Gustaw Michalewski[1], Marek Witkowski[2]

Rola sieci i systemów teleinformatycznych w procesie podejmowania decyzji w sytuacjach kryzysowych

1. Wstęp

Sprawny obieg informacji na potrzeby funkcjonowanie organów odpowiedzialnych za bezpieczeństwo państwa w sytuacjach kryzysowych w dużej mierze zależy od odpowiednio dobranych systemów i sieci teleinformatycznych. Ważnym aspektem infrastruktury teleinformatycznej jest jej niezawodność w każdych warunkach, ze szczególnym uwzględnieniem sytuacji, kiedy nastąpi kryzys. W takiej sytuacji, która zagraża bezpieczeństwu, należy wypracować decyzje, w celu podjęcia takich działań, które przywrócą stan sprzed kryzysu. Podejmowanie decyzji w organizacjach zhierarchizowanych będących elementem systemu bezpieczeństwa narodowego ukierunkowane jest na osiągnięcie zgodnie z ich przeznaczeniem głównego dla nich celu, jakim jest utrzymanie określonego poziomu bezpieczeństwa państwa postrzeganego jako dobro wspólne wszystkich obywateli bez względu na ich przynależność społeczną, zawodową, religijną czy polityczną.

Autorzy artykułu za cel główny przyjęli przedstawienie zasadniczych problemów związanych z podejmowaniem decyzji w sytuacjach kryzysowych, która pozostaje w kompetencjach instytucji i organizacji odpowiedzialnych za system kierowania bezpieczeństwem państwa. Kolejnym celem było zaprezentowanie zagadnień dotyczących sieci i systemów teleinformatycznych, które mogą być wykorzystane do zapewnienia obiegu informacji, ze szczególnym uwzględnieniem sytuacji kryzysowych. Wskazano także pożądane kierunki modernizacji środków łączności i informatyki, które mogą przyczynić się do podniesienia poziomu niezawodności wymiany informacji pomiędzy elementami odpowiedzialnymi za bezpieczeństwo państwa.

[1] Wyższa Szkoła Oficerska Wojsk Lądowych imienia generała Tadeusza Kościuszki we Wrocławiu, Wydział Zarządzania.

[2] Wyższa Szkoła Oficerska Wojsk Lądowych imienia generała Tadeusza Kościuszki we Wrocławiu, Wydział Zarządzania.

2. Podejmowanie decyzji w sytuacjach kryzysowych

Podejmowanie decyzji, jako proces zmierzający do wyłonienia jednego z możliwych do zastosowania sposobu działania, odnosi się do różnorodności ogólnych warunków, w których ktoś się znajduje lub coś się dzieje, rozumianych jako sytuacja[3]. Owa odmienność sytuacji, oprócz ogólnej motywacji celowego działania osoby ludzkiej – jest przyczyną, dla której decydent podejmuje trud wyłonienia właściwej dla niej, dla różnych stanów, różnych elementów składających się na rzeczywistość, metody postępowania.

Jak zatem można wnioskować, podmiotem podejmującym decyzje w sytuacji kryzysowej będzie osoba odpowiedzialna za właściwe funkcjonowanie systemu lub układu, a przedmiotem podejmowania decyzji będzie sposób działania – zmierzający do przywrócenia jego uporządkowania i właściwej współpracy jego elementów, zapewniającej osiąganie celów, dla których został zorganizowany[4]. W odniesieniu więc do elementów systemu bezpieczeństwa państwa decyzje podejmować będą kierownicy poszczególnych komórek organizacyjnych w strukturze podsystemu kierowania na odpowiednim poziomie jej hierarchii w odniesieniu do elementów, działań, zakłóceń odpowiednio zapewniających lub uniemożliwiających zapewnienie porządnego stanu bezpieczeństwa w obszarach kompetencyjnie przewidzianych zgodnie z usytuowaniem w strukturze systemu.

3. Obieg informacji w procesie podejmowania decyzji

Postrzegając podejmowanie decyzji jako proces informacyjno-decyzyjny przetwarzający informacje na decyzje[5], nie trudno zauważyć, że jego skuteczność zależeć będzie od właściwego projektowania i funkcjonowania obiegu informacji pomiędzy podmiotami uczestniczącymi w jego realizacji. W organizacji zhierarchizowanej odpowiedzialnej za bezpieczeństwo państwa sposób zorganizowania przepływu informacji ukierunkowany będzie na poszerzenie świadomości sytuacyjnej w zakresie środowiska, w którym prowadzone są działania

[3] https://sjp.pwn.pl/sjp/sytuacja;2576918.html (dostęp: 21.04.2017).

[4] Por. T. Łagowski, *Wielokryterialne decyzje w przeobrażeniu zarządzania organizacjami w procesie globalizacji*, PJWSTK, Warszawa 2011, s. 78.

[5] J. Michniak, *Zarządzanie w sztabach wojskowych*, AON, Warszawa 2009, s. 80.

skoncentrowane na zapewnieniu bezpieczeństwa wewnętrznego i zewnętrznego państwa. Mając z kolei na uwadze wielokryterialny charakter podejmowanych decyzji, system obiegu informacji powinien uwzględniać zmienne i złożone środowisko budowania bezpieczeństwa, a także różnorodność funkcji, jakie spełniać mają organy kierowania bezpieczeństwem i elementy podsystemu wykonawczego.

Ponadto kompleksowe i dynamiczne środowisko podczas reagowania kryzysowego czy też na polu walki, dla zbudowania świadomości sytuacyjnej niezbędnej do racjonalnego podejmowania decyzji, wymaga zapewnienia po pierwsze, obrazu zbliżonego do rzeczywistego, po drugie, stworzenia współdzielonych baz danych. Wymogi te przyczyniły się do rozwoju koncepcji działań sieciocentrycznych postrzeganych przez teoretyków myśli wojskowej jednocześnie jako koncepcja i metoda prowadzenia działań[6]. Idea działania w środowisku sieciocentrycznym przekłada przewagę informacyjną na zdolność do działania przez wydajne połączenie dysponujących wiedzą różnego rodzaju narzędzi zaspokajania potrzeb informacyjnych w obszarze działania. Uzyskana w wyniku funkcjonowania środowiska sieciocentrycznego świadomość sytuacyjna prowadzi w ten sposób do synchronizacji działań ukierunkowanych na realizację zamiaru decydenta[7].

Dla spełnienia powyższych wymagań obieg informacji realizowany podczas procesu podejmowania decyzji skoncentrowany powinien być na maksymalnym wykorzystaniu wszystkich źródeł informacji. A ponieważ przedstawiony powyżej model podejmowania decyzji stosowany w organizacjach zhierarchizowanych obejmuje etap realizacji decyzji, wykorzystywany obieg informacji musi ponadto zapewnić dostęp do informacji wszystkim jego uczestnikom, również wykonawcom. Dlatego też przepływ informacji w organizacji odpowiedzialnej za zapewnienie bezpieczeństwa realizowany jest w układzie składającym się z następujących elementów: źródło informacji, narzędzia zaspokajania potrzeb informacyjnych, analityk, decydent, wykonawca. Dla zwiększenia poziomu użyteczności informacji pomiędzy wymienionymi elementami zachodzą sprzężenia zwrotne wynikające z konieczności zaspokajania różnorodnych potrzeb informacyjnych występujących zarówno w różnych podmiotach uczestniczących w procesie podejmowania decyzji (analityk, decydent, wykonawca), jak i w różnych fazach, etapach i czynnościach tego procesu.

---

[6] T. Szubrycht, *Sieciocentryczność – mity i rzeczywistość*, „Zeszyty Naukowe AMW" 2004, nr 4, s. 143–145.

[7] *Podstawy dowodzenia w aspekcie działań sieciocentrycznych*, J. Kręcikij, J. Wołejszo (red. nauk.), AON, Warszawa 2013, s. 10.

Przedstawione dotychczas informacje i opinie specjalistów teorii decyzji wskazują, iż umiejętności analityczne oceniania sytuacji kryzysowych i czynników wpływających na podejmowane działania jako reakcja na te sytuacje są podstawą procesu decyzyjnego[8]. Jak sugerują przykłady z historii, tej odległej i najbliższej współczesności, indywidulane predyspozycje decydentów nadal będą miały znaczący wpływ na jakość podejmowanych decyzji. Niemniej jednak – przy uwzględnieniu konieczności wykorzystania wielokryterialnych metod podejmowania decyzji przy rozwiązywaniu problemów w sytuacjach kryzysowych – doniosłe znaczenie ma również informacyjne zasilenie procesu decyzyjnego. Z kolei jego sprawną realizację można osiągnąć przez właściwe, a więc świadome uwarunkowań i ograniczeń, zidentyfikowanie potrzeb informacyjnych, a później ich planowe zaspokojenie[9].

Pierwotnie identyfikowane potrzeby informacyjne implikują wyznaczenie celu działania ukierunkowanego na zaspokojenie tej potrzeby[10]. Powstała potrzeba odzwierciedla sytuację decydenta, którego celem będzie rozwiązanie powstałej sytuacji przez podjęcie konkretnej decyzji.

Reasumując, istnieje bliska zależność pomiędzy potrzebami informacyjnymi, celami, do jakich zmierza organizacja, i podejmowaniem decyzji prowadzącym do osiągnięcia tych celów. Dokonując dogłębnej analizy tej zależności w aspekcie struktury procesu decyzyjnego w sytuacjach kryzysowych, realizowany obieg informacji będzie umożliwiał zaspokojenie trzech rodzajów potrzeb informacyjnych występujących podczas jego realizacji: opisujących problem decyzyjny, poszukujących sposobu rozwiązania problemu decyzyjnego oraz wspomagających decyzje wyboru wariantowanego sposobu przyszłego działania w sytuacji kryzysowej[11].

Projektując obieg informacji dla skutecznej realizacji procesu decyzyjnego organizacji zapewniającej bezpieczeństwo, należy pamiętać, że powinien on zapewniać jednolitą interpretację przesyłanych informacji. Jak zauważa T. Łagowski, podczas realizacji procesów decyzyjnych o charakterze wielokryterialnym zachodzi potrzeba częstego korzystania z wielu obszarów wiedzy w układzie równoległym, które posługują się różnym, nieprzystającym do siebie aparatem

---

[8] J. Kręcikij, *Działania sieciocentryczne. Wybrane problemy*, AON, Warszawa 2008, s. 52.

[9] G. Michalewski, *Potrzeby informacyjne w procesie podejmowania decyzji Polskiego Kontyngentu Wojskowego*, AON, Warszawa 2014, s. 133.

[10] P. Sienkiewicz, *Analiza systemowa. Podstawy i zastosowania*, Bellona, Warszawa 1994, s. 59.

[11] W. Flakiewicz, *Systemy informacyjne w zarządzaniu*, C.H. Beck, Warszawa 2002, s. 40.

pojęciowym[12]. Dlatego dla zapewnienia właściwej komunikacji opartej na jednakowym interpretowaniu informacji ustala się dziedzinową nomenklaturę, która zapewnia po pierwsze, rozumienie przekazywanych w obiegu informacji wiadomości, po drugie, ogranicza negatywny wpływ na przesyłanie informacji zakłóceń w funkcjonowaniu wykorzystywanych w podsystemie łączności środków technicznych[13]. Ponadto brak ujednoliconego aparatu pojęciowego może obniżać użyteczność informacji, co wynika z mniejszej możliwości, niż potencjalnie byłoby to możliwe do osiągnięcia przy wykorzystaniu informacji w procesie podejmowania decyzji.

W świetle przeprowadzonych rozważań oraz uwzględniając założenia teoretyczne i praktykę funkcjonowania organizacji zhierarchizowanych, można wywnioskować, że właściwie zaprojektowany i funkcjonujący system obiegu informacji w procesie podejmowania decyzji w sytuacjach kryzysowych powinien pozwalać na:

- monitorowanie sytuacji bezpieczeństwa;
- ostrzeganie (system alarmowania i ostrzegania);
- prognozowanie zagrożeń i rozwoju sytuacji;
- podejmowanie decyzji;
- opracowanie niezbędnych dokumentów (plany działania, rozkazu, dyrektywy);
- reagowanie na sytuacje kryzysowe (wypadki, siły szybkiego reagowania (QRF) itp.)
- podejmowanie działań (ratowniczych itp.);
- wprowadzanie korekt w działaniu (decyzjach);
- aktualizację i modyfikację planów;
- modyfikację procedur (system „Lessons Learned"[14]);
- bieżące zaspokajanie potrzeb materiałowych i zasobowych (logistyka), w celu utrzymywania żywotności i gotowości elementów wykonawczych systemu bezpieczeństwa do działania.

[12] T. Łagowski, *Wielokryterialne decyzje w przeobrażeniu zarządzania organizacjami w procesie globalizacji*, PJWSTK, Warszawa 2011, s. 52.

[13] Między innymi w tym celu w SZ RP stosuje się przepisy korespondencji radiowej.

[14] Systemy zbierania i wykorzystania doświadczeń funkcjonujące w większości sił zbrojnych członków NATO.

4. Wykorzystanie sieci i systemów teleinformatycznych na potrzeby wypracowania i podjęcia decyzji

Sytuacje kryzysowe, które miały miejsce na terenie naszego kraju w ciągu ostatnich lat, ujawniły, że sieci i systemy teleinformatyczne zaimplementowane na poszczególnych szczeblach systemu kierowania bezpieczeństwem państwa oraz w elementach współuczestniczących w niesieniu pomocy w sytuacjach zagrożenia nie zapewniły właściwego poziomu wymiany informacji pomiędzy elementami odpowiedzialnymi za bezpieczeństwo państwa oraz jego obywateli[15].

Taka sytuacja przyczyniała się do:

- opóźnienia przekazania informacji o zaistniałych zagrożeniach;
- spowolnienia podjęcia adekwatnych do zaistniałej sytuacji działań, w celu zminimalizowania strat;
- nieadekwatnego do sytuacji wykorzystania posiadanych sił i środków;
- nieskoordynowanych działań służb, straży oraz innych instytucji, które brały udział w akcjach ratowniczych.

Ponadto przestarzałe i niekompatybilne środki łączności stosowane do przekazywania informacji okazały się zawodne i nie zapewniały sprawnego funkcjonowania elementów odpowiedzialnych za przywrócenie bezpieczeństwa w sytuacjach zagrożenia życia i zdrowia poszkodowanej ludności. Niedomagania w ciągłości zarządzania mogą spowodować podjęcie nieodpowiedniej do zaistniałej sytuacji decyzji. Idąc dalej, brak informacji o aktualnej sytuacji może powodować opóźnienia w podjęciu reakcji na powstałe zagrożenia, a w konsekwencji doprowadzić do wzrostu niebezpieczeństw.

Sprawne środki łączności i informatyki będą znacząco wpływały na sprawną wymianę informacji pomiędzy elementami bezpośrednio odpowiedzialnymi za zapewnienie bezpieczeństwa państwa, jak również z elementami współuczestniczącymi w zapewnieniu sprawnego funkcjonowania państwa w sytuacjach kryzysowych.

Do sprawnego funkcjonowania elementów kierowania bezpieczeństwem narodowym oraz do przechowywania, przetwarzania i wymiany informacji pomiędzy instytucjami, organami administracji publicznej, służbami oraz strażami niezbędne są sieci i systemy teleinformatyczne.

---

[15] Zob. M. Witkowski, *Systemy teleinformatyczne w zarządzaniu kryzysowym*, WSOWL, Wrocław 2014.

Od sieci i systemów teleinformatycznych (rysunek 1), wykorzystywanych na potrzeby zapewnienia bezpieczeństwa państwa, a także przywrócenia poziomu bezpieczeństwa do stanu sprzed kryzysu, oczekuje się ciągłości wymiany informacji.

Rysunek 1. Sieci i systemy teleinformatyczne wykorzystywane na potrzeby systemu kierowania bezpieczeństwem państwa

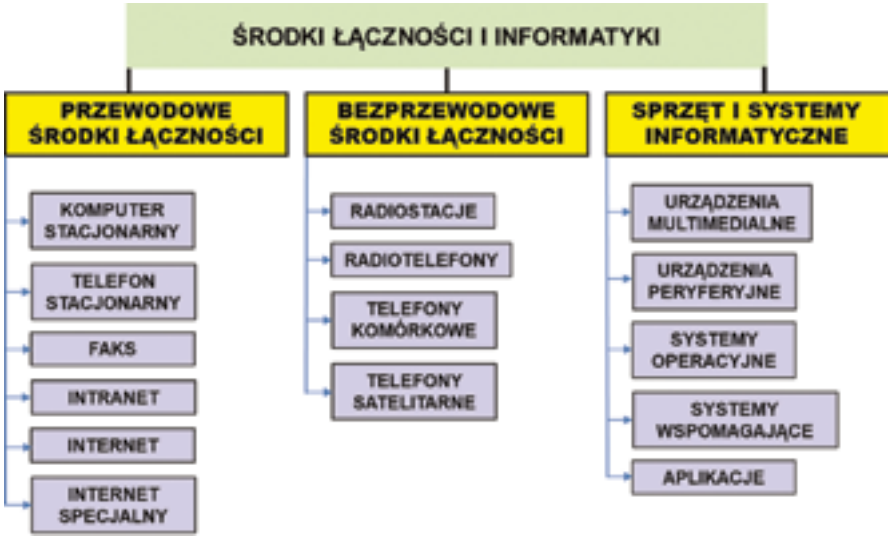
Źródło: opracowanie własne.

Dlatego ich niezawodne funkcjonowanie na każdym poziomie struktur odpowiedzialnych za bezpieczeństwo państwa pozwoli na nieprzerwany dostęp do aktualnych danych przez zaimplementowane w nich środki łączności i informatyki, co przyczyni się do kompleksowej analizy zaistniałej sytuacji kryzysowej, następnie na podstawie przeprowadzonych procesów decyzyjnych umożliwi podjęcie odpowiednich do sytuacji działań.

Dla lepszego zobrazowania środków teleinformatycznych oraz mediów transmisyjnych, które wykorzystuje się w elementach odpowiedzialnych za bezpieczeństwo państwa, przedstawiono ich autorski podział na rysunku 2.

Przedstawiony na rysunku 2 podział środków łączności i informatyki składa się zasadniczo z trzech grup.

Do pierwszej grupy możemy zaliczyć przewodowe środki łączności, takie jak: komputer stacjonarny, telefon stacjonarny, faks, które funkcjonują głównie opierając się na infrastrukturze stacjonarnej operatorów publicznych oraz resortowych (MON, MSWiA, PKP).



Rysunek 2. Podział środków łączności i informatyki

Źródło: opracowanie własne.

Wymieniona infrastruktura telekomunikacyjna zapewnia dostęp do:

- sieci internetowej, w wymiarze lokalnym (Intranet);
- sieci internetowej, w wymiarze globalnym (Internet);
- sieci internetowej specjalnej (OPAL, MILNET-Z, MILNET-I, SEC-WAN, INTER-MON);
- publicznej sieci telekomunikacyjnej (wykorzystywana głównie na potrzeby telefonii stacjonarnej oraz do przesyłania faksów);
- resortowej sieci przewodowej (do przesyłania jawnej i niejawnej korespondencji).

Do tej grupy urządzeń można zaliczyć także centrale telefoniczne, których obecne możliwości nie skupiają się jedynie na usługach głosowych, ale stanowią podstawę do zbudowania rozległego systemu wymiany informacji.

W wyniku zastosowania nowoczesnej technologii możliwe stało się usprawnienie pracy jej użytkowników oraz znacznie przyczyniło się do skrócenia czasu przekazywania wiadomości. Dużym udogodnieniem jest zastosowanie cyfrowych central telefonicznych, które mają możliwość przesyłania informacji o numerze telefonu, z którego następuje przekazanie informacji. Dzięki tej funkcji w łatwy sposób można zweryfikować dzwoniącego i upewnić się, czy dane przekazywane są prawdziwe i pochodzą z zaufanego źródła (od uprawnionej osoby). Ponadto kolejną zaletą tej technologii jest to, że wszelkie zgłoszenia są automatycznie nagrywane i można je ponownie odsłuchać w razie jakichkolwiek wątpliwości.

Dodatkowo, dzięki połączeniu cyfrowych aplikacji do tego rodzaju central, istnieje możliwość zestawiania połączeń bezpośrednio z komputera do aplikacji wspomagających podejmowanie decyzji bez potrzeby używania dodatkowych urządzeń łączności.

Użycie przewodowych środków łączności, w połączeniu z systemami informatycznymi oraz kompatybilnymi protokołami wymiany danych, umożliwiło przygotowanie narzędzi, które wspomagają procesy decyzyjne na poszczególnych szczeblach systemu zarządzania kryzysowego oraz na potrzeby elementów współpracujących z organami odpowiedzialnymi za bezpieczeństwo państwa i jego obywateli w czasie kryzysu.

Na potrzeby wymiany informacji w elementach zarządzania kryzysowego należy także wykorzystać drugą grupę środków łączności. Ta grupa środków i urządzeń bezprzewodowych może zapewnić sprawną wymianę informacji, niezależną od infrastruktury stacjonarnej. Możliwe jest to dlatego, że łączność bezprzewodowa opiera się przede wszystkim na urządzeniach, które do przesyłania informacji wykorzystują fale radiowe.

W skład grupy środków bezprzewodowych wchodzą przede wszystkim:
- radiostacje,
- radiotelefony,
- telefony komórkowe,
- telefony satelitarne[16].

Wymienione środki łączności wraz z niezbędną infrastrukturą telekomunikacyjną w postaci: satelitów telekomunikacyjnych, stacji bazowych łączności komórkowej oraz przemienników radiowych, mogą zostać wykorzystane do utworzenia bezprzewodowej, wielostrefowej i rozległej sieci telekomunikacyjnej. Ta grupa współpracujących ze sobą urządzeń łączności będzie odgrywać szczególną rolę w sytuacjach, kiedy stacjonarna (przewodowa) infrastruktura ulegnie awarii lub zostanie zniszczona.

Dodatkowym atutem nowoczesnej łączności bezprzewodowej jest to, że przesyłanie informacji drogą radiową jest zabezpieczone przed nieuprawnionym dostępem. Taka niejawna transmisja jest możliwa chociażby przez szyfrowanie interfejsu radiowego oraz autoryzację stacji ruchomych, co znacznie zwiększa poziom bezpieczeństwa przesyłanych informacji.

---

[16] M. Witkowski, *Systemy teleinformatyczne wspomagające zarządzanie kryzysowe*, w: *Metodologia badań bezpieczeństwa narodowego: Bezpieczeństwo 2010,* P. Sienkiewicz (red. nauk.), AON, Warszawa 2011. W publikacji tej przedstawiono przykłady zastosowania środków łączności na potrzeby zarządzania kryzysowego.

Nowoczesne środki bezprzewodowe oferują organom odpowiedzialnym za bezpieczeństwo w czasie sytuacji kryzysowych całościowe rozwiązania teleinformatyczne, które wspomagają wypracowanie decyzji w każdej fazie i etapie zarządzania kryzysowego.

Trzecia grupa środków składa się ze środków informatycznych w postaci urządzeń multimedialnych, osprzętu komputerowego wraz z dedykowanym oprogramowaniem (np. systemy operacyjne, systemy wspomagające, zbiory bazodanowe, aplikacje) wraz z urządzeniami peryferyjnymi, takimi jak plotery, drukarki, skanery itp.

Podstawowym zadaniem środków i systemów informatycznych jest wspomagania elementów zarządzania kryzysowego na każdym poziomie. Głównie na potrzeby centrów, organów i zespołów zarządzania kryzysowego do gromadzenia i analizy danych, zarządzania bazą sił i środków oraz na potrzeby kierowania, koordynacji działań czy wypracowania i podjęcia decyzji. Wymienione urządzenia i systemy informatyczne wykorzystuje się także na potrzeby służb dyżurnych, przy obsłudze zgłoszeń i zdarzeń, podczas koordynacji działań ratowniczych oraz w czasie sporządzaniu dokumentacji z przeprowadzonych akcji.

Nowoczesne środki łączności i informatyki, w połączeniu z infrastrukturą telekomunikacyjną, mogą przyczynić się do sprawniejszego obiegu informacji pomiędzy elementami odpowiedzialnymi za bezpieczeństwo państwa.

Na potrzeby koordynacji działań oraz wymiany informacji należy wykorzystać takie urządzenia łączności i informatyki (określane także mianem środków teleinformatycznych) oraz media transmisyjne, które sprostają stawianym im wymaganiom. Powinny być to takie środki telekomunikacyjne i media transmisyjne, które będą się charakteryzować dużą odpornością na awarie, zakłócenia oraz ataki (celowe i niecelowe) na infrastrukturę krytyczną państwa. Tylko dobrze wyselekcjonowane urządzenia i systemy teleinformatyczne zapewnią właściwy dostęp do informacji, która jest niezbędna do wypracowania wariantów działania i podjęcie najbardziej adekwatnej do zaistniałej sytuacji decyzji.

5. Kierunki modernizacji środków łączności i informatyki

Uwzględniając problem podejmowania decyzji w sytuacjach kryzysowych, celem modernizacji środków wykorzystywanych do zapewnienia odpowiedniego obiegu informacji w tym łączności i informatyki jest usprawnienie procesów

informacyjnych, a w konsekwencji zapewnienie warunków do podejmowania efektywnych decyzji.

Zidentyfikowane kierunki modernizacji związane są z wymaganiami, jakie spowodowane są kompleksowym środowiskiem prowadzenia działań w sytuacjach kryzysowych, nowymi technologiami, prognozą zagrożenia, poziomem zarządzania, potrzebami zapewnienia bezpieczeństwa w nowo zidentyfikowanych obszarach. Dlatego autorzy publikacji przedstawili modelowe wykorzystanie środków, sieci i systemów teleinformatycznych do sprawnego obiegu informacji i podjęcia decyzji w sytuacjach kryzysowych, które zostało zaprezentowane w tabeli 1.

Tabela 1. Modelowe wykorzystanie środków, sieci i systemów teleinformatycznych do wymiany informacji w sytuacjach kryzysowych

Środki, sieci i systemy teleinformatyczne wykorzystywane do wymiany informacji w sytuacjach kryzysowych	
Przewodowe środki łączności	– telefony stacjonarne – na potrzeby zapewnienia łączności z organem nadrzędnym, podrzędnym, sąsiednimi i elementami współdziałającymi; – urządzenia faksujące (faks, faks-serwer) – na potrzeby przesyłania informacji do struktur nadrzędnych, podrzędnym, sąsiednich, jednostek współpracujących, służb oraz straży.
Bezprzewodowe środki łączności	– telefony komórkowe – dla osób funkcyjnych; – telefony satelitarne – do zapewnienia łączności z elementami nadrzędnymi, sąsiednimi oraz współdziałającymi, szczególnie wtedy, kiedy użycie innych środków łączności jest niemożliwe; – radiostacje średniej oraz małej mocy – w paśmie KF/UKF przewidzianym do użycia na potrzeby bezpieczeństwa państwa (w tym ZK); – radiotelefony cyfrowe (stacjonarne i przenośne) – dla osób funkcyjnych oraz organów współuczestniczących; – urządzenia do budowy bezprzewodowych sieci komputerowych (np. technologia LTE, Wi-Fi) – do zapewnienia łączności w sieciach LAN oraz WAN.
Środki informatyczne i urządzenia końcowe (peryferyjne)	– komputery stacjonarne; – komputery przenośne (laptopy, desktopy, palmtopy, tablety); – smartfony; – drukarki; – plotery; – skanery; – rzutniki multimedialne.

Środki, sieci i systemy teleinformatyczne wykorzystywane do wymiany informacji w sytuacjach kryzysowych	
Sieci telekomunikacyjne (media transmisyjne)	– urządzenia teletransmisyjne do budowy sieci przewodowej i bezprzewodowej; – urządzenia komutacyjne (zwielokrotniające); – urządzenia do budowy przewodowych sieci komputerowych (np. modemy) – do utrzymania łączności w sieciach lokalnych (LAN) oraz rozległych (WAN); – skrętki kablowe; – kable metalowe; – przewody optyczne (światłowodowe); – przewody teleinformatyczne.
Systemy informatyczne	– systemy operacyjne; – programy do wymiany informacji za pośrednictwem sieci Internet; – aplikacje, symulatory oraz inne systemy monitorowania zagrożeń dostępne za pośrednictwem sieci internetowych (LAN, WAN); – systemy do pobierania, gromadzenia, przetwarzania oraz archiwizowania informacji; – systemy do gromadzenia, przeprowadzania analiz oraz udostępniania danych mapowych; – aplikacje cyfrowe do prowadzenia baz danych, analiz oraz symulacji zjawisk hydrologiczno-meteorologicznych; – systemy do uruchamiania sygnałów alarmowych (syren); – systemy do przekazywania informacji tekstowych o zagrożeniach (poczta elektroniczna, SMS, CB-SMS) z wykorzystaniem łączy internetowych oraz sieci telefonii komórkowej.

Źródło: opracowanie własne.

6. Podsumowanie i kierunki dalszych badań

Analiza literatury i wieloletnia obserwacja autorów środowiska bezpieczeństwa wskazują na potrzebę ciągłego doskonalenia systemów teleinformatycznych zarówno pod kątem zwiększania efektywności procesów informacyjnych w kontekście podejmowania decyzji, jak i bezpieczeństwa teleinformatycznego.

Systemy łączności i informatyki oraz infrastruktura telekomunikacyjna, która ma zapewnić sprawne funkcjonowanie państwa, a szczególnie w sytuacjach kryzysowych, powinna składać się z nowoczesnych rozwiązań technologicznych. Tego typu rozwiązania zapewnią najwyższy z możliwych do osiągnięcia poziom niezawodności i bezpieczeństwa obiegu informacji pomiędzy elementami odpowiedzialnymi za funkcjonowanie państwa. Oczywiście jak na razie żadna

technologia nie gwarantuje stuprocentowej pewności, że sprosta stawianym jej wymaganiom, należy jednak dobierać takie środki, media transmisyjne i systemy teleinformatyczne, które zapewnią sprawną wymianę danych w każdych warunkach. Autorzy publikacji zdają sobie sprawę, że aby taką infrastrukturę teleinformatyczną zbudować, potrzeba czasu i znacznych nakładów finansowych, dlatego należy utrzymywać posiadane środki komunikacji w ciągłej sprawności technicznej. Niemniej jednak należy dążyć do tego, aby w miarę możliwości, zmodernizować aktualnie eksploatowane urządzenia łączności i sukcesywnie dokonywać wymiany analogowych środków łączności na cyfrowe urządzenia teleinformatyczne.

Bibliografia

Flakiewicz W., *Systemy informacyjne w zarządzaniu*, C.H. Beck, Warszawa 2002, s. 40.

Kręcikij J., *Działania sieciocentryczne. Wybrane problemy*, AON, Warszawa 2008, s. 52.

Łagowski T., *Wielokryterialne decyzje w przeobrażeniu zarządzania organizacjami w procesie globalizacji*, PJWSTK, Warszawa 2011, s. 52 i 78.

Michalewski G., *Potrzeby informacyjne w procesie podejmowania decyzji Polskiego Kontyngentu Wojskowego*, AON, Warszawa 2014, s. 133.

Michniak J., *Zarządzanie w sztabach wojskowych*, AON, Warszawa 2009, s. 80.

Podstawy dowodzenia w aspekcie działań sieciocentrycznych, J. Kręcikij, J. Wołejszo (red. nauk.), AON, Warszawa 2013, s. 10.

Sienkiewicz P., *Analiza systemowa. Podstawy i zastosowania*, Bellona, Warszawa 1994, s. 59.

Szubrycht T., *Sieciocentryczność – mity i rzeczywistość*, „Zeszyty Naukowe AMW" 2004, nr 4, s. 143–145.

Witkowski M., *Systemy teleinformatyczne wspomagające zarządzanie kryzysowe*, w: *Metodologia badań bezpieczeństwa narodowego: Bezpieczeństwo 2010*, P. Sienkiewicz (red. nauk.), AON, Warszawa 2011.

Witkowski M., *Systemy teleinformatyczne w zarządzaniu kryzysowym*, WSOWL, Wrocław 2014.

Źródła sieciowe

https://sjp.pwn.pl/sjp/sytuacja;2576918.html (dostęp: 21.04.2017).

* * *

Role of Networks and ICT Systems in Decision-Making in Crisis Situations

Summary

In the article there is presented Information and Communication Technology used in Crisis Management Centers, which can facilitate the exchange of information for decision making. The authors describe the impact of networks and information systems on the efficiency, security and continuity of the information flow for the purpose of developing and making decisions in emergency situations. The paper has also indicated the direction of the modernization of communication and particular IT tools have also been proposed, which can contribute to improving the reliability of the exchange of information between elements responsible for national security.

Keywords: ICT (Information and Communication Technology), crisis management, decision making, national security.