FUNKCJONOWANIE SYSTEMU TELEKOMUNIKACYJNEGO ADMINIMSTRACJI PUBLICZNEJ

Jacek Matyszczak

WYMAGANIA FIZYCZNE I ŚRODOWISKOWE
Obszar publiczny

Rozwój systemów teleinformatycznych, a także systematycznie rosnące zapotrzebowanie administracji publicznej na szybką transmisję danych i dostępność do coraz to nowych usług przyczyniły się do rozpoczęcia prac nad budową rozległej sieci teleinformatycznej, zdolnej sprostać współczesnym wymaganiom. W niniejszym opracowaniu przedstawiono analizę aktualnego stanu systemu telekomunikacyjnego administracji publicznej, uzasadniającą planowane kierunki zmian. W przedstawionym ujęciu system telekomunikacyjny, dalej zwany systemem, jest rozumiany jako wspólna platforma teleinformatyczna, umożliwiająca połączenie sieci teleinformatycznych poszczególnych resortów. Będzie on zaspokajać potrzeby administracji publicznej, systemu kierowania bezpieczeństwem narodowym, bezpieczeństwem i porządkiem publicznym oraz potrzeby ratownictwa.[1] Do zadań związanych z opracowaniem programu budowy systemu prezes Rady Ministrów powołał w 2006 roku międzyresortowy zespół, którego kierownictwo powierzył prezesowi Urzędu Komunikacji Elektronicznej.[2]

1) Obecnie administracja publiczna korzysta z telekomunikacyjnej infrastruktury resortowej oraz systemów telekomunikacyjnych największych operatorów, takich jak: Telekomunikacja Polska SA, EXATEL, Telekomunikacja Kolejowa, Netia SA oraz Telefonia Dialog.

2) Międzyresortowy zespół powołano na mocy *Zarządzenia Prezesa Rady Ministrów nr 89 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. Zostało ono znowelizowane Zarządzeniem Prezesa Rady Ministrów nr 145 z dnia 20 września 2006 r. zmieniającym zarządzenie w sprawie utworzenia Zespołu Międzyresortowego.*

OGÓLNA CHARAKTERYSTYKA SYSTEMU TELEKOMUNIKACYJNEGO ADMINISTRACJI PUBLICZNEJ

Administracja publiczna do wykonywania swoich obowiązków korzysta obecnie z wielu systemów łączności i informatyki. Nie zawsze mogą być one wykorzystywane do wzajemnego przekazywania danych i komunikowania się, gdyż zwykle są przeznaczone do zadań wynikających z funkcji jednostek organizacyjnych, dla których zostały zbudowane. Na przykład, w Ministerstwie Spraw Wewnętrznych i Administracji korzysta się między innymi z sieci PESEL-NET – na potrzeby przekazu danych, oraz z sieci transmisyjnej dla Policji – POLWAN. W Ministerstwie Finansów używa się systemów na potrzeby izb skarbowych i urzędów skarbowych, natomiast urząd ceł ma własny system teleinformatyczny. Szacuje się, że w kraju działa kilkaset systemów, których obsługą zajmuje się wiele zespołów ludzkich. Potencjalny użytkownik kilku systemów najczęściej musi posiadać na swoim stanowisku pracy dedykowane do nich terminale. Ze względu na ograniczenia finansowe podmiotów użytkujących te systemy, duża ich część nie ma zabezpieczeń w zakresie niezawodności, integralności i wiarygodności. Ze względu na istnienie niezależnych infrastruktur dla każdego z nich, a co za tym idzie różnych standardów rozwiązań i interfejsów, brakuje możliwości zastosowania jednolitych mechanizmów zarządzania, bezpieczeństwa i ochrony. Problem ten w znacznym stopniu dotyka również systemów i sieci teleinformatycznych przeznaczonych do przekazywania i przetwarzania informacji niejawnych.

Systemy teleinformatyczne przeznaczone do przekazywania (przetwarzania) informacji niejawnych są zaliczane do tzw. systemów łączności specjalnej. Potocznie są rozumiane jako systemy zapewniające skuteczną komunikację służbom bezpieczeństwa publicznego i ratownictwa.

Ze względu na przeznaczenie stosuje się ich podział na cztery grupy: bezpieczną łączność rządową, łączność na potrzeby kierowania bezpieczeństwem narodowym, łączność na potrzeby armii oraz bezpieczną sieć administracji publicznej. Wytwarzanie, przetwarzanie, przechowywanie lub przekazywanie informacji niejawnych z wykorzystaniem technik komputerowych lub technik transmisji danych może być dokonywane jedynie

w systemach i sieciach teleinformatycznych, w stosunku do których został przeprowadzony proces akredytacji.[3] Połowa spośród ponad dwudziestu akredytowanych systemów ma jedynie dopuszczenie do przekazywania informacji niejawnych stanowiących tajemnicę służbową, bowiem stosowane w nich urządzenia i sieci nie spełniają wymagań w zakresie utajniania informacji o wyższej klauzuli. W systemach, o których mowa, wykorzystuje się różne standardy i technologie, począwszy od sieci PSTN, standardu ISDN, sieci publicznej i dedykowanej (transmisji opartej na protokołach IP), po sieci GSM i łącza satelitarne. Analizując listę certyfikowanych rozwiązań ochrony kryptograficznej[4], zauważamy przewagę szyfrujących urządzeń przeznaczonych do tradycyjnej sieć telefonicznej. Sieć ta jest wykorzystywana również do przesyłania informacji niejawnych zaszyfrowanych w trybie off-line. Szyfratory IP stanowią obecnie niewielką grupę certyfikowanych urządzeń stosowanych do utajniania informacji. Niestety w tej grupie nie ma szyfratorów umożliwiających ochronę informacji stanowiących tajemnicę państwową.[5] Obecnie brakuje akredytowanego, jednolitego i uniwersalnego rozwiązania (w postaci systemu lub sieci teleinformatycznej), które obejmowałoby wszystkie jednostki organizacyjne administracji publicznej. Taką interoperacyjność ma zapewnić budowany system.

WPŁYW POTENCJALNYCH ZAGROŻEŃ NA SYSTEM TELEKOMUNIKACYJNY

Zagrożenia mające istotny wpływ na bezpieczeństwo infrastruktury telekomunikacyjnej administracji publicznej to głównie działania o cha-

---

3) Ustawa z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych (DzU z 2005 r. nr 196, poz. 1631).

4) Lista certyfikowanych rozwiązań ochrony kryptograficznej jest dostępna na stronie internetowej Agencji Bezpieczeństwa Wewnętrznego – http:// www.abw.gov.pl/.

5) Obecnie administracja publiczna korzysta z telekomunikacyjnej infrastruktury resortowej oraz systemów telekomunikacyjnych największych operatorów,

rakterze terrorystycznym. Mogą być one przeprowadzane w formie bezpośredniego fizycznego ataku na elementy infrastruktury telekomunikacyjnej albo pośrednio, poprzez oddziaływanie na inne elementy infrastruktury krytycznej. Przez pojęcie infrastruktury krytycznej rozumiemy kluczowe elementy gospodarki narodowej, których uszkodzenie lub zniszczenie miałoby negatywny wpływ na funkcjonowanie społeczeństwa, zagrażając bezpieczeństwu lub gospodarce państwa.

W atakach terrorystycznych mogą być wykorzystywane:

- konwencjonalne ładunki wybuchowe lub broń biologiczna i chemiczna, pozwalająca uzyskać efekt psychologiczny nieporównywalnie większy niż wywołany wybuchem zwykłej bomby;
- urządzenia wytwarzające wysokoenergetyczne impulsy elektromagnetyczne (Elektro Magnetic Pulse – EMP) oraz promieniowanie mikrofalowe – zakłócające propagację sygnałów radiowych oraz pracę systemów elektronicznych. W skrajnych wypadkach mogą one prowadzić do całkowitego zniszczenia tych systemów. Ostatnie doświadczenia z konfliktów zbrojnych potwierdziły wysoką sprawność urządzeń EPM. Stosowało je lotnictwo USA, najpierw przeciwko instalacjom radarowym Iraku (1991 r.), a później przeciwko infrastrukturze teleinformatycznej byłej Jugosławii. Zdaniem przedstawicieli armii rosyjskiej, urządzenia takie stosowała również strona czeczeńska do niszczenia rosyjskiego systemu komunikacji elektronicznej. Tylko kwestią czasu jest wykorzystanie tego typu urządzeń przez grupy terrorystyczne, bowiem zbudowanie broni EMP z powszechnie dostępnych elementów zajęło specjalistom z Departamentu Obrony USA jedynie dwa tygodnie, a jej jednostkowy koszt nie przekroczył 500 USD. Skonstruowane w ten sposób urządzenie mieściło się w półciężarówce, ale jego miniaturyzacja dzięki wykorzystaniu nowych technologii nie nastręcza obecnie większego problemu;
- środki informatyczne do zdobywania kodów i haseł, pozwalających przeprowadzić atak na elementy infrastruktury krytycznej;
- sieć internetowa – za jej pomocą wykonuje się działania blokujące, niszczące lub zniekształcające informację przetwarzaną, przechowywaną i przekazywaną w systemach informatycznych

administracji lub podmiotów gospodarczych. Ataki prowadzi się zdalnie, w tym również spoza kraju. W wypadku gdy cała infrastruktura państwowa zostanie dotknięta zorganizowanym atakiem internetowym, jak to miało miejsce w Estonii, można mówić o cyberkonflikcie.

WYMAGANIA FUNKCJONALNE DLA SYSTEMU TELEINFORMATYCZNEGO

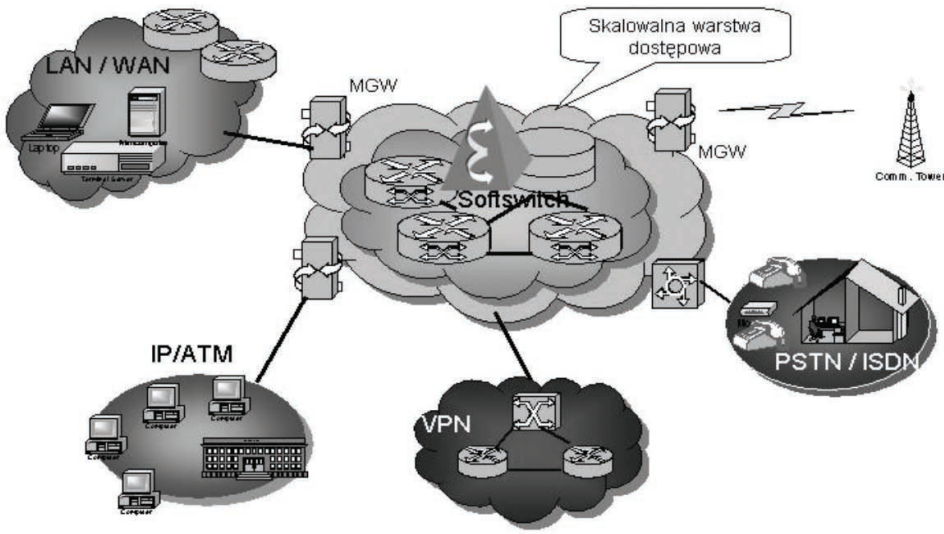
Zasadniczym celem budowy systemu jako wspólnej sieci teleinformatycznej dla wszystkich podmiotów administracji publicznej jest umożliwienie im sprawnego wykonywania zadań w wymiarze krajowym i międzynarodowym. Przyjęto założenie, że skład i struktura systemu będą dostosowane do kierowania państwem w czasie pokoju, a także w sytuacji kryzysowej i podczas wojny. Pierwszy etap jego budowy obejmie funkcje na czas pokoju. Następnie sukcesywnie będzie on rozbudowywany o funkcje niezbędne do kierowania obronnością państwa.

Z uwagi na wymaganą stabilność technologiczną założono, że system powstanie w okresie nie dłuższym niż pięć lat. Przyjęto również, że zapewni on:

- niezawodną, odpowiedniej jakości łączność, gwarantującą właściwe funkcjonowanie struktur rządowych, administracji państwowej i samorządowej, a także sił zbrojnych oraz służb odpowiedzialnych za bezpieczeństwo i ratownictwo w czasie pokoju, kryzysu i wojny;
- natychmiastową dostępność;
- skalowanie sieci w celu sprostania bieżącym i przyszłym, jeszcze niezdefiniowanym wymaganiom ruchu IP;
- zdolność dostosowywania się do zmiennej liczby użytkowników systemu, szczególnie w sytuacjach kryzysowych i podczas wojny;
- efektywne wykorzystanie posiadanych zasobów;
- możliwość wykorzystania systemów resortowych bez naruszania ich struktury;
- konwergencję usług i aplikacji.

KONCEPCJA SYSTEMU TELEINFORMATYCZNEGO

Opracowana przez międzyresortowy zespół koncepcja zakłada zbudowanie sieci nakładkowej, która w sposób wirtualny objęłaby istniejącą resortową infrastrukturę telekomunikacyjną. Byłaby ona rozwijana w kierunku sieci konwergentnej z integracją usług i ewolucyjnym przejściem do sieci pakietowej. Zakłada się osiągnięcie wymaganej funkcjonalności sieci nakładkowej dzięki zastosowaniu rozwiązań nowej generacji – NGN (ang. *Next Generation Networks*) opartych na protokole IP. Do tworzenia sieci NGN będzie wykorzystana nowoczesna platforma pakietowa typu softswitch, która wraz z towarzyszącymi jej bramami medialnymi (MGW), poprzez obsługę mechanizmów translacji, stworzy pomost między dzisiejszymi technologiami stosowanymi w sieciach resortowych. Istotną cechą softswitch jest rozproszony system przełączania, oparty na wielu komponentach sieciowych, współpracujących ze sobą przez otwarte interfejsy i protokoły komunikacyjne, a zarządzany z jednego miejsca w sieci (rys. 1).



Rys. 1. Zastosowanie technologii softswich jako podstawowej platformy technicznej dla systemu

System zarządzania będzie nadrzędny, integrując zarazem różne systemy resortowe. Istotę samego centrum przełączania softswitcha stanowi rozległy system komutacji, spełniający w tradycyjnych rozwiązaniach funkcję przestrzenno-czasowej matrycy przełączającej. W przyjętym rozwiązaniu pole komutacji nie jest więc zlokalizowane w jednym miejscu centrali przełączającej, lecz będzie konfigurowane między oddalonymi obiektami komutacji, którymi są rozproszone bramy medialne. Należy podkreślić, że bramy te są elementami konsolidującymi różne mechanizmy transportowe sieci w ramach jednego wspólnego rozwiązania. Zdolne są do komunikowania się z siecią transportową oraz zewnętrznym sprzętem telekomunikacyjnym użytkownika.

W proponowanej architekturze systemu proces konwergencji usług będzie prowadzony etapowo. W pierwszej kolejności zostanie wyeliminowana separacja głosu i danych, którą zastąpi jednolita transmisja pakietowa, wspólna dla wszystkich przekazów multimedialnych (głos, dane i obraz). W końcowym etapie nastąpi integracja wszystkich usług telekomunikacyjnych w jednej szerokopasmowej platformie IP. Konwergencji usług będzie towarzyszyć stopniowa integracja sieci resortowych przez tworzenie kolejnych połączeń międzysieciowych oraz sieci wielousługowych, wykorzystujących różne platformy komunikacji. Ponadto będą się zacierać wymagania w przepływności sieci LAN i WAN, co ułatwi tworzenie i łączenie w całość segmentów sieci telekomunikacyjnych. Wykorzystanie wirtualnych sieci VPN (*Virtual Private Network*) pozwoli na dynamiczne tworzenie wydzielonych logicznie i bezpiecznych kanałów komunikacyjnych odległych lokalizacji przez różne rodzaje środków transportowych, między innymi sieci komutowane SDH, sieci pakietowe, a przede wszystkim przez sieć Internet. Jest oczywiste, że nie wszystkie wdrażane rozwiązania przetrwają próbę czasu, część z nich bowiem ulegnie samoistnej „likwidacji" z powodów technicznych lub ekonomicznych.

Budowany system pozwoli stworzyć jednolity dla wszystkich użytkowników system łączności z własną adresacją, zapewniający również nomadyczność użytkowników. Podstawową korzyścią zastosowania tej architektury jest możliwość wykorzystania dotychczas używanych środków łączności. Sieć Internet będzie wykorzystywana w systemie jako jedno z mediów, nigdy natomiast samodzielnie – z uwagi na brak gwarancji parametrów jakościowych i wydajnościowych, a także konieczność szyfrowania w celu zapewnienia bezpieczeństwa przesyłanych danych.

W systemie zostaną zaimplementowane elementy polityki bezpieczeństwa teleinformatycznego, takie jak:

- ograniczanie dostępności funkcji,
- ograniczanie uprawnień,
- lokalna obrona,
- weryfikacja poprawności działania.

W odniesieniu do przesyłania i przetwarzania informacji niejawnych koncepcja zakłada powstanie jednolitej platformy kryptograficznej na poziomie łączności telefonicznej oraz sieci rozległej IP. Szyfratory warstwy IP pozwolą tworzyć prywatne sieci VPN, łączące w bezpieczny sposób sieci lokalne. Jako platforma informatyczna do transmisji informacji niejawnych będzie wykorzystana jedna z sieci resortowych – odpowiednio doposażona. Informacje zastrzeżone będą przesyłane za pomocą sieci internetowej – z wykorzystaniem protokołów bezpiecznych połączeń dla abonentów uprawnionych – i tunelowane. Istotną rolę będą odgrywać wirtualne sieci budowane dla administracji samorządowej, która w dużej części posiada jedynie dostęp do Internetu.

W programie budowy systemu uwzględniono możliwość wykorzystania dotychczasowych wyników prac prowadzonych w ramach STAP (systemu teleinformatycznego administracji państwowej) i SKBN (systemu kierowania bezpieczeństwem narodowym).

PODSUMOWANIE

1. Obecnie istniejące systemy teleinformatyczne administracji publicznej nie dają możliwości stworzenia jednolitej platformy teleinformatycznej o zasięgu ogólnopolskim, zapewniającej komunikację między urzędami, bezpieczny dostęp do Internetu, nowych usług, a także stosowanie jednolitej polityki bezpieczeństwa.

2. Podjęcie działań związanych z budową nowego systemu wynikało z dynamicznego rozwoju technologii informatycznych oraz rosnącego zapotrzebowania administracji publicznej na dostęp do usług.

3. Głównym celem budowy systemu na potrzeby administracji publicznej, systemu kierowania bezpieczeństwem narodowym, bezpieczeństwem i porządkiem publicznym oraz na potrzeby ratownictwa jest zapewnienie wspólnej, bezpiecznej sieci teleinformatycznej dla wszystkich podmiotów administracji.

Literatura

1. Sutton Roger J., *Bezpieczeństwo telekomunikacji, praktyka i zarządzanie,* tłum. Grzegorz Słowikowski, Wyd. Komunikacji i Łączności 2004.

2. *Zarys koncepcji jednolitej platformy kryptograficznej,* oprac. zbiorowe Departamentu Bezpieczeństwa Teleinformatycznego ABW, Warszawa 2007.

3. *Organizacja i usługi STAP – założenia kierunkowe,* oprac. Zespół Międzyresortowy do spraw Sieci Teleinformatycznej Administracji Publicznej, Warszawa 2004.