dr inż. Michał GAWROŃSKI

SYSTEMY TELEINFORMATYCZNE WSPOMAGANIA KIEROWANIA SYSTEMEM BEZPIECZEŃSTWA NARODOWEGO

Słowa kluczowe: bezpieczeństwo narodowe, kierowanie, zarządzanie kryzysowe, system kierowania, system łączności rządowej.

STRESZCZENIE

Artykuł podejmuje problematykę wspomagania procesu kierowania bezpieczeństwem narodowym przez specjalizowane narzędzia teleinformatyczne. W treści artykułu zawarto analizę systemów branżowych, ich możliwość oraz potencjalne wykorzystanie w Systemie Kierowania Systemem Bezpieczeństwa Narodowego (SK SBN). Zawarto również postulat podjęcia problemu opracowania ogólnokrajowego systemu teleinformatycznego na potrzeby kierowania. Różnorodność aktualnie używanych systemów teleinformatycznych oraz telekomunikacyjnych nie spełnia postulatu kompleksowości oraz systemowości. Autor zwraca również uwagę na konieczność uregulowań prawnych w zakresie koordynacji działań systemu kierowania SBN i kierowania systemem zarządzania kryzysowego. Postuluje również włączenie zarządzania kryzysowego do takiego systemu.

Wstęp

Rozwój technologiczny w dziedzinie technologii informacyjnych przekłada się na potrzebę zmian w poszczególnych działach. Jednym z nich są systemy telekomunikacyjne, które do tej pory były nerwem spinającym działania poszczególnych organizacji. W przypadku organizacji, jaką jest państwo, nabierają szczególnego znaczenia. Kierowanie państwem oraz jego bezpieczeństwem wymaga niezawodnych i bezpiecznych systemów komunikacji. W dobie powszechnej informatyzacji nie ma alternatywy dla nowoczesnych systemów teleinformatycznych, łączących jednostki organizacyjne administracji, w jeden spójny organizm. Jednym z obszarów

najbardziej wrażliwych na potrzeby komunikacyjne jest kierowanie bezpieczeństwem narodowym. Pomimo wprowadzenia aktów prawnych, tworzących system kierowania bezpieczeństwem, brak jest narzędzi do wspomagania podejmowania decyzji przez właściwe osoby. Zdaniem autora, można postawić hipotezy, wynikające z aktualnego stanu systemu kierowania bezpieczeństwem narodowym.

Hipoteza 1: Aktualnie eksploatowane systemy teleinformatyczne wspomagające zarządzanie bezpieczeństwem narodowym nie tworzą kompleksowego i spójnego systemu łączności, co może prowadzić do problemów z przepływem informacji i danych między poszczególnymi organami oraz ich stanowiskami kierowania.

Hipoteza 2: Współczesne wyzwania, przed jakimi stają systemy łączności administracji publicznej, wymagają opracowanie nowoczesnego i kompleksowego systemu łączności, zapewniającego bezpieczeństwo przetwarzanym danym oraz integrującego usługi niezbędne dla sprawnego kierowania państwem.

Dla potwierdzenia postawionych tez, autor przedstawił aktualny stan systemów teleinformatycznych i teletransmisyjnych, jakie są eksploatowane w Polsce. Prezentuje spojrzenie ukierunkowane na rolę systemów teleinformatycznych wykorzystywanych do realizacji funkcji kierowniczych i zarządczych, jak również na bezpieczeństwo przetwarzanych danych i podejmowanych decyzji.

Dokonał również analizy ich możliwości i zadań ogólnych. Przedstawił również problematy związane z brakiem uregulowań prawnych w pewnych obszarach systemu kierowania bezpieczeństwem. W podsumowaniu zawarte zostały perspektywy kierunków, w jakich powinny pójść zmiany, które mogą zapewnić usprawnienie kierowania i zarządzania oraz zapewnienia bezpieczeństwa przetwarzanych danych wykorzystywanych w tym procesie.

Pojęcie bezpieczeństwa narodowego i systemu kierowania

Pojęcie bezpieczeństwa narodowego jest szeroko prezentowane w literaturze przedmiotu. Prezentowanych jest również wiele definicji bezpieczeństwa, w odniesieniu do poszczególnych dziedzin, jak również podmiotów. Dla problematyki omawianej w niniejszym artykule przyjęto definicję zawartą w Słowniku terminów z zakresu bezpieczeństwa narodowego.

Bezpieczeństwo narodowe to stan uzyskany w wyniku odpowiednio zorganizowanej obrony i ochrony przed zagrożeniami zewnętrznymi i wewnętrznymi określony stosunkiem potencjału obronnego do skali zagrożeń[1]. Bezpieczeństwo narodowe

[1] *Słownik terminów z zakresu bezpieczeństwa narodowego*, Akademia Obrony Narodowej, Warszawa 2009, wydanie czwarte, s. 16.

rozpatrywane jest systemowo, tzn. jako wyodrębniony z otaczającej rzeczywistości obiekt, tworzący zbiór elementów oraz zidentyfikowanych relacji między nimi[2]. Zatem **system bezpieczeństwa narodowego** to całość sił, środków oraz zasobów przeznaczonych przez państwo do realizacji zadań w dziedzinie bezpieczeństwa, odpowiednio do tych zadań zorganizowana, utrzymana i przygotowana, w którym wyróżnia się podsystem kierowania i szereg podsystemów wykonawczych[3].

System Bezpieczeństwa Narodowego (SBN) składa się z organów i instytucji, odpowiedzialnych za bezpieczeństwo narodowe (BN). Zgodnie z zapisem zawartym w Strategii Bezpieczeństwa Narodowego system BN tworzą wszystkie odpowiedzialne za bezpieczeństwo w świetle Konstytucji RP i właściwych ustaw organy oraz instytucje należące do władz ustawodawczej, wykonawczej i sądowniczej, w tym Sejm i Senat, Prezydent RP, Prezes Rady Ministrów, Rada Ministrów, centralne organy administracji rządowej oraz inne państwowe urzędy centralne i instytucje państwowe. W skład systemu wchodzą również siły zbrojne oraz służby i instytucje rządowe, zobowiązane do zapobiegania i przeciwdziałania zagrożeniom zewnętrznym, zapewnienia bezpieczeństwa publicznego, prowadzenia działań ratowniczych oraz ochrony ludności i mienia w sytuacjach nadzwyczajnych, a także władze samorządowe oraz inne podmioty prawne, w tym przedsiębiorcy tworzący przemysłowy potencjał obronny oraz realizujący zadania z zakresu obronności państwa[4]. W prawodawstwie polskim brak jest uregulowań systemu bezpieczeństwa, co powoduje, że nie jest samodzielnie funkcjonującą strukturą państwową[5].

Wraz z uchwaleniem ustawy o zarządzaniu kryzysowym do SBN włączono również ten obszar[6]. Ustawa o zarządzaniu kryzysowym określa zasady działania organów administracji w sytuacjach kryzysowych oraz ich zadania. Artykuł 2 ustawy definiuje zarządzanie kryzysowe jako […] *działalność organów administracji publicznej będąca elementem kierowania bezpieczeństwem narodowym* […], bezpośrednio włączając je w obszar kierowania bezpieczeństwem narodowym.

System bezpieczeństwa narodowego składa się z dwóch podsystemów:

- Podsystem kierowania – który tworzą organy władzy publicznej i kierownicy jednostek organizacyjnych, które wykonują zadania związane z bezpie-

---

[2] P. Sienkiewicz, *Analiza systemowa i podstawy jej zastosowania*, Wydawnictwo Bellona, Warszawa 1994, s. 16.

[3] *Strategia Rozwoju Systemu Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej 2022*, przyjęta uchwałą Rady Ministrów z dnia 9 kwietnia 2013 r., s. 3.

[4] Na podstawie *Strategii Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej* z 13 listopada 2007 r., s. 21.

[5] *Strategia Rozwoju Systemu Bezpieczeństwa*…, dz. cyt., s. 14.

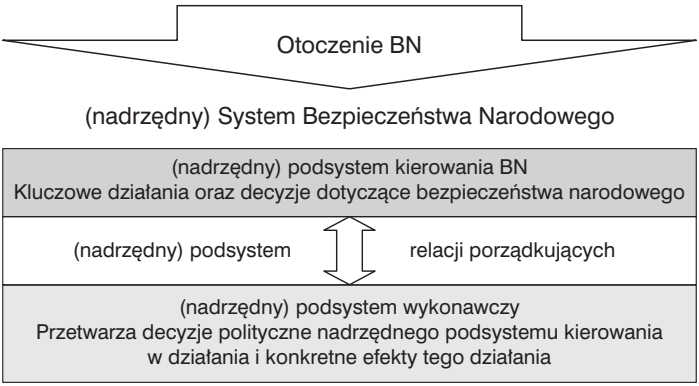
[6] Tamże, s. 18.

czeństwem narodowym oraz organy dowodzenia Sił Zbrojnych RP wraz z Naczelnym Dowódcą SZ (z chwilą jego mianowania).

- Podsystemy wykonawcze – tworzą siły i środki pozostające we właściwościach ministrów kierujących działami administracji rządowej, centralnych organów administracji rządowej, wojewodów, organów samorządu terytorialnego oraz innych instytucji państwowych i podmiotów odpowiedzialnych.

Struktury podsystemów definiowane są przez relacje porządkujące między wymienionymi elementami.

Miejsce podsystemu kierowania w systemie bezpieczeństwa narodowego zaznaczone zostało na poniższym schemacie.



Źródło: Na podstawie: W. Kitler, *Bezpieczeństwo narodowe RP. Podstawowe kategorie. Uwarunkowania. System*, AON, Warszawa 2011, s. 314.

Rys. 1. Elementy Systemu Bezpieczeństwa Narodowego.

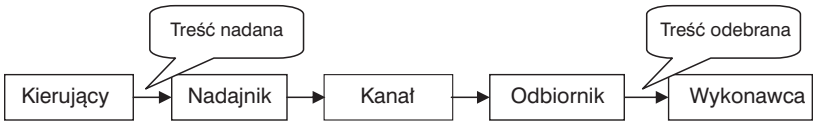
Podsystem kierowania jest elementem większego systemu, którym jest system BN. Jednak z racji jego wagi oraz rozmiaru można go traktować jako system składowy SBN.

Rozpatrując kierowanie bezpieczeństwem należy przywołać podstawowe definicje, które ukierunkują spojrzenie na aspekt wspomagania procesami kierowania i zarządzania. **Kierowanie** – działanie zmierzające do skoordynowanego wykorzystania będących w dyspozycji organu kierowniczego zasobów ludzkich i materialnych dla osiągnięcia założonych celów[7]. Kierowanie jest to zatem oddziaływanie obiektu (organu) kierującego, (wydającego rozkazy, polecenia) na drugi obiekt

[7] *Słownik terminów z zakresu…*, dz. cyt., s. 55

(obiekty), celem wywołania ich działania zgodnie z intencją obiektu kierującego. Kierowanie odbywa się zgodnie z ustaloną hierarchią w danej organizacji, wyrażoną relacjami porządkującymi między poszczególnymi poziomami organizacyjnymi.

Kierowanie jest nieodłącznie związane z przekazywaniem przez kierującego poleceń skierowanych do ich wykonawców. Kierowanie jest więc procesem, wymagającym co najmniej dwóch uczestników, nadajnika i odbiornika, kanału komunikacyjnego oraz treści. Przykładowy schemat procesu komunikacji przedstawiony jest na rys. 2.



Źródło: Opracowanie własne na podstawie: P. Sienkiewicz, *Inżynieria systemów*, Wydawnictwo MON, Warszawa 1983, s. 89.

Rys. 2. Schemat komunikacji.

Z pojęciem kierowania związane jest również pojęcie zarządzania. **Zarządzanie** – to zespół działań lub procesów mających na celu koordynację i integrację użytkowania zasobów dla osiągnięcia celu organizacyjnego przez ludzi, przy użyciu techniki i informacji w zorganizowanych strukturach[8]. Zarządzanie jest więc ciągiem działań, zmierzających do osiągnięcia założonego celu, wykorzystującym zasoby organizacji (siły i środki). Wymaga odpowiednich środków technicznych wspomagających te działania, w celu uzyskania jak najlepszych efektów. Jednym z warunków właściwego zarządzania jest wewnętrzne komunikowanie się, zapewniające przepływ informacji o realizacji i przebiegu procesów zarządzania.

W potocznym rozumieniu zarządzanie i kierowanie są często utożsamiane. Rozpatrując kierowanie i zarządzanie w odniesieniu do bezpieczeństwa narodowego należy je jednak rozróżnić. Proces zarządzania składa się z czterech części składowych: organizowanie, planowanie, kontrolowanie i aktywowanie. Są one ze sobą ściśle powiązane, jednak ze względu na ich złożoność w rozpatrywanym obszarze, mogą być postrzegane jako oddzielne procesy, również składające się z szeregu procesów składowych. Kierowanie zaś rozpatrywane jest bardziej w kontekście przewodzenia innym organom i ludziom, zaangażowanym w realizację określonego celu.

Wraz z uchwaleniem ustawy o zarządzaniu kryzysowym kierowanie bezpieczeństwem narodowym zyskało charakter interdyscyplinarny, obejmujący regulo-

[8] Tamże, s. 165

wane odrębnymi przepisami **zarządzanie kryzysowe** oraz **kierowanie obronnością państwa**. Niestety, brak jest jednak regulacji ustawowych, które łączyłyby działania podejmowane w obu wymienionych dziedzinach bezpieczeństwa narodowego, w jeden spójny system kierowania bezpieczeństwem narodowym[9]. Jakkolwiek System Kierowania Bezpieczeństwem Narodowym zdefiniowany został w Rozporządzeniu Rady Ministrów *w sprawie przygotowania systemu kierowania bezpieczeństwem narodowym*[10], to ranga tego aktu prawnego nie pozwala na stworzenie jednolitego i spójnego kompetencyjnie i decyzyjnie systemu. Konieczność uchwalenia aktu prawnego o randze ustawy zasygnalizowana została w Strategii Rozwoju SBN[11]. Rozporządzenie to nie zawiera również unormowania prawnego w zakresie włączenia systemu kierowania ZK w SK BN.

Dla zapewnienia funkcjonowania systemu kierowania BN organizuje się system stanowisk kierowania[12]. Zasady organizacji stanowisk kierowania reguluje rozporządzenie *w sprawie przygotowania systemu kierowania bezpieczeństwem narodowym*. Określa ono:

- organizację i tryb przygotowania systemu kierowania bezpieczeństwem narodowym, w tym obroną państwa, zwanego dalej „systemem kierowania";
- warunki funkcjonowania organów władzy publicznej na stanowiskach kierowania.

Zgodnie z § 8 Rozporządzenia system kierowania składa się ze stanowisk głównych oraz stanowisk zapasowych. Główne stanowiska kierowania przygotowuje się dla:

- Prezydenta Rzeczypospolitej Polskiej;
- Prezesa Rady Ministrów;
- ministrów, centralnych organów administracji rządowej oraz wojewodów;
- kierowników urzędów centralnych niewchodzących w skład administracji rządowej;
- kierowników zespolonych służb, inspekcji i straży działających pod zwierzchnictwem wojewody oraz organów administracji niezespolonej, ustalonych przez ministrów i wojewodów stosownie do kompetencji;
- organów wykonawczych samorządu terytorialnego.

---

[9] *Strategia Rozwoju Systemu Bezpieczeństwa*…, dz. cyt., s. 19–20.

[10] Rozporządzenie Rady Ministrów z dnia 27 kwietnia 2004 r. *w sprawie przygotowania systemu kierowania bezpieczeństwem narodowym* (Dz. U. z 2004 r., Nr 98, poz. 978).

[11] *Strategia Rozwoju Systemu Bezpieczeństwa*…, dz. cyt., s. 20.

[12] W. Kitler, *Bezpieczeństwo narodowe RP…*, dz. cyt., s. 338.

Zapasowe stanowiska kierowania przygotowuje się dla:
- Prezydenta Rzeczypospolitej Polskiej;
- Prezesa Rady Ministrów;
- ministrów i centralnych organów administracji rządowej, wskazanych przez Prezesa Rady Ministrów;
- wojewodów.

Wśród stanowisk kierowania wyróżnione zostało Centralne Stanowisko Kierowania Obroną Państwa (CSKOP)[13], w skład którego wchodzą:
- Stanowiska Kierowania Prezydenta RP;
- Stanowisko Kierowania Prezesa RM;
- Stanowiska ministrów i centralnych organów administracji rządowej, wskazanych przez Prezesa RM.

Główne stanowiska kierowania mogą być organizowane w siedzibach organów lub w lokalizacjach zapasowych. Organami odpowiedzialnymi za organizację są (w zależności od stanowiska kierowania)[14]:
- Minister właściwy do spraw wewnętrznych – dla stanowisk Prezydenta i Prezesa RM.
- Właściwe organy dla stanowisk ministrów, centralnych organów administracji rządowej oraz wojewodów, kierowników urzędów centralnych niewchodzących w skład administracji rządowej, kierowników zespolonych służb, inspekcji i straży działających pod zwierzchnictwem wojewody oraz organów administracji niezespolonej, ustalonych przez ministrów i wojewodów stosownie do kompetencji, organów wykonawczych samorządu terytorialnego.

W przypadku zapasowych stanowisk kierowania, lokalizacja jest uzgadniana przez organizatorów z ministrem właściwym do spraw wewnętrznych, obrony narodowej lub wojewodą, w zależności od szczebla administracji, który organizuje stanowisko. Na poziomie wojewódzkim wojewoda zapewnia marszałkowi województwa lub powołanemu komisarzowi, zapasowe stanowisko kierowania[15].

W ramach procesu organizacji stanowisk kierowania opracowuje się między innymi plan organizacji łączności, w tym również łączności specjalnej. Zadanie to realizuje minister obrony, we współpracy z ministrem właściwym ds. łączności oraz Szefem Agencji Bezpieczeństwa Wewnętrznego. Plan obejmuje koncepcję krajowe-

[13] Rozporządzenie Rady Ministrów *w sprawie przygotowania* …, dz. cyt., § 13.1.
[14] Tamże, § 11. ust. 2.
[15] Tamże, § 12. ust. 4.

go systemu łączności oraz koncepcję współdziałania z systemami łączności państw sojuszniczych. System łączności jest niezbędnym elementem systemu kierowania, ponieważ zapewnia transfer decyzji do elementów wykonawczych systemu bezpieczeństwa. Zapewnienie poufności informacjom i danym, jakie są przekazywane za pośrednictwem systemów łączności między poszczególnymi stanowiskami kierowania, jest podstawowym zadaniem systemu ochrony. Aktualnie coraz większe znaczenie zyskują systemy teleinformatyczne, działające w środowisku sieciowym. Często jest to środowisko otwarte, narażone na zagrożenia zewnętrzne (w tym penetrację przez zorganizowane grupy). Sieci wykorzystywane są również do transmisji połączeń głosowych, co zwiększa możliwości ich zakłócenia, przekłamania lub utraty. W celu zapewnienia bezpieczeństwa (systemowi, danym, informacjom), niezbędne jest stosowanie systemów ochrony informacji, których zadaniem jest kompleksowa ochrona integralności i wiarygodności oraz zapewnienie poufności.

Podstawy prawne organizacji łączności dla Systemu Kierowania Bezpieczeństwem Narodowym

Organizacja stanowisk kierowania wymaga posiadania (lub pozyskania) odpowiedniej infrastruktury, **środków łączności** (wyr. autor), transportu, zabezpieczenia medycznego, informacyjnego, sprzętu kwaterunkowego, zabezpieczenia kontrwywiadowczego oraz wszelkich środków niezbędnych do zapewnienia bezpieczeństwa. Działania te podejmowane są przez organizującego, w porozumieniu z właściwymi ministrami (w poszczególnych obszarach kompetencji). Organizacja systemów łączności wymaga stosowania właściwych środków technicznych (telekomunikacyjnych i teleinformatycznych), które zapewnią przekazywanie decyzji od decydenta do elementów wykonawczych. W obszarze administracji publicznej kierowanie odbywa się poprzez szczeble struktury, od góry do dołu. W ramach tego samego poziomu realizowane jest współdziałanie. Powszechnie wykorzystuje się różnorodne środki komunikacji (kanały komunikacyjne), począwszy od tradycyjnych łączników (kurierów) aż do nowoczesnej komunikacji cyfrowej (sieci i łącza satelitarne). Wykorzystanie środków technicznych uregulowane jest przez właściwe akty prawne, z dziedziny łączności. Szeroko rozumiana „łączność" może być wykorzystana w szczególności na potrzeby kierowania BN, dowodzenia Siłami Zbrojnymi, a także na potrzeby utrzymywania systemów obserwacji, pomiarów, analiz, nadzorowania, prognozowania i powiadamiania. Systemy łączności na potrzeby obrony składają się z resortowych sieci telekomunikacyjnych, sieci przedsiębiorców telekomunikacyjnych, jak i operatorów pocztowych (państwowych i prywatnych),

wojskowej poczty polowej, poczty specjalnej oraz poczty kurierskiej. Akty prawne regulują:

- przygotowanie i wykorzystanie systemów łączności na potrzeby obronne państwa;
- wypełnianie przez przedsiębiorstwa telekomunikacyjne zadań i obowiązków na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego;
- współdziałanie operatora publicznego z wojskową pocztą polową;
- wykonywanie przez operatorów zadań na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego.

Głównym aktem prawnym jest ustawa z dnia 16 lipca 2004 r. *Prawo telekomunikacyjne*[16]. W rozdziale VIII ustawy, zawarte zostały obowiązki na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego. Zgodnie z art. 179 ust. 2. *przedsiębiorca telekomunikacyjny jest obowiązany do wykonywania zadań i obowiązków w zakresie przygotowania i utrzymywania wskazanych elementów sieci telekomunikacyjnych dla zapewnienia telekomunikacji na potrzeby systemu kierowania bezpieczeństwem narodowym, w tym obroną państwa, realizowanych na zasadach określonych w planach, decyzjach lub umowach zawartych między przedsiębiorcami telekomunikacyjnymi a uprawnionymi podmiotami*. W art. 180f ust. 1. nałożono na przedsiębiorcę obowiązek dostarczania danych na temat infrastruktury wydzielonej na potrzeby kierowana bezpieczeństwem do Prezesa UKE oraz niezwłocznego ich aktualizowania. Obowiązek ten ma zapewnić aktualność wiedzy na temat stanu sieci telekomunikacyjnych i teleinformatycznych, które są (lub mogą być) wykorzystywane dla potrzeb systemu kierowania.

Pozostałe akty prawne związane z przygotowaniem infrastruktury telekomunikacyjnej na potrzeby systemu kierowania bezpieczeństwem oraz zasad jej wykorzystania, to:

- Rozporządzenie Prezesa Rady Ministrów z dnia 16 września 2010 r. *w sprawie szczegółowych zasad wykonywania działalności telekomunikacyjnej w Sieci Łączności Rządowej* (Dz. U. Nr 177 z 2010 r., poz. 1192).
- Rozporządzenie Ministra Infrastruktury z dnia 12 października 2010 roku *w sprawie danych dotyczących infrastruktury telekomunikacyjnej niezbędnych do przygotowania systemów łączności na potrzeby obronne państwa* (Dz. U. Nr 196 z 2010 roku, poz. 1302.

---

[16] Ustawa z dnia 16 lipca 2004 r. *Prawo telekomunikacyjne* (Dz. U. z 2004 r., Nr 171, poz. 1800, z późn. zm.).

- Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 4 lutego 2003 roku *w sprawie szczegółowych warunków wykonywania działalności telekomunikacyjnej i używania urządzeń radiowych przez jednostki organizacyjne podległe i nadzorowane przez ministra właściwego dla spraw wewnętrznych* (Dz. U. Nr 35 z 2003 roku, poz. 307).
- Rozporządzenie Rady Ministrów z dnia 3 sierpnia 2004 r. *w sprawie przygotowania i wykorzystania systemów łączności na potrzeby obronne państwa* (Dz. U. Nr 180 z 2004 roku, poz. 1855).

Systemy telekomunikacyjne, które są organizowane na potrzeby kierowania, eksploatowane są przez osoby funkcyjne organów administracji podsystemu kierowania. Od strony technicznej organizacja systemu kierowania określona jest w Rozporządzeniu Rady Ministrów w sprawie przygotowania systemu kierowania bezpieczeństwem narodowym[17]. Rozporządzenie to określa rodzaje stanowisk kierowania oraz zasady ich organizacji i eksploatacji. Zawiera też delegacje dla ministra właściwego do spraw łączności w zakresie[18]:

- opracowania koncepcji organizacji systemu łączności, jego współdziałania z systemami państw sojuszniczych;
- określenia wymagań techniczno-eksploatacyjnych dla urządzeń łączności, standardy wyposażenia stanowisk kierowania;
- zapewnienia połączenia sieci łączności stanowisk kierowania z sieciami ogólnie dostępnymi (operatorów publicznych);
- opracowania koncepcji wykonywania i odbioru robót z zakresu łączności w rejonach stanowisk kierowania;
- sprawowania nadzoru nad wykonywaniem prac infrastrukturalnych, za pośrednictwem Prezesa Urzędu Komunikacji Elektronicznej (dawniej Prezesa Urzędu Regulacji Telekomunikacji i Poczty).

Kolejnym aktem prawnym związanym z organizacją łączności na potrzeby systemu kierowania, jest Rozporządzenie Rady Ministrów w sprawie przygotowania i wykorzystania systemów łączności na potrzeby obronne państwa[19]. Rozporządzenie to zawiera definicję podstawowych terminów z zakresu łączności, w tym

---

[17] Rozporządzenie Rady Ministrów z dnia 27 kwietnia 2004 roku *w sprawie przygotowania systemu kierowania bezpieczeństwem narodowym* (Dz. U. Nr 98, poz. 978).

[18] Tamże, § 21.

[19] Rozporządzenie Rady Ministrów z dnia 3 sierpnia 2004 r. *w sprawie przygotowania i wykorzystania systemów łączności na potrzeby obronne państwa* (Dz. U. Nr 180, poz. 1855).

definicję systemu łączności specjalnej oraz użytkownika specjalnego[20]. Te dwie definicje wprowadzają do systemów łączności na potrzeby kierowania SBN określenia zawierające odniesienia do specjalistycznych narzędzi i urządzeń kryptograficznych, które realizują zabezpieczenie informacji przed potencjalnym przeciwnikiem. Rozporządzenie określa również wymagania w zakresie cech, jakimi powinny charakteryzować się systemy łączności[21] oraz ich klasyfikację. W rozporządzeniu dokonano podziału systemów łączności na:

- systemy specjalne – realizujące zabezpieczenia z wykorzystaniem metod i narzędzi kryptograficznych;
- pozostałe systemy – które nie wykorzystują metod kryptograficznych.

Zgodnie z przedstawionym podziałem, do pozostałych systemów zaliczane są wszystkie systemy łączności, które nie wykorzystują narzędzi kryptograficznych. Klasyfikacja taka nie jest do końca precyzyjna. Na rynku komercyjnym znajduje się bowiem wiele modeli urządzeń (sieciowych i końcowych), które wykorzystują mechanizmy kryptograficzne do zabezpieczenia przetwarzanych danych, jednak nie posiadając certyfikatu bezpieczeństwa kryptograficznego[22], nie mogą być używane w systemach specjalnych. Mogą być jednak wykorzystane do zbudowania sieci teleinformatycznej, która nie będzie mogła przetwarzać informacji niejawnych, w rozumieniu ustawy[23]. Systemy teleinformatyczne (nie będące systemami specjalnymi) nie posiadają (nie muszą posiadać) akredytacji ABW lub SKW, upoważniającej do przetwarzania informacji niejawnych. Nie oznacza to jednak, iż nie można zastosować takich urządzeń (komercyjnych z mechanizmami kryptograficznymi) do budowy systemu łączności. Mogą przetwarzać informacje jawne, w tym dane osobowe, które podlegają ochronie ustawowej. Bezpieczeństwo systemów

[20] **System łączności specjalnej** – system łączności zabezpieczony przed nieuprawnionym dostępem do przekazywanej w nim informacji przez zastosowanie urządzeń i narzędzi kryptograficznych.

Użytkownik specjalny – organ władzy publicznej, Siły Zbrojne Rzeczypospolitej Polskiej lub przedsiębiorcę o szczególnym znaczeniu gospodarczo-obronnym, o którym mowa w art. 3 ustawy z dnia 23 sierpnia 2001 r. *o organizowaniu zadań na rzecz obronności państwa realizowanych przez przedsiębiorców* (Dz. U. Nr 122, poz. 1320 oraz z 2002 r., Nr 188, poz. 1571).

[21] Rozporządzenie Rady Ministrów z dnia 3 sierpnia 2004 r. *w sprawie przygotowania i wykorzystania…,* dz. cyt., § 3.

[22] Certyfikacja jest to proces potwierdzenia zdolności urządzenia, narzędzia lub innego środka do ochrony informacji niejawnych, ustawa z dnia 5 sierpnia 2010 roku *o ochronie informacji niejawnych*, art. 2 pkt 11 (Dz. U. z 2010 r., Nr 182, poz. 1228).

[23] Tamże, art. 48, pkt. 1, art. 50, pkt 2.

specjalnych znajduje się pod szczególną ochroną właściwych organów państwa, tj. Agencji Bezpieczeństwa Wewnętrznego (ABW), która to służba jest właściwa dla sfery cywilnej. Zadanie zapewnienia bezpieczeństwa postawiono Szefom służb specjalnych, tj. Agencji Bezpieczeństwa Wewnętrznego oraz Służby Kontrwywiadu Wojskowego[24] (dla sfery wojskowej). Zasady organizacji (najprawdopodobniej) opierają się na przepisach ustawy o ochronie informacji niejawnych, która zawiera rozdział o bezpieczeństwie teleinformatycznym (Rozdz. 8).

Rozporządzenie o przygotowaniu i wykorzystaniu systemów łączności na potrzeby obronne państwa daje możliwość wykorzystywania ich (systemów łączności) również w czasie pokoju, zagrożeń terrorystycznych lub innych szczególnych zdarzeń[25]. W przypadku wystąpienia zagrożenia kryzysem (w czasie pokoju) może wystąpić potrzeba wykorzystania tych systemów dla potrzeb łączności między stanowiskami organizowanymi w systemie zarządzania kryzysowego oraz systemem kierowania BN. Jednak w przedmiotowym Rozporządzeniu nie uwzględniono (jak do tej pory) tego problemu. Analizując potrzeby w zakresie łączności systemu kierowania SBN, nie sposób pominąć Zarządzania Kryzysowego (ZK), ze względu na jego znaczenie dla bezpieczeństwa narodowego. Brak uregulowań prawnych w zakresie łączenia działań obu systemów w jeden system kierowania, został dostrzeżony w Strategii Rozwoju Systemu Bezpieczeństwa Narodowego, przyjętej przez Radę Ministrów w dniu 9 kwietnia 2013 r.[26].

Podsumowując problem bezpieczeństwa teleinformatycznego w obszarze kierowania bezpieczeństwem oraz administracji publicznej, należy przywołać zapisy zawarte w Celu 5 Strategii:

Cele strategii rozwoju SBN związane z bezpieczeństwem informacyjnym i teleinformatycznym[27]:

5.3. Zapewnienie bezpieczeństwa informacyjnego i telekomunikacyjnego w kontekście zintegrowanego systemu bezpieczeństwa narodowego.

5.3.1. Podwyższenie stopnia zabezpieczeń zasobów teleinformatycznych administracji publicznej i państwowej, w tym przed zagrożeniami sieci Internet oraz cyberterroryzmem.

5.3.2. Rozwijanie Systemu Reagowania na Incydenty Komputerowe.

5.3.3. Rozwijanie Sieci Łączności Rządowej.

---

[24] Rozporządzenie Rady Ministrów z dnia 3 sierpnia 2004 r. *w sprawie przygotowania i wykorzystania…,* dz. cyt., § 11, ust. 1., pkt 4.

[25] Tamże, § 10, ust. 2.

[26] *Strategia Rozwoju Systemu Bezpieczeństwa Narodowego*, s. 15–16.

[27] Tamże, s. 82.

Umieszczenie problematyki bezpieczeństwa teleinformatycznego oraz systemu łączności rządowej w dokumencie strategicznym ma ogromne znaczenie dla kierunku rozwoju tego obszaru. Pozwala mieć nadzieję na rozpoczęcie prac nad rozwojem tej dziedziny przez właściwe organy państwa.

Systemy teleinformatyczne i telekomunikacyjne wspomagające kierowanie Systemem Bezpieczeństwa Narodowego

Trudno sobie dziś wyobrazić współczesne kierowanie organizacją (jaką jest również państwo), bez wykorzystania systemów teleinformatycznych. Ilość i rozmiar danych, jakie należy przetworzyć w celu wypracowania decyzji, jest ogromna. Również czas, jaki jest przeznaczony na podjęcie decyzji, jest ograniczony. Dodatkowo rozlokowanie jednostek organizacyjnych i kierowniczych na obszarze kraju wymaga stosowania szybkich i niezawodnych, jak również bezpiecznych, metod i narzędzi wymiany danych i informacji. Dlatego też podejmowane są działania mające na celu opracowanie i wdrożenie systemów teleinformatycznych (i telekomunikacyjnych), dla potrzeb zarządzania państwem oraz bezpieczeństwem narodowym. Przed omówieniem przykładowych systemów, warto przywołać podstawowe definicje.

Pojęcie systemu informatycznego jest pojęciem prawnym, które pojawiło się ustawie o ochronie danych osobowych[28]. **Systemem informatycznym** jest zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych. Natomiast pojęcie systemu teleinformatycznego zostało zdefiniowane w ustawie o świadczeniu usług drogą elektroniczną[29]. **System teleinformatyczny** to zespół współpracujących ze sobą urządzeń informatycznych i oprogramowania, zapewniający przetwarzanie i przechowywanie, a także wysyłanie i odbieranie danych poprzez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci urządzenia końcowego w rozumieniu ustawy z dnia 16 lipca 2004 r. Prawo telekomunikacyjne. Pojęcie systemu teleinformatycznego jest pojęciem szerszym, obejmującym również procesy przesyłania danych (transmisja danych) i informacji (telekomunikacja). Podstawowymi elementami procesów transmisji i telekomunikacji są dane i informacje. W języku potocznym pojęć tych używa się wymiennie, w celu uproszczenia komu-

[28] Ustawa z dnia 29 sierpnia 1997 r. *o ochronie danych osobowych*, art. 7 pkt 2a (Dz. U. z 1997 r., Nr 133 poz. 883).

[29] Ustawa dnia 18 lipca 2002 roku *o świadczeniu usług drogą elektroniczną* (Dz. U. z 2002 r., Nr 144, poz. 1204 ze zm.).

nikacji[30]. Jednak **dana** to reprezentacja fizyczna elementarnej porcji informacji. Jest wykorzystywana do rejestrowania informacji i jej przekazu. **Informacja** zaś to zbiór faktów, zdarzeń, cech obiektów itp., zawarty w określonej wiadomości, tak ujęty i podany w takiej formie, że pozwala odbiorcy ustosunkować się do zaistniałej sytuacji i podjąć odpowiednie działania umysłowe lub fizyczne[31]. Definicja ta nadaje informacji znacznie szersze znaczenie niż danej, ponieważ stawia ją u podstaw podejmowanych decyzji. Co z kolei wiąże się z koniecznością zapewnienia atrybutów wiarygodności i integralności oraz poufności (jeżeli jest wymagana). Wśród obszarów zagrożeń, jakie można zidentyfikować dla informacji, można wyróżnić:

- Sfera dostępu do informacji – celem jest uzyskanie dostępu do wiedzy na jakiś temat.
- Sfera przepływu informacji – celem jest naruszenie integralności informacji lub danych.
- Sfera tożsamości nadawców i odbiorców informacji – celem jest podszycie się pod nadawcę lub odbiorcę informacji lub danych.

Wymienione sfery współistnieją w systemie łączności[32], jaki jest (powinien być) wykorzystywany w kierowaniu BN. We współczesnym, cyfrowym świecie, zagrożenia te nabierają szczególnej wagi w omawianym obszarze. Dlatego też niezbędne jest wdrożenie i wykorzystanie najnowszych, narodowych rozwiązań, które będą zapewniać bezpieczeństwo usług związanych z kierowaniem bezpieczeństwem narodowym, zarówno w zarządzaniu kryzysowym, jak i zarządzaniu obronnością państwa.

Poniżej przedstawiony jest przegląd systemów teleinformatycznych eksploatowanych przez poszczególne resorty i służby, wykorzystywanych do wspomagania systemu kierowania. Analizę systemów podzielono na dwie części. Pierwsza dotyczy systemów łączności i wspomagania zarządzania na potrzeby obronne państwa (w tym systemu kierowania bezpieczeństwem), natomiast druga część analizy dotyczy systemów wykorzystywanych w zarządzaniu kryzysowym.

---

[30] M. Kuraś, *System informacyjny – system informatyczny. Co poza nazwą różni te dwa obiekty?,* „Zeszyty Naukowe Akademii Ekonomicznej w Krakowie" 2004, s. 3.

[31] P. Sienkiewicz, *Inżynieria systemów*…, dz. cyt., s. 61.

[32] System łączności stanowi zintegrowane środowisko teleinformatyczne i telekomunikacyjne, zapewniające realizację potrzeb systemu kierowania w zakresie usług głosowych, transmisji danych, video- i telekonferencji.

Przegląd systemów teleinformatycznych wspomagających kierowanie bezpieczeństwem narodowym

Po transformacji ustrojowej w 1989 roku systemy łączności administracji i kierowania bezpieczeństwem państwa również musiały ulec zmianie. Wynikało to ze zmian ustrojowych (podporządkowanie sił zbrojnych i jednostek siłowych pod nadzór cywilny), jak również z rozwoju technologicznego, do jakiego Polska uzyskała dostęp. Ważnym czynnikiem warunkującym zmiany było również stosowanie wcześniej urządzeń radzieckich, które stanowiły zagrożenie dla bezpieczeństwa informacji.

Rozwój nowoczesnych technologii telekomunikacyjnych wymusił wdrożenie nowych usług telekomunikacyjnych, takich jak telefonia komórkowa, łączność cyfrowa, łączność radiowa oraz komputerowe sieci rozległe. Jednak najbardziej dynamiczny rozwój nastąpił po wstąpieniu Polski do UE, kiedy pojawiły się środki finansowe na rozwój sieci rozległych (transportowych), które stanowić miały szkielet dla nowoczesnych systemów teleinformatycznych.

Podstawy planu modernizacji systemów teleinformatycznych, realizujących wspomaganie dowodzenia siłami Policji, Straży Pożarnej, Straży Granicznej i Biura Ochrony Rządu, zawarte zostały w ustawie o programie modernizacji[33]. Celem uruchomienia tego programu miało być stworzenie warunków do pełnej realizacji ustawowych zadań przez jednostki organizacyjne przeznaczone do ochrony bezpieczeństwa i porządku publicznego, oraz istotną poprawę skuteczności ich działania[34]. Chociaż program obejmował całościową modernizację tych formacji, to wśród obszarów wymieniał również sprzęt i systemy teleinformatyczne, przeznaczone do wspomagania zarządzania bezpieczeństwem. W związku z tym, iż nie pojawił się wcześniej żaden kompleksowy program budowy lub modernizacji systemu łączności rządowej, skupiono się na modernizacji i rozbudowie sieci resortowych. W efekcie miały one stanowić w przyszłości warstwę transportową dla łączności rządowej.

Podstawowy podział systemów wspomagających kierowanie (dowodzenie) można przeprowadzić ze względu na zastosowanie środków ochrony:

- systemy specjalnego zastosowania – przeznaczone do ochrony danych oraz informacji za pomocą specjalizowanych narzędzi i mechanizmów, w tym posia-

---

[33] Ustawa z dn. 17 stycznia 2007 roku o *ustanowieniu „Programu modernizacji Policji, Straży Granicznej, Państwowej Straży Pożarnej i Biura Ochrony Rządu w latach 2007-2009"* (Dz. U. z 2007 r., Nr 35, poz. 213).

[34] Tamże, art. 2.

dających certyfikaty bezpieczeństwa kryptograficznego, teleinformatycznego lub elektromagnetycznego;
- systemy powszechne – pozostałe, umożliwiające komunikowanie się organów administracji publicznej i wymiany danych i informacji nie będących informacjami niejawnymi.

Systemy specjalne chronione są klauzulą niejawności, co uniemożliwia ich szczegółowy opis, jak również ogranicza dostępność informacji o nich. Poszukując informacji o takich systemach należy poszukiwać informacji o urządzeniach, z jakich są zbudowane oraz ich funkcji. Ciekawostką jest dostępność tych informacji w dokumentacji przetargowej, jaka jest wytwarzana przy ich ogłaszaniu[35]. Informacje takie zostały wykorzystane w niniejszym artykule.

Analiza systemów została również przeprowadzona pod kątem realizowanych usług podstawowych. Systemy teleinformatyczne wspomagające zarządzanie BN można podzielić nas:
- systemy teleinformacyjne i teleinformatyczne przetwarzania danych i wspomagania podejmowania decyzji;
- systemy teletransmisyjne – umożliwiające transmisję danych między użytkownikami końcowymi;
- systemy telekomutacyjne – systemy łączności zapewniające połączenia telekomunikacyjne teleinformatyczne, tzw. sieć szkieletowa;
- systemy łączności bezprzewodowej – systemy łączności mobilnej, zapewniające transmisje danych i transmisję głosu dla użytkowników mobilnych.

Poniżej przedstawione zostały zidentyfikowane systemy teleinformatyczne i telekomunikacyjne. Szerszy opis zamieszczono dla systemów wspomagania kierowania (dowodzenia) oraz systemu łączności rządowej.

Systemy informatyczne i teleinformatyczne

Administracja publiczna korzysta z dużej liczby systemów informatycznych, wspomagających procesy kierowania państwem oraz realizację zarządzania bezpieczeństwem obywateli i państwa. Korzysta również z systemów teleinformatycznych, które zapewniają zdalne przetwarzanie danych. Jednak systemy te nie tworzą spój-

[35] Należy zastanowić się nad możliwością wyłączenia z trybu zamówień publicznych inwestycji w systemy specjalne, z jednoczesnym zapewnieniem przejrzystości tych procesów i ich kontroli przez upoważnione służby.

nego i kompleksowego systemu łączności, dedykowane dla kierowania państwem, a w szczególności kierowania bezpieczeństwem.

Rejestr systemów informatycznych administracji publicznej został wprowadzony przez Główny Urząd Statystyczny i publikowany jest w BIP[36]. Rejestr ten zawiera 587 pozycji. Nie zawiera systemów dedykowanych dla bezpieczeństwa państwa, jak również systemów niejawnych oraz resortowych (MSW i MON). Wśród wymienionych systemów można wyróżnić systemy związane z szeroko pojmowanym bezpieczeństwem narodowym (jego poszczególnymi elementami). Przedstawiony poniżej opis podzielony został na systemy poszczególnych resortów i służb.

Resort właściwy dla spraw wewnętrznych eksploatuje wiele systemów teleinformatycznych przetwarzających dane z zakresu bezpieczeństwa publicznego, bezpieczeństwa ruchu drogowego, dokumentów paszportowych i tożsamości, oraz innych. Jednocześnie jest resortem odpowiedzialnym za prowadzenie rejestrów referencyjnych, które są wykorzystywane przez inne systemy do weryfikacji danych o obywatelach, pojazdach, nieruchomościach i innych.

Systemy będące w gestii ministerstwa właściwego do spraw wewnętrznych:

- Centralna Ewidencja Wydanych i Unieważnionych Dokumentów Paszportowych (CEWiUDP).
- Ogólnokrajowa Ewidencja Wydanych i Unieważnionych Dowodów Osobistych (OEWiUDO).
- Powszechny Elektroniczny System Ewidencji Ludności (PESEL).
- Rejestr działalności regulowanej w zakresie usług detektywistycznych.
- Rejestr lekarzy odbywających specjalizację w zakładach opieki zdrowotnej Ministerstwa Spraw Wewnętrznych.
- Rejestr nieruchomości, udziałów i akcji nabytych lub objętych przez cudzoziemców bez zezwolenia Ministra Spraw Wewnętrznych.
- Rejestr nieruchomości, udziałów i akcji nabytych lub objętych przez cudzoziemców za zezwoleniem Ministra Spraw Wewnętrznych.
- Rejestr osób posiadających licencję detektywa.
- Rejestr upoważnień do nakładania grzywny w drodze mandatu karnego.
- Rejestr zakładów produkujących lub wprowadzających do obrotu żywność, podlegających kontroli urzędowej organów Państwowej Inspekcji Sanitarnej.

Wśród wymienionych systemów nie ma typowych systemów wspomagania kierowania. Są one jednak wykorzystywane w działaniach dla zapewnienia bezpie-

[36] http://www.stat.gov.pl/cps/rde/xbcr/bip/BIP_wykaz_systemow_informacyjnych_administracji_publicznej_2013.pdf (dostęp 24.05.2013 r.).

czeństwa publicznego, ekonomicznego, gospodarczego i innych, dlatego też zostały zamieszczone w artykule.

Kolejną służbą, która wykorzystuje systemy teleinformatyczne, jest Państwowa Straż Pożarna. Komenda Główna Straży Pożarnej eksploatuje System Wspomagania Decyzji dla Stanowisk Kierowania SWD-ST. System ten jest również eksploatowany w komendach PSP niższego szczebla. Jest to typowy system wspomagania podejmowania decyzji i kierowania podległymi jednostkami. System SWD-ST[37] powstał w 2001 roku, jako system obejmujący swoim zakresem informacyjnym główne wydziały Państwowej Straży Pożarnej. System jest rozwijany już od ponad 10 lat. Składa się z dwóch części:

- System SWD-ST 3 – platforma przeznaczona dla Komendy Głównej PSP oraz komend wojewódzkich.
- System SWD-ST 2.5 – platforma przeznaczona dla komend powiatowych i miejskich.

System SWD-ST 3 stanowi oprogramowanie dziedzinowe przeznaczone dla Komendy Głównej Państwowej Straży Pożarnej oraz komend wojewódzkich PSP. Oprogramowanie to dedykowane jest dla wszystkich wydziałów tych komend, ze szczególnym wyróżnieniem służb dyżurnych KCKRiOL[38], WSKR[39] oraz służby operacyjnej. Podstawowymi zadaniami systemu SWD-ST 3 jest wspieranie procesów dowodzenia, koordynacji działań oraz szeroko rozumianego podejmowania decyzji przez osoby nadzorujące działania ratownicze.

System SWD-ST 3 wspiera następujące obszary funkcjonalne:

- Przyjmowanie zgłoszeń ratowniczych oraz obsługa i koordynacja zdarzeń ratowniczych.
- Wykorzystanie mapy cyfrowej jako środowisko wspierającego działania operacyjne.
- Zarządzanie bazą sił i środków obejmującą informacje o: jednostkach, podmiotach ratowniczych, instytucjach wspierających działania PSP, ludziach, pojazdach, sprzęcie ratowniczym.
- Obsługa informacji o zdarzeniach zgodnie z obowiązującymi przepisami (EWID99).

---

[37] Na podstawie strony producenta systemu SDW-ST, http://www.swdst.pl/index.php/info, http://www.abakus.net.pl/products/swdst25.html (dostęp 26.05.2013 r.).

[38] Krajowe Centrum Koordynacji Ratownictwa i Ochrony Ludności Komendy Głównej Państwowej Straży Pożarnej, zwane dalej KCKRiOL.

[39] Wojewódzkie Stanowisko Koordynacji Ratownictwa, zwane dalej WSKR.

- Wykorzystanie i współpraca z urządzeniami wspierającymi prace dyspozytorskie takimi jak: centrale telefoniczne, rejestratory korespondencji, bramki SMS, systemy lokalizacji pojazdów.
- Wymiana informacji pomiędzy poszczególnym komendami PSP.
- Centralne zarządzanie katalogami i słownikami.
- Analizy, statystyki oraz raporty.

System SWD-ST 2.5 jest oprogramowaniem dziedzinowym przeznaczonym dla komend powiatowych i miejskich Państwowej Straży Pożarnej. Oprogramowanie obejmuje zakresem funkcjonalnym i informacyjnym wszystkie obszary działalności PSP z szczególnym uwzględnieniem zadań realizowanych przez Wydziały Operacyjne. Podstawowym zadaniem systemu SWD-ST 2.5 jest wspomaganie służby dyżurnej w obsłudze zgłoszeń i zdarzeń, koordynacji działań ratowniczych oraz sporządzaniu dokumentacji z przeprowadzonych akcji.

System SWD-ST 2.5 wspiera następujące obszary funkcjonalne:

- Przyjmowanie zgłoszeń oraz obsługa i koordynacja zdarzeń ratowniczych.
- Współdziałanie z systemami łączności takimi jakimi jak: centrale telefoniczne, rejestratory korespondencji, monitoring pożarowy.
- Dysponowanie sił i środków do działań ratowniczych.
- Alarmowanie i powiadamianie posiadanych sił i środków poprzez: systemy komunikacji statusowej z pojazdami ratowniczymi, systemy lokalizacji i monitoringu pojazdów, Systemy alarmowania w oparciu o SMS, Systemy alarmowania jednostki.
- Obsługa mapy cyfrowej zapewniająca lokalizację miejsca zdarzenia, prowadzonych działań oraz rozmieszczenia sił i środków.
- Przekazywanie zdarzeń oraz obsługa żądań dyspozycji.
- Gromadzenie danych oraz zarządzanie bazą sił i środków obejmującą informacje o jednostkach, podmiotach ratowniczych, instytucjach wspierających działania PSP, ludziach, specjalistach, pojazdach, sprzęcie ratowniczym, środkach gaśniczych i neutralizatorach.
- Tworzenie dokumentacji zgodnie z obowiązującymi przepisami.
- Wymiana informacji z nadrzędną komendą wojewódzką.
- Analizy, statystyki oraz raporty.
- Współdziałanie z systemem SWD-ST 3.

Można stwierdzić, iż oprogramowanie to rozwiązuje problem kierowania jednostkami PSP. Jednak nie jest częścią większego systemu, co ogranicza jego zastosowanie w systemie kierowania BN i uniemożliwia automatyczne przekazywanie danych.

Komenda Główna Policji jest gestorem (użytkownikiem) systemów rejestrowych oraz systemów teleinformatycznych, w tym systemu wspomagania dowodzenia. Są to:

- Krajowy System Informatyczny (KSI).
- Policyjny rejestr imprez masowych (PRIM).
- Policyjny System Statystyki Przestępczości TEMIDA (PSSP TEMIDA).
- System Ewidencji Wypadków i Kolizji.
- System Wspomagania Dowodzenia (SWD).
- Zbiór danych osobowych modułu „BROŃ".
- Zbiór danych osobowych modułu „LICENCJA".

Wśród wymienionych systemów należy wyróżnić System Wspomagania Dowodzenia (SWD)[40]. Jest to prowadzony w systemie teleinformatycznym zbiór informacji wspomagających kierowanie działaniami Policji, podejmowanymi w celu wykonywania zadań ustawowych na podstawie zgłoszeń otrzymywanych przez dyżurnych jednostek organizacyjnych Policji oraz ustaleń dokonywanych przez poszczególne służby policyjne w związku z tymi zgłoszeniami. Podstawowe cele Systemu Wspomagania Dowodzenia Policji (SWD) to[41]:

- Wsparcie służb dyżurnych w zakresie podejmowania decyzji, alokacji sił i środków.
- Zapewnienie skrócenia czasu reakcji Policji na przyjmowane zgłoszenia.
- Zwiększenie wydajności pracy policjantów.
- Zapewnienie bieżącego dostępu do informacji dla całej służby dyżurnej, sił prewencji i ruchu drogowego.
- Zautomatyzowanie części działań poprzez wprowadzenie elektronicznej rejestracji zgłoszeń.
- Zapewnienie mobilnego dostępu do zasobów systemowych.
- Unifikacja sposobu dokumentowania działań.

System SWD policji został opracowany w celu ujednolicenia procedur postępowania, dokumentacji, analizy i raportowania działań podejmowanych we wszystkich jednostkach Policji w Polsce. System ten ma na celu kompletną, w znacznej czę-

[40] K. Olejnik, M. Maciejewski, *Dyżurny jednostki organizacyjnej policji (materiał dydaktyczny),* Słupsk 2013 r., http://www.slupsk.szkolapolicji.gov.pl/ebiblioteka/pdf17.pdf, s.9 (dostęp 26.06.2013 r.).

[41] Na podstawie materiałów z I Konferencji SIPR, http://www.cpi.gov.pl/files/fck/File/konferencje/SIPR_marzec_2011/I_Konf_SIPR_System_Wspomagania_Dowodzenia_Policji.pdf (dostęp 24.05.2013 r.).

ści elektroniczną, obsługę zdarzeń od momentu przyjęcia informacji o zdarzeniu, poprzez jego obsługę, do procesu analizowania danych, sporządzania opracowań statystycznych i raportowania. Zadaniem głównym tego systemu jest dostarczenie służbom dyżurnym oraz policjantom realizującym przedsięwzięcia związane z dyslokacją służby w jednostkach Policji na terenie całego kraju jednolitej informacji, która zapewni standaryzację pracy i usprawni proces podejmowania decyzji związanych z obsługą zdarzeń. Do zadań systemu należy również dostarczenie narzędzi do szybkiej rejestracji czynności i dostępu do danych niezbędnych w wykonywaniu obowiązków służbowych wielu funkcjonariuszy. Funkcjonalność systemu uwzględnia zadania służb dyżurnych w zakresie rejestracji, przetwarzania i nadzorowania wszystkich czynności podejmowanych przez policjantów w danej jednostce organizacyjnej Policji[42]. Z racji znaczenia tego systemu dla bezpieczeństwa publicznego, wprowadzone zostały odpowiednie zabezpieczenia związane z dostępem do SWD. Zostały one określone w dokumencie opublikowanym przez Biuro Łączności i Informatyki Komendy Głównej Policji, o nazwie „*Polityka bezpieczeństwa Systemu Wspomagania Dowodzenia jednostek organizacyjnych Policji. Poziom Wysoki, Warszawa 2011*". Dokument ten zawiera procedury bezpieczeństwa w zakresie dostępu do danych, zgodnie z ustawą o ochronie danych osobowych. System ten znajduje się na etapie wdrożenia i testów (stan na rok 2012). System SWD jest integralną częścią budowanego Systemu Informatycznego Powiadamiania Ratunkowego (SI PR) składającego się ze zintegrowanych systemów klasy SWD takich służb, jak Policja, Państwowa Straż Pożarna, Państwowe Ratownictwo Medyczne oraz Platformy Lokalizacyjno-Informacyjnej z Centralną Bazą Danych (PLI CBD) służącej do lokalizacji abonentów dzwoniących na numery alarmowe. Również ten system nie jest włączony w system nadrzędny, jednak jego założenia pozwalają na zintegrowanie go (w przyszłości) z systemem, który powstanie w oparciu o system OST112 (jest przedstawiony w dalszej części).

Straż Graniczna to kolejna służba, która eksploatuje systemy teleinformatyczne przeznaczone do wspomagania kierowania i realizacji zadań ustawowych. Systemy w gestii Komendy Głównej Straży Granicznej to:

- Centralna Baza Danych Straży Granicznej System Wspomagania Kierowania.
- Centralne Archiwum Odpraw.
- Ewidencja osób przekraczających granicę państwową.
- Ewidencja wydanych tymczasowych zaświadczeń tożsamości cudzoziemca.
- JAGAII.
- Rejestr Akt Cudzoziemców.

[42] Za K. Olejnik, M. Maciejewski, *Dyżurny jednostki organizacyjnej…*, dz. cyt., s. 32.

- Rejestr złożonych wniosków o nadanie statusu uchodźcy oraz wydanych w tych sprawach decyzji i postanowień.
- Rejestr złożonych wniosków wizowych i wydanych w tych sprawach.
- System Ewidencji Informacji.
- System Teleinformatyczny – Platforma Wymiany Informacji.
- Zbiór wniosków o pobyt tolerowany.
- Zintegrowany System Ewidencji (wersja 4 – ZSE4).
- System ODPRAWA SG.
- System Informatyczny Schengen SIS.
- System Informacji Wizowej VIS.

System Wspomagania Kierowania SG (Centralna Baza Danych Straży Granicznej System Wspomagania Kierowania) jest na etapie wdrażania. Projekt został rozpoczęty w połowie roku 2010 (ogłoszenie przetargu na zakup licencji oprogramowania i sprzęt)[43]. Projekt był realizowany przez zespół informatyków zatrudnionych w SG, co miało na ograniczyć koszty opracowania. Wewnętrzna współpraca (w ramach SG) projektantów i przyszłych użytkowników, powinna również zapewnić właściwą identyfikację potrzeb oraz pożądanej funkcjonalności systemu. W założeniach SWK miał przynieść następujące korzyści[44]:

- minimalizacja powielania dokumentowania zdarzeń w różnych systemach informatycznych i zbiorach papierowych;
- ujednolicenie procedur postępowania w przypadku analogicznych zdarzeń;
- minimalizacja (docelowo całkowita likwidacja) dokumentacji prowadzonej w formie papierowej;
- przepływ rejestrowanych w systemie zdarzeń odbywa się niemal w czasie rzeczywistym między poszczególnymi szczeblami w strukturze organizacyjnej;
- automatyczne rozliczanie czasu służby (pracy);
- dzięki elektronicznemu gromadzeniu danych łatwe wyszukiwanie, tworzenie zestawień, raportów itp.

System ten miał ułatwić i usprawnić kierowanie jednostkami Straży Granicznej, rozlokowanymi na obszarze kraju. Należy mieć nadzieję, że jego budowa umożliwi w przyszłości integrację z systemem krajowym, o ile takowy zostanie zbudowany.

---

[43] Informacje zaczerpnięte z SIWZ do zamówienia „Budowa systemu CBD SG Ewida oraz CBD SG SWK Etap I", ogłoszonego przez Komendę Główną Straży Granicznej.

[44] M. Rawski, *Informatyczny System Wspomagania Kierowania Straży Granicznej*, „Zeszyty Naukowe Wydziału Zarządzania i Dowodzenia AON" 2012, nr 1, s. 178–179.

W roku 2012 rozpoczęły się testy wdrożeniowe systemu. Oceny jego efektywności oraz realizacji założonych celów będzie jednak można dokonać dopiero po jego wdrożeniu w docelowej konfiguracji.

Systemy teletransmisyjne i sieci szkieletowe

Systemy szkieletowe stanowią podstawową infrastrukturę przenoszenia ruchu i transmisji danych. Przeznaczone są nie tylko do transmisji danych, ale również do obsługi połączeń głosowych oraz video- i telekonferencji. Dotychczas budowane były przez poszczególne resorty, dla obsługi własnych systemów teleinformatycznych. Zidentyfikowane systemy szkieletowe[45] to:

- system teletransmisyjny Policji POLWAN (sieć szkieletowa, międzywojewódzka);
- warszawską sieć szkieletową SDH – szybka sieć szkieletowa urzędów centralnych na terenie miasta stołecznego;
- wojewódzkie sieci teletransmisyjne Policji – zapewniające dołączenie komend powiatowych i gminnych do sieci wojewódzkiej;
- policyjną sieć transmisji danych (PSTD) – to sieć korporacyjna Policji, wykorzystująca protokół IP, funkcjonująca na podkładzie sieci POLWAN. Głównym zadaniem było połączenie jednostek Policji w całym kraju. Sieć służy, jako podstawowe medium teletransmisyjne dla dostępu funkcjonariuszy Policji do centralnych i lokalnych baz danych, poczty elektronicznej i innych usług. Stanowi medium transmisyjne dla systemów teleinformatycznych eksploatowanych przez Policję.
- sieć PESEL-NET – wydzielona sieć zapewniająca dostęp urzędów stanu cywilnego do zasobów centralnych systemu PESEL. Aktualnie wdrażany jest projekt Zintegrowany Moduł Obsługi Końcowego Użytkownika, który umożliwia dostęp do zasobów za pośrednictwem sieci ogólnodostępnej.
- sieć transmisji danych Straży Granicznej – realizująca przenoszenie różnego rodzaju usług, np. transmisja głosu, danych, transmisja video. Sieć zbudowana jest w oparciu o urządzenia formy Cisco. Dla zabezpieczenia przesyłanych danych wdrożono zabezpieczenia dostępne w urządzeniach sieciowych.

---

[45] M. Machnacz, *Bezpieczeństwo aktywów ministerstwa spraw wewnętrznych i administracji w infrastrukturze krytycznej państwa*, [w:] *Bezpieczeństwo w telekomunikacji i teleinformatyce,* red. B. Lent, Tom 3, Wydawnictwo BBN, Warszawa 2008, s. 51-52.

POLWAN był korporacyjną, cyfrową siecią szkieletową Policji, z 54 węzłami telekomunikacyjnymi ulokowanymi w jednostkach szczebla wojewódzkiego, Komendzie Głównej Policji, byłych KWP i niektórych większych miastach. Sieć zbudowana była w technologii Frame Relay (układ kratowy). Sieć POLWAN przenosiła wszystkie usługi (multimedia), posiadała funkcjonalność zestawiania połączeń tele/video konferencyjnych. Jej przepływność to wielokrotność 2Mbps. Wraz ze wzrostem obciążenia i ewolucją techniczną w obrębie systemów wspomagania i środków technicznych okazało się, że nie spełnia oczekiwań. Główną przyczyną była przestarzała technologia, która stwarzała duże problemy z utrzymaniem sieci oraz brakiem możliwości wdrożenia nowych usług. W związku z tym podjęto decyzję o jej modernizacji. W celu pozyskania środków unijnych na przebudowę i modernizację sieci, zdecydowano się na rozpoczęcie nowego projektu pod nazwą Ogólnopolska Sieć Teleinformatyczna na potrzeby numeru alarmowego 112 (OST112). Przyjęcie takiej koncepcji modernizacji pozwoliło na uzyskanie dofinansowania z Programu Operacyjnego Innowacyjna Gospodarka POiG, w okresie programowym na lata 2007-2013, VII oś priorytetowa (85% / 15%) (Część I – Zakup i wdrożenie urządzeń z oprogramowaniem). Część II – dzierżawa łączy została sfinansowana ze środków budżetowych. Założeniem nowego systemu było wykorzystanie istniejących lokalizacji dla osadzenia nowych urządzeń sieciowych oraz nowych rodzajów łączy.

Założenia na system OST112[46]:

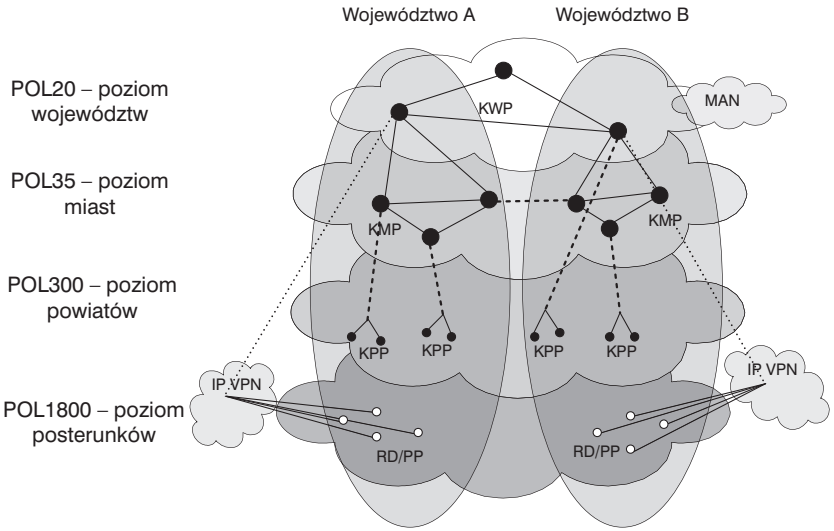
- Stworzenie nowoczesnej sieci transmisji danych, umożliwiającej integrację dotychczas eksploatowanych systemów oraz ich rozbudowę, jak również wdrożenie nowoczesnych rozwiązań teleinformatycznych.
- Zapewnienie zadawalającego poziomu współdziałania jednostek Policji, Państwowej Straży Pożarnej, Państwowego Ratownictwa Medycznego.
- Zbudowanie nowoczesnych systemów zarządzania siłami i środkami ochrony przeciwpożarowej i ratowniczymi.
- Stworzenie platformy telekomunikacyjnej dla Systemu Powiadamiania Ratunkowego (SPR) zapewniającej możliwość uruchamiania: SI WCPR/CPR, SWD PSP, SWD Policji, SWD Państwowego Ratownictwa Medycznego.
- Możliwość uruchamiania innych systemów, przeznaczonych do wspomagania zarządzania bezpieczeństwem.

Sieć OST112 nie może być traktowana jako system łączności, ponieważ nie posiada indywidualnych urządzeń końcowych. Należy traktować ją jako

[46] Opracowanie na podstawie Książki o projekcie OST112, wydanej przez Centrum Projektów Informatycznych, Warszawa 2012, www.cpi.gov.pl (dostęp 26.05.2013 r.).

sieć szkieletową, która stanowi bazę transportową (przenoszenia ruchu) dla systemów łączności i teleinformatycznych. Zastąpienie sieci POLWAN siecią OST112 stanowi ogromny skok technologiczny w obszarze łączności jednostek i służb odpowiedzialnych za bezpieczeństwo obywateli. W przypadku zrealizowania planów o wykorzystaniu jej dla potrzeb systemów administracji publicznej umożliwi również sprawne i bezpieczne realizowanie usług z zakresu kierowania i dowodzenia.

Poniższy rysunek przedstawia schemat sieci szkieletowej nałożonej na strukturę organizacyjną policji.

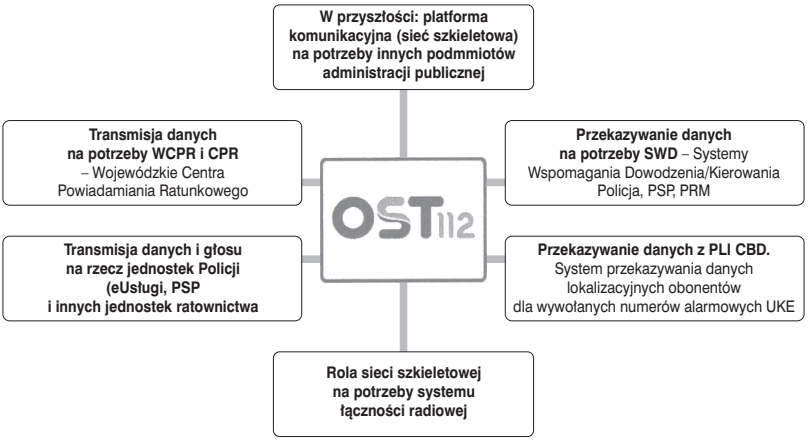


Źródło: Opracowanie własne na podstawie prezentacji Centrum Projektów Informatycznych, http://www.cpi.gov.pl/prezentacje,82.html (dostęp 10.09.2014 r.).

Rys. 3. Schemat sieci OST112, pełniącej zadania sieci szkieletowej.

Perspektywiczny model integracji usług w sieci OST112 przedstawiony został na rysunku 4.

Schemat przedstawia docelowy zbiór usług, jakie mają być udostępniane przez system OST112. Jedną z nich jest usługa platformy komunikacyjnej (sieci szkieletowej) dla potrzeb komunikacyjnych administracji publicznej. Jednak nie może stać się to wcześniej, niż po 5 latach od uruchomienia systemu, ze względu na środki unijne, jakie zostały wykorzystane do jego budowy.



Źródło: Opracowanie na podstawie książki o projekcie OST112 wydanej przez Centrum Projektów Informatycznych, Warszawa 2012, www.cpi.gov.pl (dostęp 26.05.2013 r.).

Rys. 4. Docelowa integracja usług oferowanych przez system OST112.

Podsumowując przegląd sieci szkieletowych eksploatowanych w Polsce, można zaobserwować pozytywną zmianę, jaką jest ich modernizacja i skok technologiczny. Sieci te stanowią bazę do rozwoju nowoczesnych systemów łączności, które pozwalają integrować różne rodzaje usług. Zapewniają też bezpieczeństwo przenoszonych danych na poziomie urządzeń sieciowych. Pozwalają też budować na ich bazie specjalizowane sieci łączności, zarówno resortowe, jak i publiczne, które mogą być odseparowane logicznie od pozostałych użytkowników. Daje to możliwość zastosowania specjalizowanych mechanizmów zabezpieczeń dla zapewnienia bezpieczeństwa informacjom i danym o różnych klauzulach niejawności, co z kolei umożliwi rozwój łączności rządowej oraz na potrzeby kierowania bezpieczeństwem.

Systemy specjalne na potrzeby kierowania bezpieczeństwem narodowym

Kolejnym rodzajem są systemy specjalne. Są one najbliżej związane z kierowaniem bezpieczeństwem, ponieważ zostały opracowane pod kątem realizacji zadań związanych właśnie z kierowaniem.

Geneza systemów specjalnych, przeznaczonych do zarządzania bezpieczeństwem, wywodzi się z systemów obronnych. Obronne systemy łączności mogą być wykorzystywane na potrzeby kierowania bezpieczeństwem narodowym, zgodnie

z §10.1 Rozporządzenia Rady Ministrów *w sprawie przygotowania i wykorzystania systemów łączności na potrzeby obronne państwa*[47]. W przytoczonym Rozporządzeniu zawarto również możliwość ich wykorzystania w czasie pokoju, w razie wystąpienia działań terrorystycznych lub szczególnych zdarzeń (§ 10.2). Określenie „szczególne zdarzenia" nie zostało zdefiniowane, co stwarza możliwość różnej interpretacji, zarówno negatywnej (zaostrzenie możliwości wykorzystania), jak również pozytywnej (łagodniejsze podejście do możliwości wykorzystania przez poszczególne jednostki).

Analizując dostępne informacje zidentyfikowano następujące systemy łączności (w tym również specjalne), organizowane na potrzeby kierowania:

- Sieć Łączności Rządowej – zorganizowany na podstawie Rozporządzenia Prezesa Rady Ministrów w sprawie szczegółowych zasad wykonywania działalności telekomunikacyjnej w Sieci Łączności Rządowej[48], obejmujący część jawną i niejawną. SŁR stanowi główny system łączności na potrzeby kierowania państwem.
- System mobilnej łączności niejawnej CATEL – zarządzany przez ABW. Jest to najnowszy, mobilny, system łączności, działający w oparciu o sieć GSM. Jest elementem niejawnej części Sieci Łączności Rządowej. System zapewnia obsługę kalendarza, poczty elektronicznej oraz usługę połączeń głosowych.
- Podsystem Niejawnej Łączności Telefonicznej SZ RP „CYGNUS-MIL. System ten miał zostać zorganizowany w oparciu o urządzenia rodziny SYLAN, dla potrzeb Sił Zbrojnych RP. W związku z problemami firmy TechLab2000 (zastawienie dokumentacji systemu w zamian za zobowiązania finansowe), nie jest znany stan tego systemu. W trakcie realizacji zakupów urządzeń, utraciły one certyfikat (upłynął termin ważności), w związku z czym nie można przy ich użyciu przetwarzać informacji niejawnych, zgodnie z przeznaczeniem systemu. Wobec tego prawdopodobnym jest, że zrezygnowano z budowy tego systemu.
- System niejawnej łączności rządowej SYLAN (administracja rządowa) – opracowany i produkowany przez firmę TechLab[49]. Prawdopodobnie elementy

---

[47] Rozporządzenie Rady Ministrów z dnia 3 sierpnia 2004 r. *w sprawie przygotowania i wykorzystania…,* dz. cyt.

[48] Rozporządzenie Prezesa Rady Ministrów z dnia 16 września 2010 r. *w sprawie szczegółowych zasad wykonywania działalności telekomunikacyjnej w Sieci Łączności Rządowej* (Dz. U. z 2010 r., Nr 177, poz. 1192).

[49] http://www.tl2000.pl/produkty/system_sylan (dostęp 24.05.2013 r.). Ostatni element posiadający certyfikat kryptograficzny został usunięty z Wykazu obowiązujących certyfikatów, prowadzonego przez ABW, z dn. 13.05.2013 r. System Zarządzania Kluczami posiadał

tego systemu są wycofywane z użycia, ponieważ stacja zarządzania tym systemem nie znajduje się już na liście urządzeń certyfikowanych, prowadzonej przez ABW.

Poniżej przedstawione zostały informacje na temat Sieci Łączności Rządowej, która stanowi podstawowy system łączności, przeznaczony do kierowania państwem i bezpieczeństwem narodowym.

Sieć Łączności Rządowej

Sieć Łączności Rządowej (SŁR) – to sieć telekomunikacyjna, w ramach której świadczone mają być usługi telekomunikacyjne, obejmujące łączność głosową, video- i telekonferencje, transmisję danych oraz inne usługi[50]. Sieć SŁR składa się z dwóch części:

- System jawny – przeznaczony do przekazywania informacji nie stanowiących informacji niejawnych, w rozumieniu ustawy o ochronie informacji niejawnych z 2010 r. Operatorem części jawnej jest minister właściwy do spraw wewnętrznych, natomiast organizatorem jest Komendant Główny Policji[51].
- System niejawny – wydzielony system w ramach SŁR, przeznaczony do przetwarzania informacji niejawnych, wykorzystujący narzędzia i urządzenia kryptograficzne do zapewnienia bezpieczeństwa i integralności. System umożliwiający przetwarzanie informacji o klauzuli do „Tajne" (część stacjonarna) oraz „Poufne" (część mobilna). Organizatorem systemu niejawnego jest Szef Agencji Bezpieczeństwa Wewnętrznego.

System SŁR przeznaczony jest dla jednostek administracji rządowej w głównych lub zapasowych stanowiskach kierowania. Użytkownikami systemu są[52]:

- Prezydent Rzeczypospolitej Polskiej;
- Prezes i wiceprezesi Rady Ministrów;
- Marszałek i wicemarszałkowie Sejmu oraz Senatu;
- Szef Kancelarii Prezydenta Rzeczypospolitej Polskiej;

---

certyfikat umożliwiający przetwarzanie informacji niejawnych do klauzuli „TAJNE", ważny do dn. 22.05.2013 r.

[50] Rozporządzenie Rady Ministrów z dnia 3 sierpnia 2004 r. *w sprawie przygotowania i wykorzystania*…, dz. cyt., § 1.

[51] Tamże, § 5. 1.

[52] Tamże, § 4. 2.

- Szef Kancelarii Prezesa Rady Ministrów;
- ministrowie, sekretarze i podsekretarze stanu w urzędach administracji rządowej;
- sekretarze i podsekretarze stanu w Kancelarii Prezydenta;
- sekretarze i podsekretarze stanu w Kancelarii Prezesa Rady Ministrów;
- Szefowie Kancelarii Sejmu i Kancelarii Senatu;
- wojewodowie i ich zastępcy;
- Szef Biura Bezpieczeństwa Narodowego i jego zastępcy;
- Prezes i wiceprezesi Rządowego Centrum Legislacji;
- Prokurator Generalny i jego zastępcy;
- Prezes i wiceprezesi Prokuratorii Generalnej;
- Dyrektor Rządowego Centrum Bezpieczeństwa i jego zastępcy;
- przewodniczący senackich komisji: Spraw Zagranicznych, Gospodarki Narodowej oraz Obrony Narodowej;
- przewodniczący sejmowej Komisji do Spraw Służb Specjalnych;
- Szef Sztabu Generalnego Wojska Polskiego i jego zastępcy oraz dowódcy rodzajów Sił Zbrojnych RP;
- Szef Agencji Bezpieczeństwa Wewnętrznego i jego zastępcy oraz w zakresie SŁR-N dyrektorzy jednostek organizacyjnych Agencji Bezpieczeństwa Wewnętrznego i ich zastępcy;
- Szef Agencji Wywiadu i jego zastępcy;
- Szef Służby Kontrwywiadu Wojskowego i jego zastępcy;
- Szef Służby Wywiadu Wojskowego i jego zastępcy;
- Szef Centralnego Biura Antykorupcyjnego i jego zastępcy;
- Szef Biura Ochrony Rządu i jego zastępcy;
- Komendant Główny Państwowej Straży Pożarnej i jego zastępcy oraz komendanci wojewódzcy;
- Komendant Główny Straży Granicznej i jego zastępcy oraz komendanci oddziałów;
- Komendant Główny Policji, Komendant Stołeczny Policji i ich zastępcy, komendanci wojewódzcy oraz kierownicy komórek organizacyjnych Policji właściwych w sprawach łączności;
- Szef Obrony Cywilnej i jego zastępcy;
- kierownicy urzędów administracji rządowej oraz ich zastępcy;
- Dyrektor Generalny Służby Więziennej i jego zastępcy;
- dyrektorzy generalni w urzędach administracji rządowej;
- dyrektorzy statutowych jednostek Kancelarii Prezydenta oraz jednostek organizacyjnych Biura Bezpieczeństwa Narodowego;

- kierownik komórki organizacyjnej właściwej w sprawach teleinformatyki urzędu obsługującego operatora SŁR.

Przedstawiony zakres osób funkcyjnych jest bardzo szeroki. Nie obejmuje jednak jednostek samorządu terytorialnego, które również tworzą stanowiska kierowania dla swoich organów wykonawczych[53]. W szczególnie uzasadnionych przypadkach istnieje jednak możliwość zainstalowania tym organom urządzeń końcowych, umożliwiających dostęp do SŁR, zgodnie z § 10.1. Rozporządzenia w sprawie przygotowania i wykorzystania systemów łączności. Zapis ten umożliwia dołączenie stanowisk kierowania zlokalizowanych na poziomie samorządu terytorialnego do systemu SŁR.

System jawny zbudowany jest w oparciu o komercyjne końcówki telekomunikacyjne, takie jak[54]:

- przewodowe aparaty telefoniczne analogowe;
- aparaty telefoniczne sekretarsko-dyrektorskie;
- urządzenia dyspozytorskie;
- przewodowe aparaty telefoniczne cyfrowe;
- terminale wideokonferencyjne;
- urządzenia łączności ruchomej;
- aparaty telefoniczne systemowe zgodne ze specyfikacją techniczną centrali telefonicznej SŁR.

Pomimo, iż dokumentacja części jawnej systemu nie podlega ochronie, to dostęp do dokumentacji jest ograniczony. Jest to zrozumiałe i jak najbardziej słuszne podejście. Zbyt szerokie publikowanie informacji technicznych oraz procedur korzystania z takiego systemu, może wpłynąć negatywnie na jego bezpieczeństwo. Przedstawione informacje techniczne znajdowały się w projekcie załącznika, jednak w tekście opublikowanego rozporządzenia został on pominięty. Wynika jednak z niego (projektu), iż SŁR jawny to wydzielona sieć telekomunikacyjna, posiadająca zabezpieczenia fizyczne, po stronie abonenckiej, jak i na łączach (ochrona elementów sieciowych). Należy jednak przypuszczać, że w dzisiejszych czasach takie

[53] Rozporządzenie Rady Ministrów z dnia 27 kwietnia 2004 roku *w sprawie przygotowania systemu kierowania*…, dz. cyt., § 11. ust. 1. pkt 6.

[54] Warunki techniczne, niezbędne do spełnienia w celu dołączenia do SŁR znajdowały się w projekcie rozporządzenia Prezesa Rady Ministrów w sprawie szczegółowych zasad wykonywania działalności telekomunikacyjnej w Sieci Łączności Rządowej (załącznik nr 1), opublikowany na stronie http://bip.msw.gov.pl/download/4/5531/Rozp_SLR_wer_02_11_09.pdf. (dostęp 26.05.2013 r.).

zabezpieczenia są niewystarczające dla zapewnienia bezpieczeństwa i wiarygodności informacjom przekazywanym między poszczególnymi organami władzy. Autor jest zwolennikiem stosowania zabezpieczeń kryptograficznych również dla ochrony informacji jawnych, szczególnie w zakresie ich integralności i wiarygodności. Opis części niejawnej systemu, która miała być zbudowana z urządzeń wykorzystujących mechanizmy kryptograficzne, został całkowicie usunięty z rozporządzenia. Zapewne znalazł się w dokumentach niejawnych (dokumentacja bezpieczeństwa i bezpiecznej eksploatacji) wytworzonych przez organizatora systemu (ABW).

Cześć niejawna SŁR zbudowana jest z urządzeń realizujących ochronę informacji z wykorzystaniem mechanizmów kryptograficznych. Wykorzystanie urządzeń do kryptograficznej ochrony informacji wynika z zapisów ustawy o ochronie informacji niejawnych[55]. W związku z tym powinny one (urządzenia i systemy ochrony informacji) znajdować się na liście urządzeń posiadających certyfikat bezpieczeństwa kryptograficznego, wydany przez ABW lub SKW. W związku z brakiem szczegółowych informacji na temat tego systemu, można posłużyć się jedynie informacjami zawartymi w materiałach prasowych oraz dokumentacji przetargowej. Początkowo system niejawny zbudowany był w oparciu o urządzenia systemu SYLAN, firmy TechLab2000. Jednak w roku 2013 wygasł certyfikat bezpieczeństwa kryptograficznego dla ostatniego elementu systemu (Stacja Zarządzania Kluczami), co prawdopodobnie spowodowało (lub spowoduje w najbliższym czasie) wycofanie ich z eksploatacji. Organizator systemu niejawnego (ABW) rozpoczął w roku 2009 prace nad nowymi urządzeniami[56] ochrony informacji, które miały zastąpić poprzednie. W efekcie w 2012 roku uruchomiono nowoczesny system łączności niejawnej. System ten nosi nazwę CATEL i umożliwia przetwarzanie informacji o klauzuli do „Poufne" włącznie. System działa w oparciu o sieć komórkową GSM, jednak jest niezależny od operatora komórkowego. Mechanizmy bezpieczeństwa zaimplementowane w urządzeniach systemu zapewniają identyfikację i uwierzytelnienie użytkowników, oraz poufność przesyłanych danych. Urządzeniami łączności są telefony komórkowe oraz laptopy. Pojemność systemy wynosi ok. 3500 telefonów i 400-500 laptopów. Zastosowany system kryptograficzny jest w całości produktem polskim, opracowanym przez specjalistów ABW. Całość infrastruktury odpowiedzialnej za bezpieczeństwo jest zarządzana przez Agencję, co gwarantu-

[55] Ustawa z dnia 5 sierpnia 2010 r. *o ochronie informacji...*, dz. cyt., art. 48, ust. 1., art. 50, ust. 2.

[56] Agencja Bezpieczeństwa Wewnętrznego, Raport z działalności ABW w 2010 roku, Warszawa 2011, s. 8–9.

je bezpieczeństwo danych wrażliwych[57]. Właścicielem zastosowanych rozwiązań (technicznych i programowych) jest Skarb Państwa, co powinno zapewnić proces utrzymania systemu (konserwacji, serwisowania i modernizacji), jak również podnieść jego bezpieczeństwo. Właśnie utrzymanie systemu (ważność certyfikatu bezpieczeństwa kryptograficznego) jest niezmiernie ważne, ponieważ wymagane jest odnawianie certyfikatu ze względu na postęp technologiczny w obszarze technologicznym i w obszarze Kryptoanaliza. Firmy komercyjne, posiadające urządzenia ochrony informacji w swojej ofercie, mogą zaniechać utrzymywania certyfikatu, ze względu na duże koszty oraz mały popyt na nowe urządzenia. System CATEL nie znajduje się na liście urządzeń certyfikowanych (prowadzonej przez ABW), uzyskał jednak akredytację i został wdrożony do eksploatacji. Na chwilę obecną jest prawdopodobnie jedynym systemem łączności niejawnej eksploatowanym przez administrację.

Zarządzanie kryzysowe

Analizując obszar zarządzania kryzysowego, autor nie napotkał informacji o zastosowaniu kompleksowego rozwiązania teleinformatycznego, którego zadaniem byłoby wspomaganie zarządzania kryzysowego. Ustawa o zarządzaniu kryzysowym[58] nie określa narzędzi, jakie mogą (lub powinny) być wykorzystane do zapewnienia wsparcia organów realizujących proces zarządzania ani systemów łączności, jakie powinny być przygotowane. Określa jedynie, że plan zarządzania kryzysowego powinien zawierać organizację łączności[59], bez sprecyzowania jak i za pomocą jakich środków. Jednym z zadań centrów zarządzania kryzysowego, jest zapewnienie przepływu informacji, w celu zapewnienia współdziałania w zakresie informowania i przekazywania poleceń[60]. Zgodnie z Rozporządzeniem Rady Ministrów w sprawie określenia organów administracji rządowej, które utworzą centra zarządzania kryzysowego oraz sposobu ich funkcjonowania[61], nakłada się na centra

[57] Dane wrażliwe to dane niezbędne do poprawnej i bezpiecznej pracy systemu ochrony informacji.

[58] Ustawa z dn. 26 kwietnia 2007 r. *o zarządzaniu kryzysowym* (Dz. U. z 2007 r., Nr 89, poz. 590).

[59] Tamże, art. 5, ust. 2. pkt 3, lit. b.

[60] Tamże, art. 13, ust. 2, pkt 1 i 8.

[61] Rozporządzenie Rady Ministrów z dnia 15 grudnia 2009 r. *w sprawie określenia organów administracji rządowej, które utworzą centra zarządzania kryzysowego oraz sposobu ich funkcjonowania* (Dz. U. Nr 226 poz. 1810).

obowiązek ciągłości działania i zapewnienia łączności w sytuacjach awaryjnych (§ 4.1, pkt 1 i 2). W związku z tym, iż brak jest wskazań co do sposobu realizacji procesu informowania, można założyć, że do komunikacji będą wykorzystywane powszechnie dostępne media, takie jak powszechna sieć Internet, łączność przewodowa (operatorzy publiczni), sieci komórkowe, sieci radiowe. Brak takich uregulowań może być zaletą, ponieważ umożliwia swobodny wybór środków łączności oraz narzędzi wspomagających, jak również może być przyczyną problemów w ich integracji z innymi systemami.

Prawdopodobnie pierwszą próbą wykorzystania ogólnokrajowego systemu informatycznego do wspomagania zarządzania było wdrożenie systemu Euromaster 2012. System ten został wdrożony przez spółkę PL.2012 z przeznaczeniem wspomagania zarządzania imprezą masową, jaką był turniej piłkarski EURO 2012.

W celu usprawnienia komunikacji i informacji zarządczej oraz uproszczenia procesu raportowania w ramach struktur koordynacyjno-zarządczych przewidzianych na czas Turnieju, w maju 2012 r. spółka PL.2012 wdrożyła system Euromaster. Zadaniem systemu było dostarczanie czytelnych i aktualnych informacji na temat bieżącej sytuacji w danym obszarze. Dostęp do odczytu informacji zawartych w systemie mieli pracownicy wszystkich podmiotów publicznych biorących udział w organizacji imprezy. Odpowiedzialne za zasilanie systemu danymi były następujące podmioty: Krajowy Sztab Operacyjny, Sztaby Miejsko-Wojewódzkie, Sztab MSW/MAiC, Sztab MTBiGM, Sztab MZ[62].

System Euromaster zapewniał zbieranie i raportowanie informacji o zdarzeniach oraz udostępniał informacje za pośrednictwem przeglądarki internetowej, oraz aplikacji osadzonej na smartfonach.

Raportowanie doraźne odbywało się przede wszystkim z wykorzystaniem narzędzia EuroMaster oraz drogą mailową. Zaletą aplikacji EuroMaster była bieżąca dostępność aktualnej informacji zarówno pod kątem poszczególnych obszarów organizacyjnych jak i miejsc operacji turniejowej bieżąco dla wszystkich użytkowników systemu. Jakość raportowania doraźnego, a szczególnie czas po jakim informacja o zdarzeniu docierała do CO KSzO różniła się znaczenie w zależności od podmiotu/struktury, który/a dostarczał/a informacje[63].

Od dnia 04.06 do 01.07.2012 r. do EuroMaster wpisano ponad 8 tysięcy komunikatów i zapisano ponad 300 zdarzeń[64].

---

[62] Sprawozdanie z realizacji przedsięwzięć EURO 2012 oraz z wykonanych działań dotyczących realizacji przygotowań Polski do finałowego turnieju Mistrzostw Europy w Piłce Nożnej UEFA EURO 2012 (styczeń–grudzień 2012 r.), s. 7–8.

[63] Tamże, s. 87.

[64] Tamże, s. 90.

Z dostępnych informacji wynika, iż system sprawdził się, jednak nie podjęto działań zmierzających do jego wdrożenia na poziomie ogólnokrajowym. Można wyrazić tylko żal, iż nie wykorzystano szansy na przetestowanie tego systemu w skali kraju (przynajmniej pilotażowo). Nadal podstawowym sposobem przekazywania informacji pozostają środki telekomunikacyjne oraz poczta elektroniczna. Jednak wobec rosnącego zagrożenia w sferze cyberprzestrzeni należy rozważyć ich bezpieczeństwo, zarówno pod kątem wiarygodności stron komunikacji, jak i samej informacji.

Wobec braku informacji o systemie ogólnokrajowym (pomimo wysłania zapytania do Rządowego Centrum Bezpieczeństwa), przeprowadzono poszukiwania aplikacji i systemów informatycznych, które mogą znaleźć zastosowanie w zarządzaniu kryzysowym.

Wśród zidentyfikowanych narzędzi można wymienić:

- produkty firmy GeoInvent: Zapora i Mapa porządku[65];
- system wspomagania reagowania kryzysowego Alaska, opracowany przez resortowe Centrum Zarządzania Projektami Informatycznymi[66];
- system C3M, wykorzystywany przez Wielkopolski Urząd Wojewódzki w Poznaniu oraz powiaty i gminy, jak również podmioty administracji zespolonej i niezespolonej[67];
- system DART firmy SPRINT S.A. – przeznaczony do wspomagania zarządzania centrum zarządzania kryzysowego[68].

Analizując cechy systemów wspomagania można zauważyć, iż głównymi funkcjami są zbieranie, agregacja i prezentowanie danych odnośnie sytuacji na podległym obszarze. Systemy mogą przetwarzać dane na temat sytuacji z różnych obszarów (porządek publiczny, sytuacja powodziowa, zagrożenia pożarowe, itp.), pochodzące od różnych jednostek. Mają zapewnić prawidłowy przepływ informacji między poszczególnymi jednostkami kierującymi, jak i wykonawczymi, oraz wspomóc efektywne dysponowanie środkami i siłami. Posiadają również funkcje prezentowania wariantów zagrożeń dla podanych danych, jak rów-

---

[65] Strona www.geoinvent.com.pl/zarzadzanie_kryzysowe.html (dostęp 29.05.2013 r.).

[66] Strona http://www.rczpi.wp.mil.pl/pl/50.html (dostęp 29.05.2013 r.).

[67] J. Dembny, *Wspomaganie zarządzania kryzysowego z wykorzystaniem elementów systemów informacji geograficznej – GIS – na przykładzie rozwiązań opracowanych w województwie wielkopolskim*, publikacja Wydziału Bezpieczeństwa i Zarządzania Kryzysowego, WUW w Poznaniu (dostęp 29.05.2013 r.).

[68] http://www.sprint.pl/dart-czk.html (dostęp 30.05.2013 r.).

nież umożliwiają przywołanie danych archiwalnych (o ile takowe znajdują się w zasobach).

Wśród systemów wspomagających można wyróżnić:

- systemy wspomagające zarządzanie w sytuacjach zagrożeń naturalnych – np. Zapora, Alaska;
- systemy wspomagające zarządzanie w zabezpieczeniu imprez masowych – np. DART.

Należy również zwrócić uwagę, iż poziom struktury administracji, do którego maksymalnie stosowane i przeznaczone są wymienione systemy, to poziom województwa. Należy je traktować zatem jako narzędzia lokalne, umożliwiające wspomaganie działań terenowych organów administracyjnych. W sytuacjach zagrożeń obejmujących obszar więcej niż jednego województwa, powiatu lub gminy, należy liczyć się z pojawieniem się problemów w zakresie komunikacji i zarządzania zasobami. Wyjątkami będą te jednostki administracyjne, które wprowadziły wspólne środowisko narzędziowe na swoim obszarze oraz w jednostkach podległych (np. województwo wielkopolskie)[69]. Analizując materiały informacyjne na temat systemów wspomagania można zauważyć przewagę funkcji zbierania danych i zobrazowania, nad wymianą informacji i wspomaganiem podejmowania decyzji. Wspomaganie podejmowania decyzji rozumianym jako przedstawienie wariantów rozwoju sytuacji w aktualnym stanie zagrożenia.

Podsumowanie

Aktualnie administracja publiczna nie posiada kompleksowego systemu łączności, który integrowałby różne rodzaje usług, w ramach wspólnej sieci teleinformatycznej. Przedstawione systemy teleinformatyczne (poszczególnych służb) realizują zadania wspomagania kierowania (dowodzenia), w obszarze ich działania. Nie tworzą jednak rozwiązania kompleksowego, na skalę kraju. Brak jest mechanizmów komunikacji między nimi, przepływu danych oraz wspólnych procedur kierowania. Nie posiadają mechanizmów umożliwiających współdziałanie miedzy poszczególnymi służbami. Braki te nie wynikają z błędnego zaprojektowania, lecz z przyjętego zakresu działania – dla danej służby. Są nowymi rozwiązaniami (narzędziami), co stwarza możliwość ich integracji w jeden, ogólnokrajowy system, który prawdopodobnie wymagałyby rozbudowy o nowe moduły funkcjonalne, bez

[69] J. Dembny, *Wspomaganie zarządzania kryzysowego…*, dz. cyt., s. 2.

konieczności radykalnych zmian. Taki ewolucyjny proces rozwoju systemów wydaje się być właściwym kierunkiem rozwoju.

Prace konceptualne nad systemem ogólnokrajowym, nazwanym OCSŁ-STAP[70], prowadzone były od 2006 roku, kiedy to powołany został zespół międzyresortowy do opracowania koncepcji systemu teleinformatycznego na potrzeby administracji[71]. Zespół działał do roku 2008, w którym to nastąpiło przyjęcie sprawozdania z jego prac. W nawiązaniu do opracowanej koncepcji rozpoczęto prace nad koncepcją systemu OCSŁ-STAP, prowadzone przez Centrum Projektów Informatycznych MAiC. Prace te nie wyszły jednak poza sferę konceptualną. Jednym z celów tego systemu było zwiększenie bezpieczeństwa przetwarzanych informacji, poprzez zastosowanie mechanizmów kryptograficznych. Świadczy to o dostrzeżeniu wagi zagrożeń, jakie występują dla danych przetwarzanych za pośrednictwem rozległych sieci teleinformatycznych. Z drugiej strony nie ma dziś alternatywy dla tego rodzaju systemów, zarówno technologicznych, jak i ekonomicznych. Z dostępnych informacji można wywnioskować, iż realizacja projektu OCSŁ-STAP (wstrzymanego) będzie kontynuowana w ramach systemu OST112, który ma potencjalną możliwość (pojemność) integracji sieci administracji publicznej. Być może wykorzystanie systemu OSR112 znajdzie się w zaktualizowanej koncepcji systemu łączności, której ma dokonać zespół międzyresortowy, powołany przez Ministra Administracji i Cyfryzacji[72]. Do zadań zespołu należy […] *przegląd i aktualizacja dokumentu „Koncepcja organizacji Systemu Łączności na potrzeby administracji publicznej, systemu kierowania bezpieczeństwem narodowym, bezpieczeństwem i porządkiem publicznym oraz potrzeby ratownictwa"* […][73]. Będzie to kontynuacja prac poprzedniego zespołu, który opracował dokument. Dodatkowo zespół ma opracować wymagania techniczno-eksploatacyjne dla urządzeń, które będą wykorzystywane dla organizacji systemu łączności. Rozpoczęcie prac zespołu, może być początkiem kolejnego etapu

---

[70] Ogólnopolski Cyfrowy System Łączności – System Teleinformatyczny Administracji Publicznej.

[71] Zarządzenie nr 89 Prezesa Rady Ministrów z dnia 1 czerwca 2006 r. w *sprawie utworzenia Międzyresortowego Zespołu do spraw opracowania programu zapewnienia łączności na potrzeby administracji publicznej, systemu kierowania bezpieczeństwem narodowym, bezpieczeństwem i porządkiem publicznym oraz na potrzeby ratownictwa*, Biuletyn Informacji Publicznej Kancelarii PRM.

[72] Zarządzenie nr 9 Ministra Administracji i Cyfryzacji z dnia 19 kwietnia 2013 r. *w sprawie powołania Międzyresortowego Zespołu do spraw organizacji systemu łączności na potrzeby systemu kierowania bezpieczeństwem narodowym*, Dz. Urzędowy MAiC, Warszawa, 24.04.2013 r., poz. 12.

[73] Tamże, §1 ust. 2 pkt 1.

rozwoju nowoczesnego i kompleksowego systemu łączności dla potrzeb kierowania bezpieczeństwem.

W obszarze zarządzania kryzysowego niezbędna wydaje się zmiana podejścia, tj. zintegrowanie prawne stanowisk zarządzania z systemem kierowania BN. Uregulowanie prawne tego zagadnienia pozwoli na zwiększenie efektywności działania i wykorzystania dostępnych sił i środków, zarówno militarnych, jak i pozamilitarnych. Skróci również czas wprowadzenia do działań jednostek ministerstwa obrony, do usuwania zagrożeń lub zapobiegania im. Należy rozważyć również zmianę podejścia do zarządzania środkami i siłami będącymi w dyspozycji centrów zarządzania kryzysowego, z zarządzania posiadanymi zasobami na zarządzanie potencjałem sił i środków do usuwania poszczególnych zagrożeń lub ich skutków. Taki sposób zobrazowywania posiadanych sił i środków może zwiększyć efektywność dysponowania nimi, zapobiegać zbędnemu blokowaniu zasobów w odwodzie, jak również przesuwać je między likwidowanymi zagrożeniami.

W środowisku naukowym prowadzone były prace nad wykorzystaniem systemów informatycznych w procesie zarządzania bezpieczeństwem narodowym. Prace badawcze nad tym problemem prowadzone były w 2009 roku przez Instytut Łączności. Była to praca statutowa, w wyniku której powstało opracowanie „Aplikacje informatyczne dla Systemu Kierowania Bezpieczeństwem Narodowym”[74]. Pomimo wysłania prośby o dostęp do pracy, autorowi nie udało się uzyskać żadnej odpowiedzi.

Podsumowując rozważania na temat systemów teleinformatycznych wspomagania zarządzania bezpieczeństwem narodowym należy stwierdzić, iż opracowanie i wdrożenie kompleksowego, bezpiecznego i nowoczesnego systemu jest warunkiem niezbędnym do prawidłowego funkcjonowania systemu kierowania bezpieczeństwem narodowym. System ten powinien być opracowany przez polskie środowisko naukowe i zrealizowany przez polskie firmy, pod nadzorem właściwych służb (ABW, SKW). Wykorzystanie krajowego potencjału i myśli, zapewni pełną weryfikowalność i kontrolę zastosowanych mechanizmów bezpieczeństwa oraz ich realizację. Zapewni również utrzymanie go na właściwym poziomie bezpieczeństwa. Realizacja wymagać będzie dużych nakładów finansowych, ponieważ opracowanie systemów zabezpieczeń jest kosztowne i czasochłonne. Jednak, zdaniem autora, poniesione nakłady przyczynią się do zwiększenia efektywności funkcjonowania Systemu Kierowania Bezpieczeństwem Narodowym.

---

[74] B. Kowalczyk, B. Chojnacki, P. Godlewski, i in., *Aplikacje informatyczne dla Systemu Kierowania Bezpieczeństwem Narodowym, Instytut Łączności-Państwowy Instytut Badawczy, Praca statutowa*, Warszawa 2009.

***

Keywords: national security, management, crisis management, system management, government's communications system

SUMMARY

The article presents the problem of supporting the process of national security management by specialized ICT tools. There are analyzes the system industry, ability and potential use in SK BN in the article. Author accents needs to implement a national ICT system for management of security. The variety of currently used communication and telecommunications systems, does not satisfy the postulate of complexity and the system properties. Author draws attention to the need for regulation of co-ordination and management system BN management crisis management system. Advocates the inclusion of disaster management to such a system.

Bibliografia

Agencja Bezpieczeństwa Wewnętrznego, Raport z działalności ABW w 2010 roku, Warszawa 2011.

Centrum Projektów Informatycznych, książka o projekcie OST112, Warszawa 2012, www.cpi.gov.pl.

Dembny J., *Wspomaganie zarządzania kryzysowego z wykorzystaniem elementów systemów informacji geograficznej – GIS – na przykładzie rozwiązań opracowanych w województwie wielkopolskim*, publikacja Wydziału Bezpieczeństwa i Zarządzania Kryzysowego, WUW w Poznaniu 2010.

Kitler W., *Bezpieczeństwo narodowe RP. Podstawowe kategorie. Uwarunkowania. System*, AON, Warszawa 2011.

Kowalczyk B., Chojnacki B., Godlewski P., i inni, *Aplikacje informatyczne dla Systemu Kierowania Bezpieczeństwem Narodowym*, Instytut Łączności-Państwowy Instytut Łączności, Warszawa 2009.

Kuraś M., *System informacyjny – system informatyczny. Co poza nazwą różni te dwa obiekty?*, „Zeszyty Naukowe Akademii Ekonomicznej w Krakowie" 2004.

Machnacz M., *Bezpieczeństwo aktywów ministerstwa spraw wewnętrznych i administracji w infrastrukturze krytycznej państwa*, [w:] *Bezpieczeństwo w telekomunikacji i teleinformatyce*, red. B. Lent, Tom 3, Wydawnictwo BBN, Warszawa 2008.

Olejnik K., Maciejewski M., *Dyżurny jednostki organizacyjnej policji (materiał dydaktyczny)*, Słupsk 2013.

Rawski M., *Informatyczny System Wspomagania Kierowania Straży Granicznej*, „Zeszyty Naukowe Wydziału Zarządzania i Dowodzenia AON" 2012, nr 1, Warszawa 2012.

Sienkiewicz P., *Analiza systemowa i podstawy jej zastosowania*, Wydawnictwo Bellona, Warszawa 1994.
Sienkiewicz P., *Inżynieria systemów*, Wydawnictwo MON, Warszawa 1983.
Słownik terminów z zakresu bezpieczeństwa narodowego, Akademia Obrony Narodowej, red. W. Łepkowski, wydanie czwarte, Warszawa 2009.

Akty prawne:

Rozporządzenie Rady Ministrów z dnia 27 kwietnia 2004 r. *w sprawie przygotowania systemu kierowania bezpieczeństwem narodowym* (Dz. U. z 2004 r., Nr 98 poz. 978).
Rozporządzenie Rady Ministrów z dnia 3 sierpnia 2004 r. *w sprawie przygotowania i wykorzystania systemów łączności na potrzeby obronne państwa* (Dz. U. Nr 180, poz. 1855).
Rozporządzenie Prezesa Rady Ministrów z dnia 16 września 2010 r. *w sprawie szczegółowych zasad wykonywania działalności telekomunikacyjnej w Sieci Łączności Rządowej* (Dz. U. Nr 177 z 2010 r., poz. 1192).
Rozporządzenie Rady Ministrów z dnia 15 grudnia 2009 r. *w sprawie określenia organów administracji rządowej, które utworzą centra zarządzania kryzysowego oraz sposobu ich funkcjonowania* (Dz. U. Nr 226 poz. 1810).
Strategia Rozwoju Systemu Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej 2022, przyjęta uchwałą nr 67 Rady Ministrów z dnia 9 kwietnia 2013 r., Monitor Polski z 16 maja 2013 poz. 377.
Ustawa z dn. 26 kwietnia 2007 r. *o zarządzaniu kryzysowym* (Dz. U. z 2007r., Nr 89 poz. 590).
Ustawa z dnia 16 lipca 2004 r. *Prawo telekomunikacyjne* (Dz. U. z 2004 r., Nr 171, poz. 1800, z późn. zm.).
Ustawa z dnia 5 sierpnia 2010 r. *o ochronie informacji niejawnych* (Dz. U. z 2010 r., Nr 182 poz. 1228).
Ustawa z dnia 29 sierpnia 1997 r. *o ochronie danych osobowych* (Dz. U. 1997 nr 133 poz. 883).
Ustawa z dnia 18 lipca 2002 r. *o świadczeniu usług drogą elektroniczną* (Dz. U. z 2002 r., Nr 144, poz. 1204 ze zm.).
Ustawa z dnia 17 stycznia 2007 roku *o ustanowieniu „Programu modernizacji Policji, Straży Granicznej, Państwowej Straży Pożarnej i Biura Ochrony Rządu w latach 2007-2009"* (Dz. U. z 2007 r., Nr 35, poz. 213).
Zarządzenie nr 89 Prezesa Rady Ministrów z dnia 1 czerwca 2006 r. *w sprawie utworzenia Międzyresortowego Zespołu do spraw opracowania programu zapewnienia łączności na potrzeby administracji publicznej, systemu kierowania bezpieczeństwem narodowym, bezpieczeństwem i porządkiem publicznym oraz na potrzeby ratownictwa,* Biuletyn Informacji Publicznej Kancelarii Prezesa Rady Ministrów.
Zarządzenie nr 9 Ministra Administracji i Cyfryzacji z dnia 19 kwietnia 2013 r. *w sprawie powołania Międzyresortowego Zespołu do spraw organizacji systemu łączności na potrzeby systemu kierowania bezpieczeństwem narodowym*, Dz. Urzędowy MAiC, Warszawa, 24.04.2013 r., poz. 12.

Strony internetowe:

www.stat.gov.pl/cps/rde/xbcr/bip/BIP_wykaz_systemow_informacyjnych_administracji_publicznej_2013.pdf.

www.swdst.pl/index.php/info, http://www.abakus.net.pl/products/swdst25.html.

www.cpi.gov.pl/files/fck/File/konferencje/SIPR_marzec_2011/I_Konf_SIPR_System_Wspomagania_Dowodzenia_Policji.pdf.

Ministerstwo Sportu i Turystyki, Sprawozdanie z realizacji przedsięwzięć EURO 2012 oraz z wykonanych działań dotyczących realizacji przygotowań Polski do finałowego turnieju Mistrzostw Europy w Piłce Nożnej UEFA EURO 2012 (styczeń–grudzień 2012 r.), http://www.msport.gov.pl/sprawozdania-z-realizacji-przedsiewziec-euro-2012.

www.geoinvent.com.pl/zarzadzanie_kryzysowe.html.

www.rczpi.wp.mil.pl/pl/50.html.

www.sprint.pl/dart-czk.html.