

Piotr SIENKIEWICZ
prof. dr hab. inż.
Akademia Obrony Narodowej

Michał GAWROŃSKI
mgr inż.
Wojskowy Instytut Łączności

kpt. Tomasz CZAJKA
mgr inż.
Wojskowy Instytut Łączności

**Zarządzanie ochroną informacji
w systemie teleinformatycznym administracji publicznej**

1. WSTĘP

Prace nad koncepcją systemu telekomunikacyjnego administracji publicznej zostały zapoczątkowane zarządzeniem nr 89 Prezesa Rady Ministrów z dn. z dnia 1 czerwca 2006 r. o utworzeniu Miedzyresortowego Zespołu do spraw opracowania programu zapewnienia łączności na potrzeby administracji publicznej, systemu kierowania bezpieczeństwem narodowym, bezpieczeństwem i porządkiem publicznym oraz na potrzeby ratownictwa. Zespół ten miał za zadanie opracowanie planu budowy takiego systemu. Wyniki prac wstępnych zostały zaprezentowane na sesji Krajowego Sympozjum Telekomunikacji i Teleinformatyki w roku 2008. Sesja ta odbyła się pod patronatem Biura Bezpieczeństwa Narodowego. Wyniki prac zostały również zaprezentowane w publikacji Biura Bezpieczeństwa Narodowego [1]. Wśród opublikowanych materiałów jest artykuł dr Jacka Matuszczaka [8], który przedstawia wymagania funkcjonalne i środowiskowe, ogólną charakterystykę, analizę zagrożeń, wymagania funkcjonalne oraz koncepcję systemu teleinformatycznego administracji publicznej. W koncepcji zasygnalizowany został problem konieczności zapewnienia bezpieczeństwa informacji poprzez zastosowanie metod kryptograficznych. Nieodłącznie z zagadnieniem bezpieczeństwa informacji wiąże się polityka bezpieczeństwa teleinformatycznego, w skład, której wchodzi również kryptograficzne metody ograniczenia dostępu użytkowników do materiałów klasyfikowanych.

Zastosowanie metod kryptograficznych jest najlepszą metodą zapewnienia poufności informacji przesyłanych i przetwarzanych w systemie telekomunikacyjnym administracji publicznej. Dodatkowo można zapewnić również funkcje integralności, niezaprzeczalności nadania i odbioru, jak również zapoznania się z informacjami. Systemy telekomunikacyjne i teleinformatyczne, wykorzystywane dla potrzeb bezpieczeństwa państwa (nazywane systemami specjalnymi), powinny podlegać szczególnej ochronie. System administracji publicznej z całą pewnością mieści się w tej kategorii. Sprawność działania oraz wiarygodność informacji i danych przetwarzanych i przesyłanych za pośrednictwem sieci TI i TK powinny mieć najwyższy z możliwych do osiągnięcia stanów (poziomów bezpieczeństwa i wiarygodności). Wprowadzenie urządzeń kryptograficznych do systemu łączności nieodłącznie wiąże się z koniecznością opracowania i wdrożenia sprawnego systemu zarządzania danymi dla systemu ochrony informacji działającego w systemie telekomunikacyjnym. Należy również zwrócić uwagę na fakt, iż nie wszystkie informacje wytwarzane, przetwarzane i przesyłane w systemie TI muszą być zabezpieczone

z wykorzystaniem szyfrowania. Jednak powinna być zapewniona ich wiarygodność oraz pełna rozliczalność korzystania z nich przez użytkowników systemu. Wymagania te również powinny być realizowane z zastosowaniem metod kryptograficznych.

Niniejsze opracowanie jest próbą przedstawienia wymagań na system zarządzania informacjami niezbędnymi dla poprawnej i zgodnej z oczekiwaniami użytkowników systemu ochrony informacji systemu telekomunikacyjnego administracji publicznej.

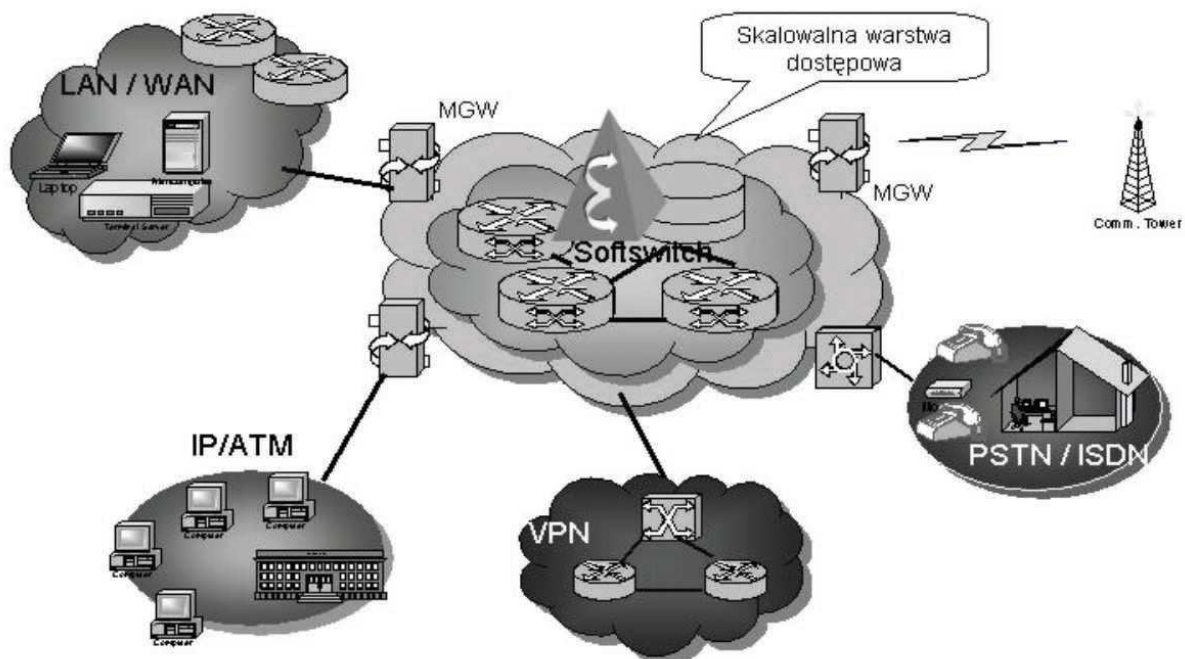
2. WYMAGANIA FUNKCJONALNE I KONCEPCJA SYSTEMU

Wymagania funkcjonalne dla systemu teleinformatycznego administracji publicznej zostały wyspecyfikowane w artykule [8]. Przy opracowywaniu wymagań przyjęto założenie, że skład i struktura systemu będą dostosowane do kierowania państwem w czasie pokoju, w czasie sytuacji kryzysowej, a także w czasie wojny. Pierwszy etap prac powinien dostosować system do wymagań czasu pokoju.

System ma zapewnić [8]:

- 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.

Na podstawie zdefiniowanych wymagań funkcjonalnych przedstawiona została koncepcja systemu teleinformatycznego. Koncepcja opracowana przez Międzyresortowy Zespół „zakłada zbudowanie sieci nakładkowej, która w sposób wirtualny objęłaby istniejącą resortową infrastrukturę telekomunikacyjną.” [8]. Koncepcja sieci zakłada wykorzystanie rozwiązań opartych na protokole IP. Poniżej przedstawiony jest schemat takiej sieci [8].



Schemat sieci dla administracji publicznej [8]

Koncepcja systemu zakłada powołanie jednego centrum zarządzania siecią. System zarządzania powinien być nadrzędny, integrując zarazem różne systemy resortowe [8]. Przewiduje ona również (koncepcja) zastosowanie szyfrowania, jako metody zapewnienia bezpieczeństwa informacji przesyłanej poprzez sieć. Dodatkowo należy również stwierdzić, iż należy chronić nie tylko informację przesyłaną, ale informację w ogóle. Należy chronić informację od momentu jej wytworzenia, poprzez składowanie, przetwarzanie, udostępnianie przesyłanie i kasowanie, czyli przez cały cykl życia informacji.

Zapoznając się z koncepcją systemu przedstawioną w pracy [8], należy zwrócić uwagę na konieczność postania „jednolitej platformy kryptograficznej na poziomie łączności telefonicznej oraz sieci rozległej IP”. Podejście takie zakłada opracowanie od podstaw systemu ochrony informacji, obejmującego zarówno środki sprzętowe jak i programowe, indywidualne jak i grupowe. W pierwszych etapach opracowania systemu należałoby się jednak zastanowić nad możliwością włączenia istniejących systemów ochrony informacji do powstającego systemu.

3. URZĄDZENIA ZABEZPIECZENIA INFORMACJI

Zapewnienie bezpieczeństwa informacji w takim systemie będzie wymagać zastosowania różnorodnych metod, urządzeń i mechanizmów. System zabezpieczenia informacji nazywać będziemy systemem ochrony informacji (SOI) dla potrzeb sieci

teleinformatycznej (TI). Zakładając budowę systemu TI dla potrzeb administracji od „podstaw”, można pominąć integrację i zabezpieczenie dotychczas eksploatowanych. Podejście takie znacznie ułatwia opracowanie koncepcji i projektu systemu zabezpieczenia informacji. Jeżeli jednak przyjęta zostanie częściowej integracji już eksploatowanych systemów ochrony informacji, należy zapewnić możliwość współpracy między różnymi urządzeniami i systemami.

Zabezpieczenie informacji może być zrealizowane poprzez zastosowanie dedykowanych urządzeń ochrony informacji (już opracowanych) oraz poprzez opracowanie nowych (dedykowanych), zgodnie ze zidentyfikowanymi potrzebami systemów i użytkowników. Można wyróżnić następujące rodzaje urządzeń ochrony informacji:

1. urządzenia do ochrony łączy grupowych – instalowane na łączach między węzłami (centralami) łączności,
2. urządzenia indywidualne – instalowane u użytkowników systemów łączności i transmisji, połączenia telefoniczne i sieciowe (teleinformatyczne),
3. urządzenia indywidualne mobilne – przeznaczone do użytku w ruchu i warunkach polowych (poza stałym miejscem pracy, służby),
4. urządzenia do ochrony informacji w trybie offline – służące do zabezpieczenia informacji składowanej na stacjach roboczych,
5. urządzenia do zabezpieczenia baz danych – składowanych w miejscach posadowienia serwerów systemów teleinformatycznych,
6. urządzenia do ochrony transmisji w sieciach radiowych – eksploatowanych przez służby mundurowe, służby ratownicze.
7. urządzenia do identyfikacji użytkowników – przeznaczone do przenoszenia i zabezpieczenia informacji o użytkownikach systemu, ich rolach, zadaniach i możliwościach dostępu do informacji, jak również gwarantujących tożsamość użytkownika.

W systemie ochrony informacji mogą występować również narzędzia kryptograficzne, które nie są oddzielnymi urządzeniami, jednak realizują zadania zabezpieczenia informacji.

Wspólną cechą wymienionych urządzeń i mechanizmów jest konieczność zapewnienia im danych kryptograficznych (kluczy kryptograficznych), umożliwiających poprawne realizowanie funkcji zabezpieczeń. Spełnienie tego wymagania realizowane jest poprzez system zarządzania systemem ochrony informacji. System taki nazywany jest Systemem Zarządzania Danymi Kryptograficznymi – SZDK. W nazewnictwie anglojęzycznym nosi nazwę Key Management System (KMS).

Dodatkowo w systemie występują urządzenia przeznaczone do dystrybucji danych kryptograficznych (DK) od centrów wytwarzania do miejsca eksploatacji. Urządzenia takie noszą nazwę nośników DK i również muszą posiadać odpowiednie zabezpieczenia (zgodnie z klauzulą przenoszonych danych).

4. ROLA I MIEJSCE SZDK W SYSTEMIE OCHRONY INFORMACJI SYSTEMU TI

Zastosowanie mechanizmów kryptograficznych pociąga za sobą konieczność stworzenia całej infrastruktury, której zadaniem będzie planowanie, wytwarzanie i dostarczanie danych kryptograficznych niezbędnych do poprawnej pracy systemu ochrony informacji sieci teleinformatycznej. Zadania te są realizowane przez system zarządzania danymi kryptograficznymi – SZDK. System SZDK może składać się z jednej stacji, zaopatrującej w niezbędne dane wszystkie elementy systemu, lub z wielu stacji, połączonych w wydzieloną logicznie sieć dystrybucji.

Współczesne stacje zarządzania realizują zadania z zakresu planowania powiązań kryptograficznych, generacji danych, ich zabezpieczenia na wszystkich etapach życia, dostarczenie do urządzeń (miejsc eksploatacji), jak również wytwarzają całość dokumentacji niezbędnej dla sprawnego i bezpiecznego procesu dystrybucji, jak również właściwego wykorzystania urządzeń ochrony informacji.

Systemy zarządzania posiadają właściwe narzędzia, umożliwiające planowanie i generowanie (wytwarzanie) danych kryptograficznych. Proces dystrybucji realizowany może być w różny sposób, w zależności od potrzeb i możliwości. Dystrybucja nie jest procesem skomplikowanym, jeżeli obsługiwana jest mała liczba urządzeń. Skala trudności wzrasta znacznie wraz ze wzrostem liczby urządzeń ochrony informacji obsługiwanych przez jedną stację. Liczba urządzeń warunkuje bowiem liczbę potrzebnych danych kryptograficznych wytwarzanych przez system oraz sam proces dystrybucji. Większa liczba danych niezbędnych do rozprowadzenia powoduje również wzrost zagrożenia, jakim podlegają dane. Problemy te próbuje się rozwiązać poprzez opracowanie kompleksowych systemów zarządzania danymi kryptograficznymi, które to będą wspomagać użytkownika w zarządzaniu systemem ochrony informacji. Niezmiernie ważne jest tu słowo *wspomagać*, gdyż nawet najlepszy system nie zastąpi użytkownika w podejmowaniu decyzji. Może jednak wspomagać jego pracę oraz kontrolować jego decyzje w zakresie utrzymania spójności systemu. System zarządzania powinien być centralnym elementem takiego systemu ochrony informacji, odpowiedzialnym za jego właściwą organizację i działanie. Ma on bowiem wszelkie dane niezbędne do prawidłowego konfigurowania systemu, umożliwienia realizacji

procesów uwierzytelnienia użytkowników systemu, zapewnia dane do realizacji praw dostępu do zasobów i funkcji ochrony dostępu do urządzeń systemu. System zarządzania, będąc najważniejszym elementem bezpiecznego systemu ochrony informacji, musi podlegać szczególnej ochronie i zabezpieczeniom, zarówno fizycznym jak i organizacyjnym. Dlatego też jest niezmiernie trudno zdobyć informacje o istniejących wykonaniach systemów zarządzania danymi kryptograficznymi, zarówno na rynku komercyjnym jak i specjalnym (służby ochrony państwa). Dlatego też zagadnienie budowy systemu zarządzania jest niezmiernie ciekawe i zarazem jest wyzwaniem. Zaprojektowanie systemu, jak również jego realizacja, pozwoli na opracowanie mechanizmów zapewniających bezpieczną i prawidłową pracę systemu ochrony informacji. Szczęólnego znaczenia nabiera opracowanie systemu dla specjalnych sieci teleinformatycznych, dla których określa się znacznie ostrzejsze wymagania bezpieczeństwa niż dla systemów komercyjnych. Ilość zadań realizowanych przez takie sieci pociąga za sobą konieczność zastosowania różnych mechanizmów kryptograficznych. Zastosowanie różnych mechanizmów w połączeniu z dużą ilością danych kryptograficznych, powoduje, iż człowiek nie jest w stanie zapanować nad całym procesem konfiguracji, generacji i dystrybucji. Ilość kombinacji połączeń przekracza często możliwość percepcji człowieka. Dlatego też tak ważny jest element wspomagający, odpowiadający za proces konfiguracji – system zarządzania danymi kryptograficznymi.

Rozbudowa systemów ochrony informacji powoduje również rozbudowę systemów zarządzania. W pewnym momencie okazuje się, że jednostanowiskowa stacja, usytuowana w centralnym miejscu sieci telekomunikacyjnej, nie nadaża z obsługą urządzeń ochrony informacji. Rozwiązaniem jest właśnie zaprojektowanie i wykonanie systemu zarządzania planowaniem, generacją i elektroniczną dystrybucję danych kryptograficznych.

Dodatkowym elementem współczesnego i nowoczesnego systemu ochrony informacji powinien być system zarządzania uprawnieniami użytkowników systemu. System takie, będąc częścią systemu ochrony informacji, odpowiada za udostępnienie użytkownikom informacji zgodnie z przyjętą polityką bezpieczeństwa oraz zgodnie z posiadanymi przez nich uprawnieniami. W odniesieniu do systemu TI dla administracji publicznej system ochrony informacji być może będzie realizował więcej zadań z zakresu zapewnienia integralności danych, oraz niezaprzeczalności nadania i odbioru, a mniej z zakresu poufności. Nie zmienia jednak to zakresu wymagań dla systemu SZDK.

Rozpatrując taki system na potrzeby systemu TI administracji publicznej można przyjąć, iż będzie on usytuowany w centrum takiego systemu. Centralny punkt (stacja) będzie zajmować się wytarzaniem DK oraz udostępnianiem ich użytkownikom końcowym. W celu

zwiększenia elastyczności systemu planowania połączeń utajnionych oraz określania praw dostępu użytkowników do zasobów systemu, należy rozważyć możliwość powołania lokalnych centrów planowania i redystrybucji DK. W dobie powszechnej obecności internetu można przyjąć, iż dostarczanie DK będzie odbywać się drogą elektroniczną, jednak nie można całkowicie wyeliminować dystrybucji z wykorzystaniem indywidualnych nośników, dostarczanych przez kurierów. Dystrybucja taka będzie mieć miejsce przy rozbudowie systemu o nowych użytkowników, jak również w sytuacjach, gdy zajdzie konieczność całkowitego „odcięcia” się od skompromitowanych danych.

5. ANALIZA POTRZEB INFORMACYJNYCH SZDK

System SZDK wymaga dostarczenia danych i informacji, na podstawie których będą realizowane zadania konfiguracji połączeń, ustalania praw dostępu oraz dystrybucji wytworzonych danych. Dane te są niezbędne do zaplanowania i wytworzenia danych kryptograficznych, wykorzystywanych przez urządzenia i narzędzia ochrony. Proces pozyskiwania informacji nie jest łatwy, szczególnie w systemie rozproszonym, o różnorodnych środkach łączności i narzędziach przetwarzania danych.

Rozważając proces analizowania potrzeb komunikacyjnych na etapie opracowywania koncepcji, a później projektu systemu, należy rozpocząć od zdefiniowania potrzeb poszczególnych użytkowników systemu oraz zasad wymiany informacji między poszczególnymi jednostkami. Analiza taka powinna zawierać nie tylko potrzeby komunikacyjne, ale również klauzulę przesyłanych informacji (zgodnie z ustawą o ochronie informacji niejawnych [10]). Zebrane dane powinny umożliwić określenie wagi informacji oraz niezbędnego sposobu zabezpieczenia, na danym szczeblu oraz dla danego rodzaju informacji. Inne będą potrzeby zabezpieczenia informacji na szczeblu gminy, a inne na szczeblu wojewódzkim i wyższym. Posiadając niezbędne dane należy wypracować odpowiednie metody zabezpieczeń oraz określić dane, niezbędne do ich realizacji.

W rozproszonym systemie teleinformatycznym należy rozważyć możliwość zastosowania hierarchicznego systemu dystrybucji dokumentów kryptograficznych, poprzez szczeble dystrybucji odpowiadające strukturze administracji publicznej, której system teleinformatyczny ma być chroniony. Struktura taka ułatwia właściwe zapewnienie potrzeb komunikacyjnych poszczególnych jednostek systemu.

Na podstawie analizy podobnych systemów oraz doświadczeń, można sformułować następujące wymagania informacyjne systemu SZDK:

- dane o użytkownikach;

- dane o jednostkach administracji publicznej;
- dane o miejscach eksploatacji urządzeń ochrony informacji;
- dane o klauzuli przetwarzanych (przesyłanych) informacjach;
- dane o wymaganiach zabezpieczeń informacji przesyłanych w systemie;
- dane o potrzebach komunikacyjnych użytkowników systemu;
- dane o systemach ochrony informacji, zastosowanych w systemie TI;
- dane o DK niezbędnych dla poprawnej pracy systemu ochrony informacji;
- dane o zasadach komunikacji między poszczególnymi szczeblami i osobami (gremiami) decyzyjnymi w systemie;
- dane o czasie zmiany dokumentów (DK);
- dane o rozbudowie i zmianie konfiguracji systemu.

Doświadczenie z dotychczas prowadzonych prac pokazuje, iż w trakcie opracowywania projektu systemu oraz jego wdrażania pojawią się kolejne wymagania jak i potrzeby. System SZDK powinien być na tyle elastyczny, by umożliwiać ich wprowadzenie do projektu, a po wdrożeniu umożliwiać rozbudowę bez konieczności jego wyłączenia z pracy.

Wydaje się, iż rozproszenie elementów systemu SZDK w strukturę hierarchiczną umożliwi podział zadań między mniejsze jednostki (obszarowo i ilościowo), które będą mogły szybciej reagować na potrzeby użytkowników. Oczywiście jednostka nadrzędna powinna spełniać zadania stacji podrzędnych, jak również zadania kontrolne (dla efektów pracy stacji podrzędnych).

Wytwarzanie danych powinno jednak być realizowane w miejscu centralnym systemu, odpowiedzialnym za cały system. Oczywiście jest też, iż ten element powinien być najlepiej chroniony i zabezpieczony.

Sam proces zbierania informacji powinien być usystematyzowany, i maksymalnie uproszczony oraz zabezpieczony, ponieważ wiarygodność tych informacji będzie mieć wpływ na poprawne i bezpieczne działanie całego systemu TI.

6. METODY POZYSKIWANIA INFORMACJI O POTRZEBACH UŻYTKOWNIKÓW SYSTEMU

System zarządzania wymaga ciągłego dostarczania danych o potrzebach komunikacyjnych użytkowników. Potrzeby te, to:

1. połączenia chronione między użytkownikami indywidualnymi realizowane z wykorzystaniem indywidualnych środków łączności;

2. połączenia chronione między węzłami (centralami) realizowane przez środki do ochrony łączy grupowych;
3. połączenia chronione między sieciami lokalnymi, realizowane przez środki sieciowe (szyfratory IP);
4. potrzeby użytkowników w zakresie dostępu do materiałów klasyfikowanych realizowane przez system na podstawie uprawnień zapisanych w indywidualnych identyfikatorach oraz serwerach;
5. potrzeby związane z rekonfiguracją eksploatowanego systemu;
6. potrzeby związane z rozbudową eksploatowanego systemu.

Analizując wymagania przyszłych użytkowników i zadania systemu zapewne będzie można określić jeszcze więcej potrzeb użytkowników. W trakcie prac nad projektem i budową systemu niezbędne będzie opracowanie metod pozyskiwania informacji o potrzebach użytkowników, które pozwolą na szybkie zebranie i zrealizowanie. System zarządzania SZDK powinien posiadać narzędzia, pozwalające na nie tylko na zebranie potrzeb, ale również na ich wstępną, automatyczną weryfikację przez wytworzeniem odpowiednich danych kryptograficznych. Jednak, by zbudować taki mechanizm, niezbędne będzie wypracowanie zasad identyfikacji potrzeb, metody ich rejestracji oraz kryteria weryfikacji.

Opracowując założenia na system TI oraz system ochrony informacji niezbędnym jest przeprowadzenie dogłębnej analizy procesów przetwarzania informacji, ustalenie zasad ich zbierania i udostępniania, jak również metod ich zabezpieczenia. Należy rozpatrywać nie tylko procesy zabezpieczenia przesyłanych informacji (komunikacja głosowa, faxowa, mailowa), ale również proces przechowywania, przetwarzania i udostępniania informacji zgromadzonych i zapisanych w zasobach systemu. Drugim obszarem będą zasady udostępniania zgromadzonych zasobów informacyjnych systemu.

Wydaje się, że zbieranie danych i informacji o potrzebach powinno przebiegać w dwóch etapach. Pierwszym etapem powinno być zebranie informacji o wymaganiach użytkowników i zasadach przetwarzania informacji na etapie projektowania systemu. Etap ten powinien być przeprowadzony jednocześnie z etapem analizowania potrzeb w zakresie potrzeb telekomunikacyjnych użytkowników. Budowa systemu zabezpieczeń nie powinna być odkładana na tzw. „potem”, ponieważ „dokładanie” tak ważnego systemu (ochrona) do już istniejącego (telekomunikacyjnego) może być skazane na porażkę.

Efektom prac w tym etapie powinny być określone metody i zasady dostępu do informacji, potrzeby informacyjne użytkowników, metody i zakres dostępu do informacji

poszczególnych grup użytkowników. Celowym również jest zidentyfikowanie potencjalnych, niestandardowych sytuacji w działaniu i wykorzystaniu systemu. Należy dołożyć starań, w ścisłym porozumieniu z użytkownikami, by opracować metody postępowania w takich sytuacjach. Można tu wymienić takie jak rozbudowa systemu o nowe lokalizacje, nowych użytkowników, zmiany dotychczas realizowanych połączeń (indywidualnych, międzycentralowych, rekonfiguracja urządzeń sieciowych), usunięcie użytkowników (indywidualnych, węzłów). Sytuacją niestandardową będzie również wymiana dokumentów kryptograficznych w systemie, w sytuacji skompromitowania dotychczas używanych lub niezwłoczna rekonfiguracja połączeń chronionych.

Metody zbierania informacji o potrzebach użytkowników mogą być różne. W zależności od skali systemu (lokalny, strefowy, globalny – w skali kraju), można zastosować rozmowy z wybranymi (lub wszystkimi) użytkownikami, analizę dokumentacji, analizę zasad przetwarzania informacji, analizę przepływu informacji, metody wywiadów wg ustalonego scenariusza, itp.. W przypadku systemów globalnych (w skali kraju) nie będzie możliwe przeprowadzenie rozmów ze wszystkimi użytkownikami. Na podstawie analizy wstępnej można wybrać reprezentantów, z którymi przeprowadzi się szczegółowe rozmowy. Wsparciem będzie analiza dokumentacji (w przypadku administracji publicznej aktów prawnych) oraz zasad komunikacji, między poszczególnymi szczeblami administracji. Struktura administracji jest hierarchiczna, co ułatwia opis. Jednocześnie jest bardzo rozległa, zarówno obszarowo jak i zadaniowo, co z kolei komplikuje analizę. Dlatego też wybór odpowiednich metod będzie miał wpływ na powodzenie całego zagadnienia.

W trakcie prac nad opracowywaniem szczegółowych założeń na system teleinformatyczny administracji publicznej należy przyjąć jedną z dostępnych metodyk, wykorzystywanych w inżynierii programowania metod. Wybór właściwej metody specyfikacji wymagań na system, powinien być poprzedzony ich przeglądem, pod kątem możliwości wykorzystania w opisie tak szerokiego systemu. Wybrana metoda powinna umożliwiać całościowe opisanie systemu, oraz wspomagać działania zespołu analityków, projektantów, programistów i testerów na wszystkich etapach prac na systemem. Pożądane jest również, by narzędzie umożliwiało współpracę różnych grup z różnych dziedzin, w tym przypadku z zakresu teleinformatyki i zabezpieczeń.

Drugim obszarem, którym należy się zająć, to zbieranie i przetwarzanie informacji o potrzebach użytkowników w trakcie eksploatacji systemu. Narzędzie takie, a właściwie funkcjonalność systemu, powinna być zlokalizowana w obszarze zarządzania systemem teleinformatycznym. Wszelkie zmiany konfiguracji systemu powinny być realizowane przez

takie centrum. W związku z tym właściwi operatorzy, odpowiedzialni za utrzymanie działania systemu, powinni posiadać aktualne informacje o stanie systemu i jego elementów składowych oraz o potrzebach użytkowników. Zarówno tych związanych z bieżącą eksploatacją, jak i związanych ze scenariuszami przewidzianymi dla sytuacji niestandardowych. Opracowane zmiany systemu, konfiguracyjne jak i związane z dostępem użytkowników do zasobów, powinny być przekazywane do zarządzania bezpieczeństwem. System ochrony informacji jest bowiem dostawcą usług zabezpieczających dla systemu teleinformatycznego. W tym zakresie jest system podrzędnym, a w związku z tym działającym na podstawie potrzeb zgłaszanych przez system zarządzania system TI. Dlatego też adekwatność potrzeb użytkowników jest niezmiernie ważna w procesie ich zabezpieczenia. Adekwatność potrzeb może być rozumiana jako potrzeby użytkowników wynikające z ich funkcji, umiejscowienia w strukturze systemu oraz zakresu dostępu do informacji zgromadzonych w systemie. W naszej pracy często spotykamy się z nadmiarowymi żądaniami użytkowników, próbujących zapewnić sobie nadmiarowe możliwości komunikacyjne, które mogą być „kiedyś” przydatne. W tak sformalizowanej strukturze nie powinno być miejsca na „życzeniowość”, ponieważ nie jest to wskazane, a czasami może być niebezpieczne.

Jednocześnie należy jednak zapewnić metody szybkiej i skutecznej realizacji potrzeb, które będą się pojawiać w trakcie eksploatacji systemu. Oznacza to konieczność zapewnienia funkcjonalności systemu umożliwiających przygotowywanie takich scenariuszy, potencjalnych potrzeb użytkowników oraz sytuacji niestandardowych. Przygotowanie narzędzie do realizacji takich potrzeb może być zadaniem trudnym do realizacji, w stopniu całkowicie pokrywającym potrzeby użytkowników.

7. PODSUMOWANIE

Opracowanie i wdrożenie nowoczesnego i bezpiecznego systemu teleinformatycznego dla potrzeb administracji publicznej jest zagadnieniem bardzo obszernym i trudnym. Nie jest również zadaniem tanim. Dokładając do tego system ochrony informacji należy uwzględnić go już na etapie analizowania potrzeb i projektu. Pozwoli to na zapobieżenie sytuacji, gdy system TI działa poprawnie przed dołączeniem elementów zabezpieczających, a później już nie. Urządzenia i mechanizmy kryptograficzne mają duże wymagania, co do jakości systemu transmisji danych i zasad przetwarzania informacji.

Podjmując zagadnienie ochrony informacji w systemie TI należy również mieć na uwadze konieczność uzyskania stosownych certyfikatów bezpieczeństwa urządzeń i narzędzi

kryptograficznych przeznaczonych do ochrony informacji niejawnych. Wymóg ten nakłada na opracowujących system ochrony informacji wymagania formalne merytoryczne co do stosowanych metod i rozwiązań, oraz do wytwarzanej dokumentacji. Przed wdrożeniem systemu niezbędne będzie uzyskanie akredytacji dla całego systemu ochrony informacji. Jedną opracowanie bezpiecznego systemu bez zastosowania metod kryptograficznych nie jest możliwe, szczególnie w czasach tak szybkiego rozwoju.

Międzyresortowy zespół został rozwiązany w roku 2010. Należy mieć nadzieję, iż wyniki jego pracy zostaną wykorzystane w pracach kolejnych zespołów, których zadaniem będzie opracowanie projektu systemu. Tak jest bowiem potrzeba, od której nie da się uciec, jeżeli myśli się o sprawnym i bezpiecznym zarządzaniu państwem, w czasie pokoju jak i zagrożenia.

Literatura

- [1] Biblioteka Bezpieczeństwa Narodowego, Tom 3, „Bezpieczeństwo w telekomunikacji i teleinformatyce”, wyd. rok 2008.
- [2] <http://www.securityrevue.com/article/2010/09/niemkore-aspemy-istoty-i-ochrony-infrastruktury-krytycznej/> .
- [3] Ustawa o zarządzaniu kryzysowym z dn. 14.04.2007 r. Dziennik Ustaw z 2007, Nr 89, poz. 590.
- [4] Ustawa o zmianie ustawy o zarządzaniu kryzysowym, Dz. U. z dnia 19 sierpnia 2009.
- [5] Dane z Rządowego Centrum Bezpieczeństwa.
- [6] „Zagrożenia krytycznej infrastruktury teleinformatycznej w dobie rozwoju społeczeństwa informacyjnego”, kmdr por. dr inż. Grzegorz Krasnodębski, Akademia Marynarki Wojennej.
- [7] Biuro Bezpieczeństwa Narodowego, projekt ustawy o bezpieczeństwie, Warszawa 2007.
- [8] „Funkcjonowanie systemu telekomunikacyjnego administracji publicznej”, dr Jacek Matyszczak, Biblioteka Bezpieczeństwa Narodowego, Tom 3, „Bezpieczeństwo w telekomunikacji i teleinformatyce”, wyd. rok 2008

Streszczenie

Budowa systemu telekomunikacyjnego dla administracji publicznej jest wyzwaniem, które należy podjąć dla sprawnego funkcjonowania organów administracyjnych (rządowej i samorządowych), jak i dla służb odpowiadających za bezpieczeństwo obywateli w czasie pokoju i zagrożenia. Zbudowanie nowoczesnego systemu nie jest zadaniem łatwym i tanim. Dodatkowo, w dobie lawinowo zwiększającego się niebezpieczeństwa ataków cybernetycznych, system taki musi posiadać odpowiednie zabezpieczenia, zarówno organizacyjne jak i techniczne. Informacje przetwarzane w takim systemie będą posiadać różną wagę oraz będą przeznaczone dla różnych osób (zajmujących stanowiska na poszczególnych szczeblach struktury). Biorąc pod uwagę skalę systemu, jego zadania i różnorodność przyszłych użytkowników należy zadbać, by informacje przetwarzane w tym systemie były wiarygodne, posiadały właściwy stopień poufności i integralności. Tylko informacja pewna jest wartościowa. Dlatego też system telekomunikacyjny powinien zabezpieczać przetwarzanie informacji z wykorzystaniem metod kryptograficznych, jako tych, które spełniają współczesne wymagania. System ochrony, będący integralną częścią systemu telekomunikacyjnego, powinien być kompleksowym rozwiązaniem, zabezpieczającym wszystkie etapy cyklu życia informacji. Jednym z elementów składowych systemu ochrony informacji jest system zarządzania kluczami, którego zadaniem jest dostarczenie danych niezbędnych do prawidłowego funkcjonowania systemu zabezpieczeń. Artykuł podejmuje temat analizy potrzeb systemu telekomunikacyjnego w zakresie wymagań na ochronę przetwarzanych informacji, jak również wynikających z tego potrzeb systemu ochrony.

Abstract

The telecommunication system for public administration will ensure communication for government entities. System for public administration will be used in different times, by different users. There will cryptographic protection in this system. Every protection system needs a key management system (KMS), which will be produce a cryptographic data for crypto units. His primary task is to provide a specific data for security system, according with plan of connection. This article describes basic requirements for KMS.