Sieci i usługi telekomunikacyjne w zarządzaniu kryzysowym

Bolesław Kowalczyk,
Marian Kowalewski, Henryk Parapura

W artykule opisano zasady obiegu informacji, charakterystykę sieci łączności elektronicznej oraz propozycję wykorzystania nowoczesnych usług telekomunikacyjnych w procesie zarządzania kryzysowego.

zarządzanie kryzysowe, sieci łączności elektronicznej zarządzania kryzysowego, usługi telekomunikacyjne dla zarządzania kryzysowego

Wprowadzenie

Burzliwy rozwój wszystkich dziedzin życia, rozwój gospodarki, a także występujące w ostatnich latach gwałtowne zjawiska atmosferyczne, powodują szereg zdarzeń mających znamiona katastrof, których skutki są tragiczne dla ludności. Działania polegające głównie na ograniczaniu następstw takich zdarzeń, ostrzeganiu ludności, ratownictwie poszkodowanych i przywracaniu warunków normalnego funkcjonowania gospodarki i bytowania ludności, wymagają wielkiego wysiłku zarówno zespołów ratowniczych, służb publicznego bezpieczeństwa, jak i organów zarządzania kryzysowego. W takich warunkach niezbędna jest informacja, której przekazanie właściwemu adresatowi w odpowiednim czasie, decyduje o powodzeniu akcji.

Podstawowym warunkiem efektywnego zarządzania kryzysowego jest umiejętność zorganizowania współpracy oraz sprawnej koordynacji i dowodzenia (kierowania) działaniami wielu podmiotów biorących udział zarówno w akcjach ratunkowych, jak również w pracach planistycznych i zapobiegawczych. Niezmiernie istotnym elementem tych działań jest możliwość wymiany informacji o sytuacji kryzysowej① między tymi podmiotami, w sposób szybki i dokładny. Informacja, kiedy i gdzie powstało zagrożenie oraz ocena potencjalnych skutków dla otoczenia, umożliwia wypracowanie najskuteczniejszych sposobów działania (decyzji) prowadzących do eliminacji i zmniejszenia spowodowanych nim strat. Przekaz informacji musi przy tym charakteryzować się określonym standardem w celu zachowania kompatybilności współpracy poszczególnych podmiotów [5].

Ogromne znaczenie dla sprawnej realizacji funkcji związanych z przekazywaniem i przetwarzaniem informacji ma właściwie zorganizowany system łączności. W sytuacjach nadzwyczajnych zagrożeń musi to być system zapewniający sprawny przekaz i przetwarzanie informacji między elementami szeroko rozumianego systemu ochrony ludności [1].

① *W opracowaniach dotyczących bezpieczeństwa używa się wymiennie pojęć kryzys i sytuacja kryzysowa. Kryzys interpretowany jest jako zdarzenie zerwania stabilności funkcjonowania określonego, istniejącego układu (stanu rzeczy, porządku), natomiast zjawiska po nim następujące, aż do uzyskania stabilności w nowej sytuacji (zazwyczaj jakościowo innej) określane są jako sytuacja kryzysowa [2].*

Obieg informacji jako warunek sprawnego funkcjonowania systemu zarządzania kryzysowego

Sprawne funkcjonowanie centrów zarządzania kryzysowego (CZK) wszystkich szczebli w systemie zarządzania kryzysowego możliwe jest gdy:

- są zapewnione warunki do ciągłego funkcjonowania systemu łączności (wspomagającego ratownictwo i zarządzanie kryzysowe), który powinien być włączony w system ogólnokrajowy,
- określono standardy systemów informatycznych, baz danych, map cyfrowych oraz systemu informacyjnego (m.in. dotyczące formy i sposobu przekazywanej informacji),
- istnieje ściśle zorganizowany system pozyskiwania i przekazywania informacji, do szczebla centralnego włącznie,
- jest określony sposób zbierania informacji (np.: z systemów monitorowania i wykrywania zagrożeń),
- są określone sposoby ostrzegania i alarmowania ludności (m.in. radio, telewizja - teletekst, internet i inne).

Skala wymiany informacji między podmiotami i uczestnikami systemu zarządzania kryzysowego województwa (powiatu, gminy) obsługiwanych przez CZK jest zależna od lokalnych uwarunkowań i zagrożeń. Potrzeby informacyjne organów bezpieczeństwa, ratownictwa i zarządzania kryzysowego sprowadzają się głównie do:

- przekazywania informacji w celu realizacji bieżących działań zmierzających do utrzymania w gotowości personelu i odpowiednio zorganizowanych służb,
- przyjmowania i obsługi zgłoszeń o zdarzeniach i katastrofach,
- przyjmowania i przekazywania informacji z systemów monitorowania i wykrywania zagrożeń,
- obsługi zdarzeń i katastrof,
- zarządzania siłami i środkami (kierowanie, dowodzenie i współdziałanie),
- alarmowania i ostrzegania ludności.

Istotą zarządzania kryzysowego jest działalność realizowana w czterech następujących po sobie fazach [1]:

- zapobiegania,
- przygotowania,
- reagowania,
- odbudowy.

Każdą fazę tego procesu cechuje inny jakościowo rodzaj zadań realizowanych przy jednoczesnej wymianie informacji za pomocą technicznych środków łączności ze zmiennym natężeniem ruchu telekomunikacyjnego zarówno w ramach funkcji wewnętrznych, jak i zewnętrznych.

System łączności zarządzania kryzysowego powinien być gotowy do funkcjonowania:

- w trybie zwyczajnym, polegającym na całodobowym zarządzaniu lokalnymi zdarzeniami przy wykorzystaniu rozwiniętych stanowisk kierowania służb ratowniczych współpracujących ze stanowiskiem koordynującym (centrum zarządzania kryzysowego),
- w trybie kryzysowym (w sytuacjach nadzwyczajnych zagrożeń), gdy lokalne zdarzenia zaczynają rozwijać się w lokalny kryzys uniemożliwiający postępowanie według przyjętych procedur działania, co wymaga podjęcia szczególnych działań.

W czasie rutynowych działań organów zarządzania kryzysowego są wykorzystywane głównie usługi telekomunikacyjne świadczone przez lokalnych operatorów. W niewielkim zakresie wykorzystuje się w codziennej działalności usługi systemów wewnętrznych (specjalnego przeznaczenia) lub sieci radiowe (nie dotyczy jednak służb ratowniczych i publicznego bezpieczeństwa, które w swoich rutynowych działaniach korzystają z własnych systemów łączności, głównie radiowej).

Ocenia się, że w czasie rutynowych działań organów zarządzania kryzysowego około 70% informacji jest przekazywanych za pomocą stacjonarnych sieci telefonicznych, 15% przez publiczne sieci łączności ruchomej, 7% przez sieci radiowe PMR (*Professional Mobile Radio*) i 8% za pomocą poczty elektronicznej.

Służby ratownicze i publicznego bezpieczeństwa w większym stopniu wykorzystują sieci radiowe PMR, gdyż około 50% informacji jest przekazywanych tą drogą. W nieco mniejszym stopniu wykorzystują natomiast stacjonarne sieci telefoniczne, za ich pomocą przekazują około 45% informacji.

W ostatnich latach zauważa sie wzrost wykorzystywania poczty elektronicznej do przesyłania wiadomości o różnej treści i przeznaczeniu, szczególnie w sieciach lokalnych (LAN), a także w sieciach rozległych (WAN). W kolejnych latach należy oczekiwać znacznego wzrostu wykorzystania różnych, nowoczesnych usług łączności elektronicznej przez służby publicznego bezpieczeństwa, ratownictwa i organa zarządzania kryzysowego.

Sieci łączności elektronicznej dla zarządzania kryzysowego

System zarządzania kryzysowego nie dysponuje obecnie przeznaczonymi do tego celu sieciami łączności elektronicznej[①]. Doświadczenia ostatnich lat pokazują jednak, że należy podjąć działania w celu zorganizowania takich sieci. Efektywnym rozwiązaniem jest organizacja sieci łączności elektronicznej dla zarządzania kryzysowego na obszarach województw. Na potrzeby centrów zarządzania kryzysowego w województwie (wojewódzkiego, powiatowych/miejskich i gminnych) powinny być zorganizowane następujące sieci:

- łączności telefonicznej,
- łączności radiowej,
- informatyczne (lokalne i WAN), zapewniające dostęp do różnych aplikacji wspomagania procesów decyzyjnych i zarządzania informacją.

Doskonałym punktem wyjścia do organizowania sieci łączności dla zarządzania kryzysowego jest wdrażanie przez MSWiA ogólnopolskiej sieci teleinformatycznej OST 112 oraz szerokopasmowych sieci regionalnych, powiatowych i gminnych przez organa samorządowe.

① *Wyjątkiem są tzw. sieci radiotelefoniczne wojewodów zapewniające łączność radiową na obszarach województw.*

Tworzenie OST 112 wynika z zaleceń UE (Dyrektywa 2002/22/WE Parlamentu Europejskiego i Rady z dnia 7 marca 2002 r.). Celem głównym realizowanego projektu jest poprawa jakości współdziałania jednostek organizacyjnych Policji, Państwowej Straży Pożarnej i Państwowego Ratownictwa Medycznego w zakresie obsługi wywołań na numery alarmowe [6]; termin wykonania jest przewidziany na koniec 2011 r. W ramach realizowanych przedsięwzięć zamierza się przyłączyć do jednej sieci teleinformatycznej około 870 jednostek organizacyjnych służb publicznego bezpieczeństwa i ratownictwa, istotnych z punktu widzenia funkcjonowania centrów powiadamiania ratunkowego oraz wojewódzkich centrów powiadamiania ratunkowego, a w efekcie zapewnienić we wskazanych lokalizacjach pełny zakresu usług teleinformatycznych i łączności telefonicznej.

W ramach projektu będzie zaimplementowanych:

- 20 głównych węzłów IP/MPLS (*Internet Protocol/Multiprotocol Label Swiching)*, połączonych łączami o przepływności 10 Gbit/s, 1 Gbit/s i 100 Mbit/s (w Warszawie i w komendach wojewódzkich policji – KWP),
- 45 węzłów IP/MPLS dołączonych do węzłów głównych łączami 100 Mbit/s (w komendach miejskich policji – KMP),
- ponad 200 węzłów IP/MPLS w komendach powiatowych policji – KPP dołączonych do węzłów łączami 30 Mbit/s.

Wymieniona liczba węzłów i traktów transmisyjnych (głównie światłowodowych) będzie szkieletem ogólnopolskiej sieci OST 112, pracującej w technice IP/MPLS. Dzięki zastosowaniu protokołu IP/MPLS sieć zostanie przystosowana do świadczenia usług transmisji danych dla podmiotów podległych MSWiA. Planowany jest następujący zakres implementacji sieci, usług i udogodnień przy wykorzystaniu OST 112:

- sieć rządowej telefonii VoIP,
- sieć telefonii VoIP dla Policji,
- usługa wideotelefonii,
- dostęp do różnych zasobów danych,
- sieć wirtualna dla Państwowej Straży Pożarnej,
- sieć wirtualna dla centrów powiadamiania ratunkowego,
- dostęp do platformy lokalizacyjno-informacyjnej z centralną bazą danych – PLI CBD.

Sieć OST 112 jest nowoczesna, przeznaczona dla służb publicznego bezpieczeństwa i ratownictwa, a także dla administracji państwowej do szczebla województwa.

Obecnie trwają prace przygotowawcze do budowy szerokopasmowych sieci światłowodowych przez jednostki samorządu terytorialnego (JST). Podział kompetencji JST jest następujący:

- jednostki wojewódzkie budują sieci szkieletowe i dystrybucyjne,
- jednostki powiatowe, miejskie/gminne budują sieci dostępowe.

Przykładem jest projekt *Sieć szerokopasmowa Polski Wschodniej*, (SSPW), realizowany na terenie 5 województw: lubelskiego, podlaskiego, podkarpackiego, świętokrzyskiego oraz warmińsko-mazurskiego [6]. Celem projektu jest zapewnienie do końca 2014 r. dostępu do usług szerokopasmowych dla 90% mieszkańców, 100% instytucji publicznych i przedsiębiorców w ww. województwach.

W ramach projektu SSPW zostanie zbudowana wydajna szkieletowa sieć światłowodowa, spełniająca wymagania stawiane tzw. sieciom następnej generacji NGN (*Next Generation Network*). Zostaną też przygotowane obiekty (punkty dystrybucyjne), stanowiące punkty styku z operatorami sieci dostępowych. Sieć będzie otwarta na równych zasadach dla wszystkich przedsiębiorców telekomunikacyjnych deklarujących usługi szerokopasmowe lub ich nowoczesne zastosowania wszystkim mieszkańcom regionu, również tym, którzy w oparciu o tę infrastrukturę będą rozbudowywać własne systemy dostępu szerokopasmowego (wielu obecnych na rynku operatorów wstępnie zadeklarowało już chęć tego rodzaju współpracy przy rozwoju usług szerokopasmowych w regionie).

Sieć SSPW zapewni m.in.:

1) dzierżawę infrastruktury pasywnej sieci

– dzierżawę kanalizacji teletechnicznej,
– dzierżawę ciemnych włókien światłowodowych,

2) usługi transmisyjne wykorzystujące platformę IP

– usługi dostępu do internetu,
– usługi telefonii (w technologii VoIP (*Voice over IP*)),
– usługi multimedialne: przesyłanie programów telewizyjnych Web TV, IPTV w standardzie zwykłym oraz wysokiej rozdzielczości HD (*High Definition*), wideo na żądanie VoD (*Video on Demand*),
– usługi sterowania, zarządzania i kontroli urządzeń, działające automatycznie bez udziału użytkownika M2M (*Machine to Machine*), a także różnego rodzaju monitoring,
– aplikacje i inne usługi o wartości dodanej VAS (*Value Added Services*), o różnej specyfice, które będą się pojawiać w przyszłości w miarę rozwoju rynku.

Sieć SSPW będzie zbudowana jako sieć hierarchiczna, składająca się z dwóch warstw:

– warstwy szkieletowej,
– warstwy dystrybucyjnej.

Szkielet sieci tworzą węzły szkieletowe wraz z łączącymi je elementami pasywnymi. Warstwa szkieletowa sieci odpowiada za połączenie z sieciami krajowymi i międzynarodowymi przez punkty styku, transport danych w szkielecie sieci i agregację ruchu z warstwy dystrybucyjnej. Węzły sieci szkieletowej będą instalowane w miastach powiatowych.

Sieć szkieletowa składa się z:

– części pasywnej – pomieszczeń węzłów szkieletowych, wraz z instalacjami niezbędnymi do zapewnienia bezpiecznej i nieprzerwanej pracy urządzeń aktywnych sieci szkieletowej, kanalizacji kablowej, kabli światłowodowych oraz pasywnego osprzętu światłowodowego,
– części aktywnej – urządzeń aktywnych sieci szkieletowej.

Zakłada się wykorzystanie w sieci SSPW protokołu transmisyjnego MPLS (*Multiprotocol Label Switching*).

Z powyższego wynika, że na obszarach województw istnieje lub będzie istniała infrastruktura telekomunikacyjna, wymagana do organizowania sieci łączności elektronicznej na potrzeby organów zarządzania kryzysowego.

Usługi telekomunikacyjne dla organów zarządzania kryzysowego

W kolejnych latach należy oczekiwać znacznego wzrostu wykorzystania różnych, nowoczesnych usług łączności elektronicznej przez służby publicznego bezpieczeństwa, ratownictwa i organa zarządzania kryzysowego [3].

Wzrośnie wykorzystanie telefonii VoIP, jako nowoczesnego sposobu komunikacji telefonicznej w sieciach teleinformatycznych. Realizacja tej usługi polega na wykorzystaniu mechanizmu transmisji sygnałów akustycznych w postaci pakietowej (podobnie jak ma to miejsce w przypadku transmisji danych) w tej samej sieci, która jest wykorzystywana do transmisji danych. Tradycyjna telefonia, wykorzystująca komutację łączy korzysta z odrębnej, dedykowanej sieci telefonicznej.

Użytkownicy aparatów IP mogą korzystać z aplikacji XML na ekranie telefonu IP. Aparat IP jako terminal współpracujący z aplikacją wykorzystującą protokół XML umożliwia przesyłanie komend sterujących, komunikatów jak i odbierania wiadomości. Otwartość protokołu umożliwia integrację z dowolną aplikacją pracującą w architekturze klient-serwer.

W ramach oferowanych i rozwijających się teleusług, usług dodatkowych i udogodnień możliwe jest wykorzystanie przez organy zarządzania kryzysowego, służby ratownicze i bezpieczeństwa publicznego:

- telekonferencji, realizowanej doraźnie (*ad hoc*), albo jako telekonferencji zaplanowanej (*meet me*) gdzie inicjator ustanawia numer telefoniczny, na który wdzwaniają się poszczególni uczestnicy telekonferencji,
- przenoszenia numeru użytkownika na inne zakończenie sieci telefonicznej oraz ustawienie jego aparatu telefonicznego i uprawnień (tzw. nomadyczność użytkowników telefonii stacjonarnej), dzięki nadanemu profilowi i hasłu (PIN) za pomocą, którego użytkownik loguje się w sieci,
- linii współdzielonej (*Shared Line*) jako usługi, za pomocą której użytkownik ma możliwość zdefiniowania dodatkowych numerów, które będą wydzwaniane oprócz podstawowego,
- szyfrowania rozmowy telefonicznej oraz strumienia sterującego, obejmującego strumień cyfrowy przesyłany między aparatami telefonicznymi oraz ruch sygnalizacyjny do jednostki sterującej połączeniem,
- priorytetowania połączeń telefonicznych, umożliwiającego użytkownikowi o wyższym priorytecie, zasygnalizować wysoki priorytet połączenia lub nawet rozłączyć połączenie o niższym priorytecie,
- poczty głosowej, umożliwiającej użytkownikom na pozostawianie i odsłuchiwanie wiadomości za pomocą aparatu telefonicznego funkcjonującego w systemie wraz z przeglądaniem pozostawionych wiadomości głosowych w poczcie głosowej za pomocą przeglądarki internetowej,
- usług informacyjno-powiadamiających, zapewniających wybranym użytkownikom (wyższemu personelowi) przekazywanie podwładnym krótkich, pilnych wiadomości tekstowych lub głosowych,
- automatycznego zestawiania wirtualnych grup rozmownych, obejmujących różne urządzenia końcowe, np. aparat telefoniczny, stacje ruchomą GSM/UMTS/LTE, radiotelefon sieci analogowej i inne,
- wielosystemowych zakończeń sieci (*Dual-Mode Phone*), umożliwiających ograniczanie liczby urządzeń końcowych używanych przez użytkowników,

– łączności telefonicznej między użytkownikami telefonii stacjonarnej i użytkownikami sieci ruchomych (radiotelefonicznych),
– usługi telefonicznej przez internet lub sieć współpracującą.

Tak więc organy zarządzania kryzysowego mogą wykorzystywać **usługi wideotelefoniczne**:

– wideotelefonię, polegającą na zestawieniu połączenia składającego się z kanału rozmównego oraz kanału wizyjnego, z użyciem wideotelefonu lub kamery dołączonej do komputerowej stacji roboczej (komputera przenośnego); zestawienie połączenia dokonuje się po wybraniu numeru aparatu użytkownika pożądanego; system automatycznie sprawdza czy są dostępne warunki (sieć, typ urządzenia końcowego) do zestawiania połączenia; wideotelefon powinien umożliwiać przeprowadzenie również zwykłej rozmowy telefonicznej;
– wideokonferencję, polegającą na zestawieniu połączenia składającego się z kanału rozmównego oraz kanału wizyjnego, z użyciem wideotelefonu lub kamery dołączonej do komputerowej stacji roboczej (komputera przenośnego), między więcej niż dwoma użytkownikami; wideokonferencja może być zestawiana doraźnie (*ad hoc*), albo jako telekonferencja zaplanowana (*meet me*);
– wideokonferencje planowane typu grupowego, w których wykorzystuje się grupowe terminale wideokonferencyjne o większych rozmiarach ekranów oraz podwyższonej jakości transmisji dźwięku i obrazu; w zależności od potrzeb, system zarządzania konferencją umożliwia rezerwacje zasobów, rozsyłanie informacji i zaproszeń na sesje wideokonferencyjne.

Możliwe jest także wykorzystanie zestawu **usług poczty elektronicznej** i jej integracji z aparatami telefonicznymi IP:

– poczty elektronicznej prywatnej, umożliwiającej przesyłanie wiadomości tekstowych oraz załączonych dokumentów w formie plików, między komputerami użytkowników w zamkniętej grupie w obrębie systemu; usługa nie umożliwia przesyłania wiadomości poza ustaloną grupę użytkowników; wiadomości mogą być przesyłane w kanale z szyfrowaniem;
– poczty elektronicznej publicznej, umożliwiającej przesyłanie wiadomości tekstowych oraz załączonych dokumentów w formie plików, między komputerami użytkowników pracujących w systemie, a użytkownikami innych sieci, w tym internetu;
– komunikatora tekstowego (*chat*), umożliwiającego dialog polegający na wymianie komunikatów tekstowych przez ich wpisanie w oknie programu komunikacyjnego; komunikaty są odbierane przez jedną lub więcej osób, które następnie udzielają odpowiedzi;
– powiadomienia i komunikatów tekstowych, umożliwiających wysyłanie komunikatów tekstowych w formie krótkiej wiadomości tekstowej, powiadomienia/alarmu na telefon IP lub komunikator tekstowy.

Usługa **mobilne biuro** umożliwia wybranej grupie użytkowników, którzy z racji swoich obowiązków przebywają poza stałą siedzibą, dostęp do najważniejszych usług i aplikacji, wykorzystywanych przez nich w miejscu pracy. W celu uzyskania dostępu może być wykorzystana publiczna sieć łączności ruchomej GSM/GRPS/EDGE lub UMTS/HSDPA. Jako stacje ruchome mogą być użyte zaawansowane aparaty typu smartphon lub urządzenia przenośne PDA. Usługa mobilnego biura zapewnia:

– dostęp do poczty elektronicznej, a więc odbieranie lub wysyłanie wiadomości z dowolnego miejsca oraz odczytywanie i przeglądanie załączników do poczty,
– dostęp do kalendarza, notatek oraz zadań i ich synchronizację z centralnym systemem kalendarza i systemem pracy grupowej,

- raportowanie stanu wykonania zadań i ich statusu,
- dostęp do centralnej książki kontaktów w celu uzyskania informacji o numerach telefonicznych, adresach e-mail oraz innych przydatnych danych, np. dział, przełożony, stanowisko,
- prowadzenie dialogu za pomocą krótkich komunikatów tekstowych,
- dostęp do informacji o pozostawionych wiadomościach oraz nieodebranych telefonach na telefonie stacjonarnym (jest to uzupełnienie usługi *single-number-reach*),
- dostęp do aplikacji centralnych, co oznacza, że użytkownik może mieć w miejscu, w którym przebywa dostęp do tych samych danych co w miejscu pracy.

Usługi wirtualnych spotkań i odpraw są przydatne dla zespołów kierowania i zarządzania kryzysowego oraz innych grup kierowniczych na szczeblu centralnym i wojewódzkim. Wirtualne spotkania mogą być organizowane:

- gdy użytkownicy wyłącznie się słyszą (*Voice Virtual Meeting*),
- gdy użytkownicy widzą się i słyszą (*Video Virtual Meeting*),
- gdy użytkownicy widzą się, słyszą jak również pracują na wspólnym dokumencie elektronicznym (*Web Virtual Meeting*),
- gdy część użytkowników z racji posiadanego terminala komunikacyjnego korzysta z ograniczonej listy mediów np. słyszy tylko głos.

Usługa wirtualnych odpraw (narad) jest przeznaczona dla osób ze szczebla wysokiej kadry kierowniczej, znajdujących się w oddalonych od siebie geograficznie lokalizacjach. Rozwiązanie to zapewnia – mimo przebywania w różnych miejscach – spotkanie o takim samym stopniu realizmu i przekazu treści oraz intensywności dyskusji, jaki towarzyszy spotkaniu przy jednym stole. Efekt będzie osiągany dzięki odpowiedniemu, technicznie uwarunkowanemu i bardzo rygorystycznemu ułożeniu dużych ekranów plazmowych, kamer, mikrofonów, głośników, oświetlenia, mebli i elementów wystroju pomieszczenia. System wirtualnych odpraw umożliwia również uczestnictwo osób dostępnych tylko przez kanał łączności głosowej, jak również zdalne pokazywanie dokumentów, prezentacji oraz przedmiotów.

Duże znaczenie praktyczne mają **usługi dystrybucji danych** (obrazu, treści), umożliwiające przenoszenie treści istotnych do działania danej organizacji (np. ważne wydarzenia przekazywane do wszystkich na żywo, przygotowane wcześniej, udostępniane w sieci szkolenia itp.) i wyświetlania takiego obrazu bezpośrednio na ekranie komputerowej stacji roboczej użytkownika, dołączonej do LAN/WAN. Użytkownik korzystający z systemu dystrybucji ma możliwość wyboru treści przez odpowiedni portal. Po zażądaniu przez użytkownika dostępu do danego przekazu, zawierającego żywy lub nagrany wcześniej strumień danych, odpowiedni portal kieruje przeglądarkę użytkownika do właściwego, najbliższego w sieci urządzenia przechowującego daną treść, przygotowaną uprzednio przez administratora sieci do dystrybucji.

Wzrasta rola **usługi dostępu do zasobów centralnych i lokalnych baz danych**. Stosowane rozwiązania umożliwią optymalizację zasobów przepływności łączy w sieci rozległej oraz zapewniają konsolidację infrastruktury w centrach danych. W wymiarze WAN usługa zapewni:

- akceptowalny czas ładowania, pobierania i otwierania plików danych,
- optymalną przepływność łączy,
- stałe parametry transmisji, takie jak opóźnienie i zmienność opóźnienia pakietów.

Optymalizacja dostępu do zasobów centralnych, przez wykorzystanie w systemie protokołów CIFS (*Common Internet File System)* i NFS (*Network File System*), umożliwi konsolidację zasobów infrastruktury serwerowej i dyskowej, umieszczonych w zdalnych jednostkach do poziomu centrum danych oraz zmniejszy zużycie zasobów w sieci rozległej poprzez zaawansowane algorytmy kompresji i eliminacji redundancji danych. Usługa umożliwi dystrybucję plików do lokalnych urządzeń przechowujących treści w celu zwiększenia ich dostępności (*prepositioning*).

Wnioski

Przekazywanie we właściwym czasie informacji z systemów monitorowania i wykrywania zagrożeń, informacji o zdarzeniach, katastrofach i ich obsłudze, także dotyczących zarządzania siłami i środkami oraz alarmowania i ostrzegania ludności, jest podstawą sprawnego i efektywnego zarządzania kryzysowego.

Podejmowane w skali kraju działania zmierzające do wdrażania ogólnokrajowych systemów teleinformatycznych (OST 112) i sieci szerokopasmowych na obszarach województw, stanowią podstawę do organizowania sieci łączności elektronicznej dla organów zarządzania kryzysowego, w szczególności umożliwiania dostępu do informacji o zagrożeniach i ich skali, gromadzonych w zbiorach danych.

Organizowane sieci łączności elektronicznej dla organów zarządzania kryzysowego powinny zapewniać nowoczesne usługi telekomunikacyjne, usprawniające prace organów zarządzania kryzysowego, a także efektywne zarządzanie siłami i środkami przeznaczonymi do zwalczania skutków zagrożeń.

Bibliografia

[1] Chrzęstek J.: *Potrzeby i wymagania stawiane systemom łączności województwa do działania w sytuacjach nadzwyczajnych zagrożeń*. Zeszyty naukowe SGSP, nr 33, Warszawa, 2005

[2] Kołodziński E.: *Wprowadzenie do zarządzania bezpieczeństwem podmiotu, Zagadnienia inżynierii bezpieczeństwa*. www. ptib.pl

[3] Kowalczyk B., Kowalewski M., Parapura H. i inni: *Aplikacje informatyczne dla Systemu Kierowania Bezpieczeństwem Narodowym*. Praca statutowa, Warszawa, Instytut Łączności – Państwowy Instytut Badawczy, 2009

[4] *Perspektywiczne sieci i usługi komunikacji elektronicznej na potrzeby bezpieczeństwa i zarządzania kryzysowego*. Praca statutowa, Warszawa, Instytut Łączności – Państwowy Instytut Badawczy, 2010

[5] Strzoda M.: *Zarządzanie informacjami w organizacji*, Warszawa, AON, 2004

[6] *Studium wykonalności dla projektu Ogólnopolska Sieć Teleinformatyczna na Potrzeby Obsługi Numeru Alarmowego 112*. Warszawa, CPI MSWiA, 2009

[7] *Studium wykonalności projektu Sieć Szerokopasmowa Polski Wschodniej.* Praca zbiorowa. Wyd. uzupełnione, Warszawa, 2010

Bolesław Kowalczyk

Dr inż. Bolesław Kowalczyk – absolwent Wojskowej Akademii Technicznej; pracownik Instytutu Łączności (od 1998), obecnie na stanowisku adiunkta; zainteresowania naukowe: sieci i usługi telekomunikacyjne dla służb publicznego bezpieczeństwa, ratownictwa i zarządzania kryzysowego, badanie jakości usług świadczonych przez publiczne sieci łączności elektronicznej.

e-mail: B.Kowalczyk@itl.waw.pl

Marian Kowalewski

Prof. nzw. dr hab. inż. Marian Kowalewski – absolwent Wyższej Szkoły Oficerskiej Wojsk Łączności; nauczyciel akademicki; pracownik naukowy Instytutu Łączności (od 1997); autor wielu podręczników, skryptów akademickich i artykułów; zainteresowania naukowe: planowanie i projektowanie oraz efektywność systemów telekomunikacyjnych.

e-mail: M.Kowalewski@itl.waw.pl

Henryk Parapura

Inż. Henryk Parapura – absolwent Wyższej Szkoły Oficerskiej Wojsk Łączności; pracownik Instytutu Łączności (od 2008), obecnie na stanowisku głównego specjalisty; zainteresowania zawodowe: problematyka sieci i usług telekomunikacyjnych dla służb publicznego bezpieczeństwa, ratownictwa i zarządzania kryzysowego.

e-mail: H.Parapura@itl.waw.pl