Krzysztof Szczypiorski
Instytut Telekomunikacji
Politechnika Warszawska, Warszawa
E-mail: K.Szczypiorski@tele.pw.edu.pl

Ochrona informacji w zarządzaniu sieciami telekomunikacyjnymi

W artykule przedstawiono spojrzenie na ochronę informacji pod kątem zarządzania sieciami telekomunikacyjnymi. Dla podstawowych usług i mechanizmów bezpieczeństwa zaproponowano model zarządzania (aspekt zarządzania bezpieczeństwem). W dalszej części poruszono kwestie tworzenia bezpiecznych sieci zarządzania telekomunikacją - TMN (aspekt bezpieczeństwa zarządzania).

Krzysztof Szczypiorski
Institute of Telecommunications
Warsaw University of Technology, Warsaw, Poland
E-mail: K.Szczypiorski@tele.pw.edu.pl

Information Security in Management of Telecommunications Networks

The article presents information security from the telecommunications network management point of view. A management model is proposed for the basic security services and mechanisms (management of security). Issues concerning the creation of secure Telecommunications Management Network (security of management) are described.

Krzysztof Szczypiorski
Instytut Telekomunikacji
Politechnika Warszawska, Warszawa
E-mail: K.Szczypiorski@tele.pw.edu.pl

Ochrona informacji w zarządzaniu sieciami telekomunikacyjnymi

W artykule przedstawiono spojrzenie na ochronę informacji pod kątem zarządzania sieciami telekomunikacyjnymi. Dla podstawowych usług i mechanizmów bezpieczeństwa zaproponowano model zarządzania (aspekt zarządzania bezpieczeństwem). W dalszej części poruszono kwestie tworzenia bezpiecznych sieci zarządzania telekomunikacją - TMN (aspekt bezpieczeństwa zarządzania).

1. Wprowadzenie

Zastosowanie w sieciach telekomunikacyjnych nowoczesnych metod ochrony informacji staje się codziennością. Przy upowszechnieniu zabezpieczeń pojawiają się nieuniknione pytania: Jak tym wszystkim zarządzać? Czy działanie mechanizmów bezpieczeństwa można zautomatyzować?

Aby odpowiedzieć na te kwestie należy zbadać **dwie** relacje występujące pomiędzy zarządzaniem a bezpieczeństwem:

1. **zarządzanie bezpieczeństwem** - wiąże się z **zarządzaniem usługami i mechanizmami bezpieczeństwa**; jest to dostarczanie informacji zarządzania do tych usług i mechanizmów, jak i zbieranie oraz przechowywanie informacji o tych usługach i mechanizmach; przykłady:
   - zarządzanie kluczami (w tym dystrybucja klucza),
   - dostarczanie sprawozdań dotyczących zdarzeń w systemie związanych z bezpieczeństwem (w tym przebiegu niektórych funkcji);
2. **bezpieczeństwo zarządzania** - wiąże się z bezpieczną i rzetelną pracą sieci zarządzania (np. TMN); jest skomplikowanym, żmudnym (nie kończącym się) procesem; przykłady:
   - rzetelność informacji przechowywanych w bazach danych: ich dostępność, poprawność itp.
   - odpowiedzialność od strony bezpieczeństwa za wszystkie poczynania związane z zarządzaniem.

Dwa następne rozdziały prezentują kolejno wymienione powyżej związki. W pierwszym z nich (*2. Zarządzanie bezpieczeństwem: usługi ochrony informacji i zarządzanie nimi*) został zaproponowany model zarządzania usługami ochrony informacji, natomiast w drugim (*3. Bezpieczeństwo zarządzania: tworzenie bezpiecznego TMN*) schemat projektowania bezpiecznego systemu otwartego na przykładzie TMN.

W przypadku sieci telekomunikacyjnych dochodzi trzecia relacja:

- **świadczenie usług ochrony informacji (bezpieczeństwa)** - dostarczanie końcowym użytkownikom (klientom) **usług** bezpieczeństwa opisanych w następnym rozdziale.

2. Zarządzanie bezpieczeństwem: usługi ochrony informacji i zarządzanie nimi

2.1 Podstawowe usługi i mechanizmy ochrony informacji - wprowadzenie

Przyjmując porządek określony w normie [ISO 7498-2] - **ochrona informacji w systemach otwartych dostarcza** następujących **podstawowych, uniwersalnych[1] usług**:

- **kontrolę dostępu (access control)[2]** - ochronę przed nieuprawnionym dostępem do zasobów,
- **integralność danych (data integrity)** – gwarancję spójności danych; ochronę przed modyfikacją, wtrąceniem, wymazaniem danych,
- **uwierzytelnienie (authentication)** - kontrolę tożsamości stron lub danych wymienianych pomiędzy nimi np. podczas sesji komunikacyjnej,
- **niezaprzeczalność (non-repudation)** - metodę rozstrzygnięcia ewentualnego sporu pomiędzy nadawcą a odbiorcą dotyczącego zarówno faktu nadania i odbioru informacji jak i jej treści,
- **poufność danych (confidentiality) -** ochronę danych przed nieuprawnionym uzyskaniem przez strony nieupoważnione.

Kontrola dostępu jest pierwotna względem pozostałych usług, realizuje się ją przed wykorzystaniem zasobów. Poufność może być zapewniona niezależnie od integralności, uwierzytelnienia i niezaprzeczalności. Niezaprzeczalność zawsze wiąże się z uwierzytelnieniem, natomiast uwierzytelnienie z integralnością.

Dla systemów informacyjnych oprócz wspomnianych podstawowych pięciu usług wprowadza się ([ISO 10181-1]) usługę[3] związaną w dużym stopniu z przetwarzaniem danych: **audyt i alarmy (security audit and alarms)**. Jest to zbiór metod umożliwiających wgląd do systemu, oceny poprawności jego pracy z punktu widzenia bezpieczeństwa.

W modelu odniesienia OSI - warstwa sesji - służąca do nawiązania połączenia jest „uwolniona" od usług ochrony informacji. Poufność może być realizowana we wszystkich pozostałych warstwach. Kontrola dostępu, integralność danych, uwierzytelnienie - w warstwach: sieciowej, transportowej oraz prezentacji i aplikacji. Niezaprzeczalność - w warstwach najwyższych.

Usługi audytu i alarmów są stosowane do odnotowywania zdarzeń związanych z bezpieczeństwem występujących w środowisku OSI traktowanym jako całość.

Podstawowe usługi są budowane na bazie mechanizmów**. Wyróżnia się następujące mechanizmy [ISO 7498-2]:**

- **szyfrowanie,** które może zapewnić poufność informacji lub strumienia danych; wyróżnia się dwie klasy algorytmów szyfrujących: symetryczne (tj. z kluczem tajnym) i asymetryczne (tj. z kluczem publicznym),
- **podpis cyfrowy,** dla którego określa się dwie procedury: podpisywanie oraz weryfikację; w pierwszej stosuje się informację, która jest unikalną i poufną (prywatną) własnością podpisującego, w drugiej - informację publicznie dostępną,
- **mechanizmy kontroli dostępu**, używane w celu określenia i przestrzegania praw dostępu do zasobów,
- **mechanizmy integralności danych,** używane do zachowania integralności danych; najczęściej korzysta się z kryptograficznych sum kontrolnych (funkcji skrótu),

---

[1] tj. związanych zarówno z komunikacją jak i przetwarzaniem danych

[2] lepszym aczkolwiek nie spopularyzowanym tłumaczeniem mogłoby być: sterowanie dostępem

[3] a właściwie dwie usługi - są one jednak rozważane jako całość

- **wymiana uwierzytelniająca**, używana do uwierzytelnienia stron; opiera się na trzech parametrach zmiennych w czasie: na technice wyzwania, znacznikach czasu, liczbach kolejnych,
- **wypełnianie ruchu**, które zapewnia ochronę przed analizami ruchowymi - np. ukrywa informację o aktywności źródła,
- **sterowanie doborem trasy**, które umożliwia dobór trasy w taki sposób by transmitowane dane mogły podążać jedynie przez fizycznie bezpieczne łącza lub podsieci,
- **mechanizmy notaryzacji,** które służą do zabezpieczenia komunikacji przed zaprzeczeniem.

2.2 Polityka bezpieczeństwa

Nadanie sensu usługom i mechanizmom stosowanym w systemie informacyjnym wymaga precyzyjnego zdefiniowania procedur zarządzania w postaci polityki bezpieczeństwa.

Polityka bezpieczeństwa jest zbiorem zasad, które określają co najmniej jeden zestaw kompetencji dla jednego lub wielu elementów[4]. **Kompetencje** (activites) wyrażają zakres działania danego elementu, jego funkcjonowanie, sposób komunikacji z innymi obiektami[5]. Polityka definiuje dla danej **domeny** pojęcie bezpieczeństwa, precyzując sposób realizacji każdej usługi ochrony informacji. Dana domena jest **zarządzana** przez **urząd bezpieczeństwa**, odpowiedzialny za realizację polityki, urząd, który w ramach swojej działalności może swoją władzę „przekazywać" (delegować) innym podmiotom np. zarządcom poszczególnych usług ochrony informacji.

2.3 Zarządzanie bezpieczeństwem

Zarządzanie bezpieczeństwem wiąże się ze sterowaniem od strony zabezpieczeń komunikacją i przetwarzaniem danych m.in. poprzez wymianę informacji niezbędnych do przeprowadzenia tego procesu. Zarządzanie bezpieczeństwem jest działalnością wykraczającą poza podstawowe operacje telekomunikacyjno-obliczeniowe występujące w systemie informacyjnym.

Ze względu na charakter zarządzanych obiektów wyróżniamy trzy obszary zarządzania:
- **zarządzanie usługami**, czyli zarządzanie kontrolą dostępu, poufnością, integralnością, uwierzytelnieniem, niezaprzeczalnością, audytem i alarmami,
- **zarządzanie kluczami**,
- **zarządzanie polityką bezpieczeństwa**.

Zarządzanie kluczami jest niezbędne do poprawnej realizacji większości usług ochrony informacji (klucz jest parametrem szyfru, szyfr jest składnikiem większości usług ochrony informacji). Natomiast zarządzanie polityką bezpieczeństwa jest konieczne do właściwej pracy urzędów bezpieczeństwa, czy też delegowanych przez nie zarządców poszczególnych usług ochrony informacji.

2.3.1 Informacje bezpieczeństwa

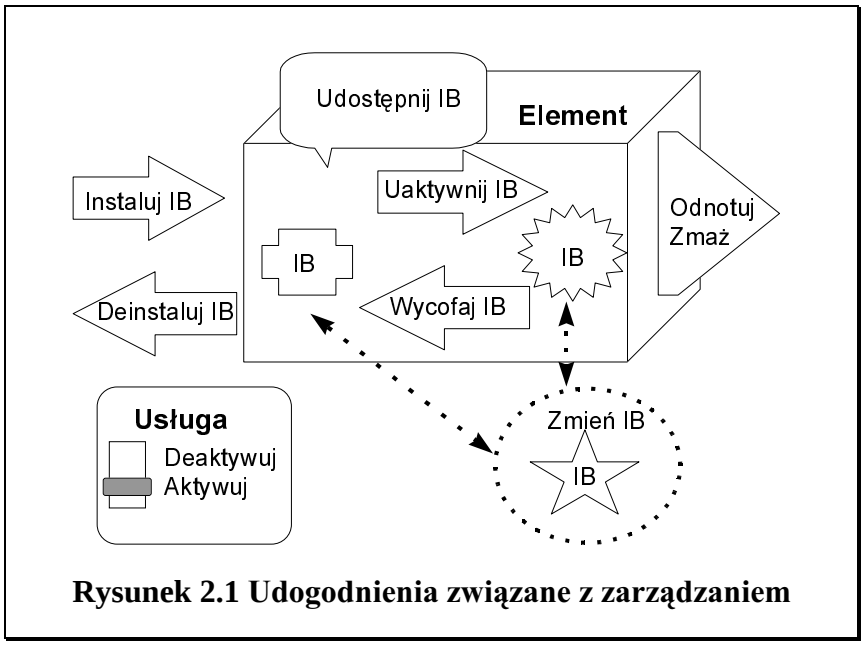
Zarządzanie bezpieczeństwem wiąże się z przetwarzaniem, badaniem stanu, porządkowaniem tzw. **informacji bezpieczeństwa IB** (SI - Security Information), które są niezbędne do realizacji usług bezpieczeństwa ([ISO 10181-1]). Przykładami tego typu informacji są:
- informacje konieczne do zrealizowania specyficznej usługi ochrony informacji np. informacja uwierzytelniająca zawierająca dane o tęczówce konkretnego człowieka,
- informacje wspólne dla kilku usług bezpieczeństwa:

[4] elementem jest każdy obiekt zarówno podmiot, jak i funkcja
[5] przykładami kompetencji są operacje związane ze specyficzną funkcją zarządzania albo usługą ochrony informacji

- **etykiety bezpieczeństwa (security labels)** - używane do oznaczenia atrybutów bezpieczeństwa dla danego podmiotu,
- **kryptograficzne sumy kontrolne (cryptographic checkvalues)** - czyli podpisy cyfrowe, skróty i koperty,
- **certyfikaty (security certificates)** - cyfrowe świadectwa wydane przez określony urząd bezpieczeństwa,
- **tokeny (tokens)** - zbiory danych zabezpieczone, co najmniej jedną usługą ochrony informacji,

- zasady polityki bezpieczeństwa.

2.3.2 Podstawowe udogodnienia



Rysunek 2.1 Udogodnienia związane z zarządzaniem

Z zarządzaniem wiążą się tzw. **udogodnienia (facilities)**[6] czyli akcje związane z informacjami bezpieczeństwa, bądź z usługami ([ISO 10181-1]). Następujące udogodnienia (Rysunek 2.1 Udogodnienia związane z zarządzaniem) są przeprowadzone przez urząd bezpieczeństwa i współpracujący z nim element:

- **Instaluj IB (Install SI)** - ustanowienie inicjującego zbioru IB przyporządkowanemu pewnemu elementowi,
- **Deinstaluj IB (Deinstall SI)** - usunięcie IB, które deklaruje przynależność elementu do domeny bezpieczeństwa,
- **Zmień IB (Change SI)** - modyfikacja IB skojarzonej z elementem,
- **Uaktywnij IB (Validate SI)** - aktywne powiązanie IB z elementem, przeprowadzana przez urząd bezpieczeństwa,
- **Wycofaj IB (Invalidate SI)** - deaktywacja użycia (ale nie usunięcie z systemu) IB skojarzonego z elementem, przeprowadzane przez urząd bezpieczeństwa,
- **Deaktywuj/Aktywuj usługę - (Disable/Re-enable security service)** - deaktywacja usługi lub jej poziomu,
- **Odnotuj (Enrol)** - rejestracja przez urząd bezpieczeństwa informacji skojarzonej z danym podmiotem (np. rejestracja żądania),

[6] tzw. management related facilities

- **Zmaż (Un-enrol)** - usunięcie informacji; oczywiście polityka bezpieczeństwa może nie dopuszczać by niektóre informacje były usuwane,
- **Udostępnij IB (Distribute SI)** - udostępnienie danej informacji innym podmiotom,
- **Stwórz listę IB (List SI)** - tworzenie listy IB skojarzonych z danych elementem.

Oprócz wymienionych uniwersalnych udogodnień związanych z zarządzaniem wyróżnia się **udogodnienia związane z operacjami**[7]:

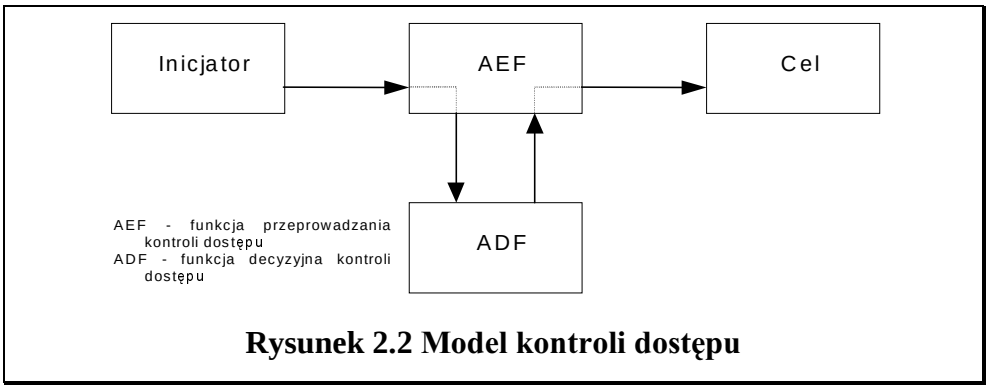
- **Rozpoznaj zaufany urząd bezpieczeństwa (Identify trusted security authorites)** - dzięki temu udogodnieniu dany element jest w stanie rozpoznać właściwy urząd bezpieczeństwa o odpowiednich kompetencjach (tj. wynikających z polityki bezpieczeństwa),
- **Rozpoznaj bezpieczne zasady współpracy (Identify secure interaction rules)** - dzięki temu udogodnieniu dwa elementy negocjują lub wykorzystują ustalone zasady współpracy,
- **Nabyj IB (Acquire SI)** - nabycie IB - pierwotne względem aktywności podmiotu,
- **Generuj IB (Generate SI)** - generacja IB dla konkretnej usługi bezpieczeństwa,
- **Weryfikuj IB (Verify SI)** - weryfikacja ważności IB.

Udogodnienia związane z zarządzaniem i operacjami, a także informacje bezpieczeństwa określają zasady sterowania daną usługą ochrony informacji - są funkcjonalnym opisem modelu. Dopiero ich całościowe przedstawienie daje obraz **zarządzania** daną usługą. Udogodnienia związane z zarządzaniem odnoszą się do działalności urzędu bezpieczeństwa (lub jego delegata), który operując na informacjach bezpieczeństwa i łącząc je w różnych relacjach z podmiotem, pośrednio czuwa nad prawidłowym przebiegiem operacji.

2.4 Przykład: Zarządzanie kontrolą dostępu[8]

Kontrola dostępu (czasem określana mianem autoryzacji) jest usługą dzięki, której tylko uprzywilejowane podmioty mogą otrzymać dostęp do zasobów. Podmiotem może być zarówno człowiek jak i proces, zasobem - proces, system sieciowy.

2.4.1 Model



Rysunek 2.2 Model kontroli dostępu

W modelu ([ISO 10181-3], [RACE CFS H211], [RACE CFS H407]) kontroli dostępu wykorzystuje się następujące określenia:

- **inicjator (initiator)** - podmiot, który próbuje uzyskać dostęp do innego podmiotu,
- **cel**[9] **(target)** - podmiot, do którego następuje **próba dostępu, czyli akcja,**

[7] tzw. operational related facilities
[8] można to nazwać w skrócie: **zarządzaniem dostępem**
[9] podmiot docelowy

- **informacja kontroli dostępu (ACI - Access Control Information)** - dowolna informacja używana przy procesie kontroli dostępu,
- **funkcja decyzyjna kontroli dostępu (ADF - Access control Decision Function)** - specjalistyczna funkcja kontrolująca decyzję o dostępie poprzez zastosowanie reguł polityki bezpieczeństwa na pożądanej akcji, ACI i kontekstu, w jakim żądanie zostało użyte,
- **informacja decyzyjna kontroli dostępu (ADI - Access control Decision Information)** - zbiór ACI niezbędnych ADF do podjęcia decyzji,
- **funkcja przeprowadzająca kontrolę dostępu (AEF - Access control Enforcement Function)** - specjalistyczna funkcja będąca ścieżką dostępu pomiędzy inicjatorem a celem, przeprowadzająca kontrolę dostępu.

AEF jest odpowiedzialna za poprawność akcji zdeterminowanych przez ADF wykonywanych pomiędzy inicjatorem a celem. Kiedy podmiot inicjujący żąda wykonania akcji na podmiocie docelowym, AEF komunikując się z ADF otrzymuje informację o podjętej decyzji. Decyzja jest przeprowadzana na podstawie ADI skojarzonych z inicjatorem, celem i akcją.

2.4.2 Zarządzanie

2.4.2.1 Udogodnienia

Tabela 2-1 Kontrola dostępu - udogodnienia

Udogodnienia związane z zarządzaniem	**Podmiot**	Urząd bezpieczeństwa (SDA - Security Domain Authority)		
		• Instaluj ACI • Zmień ACI • Odwołaj ACI • Odwołaj ADI • Stwórz listę ACI • Deaktywuj komponent[10] • Aktywuj komponent		
Udogodnienia związane z operacjami	**Podmiot**	**Inicjator**	**Cel**	-
	Funkcja	-	-	**ADF**
		• Nabyj ACI inicjatora • Generuj ACI związane z żądaniem dostępu • Pobierz ACI	• Nabyj ACI	• Nabyj ACI inicjatora albo celu • Weryfikuj ACI i stwórz z niego ADI • Pobierz ACI • Zdecyduj o dostępie

2.4.2.2 Informacje

Tabela 2-2 Kontrola dostępu - informacje

Elementy danych zarządzane przez SDA	• identyfikatory (np. SDA, inicjatora, celu)	• kryteria wyboru ACI	• okres ważności	
Informacje używane w operacjach	• ACI/ADI • listy kontroli dostępu • certyfikaty kontroli dostępu	• zdolności • tokeny kontroli dostępu	• etykiety	
Informacje sterujące	• okres	• status systemu	• poziom uwierzytelnienia	• ścieżka komunikacyjna

3. Bezpieczeństwo zarządzania: tworzenie bezpiecznego TMN

3.1 Ochrona informacji w TMN

Wszelkie metody zabezpieczeń stosowane w sieci zarządzania telekomunikacją TMN mają swój rodowód w rekomendacjach ITU-T i standardach ISO/IEC. Stąd też nakreślone w poprzednim rozdziale szkielety zabezpieczeń, a także udogodnienia związane z zarządzaniem i operacjami są bezpośrednio przenoszone do TMN. Przemyślane - czyli zgodne z polityką bezpieczeństwa zarządzanie bezpieczeństwem jest podstawą bezpiecznego zarządzania i wykracza poza typowo techniczne ramy - staje się obszarem organizacji przedsiębiorstw. Zarządzania bezpieczeństwem w

[10] komponentem jest ADF albo AEF

żaden sposób nie można zautomatyzować, co wynika z charakteru spotykanych w rzeczywistości zagrożeń.

Niniejszy rozdział stanowi wprowadzenie do tworzenia bezpiecznego TMN na etapie koncepcyjno-projektowym, a także sygnalizuje niektóre aspekty związane z eksploatacją bezpiecznego TMN.

3.2 Projektowanie bezpiecznego TMN - wprowadzenie

Przy tworzeniu bezpiecznego TMN można wyróżnić trzy fazy [RACE CFS H210]:

- **fazę początkową**,
- **fazę projektowania, przeglądu i zatwierdzenia** (design, review and accreditaion phase),
- **fazę operacyjną** (operational phase).

3.2.1 Faza początkowa

W fazie początkowej wyłania się interdyscyplinarną grupę ekspertów sterującą całym procesem analizy, wprowadzania, realizacji i obsługi zabezpieczeń w TMN. Grupa powinna stanowić rzeczywisty przekrój wszystkich stron powiązanych z zarządzaniem: użytkowników, przedstawicieli poszczególnych działów operatora, a także prawników, ekonomistów, specjalistów od bezpieczeństwa, inżynierów i techników implementujących system.

3.2.2 Faza projektowania, przeglądu i zatwierdzenia

Podczas fazy projektowania, przeglądu i akredytacji (rysunek 3.1): ustala się **strategię zabezpieczeń**, określa się **chronione zasoby**, przeprowadza się **analizę ryzyka**, na podstawie której określa się **wymagania bezpieczeństwa**. Następnie proponuje się **rozwiązania** spełniające wymagania, przeprowadza się **ocenę „koszty / zyski”** i tworzy się ostateczną **politykę bezpieczeństwa**. Wynikiem całej fazy jest tzw. **projekt zabezpieczeń**.

Strategia zabezpieczeń

Strategia zabezpieczeń określa zasady zarządzania bezpieczeństwem na poziomie organizacyjnym. Dotyczy to w szczególności zabezpieczeń zasobów obliczeniowych i sieciowych. Istotnym czynnikiem kształtującym strategię zabezpieczeń są przepisy prawne. Ma to szczególne znaczenie przy rozważaniu zabezpieczeń styku fizycznego X - łączącego zarówno operatorów lokalnych (krajowych) jak i międzynarodowych.

Określenie strategii wiąże się ze: stworzeniem oficjalnego słownika wyrazów powiązanych z bezpieczeństwem, nakreśleniem celu zabezpieczeń, zdefiniowaniem zakresu zabezpieczeń, zdefiniowaniem relacji i odpowiedzialności pomiędzy wszystkimi uczestniczącymi stronami.

Określenie chronionych zasobów

Określenie zasobów, które podlegają ochronie i określenie poziomu zabezpieczeń jest niezbędnym i nie podlegającym dyskusji krokiem przy projektowaniu bezpiecznego TMN. Określenie powinno zawierać opis rozmieszczenia i typ każdego z zasobów (architekturę), i koszt związany z wyjawieniem danych lub przejęciem sprzętu. Przykładami zasobów są: funkcje TMN, dane przechowywane w TMN (zarządzane obiekty), sprzęt.

Analiza ryzyka

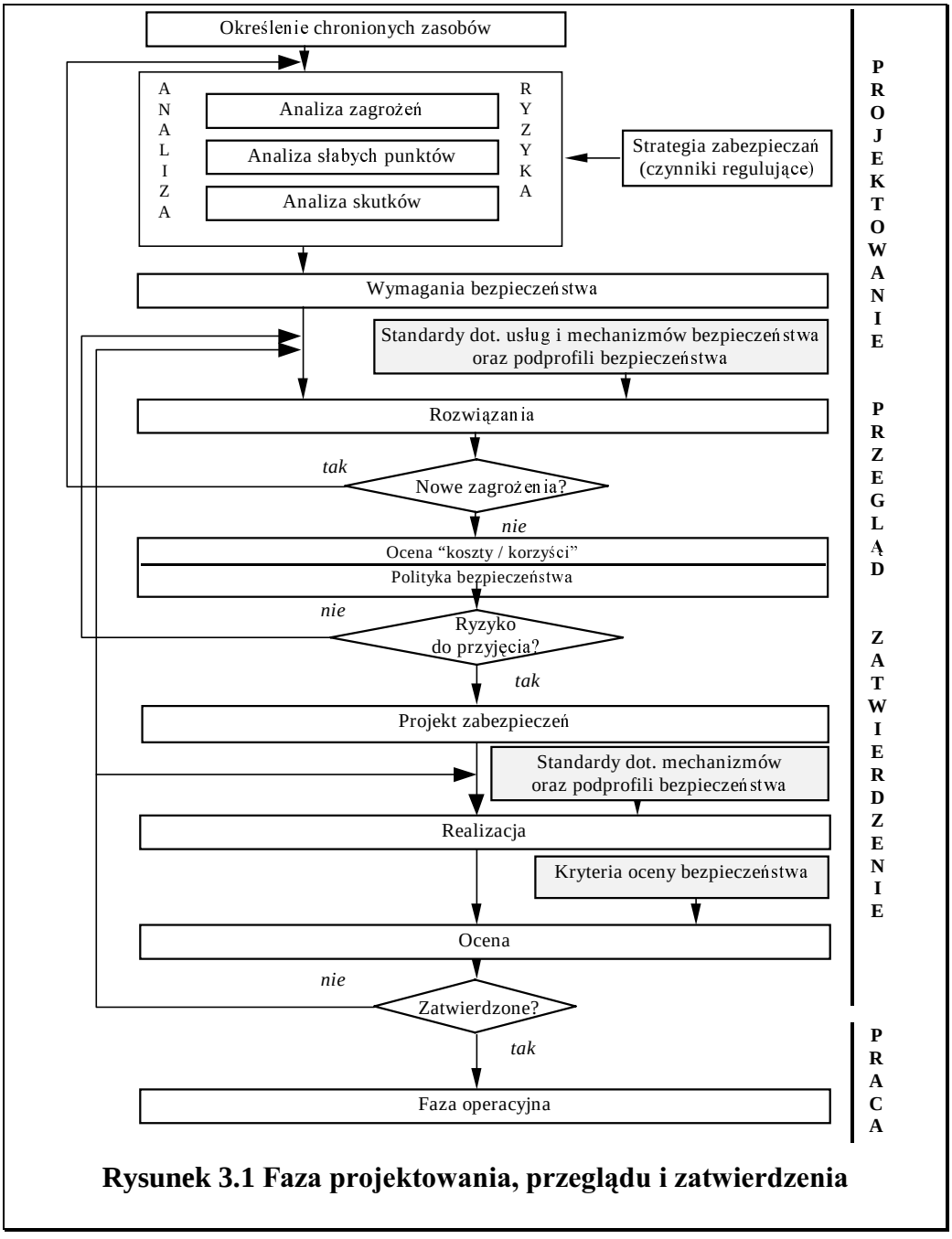
Analiza ryzyka jest szczegółową **analizą zagrożeń** (threats), **słabych punktów** (vulnerabilites) i **skutków** (impacts).

Wymagania bezpieczeństwa

Wymagani bezpieczeństwa są określane po wykonaniu analizy ryzyka i przeanalizowaniu problemów natury prawnej.

Rozwiązania

Proponowane rozwiązania mają na celu spełnienie określonych w poprzednim punkcie wymagań. Usługi i mechanizmy bezpieczeństwa mogą być wybrane z **biblioteki technik ochrony informacji**. Usługi i mechanizmy bezpieczeństwa grupuje się w tzw. pod-profile bezpieczeństwa (oferujące pożądany poziom bezpieczeństwa np. militarny – znaczny, komercyjny – przeciętny).



Rysunek 3.1 Faza projektowania, przeglądu i zatwierdzenia

Ocena „koszty / korzyści”

Zaproponowane rozwiązania są oceniane pod kątem potencjalnych kosztów i korzyści. Koszty określające pożądany poziom bezpieczeństwa nie powinny przekraczać zysków z zastosowanych usług bezpieczeństwa.

Polityka bezpieczeństwa

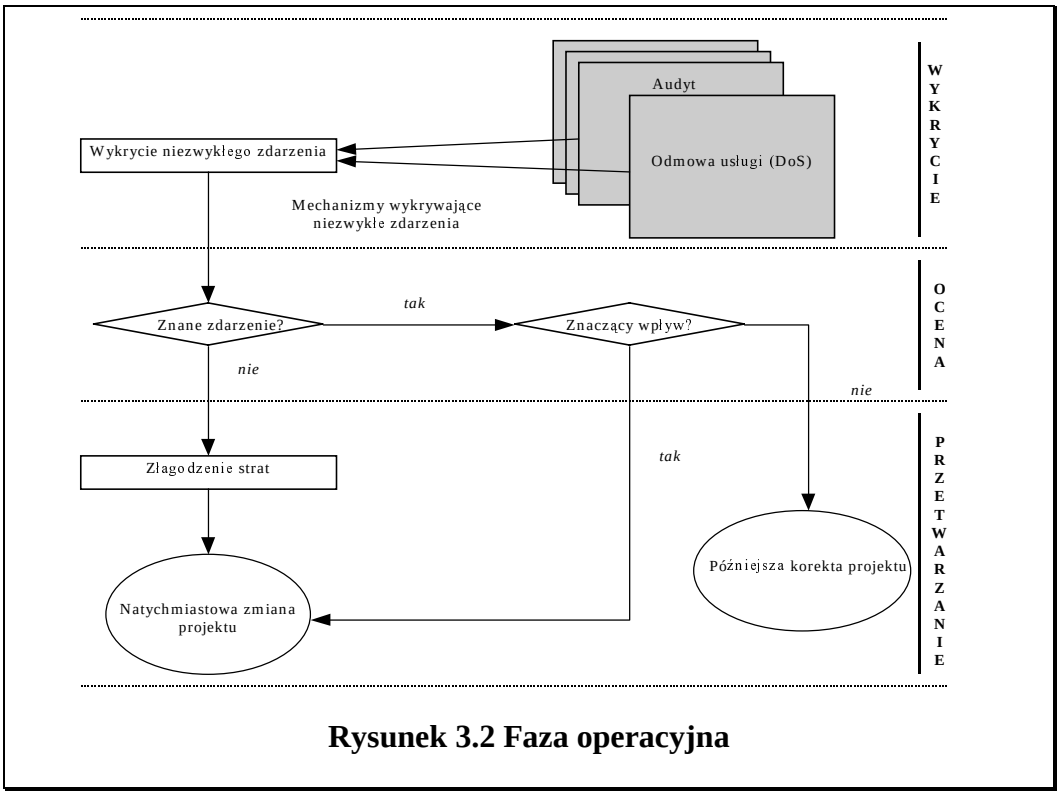
Polityka bezpieczeństwa jest zbiorem praw, zasad i sposobów, które regulują zarządzanie, przetwarzanie, użycie, zabezpieczenie i rozpowszechnianie informacji i zasobów systemu.

Projekt zabezpieczeń

Jest ostatecznym wynikiem działań przeprowadzanych w fazie projektowania, przeglądu i zatwierdzenia. Zawiera definicję zabezpieczanych zasobów, wyniki analizy ryzyka i politykę bezpieczeństwa.

3.2.3 Faza operacyjna

Faza operacyjna (rysunek 3.2) określa szkielet funkcjonowania zabezpieczeń w działającym TMN. W tej fazie można wyróżnić trzy etapy: wykrycie, ocena, przetwarzanie zdarzeń związanych z bezpieczeństwem.



Rysunek 3.2 Faza operacyjna

Wykrycie

Wykrycie zdarzeń związanych z bezpieczeństwem jest uwarunkowane dwoma czynnikami: **polityką bezpieczeństwa,** dzięki której zdarzenia istotne z punktu widzenia bezpieczeństwa są rozpoznawane i obsługiwane oraz **mechanizmami wykrywającymi niezwykłe zdarzenia**.

Ocena

Ocena zdarzenia polega na odpowiedz na pytanie czy dane zdarzenie jest znane. Jeśli tak jest podejmowana decyzja, czy zdarzenie ma znaczący wpływ na stan systemu. Jeśli zdarzenie nie jest

znane powinno nastąpić złagodzenie strat i szybkie skorygowanie projektu zabezpieczeń (są to procesy ostatniego etapu przetwarzania).

Przetwarzanie

Jeśli zdarzenie nie jest znaczące - powinno zostać rozpatrzone w przyszłości przy korekcie projektu zabezpieczeń. Jeśli natomiast zostało uznane za znaczące powinno zostać obsłużone podobnie jak zdarzenie nieznane (złagodzenie strat i szybkie skorygowanie projektu).

4. Podsumowanie

Ewolucja ataków na sieci, starzenie się algorytmów kryptograficznych, wzrost mocy obliczeniowej maszyn oraz przepustowości sieci prowadzi do tego, że zabezpieczenia systemów informacyjnych muszą być ustawicznie nadzorowane i modyfikowane przez wyszkolony personel.

Niektóre usługi, takie jak kontrola dostępu, poufność, integralność i uwierzytelnienie, mogą zostać w dużym stopniu zautomatyzowane, jednak zarządzanie kluczami oraz niezaprzeczalność na pewnym etapie wymagają decyzji człowieka.

Precyzyjne określenie zabezpieczeń dla pozostającej wciąż w sferze koncepcyjnej sieci zarządzania telekomunikacją jest niemożliwe. Próba stworzenia architektury bezpieczeństwa na tym poziomie abstrakcji jest jednak konieczna - zarządzanie obszarami funkcjonalnymi (takimi jak bezpieczeństwo czy rozliczenia) nie może być narażone na przekłamania.

Prawdopodobnym czynnikiem, który zdeterminuje wprowadzenie zabezpieczeń dla TMN będzie rynek telekomunikacyjny. W ciągu paru lat powinny pojawić się bezpieczne platformy zarządzania wyposażone w silne mechanizmy kryptograficzne.

Zaprezentowane w tym artykule zagadnienia mogą być użyteczne przy zabezpieczaniu dowolnych rozproszonych systemów informacyjnych, w szczególności sieci zamkniętych, w których aspekt otwartości i standaryzacji nie jest tak istotny jak w TMN.

Dokładne omówienie tematyki znajduje się w pracy [Szczypiorski, 1997], której niniejszy artykuł jest skrótem.

5. Literatura

[ISO 7498-2] ISO/IEC 7498-2 | ITU-T X.800, ”OSI - Basic Reference Model, Part 2: Security Architecture”, 1991

[ISO 10181-1] ISO/IEC 10181-1 | ITU-T X.810, “OSI - Security Frameworks for Open Systems - Overview”, 1995

[ISO 10181-3] ISO/IEC 10181-3 | ITU-T X.812, “Security Frameworks for Open Systems - Part 3: Access Control”, 1994

[RACE CFS H210] RACE CFS H210, "TMN Security Architecture", Issue E, December 1994

[RACE CFS H211] RACE CFS H211, "Security of Service Management", Issue E, December 1994

[RACE CFS H407] RACE CFS H407, "Management of Security", Issue E, December 1994

[Szczypiorski, 1997] Krzysztof Szczypiorski, „Ochrona informacji w zarządzaniu sieciami telekomunikacyjnymi”, praca dyplomowa, Instytut Telekomunikacji Politechniki Warszawskiej, Warszawa 1997