

**Artur SZLESZYŃSKI\***

## **KONCEPCJA DOSTOSOWANIA SIECI TELEINFORMATYCZNEJ DO SIECIOCENTRYCZNEJ WYMIANY INFORMACJI**

### **Wstęp**

Istotą działań sieciocentrycznych jest stworzenie szybkiej i efektywnej platformy wymiany informacji, która pozwoli uzyskać przewagę taktyczną, strategiczną i operacyjną nad przeciwnikiem. Termin „sieciocentryczność”, a ściślej Walki Sieciocentrycznej<sup>1</sup> (z ang. Network Centric Warfare) pochodzi z literatury anglojęzycznej<sup>2</sup>. Dotyczy on takiej organizacji procesu gromadzenia, przetwarzania, selekcji i dystrybucji informacji, która zapewnia dostępność potrzebnych danych we właściwym miejscu i czasie. Nieistotny staje się czynnik lokalizacji geograficznej źródła informacji. Informacje potrzebne plutonowi czy drużynie mogą być pobierane z serwerów ulokowanych tysiące kilometrów od odbiorcy informacji. Podobny mechanizm można zaobserwować w systemach telefonii komórkowej oferujących abonentowi dostęp do sieci Internet.

Patrząc na opisaną funkcjonalność z punktu widzenia wymagań użytkownika w stosunku do sieci (jej operatora), znaczenie ma fakt dostarczenia potrzebnych informacji<sup>3</sup>, w jak najkrótszym czasie. Wykorzystanie danych dostarczonych za pomocą medium transmisyjnego, jakim jest sieć teleinformatyczna, będzie skutkowało osiągnięciem określonego zysku. Z powyższego założenia wynika, że dostępność informacji jest jednym z kluczowych czynników, który pozwala uzyskać przewagę nad przeciwnikiem na polu walki oraz konkurentem biznesowym.

### **1. Geneza i identyfikacja problemu**

Koncepcja dostępności informacji niezbędnej do osiągnięcia założonych celów działania pojawia się w obszarze systemów wspomagających procesy decyzyjne w przedsiębiorstwach. Każdy projekt biznesowy wymaga posiadania odpowiednich zasobów

---

\* kpt. mgr inż. Artur SZLESZYŃSKI - Wyższa Szkoła Oficerska Wojsk Lądowych

<sup>1</sup> Zob. J. Janczak, *Uwarunkowania działań sieciocentrycznych determinujące organizację sieci teleinformatycznych*, s. 22, J. Moffat, *Complexity theory ...*, s. 4.

<sup>2</sup> J. Janczak, *Organizacja sieci teleinformatycznych w działaniach sieciocentrycznych*, s. 47.

<sup>3</sup> Por. A. Michalski, *Dostępność informacji...*, s. 11

materiałowych (narzędzi, pieniędzy itp.), pracowników mogących osiągnąć wyznaczone w projekcie cele oraz czasu potrzebnego na doprowadzenie projektu do końca. Opisany schemat działania wykorzystywany jest w systemach informatycznych bazujących na metodach zarządzania klasy MRPII lub ERP. Podobną klasę problemów spotyka się w działaniu jednostek wojskowych. Tym co odróżnia typową instytucję biznesową od sił zbrojnych, jest brak występowania strat (czasami bardzo znacznych) ponoszonych w zasobach materiałowych i kadrze realizującej dane przedsięwzięcie. Kolejnym kryterium jest czas realizacji danego zadania prowadzonego przez siły zbrojne, który nie może zostać wydłużony. Opóźnienie będzie skutkowało powstawaniem jeszcze większych strat. Opisana sytuacja jest typowa dla konfliktu zbrojnego.

Literatura przedmiotu podaje, że dla użytkownika informacji istotne jest uzyskanie i utrzymanie połączenia z siecią. Problemem użytkownika nie powinno być indywidualne gromadzenie, przetwarzanie i przesyłanie informacji. Podobną „filozofię” funkcjonowania sieci teleinformatycznej można zauważyć w eksploatowanych powszechnie komercyjnych sieciach telekomunikacyjnych. Dostęp do różnego rodzaju usług najlepiej jest widoczny w sieciach telefonii komórkowej. Urządzenie końcowe, którym jest telefon użytkownika sieci bezprzewodowej, dawno przestał służyć tylko do prowadzenia rozmów. Liczba funkcji aparatu telefonicznego oraz możliwości usługowe sieci pozwalają na realizowanie usług dostępu do sieci Internet (transmisja danych), korzystanie z elektronicznego asystenta (prowadzenie elektronicznego terminarza, synchronizacja informacji przechowywanych wewnątrz urządzenia z systemem informatycznym znajdującym się na terenie firmy) wymianę wideofoniczną, wysyłanie krótkich wiadomości tekstowych (ang. Small MessageS – SMS) czy korzystanie z usług nawigacyjnych i lokalizacyjnych (integracja z systemem GPS – Global Positioning System).

W dostępnej literaturze można znaleźć sugestię, że w przypadku tak znacznych potrzeb związanych z potrzebą szybkiej i niezawodnej transmisji danych, ich zaspokojenie możliwe będzie tylko we współpracy z operatorami komercyjnymi<sup>4</sup>. Kompatybilność sprzętu teleinformatycznego wojskowego ze sprzętem telekomunikacyjnym wykorzystywanym przez operatorów komercyjnych sprawia, że tego typu współpraca możliwa jest do zrealizowania. Nie należy definitywnie odrzucać tego rodzaju współdziałania, gdyż w określonych sytuacjach może ono wspomagać funkcjonowanie infrastruktury wojskowej. Problemem, który pojawia się przy rozważaniu tego typu współpracy, jest fakt wyłączenia medium transmisyjnego spod kontroli organów wojskowych. Wymieniony problem można bagatelizować, wykazując, że jest on mało istotny, jeżeli rozważy się korzyści wynikające ze współpracy z operatorem komercyjnym. Nie należy jednak zapominać, że jednym z wymagań stawianych przed systemem łączności wojskowej jest utrzymanie skrytości rozumianej jako zachowanie poufności przekazywanych informacji oraz niejawności struktury i organizacji systemu łączności wojskowej. Według założeń teoretyków funkcjonowanie systemu sieciocentrycznego ma uprościć procesy obiegu informacji oraz decyzyjne, poprzez spłaszczenie struktury systemu dowodzenia<sup>5</sup>. Prawdopodobnie nie będą istniały stanowiska dowodzenia w postaci takiej, jak ma to miejsce obecnie. Skoro system teleinformatyczny ma działać sprawnie, to organ decyzyjny może znajdować się setki kilometrów od pododdziałów realizujących

---

<sup>4</sup> P. Dela, *Architektura sieci teleinformatycznej...*, s. 43

<sup>5</sup> J. Janczak, *Organizacja ...*, s. 26.

zadania. Problem, który należy rozwiązać w celu uzyskania założonego wcześniej efektu, można sformułować w postaci następującego pytania – jaka powinna być organizacja sieci teleinformatycznej, a w szczególności sieci radiowych pola walki, wykorzystywanej dla potrzeb dowodzenia podległymi siłami, która pozwoli osiągnąć cel (cele) misji bez ograniczania wymagań taktyczno – operacyjnych i eksploatacyjno – technicznych stawianych przed wojskowym systemem teleinformatycznym. Kolejnym problemem związanym z opracowaniem koncepcji organizacji sieci teleinformatycznej dla potrzeb sieciocentrycznej wymiany informacji, jest infrastruktura techniczna mogąca zapewnić realizację zadań postawionych przed siecią teleinformatyczną.

## 2. Propozycje rozwiązań

Do zbioru wymagań, taktyczno – operacyjnych<sup>6</sup> stawianych wojskowemu systemowi teleinformatycznemu należą:

- terminowość,
- wierność,
- skrytość.

Do grupy wymagań eksploatacyjno – technicznych<sup>7</sup> należą:

- gotowość operacyjna,
- przepustowość,
- trwałość,
- mobilność i adaptacyjność,
- bezpieczeństwo.

Wszystkie z wymienionych wymagań muszą zostać spełnione, żeby rozwiązanie uznać za bezpieczne i realizujące potrzeby organu dowodzenia. Analizując posiadane obecnie przez SZRP wyposażenie telekomunikacyjne i informatyczne, można przyjąć, że istnieje zaplecze techniczne pozwalające na zrealizowanie idei sieciocentrycznej wymiany informacji. Jednak przyjęta organizacja systemu łączności wykorzystywanego dla potrzeb dowodzenia wojskami, a szczególności systemu radiokomunikacyjnego, może implikować problemy w funkcjonowaniu sieciocentrycznej wymiany informacji. Obecnie łączność dzielona jest na trzy elementy funkcjonalne, łączność<sup>8</sup> dowodzenia, współdziałania, alarmowania (powiadamiania lub ostrzegania – w zależności od szczebla poddziału lub oddziału) rys 1.

Przedstawiony podział nie obejmuje łączności specjalistycznej (przeznaczonej do zapewnienia dowodzenia pododdziałami rodzajów wojsk), która jest elementem łączności dowodzenia, np. sieć radiowa zabezpieczenia logistycznego. Z faktu wydzielenia, z systemu łączności, sieci specjalistycznych wynika niedogodność polegająca na konieczności przydzielenia poszczególnym sieciom radiowym odmiennych planów częstotliwości i kodów realizujących szyfrowanie transmitowanych informacji. Rozdzielenie częstotliwościowe skutkuje brakiem łączności pomiędzy elementami funkcjonalnymi

<sup>6</sup> J. Michniak, *Dowodzenie i łączność*, s. 107.

<sup>7</sup> Tamże, s. 108.

<sup>8</sup> Pod pojęciem łączności należy rozumieć połączenie usług telekomunikacyjnych przewodowych i bezprzewodowych oraz realizację usług pocztowych w ramach jednego systemu.

mi systemu łączności, stanowiącego element systemu dowodzenia. Próbą pokonania opisanej niedogodności jest utworzenie urządzeń jedno i wielokanałowego radiodostępu simpleksowego (JRS i WRS).



Rys. 1. Rodzaje łączności wojskowej

*Źródło: Opracowanie własne na podstawie J. Michniak, Dowodzenie i łączność*

Istotą działania urządzeń pracujących w trybie jedno i wielokanałowego dostępu simpleksowego jest zapewnienie możliwości współpracy (integracja) użytkowników systemu telekomunikacyjnego, pracujących w innych sieciach radiowych oraz użytkowników urządzeń stacjonarnych. Korzystanie z usług JRS i WRS wymaga posiadania podłączonego do radiostacji, rodziny PR4G, specjalnego mikrotelefonu<sup>9</sup>. Użytkownik musi zarejestrować się w radiowym punkcie dostępowym (RPD). Urządzenie korzystające z usług RPD określane jest terminem RPA – radiowy punkt abonencki.

Urządzenia JRS i WRS zapewniają bezpieczną wymianę danych, ponieważ każdy użytkownik musi zostać zweryfikowany przez RPD. Użytkownik radiostacji uzyskuje możliwość pracy w trybie bezpołączeniowym (SMS i poczta głosowa), z którego nie mógł korzystać, gdy nie był RPA. Analizując działanie systemu JRS z punktu widzenia niezawodności rozumianej jako zdolność do zapewnienia ciągłości działania i dostępności informacji może wystąpić pewien problem polegający na braku dostępu do RPD w przypadku pracy poza zasięgiem środków radiowych wykorzystywanych w RPD. Wadą opisanego rozwiązania jest duża złożoność techniczna, jej skutkiem jest skomplikowana procedura konfiguracji sieci.

Kolejnym problemem jest brak obsługi użytkownika, który znajdzie się w zasięgu pracy innego RPD. Wynika to z faktu, iż do pracy z RPD wymagane jest posiadanie przez radiostację odpowiedniego planu częstotliwości oraz kluczy kryptograficznej ochrony informacji. Nie istnieje w systemie możliwość łatwego „przejmowania” użytkowników, tak jak ma to miejsce w przypadku stacji bazowych w systemie telefonii

<sup>9</sup> Np. mikrotelefon MTW-PR4G.

komórkowej. Brak przejmowania obsługi użytkownika będącego w ruchu znacznie ogranicza dostępność informacji. Ponieważ RPD znajdują się na szczeblu stanowiska dowodzenia batalionu, można stwierdzić, że działanie użytkownika związane jest z pracą w zasięgu działania środków radiowych tworzących RPD. Sposobem eliminacji opisanego zjawiska jest umieszczenie w strukturze pomocniczego węzła łączności aparatu WRS. Otwartą pozostaje kwestia automatycznego przesłania informacji o użytkowniku z RPD znajdującego się w węzle łączności SD batalionu do aparatu WRS w celu przejścia obsługi użytkownika. Brak jednoznacznej odpowiedzi wynika z faktu, iż dokumentacja techniczna JRS i WRS nie określa tej kwestii w sposób jednoznaczny. Skoro kwestia ta nie jest określona w sposób jednoznaczny, można założyć, że jedynym rozwiązaniem jest tworzenie dodatkowych (redundantnych) RPD, w których będą rejestrować się RPA. Dodatkowe RPD będą umieszczone w pomocniczym węzle łączności. Bazą techniczną do realizacji dodatkowych RPD będzie aparatura WRS.

Sieć radiokomunikacyjna powinna zapewnić wymianę informacji za pomocą medium radiowego. Ponieważ radiostacje eksploatowane w wojskach lądowych są radiostacjami pracującymi w zakresie UKF, szybkość transmisji danych nie jest wysoka. Maksymalnie można uzyskać szybkość transmisji 16 kb/s przy stałej częstotliwości roboczej. Korzystając z usług JRS i WRS, radiostacja pracuje w rodzaju pracy skaczącej częstotliwości z wykorzystaniem ochrony kryptograficznej przesyłanych informacji. W tym rodzaju pracy maksymalna szybkość transmisji wynosi 4,8 kb/s. Fakt ten wymaga doboru odpowiedniego sposobu transmisji danych, który pozwoli efektywnie wymieniać informacje. Wiadomości będą przekazami tekstowymi i sformatowanymi, gdyż ich przesyłanie nie będzie powodować zbyt długiej zajętości łącza. Opisany sposób wymiany wiadomości wykorzystywany jest w systemach kierowania środkami walki np. ŁOWCZA lub TOPAZ.

Kolejną kwestią związaną z dostępnością informacji są kwestie pokrycia sygnałem obszaru działania danego pododdziału. W terenie otwartym zasięg środków łączności jest wystarczający i w pełni pokrywa obszar działania sygnałem. W przypadku wykonywania zadań w terenie zurbanizowanym, górzystym lub w sąsiedztwie obszarów leśnych, działanie systemu łączności radiokomunikacyjnej będzie podlegało ograniczeniom. Ograniczenie zasięgu działania wynika z właściwości propagacyjnych fal radiowych zakresu UKF<sup>10</sup>. Zakładając, że kryterium terminowego dostarczenia informacji jest parametrem krytycznym, należy stworzyć sieć nadajników przekazujących wiadomości. Sieć ta umożliwi uzyskanie odpowiedniego pokrycia terenu sygnałem, zapewniając odpowiedni poziom dostępności informacji. Rozwiązanie to posiada wadę, retransmisja sygnału zwiększa pokrycie sygnałem terenu, ale zwiększa też zajętość kanału, co ogranicza jego przepustowość. Analizując opisane rozwiązanie za pomocą równania natężenia ruchu Erlanga<sup>11</sup> (1)

$$A = \frac{1}{T} \sum_{i=1}^n t_i \quad (1)$$

gdzie:

A – natężenie ruchu sieci telekomunikacyjnej,

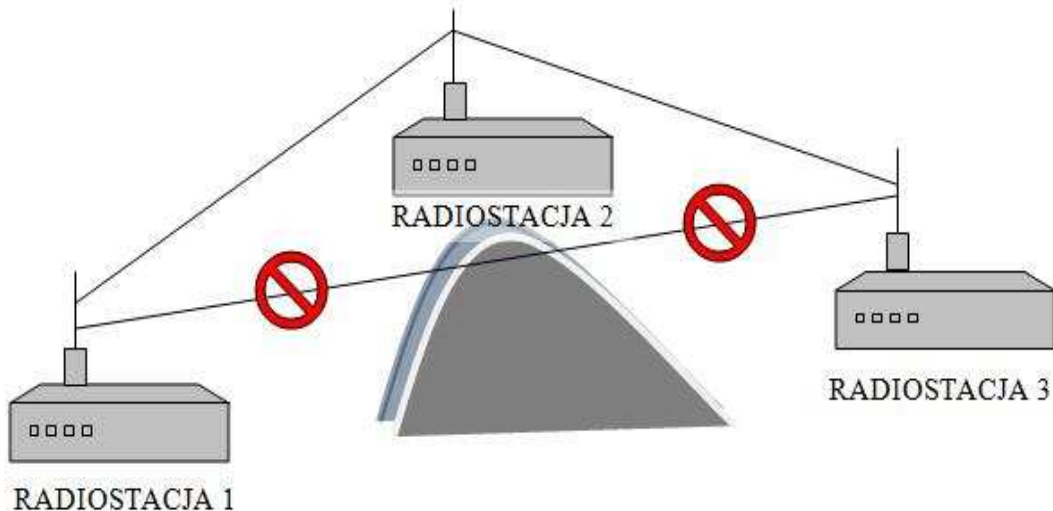
<sup>10</sup> J. Szóstka, *Fale i anteny*, s. 320.

<sup>11</sup> J. Jajszczyk, *Wstęp do telekomunikacji*, s. 355.

$T$  – całkowity czas obserwacji,  
 $t_i$  – czas zajętości kanału telekomunikacyjnego przez poszczególnych użytkowników.

Widać, że pojawienie się dodatkowego ruchu, niezbędnego z punktu widzenia dostępności informacji, będzie skutkowało zmniejszeniem przepustowości sieci. Dzieje się tak, ponieważ część czasu pracy sieci telekomunikacyjnej przeznaczana jest na powtarzanie wiadomości wysłanych wcześniej. Realizacja tej funkcjonalności wymaga urządzeń radiokomunikacyjnych pracujących w standardzie podziału czasu dostępu do medium (ang. Time Division Multiple Access – TDMA). Korzystając z opisanej funkcjonalności należy wybrać urządzenia oraz szczeliny czasowe w ramach których będzie realizowana cyfrowa retransmisja sygnału.

Opisany wcześniej problem związany z niską szybkością transmisji danych oraz obniżającym wpływem retransmisji, każą rozważyć konieczność zakupu urządzeń, które pozwolą zrealizować opisaną funkcjonalność bez znaczącego ograniczenia przepustowości sieci radiowej rys. 2.



Rys 2. Przykład pracy radiostacji w trybie cyfrowej retransmisji sygnału

*Źródło: Opracowanie własne*

Ponieważ istnieje ograniczenie związane z wykorzystaniem Radiowych Punktów Dostępnych związanych z koniecznością wprowadzenia do radiostacji odpowiedniego planu częstotliwości oraz kluczy kryptograficznej ochrony informacji, należałoby rozważyć modyfikację radiostacji pola walki tak, by pozwalały one na łatwe przenoszenie użytkownika pomiędzy istniejącymi w sieci RPD. Realizacja opisanego wymagania pozwoli zapewnić odpowiednią dostępność informacji.

Konieczność szybkiej i sprawnej wymiany informacji wewnątrz i na zewnątrz stanowisk dowodzenia wymaga wyposażenia stanowisk dowodzenia w urządzenia pracujące w zakresie mikrofalowym. Fale radiowe zakresu mikrofal zapewniają odpowiednią szybkość transmisji np. 115 kb/s (w standardzie GPRS) do 11 Mb/s (w standardzie Wi-Fi). Możliwość przesyłania sygnału za pomocą modulacji OFDM, pozwala uzyskać optymalną trasę propagacji w zależności od miejsca lokalizacji elementów systemu.

Opisane rozwiązanie obarczone jest wadami. Pierwszą z nich jest konieczność stosowania anten aperturowych do kierunkowego przesyłania sygnałów pomiędzy punktami sieci bezprzewodowej. Stosowanie anten o promieniowaniu dookólnym, prostszych w konstrukcji i niewymagających justowania listka głównego charakterystyki antenowej, znacznie ogranicza zasięg łączności ze względu na niski zysk energetyczny anteny. Niedogodność ta powoduje, że wykorzystanie wyższych częstotliwości roboczych sieci radiowej może być stosowane w ograniczonym obszarze np. do zapewnienia łączności wewnątrz stanowiska dowodzenia i połączenia stanowiska dowodzenia z węzłem łączności. Połączenia z węzłami łączności stanowisk dowodzenia szczebla batalionu a stanowiskami dowodzenia szczebli wyższych powinny być realizowane z użyciem urządzeń szerokopasmowych, zapewniających szybkość transmisji danych na poziomie od 512 kb/s do 2 Mb/s. Węzły łączności stanowisk dowodzenia szczebla batalionu będą pełniły rolę węzłów dostępowych dla użytkowników sieci telekomunikacyjnej szczebla kompanii i plutonu. Urządzenia radiowe wykorzystywane w plutonie i kompanii powinny posiadać możliwość zmiany trasowania informacji w sieci. W tym celu w węzle łączności powinna być przetwarzana informacja o aktualnym położeniu abonentów, a następnie zgodnie z algorytmem trasowania opartym na określeniu długości trasy oraz parametrów propagacyjnych wybieranoby urządzenia pełniące rolę lokalnych (znajdujących się wewnątrz sieci radiowej) urządzeń retransmisyjnych.

Zakładając, że działania pododdziałów będą charakteryzowały się dużą dynamiką, która może być przyczyną częstego znajdowania się części użytkowników poza systemem telekomunikacyjnym, konieczne jest posiadanie sieci urządzeń przekaźnikowych. Dodatkowo, jako uzupełnienie proponowanego rozwiązania, można korzystać z medium przewodowego np. sieć przewodowa operatora komercyjnego lub medium radiowego, jakim jest telefonia komórkowa. Pamiętać należy, że zarządzanie i kierowanie siecią telekomunikacyjną komercyjną jest całkowicie wyłączone z nadzoru sił zbrojnych. O ile korzystanie w warunkach kraju jest uzasadnione, o tyle należy do proponowanego rozwiązania podchodzić ze szczególną ostrożnością w przypadku krajów, w których ludność nie jest przyjaźnie nastawiona do wojsk rozmieszczonych na jego terytorium. W przypadku braku kontroli nad funkcjonowaniem sieci telekomunikacyjnej wykorzystywanej, jako medium transmisyjne, należy liczyć się z ograniczeniem poziomu poufności informacji. Może to wynikać ze specyficznych wymagań technicznych operatora, który może mieć problemy z przesyłaniem informacji szyfrowanej strumieniowo lub pakietów korzystających z protokołu IPSec (w wersji z szyfrowaną zawartością pakietu ESP ang. Encapsulated Security Payload). Opisane rozwiązanie było proponowane, jako jeden z mechanizmów ochrony poufności informacji w teleinformatycznych systemach wspomagających proces dowodzenia<sup>12</sup>.

## Podsumowanie

W proponowanym rozwiązaniu przyjęto pełną niezależność sieci telekomunikacyjnej od operatorów komercyjnych. Założenie to wynika z faktu, iż pododdziały mogą działać w terenie, gdzie korzystanie z infrastruktury telekomunikacyjnej operatora komercyjnego jest niemożliwe lub korzystanie z niej nie będzie uzasadnione. W rozważaniach skupiono się na szczeblu plutonu – kompanii, ponieważ to te pododdziały biorą udział we wszystkich rodzajach działań. Dostarczenie potrzebnych informacji na ten

---

<sup>12</sup> I. Józwiak, i inni, *Techniczne możliwości eliminacji...*, s. 168.

szczebel dowodzenia, czyli tam, gdzie jest ona najbardziej potrzebna, ma kluczowe znaczenie dla powodzenia wykonywanej przez pododdział misji. Jednocześnie przesłanie dużej ilości danych jest kłopotliwe lub niemożliwe, ze względu na posiadane przez pluton/kompanię wyposażenie teleinformatyczne.

Proponowane rozwiązanie wymaga nowego podejścia do planowania systemu łączności, w szczególności do planowania sieci radiowych pola walki. Należy ponownie zdefiniować wymagania dla systemów jedno i wielokanałowego radiodostępu simpleksowego. System powinien umożliwiać łatwe konfigurowanie urządzeń w nim pracujących. Aktualnie eksploatowane rozwiązania (radiostacje pola walki) nie gwarantują wykonania opisanego wymagania. Proponowanym rozwiązaniem jest stosowanie urządzeń umożliwiających automatyczną akredytację w radiostacji w systemie z możliwością usunięcia akredytacji w przypadku zagrożenia przejęciem urządzenia przez osoby nieuprawnione. Funkcjonalność odebrania akredytacji powinna być realizowana lokalnie i zdalnie.

Ważną cechą systemu sieciocentrycznego jest sprawna wymiana informacji przy założeniu, że proces ten jest bezpieczny, czyli gwarantuje zachowanie poufności przekazywanych informacji przy jednoczesnym zapewnieniu wierności i dostępności. Spełnienie wymienionych wymagań nie jest zadaniem prostym, gdyż wymaga nowego sprzętu i innego niż obecny sposobu organizowania systemu i określeniu procedur jego funkcjonowania. Konieczne jest odpowiednie przygotowanie personelu odpowiedzialnego za działanie poszczególnych elementów systemu, należy tu rozumieć szkolenia personelu odpowiedzialnego za zarządzanie pracą sieci teleinformatycznej oraz użytkowników urządzeń pracujących w systemie. Wiele incydentów związanych z bezpieczeństwem teleinformatycznym wynika z niewłaściwej konfiguracji elementów funkcjonalnych systemu oraz z braku umiejętności właściwej obsługi urządzenia.

## LITERATURA

1. Dela P., *Architektura sieci teleinformatycznych w świetle koncepcji NCW*, [w:] „Sieci teleinformatyczne w działaniach sieciocentrycznych”, [w:] *Materiały z międzynarodowej konferencji naukowej* pod red. J. Janczak, A. Wisz, Akademia Obrony Narodowej, Warszawa 2007, ISBN: 978-83-7523-002-4.
2. Jajszczyk J., *Wstęp do telekomutacji*, WNT, Warszawa 2000, ISBN 83-204-2600-6.
3. Janczak J., *Organizacja sieci teleinformatycznych w działaniach sieciocentrycznych*, [w:] *Problemy automatyzacji dowodzenia i kierowania*, pod red. E. Sędka, Przemysłowy Instytut Telekomunikacji, Warszawa 2008, ISBN: 83-906662-9-4.
4. Janczak J., *Uwarunkowania działań sieciocentrycznych determinujące organizację sieci teleinformatycznych*, [w:] „Sieci teleinformatyczne w działaniach sieciocentrycznych” [w:] *Materiały z międzynarodowej konferencji naukowej* pod red. J. Janczak, A. Wisz, Akademia Obrony Narodowej, Warszawa 2007, ISBN: 978-83-7523-002-4.
5. Józwiak J., Laskowski W., Szleszyński A., *Techniczne możliwości eliminacji zagrożeń bezpieczeństwa informacji w teleinformatycznych systemach wspomagających procesy decyzyjne*, [w:] *Problemy automatyzacji dowodzenia i kierowania*, pod red. E. Sędka, Przemysłowy Instytut Telekomunikacji, Warszawa 2008, ISBN: 83-906662-9-4.



6. Michalski A., *Dostępność informacji w organizacji gospodarczej*, Wydawnictwo Politechniki Śląskiej, Gliwice 2007, ISBN 978-83-7335-460-9.
7. Michniak J., *Dowodzenie i łączność*, Akademia Obrony Narodowej, Warszawa 2003.
8. Szóstka J., *Fale i anteny*, Wydawnictwa Komunikacji i Łączności, Warszawa 2000, ISBN: 83-206-1363-9.
9. Moffat J., *Complexity Theory and Network Centric Warfare*, CCRP, 2003, ISBN: 1-893723-11-9.
10. *Instrukcja eksploatacji mikrotelefonu wielofunkcyjnego do radiostacji rodziny PR4G*, ISŁ, WAT, Warszawa 2002.

*Artykuł recenzował: ppłk dr hab. inż. Dariusz SKORUPKA*