ZESZYTY NAUKOWE WSOWL

Nr 4 (162) 2011 ISSN 1731-8157

Marek WITKOWSKI*

BEZPIECZEŃSTWO SYSTEMÓW TELEINFORMATYCZNYCH W ZARZĄDZANIU KRYZYSOWYM

W artykule zostały przedstawione sieci i systemy teleinformatyczne, które wykorzystywane są do zapewnienia łączności na potrzeby zarządzania kryzysowego. Zaprezentowano przewodowe i bezprzewodowe środki łączności oraz przedstawiono ich wady i zalety, w realizacji zadań na rzecz bezpieczeństwa państwa.

Słowa kluczowe: *bezpieczeństwo teleinformatyczne, sieci teleinformatyczne, systemy teleinformatyczne, zarządzanie kryzysowe*

WSTĘP

Ważnym elementem sprawnego zarządzania jest odpowiednio zorganizowany obieg informacji. Ponadto sieci i systemy wytwarzające, przechowujące, przetwarzające i przesyłające informacje powinny być zabezpieczone przed nieuprawnionym dostępem. Szczególnego znaczenia nabiera ta problematyka w systemie zarządzania kryzysowego, gdzie informacja decyduje o sposobie realizacji. Podjęcie błędnej decyzji, na podstawie fałszywych informacji, może doprowadzić do zagrożenia życia lub mienia obywateli. Dlatego, aby zapewnić odpowiedni poziom bezpieczeństwa informacji, należy używać właściwie zabezpieczonych sieci i systemów teleinformatycznych.

1. BEZPIECZEŃSTWO TELEINFORMATYCZNE W ZARZĄDZANIU KRYZYSOWYM

Bezpieczeństwo sieci i systemów teleinformatycznych (SiS TI) można rozpatrywać jako całość pod pojęciem bezpieczeństwa teleinformatycznego, które zgodnie z decyzją Ministra Obrony Narodowej w sprawie organizacji szczególnej ochrony systemów i sieci teleinformatycznych w resorcie obrony narodowej to: *całokształt przedsięwzięć zmierzających do zapewnienia bezpieczeństwa systemów i sieci teleinformatycznych oraz ochrony informacji wytwarzanej, przetwarzanej, przechowywanej lub przekazywanej w tych systemach i sieciach przed przypadkowym lub celowym ujawnie-*

* kpt. mgr inż. Marek WITKOWSKI - Instytut Dowodzenia Wyższej Szkoły Oficerskiej Wojsk Lądowych

niem, modyfikacją, zniszczeniem lub uniemożliwieniem jej przetwarzania poprzez zastosowanie w sposób kompleksowy technicznych, programowych, kryptograficznych oraz organizacyjnych środków i metod[1]. Jest to bardzo rozbudowana definicja, ale w sposób całościowy obejmuje problematykę, która podjęta została w tej publikacji. W ujęciu segmentowym (fragmentarycznym), system teleinformatyczny można rozpatrywać, jako: *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*[2].

Kolejne pojęcia z zakresu bezpieczeństwa teleinformatycznego, zaczerpnięte zostały z decyzji Ministra Obrony Narodowej w sprawie organizacji i funkcjonowania systemu reagowania na incydenty komputerowe w resorcie obrony narodowej[3]. Zgodnie z tą decyzją, system teleinformatyczny to: *system, który tworzą urządzenia, narzędzia, metody postępowania i procedury stosowane przez wyspecjalizowanych pracowników, w sposób zapewniający wytwarzanie, przechowywanie, przetwarzanie lub przekazywanie informacji*. Natomiast, według tej samej decyzji, sieć teleinformatyczna to: *organizacyjne i techniczne połączenie systemów teleinformatycznych*. Ustawa z dnia 16 lipca 2004 r. Prawo telekomunikacyjne, definiuje sieć teleinformatyczną jako: „*sieć telekomunikacyjną, obejmującą systemy transmisyjne oraz urządzenia komutacyjne lub przekierowujące, a także inne zasoby, które umożliwiają nadawanie, odbiór lub transmisję sygnałów za pomocą przewodów, fal radiowych, optycznych lub innych środków wykorzystujących energię elektromagnetyczną, niezależnie od ich rodzaju*[4].

Kolejne pojęcie związane z tą publikacją to – zarządzanie kryzysowe. W ustawie o zarządzaniu kryzysowym postrzegane jest jako: *działalność organów administracji publicznej będąca elementem kierowania bezpieczeństwem narodowym, która polega na zapobieganiu sytuacjom kryzysowym, przygotowaniu do przejmowania nad nimi kontroli w drodze zaplanowanych działań, reagowaniu w przypadku wystąpienia sytuacji kryzysowych, usuwaniu ich skutków oraz odtwarzaniu zasobów i infrastruktury krytycznej*[5].

W literaturze przedmiotu można znaleźć różne podejścia do problematyki zarządzania kryzysowego, a także bezpieczeństwa sieci i systemów teleinformatycznych. Na potrzeby tego artykułu oraz zawartych w nim rozważań, nie będą przedstawiane inne niż powyżej przywołane ujęcia tych zagadnień, ani nie będzie przeprowadzana analiza porównawcza. Zaprezentowane definicje, w sposób wystarczający objaśniają zastosowane pojęcia. Dalsza uwaga skoncentrowana zostanie na omówieniu zagadnienia sieci i systemów teleinformatycznych. Następnie przedstawione zostaną zagrożenia, na jakie mogą zostać narażone elementy systemu zarządzania kryzysowego, w przypadku stosowania niezabezpieczonych sieci i systemów.

---

[1] Decyzja Nr 24/MON Ministra Obrony Narodowej z dnia 31 stycznia 2006 r. w sprawie organizacji szczególnej ochrony systemów i sieci teleinformatycznych w resorcie obrony narodowej.

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

[3] Decyzja Nr 357/MON Ministra Obrony Narodowej z dnia 29 lipca 2008 r. w sprawie organizacji i funkcjonowania systemu reagowania na incydenty komputerowe w resorcie obrony narodowej.

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

[5] Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U. z 2007 r. Nr 89, poz. 590, art. 2 z późn. zm.).

Sieć teleinformatyczna jest integralną częścią systemu lub systemów teleinformatycznych. Sieci teleinformatyczne, ze względu na wykorzystywaną technikę przesyłania informacji, możemy podzielić na dwie zasadnicze grupy:

- przewodowe;
- bezprzewodowe.

Sieci TI przewodowe – wykorzystują do transmisji informacji medium przewodowe, takie jak: kable miedziane, kable komputerowe (skrętki), przewody telekomunikacyjne, kable teleinformatyczne oraz kable światłowodowe.

Sieci TI bezprzewodowe – to sieci, których medium transmisyjnym jest fala elektromagnetyczna.

SiS TI są narażone na różnego rodzaju zagrożenia, które mogą pochodzić z zewnątrz (np. poprzez łącza internetowe) lub z wnętrza firmy (niewłaściwa obsługa, brak zabezpieczeń). Zagrożenie rozumiane jest tutaj jako: *potencjalna możliwość naruszenia bezpieczeństwa systemu lub sieci teleinformatyczne*[6]. Zagrożenia mogą być spowodowane zarówno przez użytkowników[7] oraz przez oprogramowanie i sprzęt. Włamania do systemów informatycznych są coraz częstsze, ponieważ dostęp do zasobów komputerowych stał się możliwy przez podłączenie urządzeń wymiany informacji w sieć Internet. Wiąże się to ze zwiększonym zagrożeniem dla wytwarzanych, przetwarzanych i przesyłanych informacji (baz danych) oraz innych zasobów, które stanowić mogą tajemnicę danej organizacji. Celem ataków stają się także instytucje państwowe, odpowiedzialne za kwestie bezpieczeństwa. Ich skutkiem może być osłabienie lub całkowite sparaliżowanie krytycznej infrastruktury teleinformatycznej państwa. Stanowić to może poważne zagrożenie dla samego bezpieczeństwa obywateli oraz ich mienia (konta bankowe, inwestycje finansowe, dorobek naukowy). Powszechność dostępu do sieci Internet oraz usług z nim związanych, zwiększa znacznie poziom realnych zagrożeń. Dorothy E. Denning, przedstawia dwa rodzaje przestępstw[8]. Pierwszym jest kradzież własności intelektualnej. Drugim rodzajem jest fałszerstwo, które traktuje jako piractwo komputerowe. Prawdopodobieństwo ataku terrorystycznego w sieci (cyberterroryzm) stało się realnym zagrożeniem. Zaangażowanie Polski, zarówno polityczne, jak i militarne – na arenie międzynarodowej, w walce z terroryzmem, spowodowało wzrost liczby potencjalnych zagrożeń, skierowanych przeciwko naszemu państwu. Dlatego, należy podjąć wszelkiego rodzaju przedsięwzięcia, aby nie dopuścić do obniżenia poziomu naszego bezpieczeństwa. Do podstawowych zagrożeń, związanych z eksploatacją systemów teleinformatycznych, możemy zaliczyć: naruszenie integralności danych, włamania do systemów komputerowych, nieuprawniony dostęp do baz danych, kopiowanie, niszczenie, bądź nieuprawnioną modyfikację danych. Ataki w cyberprzestrzeni mogą przyjmować różną formę – od wysłania niechcianej poczty, poprzez włamanie się do systemów informatycznych zainstalowanych na naszych komputerach – do przejęcia nad nimi całkowitej kontroli. Mogą to być ataki pasywne lub aktywne. Ataki pasywne

---

[6] Decyzja Nr 357/MON Ministra Obrony Narodowej z dnia 29 lipca 2008 r. w sprawie organizacji i funkcjonowania systemu reagowania na incydenty komputerowe w resorcie obrony narodowej.

[7] M. Witkowski, *Analiza systemowa zjawiska cyberterroryzmu na przełomie XX – XXI w. w warunkach RP*, praca studyjna pod kierunkiem: P. Sienkiewicza, AON, Warszawa 2005, s. 29 - 30.

[8] E. Dorothy Denning, *Wojna informacyjna i bezpieczeństwo informacji*, Wydawnictwa Naukowo-Techniczne, Warszawa 2002, s. 59.

polegają na podsłuchiwaniu lub monitorowaniu przesyłanych danych. Takie ataki są bardzo trudne do wykrycia, ponieważ nie wiążą się z jakimikolwiek zmianami danych. Ataki aktywne polegają na modyfikacji lub tworzeniu danych fałszywych[9], w celu przechwycenia danych lub podszywaniu się pod uprawnionego użytkownika. Aby wyeliminować lub ograniczyć tego typu zagrożenia dla sieci i systemów teleinformatycznych, powinny zostać opracowane stosowne procedury ochrony zasobów. W literaturze dotyczącej tej problematyki określane jest to terminem polityka bezpieczeństwa. Poprawnie skonstruowana polityka bezpieczeństwa, powinna do zagadnień związanych z bezpieczeństwem teleinformatycznym podchodzić kompleksowo, ze szczególnym uwzględnieniem problematyki związanej z:

- identyfikacją i uwierzytelnianiem;
- kontrolą dostępu;
- śledzeniem odpowiedzialności;
- badaniem (audytem) stanu bezpieczeństwa;
- ochroną współdzielonych zasobów;
- dokładnością ochrony;
- niezawodnością ochrony;
- ochroną komunikacji[10].

Niezgodne z procedurami bezpieczeństwa postępowanie użytkowników oraz brak znajomości przepisów, a także własna wygoda i niechęć w stosowaniu zabezpieczeń, przyczynia się do obniżenia poziomu bezpieczeństwa sieci i systemów teleinformatycznych. Nie zawsze jest to celowe działanie ze strony użytkownika, często wynika z braku świadomości zagrożeń oraz skutków takiego postępowania. Aby do tego nie dopuścić, należy regularnie prowadzić szkolenia dla personelu obsługującego, nie zapominając o personelu technicznym. Powinny to być jednak szkolenia prowadzone niezależnie, gdyż innego rodzaju wiedzy wymaga się od pierwszej grupy użytkowników, a innego od drugiej. Szkolenia takie powinny prowadzić osoby posiadające odpowiednią wiedzę z omawianej problematyki[11].

2. WADY I ZALETY SIECI I SYSTEMÓW TELEINFORMATYCZNYCH WYKORZYSTYWANYCH NA POTRZEBY ZARZĄDZANIA KRYZYSOWEGO

Zarządzanie kryzysowe opiera się na wielopoziomowych strukturach, od szczebla centralnego, poprzez szczebel ministerialny, wojewódzki, powiatowy, na gminie kończąc. Pomiędzy elementami wymienionych struktur występują różnego rodzaju zależności przełożeństwa i podległości. Wymiana informacji ma zasadnicze znaczenie dla sprawnego przebiegu procesu zarządzania i podjęcia określonych decyzji. Zadania związane ze sprawnym przesyłaniem informacji na potrzeby Zespołów Zarządzania

---

[9] M. Witkowski, *Analiza systemowa zjawiska cyberterroryzmu na przełomie XX – XXI w. w warunkach RP*, praca studyjna pod kierunkiem P. Sienkiewicz, AON, Warszawa 2005, s. 30 - 33.

[10] Wyjaśnienie użytych pojęć można znaleźć na stronie: [online]. [dostęp: 24.10.2011]. Dostępny w Internecie: http://www.iniejawna.pl/pomoce/przeciw_zagr.html.

[11] A. Szleszyński, M. Witkowski, *Szkolenie użytkowników w procesie ochrony informacji wykorzystywanych w systemach wsparcia dowodzenia*, [w:] „Zeszyt Naukowe WSOWL", nr 2/2010, WSOWL, Wrocław 2010, s. 193 - 202.

Kryzysowego (ZZK) realizują Centra Zarządzania Kryzysowego (CZK). Wiąże się to z koniecznością zorganizowania i zabezpieczenia sieci i systemów teleinformatycznych na wszystkich poziomach odpowiedzialnych za sprawne funkcjonowanie organów, wchodzących w skład struktur zarządzania kryzysowego. Wymienione centra odpowiadają za sprawne przekazanie informacji (decyzji) do organów wykonawczych, którymi są ZZK niższych szczebli. Informacje przekazywane są pomiędzy centrami, które wyposażone są w środki teleinformatyczne umożliwiające taką wymianę (obieg informacji). Do tego celu wykorzystuje się przewodowe i bezprzewodowe sieci i systemy teleinformatyczne. Wykorzystywane SiS TI powinny charakteryzować się dużą odpornością na zakłócenia oraz niezawodnością, które są cechami niezbędnymi w sytuacjach zagrożenia kryzysowego. Ponadto, wymiana informacji pomiędzy strukturami zarządzania kryzysowego musi być odpowiednio chroniona przed nieuprawnionym dostępem oraz konsekwencjami takiego dostępu[12]. Do tych celów wykorzystywane są urządzenia, media transmisyjne oraz dedykowane rozwiązania, które zapewnią właściwy obieg informacji i poziom bezpieczeństwa. Dla ułatwienia, przyjęto, że wymienione wcześniej środki, zostaną podzielone na dwie grupy: przewodowe oraz bezprzewodowe. Do pierwszej grupy zaliczyć możemy: sieci telekomunikacyjne operatorów publicznych i resortowych, które świadczą usługi telefonii stacjonarnej oraz przesyłania wiadomości za pomocą faksów i Internetu. Wymienione środki są zależne od lokalnych sieci i całej infrastruktury przewodowej, dlatego korzystanie z wymienionych urządzeń może odbywać się tylko w systemie stacjonarnym (budynki, stałe miejsca pracy). Tej grupy urządzeń nie wykorzystamy podczas prowadzenia akcji w terenie lub w miejscach doraźnie wybranych bez rozwiniętej infrastruktury przewodowej.

Kolejną grupę stanowią bezprzewodowe środki łączności, do których zaliczyć można:

- środki radiowe;
- telefonię komórkową;
- telefonię satelitarną.

Celem tworzenia systemu łączności za pomocą urządzeń radiowych jest zapewnienie sprawnego obiegu informacji pomiędzy wszystkimi podmiotami odpowiedzialnymi za bezpieczeństwo i zarządzenie w warunkach wystąpienia kryzysu. Przenośne środki łączności radiowej są niezastąpione, w przypadku wystąpienia braków w dostawie energii. Urządzenia tego typu posiadają własne źródła zasilania, w postaci akumulatorów i baterii, które umożliwiają pracę nawet do kilkunastu godzin. Ponadto prezentowane urządzenia są niezależne od przewodowej infrastruktury telekomunikacyjnej. Można je wykorzystywać zarówno w warunkach stacjonarnych, jak również podczas prowadzenia akcji ratowniczych w terenie. System łączności radiowej może opierać się na następujących urządzeniach:

- radiostacje;
- radiotelefony;
- telefony bezprzewodowe.

[12] Problematyka ta została omówiona w artykule: J. Chrząstek, *Potrzeby i wymagania stawiane systemom łączności do działania w sytuacjach nadzwyczajnych zagrożeń*, [w:] „Zeszyty Naukowe SGSP", nr 33/2005, Warszawa 2005.

System łączności radiowej zorganizowany jest na potrzeby koordynacji, zarządzania oraz ostrzegania i alarmowania. Łączność ta odbywa się z wykorzystaniem radiostacji analogowych oraz cyfrowych.

Radiostacje analogowe są sprzętem starego parku technologicznego, które nie posiadają żadnych elementów ochrony informacji w czasie prowadzenia wymiany radiowej. Zakłócenie pracy tego typu urządzenia jest bardzo proste, gdyż każdy użytkownik radiostacji (posiadającej ten sam zakres częstotliwości) może wprowadzać fałszywe informacje lub zakłócać pracę w sieciach i kierunkach radiowych zarządzania kryzysowego. Jest to możliwe do zrealizowania, ponieważ częstotliwości pracy radiostacji głównych oraz przekaźników radiowych, są umieszczane w jawnych planach lub w Internecie. W kilka minut, w sieci Internet, można uzyskać konkretne dane korespondentów, obowiązujące kryptonimy radiowe, czasy seansów radiowych oraz instrukcje prowadzenia wymiany radiowej. Zdaniem autora, obniża to w znaczący sposób poziom bezpieczeństwa i wyklucza stosowanie tego typu urządzeń w systemie zarządzania bezpieczeństwem państwa. Dlatego analogowe środki radiowe powinno się sukcesywnie zastępować urządzeniami nowej generacji, np. radiostacjami cyfrowymi. Nowoczesne środki łączności bezprzewodowej posiadają różnego rodzaju moduły ochrony informacji (kryptograficzne, kodujące lub szyfrujące), co praktycznie uniemożliwia prowadzenie podsłuchu oraz przechwycenie korespondencji radiowej przez nieuprawnionych użytkowników. Kolejną zaletą radiostacji cyfrowych jest to, że częstotliwości pracy takich urządzeń nie są stałe – jak to miało miejsce w przypadku urządzeń analogowych. W nowoczesnych radiostacjach częstotliwości pracy, podczas nadawania jednej wiadomości, mogą zmieniać się nawet kilkaset razy na sekundę. Dostęp do tego typu urządzeń jest ograniczony – zakupić je mogą tylko określone grupy użytkowników, a posiadanie modułów zabezpieczających przed nieuprawnionym dostępem jest ściśle określone i nadzorowane przez organa bezpieczeństwa państwa (np. ABW, SKW). Zakup tego typu urządzeń łączności wymaga dużych nakładów finansowych (kilkaset tysięcy złotych), ale będą to środki, które zapewnią stabilną i bezpieczną wymianę radiową.

Kolejną grupę radiowych środków łączności, wykorzystywanych na potrzeby zarządzania kryzysowego stanowią urządzenia radiotelefoniczne. W ich skład mogą wchodzić stacje przekaźnikowe, które są wyposażone w przemienniki częstotliwości – pośredniczące w wymianie radiowej oraz urządzenia końcowe, w postaci radiotelefonów. Mogą to być urządzenia w wersji: przenośnej, przewoźnej lub bazowej. Zakup takiego radiotelefonu wraz z anteną, dodatkowym źródłem zasilania oraz innymi akcesoriami nie wymaga specjalnego zezwolenia. Częstotliwości pracy radiotelefonów są dostępne na stronach internetowych producentów tych urządzeń. Podobnie jak w przypadku urządzeń analogowych, prowadzenie „sabotażu radiowego" jest bardzo łatwe do zrealizowania. Częstotliwości pracy poszczególnych służb, dbających o nasze bezpieczeństwo z podziałem na konkretne województwa są dostępne na stronach internetowych. Autor poda tylko jedną z nich[13], ponieważ nie jest zwolennikiem przekazywania tego typu informacji. W opinii autora, dane tego typu powinny być niejawne. Ponadto, urządzenia wykorzystywane przez służby użyteczności publicznej powinny posiadać moduły przynajmniej szyfrujące transmisję, a ich zakup nie powinien być możliwy bez

[13] [online]. [dostęp: 25.10.2011]. Dostępny w Internecie: http://radioscannerpolska.pl/index.html.

stosownych zezwoleń. Reasumując – nie jest to środek łączności, który powinien być używany do tak ważnych przedsięwzięć, jak zarządzanie bezpieczeństwem.

Kolejną grupę środków radiowych stanowi telefonia komórkowa, której podstawowym medium transmisyjnym jest fala elektromagnetyczna. Jednak komunikacja między poszczególnymi stacjami pośredniczącymi, może odbywać się z wykorzystaniem traktów przewodowych. Telefony komórkowe stały się niezbędnym elementem naszego życia, zapewniają nam łączność praktycznie w każdym miejscu. Jest to środek łączności, który traktować należy jako środek uzupełniający potrzeby łączności. W sytuacjach kryzysowych, jak pokazały doświadczenia powodzi w 2010 roku, nie sprawdził się, ponieważ stacje bazowe zostały zalane, bądź wyłączone przez operatorów, aby nie uległy poważniejszym uszkodzeniom[14]. Należy pamiętać, że telefonia komórkowa ma ograniczone możliwości połączeń – dlatego, w sytuacji zagrożenia, nie wszyscy abonenci będą mieli możliwość połączenia się z żądanym numerem[15]. Jest to spowodowane ograniczonym dostępem do poszczególnych komponentów telefonii mobilnej i stacji pośredniczących.

Następną grupę urządzeń łączności stanowią trankingowe sieci lokalne standardu TETRA (Terrestial Trunked Radio – naziemna zbiorowa łączność radiowa). Sieci tego rodzaju mogą opierać się na analogowej sieci trankingowej EDACS (Enhanced Digital Access Communication System) lub nowoczesnej sieci cyfrowej systemu TETRA 2. Zmodernizowana wersja systemu umożliwia przesyłanie głosu oraz transmisję danych. W przypadku wdrożenia systemu TETRA 2 z systemem TEDS (TETRA Enhanced Data Service), pokrycie sygnałem radiowym (pasmo 380 – 400 MHz) obszaru aglomeracji miejskich wymaga zainstalowania co najmniej kilkunastu stacji bazowych[16]. Systemy standardu TETRA wykorzystywane są w systemie zarządzania kryzysowego niektórych aglomeracji miejskich. Przykładem może być Wrocław, gdzie dla poprawy bezpieczeństwa miasta nastąpi rozbudowa zasięgu i pojemności istniejącego systemu łączności ratowniczej TETRA z opcją rozszerzenia zasięgu do obszaru całej aglomeracji wrocławskiej. Kolejnym etapem tego przedsięwzięcia będzie włączenie lokalnego systemu TETRA do systemu łączności ogólnokrajowej oraz pełne wykorzystanie systemu TETRA na potrzeby:

- Policji;
- Państwowej Straży Pożarnej;
- Pogotowia Ratunkowego;
- Centrum Zarządzania Kryzysowego;

[14] [online]. [dostęp: 30.10.2011]. Dostępny w Internecie: http://www.wiadomosci.swidnickie.pl/ wiadomosci-24/1-wiadomosci24/5121-gotowi-na-kryzys.

[15] [online]. [dostęp: 30.10.2011] Dostępny w Internecie: http://media2.pl/telekomunikacja/64470-Powodz-Problemy-z-lacznoscia-komorkowa.html.

[16] M. Kowalewski, B. Kowalczyk, Z. Hendler, *System łączności na potrzeby służb bezpieczeństwa publicznego i zarządzania kryzysowego w aglomeracji miejskiej*, [w:] „Telekomunikacja i Techniki Informacyjne" nr 3-4/2008, Warszawa 2008, s. 33 - 48.

- istotnych zakładów komunalnych (m.in. wodnych i kanalizacyjnych, energetycznych, gazowych, zarządzanie transportem komunalnym i sterowanie ruchem), także patrole saperskie[17].

Eksploatacja tej grupy łączności, opartej na standardzie TETRA, wymaga znacznych nakładów finansowych, zakupienia specjalistycznych urządzeń (takich jak: centrale łączności ruchomej, mobilne i bazowe stacje nadawczo-odbiorcze, radiotelefony – przenośne, przewoźne i stacjonarne) oraz wybudowanie sieci szkieletowej i dostępowej na potrzeby omawianego systemu.

Ostatnią grupą zapewniającą łączność, jest telefonia satelitarna, która może być używana do uzupełnienia pokrycia obszarów i uzyskania łączności, których nie zapewniają inne jej środki. Telefonia ta zapewnia szeroką gamę usług, ale żeby z niej korzystać, trzeba posiadać specjalistyczny sprzęt i mieć opłacony abonament za korzystanie z jego usług. Dzięki systemom łączności satelitarnej, mamy dostęp do szeregu usług, między innymi:

- baz danych i lokalnych sieci komputerowych;
- Internetu (szybkie łącza);
- transferu plików;
- obsługi poczty elektronicznej;
- połączeń sieci lokalnych LAN z sieciami rozległymi WAN;
- wysokiej jakości wideofonii i wideokonferencji;
- dołączenia do sieci stacjonarnej systemów radiowego dostępu abonenckiego itp[18].

Należy pamiętać, że Polska nie posiada własnych systemów satelitarnych do obsługi tego typu połączeń. Istnieje więc niebezpieczeństwo odmowy świadczenia usługi dostępu do satelity telekomunikacyjnego przez nieprzychylne Polsce państwo, w sytuacjach zagrożeń.

PODSUMOWANIE

Reasumując, w sytuacjach szczególnych zagrożeń systemy telekomunikacyjne powinny:

- zapewnić bezstratną obsługę strumieni ruchu o różnym charakterze i różnym natężeniu;
- posiadać dużą zdolność adaptacyjną do zmiennych w czasie i przestrzeni warunków (większość użytkowników jest mobilna, nieznany jest czas, miejsce, zasięg, zakres wystąpienia sytuacji kryzysowej);
- posiadać dużą żywotność;
- charakteryzować się wysoką niezawodnością i gotowością do działania[19].

[17] [online]. [dostęp: 27.10.2011] Dostępny w Internecie: http://www.e2012.eu/pl/bezpiecze%C5%83stwo/1034/2/.

[18] J. Chrzęstek, *Struktura organizacyjna systemu łączności ratownictwa i zarządzania kryzysowego na poziomie lokalnym*, [w:] „Zeszyty Naukowe SGSP", nr 40/2010, Warszawa 2010.

Ponadto sieci i systemy teleinformatyczne wykorzystywane na potrzeby zarządzania kryzysowego powinny charakteryzować się niżej wymienionymi cechami:

1. Środki łączności, wydzielane na potrzeby zarządzania kryzysowego, powinny charakteryzować się odpowiednią mocą kryptograficzną, trudną do podsłuchania i przechwycenia informacji.
2. Częstotliwości poszczególnych urządzeń łączności powinny być niejawne.
3. Wykorzystywane środki łączności powinny być, w jak największym stopniu, autonomiczne – niezależne od sieci przewodowych.
4. Używane sieci i systemy teleinformatyczne powinny posiadać własne źródła zasilania.
5. Urządzenia łączności powinny być mobilne, dostosowane do pracy w różnych warunkach.
6. Pozyskiwany sprzęt teleinformatyczny, powinien być kompatybilny z innymi urządzeniami używanymi przez służby (organy), odpowiedzialne za bezpieczeństwo państwa.
7. Przepisy korespondencji radiowej, w czasie wykonywania wspólnych akcji ratunkowych, powinny być ujednolicone dla wszystkich korespondentów danej sieci lub kierunku radiowego.
8. Sprawdzenie tożsamości korespondenta, podczas przyjmowania i przekazywania wiążących decyzji (np. rozkazy, meldunki, kierowanie sił i środków do udziału w akcjach), powinno być bezwzględnie egzekwowane i potwierdzane za pomocą urządzeń, dostępnych tylko dla zamkniętej grupy użytkowników (sieci specjalne, niejawne, resortowe).

Zaproponowane wymagania są zgodne z rozporządzeniem Rady Ministrów w sprawie przygotowania i wykorzystania systemów łączności na potrzeby obronne państwa. Zgodnie z tym rozporządzeniem, do zapewnienia funkcjonowania państwa w razie zagrożenia bezpieczeństwa i w czasie wojny wykorzystywane są obronne systemy łączności, które powinny cechować się w szczególności:

- niezawodnością;
- odpornością na zakłócenia;
- zdolnością zapewnienia użytkownikom specjalnym bezpiecznego przekazywania informacji;
- zdolnością zachowania ciągłości łączności podczas zmian miejsc pracy, w ramach stanowisk kierowania;
- zdolnością do elastycznej rekonfiguracji systemu;
- zdolnością do preferencyjnej obsługi użytkowników specjalnych[20].

Z inicjatywy Centrum Projektów Informatycznych (CPI) MSWiA, miał powstać nowoczesny system łączności, który spełniałby wyżej wymienione wymagania. System

[19] Z. Fiołna, *Podsystem łączności w systemie kierowania reagowaniem kryzysowym*, [w:] *Organizacja łączności dla potrzeb kierowania reagowaniem kryzysowym na obszarze kraju*, pod red. J. Michniak, AON, Warszawa 2004, s. 100.

[20] Rozporządzenie Rady Ministrów z dnia 3 sierpnia 2004 r. w sprawie przygotowania i wykorzystania systemów łączności na potrzeby obronne państwa (Dz. U. z 2004 r. Nr 180, poz. 1855, § 10).

ten zwiększyłby poziom bezpieczeństwa publicznego w czasie zagrożeń oraz poprawiłby współdziałanie służb podczas EURO 2012. Zamówienie publiczne na: „Zaprojektowanie, budowę i wdrożenie Ogólnokrajowego Cyfrowego Systemu Łączności Radiowej – etap I", ze względu na przekroczenie limitu środków finansowych, zostało jednak unieważnione przez Ministerstwo Rozwoju Regionalnego[21] (13 kwietnia bieżącego roku).

Autor zdaje sobie sprawę, że ukazana problematyka nie zamyka zagadnień związanych z bezpieczeństwem teleinformatycznym w rozbudowanym systemie zarządzania kryzysowego, a w szerszym kontekście bezpieczeństwa państwa. Jest to tylko próba podjęta dla zainteresowania problematyką szerszego grona znawców tych zagadnień. Bezpieczeństwo teleinformatyczne to ideał, do którego należy dążyć, lecz trzeba mieć świadomość, iż nigdy nie zostanie osiągnięty.

LITERATURA

1. Chrzęstek J., *Struktura organizacyjna systemu łączności ratownictwa i zarządzania kryzysowego na poziomie lokalnym,* [w:] „Zeszyty Naukowe SGSP", nr 40/2010.
2. Chrząstek J. *Potrzeby i wymagania stawiane systemom łączności do działania w sytuacjach nadzwyczajnych zagrożeń*, [w:] „Zeszyty Naukowe SGSP", nr 33/2005, Warszawa 2005.
3. Decyzja Nr 24/MON Ministra Obrony Narodowej z dnia 31 stycznia 2006 r. w sprawie organizacji szczególnej ochrony systemów i sieci teleinformatycznych w resorcie obrony narodowej.
4. Decyzja Nr 357/MON Ministra Obrony Narodowej z dnia 29 lipca 2008 r. w sprawie organizacji i funkcjonowania systemu reagowania na incydenty komputerowe w resorcie obrony narodowej.
5. Denning Dorothy E., *Wojna informacyjna i bezpieczeństwo informacji*, Wydawnictwa Naukowo-Techniczne, Warszawa 2002, s. 59.
6. Fiołna. Z, *Podsystem łączności w systemie kierowania reagowaniem kryzysowym*, [w:] *Organizacja łączności dla potrzeb kierowania reagowaniem kryzysowym na obszarze kraju*, pod red. Michniak J., AON, Warszawa 2004, s. 100.
7. Kowalewski M., Kowalczyk B., Hendler Z., *System łączności na potrzeby służb bezpieczeństwa publicznego i zarządzania kryzysowego w aglomeracji miejskiej*, [w:] „Telekomunikacja i Techniki Informacyjne", nr 3-4/2008, Warszawa 2008, s. 33-48.
8. Rozporządzenie Rady Ministrów z dnia 3 sierpnia 2004 r. w sprawie przygotowania i wykorzystania systemów łączności na potrzeby obronne państwa (Dz. U. z 2004 r. Nr 180, poz. 1855, § 10).
9. Szleszyński A., Witkowski M., *Szkolenie użytkowników w procesie ochrony informacji wykorzystywanych w systemach wsparcia dowodzenia*, [w:] „Zeszyt Naukowe WSOWL", nr 2/2010, WSOWL, Wrocław 2010, s. 193-202.
10. Ustawa z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (Dz. U. z 2004 r. Nr 171, poz. 1800 z późn. zm.).

[21] [online]. [dostęp: 30.10.2011]. Dostępny w Internecie: http://cpi.mswia.gov.pl/portal/cpi/138/3143/OCSLR__etap_I.html.

11. Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. z 2002 r. Nr 144, poz. 1204).
12. Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U. z 2007 r. Nr 89, poz. 590, art. 2 z późn. zm.).
13. Witkowski M., *Analiza systemowa zjawiska cyberterroryzmu na przełomie XX – XXI w. w warunkach RP*, praca studyjna pod kierunkiem P. Sienkiewicz, AON, Warszawa 2005, s. 29-30.
14. [online]. [dostęp: 25.10.2011]. Dostępny w Internecie: http://radioscannerpolska.pl/ index.html.
15. [online]. [dostęp: 27.10.2011]. Dostępny w Internecie: http://www.e2012.eu/pl/ bezpiecze%C5%83stwo/1034/2/.
16. [online]. [dostęp: 24.10.2011]. Dostępny w Internecie: http://www.iniejawna.pl/ pomoce/przeciw_zagr.html.
17. [online]. [dostęp: 30.10.2011]. Dostępny w Internecie: http://media2.pl/ telekomunikacja/64470-Powodz-Problemy-z-lacznoscia-komorkowa.html.
18. [online]. [dostęp: 30.10.2011]. Dostępny w Internecie: http://www.wiadomosci. swidnickie.pl/wiadomosci-24/1-wiadomosci24/5121-gotowi-na-kryzys.
19. [online]. [dostęp: 30.10.2011]. Dostępny w Internecie: http://cpi.mswia.gov.pl/ portal/cpi/138/3143/OCSLR__etap_I.html.

SECURITY OF ICT SYSTEMS IN CRISIS MANAGEMENT

Summary

The article presents ICT (Information and Communication Technology) networks and systems that are used to provide communications for crisis management purposes. The articles describes wired and wireless communication assets and discusses their advantages and disadvantages when they are used to carry out national security tasks.

Key words: *ICT security, ICT networks, ICT systems, crisis management*