.org/wiki/Telekomunikacja.
[2] http://pl.wikipedia.org/wiki/Teleinformatyka.

Stąd też **celem** niniejszego artykułu w kontekście sytuacji problemowej jest określenie zmian zachodzących pod wpływem rozwoju technologii informatycznej w zakresie bezpieczeństwa usług teleinformatycznych w resorcie obrony narodowej.

Przeprowadzenie analizy obowiązującej dokumentacji dotyczącej zapewnienia bezpieczeństwa dla systemów teleinformatycznych w resorcie obrony narodowej, Strategii Bezpieczeństwa Narodowego RP oraz dostępnej literatury były podstawą do sformułowania problemu wyrażonego pytaniem: Jaki wpływ na bezpieczeństwo usług teleinformatycznych ma rozwój i synergia w sektorze IT[3]?

Wnioski z analizy współczesnych zagrożeń cyberterroryzmu[4] i cybersabotażu[5] poprzez dokonanie kontrolowanego ataku w cyberprzestrzeni[6] prowadzą do dokonania oceny stanu bezpieczeństwa teleinformatycznego w odpowiednich służbach państwa. *Według Pierre'a Levy'ego cyberprzestrzeń ma charakter „plastyczny, płynny, obliczalny z dużą dokładnością i przetwarzalny w czasie rzeczywistym, hipertekstualny, interaktywny i wreszcie wirtualny. Uważam go za znamienną cechę cyberprzestrzeni. To nowe środowisko umożliwia współdziałanie i sprzęganie wszystkich narzędzi tworzenia informacji, rejestrowania, komunikacji i symulacji. Perspektywa powszechnej numeryzacji informacji i przekazów uczyni prawdopodobnie z cyberprzestrzeni główny kanał informacyjny i główny nośnik pamięciowy ludzkości, poczynając od pierwszych lat przyszłego stulecia*[7].

Złożoność tej problematyki wymagała postawienia kilku problemów szczegółowych, które ukierunkowały dalsze dociekanie naukowe:

- Jakie zmiany nastąpiły w obszarze sieci teleinformatycznych w celu zapewnienia odpowiedniego poziomu bezpieczeństwa teleinformatycznego?
- Jakie są obecnie największe zagrożenia dla utrzymania bezpieczeństwa teleinformatycznego w sektorze administracji publicznej?
- Jakie należy podjąć działania w celu poprawienia bezpieczeństwa usług teleinformatycznych MON?
- Jakie są szanse rozwoju bezpieczeństwa sieci teleinformatycznej MON?

Mając na uwadze pragmatyczny i poznawczy charakter przedmiotowego artykułu, należy określić obszar opisywanej sieci telekomunikacyjnej w zakresie od funkcjonalności sieci w Ministerstwie Obrony Narodowej do zabezpieczenia szeregu usług użytkownikom końcowym resortu obrony narodowej. Ponadto w rozważaniach uwzględniono bezpieczeństwo w aspek-

[3] Information Technology z ang.– technologia informacyjna.
[4] Przestępstwo o charakterze terrorystycznym popełnione w cyberprzestrzeni.
[5] Celowe zakłócenie prawidłowego funkcjonowania cyberprzestrzeni.
[6] Sieć do otwartego komunikowania się za pośrednictwem połączonych komputerów i pamięci informatycznych pracujących na całym świecie.
[7] http://techsty.art.pl/hipertekst/cyberprzestrzen.htm.

cie sieci INTERMON[8] i MIL-WAN[9]. W tym miejscu należy krótko scharakteryzować system teleinformatyczny MIL-WAN, który jest rozległą siecią komputerową (WAN[10]) resortu obrony narodowej łączącą lokalne sieci komputerowe (LAN[11]) jednostek organizacyjnych. Zadaniem systemu teleinformatycznego jest zapewnienie usług teleinformatycznych na potrzeby resortu obrony narodowej. Dostęp do systemu otrzymują tylko i wyłącznie osoby pracujące w resorcie obrony narodowej, które pozytywnie przeszły postępowanie sprawdzające w zakresie poświadczenia bezpieczeństwa osobowego. Co więcej posiadają konto dostępowe w systemie i są uwierzytelnieni w tym systemie. System teleinformatyczny MIL-WAN zlokalizowany jest na terenie całego kraju i poza jego granicami. Wykorzystuje w systemie łącza operatorskie korporacyjnych sieci rozległych, zapewniając bezpieczeństwo i poufność przesyłanych danych.

Obecnie telekomunikacja w coraz większym stopniu zależy od rozwiązań informacyjnych i zaczyna odgrywać coraz większe znaczenie. Komu powinno więc zależeć na bezpieczeństwie informacji? *Nie ul*ega *wątpliwości, że każda organizacja potrzebuje chronić swoje informacje i postępować z nimi w sposób gwarantujący ich bezpieczeństwo*[12].

W firmach, instytucjach rządowych lub innych organizacjach rzadko zdarza się, by nie występowały informacje, których ujawnienie, niedostępność lub bezprawna zmiana przyniesie istotną szkodę interesom organizacji. *System teleinformatyczny, jako miejsce o szczególnej koncentracji wrażliwej informacji, stanowi zatem miejsce, które należy szczególnie ochronić*[13]. Przy czym w miarę jak dynamicznie rozwija się technologia informatyczna, tak szybko sposób ochrony w tym obszarze wymaga permanentnego doskonalenia utrzymywania bezpieczeństwa systemu na odpowiednim poziomie. W opinii P. Sienkiewicza *wyrazem potrzeb informacyjnych w organizacji jest zjawisko popytu informacyjnego, związane z koniecznością likwidowania (ograniczania) luki informacyjnej*[14]*.* Skoro informacja jest cenna, to jak ją skutecznie zabezpieczyć? Można zatem stwierdzić, że przez bezpieczeństwo rozumie się też s*tan nie zagrożenia, spokoju, pewności*[15] lub s*tan jednostki*

[8] INTERMON – wydzielona sieć informacyjna pracująca na protokole TCP/IP resortu obrony narodowej przeznaczona do wymiany informacji jawnej, posiadająca organizowany dostęp do zasobów sieci Internet.

[9] MIL-WAN – odseparowany system teleinformatyczny, w którym przetwarzane są informacje do klauzuli Zastrzeżone.

[10] Z ang.WAN – Wide Area Network, rozległa sieć komputerowa

[11] Z ang. LAN – Local Area Network, lokalna sieć komputerowa.

[12] http://www.centrum.bezpieczenstwa.pl/artykuly/BITSR_18_isecMan.pdf.

[13] A.E. Patowski, *Dokumentowanie systemu bezpieczeństwa teleinformatycznego – plan bezpieczeństwa teleinformatycznego organizacji*, [w:] *Bezpieczeństwo teleinformatyczne pod redakcją* K. Lidermana, WAT, Warszawa 2006, s. 33.

[14] M. Wrzosek, *Procesy informacyjne w zarządzaniu organizacją zhierarchizowaną*, AON, Warszawa 2010.

[15] *Słownik języka polskiego*, Warszawa 1979, s. 21.

lub grupy, który polega na braku zagrożenia[16], zarówno w warstwie fizycznej, jak i aplikacyjnej systemu.

Niezależnie od kształtującego się systemu bezpieczeństwa teleinformatycznego zaczęto kłaść nacisk na stworzenie procedur i zasad dotyczących zarządzania bezpieczeństwem. *Wzrost świadomości wagi informacji i jej bezpieczeństwa znajduje swoje odzwierciedlenie w dynamicznym rozwoju standardów międzynarodowych dla systemów zarządzania bezpieczeństwem informacji i rosnącym zainteresowaniem przedsiębiorców tą problematyką*[17]*.* Szereg zasad ściśle formułują techniki bezpieczeństwa i normy. Należy do nich między innymi norma PN-ISO/IEC 17799:2007 mówiąca, że *bezpieczeństwo informacji oznacza jej ochronę przed wszelkimi zagrożeniami, co ma na celu zapewnienie ciągłości działań, minimalizacji ryzyka i maksymalizacji zwrotu z inwestycji oraz możliwości biznesowych*[18]. Potrzeba utrzymania pewnych informacji w tajemnicy i w sposób odseparowany od osób i organizacji niepowołanych sprawiła, iż rozpoczęła się szersza forma audytu bezpieczeństwa zajmująca się zarządzaniem bezpieczeństwem informacji.

Jednym z najważniejszych dokumentów normatywnych regulujących wymogi bezpieczeństwa budowy systemu teleinformatycznego w organizacji publicznej jest Ustawa o ochronie informacji niejawnych (Dz.U.2010.182.1228). Przepisy ustawy mają zastosowanie również do *jednostek organizacyjnych podległych Ministrowi Obrony Narodowej lub przez niego nadzorowanych*[19]*.* Rozdział 8 wyżej wymienionej ustawy, poświęcony bezpieczeństwu teleinformatycznemu, określa proces przygotowania stosownej dokumentacji dla systemów teleinformatycznych. W myśl art. 48 ust. 1 s*ystemy teleinformatyczne, w których mają być przetwarzane informacje niejawne, podlegają akredytacji bezpieczeństwa teleinformatycznego*[20]. Zatem poprzez *dopuszczenie do eksploatacji dowolnego systemu teleinformatycznego*[21] należy rozumieć zgodę komórki nadzorującej, którą jest Służba Kontrwywiadu Wojskowego i Agencja Bezpieczeństwa Wewnętrznego. Proces ten ma na celu opracowanie Szczególnych Wymagań Bezpieczeństwa (SWB)[22] dla każdego nowo powstającego systemu

[16] A. Nowak, W. Scheffs, *Zarządzanie bezpieczeństwem informacyjnym*, Warszawa 2010, s. 22.

[17] Tamże, s. 25.

[18] PN-ISO/IEC 17799:2007, Technika informatyczna – Techniki bezpieczeństwa – Praktyczne zasady zarządzania bezpieczeństwem informacji, PKN, Warszawa 2007, s. 9.

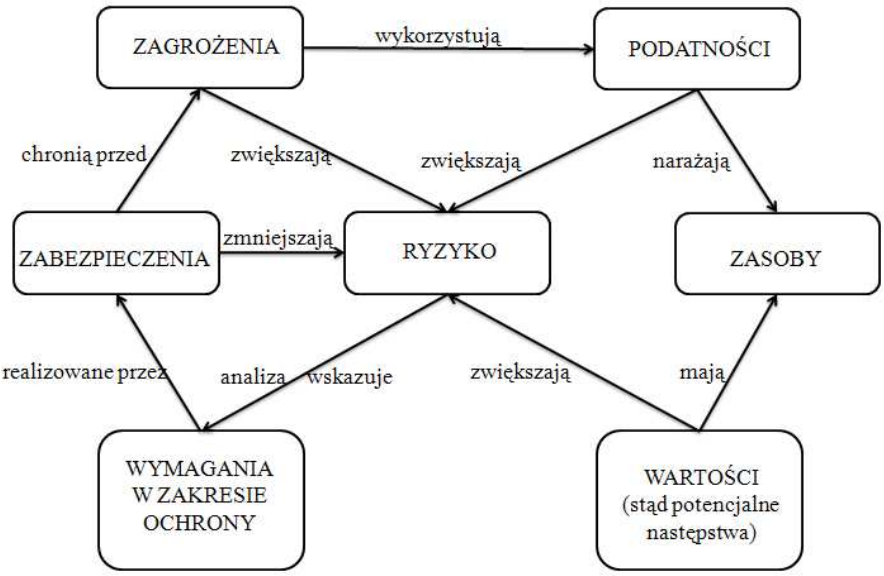
[19] Ustawa o ochronie informacji niejawnych, art. 1, ust. 2, pkt 2, Dz.U.2010.182.122.

[20] Ustawa o ochronie informacji niejawnych, art. 48, ust. 1, Dz.U.2010.182.1228.

[21] Ustawa o ochronie informacji niejawnych, art. 48, ust. 1, Dz.U.2010.182.1228.

[22] Dokument tworzony w celu dopuszczenia systemu lub sieci teleinformatycznej do wytwarzania, edytowania lub archiwizacji dokumentów niejawnych posiadających klauzulę ZASTRZEŻONE, POUFNE, TAJNE i ŚCIŚLE TAJNE. Dokument ten określa budowę, konfigurację, specyfikę pracy oraz zagrożenia systemu lub sieci teleinformatycznej, wynikające z niepowołanego dostępu do danych niejawnych. Organem zatwierdzającym SWB są służby ochrony państwa, czyli Agencja Bezpieczeństwa Wewnętrznego i Służba Kontrwywiadu Wojskowego.

teleinformatycznego. *Powinien on zawierać w szczególności wyniki procesu szacowania ryzyka dla bezpieczeństwa informacji niejawnych przetwarzanych w systemie teleinformatycznym oraz określać przyjęte w ramach zarządzania ryzykiem sposoby osiągania i utrzymywania odpowiedniego poziomu bezpieczeństwa systemu, a także opisywać aspekty jego budowy, zasady działania i eksploatacji, które mają związek z bezpieczeństwem systemu lub wpływają na jego bezpieczeństwo*[23]. Jakie relacje zachodzą między elementami bezpieczeństwa, przestawia poniższy schemat.



Źródło: A. Białas, *Podstawy bezpieczeństwa systemów teleinformatycznych*, Gliwice 2002.

Rys. 1. Relacje pomiędzy zarządzaniem ryzykiem

Przebieg i wyniki procesu szacowania ryzyka mogą zostać przedstawione w odrębnym dokumencie niż dokument Szczególnych Wymagań Bezpieczeństwa. Następnie opracowuje się Procedury Bezpiecznej Eksploatacji (PBE)[24]. Ma to miejsce na etapie wdrażania oraz modyfikacji eksploatacji systemu teleinformatycznego w resorcie obrony narodowej.

Ponadto podstawowe kryteria bezpieczeństwa teleinformatycznego regulują następujące decyzje Ministra Obrony Narodowej:

[23] Ustawa o ochronie informacji niejawnych, art. 49, Dz.U.2010.182.122.

[24] Dokument tworzony w celu dopuszczenia systemu lub sieci teleinformatycznej do wytwarzania, edytowania lub archiwizacji dokumentów niejawnych posiadających klauzulę ZASTRZEŻONE, POUFNE, TAJNE i ŚCIŚLE TAJNE. Dokument ten określa szczegółowe role i zasady eksploatacji systemu.

1. Decyzja Nr 30/MON Ministra Obrony Narodowej z dnia 8 marca 2000 roku w sprawie powoływania pełnomocników do spraw ochrony informacji niejawnych, administratorów systemu i sieci teleinformatycznych oraz utworzenia pionów ochrony w jednostkach organizacyjnych resortu obrony narodowej,
2. Decyzja Nr 181/MON Ministra Obrony Narodowej z dnia 6 października 2000 roku w sprawie organizacji szczególnej ochrony systemów sieci teleinformatycznych w resorcie obrony narodowej,
3. Decyzja Nr 357/MON Ministra Obrony Narodowej z dnia 29 lipca 2008 roku w sprawie organizacji i funkcjonowania systemu na incydenty komputerowe w resorcie obrony narodowej,
4. Decyzja Nr 7/MON Ministra Obrony Narodowej z dnia 20 stycznia 2012 roku w sprawie organizacji ochrony systemów teleinformatycznych do przetwarzania informacji niejawnych w resorcie obrony narodowej.

Z kolei informacja oprócz szeregu zabezpieczeń, które ze sobą niesie, rozpoczyna swój obieg przy pomocy narzędzi informatycznych, stając się częścią ogólnie dostępnej usługi teleinformatycznej, np. dowolny serwis www, poczta elektroniczna czy komunikatory sieciowe.

Powszechny stał się dostęp do szeregu instytucji administracji publicznej przez Internet, mowa tu chociażby o Elektronicznej Platformie Usług Administracji Publicznej (ePUAP)[25], za pośrednictwem której każdy obywatel może za pomocą skrzynki podawczej przesłać wniosek, skargę, zapytanie, itp. do zainteresowanego urzędu w kraju. Jest to jedna z wielu form elektronicznego usługodawstwa działająca na rzecz obywatela. Kolejnym przykładem dobrej usługi na rzecz obywatela jest możliwość złożenia elektronicznego zeznania podatkowego. Powyższe przykłady mają swoje zalety, mam tu na myśli oszczędność czasu.

W przypadku ePUAP jest to zamierzony i świadomy dostęp do informacji zamieszczonych na portalu, czyli usługa ma za zadanie zaspokoić podstawowe potrzeby użytkownika. W systemach teleinformatycznych resortu obrony narodowej oprócz ePUAP funkcjonują następujące usługi i oprogramowania:

1. systemy operacyjne na bazie MS Windows dopuszczone do użytkowania,
2. systemy wirtualizacji dopuszczone do użytkowania,
3. usługa Active Directory w oparciu o system MS Windows,
4. usługa antywirusowa,
5. usługa poczty elektronicznej oparta na oprogramowaniu MS Exchange,
6. elektroniczny obieg dokumentów: ”SI ARCUS” ,
7. VoIP/VTC.

[25] Ogólnopolska platforma teleinformatyczna służąca do komunikacji obywateli z jednostkami administracji publicznej w ujednolicony, standardowy sposób.

Z punktu widzenia klienta, np. zadaniem elektronicznego obiegu dokumentów jest zapewnienie elektronicznej wersji obiegu dokumentów poprzez wprowadzenie ich przez kancelarie jawne, następnie skierowanie do dekretacji komórek odpowiedzialnych merytorycznie, w dalszej kolejności dokonanie kolejnych dekretacji do osób bezpośrednio zainteresowanych wewnątrz komórki w celu realizacji. SI ARCUS jest jednym z zasadniczych projektów informatycznych przewidzianym do realizacji w „Strategii Informatyzacji Resortu Obrony Narodowej na lata 2008–2012". Program wykonany został w technologii Lotus Notes/Domino przez programistów w Urzędzie Ministra Obrony Narodowej. Z kolei VoIP (ang. Voice over Internet Protocol) to określenie technologii umożliwiającej przesyłanie głosu za pomocą łączy internetowych lub dedykowanych sieci wykorzystujących protokół IP, popularnie nazywanej telefonią internetową. Głos w postaci danych przesyłany jest przy użyciu protokołu IP. Natomiast VTC (ang. Video Tele Conference) to wideokonferencja prowadzona przy pomocy technologii telekomunikacyjnej pomiędzy co najmniej dwoma lokalizacjami. Także można stwierdzić, że głównym celem usługi jest *dostarczenie wartości odbiorcy poprzez umożliwienie mu uzyskania przez niego wyników*[26], np. elektronicznego dokumentu, głosu, obrazu.

Jakie są więc zagrożenia dla utrzymania bezpieczeństwa systemu teleinformatycznego Ministerstwa Obrony Narodowej? Zagrożenia dla Sytemu mogą nadejść zewsząd. Można przez to rozumieć zarówno zamierzony atak zewnętrzny, jak i wewnętrzny, taki do którego dostęp posiada osoba pracująca w resorcie. Dochodzi wtedy do utraty poufności, czyli do *nieautoryzowanego ujawnienia informacji przez nieuprawniony dostęp do systemu*[27]. Należy również wziąć pod uwagę utratę integralności, czyli nieautoryzowaną modyfikację zasobów systemu oraz utratę dostępności, czyli brak dostępu spowodowany powodzią, przerwą w dostawie energii elektrycznej lub też zawirusowaniem systemu teleinformatycznego. W związku z powyższym potencjalnego zagrożenia naruszenia bezpieczeństwa systemu teleinformatycznego MIL-WAN należy upatrywać w użytkownikach wewnętrznych lub fizycznym zerwaniu łączy telekomunikacyjnych w punkcie styku sieci[28] MIL-WAN.

Jakie należy podjąć działania w celu poprawienia bezpieczeństwa? Aby zapewnić odpowiedni poziom bezpieczeństwa systemu teleinformatycznego, należy zapewnić systemowi następujące cechy:

[26] Definicja usługi wg ITIL Foundation.

[28] Punkt styku sieci – fizyczny lub logiczny punkt połączenia sieci telekomunikacyjnych przedsiębiorców telekomunikacyjnych lub użytkowników specjalnych, niebędący zakończeniem sieci; Rozporządzenie Ministra Infrastruktury z dnia 21 lipca 2008 r. w sprawie szczegółowych wymagań dla zapewnienia dostępu telekomunikacyjnego;Dz.U. nr 145, poz. 919 z dnia 8 sierpnia 2008 r.

1. odrębną, samodzielną sieć teleinformatyczną,
2. logowanie do domeny wymuszane na każdym użytkowniku rejestrującym się,
3. firewalle,
4. VPN,
5. dokumenty wytwarzane w Systemie, zarówno w formie elektronicznej, jak i papierowej,
6. posiadanie poświadczenia bezpieczeństwa przez użytkownika i administratorów,
7. używanie służbowego nośnika danych – pendrive.

Zwalczanie zagrożeń bezpieczeństwa systemów teleinformatycznych i sieci telekomunikacyjnych ma na celu *przeciwdziałanie przestępczości komputerowej oraz innym wrogim działaniom wymierzonym w infrastrukturę telekomunikacyjną, w tym zapobieganie atakom na elementy tej infrastruktury*[29]. Strategia Bezpieczeństwa Narodowego z 2007 roku w zakresie Bezpieczeństwa Teleinformatycznego określa *interesy narodowe i formułuje cele strategiczne*[30] w celu bezpiecznego rozwoju cywilizacji suwerennego państwa. Stawia to przed każdą z instytucji podległych Prezesowi Rady Ministrów szereg obowiązków w tym zakresie.

Należy zatem określić szanse rozwoju systemów teleinformatycznych Ministerstwa Obrony Narodowej poprzez:

1. dostosowanie zapisów dokumentacji do obecnie obowiązujących przepisów prawa,
2. stworzenie możliwości łączenia się sytemu teleinformatycznego Mil-WAN z innymi systemami o równorzędnych klauzulach,
3. dopuszczenie do eksploatacji nowego oprogramowania.

Podsumowując, militarne sieci teleinformatyczne z racji rodzaju przetwarzanych informacji należą do grupy szczególnie narażonej na ataki cyberterrorystów. Dlatego też zarządzanie i koordynacja bezpieczeństwa teleinformatycznego powinny należeć do podstawowych zadań każdej organizacji i być świadczone na najwyższym poziomie.

TELEINFORMATIC SERVICES SECURITY OF THE NATIONAL DEFENCE SECTOR

Abstract: Telecommunication increasingly depends on information solutions and is beginning to gain more and more importance. It rarely happens that in companies, governmental institutions or other organizations there appears information whose releasing, inaccessibility or illegal change would

[29] Strategia Bezpieczeństwa Narodowego, Warszawa 2007, s. 20 pkt 80.
[30] Strategia Bezpieczeństwa Narodowego, Warszawa 2007, s. 3.

not bring about an essential harm to this organization's interests. Therefore the aim of this article is to define ongoing changes resulting from the development of information technology in teleinformatic services security in the national defence sector. The article includes binding regulations, threats and opportunities of teleinformatic systems' development.