Polskie Towarzystwo Informatyczne

PTI

Interoperacyjność i bezpieczeństwo systemów informatycznych administracji publicznej

Bolesław Szafrański
Grzegorz Bliźniuk
Jerzy Karbowski
Zbigniew Świerczyński
Romuald Weydmann
Leopold Żurek

Interoperacyjność i bezpieczeństwo systemów informatycznych administracji publicznej

Interoperacyjność
i bezpieczeństwo
systemów
informatycznych
administracji
publicznej

Interoperacyjność i bezpieczeństwo systemów informatycznych administracji publicznej

Redakcja naukowa:

Bolesław Szafrański
Grzegorz Bliźniuk
Jerzy Karbowski
Zbigniew Świerczyński
Romuald Weydmann
Leopold Żurek

PTI

Polskie Towarzystwo Informatyczne – Oddział Górnośląski
Katowice 2006

Recenzenci
prof. dr hab. Aleksander Katkow
prof. dr hab. Maria Nowicka-Skowron
prof. P.Cz. dr hab. Henryk Piech

Projekt okładki
Marek J. Piwko

Redakcja techniczna
Grzegorz Bociek, mgr inż. Jerzy S. Nowak

Copyright © 2006 Polskie Towarzystwo Informatyczne

Utwór w całości ani we fragmentach nie może być powielany ani rozpowszechniany za pomocą urządzeń elektronicznych, mechanicznych, kopiujących, nagrywających i innych, w tym również nie może być umieszczany ani rozpowszechniany w postaci cyfrowej zarówno w Internecie, jak i w sieciach lokalnych bez pisemnej zgody posiadacza praw autorskich.

ISBN 10: 83-922624-0-9
ISBN 13: 978-83-922624-0-4

Wydawca: Polskie Towarzystwo Informatyczne
Oddział Górnośląski
40-074 Katowice, ul. Raciborska 3
tel. (0 32 251 9811), e-mail: Katowice@pti.org.pl; www.pti.katowice.pl

Fotokopie, druk i oprawę wykonano
w Zakładzie Graficznym Politechniki Śląskiej w Gliwicach

Spis treści

1. Wprowadzenie ... 9

2. Analiza zależności między zapewnieniem bezpieczeństwa teleinformatycznego a zapewnieniem interoperacyjności w warunkach przetwarzania informacji o różnych klauzulach tajności ... 12
   2.1. Pojęcie i znaczenie interoperacyjności systemów informatycznych administracji publicznej ... 12
   2.2. Bezpieczeństwo teleinformatyczne a interoperacyjność teleinformatyczna ... 16

3. Interoperacyjność i bezpieczeństwo w ustawie o informatyzacji podmiotów realizujących zadania publiczne ... 19
   3.1. Wprowadzenie ... 19
   3.2. Interoperacyjność ... 20
   3.3. Bezpieczeństwo ... 28
   3.4. Podsumowanie ... 30

4. Przetwarzanie informacji o różnych klauzulach tajności na podstawie analizy aktów prawnych i normatywnych ... 32
   4.1. Wprowadzenie ... 32
   4.2. Wykaz analizowanych aktów prawnych i normatywnych ... 33
   4.3. Aspekty organizacyjno-prawne ... 33
   4.4. Aspekty techniczne ... 35
   4.5. Aspekty ekonomiczne ... 37
   4.6. Uogólnienie wniosków z przeprowadzonej analizy ... 37

5. Model przetwarzania informacji ze źródeł informacji o różnych klauzulach tajności ... 39
   5.1. Model systemu bezpieczeństwa ... 39
   5.2. Założenia modelu ... 40
   5.3. Sformułowanie modelu ... 41
   5.4. Opis i dyskusja modelu ... 43

6. Identyfikacja zagrożeń dla bezpieczeństwa teleinformatycznego i występujących ograniczeń dla możliwości zapewniania interoperacyjności systemów teleinformatycznych ... 54
   6.1. Przesłanki ... 54
   6.2. Zarządzanie bezpieczeństwem a zarządzanie interoperacyjnością ... 55
   6.3. Zagrożenia organizacyjno-prawne ... 57
   6.4. Zagrożenia techniczne ... 59
   6.5. Zagrożenia uboczne ... 60

7. Modele i mechanizmy ochrony przetwarzania informacji o rożnych klauzulach tajności 62
7.1. Uwagi wstępne 62
7.2. Klasyfikacja mechanizmów ochrony danych 63
7.3. Analiza przydatności mechanizmów ochrony danych do ochrony przetwarzania informacji o zróżnicowanych klauzulach tajności 70
7.4. Analiza i klasyfikacja mechanizmów ochrony danych w wybranym oprogramowaniu systemowym 75
7.5. Wnioski 80

8. Model identyfikacji i szacowania kosztów ochrony przetwarzania informacji o różnych klauzulach tajności 82
8.1. Opis struktury kosztów systemów przetwarzających informacje niejawne 82
8.2. Model struktury kosztów systemów przetwarzających informacje niejawne 89

9. Specyfikacja modelowych wymagań technicznych, organizacyjnych i prawnych w dziedzinie bezpieczeństwa teleinformatycznego przetwarzania informacji o różnych klauzulach tajności 93
9.1. Założenia i struktura modelowych wymagań 93
9.2. Interoperacyjność i bezpieczeństwo zasobów informacyjnych kluczowych dla realizacji zadań publicznych 94
9.3. Zawyżanie klauzul tajności 95
9.4. Definicja bezpieczeństwa informacyjnego 96
9.5. Polityka nakazowa i uszczelniająca 97
9.6. Wypadkowe klauzule tajności 97
9.7. Problem interesu publicznego 98
9.8. Audyt bezpieczeństwa 99
9.9. Mechanizmy ochrony 100
9.10. Koszty 100

10. System rejestrowy PESEL a modelowe wymagania 102
10.1. Charakterystyka systemu rejestrowego PESEL w zakresie przetwarzania informacji niejawnych pod kątem specyfikacji modelowych wymagań 102
10.2. Charakterystyka systemu informatycznego używanego do prowadzenia rejestru PESEL 109
10.3. Analiza i ocena spełniania specyfikacji modelowych wymagań prawnych i organizacyjnych 109
10.4. Wnioski z przeprowadzonej analizy 112

11. Wnioski, propozycje, wytyczne 113
11.1. Wnioski, propozycje 113
11.2. Kierunki wykorzystania wyników 116

Bibliografia 117

Załącznik nr 1: „Uogólniony materiał analityczny dotyczący aktów prawnych i normatywnych" 119

Załącznik nr 2: „Uogólniony materiał analityczny dotyczący mechanizmów ochrony danych" 135

Młodzi ludzie znają reguły.
Starzy ludzie znają wyjątki.
Oliver Wendel Holmes

1. Wprowadzenie

We wszystkich organizacjach o takiej wielkości, złożoności i takim znaczeniu społeczno-gospodarczym, jak w przypadku administracji publicznej bezwzględnie krytycznym problemem jest zapewnienie Bezpieczeństwa Informacyjnego. Bezpieczeństwo informacyjne jest cechą systemu informacyjnego danej organizacji dotyczącą przede wszystkim poufności, integralności i dostępności danych (informacji) w niej gromadzonych, przetwarzanych, otrzymywanych i wydawanych. Dotyczy ono obszarów przetwarzania tradycyjnego i elektronicznego, choć należy jasno stwierdzić, że w ostatnich latach punkt ciężkości przeniósł się nieodwracalnie w stronę przetwarzania wspomaganego narzędziami, środkami i metodami informatyki.

Obowiązek określenia wymaganego poziomu bezpieczeństwa informacyjnego szeroko pojętej administracji publicznej spoczywa na najwyższych władzach ustawodawczych i wykonawczych, które w konsekwencji odpowiadają za stworzenie warunków do jego osiągnięcia i utrzymania.

Zupełnie naturalną rzeczą, wielokrotnie potwierdzaną w praktyce większości wielkich organizacji poddanych procesom głębokiej informatyzacji jest to, że w pierwszej, często trwającej latami fazie informatyzacji za „obszary informatyczne" uznawało się wszystko co wiązało się z wprowadzaniem, przetwarzaniem lub wydawaniem danych w postaci elektronicznej. W związku z tym służby informatyczne bardzo głęboko wkraczały na teren obszarów merytorycznych będąc siłą napędową (co najmniej w intencji) procesu wdrażania technologii informatycznych. Z realnej oceny sytuacji wynikało bowiem, że przy bardzo ograniczonej identyfikacji komórek merytorycznych z realizowanymi przedsięwzięciami informatycznymi, bez bezpośredniego zaangażowania służb informatycznych, nie byłoby szans na pozytywne wdrożenie technologii informatycznych lub proces wdrożenia uległby znacznemu opóźnieniu.

Obecnie sytuacja jest już odmienna i dlatego należy jak najszybciej rozpocząć lub dokończyć już rozpoczęte procesy rzeczywistego **rozgraniczenia**, pod względem organizacyjnym i kompetencyjnym, **działalności informatycznej** (łącznie z telekomunikacyjną) i **działalności podstawowej**.

Ważnym celem do osiągnięcia w tym względzie jest „wyzwolenie się" działalności podstawowej ze skutków wieloletniego uzależnienia komórek organizacyjnych, ich kierownictw i pojedynczych specjalistów od dominacji specjalistów informatyki.

Jednym z najistotniejszych obszarów wymagających pilnego uporządkowania jest obszar związany z szeroką problematyką zarządzania bezpieczeństwem informacyjnym, w tym przede wszystkim zarządzania niejawnością informacji przetwarzanych z wykorzystaniem metod, narzędzi i technologii informatycznych.

Niniejsza książka stanowi próbę monograficznego ujęcia kilku ważnych problemów z tej dziedziny, przy czym skupia się raczej na kwestiach identyfikacji niż rozwiązywania problemów. Znaczące części książki są efektem prac wykonanych na zlecenie Ministerstwa Nauki i Informatyzacji oraz Ministerstwa Spraw Wewnętrznych i Administracji.

W rozdziale drugim omówiono wzajemne zależności między interoperacyjnością i wskazanymi aspektami bezpieczeństwa informatycznego, a w rozdziale trzecim wybrane aspekty interoperacyjności i bezpieczeństwa teleinformatycznego zawarte w ustawie o informatyzacji działalności podmiotów realizujących zadania publiczne.

W rozdziale czwartym przedstawiono wyniki szerokiej analizy aktów prawnych i normatywnych pod kątem przetwarzania informacji o różnych klauzulach tajności. Uzupełnieniem tego rozdziału jest załącznik nr 1, zawierający uogólniony materiał analityczny.

Rozdział piąty jest poświęcony prezentacji modelu przetwarzania informacji o różnych klauzulach tajności w systemach informatycznych administracji publicznej. Jest to rozdział bardzo ważny dla całości książki. Zdefiniowany w nim model identyfikacyjny daje podstawę do analizy wzajemnej zależności interoperacyjności i bezpieczeństwa ograniczonego do kwestii poufności informacji.

W rozdziale szóstym zidentyfikowano i omówiono najważniejsze zagrożenia i ograniczenia występujące w dziedzinie bezpieczeństwa i interoperacyjności.

Rozdział siódmy został poświęcony analizie przydatności standardowych mechanizmów ochrony danych do zapewnienia bezpieczeństwa przetwarzania informacji niejawnych. Podstawą do sformułowania ogólnych wniosków w tym zakresie była analiza mechanizmów ochrony w systemach operacyjnych Unix, Windows i systemie bazy danych Oracle. Dodatkowo przeprowadziliśmy podobną lecz wstępną analizę w rozwiązaniach portalowych. Uzupełnieniem tego rozdziału jest załącznik nr 2, zawierający uogólniony materiał analityczny.

W rozdziale ósmym przedyskutowano problem wpływu przetwarzania informacji o różnych klauzulach tajności na koszty systemu bezpieczeństwa. Zasadniczym efektem tego rozdziału jest prezentacja „prototypu" modelu do szacowania zidentyfikowanych składników kosztowych systemu bezpieczeństwa.

Rozdział dziewiąty stanowi podsumowanie prac analitycznych, ponieważ zawiera specyfikację najważniejszych modelowych wymagań dotyczących jednocześnie poufności i interoperacyjności.

W rozdziale dziesiątym przedstawiono wyniki analizy spełniania wymagań sformułowanych w rozdziale dziewiątym przez system rejestrowy PESEL.

Rozdział jedenasty stanowi podsumowanie książki. Obok wniosków i wytycznych, zawiera uzupełniające w stosunku do rozdziału dziewiątego propozycje w kwestiach organizacyjno-prawnych oraz technicznych.

Książka może być przydatna dla praktyków i decydentów informatyki oraz szerokich kręgów specjalistów i decydentów z jednostek administracji publicznej korzystających z rozwiązań informatycznych.

2. Analiza zależności między zapewnieniem bezpieczeństwa teleinformatycznego a zapewnieniem interoperacyjności w warunkach przetwarzania informacji o różnych klauzulach tajności

2.1. Pojęcie i znaczenie interoperacyjności systemów informatycznych administracji publicznej

W ujęciu Unii Europejskiej „informatyzacja administracji", to zintegrowane działanie zmierzające do stworzenia tańszej i skuteczniejszej administracji i w rezultacie do poprawy zarządzania państwem i obniżenia kosztów działania administracji [3].

Miarą skuteczności administracji jest jakość wypełniania zadań przede wszystkim na rzecz obywateli. Istnieją bardziej intuicyjne niż precyzyjnie udokumentowane oceny wskazujące na to, że pracownicy administracji publicznej przeznaczają nawet 50%–80% czasu pracy na dotarcie do informacji niezbędnej dla wykonania codziennych zadań, zwłaszcza wtedy, gdy pożądane informacje są rozproszone zarówno geograficznie, jak i kompetencyjnie.

Biorąc to pod uwagę zakłada się, że informatyzacja administracji publicznej powinna być głównym czynnikiem, który przyczyni się do korzystnej zmiany proporcji między czasem traconym na pozyskiwanie informacji i czasem przeznaczanym na merytoryczną analizę i wykorzystanie tych informacji.

Problem skutecznej informatyzacji wiąże się bezpośrednio z zagadnieniem interoperacyjności systemów informacyjnych, zwłaszcza wtedy, gdy rozważamy go w kontekście wsparcia procesów informacyjnych narzędziami i metodami informatyki. Jednakże trzeba wyraźnie podkreślić, że interoperacyjność nie odnosi się wyłącznie do technologii czy systemów informatycznych. Problemy z nią związane zostały dostrzeżone i w wielu przypadkach skutecznie rozwiązywane na długo przez wprowadzeniem samego pojęcia interoperacyjności. Można np. przyjąć bez większych uproszczeń, że podejmowane i rozwijane od dziesiątków lat działania standaryzacyjne wpisywały się w ogólną problematykę interoperacyjności.

Dlatego przystępując do analizy wzajemnych zależności między interoperacyjnością systemów informacyjnych wspieranych narzędziami i metodami informatycznymi (w skrócie interoperacyjnością teleinformatyczną) i bezpieczeństwem informacyjnym warto przyjąć definicję, która nie utraci swego uniwersalnego znaczenia na skutek odwoływania się do kwestii technicznych lub technologicznych. Takie założenia spełnia następująca definicja [23] interoperacyjności:

> Interoperacyjność jest zdolnością dwóch lub większej liczby komponentów do wymiany informacji, rozumienia jej oraz wykorzystania.

Autor definicji podkreślił w swej pracy, że „komponent" jest pojęciem wieloznacznym, bowiem interoperacyjność może zachodzić między całymi systemami, bądź konkretnymi klasami podsystemów. Korzystając z tak szerokiego podejścia do podmiotów interoperacyjności na użytek niniejszej publikacji przyjmiemy węższy zakres znaczeniowy interoperacyjności poprzez ograniczenie go do pojęcia **interoperacyjności teleinformatycznej**, którą przez analogię zdefiniujemy następująco:

> Interoperacyjność teleinformatyczna jest zdolnością dwóch lub większej liczby systemów informatycznych do wymiany informacji, rozumienia jej oraz wykorzystania.

Z punktu widzenia celów publikacji należy zwrócić uwagę na to, że interoperacyjność teleinformatyczna, podobnie jak interoperacyjność w najszerszym sensie to przede wszystkim wymiana, rozumienie i wykorzystywanie informacji.

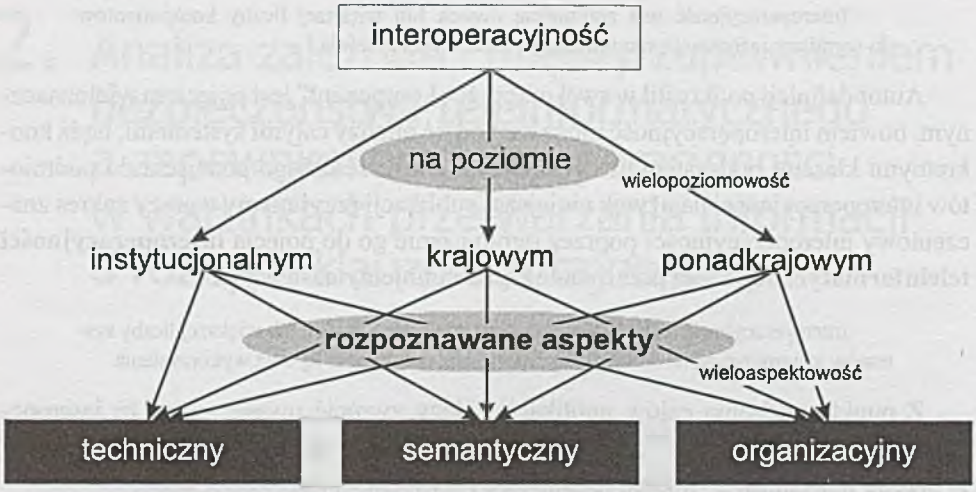
Podkreślenie tego faktu dlatego jest istotne, że często interoperacyjność jest rozumiana wyłącznie jako zdolność do zgodnej i bezkolizyjnej wymiany informacji (danych). Tymczasem samo zapewnienie warunków do skutecznej wymiany informacji (danych) nie wystarczy, by współdziałające w realizacji zadań publicznych systemy informatyczne można było określić jako **interoperacyjne**.

Literatura przedmiotu, jak i oficjalnie przyjmowane dokumenty wskazują na wieloaspektowość i złożoność procesów służących zapewnieniu interoperacyjności. Ostatecznym dowodem przesądzającym o tym, czy systemy informatyczne w stosunku do siebie są interoperacyjne czy nie, jest dopiero potwierdzone w praktyce osiągnięcie celu, stanowiącego przyczynę, dla której zainicjowano współdziałanie systemów informatycznych.

Najogólniej można napisać, że takim celem osiągnięcia interoperacyjności systemów informatycznych eksploatowanych w jednostkach administracji publicznej jest przede wszystkim stworzenie warunków do „bezkolizyjnej" realizacji zadań publicznych w sytuacji konieczności współdziałania dwóch lub więcej systemów informatycznych. Zgodnie z powyższą definicją zapewnienie właściwej wymiany informacji nie przesądza jeszcze o osiągnięciu cechy interoperacyjności, bowiem wymieniane informacje muszą być jeszcze w sposób zgodny i spójny rozumiane i wykorzystywane.

Właśnie dlatego interoperacyjność [3,23] najczęściej jest rozważana (rys. 2-1) nie tylko na wielu poziomach, ale również wieloaspektowo. Wielopoziomowość interoperacyjności teleinformatycznej odnosi się zwykle do „zasięgu" jej oddziaływania. W tym względzie w przypadku administracji publicznej można wyróżnić trzy zasadnicze poziomy:

- instytucjonalny,
- krajowy,
- ponadkrajowy.



Rys. 2-1. Wielopoziomowość i wieloaspektowość interoperacyjności

Poziom instytucjonalny dotyczy organizacji objętej wspólnym kierownictwem i wspólną dokumentacją regulującą wspólne dla niej zasady funkcjonowania i zasady odpowiedzialności. W warunkach administracji publicznej poziomowi instytucjonalnemu odpowiadają np. ministerstwa, urzędy centralne...

Poziom krajowy w odniesieniu do administracji publicznej w praktyce dotyczy działalności ponadsektorowej a **poziom ponadkrajowy** relacji między polską administracją publiczną i administracjami innych krajów, w tym administracją Unii Europejskiej (w tym miejscu przyjęto pewne uproszczenie, bo dla kompletności podziału w zasadzie należało zastąpić poziom ponadkrajowy poziomami międzykrajowym (np. współpraca bilateralna) i ponadkrajowym (np. Unia Europejska).

Odwołując się do wieloaspektowości interoperacyjności teleinformatycznej wymienia się najczęściej trzy główne aspekty:

- techniczny,
- semantyczny,
- organizacyjny.

Aspekt techniczny dotyczy przede wszystkim technologicznych podstaw wymiany informacji. Musi on być rozumiany bardzo szeroko, ponieważ nie chodzi tu tylko o parametry i standardy techniczne stosowanych łączy (np. protokołów transmisji), urządzeń (aktywnych urządzeń sieciowych i infrastruktury przetwarzania) i oprogramowania (systemy operacyjne, systemy baz danych, systemy aplikacyjne i w innej płaszczyźnie np. portale) ale również o kluczową dla interoperacyjności zgodność syntaktyczną wymienianych informacji (danych).

Aspekt semantyczny odnosi się do problemu jednoznaczności znaczeniowej wymienianych i przetwarzanych informacji. Należy w tym miejscu podkreślić, że zapewnianie interoperacyjności dotyczy systemów informatycznych, które po-

wstawały w technologicznie różnych czasach i które odzwierciedlały adekwatne do obowiązujących wtedy unormowań prawnych wizje i procedury realizacji zadań publicznych.

Warto w tym miejscu zauważyć, że niekiedy dyskutując ogólne problemy interoperacyjności używa się pojęcia informacyjnej interoperacyjności (jak w rozdziale 3), które łączy się kwestię zgodności syntaktycznej oraz spójności semantycznej.

W tym miejscu wystarczy przypomnieć, jak drastycznie w ostatnich kilkunastu latach zmieniały się reguły dotyczące dokumentowania gospodarki finansowej państwa i co za tym idzie zasady działania systemów komputerowej rachunkowości. W takim samym stopniu uwagi te dotyczą innych obszarów aktywności państwa i obywateli. Oczywistym skutkiem tych przeobrażeń były zmiany w sposobie reprezentacji (modele informacyjne i odpowiadające im struktury danych) i interpretacji zawartości semantycznej zasobów informacyjnych przetwarzanych w systemach informatycznych.

Problem ten jest widoczny szczególnie ostro, gdy interoperacyjność rozpatruje się nie tylko na gruncie systemów wykorzystywanych w jednej, nawet największej organizacji lecz gdy odnosi się ją do całego państwa i jeszcze szerzej do struktur międzynarodowych, takich jak Unia Europejska.

W takich przypadkach mamy do czynienia nie tylko z regułami wynikającymi z różnic systemów prawnych ale również z tak trudno poddającymi się formalizacji skutkami ukształtowanych przez lata odrębności prawnych i kulturowych. Z tego powodu aby zapewnić możliwość skutecznego współdziałania tworzy się i utrzymuje w sposób ciągły regulacje przyjmujące np. postać Wspólnych Ram Interoperacyjności dla systemów informacyjnych, a więc i systemów informatycznych administracji publicznej całej Unii Europejskiej.

Tworzenie instytucjonalnych, krajowych i ponadkrajowych ram interoperacyjności jest przejawem **organizacyjnego aspektu** interoperacyjności. Nie wystarczą bowiem nawet najlepsza spójna i zgodna technologia i najlepsze, spójne modele semantyczne, by doprowadzić do zaprojektowania systemów posiadających potwierdzone w działaniu cechy interoperacyjności. Konieczna jest jeszcze wola budowy lub włączenia się do „świata interoperacyjnego" potwierdzona w praktyce działaniami organizacyjnymi w dziedzinach planowania, legislacji, struktur organizacyjnych, niezbędnego budżetu.

Faktycznym potwierdzeniem takiej woli w warunkach Polski było uchwalenie w lutym 2005r. ustawy o informatyzacji podmiotów realizujących zadania publiczne. Stanowi ona kluczowy element organizacyjnego wsparcia dla tworzenia ww. „świata interoperacyjnego" bowiem zaprojektowano w niej określone instrumenty wpływania na rozwój infrastruktury informatycznej państwa. Należą do nich przede wszystkim:

- plan informatyzacji państwa oraz projekty informatyczne o publicznym zastosowaniu (sektorowe i ponadsektorowe),
- minimalne wymagania dla systemów teleinformatycznych używanych do realizacji zadań publicznych oraz minimalne wymagania dla rejestrów publicznych i wymiany informacji drogą elektroniczną,

- możliwość dedykowanego wsparcia finansowego przedsięwzięć o szczególnym znaczeniu dla rozwoju społeczeństwa informacyjnego.

Przedstawiając powyżej ogólne rozważania dotyczące zagadnienia interoperacyjności traktujemy je jako wstęp do zagadnienia wpływu bezpieczeństwa informacyjnego na warunki i możliwości zapewnienia interoperacyjności systemów informatycznych.

2.2. Bezpieczeństwo teleinformatyczne a interoperacyjność teleinformatyczna

W systemach informatycznych administracji publicznej gromadzone są olbrzymie zasoby informacyjne, ważne z punktu widzenia najszerzej pojętego interesu i bezpieczeństwa państwa, gospodarki i przede wszystkim obywateli. To rodzi zapotrzebowanie, jak to już wskazano w rozdziale 2, na rozwiązania organizacyjne oraz instrumenty pozwalające skutecznie planować, realizować i kierować procesami informatyzacji niezbędnymi do osiągnięcia wymaganego poziomu bezpieczeństwa informacyjnego jednostek administracji publicznej. W niniejszej publikacji zajmujemy się przede wszystkim poufnością i to w węższym sensie, bo ograniczonym do kwestii wynikających z faktu przypisania zasobom informacyjnym klauzul tajności.

Wraz z rozwojem systemów informatycznych i Internetu obserwujemy stały wzrost zagrożeń dla bezpieczeństwa informacyjnego. Z drugiej strony nowoczesne technologie teleinformatyczne rewolucjonizują nie tylko metody organizacji samych przedsiębiorstw i instytucji ale w coraz większym stopniu wpływają na wzajemne relacje między obywatelami i stworzonymi przez nich podmiotami a administracją publiczną. Coraz więcej osób i organizacji staje się lub chce się stać aktywnymi uczestnikami społeczeństwa informacyjnego. Często przyjmuje się, że czynnikiem sprawczym takich zmian jest stały cywilizacyjny rozwój społeczeństw.

Jednakże problemu bezpieczeństwa teleinformatycznego nie można rozpatrywać w oderwaniu od innych aspektów procesów informatyzacji. Istniejącą obecnie separację systemów informatycznych od otoczenia na każdym z wyżej wymienionych poziomów interoperacyjności należy rozpatrywać w kontekście zadań jakie stoją przed administracją publiczną w procesie budowy społeczeństwa informacyjnego, w tym przede wszystkim celów i zadań wynikających z ustawy o informatyzacji podmiotów realizujących zadania publiczne.

Jest to proces nieodwracalny a działania na rzecz większej otwartości systemów informatycznych stanowią stały element w kształtującym się społeczeństwie informacyjnym [19, 3].

Dlatego bezpieczeństwo informacyjne nie może być traktowane w kategoriach bezwzględnych, musi podlegać weryfikacji pod kątem osiągania zmieniających się celów będących odzwierciedleniem dążeń rozwijającego się społeczeństwa obywatelskiego.

Poufność teleinformatyczna będąca elementem bezpieczeństwa teleinformatycznego podobnie jak w przypadku do interoperacyjności może być rozpatrywana **wielopoziomowo i wieloaspektowo**.

Zasady zapewniania poufności na poszczególnych poziomach są regulowane stosownymi dokumentami, tj. na poziomie instytucjonalnym obowiązującą dokumentacją systemu bezpieczeństwa a na poziomie krajowym zbiorem aktów prawnych (ustawy plus akty wykonawcze) właściwych dla danej dziedziny z tytułu rodzaju utrzymywanych i przetwarzanych informacji.

W oczywisty sposób dokumentacja poziomu instytucjonalnego (polityka bezpieczeństwa i wynikające z niej dokumenty o charakterze instrukcyjnym lub proceduralnym) musi respektować postanowienia zbioru aktów prawnych poziomu krajowego.

Relacja między przepisami krajowymi a ponadkrajowymi nie jest tak oczywista. W stosunkach bilateralnych między Polską i innymi krajami w obszarze nie regulowanym przez dyrektywy Unii Europejskiej decydować muszą wzajemne warunki umowne. W przypadku obszarów regulowanych dyrektywami UE decydują postanowienia tych dyrektyw, o ile dotyczą również Polski.

Najważniejszym aspektem z punktu widzenia celu niniejszej publikacji jest **aspekt semantyczny poufności informacji**, ponieważ on decyduje o tym czy informacja powinna zostać zaklasyfikowana jako niejawna. Jak wcześniej napisano kwalifikacje tajności poszczególnych informacji powinny wynikać bezpośrednio z semantyki i kontekstu występowania wymienianych, gromadzonych lub przetwarzanych informacji.

Kwalifikacja tajności lub inaczej pisząc klasyfikowanie informacji ma charakter uznaniowy i z tego powodu jest najbardziej „czuła" na stan kultury bezpieczeństwa cechującej decydentów na poziomach instytucjonalnym, krajowym i ponadkrajowym.

Procesu kwalifikacji nie da się w prosty sposób zautomatyzować, stąd podkreślenie znaczenia kultury bezpieczeństwa jest tak ważne i uzasadnione.

Aspekt semantyczny dotyczący informacji, którym przypisano klauzule tajności wiąże się bezpośrednio z **aspektami organizacyjnymi i technicznymi**, bowiem o ile **pierwsze** z nich dotyczą ustanawiania regulacji prawnych oraz struktur organizacyjnych odpowiedzialnych za respektowanie tych regulacji, to **aspekty techniczne** dotyczą wymagań technicznych i organizacyjnych w stosunku do urządzeń, oprogramowania i procedur stanowiących infrastrukturę sprzętowo-programową i personalną systemu bezpieczeństwa dla systemu informatycznego przetwarzającego informacje niejawne.

Zadania (usługi) publiczne muszą być realizowane przy bezwzględnym respektowaniu ograniczeń dostępu do informacji prawnie chronionych i jednocześnie dynamicznie zwiększającej się **otwartości i interoperacyjności** systemów informatycznych w zakresie przetwarzania pozostałych informacji niezbędnych dla realizacji zadań publicznych.

Nawiązując ponownie do problemu interoperacyjności w kontekście bezpieczeństwa należy zauważyć, że praktycznie we wszystkich publikacjach dotyczących interoperacyjności problem wpływu utrzymania bezpieczeństwa informacyjnego na warunki zapewniania interoperacyjności jest **całkowicie pomijany**. Tymczasem nawet bez dogłębnej analizy można stwierdzić, że bezpieczeństwo informacyjne, zwłaszcza rozpatrywane pod kątem zapewnienia poufności informacji niejawnych może sta-

nowić i w warunkach Polski stanowi istotną barierę szybkiego postępu w zapewnieniu interoperacyjności teleinformatycznej.

Występuje bowiem sytuacja konfliktowa, w której zapewnienie poufności informacji niejawnych zderza się z narastającą presją na zwiększanie otwartości systemów informatycznych stymulowaną potrzebami społeczeństwa informacyjnego.

Problematyka identyfikacji zagrożeń mających swe źródło w gromadzeniu, wymianie i przetwarzaniu informacji o zróżnicowanych klauzulach tajności dla możliwości zapewnienia interoperacyjności systemów informatycznych zostanie omówiona w rozdziale 6.

Natomiast w tym miejscu trzeba podkreślić, że istnieje pilna konieczność uwzględniania w procesach tworzenia ram interoperacyjności kwestii dotyczących poufności danych niejawnych i to niezależnie od poziomu ich rozpatrywania.

W praktyce może się okazać, że uzgodnione technicznie (w tym syntaktycznie), semantycznie i organizacyjnie środowiska systemów informatycznych nie będą w stanie podjąć współpracy z uwagi na istniejące bariery związane z ograniczeniami towarzyszącymi obligatoryjnie przetwarzaniu informacji niejawnych, zwłaszcza wtedy, gdy realizacja zadań wymaga przetwarzania informacji o różnych klauzulach tajności.

Taką sytuacją mamy do czynienia obecnie, gdy kluczowe dla realizacji zadań publicznych informatyczne implementacje rejestrów państwowych na skutek decyzji kierowników-ministrów właściwych do tworzenia i prowadzenia tych rejestrów przetwarzają dane sklasyfikowane jako niejawne.

3. Interoperacyjność i bezpieczeństwo w ustawie o informatyzacji podmiotów realizujących zadania publiczne

3.1. Wprowadzenie

Podstawowym celem informatyzacji administracji publicznej jest zwiększenie efektywności działania administracji tradycyjnej oraz podniesienie jakości usług elektronicznej administracji publicznej, świadczonych na rzecz obywateli i podmiotów gospodarczych. Jednym z kluczowych zagadnień niezbędnych dla osiągnięcia powyższych celów jest zapewnienie interoperacyjności systemów teleinformatycznych, czyli umożliwienie efektywnej wymiany informacji w formie elektronicznej oraz zapewnienie współpracy systemów teleinformatycznych i rejestrów publicznych. Wymiana informacji w formie elektronicznej jest realizowana pomiędzy:

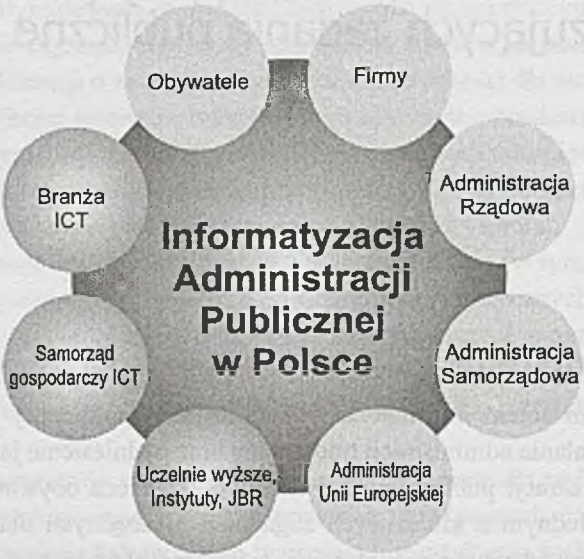
- administracją publiczną a obywatelami,
- administracją publiczną a podmiotami gospodarczymi i organizacjami,
- różnymi jednostkami polskiej administracji publicznej,
- polską administracją publiczną a administracjami innych państw.

Ustawa miała na celu umożliwienie uzyskania dostępności, interoperacyjności i neutralności technologicznej interfejsów systemów teleinformatycznych wykorzystywanych do realizacji zadań publicznych. Powinna umożliwić ministrowi właściwemu do spraw informatyzacji pełnienie roli koordynacyjnej, stymulującej i wpierającej rozwój informatyzacji w Polsce z zachowaniem zasady neutralności technologicznej wykorzystywanych rozwiązań informatycznych.

Proces informatyzacji administracji publicznej dotyczy wielu różnych podmiotów i ma znaczenie horyzontalne. Na rysunku 3-1 zostały zilustrowane najistotniejsze strony zainteresowane informatyzacją. Są to:

- obywatele i firmy (ogólniej: podmioty niepubliczne) – dla nich są realizowane usługi administracji publicznej,
- administracja rządowa, samorządowa i europejskie – polska administracja publiczna powinna być skomunikowana wewnątrz kraju, jak również z innymi administracjami UE (np. administracja układu z Schengen, administracje celne, sądowe, systemy tachografów cyfrowych itd.),

- branża i samorząd gospodarczy ICT – są zainteresowane pracą na rzecz sektora publicznego i dlatego chcą one zdefiniowanych standardów i planów informatyzacji,
- uczelnie wyższe, instytuty, JBR-y – świat nauki jest zainteresowany dostarczaniem know-how na obszar administracji publicznej.



Rysunek 3-1. Strony zaangażowane w informatyzację

3.2. Interoperacyjność

To niepolskie słowo oznacza najogólniej mówiąc „zdolność do współdziałania". Konieczność zagwarantowania interoperacyjności systemów informatycznych w polskiej administracji publicznej wymagało opracowania i wdrożenia ustawy o informatyzacji. Zanim ustawa weszła w życie, polska legislacja nie gwarantowała możliwości metodycznego zapewnienia postulowanej interoperacyjności.

Interoperacyjność w ustawie o informatyzacji (patrz: rysunek 3-2) jest rozumiana w trzech wzajemnie na siebie oddziaływujących płaszczyznach, a mianowicie:

- interoperacyjności organizacyjnej, rozumianej jako uzyskanie możliwości efektywnego współdziałania podmiotów publicznych, obywatela i biznesu – w ustawie szczególny nacisk został położony na zdolność współdziałania podczas czynności administracyjnych realizowanych przy wsparciu systemów teleinformatycznych,
- interoperacyjności informacyjnej, czyli zdolności do efektywnej wymiany informacji pomiędzy podmiotami publicznymi, obywatelem i biznesem – rozumianej zarówno w wymiarze zgodności syntaktycznej danych, jak i spójności semantycznej informacji,
- interoperacyjności technicznej, rozumianej w wymiarze technologii wymiany danych pomiędzy systemami teleinformatycznymi administracji publicznej, a obywatelem i biznesem.

Rysunek 3-2. Istota interoperacyjności na styku systemów informatycznych administracji publicznej i usług przez nie udostępnianych

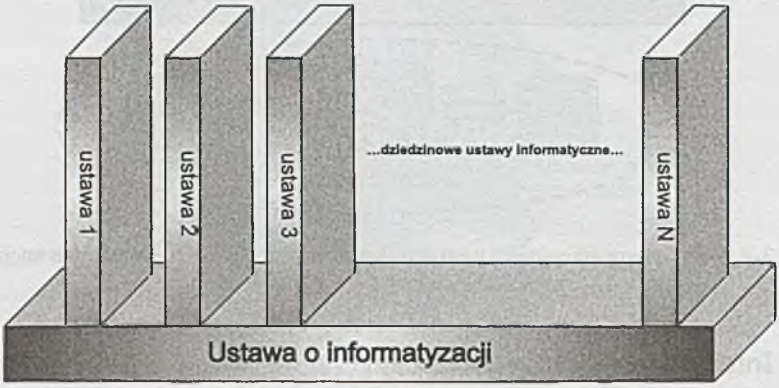
3.2.1. Interoperacyjność organizacyjna

Aby umożliwić ministrowi właściwemu do spraw informatyzacji wpływ na zwiększanie interoperacyjności organizacyjnej w skali całej administracji publicznej, konieczne było wyposażenie go w odpowiednią ustawę według reguł prawnych obowiązujących w polskim systemie prawnym. Umożliwia to, dzięki ustawowym upoważnieniom, skuteczne skoordynowanie tzw. ustaw dziedzinowych i odpowiednich aktów wykonawczych dotyczących konkretnych systemów teleinformatycznych, których jest prawie 900. Wiadomo przecież, że z uwagi na powszechność zastosowań technologii IT powstawały w przeszłości i nadal będą powstawały nowe ustawy, powołujące do życia ważne systemy teleinformatyczne. W ustawach tych najczęściej określa się ogólny zakres funkcjonalny systemów teleinformatycznych, a czasami również wymagania technologiczne dla nich. Nie jest dobrze, kiedy to w kolejnych ustawach powtarza się w zasadzie identyczne wymagania techniczne i organizacyjne dla systemów teleinformatycznych. Sytuacja taka powstała przede wszystkim na skutek wcześniejszego braku ustawy o informatyzacji. W tej właśnie ustawie zostały określone, wspólne dla wszystkich pozostałych ustaw dziedzinowych, ramy interoperacyjności systemów teleinformatycznych. Ustawa pełni rolę tzw. regulacji horyzontalnej (patrz: rysunek 3-3), stanowiącą zasadniczy punkt odniesienia dla innych ustaw dotyczących informatyzacji konkretnych dziedzin aktywności administracji publicznej. W art.2, ust.1 ustawy określono, że przepisy ustawy stosuje się do:

- organów administracji rządowej, organów kontroli państwowej i ochrony prawa, sądów, jednostek organizacyjnych prokuratury, a także jednostek samorządu terytorialnego i ich organów,

- jednostek budżetowych, zakładów budżetowych i gospodarstw pomocniczych jednostek budżetowych,
- funduszy celowych,
- samodzielnych publicznych zakładów opieki zdrowotnej,
- Zakładu Ubezpieczeń Społecznych, Kasy Rolniczego Ubezpieczenia Społecznego,
- Narodowego Funduszu Zdrowia,
- państwowych lub samorządowych osób prawnych utworzonych na podstawie odrębnych ustaw w celu realizacji zadań publicznych.

Wszystkie te organizacje i jednostki nazwano w ustawie ***podmiotami publicznymi.***



Rysunek 3-3. Horyzontalne oddziaływanie ustawy o informatyzacji

Jakie zatem są podstawy interoperacyjności organizacyjnej w obecnym kształcie ustawy o informatyzacji? Odpowiedź na to pytanie wymaga przestudiowania kilku istotnych kwestii, rozstrzygniętych w omawianej ustawie.

Przede wszystkim, autorzy projektu ustawy przyjęli założenie, że dotyczy ona systemów teleinformatycznych działających na styku administracji rządowej, samorządowej, obywatela i biznesu. Ustawa wprowadza konieczność określania kroczącego, maksymalnie pięcioletniego planu informatyzacji państwa, co będzie szczególnie istotne dla firm informatycznych. Wiadomo przecież, że najgorsze, co mogłoby je spotykać w tym zakresie, to brak jasnych reguł funkcjonowania rynku zamówień publicznych w obszarze informatyki, a szczególnie brak odpowiednio wcześnie podanej informacji o planowanych do realizacji systemach teleinformatycznych. Plany informatyzacji mogą pełnić rolę obligatoryjnych dla Rządu RP narzędzi, informujących polską branżę teleinformatyczną o możliwych zamówieniach publicznych w obszarze ICT.

W art.5, ust.2 ustawy określony został cel Planu Informatyzacji Państwa, jako:

- określenie organizacyjnych i technologicznych instrumentów rozwoju społeczeństwa informacyjnego,
- koordynację realizowanych przez więcej niż jeden podmiot publiczny projektów informatycznych o publicznym zastosowaniu,
- modernizację oraz łączenie systemów teleinformatycznych używanych do realizacji zadań publicznych,

- zapewnienie warunków bezpieczeństwa i zgodności działania systemów informatycznych używanych do realizacji zadań publicznych,
- tworzenie warunków do rozwoju współpracy międzynarodowej w zakresie informatyzacji.

Sformułowane w ustawie cele odnoszą się w decydującym stopniu do zagadnienia zapewnienia interoperacyjności organizacyjnej.

W art.5, ust.3 ustawy określona jest zawartość Planu Informatyzacji Państwa:

- określenie priorytetów rozwoju systemów teleinformatycznych używanych do realizacji zadań publicznych,
- zestawienie oraz charakterystykę ponadsektorowych i sektorowych projektów informatycznych służących realizacji priorytetów, o których mowa powyżej, szacunkowe koszty realizacji tych projektów oraz wskazanie możliwych źródeł ich finansowania,
- program działań w zakresie rozwoju społeczeństwa informacyjnego,
- określenie zadań publicznych, które będą realizowane z wykorzystaniem drogi elektronicznej, oraz terminów rozpoczęcia ich realizacji.

Ponadsektorowe projekty informatyczne ustanawia w drodze rozporządzenia (zgodnie z art.8, ust.1 ustawy) Rada Ministrów, na wniosek ministra właściwego do spraw informatyzacji. Sektorowe projekty informatyczne ustanawiają w drodze rozporządzeń (zgodnie z art.9, ust.1 ustawy) ministrowie właściwi do spraw danych działów administracji rządowej, po zasięgnięciu opinii ministra właściwego do spraw informatyzacji.

W art.17 ustawy przewidziano funkcjonowanie Rady Informatyzacji działającej przy ministrze właściwym do spraw informatyzacji, zadania Rady, tryb jej powołania i działania. Natomiast w art.19 ustawy zobowiązano ministra właściwego do spraw informatyzacji do prowadzenia Krajowej Ewidencji Systemów Teleinformatycznych i Rejestrów Publicznych. Można się spodziewać, że te instytucjonalne rozwiązania będą w istotnym stopniu wspomagać osiąganie zadowalającego poziomu interoperacyjności organizacyjnej.

Kolejnym, dość silnym założeniem ustawy, jest obligatoryjność certyfikowania przez ministra do spraw informatyzacji wszystkich systemów teleinformatycznych używanych do realizacji zadań publicznych pod względem ich zgodności z tzw. „minimalnymi wymaganiami". Nadzór ten ma mieć charakter w większy stopniu stymulowania rozwoju systemów teleinformatycznych administracji publicznej, niż standardowego kontrolowania ich zgodności z minimalnymi wymaganiami.

Delegację do ustanowienia, w drodze rozporządzenia, minimalnych wymagań dla systemów teleinformatycznych oraz rejestrów publicznych i wymiany informacji w formie elektronicznej, przez Radę Ministrów, na wniosek ministra właściwego do spraw informatyzacji, zawiera art.18 ustawy. Minimalne wymagania w zadanym zakresie zostały określone w rozporządzeniach:

- Rozporządzenie Rady Ministrów z dnia 11 października 2005 r. w sprawie minimalnych wymagań dla systemów teleinformatycznych, Dz. U. Nr 212 z dnia 28.10.2005 r. poz. 1766,

- Rozporządzenie Rady Ministrów z dnia 11 października 2005 r. w sprawie minimalnych wymagań dla rejestrów publicznych i wymiany informacji w formie elektronicznej, Dz. U. Nr 214 z dnia 28.10.2005r. poz. 1781.

Przepisy zawarte w tych rozporządzeniach rozpatrzymy w odniesieniu do *interoperacyjności informacyjnej* oraz *interoperacyjności technicznej*.

Ważnym założeniem, przyjętym w ustawie (art.21 ustawy) jest jawność zestawów testów akceptacyjnych dla oprogramowania interfejsowego, umożliwiającego wymianę danych z systemami informatycznymi, używanymi do realizacji zadań publicznych. Wytyczne odnośnie sposobu dokumentowania i przeprowadzania testów akceptacyjnych zawiera:

- Rozporządzenie Ministra Nauki i Informatyzacji z dnia 19 października 2005 r. w sprawie testów akceptacyjnych oraz badania oprogramowania interfejsowego i weryfikacji tego badania, Dz. U. Nr 217 z dnia 31.10.2005r. poz. 1836.

Kolejnym z istotnych założeń organizacyjnych, jakie znalazło swoje miejsce w ustawie o informatyzacji (art.15 ustawy), jest przyjęcie zasady, że jeżeli podmioty niepubliczne, np. obywatel i biznes, mają narzucaną przez państwo konieczność komunikowania się z nim drogą informatyczną, to odpowiednie do tego oprogramowanie jest udostępnianie nieodpłatnie. Tryb udostępniania jest określony w:

- Rozporządzeniu Rady Ministrów z dnia 27 września 2005 r. w sprawie sposobu, zakresu i trybu udostępniania danych w rejestrze publicznym, Dz. U. Nr 205 poz. 1692.

Podsumowując, główne założenia interoperacyjności organizacyjnej opierają się na następujących wytycznych:

- horyzontalność plus neutralność technologiczna i polityczna ustawy,
- plany informatyzacji,
- powoływanie ponadsektorowych i sektorowych projektów informatycznych,
- powołanie Rady Informatyzacji – ciała opiniodawczego ministra informatyzacji,
- utworzenie Krajowej Ewidencji Systemów Teleinformatycznych i Rejestrów Publicznych,
- kontrola zgodności systemów z minimalnymi wymaganiami,
- jawność zestawów testów akceptacyjnych dla oprogramowania interfejsowego,
- nieodpłatne udostępnianie podmiotom niepublicznym oraz samorządom niezbędnego oprogramowania interfejsowego.

Przytoczone wyżej postanowienia umowy stwarzają dobre ramy do zapewnienia *interoperacyjności organizacyjnej* w realizacji zadań publicznych.

3.2.2. Interoperacyjność informacyjna

Interoperacyjność informacyjna dotyczy dwóch zasadniczych kwestii, a mianowicie:

- syntaktycznej zgodności danych przesyłanych pomiędzy systemami (dotyczy sposobu opisu struktury przesyłanych danych), zwanej również interoperacyjnością syntaktyczną,
- semantycznej zgodności informacji, nazywanej często interoperacyjnością semantyczną.

Wymiana informacji pomiędzy podmiotami publicznymi i niepublicznymi powinna być analizowana przez pryzmat dwóch najważniejszych jej narzędzi. Są nimi: dokument elektroniczny i wymiana referencyjnych (bazowych) atrybutów rejestrowych.

W zakresie interoperacyjności syntaktycznej ustawa o informatyzacji ma doprowadzić do pełnej zgodności i zarządzalności formatów opisu logicznej struktury dokumentu elektronicznego w polskiej administracji publicznej, a także do wspólnego opisu formatu kluczowych atrybutów referencyjnych rejestrów publicznych. Często powtarzanym przykładem braku zgodności syntaktycznej jest na przykład różny sposób zapisu nazw miejscowości czy też nazw ulic. Dla zwykłego śmiertelnika, na przykład, „Gorzów Wielkopolski" i „Gorzów Wlkp." stanowią pojęcia równoważne. Wiadomo jednak, że dla systemów teleinformatycznych są to dwie różne nazwy miejscowości. Można oczywiście wprowadzać dodatkowe mechanizmy kojarzące różne sposoby zapisu nazw, ale jest to zawsze potencjalne miejsce powstawania niejednoznaczności interpretacyjnych, a co za tym idzie – potencjalne zagrożenia dla spójności informacji przekazywanych pomiędzy systemami.

Syntaktyczna zgodność opisu danych stanowi podstawę dla uzyskania zgodności semantycznej informacji, co jest niewątpliwie zadaniem o wiele bardziej złożonym. Rzecz w tym, aby uzyskać pełną spójność informacyjną systemów teleinformatycznych, dzięki czemu będzie można na przykład uniknąć niejednoznaczności interpretacyjnych przesyłanych informacji.

Podstawowe przepisy, służące zapewnieniu interoperacyjności informacyjnej zostały zawarte w trzech aktach wykonawczych, wydanych na podstawie art. 18 ustawy (były już one przywołane, ponieważ odnoszą się również do interoperacyjności organizacyjnej). Są to:

- Rozporządzenie Rady Ministrów z dnia 11 października 2005 r. w sprawie minimalnych wymagań dla systemów teleinformatycznych, Dz. U. Nr 212 z dnia 28.10.2005r. poz. 1766,
- Rozporządzenie Rady Ministrów z dnia 11 października 2005 r. w sprawie minimalnych wymagań dla rejestrów publicznych i wymiany informacji w formie elektronicznej, Dz. U. Nr 214 z dnia 28.10.2005r. poz. 1781.
- Rozporządzenie Ministra Nauki i Informatyzacji z dnia 19 października 2005 r. w sprawie testów akceptacyjnych oraz badania oprogramowania interfejsowego i weryfikacji tego badania, Dz. U. Nr 217 z dnia 31.10.2005 r. poz. 1836.

W pierwszym z przywołanych powyżej rozporządzeń przedstawiono wiele istotnych wymagań, które służyć mają podniesieniu poziomu interoperacyjności informacyjnej:

- W § 2 pkt 1 rozporządzenia sformułowany jest ogólny wymóg, że „systemy teleinformatyczne używane przez podmioty publiczne do realizacji zdań publicznych powinny spełniać właściwości i cechy w zakresie funkcjonalności, niezawodności, używalności, wydajności, przenoszalności i pielęgnowalności, określone w normach ISO zatwierdzonych przez krajową jednostkę normalizacyjną, na etapie projektowania, wdrażania i modyfikowania tych systemów".

- W załączniku nr 1 określono wymagania umożliwiające wymianę danych z innymi systemami teleinformatycznymi używanymi do realizacji zadań publicznych za pomocą protokołów komunikacyjnych i szyfrujących:
  - do wymiany danych z systemami teleinformatycznymi,
  - do wymiany danych z systemami teleinformatycznymi prowadzonej w formie komunikacji pomiędzy klientem i serwerem poczty elektronicznej,
  - do szyfrowania wymiany danych z systemami teleinformatycznymi,
  - do wymiany danych z systemami teleinformatycznymi w zakresie innych usług sieciowych.
- W załączniku nr 2 określono wymagania zapewniające dostęp do zasobów informacji udostępnianych przez systemy teleinformatyczne używane do realizacji zadań publicznych przy wykorzystaniu formatów danych:
  - do kodowania i szyfrowania informacji,
  - do danych zawierających dokumenty tekstowe lub tekstowo-graficzne,
  - do danych zawierających informację graficzną,
  - do kompresji dokumentów elektronicznych o dużych rozmiarach,
  - do tworzenia i modyfikacji stron WWW,
  - do definiowania układu informacji,
  - do przetwarzania dokumentów zapisanych w formacie XML.

Należy podkreślić, że jest to pierwszy w Polsce akt prawny, w którym wskazano **standard XML jako podstawę opisu struktury logicznej** dokumentu elektronicznego, tj. sposobu ułożenia informacji w dokumencie zdefiniowanym poprzez określenie elementów informacyjnych oraz powiązań pomiędzy nimi.

Drugie z powyżej wskazanych rozporządzeń (w sprawie minimalnych wymagań dla rejestrów publicznych i wymiany informacji w formie elektronicznej) jest aktem legislacyjnym, który w sposób systematyczny podaje zakres oraz definicję typów danych dla 16 kluczowych atrybutów referencyjnych rejestrów publicznych w Polsce. Jest to bardzo istotne dla zachowania interoperacyjności rejestrów publicznych i dla wskazania tych atrybutów rejestrowych, które pełnią zasadniczą rolę w wymianie danych pomiędzy kluczowymi zasobami informacyjnymi w Polsce. Rozporządzenie objęło następujące atrybuty rejestrowe:

- Numer PESEL,
- Nazwisko–człon,
- Imię,
- Numer identyfikacyjny REGON,
- Symbol jednostki podziału terytorialnego,
- Nazwa jednostki podziału terytorialnego,
- Identyfikator miejscowości,
- Nazwa miejscowości,
- Symbol ulicy,
- Nazwa ulicy,
- Numer porządkowy lokalu,

- Numer porządkowy budynku,
- Numer Krajowego Rejestru Sądowego,
- Numer identyfikacji podatkowej (NIP),
- Identyfikator działki ewidencyjnej,
- Identyfikator budynku.

Przyjęto założenie, że zakres referencyjnych atrybutów rejestrowych będzie modyfikowany zgodnie z kierunkiem rozwoju systemów teleinformatycznych używanych do realizacji zadań publicznych.

Trzecie ze wskazanych rozporządzeń (w sprawie testów akceptacyjnych oraz badania oprogramowania interfejsowego i weryfikacji tego badania) określa:

- metodykę, warunki i tryb sporządzania testów akceptacyjnych oprogramowania interfejsowego,
- sposób postępowania w zakresie badania oprogramowania interfejsowego,
- rodzaje oprogramowania interfejsowego podlegającego badaniu,
- szczegółowy zakres informacji dotyczących oprogramowania interfejsowego oraz sposób i tryb przekazywania tych informacji,
- wzór oświadczenia o wyniku badania oraz weryfikacji badania oprogramowania interfejsowego.

Oprogramowanie interfejsowe słusznie potraktowano w przepisach wyjątkowo, ponieważ pełni ono szczególną rolę w zapewnianiu interoperacyjności informacyjnej.

3.2.3. Interoperacyjność techniczna

Najniższy – co nie oznacza, że trywialny – poziom interoperacyjności, to jej wymiar techniczny. Poziom ten jest dobrze zrozumiały dla programistów, którzy zajmują się oprogramowaniem protokołów wymiany danych pomiędzy systemami teleinformatycznymi, formatami zapisu dokumentów elektronicznych i pozostałymi formatami zapisu plików. Tak więc na przykład protokół internetowy TCP/IP, czy też standard kodowania znaków UNICODE, dotyczą właśnie technicznego wymiaru interoperacyjności.

Szczegółowy zakres wymagań w zakresie technicznym został zamieszczony w przywołanym już:

- Rozporządzeniu Rady Ministrów z dnia 11 października 2005 r. w sprawie minimalnych wymagań dla systemów teleinformatycznych, Dz. U. Nr 212 z dnia 28.10.2005r. poz. 1766.

Specyfikację wymagań zawartych w tym rozporządzeniu przytoczyliśmy już z punktu widzenia ich wpływu na zapewnienie interoperacyjności informacyjnej. Mają zaś one charakter techniczny. Regulują zakres standardów dla:

- formatu kodowania znaków,
- protokołów komunikacyjnych,
- protokołów szyfrujących,
- formatu plików używanych do zapisu dokumentów elektronicznych,
- formatu plików używanych do zapisu grafiki, dźwięków, plików skompresowanych.

Zapewnieniu interoperacyjności technicznej służy też:

- Rozporządzenie Ministra Nauki i Informatyzacji z dnia 19 października 2005 r. w sprawie testów akceptacyjnych oraz badania oprogramowania interfejsowego i weryfikacji tego badania, Dz. U. Nr 217 z dnia 31.10.2005r. poz. 1836.

W załączniku nr 1 tego rozporządzenia określony został wzór specyfikacji przypadku testowego oprogramowania interfejsowego. W załączniku nr 2 określony został wzór specyfikacji scenariusza testowego oprogramowania interfejsowego. W załączniku nr 5 określony został wzór raportu podsumowującego badanie oprogramowania interfejsowego. Precyzują one łącznie techniczną stronę zapewnienia interoperacyjności systemów teleinformatycznych używanych do realizacji zadań publicznych.

3.3. Bezpieczeństwo

Ustawa o informatyzacji miała także na celu osiągnięcie wyższego poziomu bezpieczeństwa informacyjnego, w tym teleinformatycznego dla systemów informatycznych wykorzystywanych do realizacji zadań publicznych. Ustawa wprowadziła obowiązek opracowywania polityki bezpieczeństwa dla wszystkich systemów informatycznych wykorzystywanych do realizacji zadań publicznych.

W wytycznych dotyczących zakresu przygotowywania planów informatyzacji Państwa nakazuje się między innymi konieczność „zapewnienia warunków bezpieczeństwa i zgodności działania systemów teleinformatycznych używanych do realizacji zadań publicznych". W art. 18 ustawa daje wytyczne do takiego opracowania minimalnych wymagań dla systemów teleinformatycznych, aby wziąć pod uwagę w szczególności konieczność zachowania „sprawnej i bezpiecznej wymiany informacji w formie elektronicznej między podmiotami publicznymi oraz między podmiotami publicznymi a organami innych państw lub organizacji międzynarodowych".

Dlatego też, rozporządzenie Rady Ministrów z dnia 11 października 2005 r. w sprawie minimalnych wymagań dla systemów teleinformatycznych, Dz. U. Nr 212 z dnia 28.10.2005r. poz. 1766 mówi o polityce bezpieczeństwa w następujący sposób:

1. § 3. 1: Podmiot publiczny opracowuje, modyfikuje w zależności od potrzeb oraz wdraża politykę bezpieczeństwa dla systemów teleinformatycznych używanych przez ten podmiot do realizacji zadań publicznych.
2. § 3. 2: Przy opracowywaniu polityki bezpieczeństwa, o której mowa w ust. 1, podmiot publiczny powinien uwzględniać postanowienia Polskich Norm z zakresu bezpieczeństwa informacji.

Wydaje się słuszne w tym miejscu zastosowanie co najmniej następujących norm krajowych dotyczących bezpieczeństwa informacji:

- PN ISO/IEC 17799:2003 Praktyczne zasady zarządzania bezpieczeństwem informacji – wytyczne, w jaki sposób tworzyć polityki bezpieczeństwa organizacji z różnych sektorów, w tym również administracji państwowej i samorządowej,

- PN-I-07799-2:2005 Systemy zarządzania bezpieczeństwem informacji. Specyfikacja i wytyczne do stosowania – wymagania dot. systemów zarządzania bezpieczeństwem informacji – w jaki sposób zarządzać bezpieczeństwem z uwzględnieniem zarządzania ryzykiem.

Tworzący się obecnie system normalizacji międzynarodowej bazuje na normach serii 27000 – w szczególności normie 27001 – następcy PN-I-07799-2. Warto wspomnieć, że polska norma PN-I-07799-2 wyprzedziła normę międzynarodową. Daje ona wytyczne dla formułowania jasnych i jednoznacznych kryteriów bezpieczeństwa informacji i systemów je przetwarzających. Jest to szczególnie istotne dla administracji rządowej i samorządowej i może stanowić tym samym właściwy sposób realizacji wytycznych wynikających z rozporządzenia dotyczącego minimalnych wymagań dla systemów i dotyczących konieczności opracowywania polityk bezpieczeństwa teleinformatycznego. Dzięki takiemu działaniu będzie można uzyskać następujące korzyści:

- obiektywna ocena stanu bezpieczeństwa informacji w jednostce organizacyjnej,
- zgodność systemów teleinformatycznych administracji państwowej i samorządowej z przepisami prawa,
- wyznaczenie mierzalnych celów dla zarządzania bezpieczeństwem informacji, dzięki uprzedniemu zdefiniowaniu wymaganego poziomu bezpieczeństwa, któremu towarzyszy identyfikacja odpowiedzialności za poszczególne elementy bezpieczeństwa informacji, na każdym etapie jej powstawania i przechowywania,
- ograniczenie ryzyka utraty, zniekształcenia, niepowołanego dostępu do wewnętrznych informacji organizacji,
- ograniczenie strat materialnych wynikających np. z ujawnienia informacji, utraty danych i niepożądanej modyfikacji danych przechowywanych w systemach informatycznych i z wielu innych zagrożeń, na które organizacja było dotychczas szczególnie podatna,
- wzrost bezpieczeństwa działania i wiarygodności organizacji na konkurencyjnym rynku teleinformatycznym,
- umiejętność precyzyjnego określania miejsc oraz prawdziwych przyczyn powstania największych ryzyk biznesowych, dzięki czemu możliwe będzie przeciwdziałanie ich wystąpieniu,
- usprawnienie przepływu i dostępu do informacji przy jednoczesnym wzroście bezpieczeństwa użytkowania informacji,
- bieżące usuwanie podatności i ryzyka utraty informacji,
- wzrost elastyczności działania organizacji poprzez lepsze dostosowanie struktury organizacyjnej do wewnętrznych i zewnętrznych wymogów funkcjonowania,
- jasny, spójny i skoordynowany program nakładów inwestycyjnych na bezpieczeństwo informacji i informatykę,
- zmiana mentalności pracowników, wzrostu motywacji i efektywności procesów pracy,

- możliwość poddania zbudowanego systemu zarządzania bezpieczeństwem informacji niezależnej ocenie (certyfikacji) na zgodność z normą polską PN-I-07799-2 lub normą międzynarodową ISO/IEC 27001.

3.4. Podsumowanie

Analizując rozwiązania dotyczące interoperacyjności i bezpieczeństwa teleinformatycznego w ustawie o informatyzacji, należy podkreślić, że pierwowzorem były tutaj osiągnięcia programu Unii Europejskiej, który został nazwany akronimem IDA2, co oznacza: *„Interchange of Data between Administrations"*. W programie tym określono technologiczne i informacyjne aspekty interoperacyjności w jej wymiarze horyzontalnym, z którego czerpie ponad 40 programów dziedzinowych (wertykalnych) rozwijanych również w ramach IDA. Program IDA2 nie rozwiązywał wszystkich problemów, zwłaszcza dotyczących możliwości interoperacyjnego wykorzystywania rejestrów publicznych. Istotne kierunkowe rozwiązania i stosowne instrumenty zaprojektowano w ustawie o informatyzacji działalności podmiotów realizujących zadania publiczne. Są to rozwiązania oryginalne, które powinny w konsekwencji doprowadzić np. do tego, by beneficjenci usług administracji publicznej do celów identyfikacyjnych posługiwali się jednym z dwóch numerów rejestrowych, tj.:

- Numerem PESEL – dla osób fizycznych,
- Numerem Identyfikacji Podatkowej (NIP) – dla podmiotów gospodarczych niebędących osobami fizycznymi.

Powyższe identyfikatory powinny stanowić podstawowe *atrybuty referencyjne* rejestrów publicznych w Polsce. Oznacza to, że inne systemy informatyczne powinny odnosić się do tych atrybutów zawsze wtedy, kiedy będą identyfikować osobę fizyczną lub podmiot gospodarczy. Przy takim podejściu wiele z obecnie używanych identyfikatorów, takich jak na przykład numer KRS czy numer REGON mogą być traktowane jako wewnętrzne identyfikatory używane w systemach administracji publicznej bez konieczności nakładania na beneficjentów w urzędach obowiązków posługiwania się nimi. Dzięki temu obywatel nie będzie zmuszany do zapamiętywania kilku numerów ewidencyjnych, jak to ma miejsce w chwili obecnej.

Nietrudno doszukać się analogii między koncepcjami rozwoju programu IDA a wskazanym na wstępie horyzontalnym umocowaniem ustawy o informatyzacji w stosunku do ustaw dziedzinowych wprowadzających potrzebę budowy kolejnych systemów teleinformatycznych.

Kolejne sugestie zaczerpnięte z osiągnięć IDA spowodowały również między innymi to, że standard XML wraz z jego pochodnymi został uznany za podstawę opisu struktury logicznej dokumentu elektronicznego.

Podsumowując, należy wyraźnie podkreślić, że ***istota informatyzacji administracji publicznej leży w umiejętnym zastosowaniu metod i narzędzi współczesnej informatyki w celu uzyskania odpowiedniego oprzyrządowania usług administracji***

publicznej, ergonomicznych dla beneficjentów tych usług. Powyższa zasada dotyczy zarówno tradycyjnych urzędów, które bez właściwego zaplecza informatycznego nie będą w stanie efektywnie pracować, jak w również dla urzędu wirtualnego, który stanowi alternatywę urzędów tradycyjnych, nie rugując ich w żadnej mierze. Można ocenić, że ustawa o informatyzacji wraz z jej aktami wykonawczymi daje niezbędne oprzyrządowanie legislacyjne, dzięki któremu można tę ideę zmaterializować w rzeczywistości.

4. Przetwarzanie informacji o różnych klauzulach tajności na podstawie analizy aktów prawnych i normatywnych

4.1. Wprowadzenie

Celem analizy wybranych aktów prawnych oraz norm bezpieczeństwa było uzyskanie przesłanek przydatnych dla odpowiedzi na następujące pytania:

- czy zapisy zawarte w analizowanych aktach prawnych tworzą spójne ramy dla nadawania klauzul tajności?
  [zauważmy, iż pytanie to ma trzy warstwy dotyczące:
  - informacji pierwotnej (źródłowej),
  - zbiorów informacji,
  - wyniku przetwarzania informacji z wielu źródeł]
- czy zapisy zawarte w analizowanych aktach prawnych kompleksowo, kompletnie i spójnie definiują:
  - reguły oraz tryb postępowania,
  - wymagania na urządzenia, mechanizmy i techniki

  przy realizacji poszczególnych stadiów przetwarzania informacji?
- czy zapisy zawarte w analizowanych aktach prawnych dają wystarczające podstawy do budowy systemów skutecznie eliminujących lub ograniczających występowanie podatności na zagrożenia dla bezpieczeństwa informacyjnego i jednocześnie w sposób nieuzasadniony nie stwarzają barier dla interoperacyjności systemów informatycznych?
  [z zagadnieniem tym wiążą się kwestie następujące:
  - wspólna baza pojęciowa (definicje pojęć „bezpieczeństwo informacyjne", „interoperacyjność"),
  - wymagania na urządzenia, mechanizmy i techniki (i inne) zapewniające odpowiedni poziom bezpieczeństwa informacyjnego].

4.2. Wykaz analizowanych aktów prawnych i normatywnych

Analizie poddano trzy grupy aktów prawnych – są to:

- ustawy ogólne i akty wykonawcze do nich:
  - ustawa o ochronie informacji niejawnych i jej akty wykonawcze,
  - ustawa o ochronie danych osobowych i jej akty wykonawcze,
  - ustawa o informatyzacji działalności podmiotów realizujących zadania publiczne i jej akty wykonawcze,
- ustawy i akty wykonawcze dla wybranych rejestrów publicznych; są to rejestry zawierające dane o kluczowych obiektach, które są opisywane w rejestrach publicznych (osoby fizyczne, przedsiębiorcy, jednostki administracyjnego podziału kraju) – czyli:
  - Powszechny Elektroniczny System Ewidencji Ludności (PESEL),
  - Krajowy Rejestr Sądowy (KRS),
  - Krajowy Rejestr Urzędowy Podziału Terytorialnego Kraju (TERYT),
- branżowe regulacje dotyczące wybranych dziedzin życia publicznego – z uwagi na powszechność wybrano bankowość i statystykę publiczną; aktami prawnymi poddanymi analizie były:
  - ustawa prawo bankowe,
  - ustawa o statystyce publicznej i jej akty wykonawcze.

Dodatkowo poddano analizie w niezbędnym zakresie wskazówki znajdujące się w normach międzynarodowych (przyjętych oficjalnie w Polsce) dotyczących problematyki bezpieczeństwa systemów informatycznych:

- PN-I-13335-1 – „Technika informatyczna – Wytyczne do zarządzania bezpieczeństwem systemów informatycznych. Pojęcia i modele bezpieczeństwa systemów informatycznych",
- PN-ISO/IEC 17799 – „Technika informatyczna – Praktyczne zasady zarządzania bezpieczeństwem informacji",
- PN-I-07779-2 – „Systemy zarządzania bezpieczeństwem informacji – Część 2: Specyfikacja i wytyczne do stosowania".

4.3. Aspekty organizacyjno-prawne

4.3.1. Wyniki analizy aktów prawnych

Poniżej przedstawiamy zestawienie najważniejszych regulacji w aspektach prawno-organizacyjnych, określonych w przeanalizowanych ustawach ogólnych i aktach wykonawczych do nich:

- Definicje pojęć „informacje niejawne" i „dane osobowe".
- Klasyfikacja informacji niejawnych i definicje klauzul tajności dla informacji niejawnych.
- Zasady przyznawania klauzul tajności.

- Okresy ochrony poszczególnych grup informacji niejawnych.
- Wymóg akredytacji bezpieczeństwa teleinformatycznego dla systemów informatycznych przetwarzających informacje niejawne.
- Podstawowe warunki bezpieczeństwa teleinformatycznego.
- Warunki techniczne i organizacyjne dla systemów informatycznych, służących do przetwarzania danych osobowych.
- Minimalne wymagania dla systemów teleinformatycznego.
- Minimalne wymagania dla rejestrów publicznych i wymiany informacji w formie elektronicznej.
- Zasady uzyskiwania certyfikatu bezpieczeństwa teleinformatycznego dla systemów informatycznych, w których przetwarzane są informacje niejawne.
- Zasady organizacji eksploatacji systemów informatycznych, w których przetwarzane są informacje niejawne.
- Zasady zgłaszania zbioru danych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych.
- Poziomy bezpieczeństwa przetwarzania danych osobowych w systemach informatycznych.

Z kolei najistotniejsze regulacje dotyczące aspektów prawno-organizacyjnych, zawarte w ustawach i aktach wykonawczych dla wybranych rejestrów publicznych to:

- W regulacjach dla rejestru PESEL używa się pojęcia „dane osobowe", danym gromadzonym w rejestrze nie przypisuje się żadnej z klauzul tajności.
- Rejestry KRS i TERYT określa się jako rejestry jawne.
- Wymóg prowadzenia rejestrów PESEL, KRS, TERYT z wykorzystaniem systemów informatycznych.
- Zasady wymiany informacji z rejestru podmiotów gospodarki narodowej (REGON) z organami prowadzącymi rejestry i ewidencje lub systemy informacyjne administracji publicznej.

Najważniejsze branżowe regulacje dotyczące aspektów prawno-organizacyjnych dla wybranych dziedzin życia publicznego:

- Wprowadza się pojęcia „tajemnica bankowa" i „tajemnica statystyczna".
- Zabroniono gromadzenia w jednym zbiorze lub w jednej bazie danych wszystkich zebranych przez służby statystyki publicznej danych osobowych dotyczących konkretnej osoby fizycznej.
- Określono maksymalny okres przetwarzania informacji stanowiących tajemnicę bankową w celu oceny zdolności kredytowej i analizy ryzyka kredytowego.

4.3.2. Wyniki analizy aktów normatywnych

Zalecenia związane z klasyfikowaniem informacji:

- Zaleca się klasyfikowanie informacji, tak aby wskazać potrzebę, priorytety i poziom ochrony. Zaleca się wykorzystywanie systemu klasyfikowania informacji do zdefiniowania odpowiedniego zbioru poziomów ochrony i do informowania o potrzebie użycia specjalnych środków postępowania.

- Informacje i dane wyjściowe z systemów obsługujących klasyfikowane dane powinny być oznakowane w zależności od ich ważności dla instytucji i wrażliwości. Może być stosowne także oznakowanie informacji w zależności od ich krytyczności dla organizacji, np. wg kryteriów integralności i dostępności. Zaleca się, aby wytyczne klasyfikacji z góry nie zakładały, że nie jest konieczne, aby klasyfikacja jakiejkolwiek informacji była bezterminowa, ale że może zostać zmieniona zgodnie z ustaloną wcześniej polityką.
- Zaleca się, aby uważać przy interpretacji oznaczeń stosowanych w klasyfikacji dokumentów otrzymanych z innych organizacji, które mogą mieć różne definicje dla tych samych lub podobnie brzmiących oznaczeń.
- Obowiązek w zakresie określania klasyfikacji elementu informacji, a także okresowego przeglądania klasyfikacji powinien spoczywać na twórcy lub wyznaczonym właścicielu informacji. [Zwracamy uwagę, że zalecenie to jest uogólnieniem zapisu z ustawy o ochronie informacji niejawnych, gdzie mówi się tylko o twórcy („osoba upoważniona do podpisania dokumentu")]
- Zaleca się też opracowanie procedur posługiwania się informacjami, zgodnie z ich klasyfikacją, zawartymi w dokumentach, przetwarzanymi w systemach przetwarzania danych, komputerach przenośnych.
- Należy zwrócić uwagę na wymagania prawne dotyczące tzw. transgranicznego przepływu danych (informacja jest utworzona w jednym kraju i przysłana do innego kraju) – mogą one być różne w poszczególnych krajach.

Wybrane zalecenia dotyczące zabezpieczania dokumentów instytucji:

- Zaleca się uwzględnienie zjawiska starzenia się nośników używanych do przechowywania zapisów. Zaleca się, aby wdrożone procedury przechowywania i postępowania były zgodne z zaleceniami producenta nośnika.
- W przypadku zastosowania do przechowywania zapisów nośników elektronicznych, zaleca się wprowadzanie procedur zapewniających dostęp do danych (możliwość czytania danego nośnika i formatu) przez cały okres przechowywania, tak aby zabezpieczyć się przed utratą danych, spowodowaną zmianami technologii w przyszłości.

4.4. Aspekty techniczne

4.4.1. Wyniki analizy aktów prawnych

Zestawienie najważniejszych regulacji w aspektach technicznych, określonych w przeanalizowanych ustawach ogólnych i aktach wykonawczych do nich:

- Wymóg badań i certyfikacji urządzeń i narzędzi kryptograficznych wchodzących w skład systemów informatycznych przetwarzających informacje niejawne.
- Sposoby zapewnienia poszczególnych typów ochrony systemów informatycznych.
- Wymagane środki bezpieczeństwa dla poszczególnych poziomów bezpieczeństwa danych osobowych.
- Dopuszczalne formaty danych udostępnianych przez systemy teleinformatyczne używane do realizacji zadań publicznych.

- Sposób, zakres i tryb udostępniania danych zgromadzonych w rejestrze publicznym.
- Protokoły komunikacyjne i szyfrujące umożliwiające wymianę danych z innymi systemami teleinformatycznymi do realizacji zadań publicznych.
- Wymóg, aby w wymianie informacji w formie elektroniczne wymienione cechy informacyjne stosować zgodnie z określoną definicją.

Najistotniejsze regulacje dotyczące aspektów technicznych, zawarte w ustawach i aktach wykonawczych dla wybranych rejestrów publicznych to:

- Dla rejestru PESEL – wymóg posiadania urządzeń umożliwiających identyfikację osoby uzyskującej dane w systemie oraz zakresu, daty i celu ich uzyskania a także zabezpieczenia technicznego i organizacyjnego „uniemożliwiającego wykorzystanie danych niezgodnie z celem ich uzyskania" przez podmioty pozyskujące dane drogą teletransmisji.

W branżowych regulacjach dla wybranych dziedzin życia publicznego brak zapisów dotyczących aspektu technicznego.

4.4.2. Wyniki analizy aktów normatywnych

Zaleca się, aby dostęp logiczny do informacji i oprogramowania komputerowego był zastrzeżony wyłącznie dla uprawnionych użytkowników. Trzeba zapewnić, aby systemy aplikacji:

- Kontrolowały dostęp użytkowników do informacji i funkcji systemu aplikacji, zgodnie ze zdefiniowaną polityką kontroli dostępu uwzględniającą cele działalności biznesowej,
- Chroniły przed nieuprawnionym dostępem do jakiegokolwiek oprogramowania narzędziowego lub systemowego, które umożliwiałoby obejście zabezpieczeń w systemie lub aplikacji,
- Uniemożliwiały naruszenie bezpieczeństwa innych systemów, z którymi są współużytkowane zasoby informacyjne,
- Umożliwiały dostęp do informacji jedynie jej właścicielowi, innym wyznaczonym osobom lub zdefiniowanym grupom użytkowników.

Zaleca się zapewnianie, że dane wyjściowe z systemów aplikacji przetwarzających informacje wrażliwe *[pojęcie „informacje/dane wrażliwe" jest używane tutaj i w dalszym części niniejszego rozdziału w znaczeniu „informacje/dane wymagające ochrony" (zarówno na podstawie ustaw i aktów wykonawczych jak i na podstawie regulacji wewnętrznych instytucji/jednostki organizacyjnej)]* zawierają jedynie informacje przewidywane do dalszego użycia oraz, że są one wysyłane tylko do uprawnionych terminali lub miejsc, włączając w to okresowe przeglądy danych wyjściowych, tak aby zapewnić, że nadmiarowe informacje są usuwane.

Systemy wrażliwe mogą wymagać dedykowanego (izolowanego) środowiska przetwarzania. Trzeba brać pod uwagę niżej podane zagadnienia.

- Zaleca się, aby właściciel aplikacji jasno określił i udokumentował wrażliwość systemu aplikacji.

- Jeżeli aplikacja wrażliwa ma być uruchomiona we wspólnym środowisku, to zaleca się określenie i uzgodnienie z jej właścicielem tych systemów aplikacji, z którymi aktywa będą współużytkowane.

4.5. Aspekty ekonomiczne

W przeanalizowanych ustawach i aktach wykonawczych do nich (uwaga ta dotyczy wszystkich aktów prawnych, o których mowa w niniejszym rozdziale) oraz w aktach normatywnych brak zapisów bezpośrednio odnoszących się do aspektów ekonomicznych. Ale: na ekonomiczny wyraz przetwarzania informacji o różnych wartościach miar poufności (klauzulach tajności) wpływ mają pozostałe aspekty dziedzinowe, a więc organizacyjno-prawny i techniczny. Stąd, najważniejsze składniki kosztów to stanowienie, wdrażanie i kontrola regulacji prawnych, urządzenia i technologie, struktury organizacyjne i tryby postępowania w odniesieniu do poszczególnych elementów systemów informatycznych i procesów przez nie realizowanych – wszystkie zalecenia dotyczące tych składników mają swój wymiar ekonomiczny.

4.6. Uogólnienie wniosków z przeprowadzonej analizy

Na podstawie przedstawionych powyżej wyników z analizy aktów prawnych i normatywnych można sformułować poniższe wnioski ogólne.

- W aktach ustawowych najwyższej rangi nie definiuje się pojęcia bezpieczeństwa informacji (informacyjnego, systemów informatycznych, teleinformatycznego); pośrednie odwołanie do zewnętrznego źródła takiej definicji występuje w ustawie o informatyzacji działalności podmiotów realizujących zadania publiczne (cyt.: "art. 18. (...) z uwzględnieniem Polskich Norm oraz innych dokumentów normalizacyjnych zatwierdzonych przez krajową jednostkę normalizacyjną"); odwołania się do poufności, integralności i dostępności występują tylko w niektórych rozporządzeniach ministra spraw wewnętrznych i administracji, natomiast definicji tych pojęć nie ma w żadnym z analizowanych dokumentów; oznacza to, że definicja zalecana przez podstawową normę PN-ISO/IEC 17799 nie jest wprost używana w żadnym z dokumentów prawnych rangi ustawowej.

[Przywołana powyżej definicja bezpieczeństwa informacji z normy PN-ISO/IEC 17799 ma postać następującą:

Bezpieczeństwo informacji oznacza zachowanie poufności, integralności i dostępności informacji, gdzie:

- poufność jest zdefiniowana jako zapewnienie, że informacja jest dostępna tylko osobom upoważnionym,
- integralność jest zdefiniowana jako zapewnienie dokładności i kompletności informacji oraz metod jej przetwarzania,
- dostępność jest zdefiniowana jako zapewnienie, że osoby upoważnione mają dostęp do informacji i związanych z nią aktywów wtedy, gdy jest to potrzebne.]

- Normy lub raporty techniczne opracowywane przez komitety międzynarodowe nie mogą automatycznie ani zastąpić ani zdominować różniących się krajowych rozwiązań prawnych. Zasada ta obowiązuje w całości w stosunku do prawodawstwa polskiego. Dlatego są one zbiorami bardzo mocno uzasadnionych zaleceń, a nie wymagań do bezwzględnego przestrzegania. Jednakże – zdaniem autorów książki – podstawy metodologiczne analizowanych aktów normatywnych są poprawniejsze niż aktów prawnych poddanych analizie, np. w normie PN-I-07779-2 system zarządzania bezpieczeństwem informacji jest definiowany jako część całego systemu zarządzania, decyzje dotyczące bezpieczeństwa teleinformatycznego zaleca się podejmować w kontekście potrzeb biznesowych instytucji. Dlatego też postulujemy wykorzystanie norm zarządzania bezpieczeństwem informacyjnego jako platformy integracji regulacji zawartych w ustawach z zakresu bezpieczeństwa teleinformatycznego.
- Tak w aktach prawnych jak w aktach normatywnych brak ogólnych regulacji/zasad określających klauzule tajności informacji będącej wynikiem przetwarzania informacji wejściowych o różnych klauzulach tajności.
- Przeanalizowane akty prawne odnośnie dwóch wybranych rejestrów publicznych (KRS, TERYT) zawierają zapisy odnośnie kwestii poufności danych w nich gromadzonych i przetwarzanych, określając je jako jawne. Odnośnie rejestru PESEL ustawodawca i minister właściwy ds. administracji publicznej nie byli konsekwentni – określili co prawda dane jako „dane osobowe", ale nie wskazali ustawy o ochronie danych osobowych jako podstawy prawnej ochrony danych w tym rejestrze. Dodatkowo – jak pokazano rozdz.10, dla systemu PESEL, na podstawie decyzji organizacyjnej, bazie danych nadano klauzulę „poufne", zaś pojedynczym rekordom – klauzulę „zastrzeżone".
- Ani w aktach prawnych ani w aktach normatywnych nie definiuje się czy też odwołuje się do pojęcia „interoperacyjności". Podkreślić jednak należy, iż aspekty organizacyjny, techniczny i informacyjny interoperacyjności są ważnymi wątkami zapisów ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne i jej aktów wykonawczych.

5. Model przetwarzania informacji ze źródeł informacji o różnych klauzulach tajności

5.1. Model systemu bezpieczeństwa

Punktem wyjścia do definiowania modelu przetwarzania informacji pochodzących ze źródeł o różnych klauzulach tajności były modele bezpieczeństwa systemów informatycznych, ponieważ cecha przetwarzanych informacji (posiadanie klauzul tajności) wymagała skupienia się w modelu na zagadnieniu poufności, czyli jednego z głównych składników bezpieczeństwa [PN-OSO/IEC-17799, PN-I-13335-1], w tym przypadku bezpieczeństwa teleinformatycznego.

Po analizie znacznej liczby podejść do modelowania problemów bezpieczeństwa za reprezentatywny model bezpieczeństwa przyjęliśmy model opracowany przez Clementsa [19].

W wyżej wskazanej publikacji system bezpieczeństwa jest definiowany jako uporządkowana piątka:

S = (O, Z, B, R, P)

gdzie:

O = {o[1], o[2], ... ,o[m]} – zbiór obiektów podlegających zagrożeniu,

Z = {z[1], z[2], ... ,z[n]} – zbiór zagrożeń,

B = {b[1], b[2], ... , b[p]} – zbiór środków bezpieczeństwa,

$\mathbf{R} \subset \mathbf{Z} \times \mathbf{O}$ – zbiór ścieżek penetracji,

$\mathbf{P} \subset \mathbf{Z} \times \mathbf{B} \times \mathbf{O}$ – zbiór ścieżek penetracji chronionych środkami bezpieczeństwa.

Model Clementsa wprowadza język do analizy procesów zabezpieczania określonych obiektów (ze zbioru **O**) podlegających określonym zagrożeniom (ze zbioru **Z**) przy pomocy określonych środków bezpieczeństwa (ze zbioru **B**).

Dziedziną, w której model może znaleźć zastosowanie jest analiza różnych aspektów bezpieczeństwa systemów informatycznych. Może być użyteczny, po odpowiednim rozwinięciu, rozszerzeniu (np. o miary wartości obiektów podlegających ochronie oraz o miary skuteczności środków bezpieczeństwa) dla tworzenia podstaw metodologicznych prowadzenia analiz ryzyka oraz projektowania systemów bezpieczeństwa. Założone w ni-

niejszej publikacji cele były nieco inne. Wynika z nich, że w procesach modelowania powinniśmy koncentrować się na zagadnieniach poufności w powiązaniu z zapewnianiem interoperacyjności systemów informatycznych wspierających procesy realizacji zadań publicznych. Z tego względu wyżej zaprezentowany model nie jest wystarczający i dlatego dalej, po sformułowaniu stosownych założeń, przedstawiono własny model.

5.2. Założenia modelu

- Model przetwarzania informacji ma wprowadzić takie kategorie pojęciowe oraz relacje między nimi, aby zapewnić możliwość prowadzenia analiz procesów realizowanych w systemach informatycznych administracji publicznej pod kątem bezpieczeństwa w powiązaniu z interoperacyjnością systemów informatycznych.
- Mając pełną świadomość, że bezpieczeństwo informacji (informacyjne) zgodnie z przyjętą definicją [PN-OSO/IEC-17799, PN-I-13335-1] obejmuje swym zakresem cechy poufności, integralności i dostępności – rozważania w niniejszej publikacji ograniczono do problemów poufności z uwzględnieniem ich wpływu na interoperacyjność.
- Model przetwarzania powinien należeć do klasy modeli identyfikacyjnych. Oznacza to, że powinien służyć wyodrębnieniu niezbędnych kategorii pojęciowych, a nie formułowaniu normatywnych wymagań.
- Zasadniczą rolę w modelu odgrywa pojęcie informacji, przy czym traktujemy je jako pojęcie pierwotne. W miejscach, gdzie to jest konieczne dla lepszego zrozumienia prowadzonych rozważań, rozumienie informacji w modelu zostanie dodatkowo objaśnione.
- W modelu należy wyróżnić abstrakcyjną przestrzeń poufności. W szczególności do tej przestrzeni należą płaszczyzny postępowania z informacjami ustawowo (prawnie) chronionymi, np. informacjami niejawnymi (w literaturze najczęściej klasyfikacja tych informacji jest dokonywana na podstawie oceny skutków utraty poufności), informacjami osobowymi (w literaturze najczęściej: informacje prawnie chronione ze względu na przedmiot ochrony) i informacjami branżowymi (w literaturze najczęściej: informacje chronione ze względu właściciela informacji). Istota regulacji dotyczących informacji niejawnych lepiej jest widoczna na tle innych punktów widzenia na poufność informacji. Szczegółowa i pełna klasyfikacja możliwych płaszczyzn poufności wykracza poza ramy niniejszej publikacji. Jednakże dla ilustracji tego pojęcia można wyodrębnić m.in. następujące rodzaje płaszczyzn poufności:
  - Ogólne – objęte ogólnokrajowymi regulacjami prawnymi:
    a) Ochrona informacji niejawnych,
    b) Ochrona danych osobowych.
  - Branżowe – objęte ogólnokrajowymi branżowymi regulacjami prawnymi. Przykłady:
    a) Ochrona informacji handlowych (patrz: Kodeks Handlowy),
    b) Ochrona informacji bankowych (patrz: Prawo Bankowe),

c) Ochrona informacji statystycznej (patrz: Ustawa o statystyce publicznej).

– **Inne** – lokalnego znaczenia, bez ogólnokrajowych regulacji prawnych. Obowiązek ochrony informacji może wynikać z wymagań narzuconych przez organy kierownicze firm i instytucji.

Przykłady:

a) Ochrona określonych informacji gospodarczych,
b) Ochrona informacji z posiedzeń i obrad organów i ciał kolegialnych,
c) Ochrona informacji na temat przebiegu głosowań.

- Poufność informacji powinna być postrzegana w kontekście dwóch rodzajów polityk bezpieczeństwa: polityki nakazowej i polityki uszczelniającej. Polityka nakazowa wynika bezpośrednio z wymagań ustawowych obowiązujących daną organizację w zakresie zapewniania bezpieczeństwa informacji. Polityka uszczelniająca odzwierciedla dodatkowe (ponadustawowe) wymagania wprowadzone uznaniowymi decyzjami kierownictw konkretnych organizacji.

Powyższe założenia wymagają odmiennego modelu niż cytowany wcześniej model systemu bezpieczeństwa, ponieważ potrzebne są modelowe elementy pozwalające analizować relacje pomiędzy poufnością informacji a interoperacyjnością systemów informatycznych przetwarzających takie informacje.

5.3. Sformułowanie modelu

System przetwarzania informacji zdefiniujemy jako uporządkowaną siódemkę:

S P I = (I, P, M, F, Z, W, B)

gdzie:

I = {i[1], i[2], … ,i[I]} – zbiór informacji;

P = P [1] × P [2] × … × P [n] × … × P [P] – P-wymiarowa przestrzeń poufności, gdzie dla n = 1, 2, … , P:

P [n] = [0,1] – zbiór wartości miary poufności p-tego wymiaru (inaczej: płaszczyzny poufności);

M = (ME, MZ)

M – uporządkowana para, gdzie:

ME : I → P – funkcja przyporządkowująca każdej informacji wartości miar poufności w P-wymiarowej przestrzeni poufności,

MZ : 2^I → P – funkcja przyporządkowująca każdemu podzbiorowi zbioru informacji I wartości miar poufności w P-wymiarowej przestrzeni poufności;

F – funkcja częściowa definiująca algorytmy przetwarzania zbiorów informacji wejściowych w zbiory informacji wyjściowych:

F : 2^I → 2^I

System informatyczny o określonej funkcjonalności może zrealizować niektóre z tych algorytmów przetwarzania. Tworzą one zbiór realizowalnych operacji przetwarzania informacji O.

O = {o[1], o[2], ... , o[n], ... , o[O]} – zbiór realizowalnych w systemie operacji przetwarzania informacji,

gdzie dla n = 1, 2, ... , O:

o[n] = (Iwe [n], Iwy [n])

Iwe [n], Iwy [n] $\in 2^I$

Iwy [n] = F (Iwe [n])

Zbiór O jest zbiorem uporządkowanych par podzbiorów zbioru I informacji, gdzie pierwszy element pary jest zbiorem informacji wejściowych operacji Iwe [n], a drugi element pary jest zbiorem informacji wyjściowych (czyli wynikowych) operacji Iwy [n]. Zbiór wyjściowy jest definiowany przez funkcję F , argumentem jest Iwe [n].

Z = {z[1], z[2], ... , z[m], ... ,z[Z]} – zbiór zadań użytkowych systemu informatycznego.

System informatyczny posiada funkcjonalność umożliwiającą realizację zadań ze zbioru Z , jeżeli dla każdego zadania z[m] dla m = 1, 2, ... , Z, istnieje ciąg realizowalnych w systemie operacji ze zbioru O :

o[n[m,1]], o[n[m,2]], ... , o[n[m,k]], ... , o[n[m,K[m]]],

który jest równoważny realizacji zadania.

W = {w[1], w[2], ... , w[n], ... ,w[W]} – zbiór wymagań na bezpieczeństwo systemu informatycznego.

B = (Bn, Bu) – polityka bezpieczeństwa informacyjnego, odpowiednio:

Bn – polityka bezpieczeństwa nakazowa,

Bu – polityka bezpieczeństwa uszczelniająca.

B = (Bn, Bu) – uporządkowana para, gdzie:

Bn : $2^Z \rightarrow 2^W$ – funkcja przyporządkowująca zbiorowi zadań realizowanych przez system informatyczny zbiór wymagań na bezpieczeństwo systemu informatycznego wynikających z nakazowej polityki bezpieczeństwa,

Bu : $2^Z \rightarrow 2^W$ – funkcja przyporządkowująca zbiorowi zadań realizowanych przez system informatyczny zbiór wymagań na bezpieczeństwo systemu informatycznego wynikających z uszczelniającej polityki bezpieczeństwa;

W rezultacie dla ustalonego systemu informatycznego o funkcjonalności, która zapewnia realizację określonych zadań użytkowych, funkcja B definiuje wymagania wynikające z polityki nakazowej Wn , oraz wymagania wynikające z polityki uszczelniającej Wu , gdzie:

$Wn \subset W$,

$Wu \subset W$,

$Wn \cup Wu \subset W$.

5.4. Opis i dyskusja modelu

5.4.1. Informacja, poufność informacji

5.4.1.1. Informacja i zbiory informacji

U podstaw rozważań zagadnień dotyczących procesów przetwarzania w systemach informatycznych leży pojęcie **informacji**. Przetwarzaniu poddane są informacje wejściowe, w wyniku przetwarzania uzyskuje się informacje wyjściowe. W zależności od kontekstu rozpatrywania, informacje wejściowe nazywane są także źródłowymi, pierwotnymi bądź początkowymi. Odpowiednio, informacje wyjściowe nazywane są wynikowymi, pochodnymi, rzadziej udostępnianymi bądź użytkowymi.

Zbiór informacji, które mają być traktowane jako elementarne a które będą rozpatrywane w danym modelu przetwarzania informacji opracowywanym w procesie projektowania systemu informatycznego, zależny jest od celu tego systemu. W jednym przypadku zawartość zbioru informacji definiowana jest w jeden sposób, w innym przypadku w inny. W systemach informatycznych informacja jest reprezentowana przez uporządkowany układ danych. I tak przykładowo:

- informacja o obiekcie: (identyfikator obiektu, cechy obiektu),
- informacja o relacji pomiędzy obiektami: (identyfikator relacji, identyfikatory obiektów powiązanych),
- informacja o zdarzeniu: (identyfikator zdarzenia, opisy zdarzenia, data),
- informacja o stanie procesu: (identyfikator procesu, stany procesu).

Na rysunku 5-1 zaprezentowano przykładową strukturę danych. Struktura ta została przeanalizowana pod kątem jej wewnętrznych związków.

W niniejszej publikacji pojęcie informacji uznano za pierwotne i dlatego nie przedstawiamy pogłębionych rozważań dotyczących istoty rozumienia informacji. Warto jednak wskazać, że w literaturze przedmiotu obserwuje się dwa podejścia do tego problemu.

Pierwsze pochodzi od klasycznej teorii informacji, w której wiadomość staje się informacją tylko wtedy, gdy zmniejsza entropię (wzbogaca wiedzę) odbiorcy na temat opisywanego przez nią zdarzenia, podmiotu (przedmiotu), faktu czy zjawiska. Z punktu widzenia potrzeb modelowania takich obiektów, jak strumienie informacyjne, procesy przetwarzania informacji czy systemy informacyjne, największą trudność sprawia właśnie to, że znaczenie informacji ma charakter uznaniowy i w ogólnym przypadku jest różne dla różnych odbiorców.

Drugie podejście, które można nazwać technologicznym, bo wywodzi się z praktyki projektowania baz danych, wprowadza bardziej praktyczne pojmowanie informacji. W tym przypadku przez informację rozumie się po prostu zinterpretowane dane, czyli dane, którym nadano określone znaczenie. Warto podkreślić, że dobre praktyki modelowania zakładają obiektywny wyraz i niezależność budowanych modeli od subiektywnego punktu widzenia.

5.4.1.2. Poufność informacji

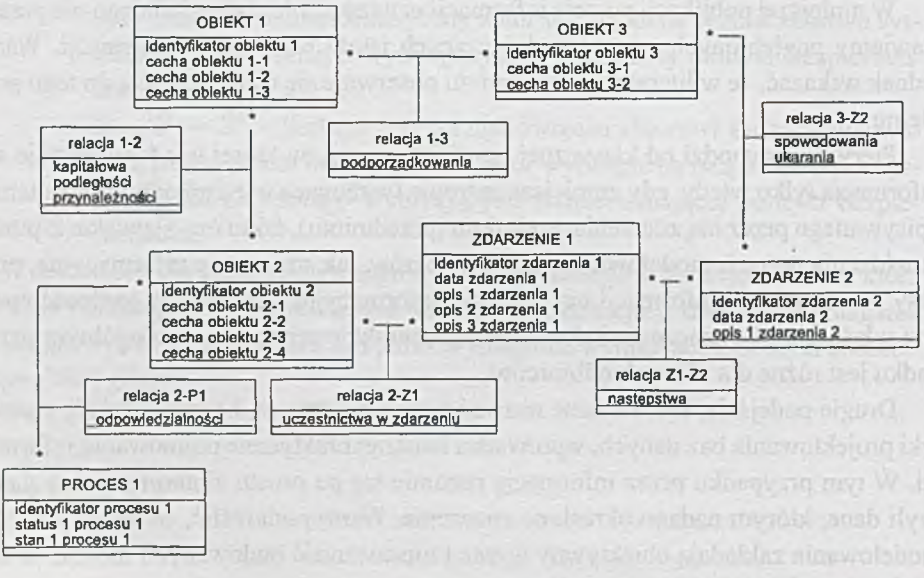
Poufność informacji może być rozważana w różnych płaszczyznach (wymiarach). W stosunku do niektórych z tych płaszczyzn istnieją regulacje prawne, które nakazują odpowiednie postępowanie z określonymi informacjami.

Informacja rozważana w każdej z tych płaszczyzn poufności może posiadać cechę poufności od minimalnej do maksymalnej. Załóżmy, że w każdej z tych płaszczyzn (wymiarów) poufności mamy uporządkowaną i unormowaną miarę o wartościach z przedziału od 0 do 1. Wartość '0' oznacza, że informacja w tej płaszczyźnie jest pozbawiona w jakimkolwiek stopniu cech poufności, natomiast wartość '1' oznacza maksymalny stopień poufności. Dla płaszczyzn poufności, do których odnoszą się regulacje prawne wprowadzane są dyskretne miary poufności. W powyższym opisie założono wzajemną niezależność miar poufności poszczególnych płaszczyzn (wymiarów). Innymi słowy stanowią one niezależne kryteria oceny.

Nasuwa się pytanie co decyduje o nadaniu wartości miar poufności w poszczególnych płaszczyznach poufności? Decydujące znaczenie ma semantyka informacji oraz kontekst (związki semantyczne) jej występowania.

Właściwość, że o wartości miar poufności informacji
(czyli w formalnym języku modelu S P I o funkcji ME : I → P)
decyduje jej semantyka, stanowi ważną cechę procesu przetwarzania w systemach informatycznych o zróżnicowanych klauzulach poufności.

Rozważmy pokrótce przykładową strukturę danych przedstawioną w postaci diagramu klas na rysunku 5-1.



Rysunek 5-1. Przykład wzajemnie powiązanych informacji

Jest rzeczą zrozumiałą, że w zależności od konkretnego znaczenia cech obiektów informacja może być w określonym stopniu poufna. Dla ilustracji przeanalizujmy kilka przykładów:

Przykład 1): PROCES 1 – to prowadzone śledztwo prokuratorskie. Już informacja o jego statusie i stanie może wymagać zachowania poufności.

Przykład 2): „Cecha obiektu 1-2" dla OBIEKTU 1 – to wyznanie pracownika. Wymaga poufności.

Przykład 3): Załóżmy, że wszystkie cechy OBIEKTU 3 oraz opisy ZDARZENIA 2 nie powodują traktowania ich jako poufne. Taką konieczność wywołuje „relacja 3-Z2", która zawiera informację o **ukaraniu** osoby (OBIEKTU 3) w wyniku zdarzenia (ZDARZENIA 2).

Przykłady ilustrują tezę, że dla prawidłowego określenia wartości miar poufności, konieczne jest rozpoznanie semantyki informacji. W niektórych przypadkach (ilustruje to przykład 3) wymaga to rozpoznania struktury powiązań danych.

5.4.1.3. Poufność zbiorów informacji

W systemach informatycznych przetwarzane są zarówno pojedyncze informacje, jak i zbiory informacji pojedynczych. Charakterystyki zbioru informacji są zależne od właściwości informacji wchodzących w jego skład.

W praktyce często stosowana jest reguła, na podstawie której nadaje się zbiorowi miar poufności wartości równe lub wyższe od maksymalnej miary informacji wchodzących w jej skład. Do tej pory nie dopracowano się reguł, na podstawie których mogłyby być automatycznie generowane „wypadkowe wartości miar poufności" wg innej, jak wyżej sformułowana zasada.

Właściwość, że nie istnieją ogólnie przyjęte i stosowane reguły, według których określane byłyby wypadkowe wartości miar poufności zbiorów na podstawie wartości miar należących do nich informacji, według innego schematu niż zasada maksymalizacji, stanowi ważną cechę procesu przetwarzania w systemach informatycznych o zróżnicowanych klauzulach poufności.

W formalnym języku modelu S P I:

stosowana jest obecnie reguła, na podstawie której funkcja $MZ : 2^I \rightarrow P$ określana jest na podstawie funkcji $ME : I \rightarrow P$ następująco:

Dla każdego wymiaru przestrzeni poufności $p = 1, 2, \ldots, P$ wartość p-tej miary poufności dowolnego zbioru $A = \{a[1], a[2], \ldots, a[K]\}$, który jest podzbiorem rodziny 2I wyznaczona jest jako:

$\max\{ ME(a[1]), ME(a[2]), \ldots, ME(a[K])\}$.

Podkreślmy tutaj, że informację należy rozpatrywać z punktu widzenia konkretnej osoby. Wiedza, jaką dana osoba posiada, wpływa na stopień zrozumienia jej znaczenia. Dotyczy to oczywiście także szczególnego aspektu semantyki informacji, mianowicie jej poufności. Przykładowo: wiedza, że system utrzymuje rejestr skazanych pozwala

już na podstawie odczytania identyfikatora osoby formułować hipotezę o jej prawdopodobnej karalności. Najczęściej, zarówno w modelowaniu teoretycznym, jak i w praktyce, pomijana jest zależność zagrożenia bezpieczeństwa informacyjnego od wiedzy wstępnej podmiotu uzyskującego informację.

5.4.1.4. Procesy przetwarzania informacji

W systemach informatycznych informacje źródłowe podlegają procesom przetwarzania. Powstają zbiory informacji, w skład których wchodzą informacje wyjściowe (częściej nazywane informacjami wynikowymi) o innej semantyce niż informacje wejściowe (czyli źródłowe lub pierwotne), które były pozyskane na wejściu systemów. Intuicja podpowiada jednak, że semantyka informacji wynikowych musi być skorelowana z semantyką informacji wejściowych (źródłowych). Innymi słowy, na podstawie cech informacji, które były podstawą znanej sekwencji przetwarzania, można określać cechy informacji wynikowych – choć zależność ta jest często złożona.

W modelu S P I procesy przetwarzania to ciągi operacji ze zbioru O . Także zadania użytkowe realizowane przez system informatyczny, to takie ciągi tych operacji, które są równoważne postawionym zadaniom. Z kolei, zbiór O jest zbiorem uporządkowanych par podzbiorów zbioru I informacji, gdzie pierwszy element pary jest zbiorem informacji wejściowych operacji Iwe [n], a drugi element pary jest zbiorem informacji wyjściowych (czyli wynikowych) operacji Iwy [n]. Zbiór wyjściowy jest definiowany przez funkcję F , która definiuje algorytmy obliczeniowe.

5.4.1.5. Poufność informacji przetworzonych

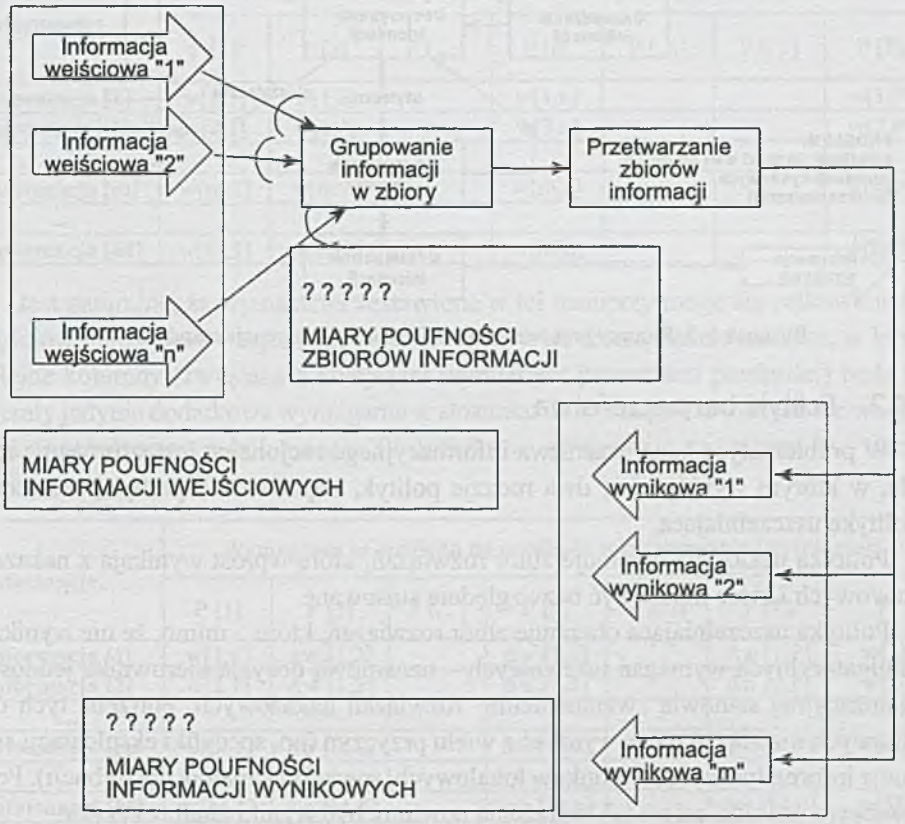
Nie istnieją jednoznaczne reguły pozwalające nadawać wartości miar poufności zbiorom informacji powstałym w wyniku realizacji określonych procesów przetwarzania informacji na podstawie miar poufności informacji wejściowych.

Właściwość, że nie istnieją jednoznaczne reguły, według których określane byłyby wartości miar poufności informacji wynikowych na podstawie wartości miar informacji wejściowej z uwzględnieniem jakim je poddano procesom przetwarzania stanowi ważną cechę procesu przetwarzania w systemach informatycznych o zróżnicowanych klauzulach poufności. Za poszukiwane rozwiązanie nie można uznać reguły – stosowanej czasem w praktyce – nadawania klauzuli według najwyższej klauzuli posiadanej przez informacje wejściowe.

W formalnym języku modelu S P I tę właściwość zapisać należy jako: nie ma reguł, na podstawie których można by określać dla każdej operacji o[n] $\in$ O wartości miar poufności MZ (Iwy [n]) na podstawie znajomości wartości miar poufności MZ (Iwe [n]). Natomiast natura zależności w ujęciu modelowym jest taka, że powinien istnieć jednoznaczny przepis określający wartości miar poufności informacji wynikowych, zbudowany na podstawie funkcji F oraz funkcji MZ.

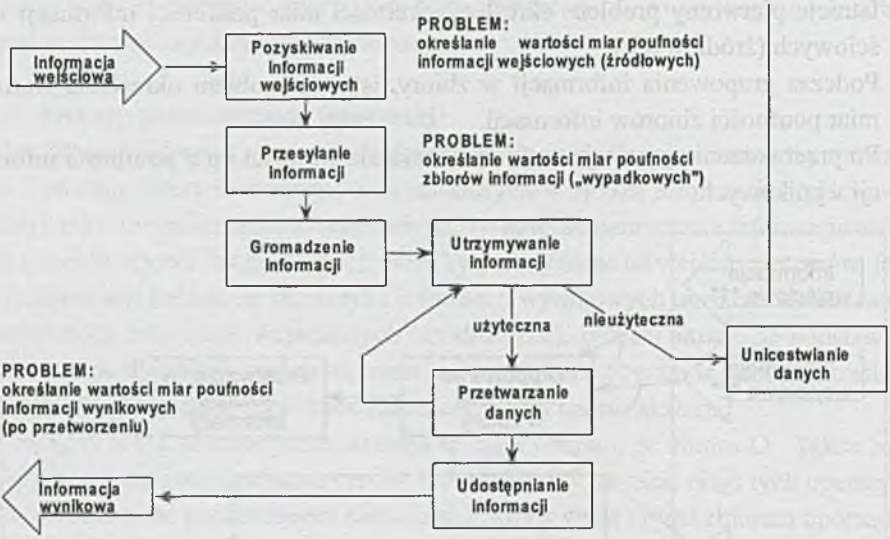
Diagram na rysunku 5-2 podsumowuje, pod kątem zagadnienia określania poufności, przebieg każdego przedsięwzięcia związanego z przetwarzaniem informacji:

- Istnieje pierwotny problem określenia wartości miar poufności informacji wejściowych (źródłowych).
- Podczas grupowania informacji w zbiory, istnieje problem określenia wartości miar poufności zbiorów informacji.
- Po przetworzeniu powstaje problem określenia wartości miar poufności informacji wynikowych.



Rysunek 5-2. Procesy przekształcania informacji w kontekście ich poufności

Diagram na rysunku 5-3 obrazuje typową (standardową) sekwencję procesów od pozyskania informacji źródłowej do udostępnienia informacji wynikowych bądź unicestwienia danych reprezentujących te informacje. Zaznaczono na nim obszary gdzie dominują problemy dotyczące określania wartości miar poufności.



Rysunek 5-3. Procesy przetwarzania informacji – sekwencja standardowa

5.4.2. Polityki bezpieczeństwa

W problematyce bezpieczeństwa informacyjnego racjonalne jest stosowanie modelu, w którym wyróżnia się dwa rodzaje polityk, odpowiednio politykę nakazową i politykę uszczelniającą.

Polityka nakazowa obejmuje zbiór rozwiązań, które wprost wynikają z nakazów ustawowych i które muszą być bezwzględnie stosowane.

Polityka uszczelniająca obejmuje zbiór rozwiązań, które – mimo, że nie wynikają z obligatoryjnych wymagań ustawowych – uznaniową decyzją kierownika jednostki organizacyjnej stanowią „wzmocnienie" rozwiązań nakazowych. Potrzeba tych dodatkowych rozwiązań może wynikać z wielu przyczyn (np. specyfiki eksploatacji systemów informatycznych, warunków lokalowych, specyfiki kanałów dystrybucji). Podstawowym uzasadnieniem ich wdrażania powinny być wyniki analizy ryzyka.

W formalnym języku modelu S P I, polityka nakazowa reprezentowana jest przez funkcję Bn , która definiuje podzbiór wymagań $Wn \subset W$, w którym wszystkie wymagania $w[n] \in Wn$ wynikają bezpośrednio z obowiązujących ustaw. Polityka uszczelniająca zaś, reprezentowana jest przez funkcję Bu , która definiuje podzbiór wymagań $Wu \subset W$. Jeżeli podzbiór $Wu \subset Wn$, polityka uszczelniająca nie ma zastosowania.

5.4.3. Zróżnicowana struktura poufności zbiorów informacji

Przed systemem informatycznym przetwarzającym informacje o różnych wartościach miar poufności postawione są wymagania wynikające z przyjętej polityki bezpieczeństwa

– nakazowej w części obligatoryjnej, oraz uszczelniającej w części wynikającej z własnej analizy ryzyka. Tryb określania tych wymagań możemy scharakteryzować jako sekwencję ustaleń zaczynających się od precyzowania wymagań związanych z jednym z wymiarów P-wymiarowej przestrzeni poufności. Schematycznie możemy wszystkie te wymagania przedstawić zbiorczo w strukturze macierzy (P × M)-wymiarowej, gdzie P – liczba uwzględnianych wymiarów przestrzeni poufności, M – liczba wyodrębnionych informacji.

Informacje:	Wymagania ze względu na poufność w płaszczyźnie (wymiarze):						
	P [1]	P [2]	P [...]	P [n]	P [...]	P [...]	P [P]
Informacja [1]	w[1,1]	w[1,2]		w[1,n]			w[1,P]
Informacja [2]	w[2,1]	w[2,2]		w[2,n]			w[2,P]
...							
Informacja [m]	w[m,1]	w[m,2]		w[m,n]			w[m,P]
...							
Informacja [M]	w[M,1]	w[M,2]		w[M,n]			w[M,P]

Jest naturalne, że wymagania zestawione w tej macierzy mogą się całkowicie lub częściowo pokrywać wzajemnie. Wygodniejszą więc formą będzie macierz, w której kolejne kolumny (związane z kolejnymi wymiarami przestrzeni poufności) będą zawierały jedynie dodatkowe wymagania w stosunku do wymagań zawartych we wszystkich poprzedzających kolumnach. Te dodatkowe wymagania nazwiemy Δw. Otrzymujemy w ten sposób macierz:

Informacje:	Wymagania ze względu na poufność w płaszczyźnie (wymiarze):						
	P [1]	P [2]	P [...]	P [n]	P [...]	P [P]	P
Informacja [1]	w[1,1]	Δw [1,2]		Δw [1,n]		Δw [1,P]	**w[1]**
Informacja [2]	w[2,1]	Δw [2,2]		Δw [2,n]		Δw [2,P]	**w[2]**
...							
Informacja [m]	w[m,1]	Δw [m,2]		Δw [m,n]		Δw [m,P]	**w[m]**
...							
Informacja [M]	w[M,1]	Δw [M,2]		Δw [M,n]		Δw [M,P]	**w[M]**

W ostatniej kolumnie zestawione są wynikowe, zbiorcze wymagania odnoszące się do poszczególnych informacji.

Powyższy schemat postępowania przy określaniu wymagań na bezpieczeństwo systemu informatycznego zilustrujemy poniżej na przykładzie, w którym przestrzeń poufności jest czterowymiarowa. Wymiary (płaszczyzny) poufności wyróżnione są ze względu na ochronę:

- Informacji niejawnych.
- Danych osobowych.
- Informacji handlowych.
- Informacji organizacyjnych wewnętrznych.

Informacje:	Wymagania na bezpieczeństwo SI ze względu na ochronę informacji:			
	Niejawnych	Osobowych	Handlowych	Wewnętrznych
Informacja [1]	w[1,N]	w[1,O]	w[1,H]	w[1,W]
Informacja [2]	w[2,N]	w[2,O]	w[2,H]	w[2,W]
...				
Informacja [m]	w[m,N]	w[m,O]	w[m,H]	w[m,W]
...				
Informacja [M]	w[M,N]	w[M,O]	w[M,H]	w[M,W]

Odpowiednio druga macierz, która określa „przyrost" wymagań Δw ze względu na dany rodzaj ochrony w stosunku do wymagań już uwzględnionych przyjmuje postać:

Informacje:	Wymagania na bezpieczeństwo SI ze względu na ochronę informacji:			
	Niejawnych	Osobowych	Handlowych	Wewnętrznych
Informacja [1]	w[1,N]	Δw [1,O]	Δw [1,H]	Δw [1,W]
Informacja [2]	w[2,N]	Δw [2,O]	Δw [2,H]	Δw [2,W]
...				
Informacja [m]	w[m,N]	Δw [m,O]	Δw [m,H]	Δw [m,W]
...				
Informacja [M]	w[M,N]	Δw [M,O]	Δw [M,H]	Δw [M,W]

Dla zapewnienia bezpieczeństwa systemu informatycznego we wszystkich uwzględnianych aspektach konieczne jest spełnienie wymagań, które łącznie je charakteryzują:

Informacje:	Łączne wymagania na bezpieczeństwo SI:
Informacja [1]	w[1]
Informacja [2]	w[2]
...	
Informacja [m]	w[m]
...	
Informacja [M]	w[M]

5.4.4. Funkcjonalność systemów informatycznych w kontekście poufności. Interoperacyjność przetwarzania informacji

W konwencji wprowadzonego modelu przetwarzania informacji S P I , funkcjonalność systemu informatycznego reprezentowana jest przez zbiór Z = {z[1], z[2], ..., z[m], ... ,z[Z]}. Przywołajmy sformułowane tam określenie:

„System informatyczny posiada funkcjonalność umożliwiającą realizację zadań ze zbioru Z , jeżeli dla każdego zadania z[m] dla m = 1, 2, ... , Z, istnieje ciąg realizowalnych w systemie operacji ze zbioru O:

o[n[m,1]], o[n[m,2]], ... , o[n[m,k]], ... , o[n[m,K[m]]],

który jest równoważny realizacji zadania".

Przy rozpatrywaniu interoperacyjności systemów informatycznych realizujących zadania publiczne, od poszczególnych systemów oczekuje się realizacji określonego zbioru zadań Z. Można to ująć następująco: zadania publiczne generują dla uczestniczących w ich realizacji systemów informatycznych wymaganą funkcjonalność.

Z drugiej strony, od zawartości zbioru zadań zależą wymagania na bezpieczeństwo systemu informatycznego. Według sformułowań zawartych w modelu S P I :

„Dla ustalonego systemu informatycznego o funkcjonalności, która zapewnia realizację określonych zadań użytkowych Z, funkcja B definiuje wymagania wynikające z polityki nakazowej Wn, oraz wymagania wynikające z polityki uszczelniającej Wu".

Wymagania odnoszą się do poszczególnych rozwiązań i elementów systemu informatycznego oraz procedur i trybu postępowania w trakcie realizacji zadań. Mogą mieć charakter bądź techniczno-technologiczny bądź organizacyjny. Zapewnienie interoperacyjności systemów informatycznych uczestniczących w realizacji zadań publicznych (reprezentowanej przez zbiory możliwych przez nie do realizacji zadań Z) jest w pewnym konflikcie z zapewnieniem bezpieczeństwa informacyjnego (reprezentowanym w modelu przez zbiory wymagań W).

Zwróćmy jeszcze uwagę na pewien istotny praktyczny aspekt procesu przetwarzania informacji, a mianowicie zagadnienie zapewnienia interoperacyjności już w trakcie określania wartości miar poufności przetwarzanych informacji.

Po pierwsze w trakcie grupowania informacji powstają zbiory informacji. Interoperacyjność poprawi się, gdy zasady wartościowania miar poufności zbioru informacji w oparciu o wartości miar poufności informacji składowych będą sformalizowane w takim stopniu, że dadzą się w jakimś stopniu zautomatyzować.

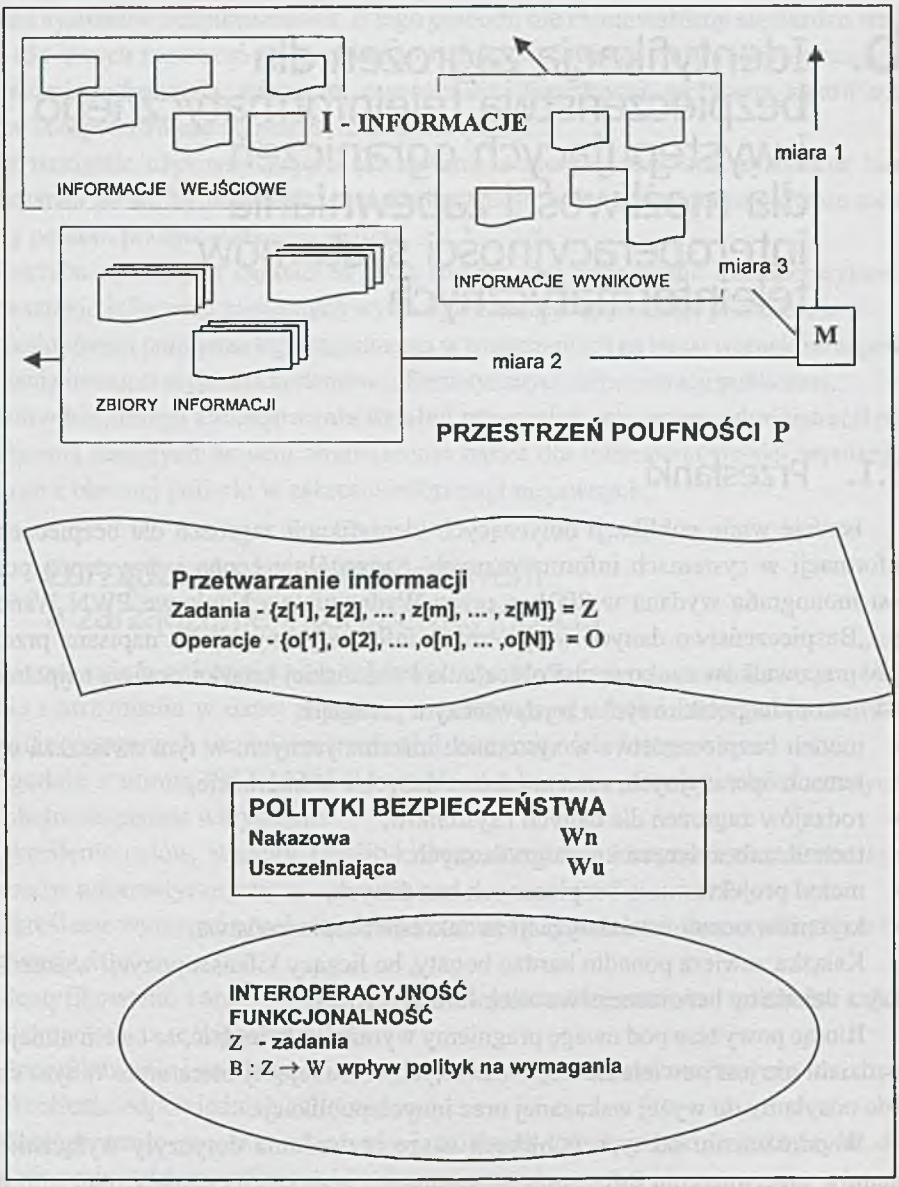
Po drugie podczas przetwarzania informacji, a więc przekształcania ich w informacje wynikowe. Interoperacyjność poprawi się, gdy zasady wartościowania miar poufności informacji wynikowych w oparciu o wartości miar poufności informacji wejściowych będą sformalizowane w takim stopniu, że dadzą się w jakimś stopniu zautomatyzować.

5.4.5. Specyfikacja istotnych cech modelowych przetwarzania informacji

- W procesach przetwarzania informacji w systemach informatycznych administracji publicznej mamy do czynienia z wieloma płaszczyznami poufności. Najważniejszą, ale nie jedyną jest płaszczyzna informacji niejawnych według obowiązujących regulacji prawnych.
- W ocenie miary poufności (analogicznie: klauzuli tajności) musi być brana pod uwagę semantyka informacji.
- Obowiązujące regulacje prawne w trosce o zapewnienie bezpieczeństwa informacyjnego w regulowanych obszarach stosują zasadę maksymalizacji oceny poufności zbiorów informacji (niejako „na wszelki wypadek"). Takie samo przesłanie dominuje w ocenie poufności informacji przetworzonych. Skutkuje to zarówno w warstwie dziedzinowej we wszystkich aspektach: prawnym, technicznym, ekonomicznym i organizacyjnym, jak i w warstwie funkcjonalnej, utrudniając w sposób zasadniczy interoperacyjność.

- Natura potrzeb użytkowych, a więc w konsekwencji specyfikacji funkcjonalności eksploatowanych systemów informatycznych administracji publicznej, cechuje się zapotrzebowaniem na zestawy informacji zawierające zarówno informacje niejawne, jak i jawne. Powstają więc w praktyce w systemach informatycznych zbiory informacji o zróżnicowanych miarach poufności (klauzulach tajności).
- W poszczególnych procesach przetwarzania informacji w systemach informatycznych dominują różne zagadnienia specyficzne. I tak w procesach:
  - pozyskania informacji źródłowej – dominuje zagadnienie określania wartości miar poufności informacji, w niektórych przypadkach na ich podstawie wartości miar poufności zbiorów informacji oraz stosownego postępowania z nimi,
  - przesyłania informacji – postępowania z informacjami niezmieniającymi swoich cech semantycznych,
  - gromadzenia informacji – dominuje tutaj zagadnienie tworzenia zbiorów z informacji pojedynczych, dla których określone są wartości miar poufności. Istnieje tu problem określenia „wypadkowej" wartości miar poufności,
  - utrzymywania informacji – ponieważ proces odnosić się może do długiego okresu, występuje specyficzne zagadnienie zmiany cech semantycznych informacji a w konsekwencji wartości miar poufności,
  - przetwarzania danych w systemach informatycznych – mamy do czynienia z powstawaniem nowych informacji. Zarówno ich cechy semantyczne, jak i w szczególności wartości miar poufności nie są zwykle oczywiste,
  - udostępniania informacji – istnieje potrzeba określania wartości miar poufności udostępnianych podzbiorów informacji wynikowych,
  - unicestwiania danych – dominuje specyfika techniczna: rzeczywiste unicestwienie, bez możliwości odtworzenia.

Najważniejsze elementy modelu przetwarzania informacji w systemach informatycznych administracji publicznej pod kątem zapewnienia bezpieczeństwa informacyjnego w sytuacji wykorzystywania źródeł informacji o różnych klauzulach tajności zobrazowano schematycznie na rys.5-4. Przy tworzeniu specyfikacji wymagań modelowych na proces kształtowania strategii postępowania w tej ważnej sprawie, prezentowany model będzie pełnił rolę punktu odniesienia i języka formułowanych tez.



Rysunek 5-4. Ilustracja modelu przetwarzania informacji w kontekście zróżnicowanej poufności i interoperacyjności

6. Identyfikacja zagrożeń dla bezpieczeństwa teleinformatycznego i występujących ograniczeń dla możliwości zapewniania interoperacyjności systemów teleinformatycznych

6.1. Przesłanki

Istnieje wiele publikacji dotyczących identyfikacji zagrożeń dla bezpieczeństwa informacji w systemach informatycznych. Szczególnie cenną i przystępną pozycją jest monografia wydana w 2001 r. przez Wydawnictwa Naukowe PWN Warszawa pt. „Bezpieczeństwo danych w systemach informatycznych". Ta napisana przez zespół pracowników naukowych Politechniki Poznańskiej książka zawiera najpełniejszy (417 stron) na polskim rynku wydawniczym przegląd:

- modeli bezpieczeństwa w systemach informatycznych, w tym zwłaszcza w systemach operacyjnych, systemach baz danych i w Internecie,
- rodzajów zagrożeń dla danych i systemów,
- technik zabezpieczeń kryptograficznych,
- metod projektowania bezpiecznych baz danych,
- kryteriów oceny i standaryzacji za zakresie bezpieczeństwa.

Książka zawiera ponadto bardzo bogaty, bo liczący kilkaset pozycji wykaz literatury z dziedziny bezpieczeństwa teleinformatycznego.

Biorąc powyższe pod uwagę pragniemy wyraźnie stwierdzić, że celem niniejszego rozdziału nie jest powielanie treści zawartych w istniejącej literaturze. W tym względzie odsyłamy do wyżej wskazanej oraz innych publikacji.

W odróżnieniu od tych publikacji nasze rozważania dotyczyły wyłącznie problemów przetwarzania informacji w warunkach wykorzystywania źródeł informacji o zróżnicowanych klauzulach tajności i skupiły się na:

- analizie i opisie przyczyn powstania zagrożeń i podatności na etapie planowania systemów bezpieczeństwa,
- analizie i opisie ograniczeń dla zapewnienia interoperacyjności systemów informatycznych.

Nie interesowały więc nas istniejące obiektywnie lub subiektywnie zagrożenia i podatności, o ile nie dotyczyły wprost przetwarzania informacji objętych ustawą o ochronie informacji niejawnych, a ich potencjalny wpływ na stan poufności teleinformatycznej nie wynikał ze świadomych lub nieświadomych błędów na etapie pla-

nowana systemów bezpieczeństwa. Z tego powodu nie zajmowaliśmy się bardzo ważnymi dla innych rozważań np. problemami niekontrolowanej emisji ujawniającej, algorytmami szyfrowania, wirusami, zagrożeniami fizycznymi, wpływem awarii systemów komputerowych na poufność informacji, itp.

W rozdziale używamy pojęcia planowanie a nie projektowanie systemów bezpieczeństwa po to, by podkreślić przede wszystkim uniwersalny a nie głównie techniczny poziom przeprowadzonej analizy.

Potrzeba rozważenia ograniczeń jakie stwarza dla zapewnienia interoperacyjności przetwarzanie informacji niejawnych wyniknęła z naszego głębokiego przekonania o:

- niesłuszności pomijania tego zagadnienia w rozważaniach na temat warunków zapewniania interoperacyjności systemów informatycznych administracji publicznej,
- potrzebie pilnego **zainicjowania działań** przez właściwe organy administracji publicznej mających na celu zmniejszenie barier dla interoperacyjności wynikających z obecnej polityki w zakresie informacji niejawnych.

6.2. Zarządzanie bezpieczeństwem a zarządzanie interoperacyjnością

Zarządzanie bezpieczeństwem teleinformatycznym jest procesem służącym osiągnięciu i utrzymaniu w danej jednostce organizacyjnej administracji publicznej (instytucji) wymaganych poziomów poufności, integralności, dostępności.

Zgodnie z normą PN-I-13335-2 zarządzanie bezpieczeństwem teleinformatycznym obejmuje przede wszystkim:

- Określenie celów, strategii i polityki bezpieczeństwa instytucji w zakresie systemów informatycznych,
- Określenie wymagań w zakresie bezpieczeństwa systemów informatycznych w instytucjach,
- Identyfikowanie i analizowanie zagrożeń i podatności zasobów systemów informatycznych na te zagrożenia,
- Identyfikowanie i analizowanie ryzyka związanego z bezpieczeństwem,
- Określenie odpowiednich zabezpieczeń,
- Monitorowanie procesu wdrożenia i działania zabezpieczeń, niezbędnych dla efektywnej ochrony informacji i usług w instytucji,
- Opracowanie i wdrożenie programu uświadamiania dotyczącego bezpieczeństwa,
- Wykrywanie i reagowanie na incydenty.

Warunkiem wstępnym skutecznego zarządzania bezpieczeństwem systemów informatycznych jest, by bezpieczeństwo było nieodłączną częścią całościowego planu zarządzania instytucją, zintegrowanego ze wszystkimi procesami funkcjonalnymi zachodzącymi w instytucji.

Przedstawione wyżej lub zbliżone podejście do kompleksowego zarządzania bezpieczeństwem teleinformatycznym musi być również zastosowane do problemu interoperacyjności. W tym przypadku istnieje także głęboko uzasadniona potrzeba ist-

nienia procesu zarządzania interoperacyjnością i zdefiniowania jego podstawowych składników.

Można nawet zaryzykować twierdzenie, że o ile teoretycznie możliwa jest ochrona bezpieczeństwa informacji odrębnie w separowanych od siebie systemach informatycznych, to rozważanie interoperacyjności przy założeniu separacji systemów informatycznych traci całkowicie sens.

Biorąc to pod uwagę, przez analogię można przyjąć, iż zarządzanie interoperacyjnością powinno objąć przede wszystkim.:

- Określenie celów, strategii i polityki w zakresie interoperacyjności systemów informatycznych,
- Określenie wymagań w zakresie interoperacyjności systemów informatycznych,
- Identyfikowanie i analizowanie zagrożeń dla interoperacyjności systemów informatycznych,
- Identyfikowanie i analizowanie ryzyka związanego z interoperacyjnością,
- Monitorowanie procesu wdrożenia i działania wszystkich aspektów interoperacyjności,
- Opracowanie i wdrożenie programu uświadamiania dotyczącego interoperacyjności,
- Wykrywanie i reagowanie na incydenty.

Podkreślając świadomie powyższe analogie trzeba jednocześnie zauważyć, że zarządzanie bezpieczeństwem i zarządzanie interoperacyjnością w swej istocie mają w większości przeciwstawne cele. W pewnym uproszczeniu można stwierdzić, że interoperacyjność jest do pewnego stopnia czynnikiem zagrażającym bezpieczeństwu teleinformatycznemu, ponieważ automatyzuje wymianę informacji przez nowe dotychczas najczęściej niechronione, wspólne kanały dystrybucji.

Z jednej strony naturalną strategią postępowania osób odpowiedzialnych za bezpieczeństwo teleinformatyczne i to niezależnie od poziomu rozpatrywania może być wstrzymywanie lub opóźnianie procesów prowadzących do interoperacyjności systemów informatycznych. Z drugiej zaś względy cywilizacyjne i ekonomiczne będą wymuszać konieczność tworzenia warunków dla interoperacyjności systemów informatycznych.

Mamy więc tu sytuację analogiczną do sytuacji z początków powstawania systemów wielodostępnych. Wtedy też zachodził konflikt pomiędzy potrzebami jednoczesnego dostępu do zasobów komputerowych i z drugiej strony wymaganiami selektywnego, zgodnego z uprawnieniami do nich dostępu. W efekcie należało stworzyć mechanizmy gwarantujące bezpieczeństwo przetwarzania informacji w warunkach systemów wielodostępnych. Z dzisiejszej perspektywy w świadomym uproszczeniu można napisać, że wyniki tamtych prac to „pionierskie" rozwiązania w dziedzinie interoperacyjności w obszarze wewnątrzkomputerowych procesów przetwarzania.

Analogia do ogólnych warunków zapewniania bezpieczeństwa i interoperacyjności systemów informatycznych jest tu oczywista. Administracja publiczna musi również doprowadzić do stworzenia warunków organizacyjnych, prawnych, technicznych i ekonomicznych zapewniających jednocześnie wymagane poziomy bezpieczeństwa

i interoperacyjności. Uznając ze względów rozwojowych prymat interoperacyjności trzeba kategorycznie stwierdzić, że warunkiem budowy i wdrożenia systemów interoperacyjnych jest skuteczne zagwarantowanie wymaganych rygorów bezpieczeństwa informacji w nich wymienianych i przetwarzanych. Z tego powodu ramy interoperacyjności muszą uwzględniać względy bezpieczeństwa.

6.3. Zagrożenia organizacyjno-prawne

Polityka w zakresie zarządzania interoperacyjnością systemów informatycznych nie może naruszać jakichkolwiek przepisów prawa, zobowiązań wynikających z ustaw, rozporządzeń danego kraju. Z uwagi na to, że wymagania wynikające z prawodawstwa mogą być różne w poszczególnych krajach, a administracja publiczna bierze udział w międzynarodowej wymianie informacji (transgraniczny przepływ danych), więc zarządzanie interoperacyjnością systemów informatycznych musi uwzględniać ten fakt.

W odniesieniu do aspektu bezpieczeństwa interoperacyjności systemów informatycznych wymagania wynikające głównie z regulacji otoczenia prawnego funkcjonowania tych systemów jednostki organizacyjnej wyznaczają łącznie nakazowy, czyli minimalny poziom bezpieczeństwa, który musi być bezwzględnie zapewniony, by przetwarzanie było prawnie legalne.

W praktyce oznacza to, że prowadząc prace koncepcyjne i techniczno-technologiczne należy pod groźbą odpowiedzialności karnej zapewnić spełnienie wymagań bezpieczeństwa w procesie interoperacyjnego współdziałania systemów informatycznych. Stan bezpieczeństwa musi być monitorowany w sposób ciągły.

Z oczywistych przyczyn uwzględnienie wymogów bezpieczeństwa w procesie zapewniania interoperacyjności systemów informatycznych rodzi zarówno skutki ekonomiczne, jak i prawne oraz techniczno-technologiczne. W dalszej części tego rozdziału wskazujemy na zagrożenia równocześnie związane z bezpieczeństwem i interoperacyjnością.

6.3.1. Zawyżanie klauzul tajności

Jedną z najważniejszych przyczyn powstawania nadmiernych ograniczeń dla zapewniania interoperacyjności jest zawyżenie klauzul tajności zasobów informacyjnych, do których dostęp jest niezbędny z punktu widzenia realizacji zadań przez interoperacyjne systemy informatyczne. Jednocześnie jest to zagrożenie z punktu widzenia bezpieczeństwa informacji, bowiem niezgodne z semantyką informacji błędne zaklasyfikowanie informacji (za niskie lub za wysokie) jest naruszeniem ustawy o ochronie informacji niejawnych i jej aktów wykonawczych. Z punktu widzenia interoperacyjności szczególnie szkodliwe jest nieuzasadnione nadawanie i tym samym zawyżanie klauzul tajności

6.3.2. Nadmierne pokrywanie niejawnością

W swej istocie to zagrożenie jest odmianą zagrożenia opisanego w 6.3.1. Polega na tym, że wynikającą z semantyki niejawnością jednych atrybutów obiektów informacyjnych obejmuje się inne w pełni jawne atrybuty. W konsekwencji nie mogą one być użyte w realizacji semantycznie jawnych zadań. Taka praktyka klasyfikowania informacji nie jest wymuszona postanowieniami ustawy o ochronie informacji niejawnej, gdyż ustawa dopuszcza, przy spełnieniu odpowiednich warunków, możliwość wydzielenia z dokumentów części jawnych od niejawnych (lub ogólniej części o różnych klauzulach tajności) w celu zapobieżenia nadmiernemu rozciąganiu klauzul tajności na całe dokumenty. Nie ma żadnych ustawowych przeszkód, by w systemach informatycznych skorzystać z tej możliwości, co ma szczególne znaczenie dla systemów przewidzianych do interoperacyjnego współdziałania.

Zagrożenia i ograniczenia, na które wskazano w 6.3.1. i 6.3.2. mają szczególne znaczenie dla zapewnienia interoperacyjności (a interoperacyjność systemów informatycznych jest warunkiem budowy społeczeństwa informacyjnego) powodują bowiem między innymi:

- zwiększone koszty budowy systemu bezpieczeństwa informacyjnego, znacznie zwiększone koszty eksploatacyjne, szkoleniowe, itd.,
- ograniczone lub utrudnione możliwości zapewnienia interoperacyjności systemów informatycznych,
- niemożliwość wykonania wielu uzasadnionych zadań przetwarzania bez naruszenia ustawy,
- narażenie pracowników na świadome lub nieświadome (przy braku odpowiednich mechanizmów) naruszenie ustawy.

6.3.3. Niezgodność organizacyjna

W istniejących systemach informatycznych mogą i najczęściej występują niezgodności w zasadach zapewniania poufności przetwarzanych w nich danych z uwagi na różne regulacje prawne, różne rozwiązania kompetencyjne, różne struktury organizacyjne i proceduralne. Wspomniane wyżej niezgodności dotyczą wszystkich poziomów rozpatrywania interoperacyjności, przy czym niezgodności prawne dotyczące systemów informatycznych jednej instytucji odnoszą się do wewnętrznej dokumentacji systemu bezpieczeństwa. Rozważanie szczegółów zasygnalizowanych tu niezgodności wykracza poza ramy książki. Natomiast trzeba pokreślić, że mogą one być źródłem zagrożeń dla interoperacyjności np. na skutek różnych procedur obsługi incydentów bezpieczeństwa, różnych interpretacji tego co w odniesieniu do bezpieczeństwa jest nakazowe a co uszczelniające, różnych procedur kontrolnych, różnych procedur weryfikacji i dokumentowania odpowiedzialności.

Weryfikacja poprawności planowania i zarządzania bezpieczeństwem systemów informatycznych jako całościowego procesu wdrażania i utrzymywania programu

bezpieczeństwa systemów informatycznych na poziomach instytucjonalnym, krajowym, ponadkrajowym powinna uwzględniać również cele interoperacyjności.

Dlatego rozpatrując problemy bezpieczeństwa w kontekście interoperacyjności należy przede wszystkim ustalić czy główne akty prawne dotyczące bezpieczeństwa informacyjnego w systemach, które mają współdziałać interoperacyjnie są zgodne, dotyczą tego samego zakresu pojęciowego, czy są w tej mierze niesprzeczne.

6.4. Zagrożenia techniczne

6.4.1. Brak kontroli przepływu informacji

Podstawową regułą bezpieczeństwa przetwarzania informacji (danych) o zróżnicowanych klauzulach tajności jest to, by informacje (dane) o wyższej klauzuli tajności nie przepłynęły do obiektów (aktywnych lub pasywnych) mających niższą klauzulę tajności. Reguła ta jest tożsama z regułą stosowaną „od zawsze" w obszarze tradycyjnego przetwarzania informacji.

W systemach informatycznych administracji publicznej stosuje się w przeważającej mierze mechanizmy ochrony danych stanowiące standardowe wyposażenie systemów operacyjnych i systemów baz danych.

Bezpieczne przetwarzanie danych o różnych klauzulach tajności wymaga od mechanizmów ochrony posiadania własności sterowaniu przepływem informacji. W związku z tym istnieje kategoryczna potrzeba sprawdzenia czy:

- wykorzystywany w konkretnym systemie informatycznym mechanizm ochrony spełnia powyższy warunek?
- Czy łącznie systemy współdziałające interoperacyjnie mają możliwości sterowania przepływem?

Jeśli odpowiedź na te pytania byłaby negatywna, to przetwarzanie informacji o zróżnicowanych klauzulach tajności mogłoby doprowadzić m.in. wprost do nieszczelności systemu bezpieczeństwa bądź drastycznych ograniczeń w przetwarzaniu danych bądź powstawania np. pozasystemowych, nieewidencjonowanych (z punktu widzenia systemu bezpieczeństwa) roboczych plików informacji (danych).

6.4.2. Brak reguł wyznaczania wypadkowej niejawności

W systemach informatycznych administracji publicznej stosuje się zasadę polegającą na przydzieleniu niższej klauzuli pojedynczym zapisom i wyższej klauzuli bazie danych zawierającej łącznie te zapisy. Stwarza to w przypadku przetwarzania danych o zróżnicowanych klauzulach zasadnicze zagrożenia z uwagi na brak bezpiecznych algorytmów o formalnie potwierdzonej poprawności „obliczania" wypadkowej klauzuli tajności.

6.5. Zagrożenia uboczne

Zagrożenia lub szkody uboczne [16] powstają jako efekt uboczny towarzyszący jakiemuś incydentowi. Czasem jest to określane efektami kaskadowymi, które ujawniają się w środowisku wzajemnie uzależnionych systemów. Zagrożenia i szkody tego typu, które w przypadku interoperacyjności przyjmują często postać ograniczeń wymagają wnikliwego rozpatrzenia i uwzględnienia w praktyce projektowania i eksploatacji systemów interoperacyjnych.

6.5.1. Nieuzasadnione koszty i bariery

Jest to niedoceniany lub wręcz niedostrzegany problem, który występuje, gdy np. w celu uzyskania z jakichkolwiek (często nieuzasadnionych) przyczyn zwiększonej separacji systemów informatycznych zawyżane są klauzule tajności zasobów informacyjnych.

W oczywisty sposób może to skutkować koniecznością ponoszenia nadmiernych kosztów budowy i utrzymywania systemu bezpieczeństwa teleinformatycznego skupionego na ochronie poufności (rozwiązania techniczne, prawne, organizacyjne, personalne) oraz ograniczeniami lub nadmiernymi kosztami zapewniania interoperacyjności systemów informatycznych.

Innym skutkiem ubocznym tej kategorii zagrożeń jest ograniczanie możliwości wzmacniania (środki już wydatkowano na ochronę poufności) pozostałych składników bezpieczeństwa informacyjnego.

W konsekwencji mogą również wystąpić przesłanki nieuzasadnionego, niegospodarnego dysponowania publicznymi środkami finansowymi,

6.5.2. Brak dostępności

Rygorystyczne i zgodne z prawem dążenie w procesach przetwarzania informacji o zróżnicowanych klauzulach tajności do spełnienia wymagań ustawy o ochronie informacji niejawnych może spowodować szkodliwe **naruszenie cechy dostępności bezpieczeństwa informacyjnego**, jeśli semantyka przetwarzanych informacji wskazuje na nieuzasadnione „zawyżenie klauzul tajności" lub „nadmierne pokrywanie niejawnością".

Taka sytuacja wystąpi, gdy realizacja semantycznie legalnego zadania natrafi na nieuzasadnione ograniczenia spowodowane wspomnianymi nieuprawnionymi praktykami w nadawaniu klauzul tajności.

6.5.3. Przekazywanie niejawności

Systemy informatyczne wykorzystywane wspólnie do realizacji zadań publicznych w warunkach zróżnicowanych klauzul informacji są narażone na problem „infekcji niejawnością", czyli przenoszenia niejawności. Zagrożenie to polega na tym,

że system informatyczny przygotowany do przetwarzania informacji jawnych w sytuacji bezpośredniego lub pośredniego (relacja przechodniości) współdziałania z innym systemem, w którym przetwarzane są informacje niejawne może przez ukryte lub niewystarczająco rozpoznane kanały dystrybucji zostać „zainfekowany" informacjami niejawnymi.

Gdy tak się stanie, to zgodnie z zasadami obowiązującymi dla przetwarzania informacji niejawnych klauzula tajności tego systemu (przetwarzanych nim informacji) powinna być podwyższona do najwyższej klauzuli informacji, które do niego przeniknęły. W praktyce oznacza to separację tego systemu od dotychczas realizowanych jawnych zadań.

6.5.4. Problem bliskości

Problem bliskości w obszarze bezpieczeństwa został szczegółowo omówiony w [16]. Odnosi się on go głównie do zagrożeń typu „gdzie drwa rąbią tam wióry lecą" (gdy zostanie zaatakowana fizycznie firma mieszcząca się na tym samym piętrze co nasza firma, to skutki tego ataku mogą również dotyczyć naszej firmy mimo to, że atak nie był w nas wymierzony).

W interesującym nas środowisku interoperacyjności problem bliskości również istnieje. Decydując się na automatyzowanie realizacji zadań publicznych dzięki interoperacyjnemu współdziałaniu systemów informatycznych przesądzamy o wzajemnym „zbliżeniu" się tych systemów i w konsekwencji o uzależnieniu realizacji zadań jednej komórki organizacyjnej od działania innej jednostki organizacyjnej.

Tym samym skutki ataku na jeden system informatyczny, z uwagi na występowanie problemu bliskości, mogą natychmiast przenieść się negatywnie na inny współdziałający z nim interoperacyjnie system informatyczny.

7. Modele i mechanizmy ochrony przetwarzania informacji o rożnych klauzulach tajności

7.1. Uwagi wstępne

Ochrona danych jest rozumiana jako zapewnienie poufności, integralności i dostępności chronionych danych. W tym rozdziale została przedstawiona klasyfikacja mechanizmów ochrony danych oraz analiza systemów informatycznych pod kątem oceny ich przydatności i możliwości zapewnienia bezpieczeństwa informacji o różnych klauzulach tajności. Informacje te mają być przetwarzane, przechowywane i przesyłane w ramach analizowanych systemów. Na pierwszym miejscu w tych rozważaniach stawiane jest zapewnienie poufności, jednak ze względu na kompleksowe rozpatrywanie problemu bezpieczeństwa teleinformatycznego, węższej analizie zostały poddane również aspekty integralności i dostępności.

Pierwotną przyczyną tworzenia mechanizmów ochrony było powstanie systemów z podziałem czasu, obsługujących jednocześnie wielu użytkowników i zapewniających długookresowe przechowywanie ich programów i danych. Ochrona powstała w istocie ze względu na niezawodność i sterowane dzielenie zasobów.

Współczesne tendencje zmierzają do przetwarzania rozproszonego w środowisku interoperacyjności systemów przetwarzania danych, co podkreśla wagę zapewniania przez te systemy kontrolowanego współdzielenia zasobów w ramach sieci komputerowych. W chwili obecnej naturalnym jest, że użytkownicy chcą wymieniać dane i programy w ramach komputerów podłączonych do sieci komputerowej, zapisywać pliki w innych lokalizacjach, odwoływać się do zewnętrznych systemów baz danych lub uruchamiać programy wymagające zasobów, którymi nie dysponują ich własne komputery.

Z modelowego punktu widzenia stan każdego systemu (stan jego ochrony) można opisać poprzez zdefiniowanie zbioru podmiotów, zbioru obiektów i opis relacji, jakie mogą zachodzić pomiędzy elementami tych dwóch zbiorów.

W skład zbioru podmiotów wchodzą aktywne jednostki biorące udział w przetwarzaniu danych, np. użytkownik, administrator, proces.

Obiektami są elementy systemu przetwarzania, które powinny być chronione. Ze względu na różnorodną specyfikę tych elementów podzielono je na dwa podzbiory:

- obiekty pasywne – tu jako przykłady można wymienić np. rekordy bazy danych, zawartość plików, itp.,
- obiekty aktywne – są to elementy, dzięki którym można przetwarzać chronione dane, np. aplikacje, procesy. Z punktu widzenia ochrony danych są one bardzo ważnymi elementami, ponieważ w wielu przypadkach możliwość skorzystania np. z aplikacji jest równoznaczna z uzyskaniem dostępu do przetwarzanych przez nią danych.

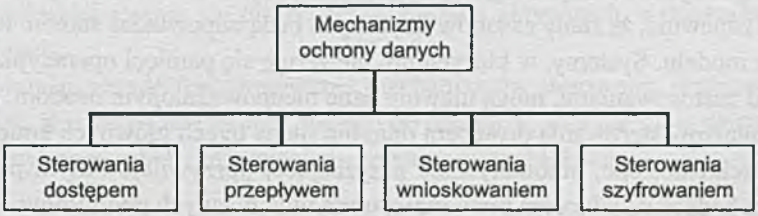
Przy okazji omawiania klasyfikacji obiektów należy podkreślić fakt, iż istnieje wiele obiektów, które mogą zostać zaklasyfikowane do różnych podzbiorów (obiektów pasywnych lub aktywnych) w zależności od aktualnego stanu systemu. Aplikacja, która jest uruchomiona będzie traktowana jako obiekt aktywny, zaś w momencie gdy jest przechowywana na dysku jako plik uruchomieniowy powinna być zaliczona do zbioru obiektów pasywnych.

Sytuacja zdefiniowania ról, jakie pełnią w trakcie działania systemu przetwarzania jego poszczególne elementy komplikuje się jeszcze bardziej, ponieważ elementy systemu nie tylko mogą zmieniać swoje przypisanie do obiektów aktywnych lub pasywnych, ale w niektórych sytuacjach obiekty mogą stać się podmiotami chcącymi uzyskać dostęp do innych obiektów. Przykładem może być aplikacja, która raz sięga po dane do bazy danych i w tym momencie powinna być analizowana jako podmiot, zaś w innym stanie systemu przetwarzania stanowi ona obiekt, do którego użytkownik chce uzyskać dostęp, np. w celu modyfikacji jej kodu. Może również wystąpić sytuacja, w której w tym samym czasie ten sam element systemu przetwarzania należy zaklasyfikować jednocześnie jako podmiot i obiekt. Tutaj przykładem może być działająca aplikacja, która jednocześnie jest podmiotem (w trakcie prób dostępu do bazy danych) i obiektem (którym jest z punktu widzenia użytkownika chcącego z niej skorzystać).

Kolejnym bardzo istotnym elementem każdego systemu ochrony są relacje (zasady), które kontrolują dostęp podmiotów do obiektów. To właśnie przede wszystkim te relacje pozwalają rozróżniać mechanizmy ochrony danych.

7.2. Klasyfikacja mechanizmów ochrony danych

Ze względu na cechy charakterystyczne zasad kontroli wszelkich form dostępu do danych wyróżnia się cztery typy mechanizmów ochrony danych: sterowanie dostępem, sterowanie przepływem, sterowanie wnioskowaniem i sterowanie szyfrowaniem [5].



Rys. 7-1. Podział mechanizmów ochrony danych

Koncepcja sterowania szyfrowaniem w ramach książki nie jest omawiana ze względu na specyfikę zagadnień związanych z szyfrowaniem danych.

7.2.1. Sterowanie dostępem

Model podstawowy sterowania dostępem

Model sterowania dostępem jest mechanizmem najczęściej stosowanym. Opisywany jest przez zbiór podmiotów, zbiór obiektów i regułę dostępu. Często do tego celu wykorzystuje się koncepcję macierzy dostępu, w której w wiersze odpowiadają nazwom przedmiotów, kolumny nazwom podmiotów. Na przecięciu kolumn i wierszy umieszcza się uprawnienia podmiotów do przetwarzania przedmiotów dostępu. W rozpatrywaniu problemów sterowaniem dostępem rozróżnia się pojęcia: polityki i mechanizmu. Polityka sterowania dostępem odzwierciedla reguły przydzielania prawa dostępu, natomiast mechanizm jest formą implementacji tej polityki za pomocą narzędzi i metod informatyki. Do zbioru ww. uprawnień mogą należeć uprawnienia różnych kategorii, w tym m. in. prawo do czytania, modyfikacji, usuwania, wykonywanie programu, zarządzanie uprawnieniami do obiektu, itd. Na rys. 7-2 przedstawiono przykładową macierz dostępu, w której określono prawa podmiotów: Podmiot_1, Podmiot_2, Podmiot_3 do obiektów: Obiekt_1, Obiekt_2, Obiekt_3.

		Obiekty systemu ochrony		
		Obiekt_1	Obiekt_2	Obiekt_3
Podmioty systemu ochrony	Podmiot_1	czytanie		czytanie, pisanie
	Podmiot_2		czytanie, wykonywanie	
	Podmiot_3			czytanie

Rys. 7-2. Przykładowa macierz dostępu

Mechanizmy sterowania dostępem realizują systemową politykę ochrony zapewniając, że fizyczne stany systemu odpowiadają stanom upoważnionym abstrakcyjnego modelu. Te mechanizmy muszą monitorować wszystkie dostępy do obiektów, a także polecenia jawnie przekazujące lub odwołujące prawa. System mógłby jednak znaleźć się w stanie fizycznym, który nie odpowiada żadnemu z upoważnionych stanów modelu. Przykładowo podmiot mógłby ominąć system plików i wydać żądanie bezpośredniego czytania z fizycznego obszaru pliku na dysku. Mechanizmy ochrony muszą także zapewnić, że stany zasobów fizycznych będą odpowiadać stanom logicznym obiektów modelu. Systemy, w których np. nie zeruje się pamięci operacyjnej między kolejnymi zastosowaniami, mogą ujawnić dane nieupoważnionym osobom.

Mechanizmy sterowania dostępem opierają się na trzech głównych koncepcjach:

- Hierarchii dostępu, automatycznie przyznającej uprzywilejowanym podmiotom prawa będące nadzbiorem praw mniej uprzywilejowanych podmiotów.

- Listach upoważnień, będących listami podmiotów mającymi prawa dostępu do poszczególnych obiektów.
- Możliwościach, które można porównać do biletów dostępu do obiektów; posiadanie możliwości bezwarunkowo upoważnia do dostępu do obiektów.

Lista upoważnień, zwana również listą sterowania dostępem, jest listą podmiotów upoważnionych do dostępu do obiektu. Listy upoważnień używane są zwykle do ochrony obiektów własnościowych, np. plików. Z każdym plikiem związana jest lista upoważnień specyfikujących identyfikatory użytkowników lub grup użytkowników i przyznane im prawa dostępu. Jedynie właściciel pliku może przekazywać prawa dostępu do pliku innym użytkownikom. Żaden z mających dostęp do pliku użytkowników nie może przenosić tych praw na innych użytkowników. Właściciel może odebrać lub ograniczyć prawa dostępu dowolnemu użytkownikowi modyfikując element odpowiadający temu użytkownikowi w liście upoważnień. Aby uzyskać dostęp do obiektu, użytkownik musi wyspecyfikować nazwę obiektu i zbiór dostępu. Użytkownikowi przydziela się dostęp do obiektu tylko wtedy, gdy znajduje się on w zbiorze dostępu. Ponadto lista upoważnień dla zbioru musi zawierać pozycję użytkownika z odpowiednimi prawami dostępu. W wielu systemach stosuje się listy upoważnień z dwiema tylko pozycjami: pierwsza określa prawa dostępu właściciela, druga – prawa dostępu pozostałych użytkowników. Prawa dostępu w tych systemach są zwykle ograniczone do praw czytania i pisania. Takie postacie list upoważnień nie są zgodne z prawem minimalnego uprzywilejowania, ale są efektywne w implementacji i przeszukiwaniu oraz są odpowiednie dla wielu zastosowań.

Zaletą list upoważnień jest to, że zapewniają właścicielowi obiektu pełną kontrolę nad tym, kto ma dostęp do jego obiektu. Właściciel może odwołać dowolne prawo dostępu użytkownika do obiektu usuwając pozycje danego użytkownika z listy. Zaletę tę traci się częściowo w systemach, w których listy upoważnień stosuje się dla niewłasnościowych obiektów i zezwala się dowolnemu użytkownikowi przydzielać i odwoływać prawa dostępu do obiektu.

Możliwość jest parą określającą unikalną nazwę (identyfikator) obiektu i zbiór praw dostępu do niego. Możliwość jest rodzajem biletu, którego posiadanie bezwarunkowo upoważnia do wybranego dostępu do konkretnego obiektu. Skoro możliwość zostanie przyznana, żadne inne sprawdzenie legalności dostępu nie jest już wymagane. Bez mechanizmu możliwości byłoby wymagane upoważnienie każdego dostępu przez przeszukiwanie listy upoważnień.

W systemie można stosować zarówno listy możliwości, jak i upoważnień, przy czym możliwości stosuje się dla obiektów bieżąco aktywnych, a upoważnienia dla nieaktywnych.

Uogólniając zasadę funkcjonowania mechanizmów sterowania dostępem można powiedzieć, iż ustalają one zasady dostępu do obiektów, lecz nie mają wpływu na to, co podmioty mogą robić z informacjami zawartymi w obiektach.

Rozszerzenia podstawowego modelu

Podczas tworzenia systemu bezpieczeństwa baz danych zbiory uprawnień mogą być rozszerzane o dodatkowe warunki, jakie muszą być spełnione, aby uprawnienia te mogły być wykorzystane. Wtedy zamiast określenia zbiór uprawnień stosuje się określenie zbiór reguł decyzyjnych.

Przykładowo rozszerzeniami standardowego mechanizmu kontroli dostępu mogą być:

- identyfikacja osoby tworzącej regułę dostępu,
- wskaźnik prawa przekazania prawa dostępu,
- reguły dodatkowych warunków dostępu.

Jako przykładowe rozwinięcie modelu podstawowego mechanizmu sterowaniem dostępem warto przybliżyć metodę zwaną *opieczętowaniem* obiektów. Jest to przykład wprowadzenia dodatkowych warunków dostępu. W metodzie tej proponuje się aby chroniony obiekt mógł być opieczętowany tylko przez wyznaczony zarządzający nim podmiot. Tylko ten podmiot może dokonywać pieczętowania i rozpieczętowania (np. przez szyfrowanie) danego obiektu. W tym systemie wszelkiego typu operacje w stosunku do zapieczętowanego obiektu powinny kończyć się generowaniem błędu. Takie podejście do ochrony danych dawałoby możliwość dostępu podmiotom posiadającym odpowiednie uprawnienia, ale tylko w określonej sytuacji lub czasie. W literaturze nazywane jest to „drugim poziomem ochrony".

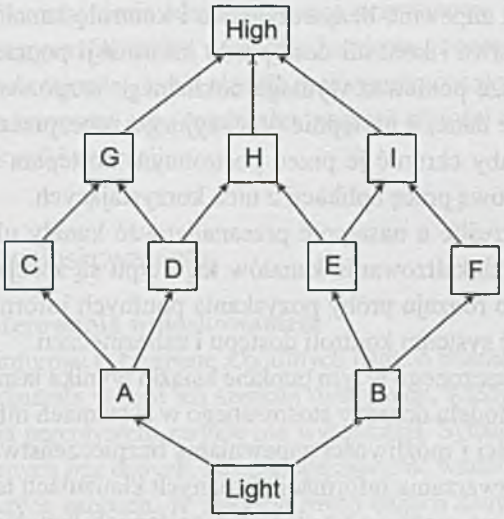
7.2.2. Sterowanie przepływem

Model podstawowy sterowania przepływem

Model systemu przepływu informacji opracowano korzystając z polityki przepływu opisanej za pomocą kraty, stanów i przejść stanów.

Krata składa się z klas ochrony i relacji zachodzących pomiędzy nimi. Klasy ochrony odpowiadają rozłącznym klasom informacji. Dla klas ochrony A i B relacja $A < B$ oznacza, że informacja klasy A jest niższa od informacji klasy B. Informacje mogą przepływać tylko między obiektami takiej samej klasy lub do obiektów wyższej klasy. Zabroniony jest przepływ obiektów do niższej klasy lub klasy nie będącej w relacji.

Najprostsza polityka przepływu określa dwie klasy informacji: jawną i niejawną. Przy takiej sytuacji wszystkie przepływy, z wyjątkiem przepływów z obiektów niejawnych do jawnych, są dozwolone. Polityka ta określa wymagania dla selektywnie zamkniętego programu usługowego, który operuje danymi niejawnymi i jawnymi. Program usługowy ma prawo zapamiętywać jawne dane klienta, ale nie ma prawa zapamiętywać lub udostępniać żadnych danych niejawnych. Przykładowa krata dla systemu, w którym wyróżniono jedenaście klas ochrony – najwyższą High, najniższą Low i pośrednie oznaczone literami od A do I została przedstawiona na rysunku 7-3.



Rys. 7-3. Przykładowa krata opisująca klasy ochrony i możliwe relacje

Model kratowy wprowadzono, aby opisać polityki i kanały przepływu informacji, ale nie to jakie znaczenie ma fakt, że informacja przepływa z jednego obiektu do drugiego.

W mechanizmie sterowania przepływem wyróżnia się zbiór obiektów pamięciowych (zawierających dane), zbiór procesów powodujących przepływ danych (inicjowanych przez użytkowników), zbiór klauzul tajności oraz relację przepływu. Mechanizm ochrony oparty na sterowaniu przepływem powinien zabronić realizacji procesów powodujących przepływ danych niezgodnych z określoną relacją przepływu (np. z obiektu pamięciowego o klauzuli tajne do użytkownika lub innego obiektu pamięciowego o niższej klauzuli). Jak łatwo zauważyć przedstawiona tu reguła działania mechanizmu sterowania przepływem jest zgodna z regułą określoną w Uwagach Wstępnych do niniejszego rozdziału.

Na potrzeby opisu tego modelu wprowadzono pojęcie systemu bezpiecznego, który jest rozumiany jako system, w którym wszystkie wykonywalne w jego ramach przepływy są bezpieczne. Istotną cechą takiego systemu jest to, że klasa ochrony dowolnego obiektu będzie co najmniej tak wysoka jak najwyższa klasa informacji zapamiętanej w tym obiekcie. Nie wynika jednak z tego, że klasa ochrony musi wzrastać w czasie. Jeśli informacje są usuwane z obiektu, jego klasa ochrony może się obniżyć.

Informacje pomiędzy obiektami mogą przepływać trzema rodzajami kanałów:

- kanałami legalnymi – służą one do przekazywania informacji zgodnie z wcześniej zaplanowaną polityką dostępu,
- kanałami pamięciowymi – są one obiektami współdzielonymi przez więcej niż jeden proces czy aplikację, np. współdzielone pliki czy zmienne globalne,
- kanałami ukrytymi – których w ogóle nie przewidziano do przesyłania informacji. Z przepływem ukrytym mamy do czynienia np. w przypadku niebezpośredniego przekazania pewnych informacji z jednego obiektu danych do innego.

Najłatwiej jest zapewnić bezpieczeństwo i kontrolę kanałów legalnych. Zapewnienie bezpieczeństwa i kontroli dostępu do informacji poprzez kanały pamięciowe jest dużo trudniejsze ponieważ wymaga dokładnego rozpoznania miejsc, w których są przechowywane dane, a następnie precyzyjnego zabezpieczenia każdej z nich indywidualnie, tak aby chronić je przed postronnym dostępem a jednocześnie umożliwiać bezproblemową pracę aplikacji z nich korzystających.

Najtrudniej określić a następnie przeanalizować kanały ukryte. Jednym z możliwych sposobów zlokalizowania kanałów tego typu są specjalistyczne audyty, które poprzez rożnego rodzaju próby pozyskania poufnych informacji sprawdzają kompletność i spójność systemu kontroli dostępu i zabezpieczeń.

Z opisu zamieszczonego w tym punkcie książki wynika jasno, że w trakcie analizy funkcjonującego modelu ochrony stosowanego w systemach informatycznych pod kątem ich przydatności i możliwości zapewniania bezpieczeństwa teleinformatycznego w warunkach przetwarzania informacji o rożnych klauzulach tajności należy zwrócić szczególną uwagę na możliwe wystąpienie opisanych kanałów typu pamięciowego i ukrytego.

Rozszerzenia podstawowego modelu

Przykładem rozwinięcia idei sterowania przepływem jest wprowadzenie w zaawansowanych systemach wielopoziomowej ochrony modyfikacji dla opisu klasy ochrony. Polega ona na tym, iż w tym wypadku klasa ochrony jest parą (A, C), gdzie A określa poziom upoważnienia, a C – kategorię. W systemach rządowych i wojskowych istnieją cztery poziomy upoważnienia:

- 0 – jawne;
- 1 – poufne;
- 2 – tajne;
- 3 – ściśle tajne.

Kategoriami mogą być np. określenia rodzaju dziedzinowego informacji, np. działania lądowe, działania morskie. W takim przypadku transmisja informacji z klasy (2, działania lądowe) do (2, działania lądowe, działania morskie) lub (3, działania lądowe) jest dozwolona, ale do (1, działania lądowe) lub (3, działania morskie) już nie.

Kolejnym przykładem rozwinięcia idei sterowania przepływem jest wprowadzenie do opisu modelu kraty podzbiorów. Dla zbioru X krata podzbioru jest kratą wyprowadzoną z nieliniowego uporządkowania zbioru zawierającego wszystkie możliwe podzbiory zbioru X. W kracie podzbioru najniższą klasą jest zbiór pusty zaś najwyższą zbiór X. Krata podzbiorów jest użyteczna dla opisu operacji typu wejście/wyjście, które są charakterystycznymi dla systemów informatycznych.

Krata podzbiorów nadaje się również dobrze do opisu polityki, dla której X jest zbiorem kategorii lub właściwości, a klasy są kombinacjami kategorii. W takiej sytuacji przepływ informacji z obiektu A do B jest dozwolony tylko wtedy, gdy B ma co najmniej właściwości obiektu A.

Innym przykładem rozwinięcia idei sterowania przepływem jest zintegrowanie go z sterowaniem dostępem. W takim wypadku każdemu procesowi przydziela się klauzule dopuszczenia do tajności, która określa maksymalny poziom tajności danych, z których proces może korzystać oraz minimalny poziom tajności danych, do których proces może zapisać wyniki operacji.

7.2.3. Sterowanie wnioskowaniem

Model podstawowy sterowania wnioskowaniem

W sytuacji, kiedy informacje czerpane z poufnych danych muszą być odtajnione lub ma być obniżona ich klauzula w celu ich szerszej dystrybucji, wtedy opisane wcześniej mechanizmy sterowania przepływem zwykle nie wystarczają. Sytuacja taka ma miejsce w przypadku statystycznych baz danych, które mogą zawierać wrażliwe informacje o organizacji lub pojedynczych osobach. W statystycznych bazach danych chodzi o umożliwienie dostępu do statystyk dotyczących danych zbiorczych, przy jednoczesnym ograniczeniu dostępu do informacji o jakimkolwiek konkretnym obiekcie.

Największym problemem jest jednak to, że statystyki zawierają ślad pierwotnej informacji. Dociekliwy użytkownik może przez korelację różnych statystyk wydobyć poufne informacje o niektórych obiektach. Celem sterownia wnioskowaniem jest zapewnienie, żeby udostępniane przez bazę danych statystyk nie doprowadziło do ujawnienia danych poufnych.

Stan informacyjny statystycznej bazy danych składa się z dwóch elementów: danych przechowywanych w bazie danych i wiedzy zewnętrznej. Baza danych zawiera informacje o wielu atrybutach różnych obiektów, przy czym każdy atrybut może przyjmować kilka możliwych wartości. Wiedza zewnętrzna dotyczy informacji użytkowników o bazie danych.

Wiedzę zewnętrzną można podzielić na:

- roboczą – wiedza o atrybutach występujących w bazie danych i rodzajach dostępnych statystyk,
- dodatkową – informacje, które zwykle nie są udostępniane przez bazę danych, mogą to być informacje poufne bądź jawne.

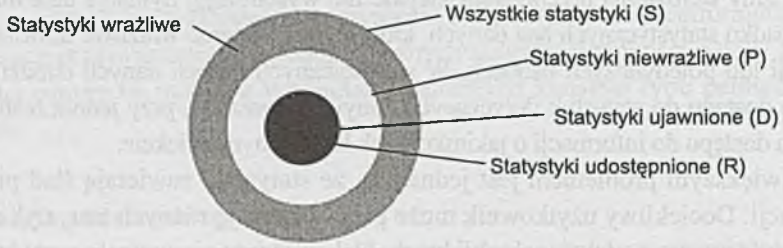
Statystyki obliczane są dla podgrup rekordów mających wspólne atrybuty. Podgrupa jest określona formułą charakterystyczną, która jest dowolnym wyrażeniem logicznym zbudowanym z wartości atrybutów, połączonych operatorami logicznymi. Zbiór rekordów, którego wartości atrybutów spełniają formułę charakterystyczną, nazywany jest zbiorem odpowiedzi dla formuły.

Statystyczna baza danych zapewnia poufność doskonałą wtedy i tylko wtedy, gdy nie ujawnia żadnych statystyk wrażliwych. Statystyka jest wrażliwa, jeśli ujawnia zbyt dużo poufnych informacji o pewnych obiektach. W praktyce statystyczna baza danych nie może zapewnić poufności doskonałej danych, ponieważ każda dozwolona statystyka zawiera pewne informacje o danych, na podstawie których została obliczona.

W podstawowym modelu sterowania wnioskowaniem można wyróżnić:

- zbiór wszystkich statystyk (S),
- podzbiór statystyk niewrażliwych (P),
- podzbiór statystyk udostępnianych (R),
- zbiór statystyk ujawnianych przez R (łącznie ze statystykami ze zbioru R).

Mając na uwadze zbiory statystyk wyróżnione w modelu, można powiedzieć, że statystyczna baza danych jest bezpieczna, jeśli $D \subseteq P$, tzn. nie istnieją statystyki wrażliwe ujawniane przez R. Optymalnym było by aby wszystkie udostępniane statystyki niewrażliwe znajdowały się w zbiorze R lub były obliczane na jego podstawie (tzn. były ujawniane przez R). O systemie, w którym $D = P$ mówi się, że jest dokładny. Jest to bardzo ważna cecha (złoty środek) ze względu na zachowanie odpowiedniego poziomu bezpieczeństwa i z drugiej strony należytej swobody korzystania z informacji.



Rys. 7-4. Model sterowania wnioskowaniem

Rozszerzenia podstawowego modelu

Rozwinięciami modelu podstawowego sterowania wnioskowaniem są najczęściej dodatkowe mechanizmy ograniczania statystyk, np.:

- sterowanie licznością zbiorów odpowiedzi,
- sterowanie stopniem pokrywania się zbiorów odpowiedzi,
- zabranianie komórek.

Sterowanie wnioskowaniem zapewniające wysoki poziom bezpieczeństwa, przez ograniczanie statystyk, nie jest wskazane w systemach uniwersalnych baz danych. Zabranianie komórek jest zbyt czasochłonne w zastosowaniu w bezpośrednich dynamicznych bazach danych. Wymianę danych można ograniczyć do publikacji tylko mikrostatystyk. Interesującym podejściem jest podział bazy danych na poziomie logicznym, może to jednak ograniczać swobodny przepływ informacji statystycznych.

7.3. Analiza przydatności mechanizmów ochrony danych do ochrony przetwarzania informacji o zróżnicowanych klauzulach tajności

Podstawową regułą bezpieczeństwa przetwarzania danych (informacji) o zróżnicowanych klauzulach niejawności jest to, by dane (informacje) o wyższej klauzuli tajności nie przepłynęły do obiektów (aktywnych lub pasywnych) mających dopuszczenie (klasyfikację) do niższej klauzuli tajności.

Techniczne rozwiązania powinny umożliwiać opracowanie i wdrożenie odpowiedniego poziomu ochrony danych. Techniczne rozwiązania są tylko jednym z elementów składowych kompletnego, bezpiecznego systemu przetwarzania informacji o różnych klauzulach tajności, jednak bez nich nie jest możliwe praktyczne wdrożenie prawnych i organizacyjnych zaleceń, które muszą być spełnione w systemach, przechowujących i przetwarzających tego typu informacje.

Rozwiązania techniczne powinny zapewniać poziom ochrony odpowiedni do klauzuli tajności oraz podatności. Nieuzasadnione jego zawyżanie może prowadzić do zbyt dużego wyizolowania informacji, a co za tym idzie utrudnić współpracę z innymi systemami, które muszą również korzystać z tych danych.

Zgodnie z założeniami przyjętymi w rozdziale 3 analiza mechanizmów ochrony została przeprowadzona przy podziale przetwarzania w systemach informatycznych na następujące procesy przetwarzania informacji w systemie:

- pozyskiwanie informacji z otoczenia,
- przesyłanie informacji,
- gromadzenie informacji,
- utrzymywanie informacji,
- przetwarzanie danych,
- udostępnianie informacji,
- unicestwianie informacji.

We wszystkich wymienionych procesach szczególną uwagę zwrócono na zagrożenia wynikające z przetwarzania i przechowywania w jednym miejscu (systemie informatycznym, aplikacji, bazie danych, itd.) danych o różnej klauzuli tajności. Analizowano możliwości nieuprawnionego dostępu użytkowników do danych o klauzuli tajności wyższej od oficjalnie przydzielonego im dopuszczenia.

W celu szczegółowej identyfikacji i analizy możliwych przepływów informacji o rożnych klauzulach tajności w trakcie eksploatacji systemów informatycznych należało dokonać dekompozycji tych systemów ze zwróceniem szczególnej uwagi na miejsca, w których informacja poufna może się znaleźć lub może być przetwarzana. Równocześnie badany był poziom i sposoby dostępu do tych miejsc, uwzględniając w badaniach możliwość występowania trzech kanałów dystrybucji danych, tj. legalnych, pamięciowych i ukrytych.

Biorąc pod uwagę wszystkie wymienne kanały przepływu informacji dokonano analizy przykładowych, najczęściej wykorzystywanych systemów operacyjnych, bazodanowych, portalowych oraz mechanizmów działania sieci teleinformatycznych. Analiza ta dała podstawy do opracowania wniosków, które zostały zaprezentowane w końcowej części tego rozdziału.

Należy podkreślić fakt występowania w systemie informatycznym dwóch typów miejsc, w których mogą znaleźć się poufne dane. Mianowicie miejsca stałego przechowywania informacji poufnej (np. bazy danych, kasety z kopiami bezpieczeństwa) oraz miejsca tymczasowego przechowywania informacji (np. tymczasowe pliki aplikacji).

W przypadku pierwszego typu miejsc dostęp do danych regulowany jest przez osobę posiadającą odpowiednie uprawnienia i wiedzę np. administratora systemu lub administratora danych poufnych. W drugim przypadku dostęp do składowanych informacji regulowany jest przez aplikacje korzystające z tych danych. Nie mają tam zastosowania reguły opracowane w ramach polityki przepływu i przetwarzania danych o rożnych klauzulach tajności. Dodatkowo dane przechowywane w plikach i katalogach tymczasowych po ich wykorzystaniu do bieżących operacji wykonywanych przez aplikacje lub system informatyczny powinny zostać stamtąd usunięte, co nie zawsze ma miejsce.

W celu zwrócenia uwagi na złożoność problemu występowania różnorodnych form przepływu danych w systemach przetwarzania danych o różnych klauzulach tajności niezgodnego ze zdefiniowaną regułą przedstawiono kilka obrazowych, możliwych do wystąpienia w systemach informatycznych przypadków.

Problem pośredniego dostępu do danych

Użytkownik X utworzył plik i zapisał w nim pewne informacje. Użytkownik ten nie przekazał żadnych uprawnień do tego pliku innym użytkownikom. Jest jednak w systemie aplikacja, której używa użytkownik X do przetwarzania danych zapisanych w tym pliku. Uruchamiając ją, proces aplikacji działa z uprawnieniami użytkownika X czyli posiada prawo dostępu do danych w pliku. Z drugiej strony aplikacja ta może posiadać w swoim ciele kod, powodujący zapis odczytanych danych do innego pliku. Dostęp do tego pliku ma użytkownik Y, który stara się pozyskać w sposób nielegalny poufne dane. W opisanej sytuacji, przy każdym dostępie do obiektów sprawdzane są istniejące dopuszczenia. Jednak na żadnym z wymienionych etapów pozyskania informacji system nie zablokuje dostępu, ponieważ z jego punktu widzenia istnieje zezwolenie na wykonywane poszczególnych czynności.

Problem tzw. plików tymczasowych

W trakcie dostępu do danych użytkownika X, który jest uprawniony do korzystania z nich, następuje przesłanie kopii tych danych do katalogów tymczasowych znajdujących się na komputerze użytkownika. Po zakończeniu pracy użytkownik X wylogowuje się z systemu. Następnie do tego samego komputera loguje się użytkownik Y, który nie ma jawnie przydzielonego prawa do zapoznania się z danymi, które zostały się w komputerze w ramach katalogów tymczasowych. Użytkownik Y zalogował się do stacji roboczej z uprawnieniami pozwalającymi mu na przeglądanie zasobów poza własnym katalogiem domowym. W związku z tym może on zapoznać się z informacją poufną, do której pierwotnie nie miał uprawnień.

Problem zmiany klauzuli tajności zbioru danych w wyniku zmiany liczności jego elementów

Użytkownik X ma uprawnienia do korzystania z informacji elementarnych zawartych w bazie danych. Informacje te opatrzone są różną klauzulą tajności, nie wyższą jednak niż poziom P. Jednak w miarę dodawania do bazy kolejnych informacji powstały zbiór danych

z racji wypadkowej wagi powinien zmienić swą klauzulę na wyższą. Jednak automatycznie modyfikacja taka nie następuje i użytkownik X w dalszym ciągu posiada prawo dostępu tak, jakby były to niepowiązane ze sobą informacje elementarne. W rzeczywistości pośrednio uzyskał on dostęp do danych o wypadkowej klauzuli wyższej od poziomu P i tym samym poziomu dopuszczenia dla użytkownika X.

Problem zbyt szczegółowego logowania zdarzeń

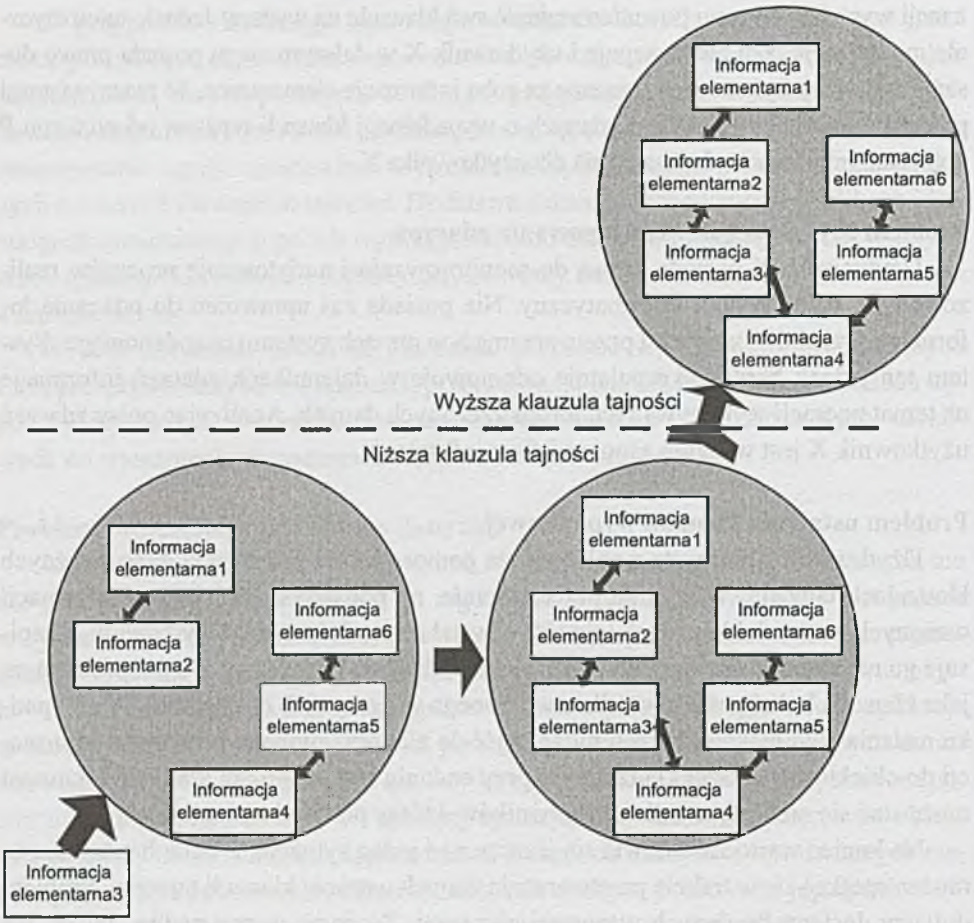
Użytkownik X posiada prawa do monitorowania i audytowania procesów realizowanych przez system informatyczny. Nie posiada zaś uprawnień do poznania informacji przechowywanych i przetwarzanych w ramach systemu bazodanowego. System ten jednak bardzo skrupulatnie odnotowuje w dziennikach zdarzeń informacje na temat operacji wykonywanych na zastrzeżonych danych. Analizując opisy zdarzeń użytkownik X jest w stanie zapoznać się z informacją.

Problem ustalania klauzuli wypadkowej

Użytkownik X korzysta z aplikacji, za pomocą której przetwarza dane o rożnych klauzulach tajności. W wyniku przetwarzania, na podstawie istniejących informacji o znanych, rożnych klauzulach tajności powstał nowy dokument. Użytkownik X zapisuje go nie nadając mu klauzuli poufności lub chcąc ją nadać boryka się z problemem jaka klauzula była by właściwa dla stworzonego w ten sposób dokumentu. W przypadku nadania zbyt niskiej klauzuli może dojść do nieuprawnionego przepływu informacji do obiektów o niższej klauzuli, zaś przy nadaniu zbyt wysokiej klauzuli dokument może stać się niedostępny dla użytkowników, którzy powinni z niego korzystać.

Na koniec warto zastanowić się jeszcze nad jedną sytuacją, z którą bardzo często można spotkać się w trakcie przetwarzania danych o rożnej klauzuli tajności. Problem dotyczy dostępu do danych w postaci zbiorczej. Zarówno w przypadku stałych jak i tymczasowych miejsc przechowywania informacji poufnej, przy zastosowaniu standardowych systemów informatycznych nie można wykluczyć wystąpienia kanałów ukrytych. Takie ukryte kanały wypływu informacji w sposób zabroniony mogą np. nastąpić w sytuacji gdy zbiór danych może zmienić swą klauzulę ze względu na liczbę przechowywanych informacji elementarnych, tzn. w przypadku gdy pojawi się kolejna informacja, która spowoduje przekroczenie pewnego ustalonego progu dla ogólnej wartości danych przechowywanych w tym zbiorze i zbiór ten powinien zostać opatrzony wyższą klauzulą.

Na rysunku 7-5 przedstawiono przepływy danych uwzględniające zależności opisane powyżej. Wynika z tego, iż w przypadku dodania do zbioru danych kolejnych informacji, niekoniecznie o wyższej klauzuli tajności, może dojść do zmiany klauzuli dla całego zbioru, a co za tym idzie powinien zmienić się krąg użytkowników, którzy będą mieli dostęp do tak zgromadzonej informacji.



Rys. 7-5. Automatyczna zmiana klauzuli tajności

Mechanizm ten powinien działać również w drugą stronę, aby w przypadku zmniejszania ogólnej wartości przechowywanych w nim danych nie powodował niesłusznego zawyżania klauzuli. Systemy informatyczne w swej standardowej postaci nie są przygotowane do właściwej reakcji w takich sytuacjach. Może to spowodować, iż dostęp do informacji, które jako zbiór elementów powiązanych ze sobą zależnościami i przez to stanowiących zupełnie inna wartość wypadkową, powinny posiadać wyższą klauzule jest nadal dozwolony dla użytkowników systemu, tak jakby dostawali się do pojedynczych elementarnych informacji. W związku z tym, systemy obsługujące procesy przetwarzania danych o rożnych klauzulach tajności powinny potrafić reagować na tego typu zdarzenia zgodnie z wcześniej wprowadzonymi zasadami.

W rzeczywistości nie ma algorytmów o formalnie potwierdzonej poprawności „obliczania" wypadkowej klauzuli tajności. Na tym etapie rozważań dla przejrzystości modelu celowo nie jest poruszany problem wyliczania wypadkowej klauzuli dla takiego zbioru. Podkreślany jest jednak fakt, że do zmiany takiej może dojść.

Opisane powyżej przykłady dowodzą, iż systemy sterowania dostępem nie spełniają podstawowej reguły bezpieczeństwa przetwarzania danych (informacji) o zróżnicowanych klauzulach niejawności mówiącej, że dane (informacje) o wyższej klauzuli tajności nie mogą przepłynąć do obiektów (aktywnych lub pasywnych) mających dopuszczenie do niższej klauzuli tajności.

Ze względu na kompleksowe rozpatrywanie i kontrolowanie przepływu informacji poufnej, system sterowania przepływem w połączeniu z mechanizmami sterowania wnioskowaniem wydaje się być rozwiązaniem odpowiednim dla środowiska interoperacyjnych systemów, w których przetwarzane są dane o rożnych klauzulach tajności.

7.4. Analiza i klasyfikacja mechanizmów ochrony danych w wybranym oprogramowaniu systemowym

W celu oceny możliwości spełnienia przez systemy informatyczne wymagań stawianych systemom przetwarzającym dane o zróżnicowanej klauzuli tajności poddano analizie wybrane systemy operacyjne, bazodanowe i portale. Na reprezentantów rodziny systemu operacyjnego wybrano system rodziny Unix i MS Windows 2000. Jako przedstawiciel baz danych został przeanalizowany system bazodanowy Oracle, zaś przykładowym portalem był MS IIS (Internet Information Services).

Analiza wykorzystania, przydatności wybranych reprezentantów została przeprowadzona na podstawie literatury [6, 7, 9, 10, 11, 12, 17, 18] oraz praktycznych doświadczeń pracowników firmy Milstar i materiałów, z których istotniejsze dokumenty zostały przedstawione w załącznikach.

System operacyjny rodziny Windows 2000

Podstawą ochrony przechowywanych i przetwarzanych danych w systemach rodziny Windows 2000 jest bezpieczeństwo systemu plików i poprawna autoryzacja użytkowników.

Bezpieczeństwo systemu plików opiera się na regułach i budowie systemu NTFS (New Technology File System), który jest rozwijany od momentu powstania systemu Windows NT. System plików NTFS daje możliwości konfigurowania uprawnień poufnych list kontroli dostępu do plików w strukturze NTFS, co stanowi listę upoważnień w tym systemie. Pozwala na tworzenie podstawowej kontroli dostępu potrzebnej do zabezpieczenia zasobów.

Bazując na liście upoważnień system sprawdza prawa dostępu użytkowników i aplikacji do plików lub procesów, które składają się na zbiór obiektów. Użytkownicy i aplikacje są w tym wypadku niczym innym jak podmiotami ubiegającymi o określony poziom dostępu do obiektów.

W systemie kontroli dostępu stosowanym w systemach MS Windows 2000 można zauważyć mocno rozwiniętą koncepcje hierarchii dostępu. W systemach rodziny Windows 2000 są zdeklarowane rożne grupy użytkowników, które zapewniają precyzyjnie

określony poziom dostępu do plików, usług i funkcji. Pomaga to w zarządzaniu uprawnieniami użytkowników. Zakres uprawnień i możliwości dostępu do plików i folderów zależy od poziomu dopuszczenia do odpowiednich klauzul tajności. Jednak jak się okazuje możliwy jest pośredni dostęp do poufnych danych z pominięciem wbudowanego w system mechanizmu kontroli dostępu.

Sprowadzając wyniki analizy do cech modelowych systemów ochrony danych, można stwierdzić, że w prezentowanym mechanizmie kontroli wyróżniono zbiory podmiotów, obiektów i reguł, które określa lista upoważnień. Mając na uwadze powyższe wyróżniki system ochrony danych w rodzinie produktów Windows 2000, w swej standardowej formie należy zaklasyfikować do grupy systemów sterowania dostępem.

Należy zwrócić również uwagę, na to, iż systemy rodziny Windows, z racji posiadanych licznych luk i błędów implementacyjnych, które zagrażają poufności, integralności oraz dostępności danych w nich przechowywanych i przetwarzanych, należą do systemów najczęściej atakowanych.

Opis wybranych cech systemu ochrony w Windows 2000 został zawarty w załączniku nr 2.

System operacyjny rodziny Unix

Podstawowym obiektem w systemie Unix jest plik. Pojęcie pliku jest w tym wypadku pojęciem bardzo szerokim. Swoje reprezentacje w postaci plików odpowiedniego typu mają różnorakie zasoby systemu, zarówno urządzenia dołączone do systemu, pamięć operacyjna, całe systemy plików jak i „zwykłe" pliki w systemie plików. W związku z tym kontrola dostępu do zasobów systemu omówiona będzie na przykładzie dostępu do pliku. Podmiotami ubiegającymi się do dostęp do obiektów są w tym wypadku użytkownicy, aplikacje i urządzenia, np. drukarka.

Prawa do plików są nadawane dla trzech rodzajów obiektów, tj. właściciela, grupy użytkowników związanych z plikiem (grupa ta jest nazywana właścicielem grupowym lub krócej grupa pliku) oraz całej reszty. W tym wypadku wymienione rodzaje obiektów składają się na strukturę hierarchii dostępu.

W systemie UNIX z każdym plikiem związana jest lista upoważnień z trzema pozycjami: pierwsza określa prawa dostępu właściciela, druga – prawa dostępu wszystkich użytkowników w grupie właściciela oraz trzecia – prawa dostępu wszystkich pozostałych użytkowników.

Systemy rodziny Unix choć są uważane za bezpieczne, posiadają ograniczenia oraz luki związane z kontrolą dostępu do przechowywanych i przetwarzanych w ich środowisku zasobów. Wynika to między innymi z małoelastycznego systemu nadawania uprawnień a jest to jeden z podstawowych aspektów bezpieczeństwa systemu Unix (kontroluje poziom dostępu do zasobów systemu).

Analizując prezentowany mechanizm kontroli wyróżniono zbiory podmiotów, obiektów, reguł, które określa lista upoważnień. Mając na uwadze powyższe wyróżniki można stwierdzić, iż systemy rodziny Unix w swej standardowej formie opierają się na mechanizmach sterowania dostępem.

Należy zwrócić również uwagę, na to, iż systemy rodziny Unix również posiadają cechy (podatności) zagrażające poufności oraz dostępności danych w nich przechowywanych i przetwarzanych.

Opisy wybranych cech analizowanego systemu oraz jego podatności zostały zawarte w załączniku nr 2.

System bazy danych Oracle

Mając na uwadze sposób działania bazy Oracle oraz jej strukturę można powiedzieć, iż w tym modelu ochrony podmiotami są użytkownicy lub procesy (usługi) chcące dostać się do danych przechowywanych w ramach obiektów. Obiektami są ogólnie rozumiane struktury pamięciowe (np. tabele, pliki zdarzeń) zaś rolę listy upoważnień pełnią uprawnienia i role obiektowe oraz systemowe. Rolami są odpowiednio zgrupowane uprawnienia posiadające swoje nazwy – występuje tu analogia do grup użytkowników posiadających zdefiniowany zbiór praw w systemach Windows. Można więc powiedzieć, że poprzez role system Oracle rozwiązuje kwestię hierarchii dostępu. Wynika z tego, że przedstawiony sposób ochrony odpowiada modelowi sterowania dostępem.

Warto wspomnieć, iż w sytuacjach próby nadużycia, obiektem do którego podmiot stara się zdobyć uprawnienia może stać się również demon lub usługa, która może być następnie wykorzystana jako narzędzie dostępu do właściwych danych. Częstymi przykładami takiego zachowania jest wykorzystywanie usługi Listener w celu nieupoważnionego dostępu do danych.

Poza systemem ochrony, którego działanie wynika z założeń projektowych a nie błędów implementacyjnych, należy ocenić inne elementy mające wpływ na jakość zabezpieczeń informacji przechowywanej w bazach Oracle. Otóż występują w nich liczne luki wynikające z nieodpowiedniego zaprojektowania systemu (np. podatności usługi Listener) oraz błędów implementacyjnych (np. opisany w załączniku brak czyszczenia bufora, który może doprowadzić do ujawnienia informacji przekazywanej w poprzednim połączeniu). Przykładowe możliwe sposoby naruszeń poufności danych w tym systemie potwierdzają tezę, iż jest to system sterowania dostępem.

Przykładowe podatności systemu Oracle zostały omówione w załączniku nr 2.

System portalowy MS Internet Information Services

Mechanizmy ochrony danych stosowane w systemach portalowych najczęściej wykorzystują zabezpieczenia analogiczne do zabezpieczeń systemu operacyjnego, w środowisku którego działają oraz systemów bazodanowych, z których dane publikowane są w ramach tychże portali.

Zawarte w załączniku nr 2 przykładowe sposoby naruszeń poufności danych w tego rodzaju systemie potwierdzają tezę, iż jest to system sterowania dostępem. W przypadku tego typu systemów jest to metoda niewystarczająca. Jest to związane z bezpośrednią dostępnością tego typu serwisów z Internetu oraz przekazywaniem poufnych danych do przeglądarki użytkownika. Przeglądarka nierzadko wchodzi w za-

awansowaną interakcję z systemem portalowym uruchamiając po obu stronach kody i aplikacje, które mogą być kanałem wycieku poufnych danych. Wspomniane kody i aplikacje, uruchamiane często z wysokimi uprawnieniami powinny być szczegółowo kontrolowane, co nie jest możliwe w przypadku systemów sterowania dostępem.

Dużym zagrożeniem dla poufności danych udostępnianych w ramach portali są przeglądarki Internetowe, które nawet w przypadku szyfrowanych transmisji tworzą jawne wpisy w swoich plikach tymczasowych zapisywanych na stacji roboczej, z której inicjowane jest połączenie. Pliki te w wielu wypadkach nie są usuwane i w sytuacji gdy do tego komputera będą miały dostęp inne osoby, to będą one mogły zapoznać się z informacjami przechowywanymi w tych plikach. Należy podkreślić, iż mogą tam trafić informacje o rożnych klauzulach tajności, a dostęp do nich następuje na zasadach ogólnych, najczęściej bez jakiejkolwiek weryfikacji użytkownika a tym bardziej poziomu jego dopuszczeń.

Podobnym zagrożeniem związanym z dostępem do danych przez przeglądarkę Internetową może być występowanie na drodze od serwera do klienta serwerów proxy, które w celu przyspieszenia pobierania informacji ze stron WWW zapisują w plikach tymczasowych najczęściej odwiedzane strony. Cache-owanie stron WWW (tak potocznie nazywa się ten proces) umożliwia późniejsze ich pobranie z lokalnego serwera, co znacznie poprawia szybkość działania, ale z drugiej strony stanowi duże zagrożenie dla poufności danych. W przypadku np. włamania do systemu takiego serwera wszystkie poufne informacje pochodzące ze stron WWW mogą być dostępne dla napastnika.

Przy okazji omawiania systemów portalowych, należy chociaż krótko wspomnieć o sieciach teleinformatycznych, które stanowią medium łączące przeglądarkę internetową z portalem.

Prawidłowe zabezpieczenie danych przesyłanych przez sieci teleinformatyczne przy uwzględnieniu potrzeby współpracy współdziałania (interoperacyjności) różnych systemów informatycznych wykorzystywanych przez administrację publiczną stanowi złożone zadanie. Poufne dane w opisywanym przypadku przesyłane są publicznymi łączami, w związku z tym istnieje realne zagrożenie związane z przechwyceniem ich, odczytaniem lub zmodyfikowaniem. Zagrożenie to można zminimalizować lub praktycznie wykluczyć stosując szyfrowanie przesyłanych informacji. Niestety nie wszystkie aplikacje komunikując się np. z serwerem umożliwiają szyfrowanie przesyłanych informacji. W takim przypadku konieczne jest zastosowanie dodatkowych narzędzi programowych lub (i) sprzętowych, które wymuszą szyfrowanie informacji przed jej wysłaniem przez sieć teleinformatyczną.

W tym miejscu należy wspomnieć, że złą praktyką jest darzenie zbyt dużym zaufaniem produktów, których podstawowym celem jest zapewnienie bezpieczeństwa informacji. Wielu użytkowników i nawet administratorów podświadomie, bezgranicznie wręcz wierzy w poprawność działania tunelu kryptograficznego, jeśli skorzysta z popularnych narzędzi do jego zestawienia. Okazuje się jednak, że i tego typu programy nie są wolne od błędów i tak np. OpenSSL w wersjach 0.9.7 i wcześniejszych

posiada luki pozwalające na wykonanie dowolnego kodu w ramach zdalnego systemu z uprawnieniami użytkownika korzystającego z bibliotek OpenSSL (w niektórych przypadkach, takich jak „sendmail" jest to root).

Uogólnienie analizy

Pierwszym i najistotniejszym wnioskiem z analizy jest ocena klasy systemów operacyjnych i baz danych wykorzystywanych w administracji publicznej. W systemach informatycznych wykorzystywanych w administracji publicznej stosuje się mechanizmy ochrony danych stanowiące standardowe wyposażenie zastosowanych systemów operacyjnych i systemów baz danych. Mechanizmy te w swej istocie są oparte na koncepcji sterowania dostępem a nie przepływem, w których reguła upoważnienia dowolnego żądania dostępu do danych polega na sprawdzeniu w macierzy dostępu czy istnieje reguła dopuszczająca jego realizację. W ten sposób (w pewnym uproszczeniu) reguluje się dostęp obiektów aktywnych (przede wszystkim użytkowników) do obiektów pasywnych (przede wszystkim danych). Nie ma w tych systemach mechanizmu sterowania przepływem, które jasno i szczegółowo określałyby prawa rozpowszechniania informacji, bez względu na to, jakie obiekty zawierają informacje.

Analizując kolejne cechy przykładowych systemów operacyjnych i bazodanowych można stwierdzić, iż w aktualnym modelu eksploatacji systemów informatycznych informacje o różnych klauzulach tajności znajdują się „obok siebie", tzn. ta sama baza danych przechowuje informacje o rożnych poziomach tajności, także ta sama przestrzeń dyskowa, katalogowa przeznaczona na pliki tymczasowe przechowuje informacje o rożnych klauzulach tajności. Prowadzi to do kłopotliwych sytuacji w trakcie korzystania z takiej bazy lub plików tymczasowych. Dzieje się tak ponieważ przy dostępie do informacji o niższej klauzuli tajności (zakładając, że obiekt, który zamierza z nich skorzystać posiada stosowne dopuszczenie), które stanowią fragment większego zbioru informacji (w skład którego wchodzą również informacje o wyższych klauzulach tajności) trudno odpowiednio zabezpieczyć dane, do których użytkownik nie powinien mieć wglądu. Całą sytuację komplikuje dodatkowo fakt, iż informacje elementarne przechowywane lub przetwarzane w ten sposób można traktować jako zbiory informacji, nierzadko połączonych między sobą pewnymi relacjami. Analizowane systemy nie potrafią właściwie reagować na zmianę klauzuli danych w postaci zbiorczej.

Co gorsze, opisane powyżej własności standardowych systemów informatycznych nie wynikają z błędnej ich implementacji, lecz z założeń opisujących ich funkcjonowanie, które przyjęte zostały na etapie ich projektowania. W związku z tym zmiana koncepcji działania tych systemów jest prawie niemożliwa. Jednak poprzez świadome administrowanie i korzystanie z nich można w znacznym stopniu zredukować ich podatności.

Kolejne cechy systemów informatycznych, które mają wpływ na obniżenie poziomu bezpieczeństwa danych, stanowią podatności wynikające z błędów implementacji i nieodpowiedniej konfiguracji stosowanych systemów.

7.5. Wnioski

Analizując działanie przykładowych systemów informatycznych wykorzystywanych do przechowywania i przetwarzania danych o rożnych klauzulach tajności można ogólnie stwierdzić (nie odnosząc się na tym etapie do żadnego konkretnego rozwiązania), że:

- analizowane systemy informatyczne stosowane do przetwarzania danych niejawnych nie dysponują skutecznymi mechanizmami sterowania przepływem (kontroli przepływu),
- istnieją miejsca np. pliki tymczasowe aplikacji, w których może dojść do naruszenia poufności chronionych informacji,
- wiele błędów związanych z ujawnieniem wrażliwych danych nie wynika z błędnego sterowania dostępem, lecz braku polityki sterowania przepływem informacji,
- wszystkie z analizowanych systemów wymagają stałej opieki mającej na celu usuwanie wykrywanych błędów i w ten sposób redukowanie występujących podatności,
- systemy w standardowej swojej konfiguracji nie dysponują mechanizmami silnego uwierzytelniania,
- systemy nie mają zaimplementowanej logiki pozwalającej na automatyczne nadzorowanie i w razie potrzeby modyfikowanie klauzuli tajności np. w stosunku do informacji zmieniającej formę przechowywania,
- ochrona sieci wymaga kombinacji szyfrowania i innych mechanizmów ochronnych. Szyfrowanie jest niezbędne, aby chronić dane, których transmisja w sieci jest dozwolona. Sterowanie przepływem informacji jest potrzebne, aby zapobiegać nieupoważnionemu rozpowszechnianiu w sieci danych niejawnych. Sterowanie dostępem jest niezbędne, aby przeciwdziałać nieupoważnionemu dostępowi do procedur zarządzania kluczami, do dzielonych baz danych i urządzeń. Jest również niezbędne ze względu na niezawodność, ponieważ uszkodzenie jednego węzła w sieci nie powinno spowodować przerwania pracy całej sieci,
- ponieważ informacje wysyłane przez sieci komputerowe (szczególnie przez publiczne sieci WAN) muszą być bezwzględnie szyfrowane, przy dużej ilości wymienianych w ten sposób informacji, bez wsparcia w postaci właściwego sprzętu i oprogramowania proces ten może stanowić duże utrudnienie organizacyjne i techniczne, uniemożliwiające wręcz osiągnięcie odpowiedniego poziomu interoperacyjności systemów administracji publicznej.

Podkreślając najważniejszy wniosek wynikający z przeprowadzonej analizy a mianowicie, że większość systemów informatycznych stosowanych do przetwarzania danych niejawnych nie dysponuje skutecznymi mechanizmami sterowania przepływem tych danych, należy wymienić skutki stosowania takich systemów do przetwarzania informacji o rożnych klauzulach tajności. Przetwarzanie i przechowywanie tego typu informacji w analizowanych systemach może prowadzić do:

- niekontrolowanego, nielegalnego przepływu danych niejawnych do miejsc i osób nie posiadających uprawnień do ich otrzymania,

- konieczności zaniechania potrzebnego przetwarzania danych niejawnych, zwłaszcza gdy mają być przetwarzane dane o różnych klauzulach niejawności lub doprowadzenia do świadomego albo nieświadomego przetwarzania danych z naruszeniem ustawy,
- uniemożliwienia bezpiecznej współpracy z innymi zewnętrznymi lub wewnętrznymi systemami rejestrowymi.

8. Model identyfikacji i szacowania kosztów ochrony przetwarzania informacji o różnych klauzulach tajności

8.1. Opis struktury kosztów systemów przetwarzających informacje niejawne

8.1.1. Elementy kosztów przetwarzania informacji

W przedstawionym wcześniej formalnym modelu przetwarzania informacji, wystąpiły takie zasadnicze kategorie pojęciowe jak: informacje, ich poufność oraz wymagania na system informatyczny realizujący procesy przetwarzania. Wymagania te zależne są od wartości miar poufności (wg nazewnictwa ustawowego: od klauzul tajności). Aby im sprostać, elementy systemu informatycznego muszą być do wymagań dostosowane. Ma to istotny wpływ na koszty przetwarzania informacji. Niniejszy rozdział poświęcony jest temu zagadnieniu.

Koszty przetwarzania informacji wiążą się z fazą cyklu życia systemu, który realizuje zadania przetwarzania informacji:

- Nakłady inwestycyjne ponoszone w trakcie budowy systemu. Obejmują one:
  - Koszty planowania przedsięwzięcia.
  - Koszty przygotowawcze.
  - Koszty finansowania inwestycji.
  - Koszty projektowania systemu.
  - Koszty sprzętu i oprogramowania.
  - Koszty wdrożenia systemu.
  - Koszty szkolenia użytkowników.
- Koszty eksploatacji systemu podczas realizacji procesów przetwarzania informacji.
  - Koszty te można rozpatrywać w dowiązaniu do poszczególnych procesów przetwarzania informacji. Zgodnie z klasyfikacją wprowadzoną w modelu przetwarzania informacji będą to więc koszty:
    a) Pozyskiwania informacji.
    b) Przesyłania informacji.
    c) Gromadzenia informacji.
    d) Utrzymywania informacji.
    e) Przetwarzania danych.
    f) Unicestwiania danych.

– Na koszty realizacji poszczególnych procesów przetwarzania składają się koszty realizującego je systemu informatycznego. Przy tym, przez system informatyczny rozumiemy także wiele systemów informatycznych współdziałających. Traktujemy, że podział na podsystemy bądź moduły systemu są w pewnym stopniu umowne. W sytuacji, gdy rozpatruje się przetwarzanie informacji o różnych klauzulach tajności (ogólniej: różnych wartościach miar poufności) takie podejście jest tym bardziej zasadne – przetwarzanie określonych grup informacji może być separowane, aż do wyodrębnienia oddzielnego systemu informatycznego. Te koszty poklasyfikujemy według rodzajów kosztów, ale w przystosowaniu do problematyki poufności:
  a) Koszty infrastruktury technicznej systemu informatycznego;
  b) Koszty organizacyjne
     1. Koszty osobowe,
     2. Koszty lokalowe (pomieszczenia z infrastrukturą, wyposażenie),
     3. Koszty zadań kontrolnych (także audyty, analizy ryzyka);
  c) Koszty dokumentacji;
  d) Koszty usług obcych;
  e) Koszty pozostałe – nie zaliczone do wyróżnionych powyżej klas.

Podkreślmy jeszcze raz, że składniki kosztów w ostatniej specyfikacji czyli według rodzajów wyodrębnione są tendencyjnie, z akcentowaniem tych składników, na które najmocniej wpływać może charakterystyka przetwarzanej informacji pod względem jej poufności.

W zależności od celu, dla jakiego określamy koszty przetwarzania informacji, możemy je wiązać z różnym okresem. Najczęściej stosuje się dwie metody:

- Koszty na cały okres życia systemu. Jako okres obliczeniowy przyjmuje się przewidywany czas funkcjonowania systemu (systemów), bądź umowny okres wynikający z praktyki lub wzorców normatywnych. Przy tym podejściu określa się koszty jako sumę nakładów inwestycyjnych i kosztów eksploatacji systemu realizującego procesy przetwarzania w tym okresie.
- Koszty roczne. Wówczas do kosztów eksploatacyjnych rocznych dodaje się przypadającą na jeden rok część nakładów inwestycyjnych – najczęściej według reguł stosowanych w amortyzacji.

Rozpatrzmy drugie spośród wymienionych wyżej podejść. Łączne nakłady inwestycyjne zostają na zasadzie proporcjonalnego narzutu dodane do faktycznych kosztów rocznych danego składnika. Przy precyzyjniejszych wyliczeniach koszty inwestycyjne odnoszące się do rzeczowych składników, mogą być dodane do poszczególnych procesów przetwarzania informacji (zamiast proporcjonalnego narzutu).

Oszacowanie – szczególnie niektórych – elementów macierzy kosztów może nastręczać poważne trudności. Dotyczy to np. kosztów „struktur organizacyjnych" z przypisaniem ich do określonego systemu informatycznego. W proponowanym modelu wskazano na najważniejsze składniki, które mają największy wpływ na koszty w związku z przetwarzaniem informacji poufnej, abstrahując od trudności związanych

z określeniem ich wartości liczbowych. Początkowo oszacowania mogą być zgrubne, sukcesywnie polepszane na drodze gruntowniejszych badań statystycznych i innych.

W rezultacie szacowany koszt przetwarzania ma strukturę macierzową, jak poniżej:

Koszty ponoszone w ramach:	Pozyskiwanie informacji, przesyłanie informacji, gromadzenie informacji, utrzymywanie informacji, przetwarzanie danych, udostępnianie informacji, unicestwianie danych						
Infrastruktura techniczna SI	$k_0[1,1]$	$k_0[1,2]$	$k_0[1,3]$	$k_0[1,4]$	$k_0[1,5]$	$k_0[1,6]$	$k_0[1,7]$
Koszty osobowe	$k_0[2,1]$	$k_0[2,2]$	$k_0[2,3]$	$k_0[2,4]$	$k_0[2,5]$	$k_0[2,6]$	$k_0[2,7]$
Koszty lokalowe	$k_0[3,1]$	$k_0[3,2]$	$k_0[3,3]$	$k_0[3,4]$	$k_0[3,5]$	$k_0[3,6]$	$k_0[3,7]$
Zadania kontrolne	$k_0[4,1]$	$k_0[4,2]$	$k_0[4,3]$	$k_0[4,4]$	$k_0[4,5]$	$k_0[4,6]$	$k_0[4,7]$
Dokumentacja	$k_0[5,1]$	$k_0[5,2]$	$k_0[5,3]$	$k_0[5,4]$	$k_0[5,5]$	$k_0[5,6]$	$k_0[5,7]$
Usługi obce	$k_0[6,1]$	$k_0[6,2]$	$k_0[6,3]$	$k_0[6,4]$	$k_0[6,5]$	$k_0[6,6]$	$k_0[6,7]$
Pozostałe	$k_0[7,1]$	$k_0[7,2]$	$k_0[7,3]$	$k_0[7,4]$	$k_0[7,5]$	$k_0[7,6]$	$k_0[7,7]$

Szacunek łącznych kosztów przetwarzania informacji przez system (systemy) może być dokonany jako suma oszacowań wszystkich elementów powyższej macierzy będących składnikami kosztów:

$$K_0 = \sum_i \sum_j k_0[i,j]$$

8.1.2. Koszty przetwarzania informacji niejawnych – jedna miara poufności

Poprzedni punkt traktował o ocenie kosztów przetwarzania informacji abstrahując od ich poufności (klauzul tajności). Dla każdego systemu realizującego procesy przetwarzania informacji występują składniki kosztów, jakie tam wyszczególniono. Ale ich wysokość zmienia się, gdy realizacja przetwarzania związana jest z funkcjonowaniem systemu bezpieczeństwa, przed którym postawione są szczególne wymagania ze względu na niejawność przetwarzanej w danym systemie (w danych systemach) informacji.

Najpierw przeanalizujmy sytuację, gdy system informatyczny przetwarza informacje poufne o jednakowych wartościach miar poufności. Przy tym poufność uwzględniamy w jednej płaszczyźnie, czyli mamy do czynienia z jedną tylko miarą poufności. Taka sytuacja jest nieco hipotetyczna, ale pozwoli to skupić się na jednolitym wpływie poufności informacji na procesy ich przetwarzania.

W niniejszej publikacji nie analizuje się konkretnych architektur wykonawczych realizujących procesy przetwarzania informacji. Nie będą więc tutaj wyszczególniane elementy, które muszą się zmienić dla zapewnienia funkcjonowania systemu bezpieczeństwa. Odnotowujemy jedynie, że zmiany będą polegać na jednej z dwóch wersji:

- Wystąpią te same elementy wykonawcze (w ogólnym sensie, a więc zarówno techniczne, jak i organizacyjne) o zwiększonych możliwościach, które są konieczne

ze względu na podwyższone wymagania formułowane dla zapewnienia bezpieczeństwa informacyjnego.

- Wystąpią dodatkowe elementy wykonawcze, które nie występują przy przetwarzaniu informacji jawnych.

W wyrazie finansowym można to przedstawić jak poniżej.

Poszczególne składniki kosztów występujące we wprowadzonej wyżej macierzy kosztów będą miały następującą strukturę wewnętrzną:

$$k[i, j] = w_0 [i, j] \times k_0 [i, j] + k_d [i, j]$$

gdzie:

$k_0 [i, j]$ – koszt [i, j]-tego elementu macierzy kosztów, gdy przetwarzaniu podlegają jedynie informacje jawne,

$w_0 [i, j]$ – współczynnik wzrostu kosztu [i, j]-tego elementu macierzy kosztów, gdy przetwarzaniu podlegają informacje poufne w stosunku do kosztu $k_0 [i, j]$, z uwzględnieniem jedynie tych samych elementów wykonawczych systemu informatycznego, które występowały także przy przetwarzaniu informacji jawnych,

$k_d [i, j]$ – addytywny wzrost kosztu [i, j]-tego elementu macierzy kosztów, gdy przetwarzaniu podlegają informacje poufne, z uwzględnieniem jedynie tych elementów wykonawczych systemu informatycznego, które nie występowały przy przetwarzaniu informacji jawnych.

Dla uzyskania wygodniejszego do obliczeń wyrażenia, wprowadźmy współczynnik wzrostu kosztu uwzględniający zarówno podwyższenie standardu nie zamienionych elementów wykonawczych, jak i dodatkowe elementy wykonawcze:

$$w[i, j] = w_0 [i, j] + k_d [i, j] / k_0 [i, j]$$

Uzyskujemy wówczas postać wyrażenia na **poszczególne składniki kosztów** występujące w macierzy kosztów:

$$k[i, j] = w [i, j] \times k_0 [i, j]$$

W rezultacie łączne koszty przetwarzania informacji poufnych przez system informatyczny wyrażają się wzorem:

$$K = \sum_i \sum_j w[i, j] \times k_0[i, j]$$

8.1.3. Koszty przetwarzania informacji niejawnych – wiele miar poufności

W kolejnym kroku przeanalizujmy sytuację, gdy system informatyczny przetwarza informacje poufne o jednakowych wartościach miar poufności, ale poufność uwzględniamy w wielu płaszczyznach, czyli mamy do czynienia z wieloma miarami poufności. Taka sytuacja także jest hipotetyczna. Prawie zawsze przetwarzane informacje nie są tak jednolite, aby pod każdym względem były jednakowo poufne względem siebie. Jeżeli mają tę samą wartość jednej miary poufności (np. jednakową klauzulę niejawności), to zwykle różnią się wartością innej miary poufności (np. z punktu widzenia ochrony danych osobowych).

Dla oszacowania łącznych kosztów sytuacja obliczeniowa nie zmienia się w stosunku do poprzednio analizowanej sytuacji, czyli przy poufności według jednej miary. Czyli:

$$K = \sum_i \sum_j w[i,j] \times k_0[i,j]$$

Ale współczynnik **w [i, j]** uwzględniać musi łączne wpływy wymagań formułowane z punktu widzenia wszystkich płaszczyzn poufności na elementy systemu informatycznego uwzględniane w [i, j]-tym elemencie macierzy kosztów.

Taka postać wyrażenia kosztów przetwarzania informacji niejawnych w sytuacji uwzględniania wielu miar poufności nie pozwala badać wpływu odrębnie w poszczególnych płaszczyznach poufności. Rozpatrzmy inny schemat szacowania kosztów.

W schemacie takim ustalamy kolejność rozpatrywania wzrostu kosztów w wyniku uwzględnienia wymagań z punktu widzenia danego wymiaru przestrzeni poufności.

Załóżmy, że w P-wymiarowej przestrzeni poufności uwzględnione już zostały wpływy 'p' miar poufności. Rozpatrujemy (p+1)-tą miarę. Ustalamy jakie wymagania na elementy systemu informatycznego uwzględniane w [i, j]-tym elemencie macierzy kosztów są dodatkowe w stosunku do wymagań wszystkich poprzedzających 'p' miar.

$$k_{p+1}[i,j] = w_{p+1}[i,j] \times k_p[i,j]$$

(Przykładowo dla miary umiejscowionej w pierwszej kolejności wyrażenie przyjmuje postać: $k_1[i,j] = w_1[i,j] \times k_0[i,j]$; odpowiednio dla miary umiejscowionej w ostatniej kolejności (czyli P-tej): $k_P[i,j] = w_P[i,j] \times k_{P-1}[i,j]$.)

Zauważmy, że $\mathbf{k_P}$ **[i, j]** (indeks: wielkie P) jest poszukiwanym [i, j]-tym składnikiem macierzy kosztów **k [i, j]** – albowiem w kolejnych krokach uwzględniony został wpływ wszystkich miar poufności.

W rezultacie otrzymujemy:

$$w[i,j] = w_1[i,j] \times w_2[i,j] \times \ldots \times w_p[i,j] \times \ldots \times w_P[i,j]$$

Kolejne współczynniki wskazują na wzrost [i, j]-tego elementu macierzy kosztów, spowodowany uwzględnieniem wymagań dodatkowych w stosunku do łącznych wymagań wszystkich poprzednio uwzględnionych wymagań. Poszczególnych współczynników nie można traktować jako oceny wpływu danej miary poufności na koszty, bo zależne są od ustalonej arbitralnie kolejności rozpatrywania wymagań. W pełni obrazuje ten wpływ jedynie miara umiejscowiona w pierwszej kolejności oraz łączny wpływ wszystkich miar poufności.

W rezultacie dochodzimy do standardowej postaci wyrażenia na koszt łączny, czyli:

$$K = \sum_i \sum_j w[i,j] \times k_0[i,j]$$

ale mając wcześniej ustaloną strukturę wewnętrzną na współczynniki **w [i, j]** obrazującą, poprzez swą mnożnikową postać, narastanie wpływu kolejnych miar poufności, w stosunku do już poprzednio uwzględnionych.

8.1.4. Koszty przetwarzania informacji o różnych klauzulach tajności

Sytuacje z jakimi się spotykamy w praktyce są niestety jeszcze bardziej złożone niż rozważane w poprzednich punktach. Można je scharakteryzować następująco:

- Uwzględniać musimy wiele miar poufności. Niektóre z nich wynikają z obowiązku przestrzegania przepisów prawnych (ogólnych lub branżowych). Obowiązek ten jest spożytkowany przez ustalenia nakazowej polityki bezpieczeństwa informacyjnego. Inne wynikają z samodzielnej analizy semantyki przetwarzanych informacji oraz analizy zagrożeń, powodując uwzględnienie innych jeszcze płaszczyzn poufności – dając podstawy do uszczelniającej polityki bezpieczeństwa informacyjnego.
- Przetwarzane informacje mają różne wartości miar poufności. Przy tym podział informacji na grupy o jednakowych wartościach dla jednej miary poufności jest zwykle różny od podziału dla innej miary.

Dokonajmy zabiegu polegającego na tym, że dzielimy wszystkie zasoby informacyjne przetwarzane w systemie informatycznym na takie grupy, że w jednej grupie znajdują się informacje o jednakowych wartościach wszystkich uwzględnianych miar poufności. Założono w tym miejscu, że wartości miar poufności są dyskretne (a nie ciągły zbiór wartości z przedziału [0, 1]). Takich grup informacji będzie więc określona liczba.

Dla poszczególnych grup informacji otrzymaliśmy więc sytuację prawie analogiczną do opisanej w poprzednim punkcie za jednym wyjątkiem. Wyjątek ten jest jednak istotny. W poprzednim punkcie z określonymi (w rozumieniu poufności) zasobami informacyjnymi i z określonymi procesami przetwarzania kojarzony był określony system informatyczny ze swoimi elementami wykonawczymi, decydującymi o poszczególnych składnikach macierzy kosztów. Przy zróżnicowanych, pod względem poufności, zasobach informacyjnych poszczególne elementy systemu informatycznego mogą być wykorzystywane rozłącznie dla wyodrębnionych grup informacji. Ze względu na rozłączność, niektóre elementy systemu informatycznego mogą być zdublowane (nawet zwielokrotnione). Wystąpić także mogą elementy systemu informatycznego zapewniające spójność przetwarzania w sytuacji rozdzielenia określonych faz procesów przetwarzania. Niektóre zaś elementy systemu informatycznego będą wspólnie używane i ich koszt musi być rozłożony na części przypisane przetwarzaniu poszczególnych grup informacji. W rezultacie proponujemy poniżej opisany schemat obliczeniowy.

Dla [i, j]-tego elementu macierzy kosztów, w miejsce pierwotnej wyceny k_0 [i, j], a więc tego składnika kosztów, który wynikał bezpośrednio z elementów systemu informatycznego, uwzględnianych w tym miejscu, potrzebnych do realizacji przetwarzania informacji jawnych, wprowadza się koszt zmodyfikowany wyznaczony według struktury:

$$km_0^g [i, j] = k_0 [i, j] \times u^g [i, j] \times w_w [i, j]$$

gdzie:

$km_0^g[i, j]$ – koszt zmodyfikowany [i, j]-tego elementu macierzy kosztów dla g-tej grupy informacji,

$k_0[i, j]$ – koszt [i, j]-tego elementu macierzy kosztów, gdy przetwarzaniu podlegają jedynie informacje jawne,

$u^g[i, j]$ – udział w kosztach [i, j]-tego elementu macierzy kosztów z tytułu współdzielenia elementów systemu informatycznego „przypadający" na g-tą grupę informacji. Koncepcje podziału kosztów mogą być różne, ale przy spełnieniu warunku, że dla wszystkich [i, j] elementów macierzy kosztów:

$$\sum_g u^g[i, j] = 1$$

$w_w[i, j]$ – współczynnik wzrostu kosztu [i, j]-tego elementu macierzy kosztów ze względu na zwielokrotnienie niektórych elementów systemu informatycznego po rozdzieleniu procesu przetwarzania informacji. W rezultacie dla [i, j]-tego elementu macierzy kosztów bierzemy do dalszych obliczeń wartość $k_0[i, j] \times w_w[i, j]$ zamiast $k_0[i, j]$.

Dla uproszczenia schematu obliczeniowego wprowadźmy współczynnik $w_r^g[i, j]$, który uwzględnia łącznie wpływ na koszty z tytułu:

- współdzielenia niektórych elementów systemu informatycznego przez różne grupy informacji, poprzez uwzględnienie współczynnika udziału g-tej grupy informacji w kosztach $u^g[i, j]$,
- dublowania niektórych elementów systemu informatycznego, poprzez uwzględnienie współczynnika $w_w[i, j]$.

$$w_r^g[i, j] = u^g[i, j] \times w_w[i, j]$$

Trzeba jeszcze wrócić do współczynnika $w[i, j]$, zdefiniowanego w poprzednim punkcie, a który oznacza wzrost kosztów przy uwzględnieniu wszystkich wymiarów przestrzeni poufności w stosunku do kosztów przetwarzania informacji jawnych. Te współczynniki określane są w sytuacji konkretnych wartości miar poufności, a więc muszą być skojarzone z konkretną grupą informacji wyodrębnionej w omawianym schemacie obliczeniowym (w poprzednim punkcie mieliśmy do czynienia z założenia z jedną grupą informacji). Tak więc w nowej postaci w wyrażeniu dodajemy indeks grupy 'g':

$$w^g[i, j] = w_1^g[i, j] \times w_2^g[i, j] \times \ldots \times w_p^g[i, j] \times \ldots \times w_P^g[i, j]$$

W rezultacie dla wyodrębnionej grupy informacji (przypomnijmy: wyodrębnionej z punktu widzenia równości wartości wszystkich miar poufności) koszty przetwarzania wynoszą:

$$K[g] = \sum_i \sum_j w^g[i, j] \times w_r^g[i, j] \times k_0[i, j]$$

Poza kosztami, które można kojarzyć z wyodrębnionymi grupami informacji występują koszty, które są ogólnymi w stosunku do poszczególnych grup a wynikają

z tego, że procesy przetwarzania zostały rozdzielone. Nazwijmy je kosztami zapewnienia spójności, a więc:

k_s [i, j] – addytywny wzrost kosztu [i, j]-tego elementu macierzy kosztów ze względu na konieczność zapewnienia spójności przetwarzania.

Ostatecznie łączny koszt przetwarzania informacji zróżnicowanych pod względem poufności przez system informatyczny wynosi:

$$K = \sum_i \sum_j (k_s[i,j] + \sum_g w^g[i,j] \times w_r^g[i,j] \times k_0[i,j])$$

gdzie:

w^g [i, j] – współczynnik wzrostu [i, j]-tego elementu macierzy kosztów przy przetwarzaniu informacji g-tej grupy uwzględniający:

- wpływ wszystkich miar P-wymiarowej przestrzeni poufności w ramach g-tej grupy informacji,
- wpływ na wzrost kosztów ze względu na wyższe wymagania stawiane elementom systemu informatycznego,
- wpływ na wzrost kosztów ze względu na konieczność zastosowania dodatkowych elementów systemu informatycznego dla zapewnienia funkcjonowania systemu bezpieczeństwa informacyjnego.

w_r^g [i, j] – współczynnik wzrostu [i, j]-tego elementu macierzy kosztów przy przetwarzaniu informacji g-tej grupy uwzględniający:

- wpływ na wzrost kosztów ze względu na zwielokrotnienie niektórych elementów systemu informatycznego przy przetwarzaniu informacji o różnych wartościach miar poufności,
- udział w kosztach „przypadający" na g-tą grupę informacji przy współużytkowaniu elementów systemu informatycznego.

k_s [i, j] – addytywny wzrost kosztu [i, j]-tego elementu macierzy kosztów ze względu na konieczność zapewnienia spójności przetwarzania przy rozdzieleniu niektórych faz przetwarzania ze względu na różnorodność informacji pod względem poufności.

Dla wykonania obliczeń według tego schematu będą potrzebne po dwie macierze współczynników dla każdej wyodrębnionej grupy informacji. Ponadto macierz bazowa kosztów przetwarzania informacji jawnych oraz macierz dodatkowych kosztów ze względu na konieczność zapewnienia spójności przetwarzania. Struktura tych macierzy analogiczna jak przedstawiona w pkt 8.1.1.

8.2. Model struktury kosztów systemów przetwarzających informacje niejawne

Model został wprowadzony metodą kolejnych kroków, poczynając od specyfikacji składowych kosztów w sytuacji przetwarzania informacji wyłącznie jawnych, poprzez stopniowe różnicowanie poufności przetwarzanych informacji, do formuł obliczeniowych w sytuacji przetwarzania informacji o różnych wartościach miar poufności rozpatrywanych w wielowymiarowej przestrzeni poufności.

Poniżej przedstawiamy proponowany schemat obliczeniowy przywołując sukcesywnie potrzebne do obliczeń dane liczbowe.

Rozpoczynamy od macierzy kosztów przetwarzania informacji jawnych.

Koszty ponoszone w ramach:	Pozyskiwanie informacji, przesyłanie informacji, gromadzenie informacji, utrzymywanie informacji, przetwarzanie danych, udostępnianie informacji, unicestwianie danych						
Infrastruktura techniczna SI	$k_0[1,1]$	$k_0[1,2]$	$k_0[1,3]$	$k_0[1,4]$	$k_0[1,5]$	$k_0[1,6]$	$k_0[1,7]$
Koszty osobowe	$k_0[2,1]$	$k_0[2,2]$	$k_0[2,3]$	$k_0[2,4]$	$k_0[2,5]$	$k_0[2,6]$	$k_0[2,7]$
Koszty lokalowe	$k_0[3,1]$	$k_0[3,2]$	$k_0[3,3]$	$k_0[3,4]$	$k_0[3,5]$	$k_0[3,6]$	$k_0[3,7]$
Zadania kontrolne	$k_0[4,1]$	$k_0[4,2]$	$k_0[4,3]$	$k_0[4,4]$	$k_0[4,5]$	$k_0[4,6]$	$k_0[4,7]$
Dokumentacja	$k_0[5,1]$	$k_0[5,2]$	$k_0[5,3]$	$k_0[5,4]$	$k_0[5,5]$	$k_0[5,6]$	$k_0[5,7]$
Usługi obce	$k_0[6,1]$	$k_0[6,2]$	$k_0[6,3]$	$k_0[6,4]$	$k_0[6,5]$	$k_0[6,6]$	$k_0[6,7]$
Pozostałe	$k_0[7,1]$	$k_0[7,2]$	$k_0[7,3]$	$k_0[7,4]$	$k_0[7,5]$	$k_0[7,6]$	$k_0[7,7]$

Na podstawie danych powyższej macierzy otrzymujemy łączny koszt przetwarzania informacji jawnych. Jest to punkt odniesienia przy ocenie wpływu poufności na koszty.

$$K_0 = \sum_i \sum_j k_0[i,j]$$

Po podzieleniu przetwarzanych informacji na 'G' grup, w których informacje mają jednakowe wartości wszystkich 'P' miar poufności, uwzględnić trzeba współczynniki zebrane dla każdej grupy (g: 1, 2, ... , G) w dwóch macierzach.

Macierz współczynników wzrostu kosztu przetwarzania uwzględniających podwyższenie standardu niektórych elementów systemu informatycznego oraz dodanie innych (dla g-tej grupy informacji).

Koszty ponoszone w ramach:	Pozyskiwanie informacji, przesyłanie informacji, gromadzenie informacji, utrzymywanie informacji, przetwarzanie danych, udostępnianie informacji, unicestwianie danych						
Infrastruktura techniczna SI	$w^g[1,1]$	$w^g[1,2]$	$w^g[1,3]$	$w^g[1,4]$	$w^g[1,5]$	$w^g[1,6]$	$w^g[1,7]$
Koszty osobowe	$w^g[2,1]$	$w^g[2,2]$	$w^g[2,3]$	$w^g[2,4]$	$w^g[2,5]$	$w^g[2,6]$	$w^g[2,7]$
Koszty lokalowe	$w^g[3,1]$	$w^g[3,2]$	$w^g[3,3]$	$w^g[3,4]$	$w^g[3,5]$	$w^g[3,6]$	$w^g[3,7]$
Zadania kontrolne	$w^g[4,1]$	$w^g[4,2]$	$w^g[4,3]$	$w^g[4,4]$	$w^g[4,5]$	$w^g[4,6]$	$w^g[4,7]$
Dokumentacja	$w^g[5,1]$	$w^g[5,2]$	$w^g[5,3]$	$w^g[5,4]$	$w^g[5,5]$	$w^g[5,6]$	$w^g[5,7]$
Usługi obce	$w^g[6,1]$	$w^g[6,2]$	$w^g[6,3]$	$w^g[6,4]$	$w^g[6,5]$	$w^g[6,6]$	$w^g[6,7]$
Pozostałe	$w^g[7,1]$	$w^g[7,2]$	$w^g[7,3]$	$w^g[7,4]$	$w^g[7,5]$	$w^g[7,6]$	$w^g[7,7]$

Macierz współczynników wzrostu kosztu przetwarzania uwzględniających zwielokrotnienie niektórych elementów systemu informatycznego, ale także uwzględniają-

cych fakt, że elementy są współużytkowane przy przetwarzaniu poszczególnych grup informacji.

Macierz dla g-tej grupy informacji.

Koszty ponoszone w ramach:	Pozyskiwanie informacji, przesyłanie informacji, gromadzenie informacji, utrzymywanie informacji, przetwarzanie danych, udostępnianie informacji, unicestwianie danych						
Infrastruktura techniczna SI	$w_r^g[1,1]$	$w_r^g[1,2]$	$w_r^g[1,3]$	$w_r^g[1,4]$	$w_r^g[1,5]$	$w_r^g[1,6]$	$w_r^g[1,7]$
Koszty osobowe	$w_r^g[2,1]$	$w_r^g[2,2]$	$w_r^g[2,3]$	$w_r^g[2,4]$	$w_r^g[2,5]$	$w_r^g[2,6]$	$w_r^g[2,7]$
Koszty lokalowe	$w_r^g[3,1]$	$w_r^g[3,2]$	$w_r^g[3,3]$	$w_r^g[3,4]$	$w_r^g[3,5]$	$w_r^g[3,6]$	$w_r^g[3,7]$
Zadania kontrolne	$w_r^g[4,1]$	$w_r^g[4,2]$	$w_r^g[4,3]$	$w_r^g[4,4]$	$w_r^g[4,5]$	$w_r^g[4,6]$	$w_r^g[4,7]$
Dokumentacja	$w_r^g[5,1]$	$w_r^g[5,2]$	$w_r^g[5,3]$	$w_r^g[5,4]$	$w_r^g[5,5]$	$w_r^g[5,6]$	$w_r^g[5,7]$
Usługi obce	$w_r^g[6,1]$	$w_r^g[6,2]$	$w_r^g[6,3]$	$w_r^g[6,4]$	$w_r^g[6,5]$	$w_r^g[6,6]$	$w_r^g[6,7]$
Pozostałe	$w_r^g[7,1]$	$w_r^g[7,2]$	$w_r^g[7,3]$	$w_r^g[7,4]$	$w_r^g[7,5]$	$w_r^g[7,6]$	$w_r^g[7,7]$

Na podstawie danych trzech powyższych macierzy możemy wyliczyć koszt przetwarzania informacji g-tej grupy.

$$K[g] = \sum_i \sum_j w^g[i,j] \times w_r^g[i,j] \times k_0[i,j]$$

Kolejną partią danych wejściowych jest macierz kosztów dodatkowych, wynikłych z konieczności zapewnienia spójności przetwarzania, w sytuacji podziału niektórych faz procesów przetwarzania. Konieczność separacji niektórych faz przetwarzania jest implikowana przez zasadniczo różne wymagania bezpieczeństwa dla informacji o różnych wartościach miar poufności.

Koszty ponoszone w ramach:	Pozyskiwanie informacji, przesyłanie informacji, gromadzenie informacji, utrzymywanie informacji, przetwarzanie danych, udostępnianie informacji, unicestwianie danych						
Infrastruktura techniczna SI	$k_s[1,1]$	$k_s[1,2]$	$k_s[1,3]$	$k_s[1,4]$	$k_s[1,5]$	$k_s[1,6]$	$k_s[1,7]$
Koszty osobowe	$k_s[2,1]$	$k_s[2,2]$	$k_s[2,3]$	$k_s[2,4]$	$k_s[2,5]$	$k_s[2,6]$	$k_s[2,7]$
Koszty lokalowe	$k_s[3,1]$	$k_s[3,2]$	$k_s[3,3]$	$k_s[3,4]$	$k_s[3,5]$	$k_s[3,6]$	$k_s[3,7]$
Zadania kontrolne	$k_s[4,1]$	$k_s[4,2]$	$k_s[4,3]$	$k_s[4,4]$	$k_s[4,5]$	$k_s[4,6]$	$k_s[4,7]$
Dokumentacja	$k_s[5,1]$	$k_s[5,2]$	$k_s[5,3]$	$k_s[5,4]$	$k_s[5,5]$	$k_s[5,6]$	$k_s[5,7]$
Usługi obce	$k_s[6,1]$	$k_s[6,2]$	$k_s[6,3]$	$k_s[6,4]$	$k_s[6,5]$	$k_s[6,6]$	$k_s[6,7]$
Pozostałe	$k_s[7,1]$	$k_s[7,2]$	$k_s[7,3]$	$k_s[7,4]$	$k_s[7,5]$	$k_s[7,6]$	$k_s[7,7]$

Po dodaniu kosztów przypisanych do wyodrębnionych grup informacji oraz uwzględnieniu danych z powyżej podanej macierzy otrzymujemy wyrażenie na poszukiwany łączny koszt przetwarzania informacji o różnych wartościach miar poufności.

Poniżej przedstawiamy proponowany schemat obliczeniowy przywołując sukcesywnie potrzebne do obliczeń dane liczbowe.

Rozpoczynamy od macierzy kosztów przetwarzania informacji jawnych.

Koszty ponoszone w ramach:	Pozyskiwanie informacji, przesyłanie informacji, gromadzenie informacji, utrzymywanie informacji, przetwarzanie danych, udostępnianie informacji, unicestwianie danych						
Infrastruktura techniczna SI	$k_0[1,1]$	$k_0[1,2]$	$k_0[1,3]$	$k_0[1,4]$	$k_0[1,5]$	$k_0[1,6]$	$k_0[1,7]$
Koszty osobowe	$k_0[2,1]$	$k_0[2,2]$	$k_0[2,3]$	$k_0[2,4]$	$k_0[2,5]$	$k_0[2,6]$	$k_0[2,7]$
Koszty lokalowe	$k_0[3,1]$	$k_0[3,2]$	$k_0[3,3]$	$k_0[3,4]$	$k_0[3,5]$	$k_0[3,6]$	$k_0[3,7]$
Zadania kontrolne	$k_0[4,1]$	$k_0[4,2]$	$k_0[4,3]$	$k_0[4,4]$	$k_0[4,5]$	$k_0[4,6]$	$k_0[4,7]$
Dokumentacja	$k_0[5,1]$	$k_0[5,2]$	$k_0[5,3]$	$k_0[5,4]$	$k_0[5,5]$	$k_0[5,6]$	$k_0[5,7]$
Usługi obce	$k_0[6,1]$	$k_0[6,2]$	$k_0[6,3]$	$k_0[6,4]$	$k_0[6,5]$	$k_0[6,6]$	$k_0[6,7]$
Pozostałe	$k_0[7,1]$	$k_0[7,2]$	$k_0[7,3]$	$k_0[7,4]$	$k_0[7,5]$	$k_0[7,6]$	$k_0[7,7]$

Na podstawie danych powyższej macierzy otrzymujemy łączny koszt przetwarzania informacji jawnych. Jest to punkt odniesienia przy ocenie wpływu poufności na koszty.

$$K_0 = \sum_i \sum_j k_0[i,j]$$

Po podzieleniu przetwarzanych informacji na 'G' grup, w których informacje mają jednakowe wartości wszystkich 'P' miar poufności, uwzględnić trzeba współczynniki zebrane dla każdej grupy (g: 1, 2, ... , G) w dwóch macierzach.

Macierz współczynników wzrostu kosztu przetwarzania uwzględniających podwyższenie standardu niektórych elementów systemu informatycznego oraz dodanie innych (dla g-tej grupy informacji).

Koszty ponoszone w ramach:	Pozyskiwanie informacji, przesyłanie informacji, gromadzenie informacji, utrzymywanie informacji, przetwarzanie danych, udostępnianie informacji, unicestwianie danych						
Infrastruktura techniczna SI	$w^g[1,1]$	$w^g[1,2]$	$w^g[1,3]$	$w^g[1,4]$	$w^g[1,5]$	$w^g[1,6]$	$w^g[1,7]$
Koszty osobowe	$w^g[2,1]$	$w^g[2,2]$	$w^g[2,3]$	$w^g[2,4]$	$w^g[2,5]$	$w^g[2,6]$	$w^g[2,7]$
Koszty lokalowe	$w^g[3,1]$	$w^g[3,2]$	$w^g[3,3]$	$w^g[3,4]$	$w^g[3,5]$	$w^g[3,6]$	$w^g[3,7]$
Zadania kontrolne	$w^g[4,1]$	$w^g[4,2]$	$w^g[4,3]$	$w^g[4,4]$	$w^g[4,5]$	$w^g[4,6]$	$w^g[4,7]$
Dokumentacja	$w^g[5,1]$	$w^g[5,2]$	$w^g[5,3]$	$w^g[5,4]$	$w^g[5,5]$	$w^g[5,6]$	$w^g[5,7]$
Usługi obce	$w^g[6,1]$	$w^g[6,2]$	$w^g[6,3]$	$w^g[6,4]$	$w^g[6,5]$	$w^g[6,6]$	$w^g[6,7]$
Pozostałe	$w^g[7,1]$	$w^g[7,2]$	$w^g[7,3]$	$w^g[7,4]$	$w^g[7,5]$	$w^g[7,6]$	$w^g[7,7]$

Macierz współczynników wzrostu kosztu przetwarzania uwzględniających zwielokrotnienie niektórych elementów systemu informatycznego, ale także uwzględniają-

cych fakt, że elementy są współużytkowane przy przetwarzaniu poszczególnych grup informacji.

Macierz dla g-tej grupy informacji.

Koszty ponoszone w ramach:	Pozyskiwanie informacji, przesyłanie informacji, gromadzenie informacji, utrzymywanie informacji, przetwarzanie danych, udostępnianie informacji, unicestwianie danych						
Infrastruktura techniczna SI	$w_r^g[1,1]$	$w_r^g[1,2]$	$w_r^g[1,3]$	$w_r^g[1,4]$	$w_r^g[1,5]$	$w_r^g[1,6]$	$w_r^g[1,7]$
Koszty osobowe	$w_r^g[2,1]$	$w_r^g[2,2]$	$w_r^g[2,3]$	$w_r^g[2,4]$	$w_r^g[2,5]$	$w_r^g[2,6]$	$w_r^g[2,7]$
Koszty lokalowe	$w_r^g[3,1]$	$w_r^g[3,2]$	$w_r^g[3,3]$	$w_r^g[3,4]$	$w_r^g[3,5]$	$w_r^g[3,6]$	$w_r^g[3,7]$
Zadania kontrolne	$w_r^g[4,1]$	$w_r^g[4,2]$	$w_r^g[4,3]$	$w_r^g[4,4]$	$w_r^g[4,5]$	$w_r^g[4,6]$	$w_r^g[4,7]$
Dokumentacja	$w_r^g[5,1]$	$w_r^g[5,2]$	$w_r^g[5,3]$	$w_r^g[5,4]$	$w_r^g[5,5]$	$w_r^g[5,6]$	$w_r^g[5,7]$
Usługi obce	$w_r^g[6,1]$	$w_r^g[6,2]$	$w_r^g[6,3]$	$w_r^g[6,4]$	$w_r^g[6,5]$	$w_r^g[6,6]$	$w_r^g[6,7]$
Pozostałe	$w_r^g[7,1]$	$w_r^g[7,2]$	$w_r^g[7,3]$	$w_r^g[7,4]$	$w_r^g[7,5]$	$w_r^g[7,6]$	$w_r^g[7,7]$

Na podstawie danych trzech powyższych macierzy możemy wyliczyć koszt przetwarzania informacji g-tej grupy.

$$K[g] = \sum_i \sum_j w^g[i,j] \times w_r^g[i,j] \times k_0[i,j]$$

Kolejną partią danych wejściowych jest macierz kosztów dodatkowych, wynikłych z konieczności zapewnienia spójności przetwarzania, w sytuacji podziału niektórych faz procesów przetwarzania. Konieczność separacji niektórych faz przetwarzania jest implikowana przez zasadniczo różne wymagania bezpieczeństwa dla informacji o różnych wartościach miar poufności.

Koszty ponoszone w ramach:	Pozyskiwanie informacji, przesyłanie informacji, gromadzenie informacji, utrzymywanie informacji, przetwarzanie danych, udostępnianie informacji, unicestwianie danych						
Infrastruktura techniczna SI	$k_s[1,1]$	$k_s[1,2]$	$k_s[1,3]$	$k_s[1,4]$	$k_s[1,5]$	$k_s[1,6]$	$k_s[1,7]$
Koszty osobowe	$k_s[2,1]$	$k_s[2,2]$	$k_s[2,3]$	$k_s[2,4]$	$k_s[2,5]$	$k_s[2,6]$	$k_s[2,7]$
Koszty lokalowe	$k_s[3,1]$	$k_s[3,2]$	$k_s[3,3]$	$k_s[3,4]$	$k_s[3,5]$	$k_s[3,6]$	$k_s[3,7]$
Zadania kontrolne	$k_s[4,1]$	$k_s[4,2]$	$k_s[4,3]$	$k_s[4,4]$	$k_s[4,5]$	$k_s[4,6]$	$k_s[4,7]$
Dokumentacja	$k_s[5,1]$	$k_s[5,2]$	$k_s[5,3]$	$k_s[5,4]$	$k_s[5,5]$	$k_s[5,6]$	$k_s[5,7]$
Usługi obce	$k_s[6,1]$	$k_s[6,2]$	$k_s[6,3]$	$k_s[6,4]$	$k_s[6,5]$	$k_s[6,6]$	$k_s[6,7]$
Pozostałe	$k_s[7,1]$	$k_s[7,2]$	$k_s[7,3]$	$k_s[7,4]$	$k_s[7,5]$	$k_s[7,6]$	$k_s[7,7]$

Po dodaniu kosztów przypisanych do wyodrębnionych grup informacji oraz uwzględnieniu danych z powyżej podanej macierzy otrzymujemy wyrażenie na poszukiwany łączny koszt przetwarzania informacji o różnych wartościach miar poufności.

$$K = \sum_i \sum_j (k_s[i,j] + \sum_g w^g[i,j] \times w_r^g[i,j] \times k_0[i,j])$$

Ostatecznie, wpływ – w wyrazie finansowym – przetwarzania informacji o różnych klauzulach tajności (ogólniej: o różnych wartościach miar poufności) na system informatyczny określa wyrażenie na **wzrost kosztów** ΔK:

$$\Delta K = \sum_i \sum_j (k_s[i,j] + \sum_g w^g[i,j] \times w_r^g[i,j] \times k_0[i,j]) - \sum_i \sum_j k_0[i,j]$$

po przekształceniu:

$$\Delta K = \sum_i \sum_j (k_s[i,j] + \sum_g w^g[i,j] \times w_r^g[i,j] - 1) \times k_0[i,j])$$

9. Specyfikacja modelowych wymagań technicznych, organizacyjnych i prawnych w dziedzinie bezpieczeństwa teleinformatycznego przetwarzania informacji o różnych klauzulach tajności

9.1. Założenia i struktura modelowych wymagań

Specyfikacja wymagań została wykonana przy następujących założeniach:

- obszar dziedzinowy specyfikacji dotyczy bezpieczeństwa przetwarzania informacji o różnych klauzulach tajności rozpatrywanego w kontekście interoperacyjności systemów informatycznych,
- wymieniony obszar dziedzinowy powinien być rozpatrywany na gruncie modelu zaprezentowanego w rozdziale drugim,
- specyfikacja modelowych wymagań powinna powstać w wyniku zastosowania metod typowych dla prac z dziedziny analizy, klasyfikacji i modelowania, a nie być efektem rutynowych prac audytorskich, projektowych bądź instrukcyjnych,
- wymienione w tytule rozdziału modelowe wymagania należy traktować jako wymagania, których potrzebę sformułowania zidentyfikowano, jak to powyżej napisano, na gruncie modelu opisanego w rozdziale piątym książki. Wymagania i propozycje mają wyznaczać kierunki stymulacji działań w obszarach objętych analizą a nie być wzorcami gotowych rozwiązań czy też wymagań np. dla SIWZ, praktyki projektowej czy wdrożeniowej,
- niniejszy rozdział powinien zawierać jedynie główne wymagania i propozycje będące efektem przeprowadzonych prac analitycznych i koncepcyjnych (wnioski i wymagania szczegółowe zostały na bieżąco formułowane w treści poszczególnych rozdziałów).

Biorąc pod uwagę powyższe założenia specyfikacje modelowych wymagań i propozycji przedstawiono w następującym układzie (strukturze):

- wymagania i propozycje zostały zawarte w poszczególnych, odrębnych podrozdziałach, przy czym zachowano konsekwentnie układ redakcyjny, w którym najpierw sformułowano i uzasadniono wymaganie i następnie przedstawiono propozycje jego realizacji. Propozycje zostały wyróżnione pismem pochyłym,
- dla każdego z wymagań i każdej z propozycji podano hasłowe charakterystyki dziedziny, której dotyczą (prawo – aspekty prawne, organizacja – aspekty organizacyjne, ekonomia – aspekty ekonomiczne lub technika – aspekty techniczno-technologiczne)

9.2. Interoperacyjność i bezpieczeństwo zasobów informacyjnych kluczowych dla realizacji zadań publicznych

Wymaganie (prawo, organizacja)

Wypełnienie celu ustawy o informatyzacji podmiotów realizujących zadania publiczne wymaga stworzenia modelu zasobów informacyjnych, których wykorzystanie jest niezbędne do zgodnej z oczekiwaniami realizacji zadań publicznych drogą elektroniczną. Zasadniczą rolę w tym względzie pełnią rejestry publiczne, w tym zwłaszcza te umocowane ustawowo. W pełni zgadzamy się z ideą zawartą między innymi w [13, 14, 21], że analiza funkcji systemów rejestrowych pozwala wyodrębnić ze zbioru rejestrów te rejestry, których referencyjność dla innych zasobów informacyjnych jest bazowa i niepodważalna. Kontynuując taką analizę można stworzyć wielopoziomową strukturę (piramidę, hierarchię) zasobów (rejestrów) referencyjnych niezbędnych dla realizacji określonego zbioru zadań publicznych. Taka wielopoziomowa struktura będzie użyteczna z punktu widzenia wspierania realizacji zadań publicznych, jeśli zostanie zapewnione interoperacyjne współdziałanie systemów informatycznych wspierających utrzymywanie i przetwarzanie tych zasobów informacyjnych.

Biorąc to pod uwagę można sformułować następujące konkluzje:

- realizacja powszechnych zadań publicznych wymaga uwolnienia zasobów informacyjnych, zwłaszcza głównych zasobów referencyjnych od „posiadania" klauzul niejawności; w przeciwnym razie szeroko opisane w książce ograniczenia nakładane przez wymagania poufności na procesy gromadzenia, przetwarzania i wydawania informacji uniemożliwią lub nadmiernie utrudnią i podrożą realizację zadań publicznych,
- powyższa konkluzja odnosi się w pierwszym rzędzie (ale nie tylko) do systemu rejestrowego PESEL, który jako jeden z bazowych rejestrów publicznych nadal bez wystarczającego uzasadnienia (patrz rozdział dziesiąty) jest systemem przetwarzającym informacje niejawne. Przy okazji warto podkreślić, że w trwających obecnie pracach nad modernizacją systemu PESEL należałoby podjąć temat zapewnienia zgodności identyfikatora – Nr PESEL – z ustawą o ochronie danych osobowych, ponieważ obecna postać tego identyfikatora narusza tę ustawę ujawniając np. datę urodzenia. Identyfikator nie powinien zawierać wiedzy na temat identyfikowanej osoby.

Propozycje (prawo, organizacja)

W celu dokonania niezbędnych zmian wynikających z powyższych konkluzji proponujemy:

- po określeniu modelu informacyjnego zasobów informacyjnych stanowiących podstawową bazę referencyjną i wykonawczą dla systemów wspierających realizację zadań publicznych dokonać:

  - identyfikacji obecnego statusu tych zasobów pod kątem klasyfikacji niejawności,
  - analizy znaczenia tych zasobów dla realizacji przede wszystkim powszechnych zadań publicznych i ocenić zasadność stosowania klauzul tajności,
  - w razie stwierdzenia nieuzasadnionego stosowania klauzul tajności przeprowadzić deklasyfikację tych zasobów informacyjnych,
  - szczególnie pilnym problemem w tym względzie jest problem systemu PESEL, dla którego wg naszej opinii nie ma uzasadnionej potrzeby utrzymywania klauzul tajności,
- rozważyć uwzględnienie w minimalnych wymaganiach dla rejestrów publicznych (po odpowiedniej modyfikacji stosownych rozporządzeń Rady Ministrów) aspektów poufności informacji w taki sposób, by problem klauzul tajności mógł być dzięki temu weryfikowany pod kątem zgodności z ogólnopaństwową polityką w zakresie interoperacyjności i bezpieczeństwa,
- dokonać nowelizacji ustaw w celu jednoznacznego rozstrzygnięcia kwestii niejawności informacji (np. tak, jak to określono dla rejestrów KRS i TERYT, gdzie napisano wprost, że są jawne) dla szczególnie ważnych zasobów informacyjnych, zgromadzonych w rejestrach ustawowych, tzn. tych umocowanych ustawowo,
- zgodzić się, że utrzymanie ustawowej zasady indywidualnej odpowiedzialności za klasyfikowanie niejawności informacji jest słuszne i jednocześnie uznać, że w uzasadnionych przypadkach należy indywidualne decyzje w tym zakresie odnieść do ograniczeń wynikających z polityki państwa w zakresie interoperacyjności i bezpieczeństwa,
- opracować politykę państwa w zakresie interoperacyjności i bezpieczeństwa; elementem takiego dokumentu powinien być opis wzajemnych relacji między interoperacyjnością i poufnością informacji; dokument ten powinien być brany pod uwagę przy opracowywaniu minimalnych wymagań dla rejestrów publicznych i skutkować modyfikacją stosownych rozporządzeń Rady Ministrów.

9.3. Zawyżanie klauzul tajności

Wymaganie (prawo, organizacja)

Zawyżanie klauzul tajności jest często traktowane jako wyraz szczególnej dbałości o bezpieczeństwo informacji. Tymczasem zgodnie z następującym zapisem ustawy o ochronie informacji niejawnej: „4. Zawyżanie lub zaniżanie klauzuli tajności jest niedopuszczalne – *cytat – art. 21 ust. 4*" powinno być traktowane jako naruszenie ustawy. W rozdziale szóstym przedstawiono metody zawyżania klauzul tajności, które w praktyce są nadal stosowane w administracji publicznej. Trzeba ponadto zwrócić uwagę na to, że ustawa o ochronie informacji niejawnych daje możliwości zapobiegania zawyżania klauzul tajności metodą nieuzasadnionego pokrywania niejawnością poprzez skorzystanie z zapisu: „4. Dopuszczalne jest przyznanie różnych klauzul taj-

ności częściom dokumentu lub poszczególnym dokumentom w zbiorze dokumentów, pod warunkiem wyraźnego ich oznaczenia i wskazania klauzuli tajności po odłączeniu dokumentu lub jego części (cytat – art. 19 ust 4)"

Wymaganie (technika, organizacja)

Zawyżanie klauzul tajności jest jedną z przyczyn powstawania ograniczeń dla zapewniania interoperacyjności systemów informatycznych. Kolejnymi ubocznymi skutkami zawyżania klauzul tajności są nieuzasadnione nadmierne koszty systemów bezpieczeństwa, koszty współdziałania systemów informatycznych i nadmierna separacja systemów.

Propozycje (organizacja)

Audyty systemów bezpieczeństwa powinny obejmować również ocenę adekwatności klasyfikacji informacji pod kątem niejawności, ze szczególnym zwracaniem uwagi na obie metody zawyżania klauzul tajności.

Dla systemów i rejestrów, które podlegają zgłoszeniu do ewidencji przewidzianych w ustawie o informatyzacji podmiotów realizujących zadania publiczne należy przewidzieć wykorzystanie instrumentu minimalnych wymagań (oczywiście wymaga to stosownych rozporządzeń wykonawczych). Wszystkie rejestry referencyjne niezbędne do realizacji określonego zbioru zadań publicznych powinny zostać poddane audytowi pod względem adekwatności klasyfikacji informacji i zastosowanych klauzul tajności.

Należy opracować tematykę i model szkoleń na temat zasad nadawania klauzul tajności i odpowiedzialności personalnej w tym zakresie.

9.4. Definicja bezpieczeństwa informacyjnego

Wymaganie (prawo)

Istnieje potrzeba merytorycznego i prawnego wprowadzenia powszechnie akceptowanej definicji bezpieczeństwa informacyjnego. Potrzeba pilnych działań w tym względzie wynika z braku jednolitej, odpowiadającej współczesnemu rozwojowi zastosowań informatycznych definicji.

Propozycje (prawo)

Stosowna definicja powinna się znaleźć w akcie prawnym najwyższej rangi, czyli ustawie. Przy opracowywaniu takiej definicji należy wziąć pod uwagę definicje pochodzące również z przyjętych w Polsce aktów normatywnych z dziedziny zarządzania bezpieczeństwem. Propozycję tę można rozszerzyć o zgłaszany wielokrotnie przez różne środowiska (np. w trakcie prac nad ustawą o informatyzacji administracji publicznej) postulat opracowania słownika podstawowych pojęć, które obowiązywałyby we wszystkich podstawowych aktach prawnych.

9.5. Polityka nakazowa i uszczelniająca

Wymaganie (organizacja, technika)

W przypadku systemów informatycznych administracji publicznej rozdzielenie tego co nakazowe od tego co uszczelniające jest bardzo istotne dla oceny systemu bezpieczeństwa, w tym dla kwestii klasyfikacji informacji pod kątem ich niejawności. Na podstawie przeprowadzonej analizy możemy przyjąć z dużym prawdopodobieństwem, że zaklasyfikowanie informacji jako niejawnych stanowi czasem świadome lecz **nieuzasadnione wzmocnienie** nakazowych wymagań odnoszących się do danych osobowych o wymagania dotyczące informacji niejawnych. Takie podejście, spowodowane zapewne źle pojętą ostrożnością **nie ma umocowania** w obowiązujących ustawach. Nie wolno „sztucznie" podnosić klauzuli tajności po to by wzmocnić system bezpieczeństwa i doprowadzić w ten sposób do nieuzasadnionego poziomu separacji systemów informatycznych. Dotyczy to przede wszystkim jednostek organizacyjnych administracji publicznej, bowiem w podmiotach gospodarczych posiadających zbiory danych (informacji) o porównywalnym znaczeniu dla obywateli takie same dane osobowe są chronione na podstawie ustawy o ochronie danych osobowych (plus ewentualnie jednej z ustaw dedykowanych takich, jak Prawo bankowe, Prawo Energetyczne...).

Propozycje (organizacja)

Należy dokonać analizy zasadności przypisania klauzul tajności do danych przetwarzanych w informatycznych systemach administracji publicznej w celu świadomego osiągnięcia stanu zgodności z zarysowaną wyżej koncepcją polityk nakazowej i uszczelniającej. W efekcie powinno to prowadzić do:

- rozważenia możliwości wyeliminowania nadanych w nieuzasadniony sposób klauzul tajności (przeprowadzenie deklasyfikacji) i ograniczenia się tam, gdzie to wynika z natury danych do stosowania rygorów ustawy o ochronie danych osobowych lub adekwatnej ustawy dziedzinowej ,
- wyodrębnienia danych (informacji), które z mocy prawa są niejawne dla zapewnienia im wymaganego poziomu ochrony tajności; pozostałe dane (atrybuty) powinny pozostać jawne.

9.6. Wypadkowe klauzule tajności

Wymaganie (prawo, technika)

Problem wypadkowych klauzul tajności jest jednym z trudniejszych problemów przetwarzania informacji o zróżnicowanych klauzulach tajności. Dotyczy on zarówno określania wypadkowej klauzuli tajności informacji gromadzonej w zbiory, jak i określania wypadkowej klauzuli tajności wyników częstobardzo skomplikowanego i wielowątkowego przetwarzania informacji o różnych klauzulach. Proste reguły polegające na tym, że poje-

dyncze zapisy (rekordy) mają niższą klauzulę tajności od klauzuli zbiorów danych zawierających łącznie te zapisy (rekordy) lub przyznawanie wynikowi przetwarzania klauzuli tajności najwyższej z klauzul posiadanych przez jakąkolwiek informację wykorzystywaną w tym przetwarzaniu są niewystarczające, bo nie są oparte na formalnie uzasadnionych podstawach. Z tego powodu nie można zastosować rozwiązań technicznych automatyzujących proces nadawania klauzul tajności w zależności od semantyki procesu przetwarzania. Kolejnym problemem w tym zakresie jest zapewnienie zasady indywidualnego prawa do nadawania klauzul i indywidualnej odpowiedzialności w tym zakresie (wymagania ustawy) i pogodzenie jej z pewnymi algorytmami wyznaczania wypadkowych klauzul tajności (wymagania efektywności przetwarzania).

Propozycje (prawo, technika)

Należy uruchomić odpowiednie tematy badawcze w tym zakresie.

9.7. Problem interesu publicznego

Wymaganie (prawo, organizacja)

W art. 23 ust. 2 ustawy o ochronie informacji niejawnych podaje się zasady oznaczania klauzulami tajności informacji stanowiących tajemnicę służbową następująco: „2. Informacje niejawne zaklasyfikowane jako stanowiące tajemnicę służbową oznacza się klauzulą:

1) „poufne" – w przypadku gdy ich nieuprawnione ujawnienie powodowałoby szkodę dla interesów państwa, interesu publicznego lub prawnie chronionego interesu obywateli,
2) „zastrzeżone" – w przypadku, gdy ich nieuprawnione ujawnienie mogłoby spowodować szkodę dla prawnie chronionych interesów obywateli albo jednostki organizacyjnej"

Powyższy zapis jest na tyle nieprecyzyjny, że jest nadużywany w administracji publicznej poprzez dowolne domniemanie zagrożenia dla interesu państwowego, publicznego lub prawnie chronionych interesów obywateli albo jednostki organizacyjnej. Tymczasem dla wielu systemów do właściwej ochrony wystarczy np. właściwe zastosowanie ustawy o ochronie danych osobowych i nie ma potrzeby sięgania do ustawy o ochronie informacji niejawnych. Oczywiście część danych, o znaczeniu specjalnym może zostać wydzielona do odrębnego przetwarzania i sklasyfikowana jako dane niejawne.

Propozycje (prawo, organizacja)

Należy dokonać przeglądu rejestrów (zwłaszcza referencyjnych) pod kątem stosowania odpowiednich mechanizmów ochrony danych osobowych i przeglądu gromadzonych danych pod kątem wydzielenia tej części danych, które mają znaczenie specjalne z punktu widzenia interesów państwa, interesu publicznego, prawnie chronionego interesu obywateli lub jednostki organizacyjnej.

Wymaganie (prawo)

Zasadniczym interesem państwowym lub publicznym jest zapewnienie wymaganych poziomów integralności i dostępności, gdyż utrata integralności lub dostępności kluczowych systemów informatycznych może doprowadzić do istotnej dezintegracji systemu informacyjnego państwa i niemożności realizacji powszechnych zadań publicznych. Dopiero w drugiej kolejności jako warunek technicznej i prawnej realizowalności należy rozpatrywać problem bezpieczeństwa.

Propozycje (prawo)

Należy doprowadzić do zmiany zapisów ustawy pod kątem ograniczenia możliwości swobodnej ich interpretacji lub opracować i upowszechnić materiał metodyczny zawierający komentarze wyjaśniające istotę tych zapisów (podobnie, jak to się stosuje np. do zapisów kodeksu karnego).

9.8. Audyt bezpieczeństwa

Wymaganie (organizacja, prawo, technika)

Nieodłącznym elementem oceny oraz stymulowania rozwoju systemów bezpieczeństwa są audyty bezpieczeństwa, czasem łączone z elementami analizy ryzyka. Aktualnie mamy do czynienia z paradoksalną sytuacją, że w wielu jednostkach administracji publicznej podstawą audytów bezpieczeństwa jest badanie zgodności przyjętych rozwiązań technicznych, organizacyjnych i częściowo prawnych z normą PN-ISO/IEC 17799 w sytuacji, gdy ta norma posługuje się niespójną z obowiązującymi w Polsce aktami prawnymi definicją bezpieczeństwa. Nie kwestionując a nawet potwierdzając zasługi tej normy dla zwiększenia jakości zarządzania bezpieczeństwem teleinformatycznym trzeba stwierdzić, że istnieje potrzeba odniesienia się w aktach prawnych do zasad prowadzenia audytów.

Propozycje (prawo, organizacja, technika)

Główne ustawy dotyczące bezpieczeństwa powstawały odrębnie, w różnych okresach czasu, były pionierskie w tym obszarze problemowym. W związku z tym istnieje potrzeba dokonania przeglądu tych ustaw i zaproponowanie, jeśli okaże się taka potrzeba (naszym zdaniem istnieje) ich nowelizacji. W tym względzie wykorzystanie norm zarządzania bezpieczeństwem informacyjnego jako platformy integracji regulacji zawartych np. w ustawach o ochronie danych osobowych i ochronie informacji niejawnych może okazać się podejściem bardzo korzystnym.

9.9. Mechanizmy ochrony

Wymaganie (technika, organizacja)

Jak wykazała analiza zamieszczona w rozdziale siódmym, w administracji publicznej eksploatowane są systemy informatyczne, które nie stosują do przetwarzania danych niejawnych mechanizmów sterowania przepływem (kontroli przepływu), co może prowadzić z wysokim prawdopodobieństwem do:

- niekontrolowanego, nielegalnego przepływu danych niejawnych do miejsc i osób nie posiadających uprawnień do ich otrzymania,
- konieczności zaniechania potrzebnego przetwarzania danych niejawnych, zwłaszcza gdy mają być przetwarzane dane o różnych klauzulach niejawności lub doprowadzenia do świadomego albo nieświadomego przetwarzania danych z naruszeniem ustawy,
- uniemożliwienia bezpiecznej współpracy z innymi zewnętrznymi lub wewnętrznymi systemami rejestrowymi.

Propozycje (technika, organizacja)

Celem głównym powinna być weryfikacja spełniania przez mechanizmy ochrony stosowane w systemach informatycznych przetwarzających informacje niejawne reguły kontroli przepływu informacji. Podstawą do takiego działania musi być z jednej strony opracowana wcześniej metodyka ustalająca aspekty techniczne i organizacyjne przeprowadzenia weryfikacji i z drugiej identyfikacja (np. przy okazji tworzenia ewidencji systemów informatycznych) środowisk przetwarzania informacji niejawnych.

9.10. Koszty

Wniosek (ekonomia, organizacja)

Ważnym problemem jest nieuzasadniony (w wielu przypadkach) wzrost nakładów finansowych ponoszonych na utrzymanie systemów informatycznych ze względu na zawyżone klauzule tajności oraz co jeszcze ważniejsze znaczący wzrost nakładów finansowych, które będą ponoszone w wypadku szerszej wymiany danych między systemami (rejestrami), w wypadku praktycznej realizacji interoperacyjności, co jest związane z implementacją mechanizmów i procedur zapewniania odpowiedniego poziomu bezpieczeństwa dla systemów wymieniających dane, które nie są jawne.

Niezależnie od tego uważamy, że istnieje ogólniejsza potrzeba badania kosztów systemów bezpieczeństwa, ponieważ one znacząco wpływają, nie zawsze z wystarczająco uzasadnionych powodów, na ogólne koszty systemów informatycznych.

Odnosząc powyższą analizę na bardziej wymierny „grunt" finansów publicznych należy stwierdzić, że nieuzasadniona nadmierna koncentracja środków finansowych na poufności może ograniczyć możliwości skutecznego rozwoju systemów informa-

tycznych lub możliwości zapobiegania lub ograniczania podatności systemów rejestrowych na utratę integralności lub dostępności.

Propozycje (ekonomia, organizacja)

Przede wszystkim należy podjąć i kontynuować prace nad modelami rejestracji i analizy kosztów systemów bezpieczeństwa. Jedna z pierwszych z prób w tym zakresie została zaprezentowana w niniejszej książce. Mogą one służyć do szacowania kosztów konkretnego systemu, do analiz porównawczych, do opracowywania normatywnych kosztów, do badania stosunku kosztów wynikających z polityk nakazowej i uszczelniającej.

10. System rejestrowy PESEL a modelowe wymagania

10.1. Charakterystyka systemu rejestrowego PESEL w zakresie przetwarzania informacji niejawnych pod kątem specyfikacji modelowych wymagań

10.1.1. Podstawa prawna prowadzenia rejestru

- Ustawa z dnia 10 kwietnia 1974 o ewidencji ludności i dowodach osobistych (Dz. U. z 2001r. Nr 87 poz. 960).
- Rozporządzenie Rady Ministrów z dnia 30 kwietnia 2002 r. w sprawie wysokości opłat za udostępnianie danych ze zbiorów meldunkowych, zbioru PESEL oraz ewidencji wydanych i utraconych dowodów osobistych oraz warunków i sposobu ich wnoszenia (Dz. U. z 2002 r. nr 62 poz. 564).
- Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 18 listopada 2002 r. w sprawie wzoru formularza wniosku o udostępnienie danych ze zbiorów meldunkowych, zbioru PESEL oraz ewidencji wydanych i utraconych dowodów osobistych (Dz. U. z 2002 r. nr 201 poz. 1702).
- Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 20 grudnia 2002 r. w sprawie trybu przekazywania danych pomiędzy organami prowadzącymi ewidencję ludności oraz powiadamianie o nadaniu numeru PESEL (Dz. U. z 2002 r. nr 236 poz. 1996).
- Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 24 grudnia 2002 r. w sprawie zgłaszania i przyjmowania danych niezbędnych do zameldowania i wymeldowania oraz prowadzenia ewidencji ludności ewidencji wydanych i utraconych dowodów osobistych (Dz. U. z 2002 r. nr 236 poz. 1999).

[Uwaga: wyniki analizy aktów prawnych dotyczących rejestru PESEL przedstawione są w rozdz. 4 oraz w załączniku nr 1]

10.1.2. Organ odpowiedzialny za prowadzenie rejestru

Ministerstwo Spraw Wewnętrznych i Administracji; wykonawstwo – Departament Rejestrów Państwowych.

10.1.3. Zasady funkcjonowania rejestru

Rejestr PESEL – Powszechny Elektroniczny System Ewidencji Ludności zawiera dane osób przebywających stale na terytorium RP, zameldowanych na pobyt stały lub czasowy trwający ponad 2 miesiące a także osób ubiegających się o wydanie dowodu osobistego lub osób, dla których odrębne przepisy przewidują potrzebę posiadania numeru PESEL. Bazy danych systemu rozmieszczone są na szczeblach:

- centralnym,
- rejonowym,
- gminnym.

Szczebel gminy jest podstawowym źródłem informacji, w którym wprowadza się dane o nowych osobach oraz aktualizuje się cechy osób istniejących.

10.1.4. Opis cech informacyjnych rejestru

Wykaz danych gromadzonych w bazie danych rejestru PESEL zgodnie z art. 44a ustęp 7 ustawy prawo o ewidencji ludności i dowodach osobistych znajduje się w tabeli 10-1.

10.1.5 Wartości miar poufności cech informacyjnych (oraz grup informacji) zbiorów danych PESEL

W poniższej tabeli zamieszczono autorską ocenę miar poufności poszczególnych cech informacyjnych a także grup informacji dla zbiorów danych rejestru PESEL. Cechy informacyjne wyspecyfikowano zgodnie z definicją struktur tablic bazy danych (obejmują więc również dane typu technicznego, np. daty aktualizacji grup informacji). Płaszczyzny poufności (w rozumieniu rozdziału 5), dla których określane są miary poufności obejmują płaszczyzny podstawowe „postępowania z informacjami niejawnymi" i „ochrona danych osobowych" oraz przykładowe płaszczyzny branżowe.

Dla uproszczenia przyjęto, że wartość „1" miary poufności oznacza większy od zera stopień poufności odpowiedniej cechy informacyjnej w danej płaszczyźnie, zaś wartość „0" oznacza, że dana cecha informacyjna jest pozbawiona cechy poufności w danej płaszczyźnie.

Tabela 10-1 - Wartości miar poufności cech informacyjnych (oraz grup informacji) zbiorów danych PESEL

Uwagi:

a) wartość „0" miary poufności oznacza, że dana cecha informacyjna jest pozbawiona cechy poufności w danej płaszczyźnie,

b) wartość „1" miary poufności oznacza większy od zera stopień poufności odpowiedniej cechy informacyjnej w danej płaszczyźnie

Lp.	Cecha informacyjna	Płaszczyzny poufności							
		Ochrona informacji niejawnych	Ochrona danych osobowych	Handlowa	Bankowa	Statystyczna	Lekarska	Dziennikarska	Postępowania karnego
Grupa: Numer ewidencyjny (NE)		**0**	**1**	**0**	**0**	**0**	**0**	**0**	**0**
1.	Numer ewidencyjny	0	1	0	0	0	0	0	0
2.	Następny numer ewidencyjny	0	1	0	0	0	0	0	0
3.	Poprzedni numer ewidencyjny	0	1	0	0	0	0	0	0
4.	Data aktualizacji grupy NE	0	0	0	0	0	0	0	0
Grupa: Nazwiska (NZ)		**0**	**1**	**0**	**0**	**0**	**0**	**0**	**0**
5.	Nazwisko aktualne - 1 człon	0	1	0	0	0	0	0	0
6.	Nazwisko aktualne - 2 człon	0	1	0	0	0	0	0	0
7.	Nazwisko rodowe - 1 człon	0	1	0	0	0	0	0	0
8.	Nazwisko rodowe - 2 człon	0	1	0	0	0	0	0	0
9.	Nazwisko poprzednie - 1 człon	0	1	0	0	0	0	0	0
10.	Nazwisko poprzednie - 2 człon	0	1	0	0	0	0	0	0
11.	Nazwisko poprzednie - 1 człon	0	1	0	0	0	0	0	0
12.	Nazwisko poprzednie - 2 człon	0	1	0	0	0	0	0	0
13.	Nazwisko poprzednie - 1 człon	0	1	0	0	0	0	0	0
14.	Nazwisko poprzednie - 2 człon	0	1	0	0	0	0	0	0
15.	Nazwisko poprzednie - 1 człon	0	1	0	0	0	0	0	0
16.	Nazwisko poprzednie - 2 człon	0	1	0	0	0	0	0	0

Lp.	Cecha informacyjna	Płaszczyzny poufności							
		Ochrona informacji niejawnych	Ochrona danych osobowych	Handlowa	Bankowa	Statystyczna	Lekarska	Dziennikarska	Postępowania karnego
17.	Nazwisko poprzednie - 1 człon	0	1	0	0	0	0	0	0
18.	Nazwisko poprzednie - 2 człon	0	1	0	0	0	0	0	0
19.	Data aktualizacji grupy NZ	0	0	0	0	0	0	0	0
Grupa: Imiona (IM)		**0**	**1**	**0**	**0**	**0**	**0**	**0**	**0**
20.	Imię - aktualne pierwsze	0	1	0	0	0	0	0	0
21.	Imię - aktualne drugie	0	1	0	0	0	0	0	0
22.	Imię - poprzednie pierwsze	0	1	0	0	0	0	0	0
23.	Imię - poprzednie drugie	0	1	0	0	0	0	0	0
24.	Imię - poprzednie pierwsze	0	1	0	0	0	0	0	0
25.	Imię - poprzednie drugie	0	1	0	0	0	0	0	0
26.	Data aktualizacji grupy IM	0	0	0	0	0	0	0	0
Grupa: Dane o rodzicach i miejscu urodzenia (UR)		**0**	**1**	**0**	**0**	**0**	**0**	**0**	**0**
27.	Imię ojca	0	1	0	0	0	0	0	0
28.	Imię matki	0	1	0	0	0	0	0	0
29.	Nazwisko rodowe matki - 1 człon	0	1	0	0	0	0	0	0
30.	Nazwisko rodowe matki - 1 człon	0	1	0	0	0	0	0	0
31.	Miejsce urodzenia	0	1	0	0	0	0	0	0
32.	Data aktualizacji grupy UR	0	1	0	0	0	0	0	0
Grupa: Dokument tożsamości i dane o obywatelstwie (DT)		**0**	**1**	**0**	**0**	**0**	**0**	**0**	**0**
33.	Seria i numer dokumentu tożsamości	0	1	0	0	0	0	0	0

Lp.	Cecha informacyjna	Płaszczyzny poufności							
		Ochrona informacji niejawnych	Ochrona danych osobowych	Handlowa	Bankowa	Statystyczna	Lekarska	Dziennikarska	Postępowania karnego
34.	Kod terytorialny wystawcy dokumentu tożsamości	0	1	0	0	0	0	0	0
35.	Obywatelstwo (niepolskie)	0	1	0	0	0	0	0	0
36.	Data uzyskania obywatelstwa RP	0	1	0	0	0	0	0	0
37	Data utraty obywatelstwa RP	0	1	0	0	0	0	0	0
38.	Data aktualizacji grupy DT	0	0	0	0	0	0	0	0
Grupa: Dane dotyczące zgonu osoby (ZG)		0	1	0	0	0	0	0	0
39.	Data zgonu	0	1	0	0	0	0	0	0
40.	Data aktualizacji grupy ZG	0	0	0	0	0	0	0	0
Grupa: Adres pobytu stałego (AS)		**0**	**1**	**0**	**0**	**0**	**0**	**0**	**0**
41.	Kod terytorialny	0	1	0	0	0	0	0	0
42.	Miejscowość	0	1	0	0	0	0	0	0
43.	Ulica	0	1	0	0	0	0	0	0
44.	Numer domu	0	1	0	0	0	0	0	0
45.	Numer mieszkania	0	1	0	0	0	0	0	0
46.	Data zameldowania	0	1	0	0	0	0	0	0
47.	Data wymeldowania	0	1	0	0	0	0	0	0
48.	Rodzaj wymeldowania	0	1	0	0	0	0	0	0
49.	Kraj wyjazdu na pobyt stały	0	1	0	0	0	0	0	0
50.	Data wyjazdu na pobyt stały	0	1	0	0	0	0	0	0

Lp.	Cecha informacyjna	Płaszczyzny poufności							
		Ochrona informacji niejawnych	Ochrona danych osobowych	Handlowa	Bankowa	Statystyczna	Lekarska	Dziennikarska	Postępowania karnego
51.	Data powrotu z wyjazdu na pobyt stały	0	1	0	0	0	0	0	0
52.	Data aktualizacji grupy AS	0	0	0	0	0	0	0	0
	Grupa: Adres czasowy (AC)	**0**	**1**	**0**	**0**	**0**	**0**	**0**	**0**
53.	Kod terytorialny	0	1	0	0	0	0	0	0
54.	Miejscowość	0	1	0	0	0	0	0	0
55.	Ulica	0	1	0	0	0	0	0	0
56.	Numer domu	0	1	0	0	0	0	0	0
57.	Numer mieszkania	0	1	0	0	0	0	0	0
58.	Data zameldowania	0	1	0	0	0	0	0	0
59.	Data wymeldowania	0	1	0	0	0	0	0	0
60.	Data aktualizacji grupy AC	0	0	0	0	0	0	0	0
	Grupa: Dane organizacyjne	**0**	**1**	**0**	**0**	**0**	**0**	**0**	**0**
61.	Data sprzeciwu wobec przetwarzania danych osoby	0	1	0	0	0	0	0	0
62.	Zastrzeżenie adresu - od kiedy	0	1	0	0	0	0	0	0
63.	Zastrzeżenie adresu - do kiedy	0	1	0	0	0	0	0	0
64.	Data założenia rekordu	0	0	0	0	0	0	0	0
65.	Priorytet pochodzenia danych	0	0	0	0	0	0	0	0
66.	Wskaźnik przynależności do banku tematycznego SEP	0	0	0	0	0	0	0	0
67.	Wskaźnik przynależności do banku tematycznego SOP	0	0	0	0	0	0	0	0

Lp.	Cecha informacyjna	Płaszczyzny poufności							
		Ochrona informacji niejawnych	Ochrona danych osobowych	Handlowa	Bankowa	Statystyczna	Lekarska	Dziennikarska	Postępowania karnego
68.	Wskaźnik przynależności do banku tematycznego CRS	0	0	0	0	0	0	0	0
69.	Informacje wskaźnikowe Zapis bez kontroli	0	0	0	0	0	0	0	0
70.	Informacje wskaźnikowe Rekord anulowany	0	0	0	0	0	0	0	0
71.	Data aktualizacji rekordu	0	0	0	0	0	0	0	0
72.	Rezerwa	0	0	0	0	0	0	0	0

10.2. Charakterystyka systemu informatycznego używanego do prowadzenia rejestru PESEL

W poniższej tabeli zamieszczono podstawowe informacje nt. systemu informatycznego wykorzystywanego do prowadzenia rejestru PESEL *[uwaga: źródłem tej tabeli jest opracowanie pt. „Klasyfikacja informacji i zagrożeń w rejestrach państwowych, w tym w Centralnej Ewidencji Pojazdów i Centralnej Ewidencji Kierowców zwanych dalej rejestrami wraz z wnioskami i propozycjami wynikającymi z przeprowadzonej analizy" firmy Milstar].*

Tabela 10-2 – Podstawowe informacje nt. systemu informatycznego używanego do prowadzenia rejestru PESEL

Klauzula poufności bazy	Poufne
Klauzula poufności rekordów bazy	Zastrzeżone
System operacyjny	IBM Z/OS (mainframe, dawny OS/390)
Motor bazy danych	Rozwiązanie własne JANTAR, narzędzie Assembler
Mechanizmy ochrony bazy danych	hasła, hierarchiczne prawa dostępu
Nazwa aplikacji	Centralny Bank Danych
Technologia wykonania	Środowisko systemowe i programowe IBM
Wprowadzanie danych	dedykowane stanowiska tylko lokalnie
Zdalny dostęp	Dedykowane stanowiska bez połączenia z siecią lokalną u użytkownika, sieć PESEL-NET
Systemy współpracujące	Rejestr zastawów Min. Sprawiedliwości, SI w Policji poprzez PESEL-NET

10.3. Analiza i ocena spełniania specyfikacji modelowych wymagań prawnych i organizacyjnych

W poniższej tabeli zamieszczono ocenę spełniania modelowych wymagań prawnych i organizacyjnych przez system informatyczny wykorzystywany do prowadzenia rejestru PESEL – ocenę tę opracowano na podstawie konsultacji z pracownikami Departamentu Rejestrów Państwowych MSWiA.

Użyte w tabeli oznaczenie RPWBT oznacza rozporządzenie Prezesa Rady Ministrów z dnia 25 sierpnia 2005 r. w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego

Tabela 10-3 – Ocena spełniania modelowych wymagań prawnych i organizacyjnych przez system PESEL

(PRAWO, ZADANIA PUBLICZNE)	
Czy istnieją akty prawne, które nakazują by system był używany do realizacji zadań publicznych drogą elektroniczną? Jeśli tak, to jakie?	NIE
Czy system jako finalny realizuje zadania publiczne zadania publiczne drogą elektroniczną:	
dla jednostek administracji publicznej?	NIE
dla obywateli?	NIE
dla innych podmiotów, które nie są jednostkami administracji publicznej?	NIE
Czy system jako „źródło danych" uczestniczy w realizacji zadań publicznych drogą elektroniczną:	
dla jednostek administracji publicznej?	TAK
dla obywateli?	NIE
dla innych podmiotów, które nie są jednostkami administracji publicznej?	TAK
czy przekazuje do systemu finalnego drogą elektroniczną?	TAK
(BEZPIECZEŃSTWO, POUFNOŚĆ, DEFINICJA)	
Czy stosuje się jednolicie definicję bezpieczeństwa informacji?	TAK
Jeśli tak, to jaka jest jej podstawa prawna lub organizacyjna?	RPWBT
(BEZPIECZEŃSTWO, POUFNOŚĆ, PRAWO)	
Czy informacje gromadzone i przetwarzane w systemie podlegają ustawie o ochronie danych osobowych:	TAK
jeśli tak, czy określono to wprost w akcie prawnym dla tego systemu?	NIE
czy wywiedziono to z przepisów ogólnych?	
Czy informacje gromadzone i przetwarzane w systemie podlegają ustawie branżowej i czy z tego tytułu nałożono na nie rygory poufności:	NIE
jeśli tak, to w jakiej ustawie i czy określono to wprost w akcie prawnym dla tego systemu?	
Czy informacje gromadzone i przetwarzane w systemie podlegają ustawie o ochronie informacji niejawnych:	TAK
jeśli tak, czy określono to wprost w akcie prawnym dla tego systemu?	NIE
czy wywiedziono to z przepisów ogólnych?	TAK
(POUFNOŚĆ, PRAWO)	
Czy w akcie powołującym system (rejestr) określono poziom niejawności zasobów informacyjnych?	NIE
jeśli tak, to na jakim poziomie?	
jeśli nie a stosuje się klauzule tajności, to na jakiej podstawie?	Decyzja organizacyjna
Czy w akcie powołującym określono poziom niejawności systemu informatycznego?	NIE
jeśli tak, to na jakim poziomie?	
jeśli nie, a stosuje się klauzule tajności, to na jakiej podstawie?	Decyzja organizacyjna
Czy w systemie gromadzone są i przetwarzane informacje o różnych klauzulach ?	TAK

jeśli tak, to jaka jest klauzula tajności informacji wejściowych (pojedynczych lub zbiorowych)?	Jawne
jeśli tak, to jaka jest klauzula tajności informacji w bazie systemu?	Pojedyncze rekordy – zastrzeżone; Cała baza - poufne
jeśli tak, to jaka jest klauzula tajności wyjściowych (pojedynczych lub zbiorowych)?	Pojedyncze rekordy – jawne; Cała baza - zastrzeżone
jeśli tak, to jaka jest reguła oznaczania („obliczania") wypadkowej klauzuli tajności informacji wyjściowych wydawanych wprost z systemu a jaka, gdy są one wynikiem przetwarzania informacji o różnych klauzulach tajności?	j.w.
(INTEROPERACYJNOŚĆ, ZADANIA PUBLICZNE)	
Czy założenia systemu uwzględniały konieczność interoperacyjnego (drogą elektroniczną) współdziałania systemu z innymi systemami do:	
do realizacji powszechnych zadań publicznych na poziomie krajowym?	NIE
do realizacji innych zadań publicznych administracji na poziomie instytucjonalnym?	NIE
do realizacji innych zadań publicznych administracji na poziomie krajowym?	NIE
do realizacji innych zadań publicznych administracji na poziomie ponadkrajowym?	NIE
(INTEROPERACYJNOŚĆ, MODEL INFORMACYJNY)	
Czy istnieje wspólny model informacyjny zasobów informacyjnych, którego elementem jest model informacyjny lub jego część rozpatrywanego systemu?	
na poziomie instytucjonalnym,	NIE
na poziomie krajowym,	NIE
na poziomie ponadkrajowym	NIE
(POUFNOŚĆ, MECHANIZMY OCHRONY)	
Czy do ochrony poufności stosuje się standardowe mechanizmy:	
systemów operacyjnych? Jeśli tak, to jakich i jaka jest w nich reguła ochrony?	TAK (IBM Z/OS – hasła, hierarchiczne prawa dostępu)
systemów bazy danych? Jeśli tak, to jakich i jaka jest w nich reguła ochrony?	Rozwiązanie własne JANTAR
innego oprogramowania? Jeśli tak, to jakich i jaka jest w nich reguła ochrony?	
Czy stosowane mechanizmy ochrony podlegały weryfikacji pod kątem kontroli przepływu?	NIE
(INTEROPERACYJNOŚĆ, POUFNOŚĆ, KOSZTY)	
Czy prowadzi się ewidencję kosztów systemu ochrony poufności?	NIE
jeśli tak, czy można na jej podstawie wyodrębnić koszty stosowania polityki nakazowej w rozbiciu na koszty spełnienia wymagań poszczególnych aktów prawnych (ustaw)?	
jeśli tak, czy można wyodrębnić koszty stosowania polityki uszczelniającej?	

10.4. Wnioski z przeprowadzonej analizy

System informatyczny wykorzystywany do prowadzenia rejestru PESEL nie spełnia większości wymagań określonych w rozdz. 9. Dla systemu PESEL, na podstawie decyzji organizacyjnej, bazie danych nadano klauzulę „poufne", zaś pojedynczym rekordom – klauzulę „zastrzeżone". Jak pokazano w tabeli 10-1 wszystkie cechy informacyjne charakteryzujące osobę fizyczną są pozbawione cechy poufności w płaszczyźnie „ochrona informacji niejawnych". Oznacza to, że brak podstaw do nadania takich klauzul.

Z tabeli 10-3 wynika, że do ochrony danych w systemie PESEL zastosowano mechanizmy ochrony danych stanowiące standardowe wyposażenie zastosowanych systemów operacyjnych i systemów baz danych. Mechanizmy te w swej istocie są oparte na koncepcji macierzy dostępu (sterowania dostępem), w których reguła upoważnienia dowolnego żądania dostępu do danych polega na sprawdzeniu w macierzy dostępu czy istnieje reguła dopuszczająca jego realizację. W ten sposób (pewnym uproszczeniu) reguluje się dostęp obiektów aktywnych (przede wszystkim użytkowników) do obiektów pasywnych (przede wszystkim danych).

11. Wnioski, propozycje, wytyczne

11.1. Wnioski, propozycje

W celu zachowania przejrzystości i łatwości odwoływania się do wniosków zastosowano analogicznie do rozdziału dziewiątego układ redakcyjny, zgodnie z którym po każdym wniosku przedstawiono propozycję jego realizacji.

Wniosek – potrzeba oceny stanu

Aktualnie organy odpowiedzialne za stan informatyzacji administracji publicznej nie mają dostatecznej wiedzy na temat stanu rejestrów publicznych. Wiedza ta jest niezbędna do określenia wyjściowych warunków merytorycznych, organizacyjnych i finansowych, opracowywania polityki państwa w zakresie interoperacyjności i bezpieczeństwa. Nie wiadomo np. jaka jest skala nadmiernego pokrywania zbiorów informacji niejawnością lub skala zawyżania klauzul tajności. Nie wiadomo jakie są ponoszone aktualnie koszty takich nieprawidłowości, jakie są koszty ewentualnej zmiany tego stanu (koszty łączne deklasyfikacji, koszty łączne wydzielenia ze zbiorów niejawnych części jawnej, itd.). Nie ma wystarczającej wiedzy na temat relacji między zadaniami publicznymi a niejawnością informacji niezbędnych do ich realizacji.

Propozycje

Oczywistą sprawą jest, że wdrożenie polityki państwa (gdyby taka istniała) w zakresie interoperacyjności i bezpieczeństwa musi być etapowe, sukcesywne. Określenie etapów oraz celów, które trzeba w ich ramach osiągnąć musi wynikać z wcześniej opracowanej i przyjętej polityki państwa, która wymaga wykonania niezbędnych prac analitycznych i koncepcyjnych. Niezależnie od pilności osiągnięcia wymaganego poziomu interoperacyjności takie prace muszą być wykonane. Propozycje w tym względzie przedstawiamy przy okazji wniosku następnego. Pozwolą one na sformułowanie harmonogramu i zakresu (głębokości) „inwentaryzacji" oraz wskazówek metodologicznych do jej przeprowadzenia. Wstępna ocena wyników inwentaryzacji powinna dać podstawy do podziału przedsięwzięć na co najmniej dwie grupy: zadania doraźne i za-

dania systemowe. Pierwsze z nich powinny być podjęte natychmiast, by usunąć stwierdzone nieprawidłowości (bieżące bariery). Drugie powinny być podjęte w ramach całościowej koncepcji przebudowy stanu informatyzacji administracji publicznej.

Wniosek – polityka w zakresie interoperacyjności i bezpieczeństwa

Punktem wyjścia do opracowania polityki w zakresie zapewniania interoperacyjności i bezpieczeństwa muszą być potrzeby wynikające z realizacji zadań publicznych wspieranych narzędziami i metodami informatyki. Potrzeby te dotyczą zasobów informacyjnych, które są niezbędne do realizacji zadań publicznych, parametrów ilościowo-jakościowych ich realizacji oraz wynikającego z nich wsparcia informatycznego, w tym niezbędnego poziomu interoperacyjności.

Propozycje

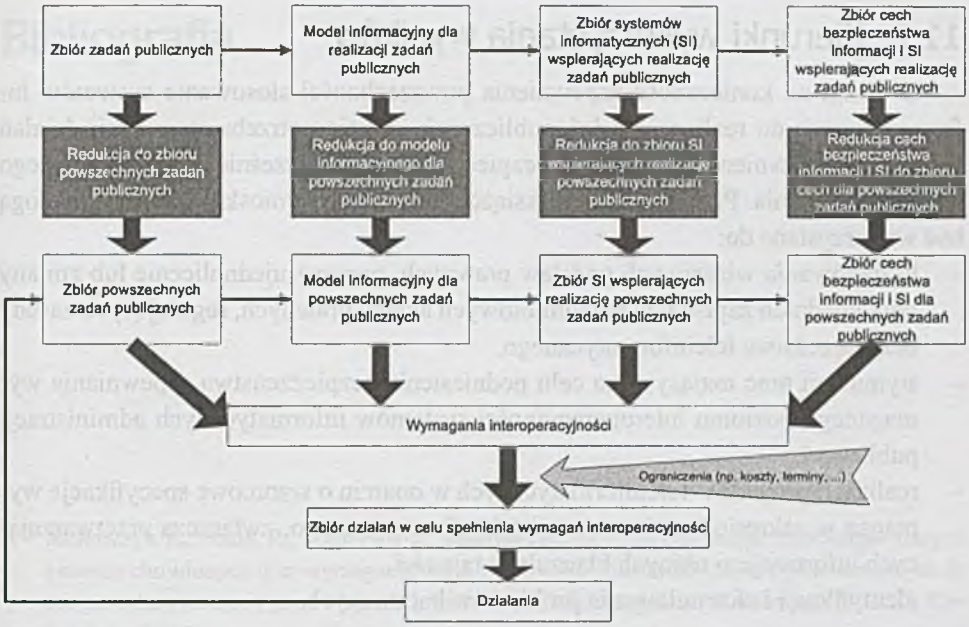
Określenie tych potrzeb będzie niemożliwe bez wykonania prac z zakresu analizy, klasyfikacji, modelowania, których efektem powinny być m. in.:

- klasyfikacja zadań publicznych,
- model informacyjny zasobów informacyjnych niezbędnych do realizacji tych zadań,
- klasyfikacja systemów informatycznych wspierających realizację zadań publicznych,
- klasyfikacja i identyfikacja cech bezpieczeństwa (poufności) zasobów informacyjnych i systemów informatycznych.

Przykładową ilustrację wyników takiej analizy przedstawiono na rys. 11-1. Warto zauważyć, że opiera się ona na wyodrębnieniu ze zbioru zadań publicznych podzbioru powszechnych zadań publicznych realizowanych drogą elektroniczną, które są dostępne dla wszystkich obywateli lub jednostek organizacyjnych. W celu zapewnienia wsparcia informatycznego musi być zagwarantowany niezbędny poziom interoperacyjności systemów informatycznych, który jest opisany zbiorem wymagań interoperacyjności. Wyniki „konfrontacji" tych wymagań z istniejącym stanem opisanym na trzecim poziomie (po redukcji) rysunku determinuje zbiór zadań, które należy podjąć.

Wniosek – kryteria ważności

Na przestrzeni ostatnich lat wielokrotnie podejmowano działania zmierzające do ponownego zdefiniowania kryteriów ważności problemów istotnych dla obywatela. Niejednokrotnie przyjęte decyzje z inspiracji organów państwowych w zasadniczy sposób zmieniały dotychczas utrwalone wieloletnie praktyki. W obszarze nas interesującym można dojść do konkluzji, że w infrastrukturze informatycznej administracji publicznej istnieją rozwiązania, które zostały wdrożone bardziej z myślą o separacji systemów i zasobów od obywateli niż z myślą działaniach na rzecz obywateli. Było to wyrazem dawniej obowiązujących zasad (kryteriów wartości, ważności).



Rys. 11-1. Przykładowe wyniki proponowanej analizy

Propozycje

Konieczne jest ponowne zdefiniowanie głównych kryteriów procesów informatyzacji. Należy przyjąć w praktyce, że priorytetem jest stworzenie warunków dla budowy społeczeństwa informacyjnego i tym samym przyjąć, że zadaniem administracji jest stworzenie warunków do interoperacyjnego działania systemów informatycznych. W takiej sytuacji wszystkie kwestie poufności muszą być w ramach prawa podporządkowane temu celowi. Nie oznacza to zgody na niezgodne z prawem naruszanie poufności informacji, lecz opracowanie i wdrożenie rozwiązań, które usuną zbędne, choć dzisiaj jeszcze obowiązujące, ograniczenia w tym względzie.

Wniosek – legislacja

Należy podjąć na gruncie ustawy o informatyzacji podmiotów realizujących zadania publiczne działania włączające problematykę bezpieczeństwa do zagadnienia interoperacyjności systemów informatycznych oraz działania zmierzające do określenia i wykorzystania platformy prawnej do integracji pojęć, zadań i organizacji bezpieczeństwa

Propozycje

W pierwszym przypadku należy przede wszystkim wykorzystać instrumenty wprowadzone ustawą, zwłaszcza wymagania minimalne i plany informatyzacji. W drugim przypadku rozważyć możliwości wykorzystania dorobku zawartego w aktach normatywnych.

11.2. Kierunki wykorzystania wyników

Z uwagi na konieczność zapewnienia powszechności stosowania systemów informatycznych do realizacji zadań publicznych istnieje potrzeba stymulacji działań służących zapewnieniu warunków bezpiecznego i jednocześnie interoperacyjnego ich współdziałania. Przedstawione w książce rozważania, wnioski i propozycje mogą być wykorzystane do:

- kształtowania właściwych podstaw prawnych, poprzez ujednolicenie lub zmiany odpowiednich zapisów w przedmiotowych aktach prawnych, regulujących zasady bezpieczeństwa teleinformatycznego,
- stymulacji prac mających na celu podniesienia bezpieczeństwa zapewniania wymaganego poziomu interoperacyjności systemów informatycznych administracji publicznej,
- realizacji projektów teleinformatycznych w oparciu o wzorcowe specyfikacje wymagań w zakresie bezpieczeństwa teleinformatycznego, zwłaszcza przetwarzających informacje o różnych klauzulach tajności,
- identyfikacji i sformułowania problemów badawczych.

Bibliografia

1. **Adamczyk A., Renk R., Radziulis J., Hołubowicz W.** – „Klasyfikacja informacji i danych prawnie chronionych oraz wymagania dotyczące środków informatycznych przeznaczonych do ich przechowywania i przetwarzania", materiały konferencyjne XI Konferencji PLOUG, Kościelisko, 2005,
2. **Benon Davies P.** – „Systemy baz danych", WNT, Warszawa, 2003,
3. **Bogucki D.** – „Jak wprowadzić krajowe standardy interoperacyjności", materiały Ministerstwa Nauki i Informatyzacji, XI, 2005,
4. **Booch G., Rumbaugh J., Jacobson I.** – UML przewodnik użytkownika, WNT, Warszawa, 2002
5. **Denning D.** – „Kryptografia i ochrona danych", WNT, Warszawa, 1992,
6. **Garfinkel S., Stafford G.** – **„Bezpieczeństwo w Unixie i Internecie", Wyd. READ ME, Warszawa 1997,**
7. **Frish A.** – „Unix – Administracja systemu", Wyd. READ ME, Warszawa 1996,
8. **Kisielnicki J., Sroka H.** – „Systemy informatyczne biznesu", PLACET, Warszawa, 2005,
9. **Loney K., Theriuault M.** – „Oracle 9i – podręcznik administratora, Implementowanie zaawansowanych rozwiązań administracyjnych", Wyd. Helion, Gliwice 2003,
10. **Microsoft Windows 2000 Server** – Praca Serwera – Wyd. Microsoft Press, Warszawa 2000,
11. **Microsoft Windows 2000 Server** – „Integracja Międzysieciowa", Wyd. Microsoft Press, Warszawa 2000,
12. **Mueller J.P.** – „Optymalizacja systemu Microsoft 2000 – Przewodnik Techniczny", Wyd. Microsoft Press, Warszawa 2001,
13. **Oleński J.** – „Ewidencje i rejestry administracji publicznej w infrastrukturze informacyjnej państwa, materiały konferencji: „Ewidencje i rejestry w administracji publicznej", CPI, Warszawa, 2005,
14. **Oleński J.** – „Integralność rejestrów państwowych podstawą taniego e-Państwa, materiały konferencji: „Suces IT – jak to się robi?", XI Forum Teleinformatyki, Legionowo, 2005,

15. **Oleński J.** – „Ekonomika informacji – metody", PWE, Warszawa, 2003,

16. **Pipkin D.** – „Bezpieczeństwo informacji", WNT, Warszawa, 2002,

17. **Scambray J., McClure S., Kurtz G.** – „Hakerzy cała prawda – sekrety zabezpieczeń sieci komputerowych", Wyd. Translator, Warszawa 2001;

18. **Stanek W.R.** – Microsoft Windows 2000 Internet Information Services 5.0, Wyd. Microsoft Press, Warszawa 2001;

19. **Stokłosa J., Bilski T., Pankowski T.** – „Bezpieczeństwo danych w systemach informatycznych" PWN, Poznań, 2001.

20. **Szafrański B.** – „Bezpieczeństwo nade wszystko", Computerworld, sierpień, 2004r.

21. **Szafrański B., Weydmann R., Żurek L.** – „Model informacyjny rejestrów państwowych i wymagania w zakresie systemu komputerowego wspomagania zarządzania rejestrami", materiały Ministerstwa Nauki i Informatyzacji, 2003,

22. **Szafrański B.** – „Interoperacyjność rejestrów publicznych w Polsce", materiały konferencji: „Ewidencje i rejestry w administracji publicznej", CPI, Warszawa, 2005,

23. **Wiśniewski M.**– „Interoperacyjność systemów informacyjnych", Gazeta it, nr 9, 2005.

Uwagi:

a) Ponadto w książce wykorzystano wybrane idee prezentowane w trakcie dyskusji seminaryjnych przede wszystkim przez zespoły: prof. Witolda Abramowicza, Zbigniewa Główki, prof. Jerzego Kisielnickiego, prof. Józefa Oleńskiego, Marka Słowikowskiego, Borysa Stokalskiego oraz przedstawicieli samorządów (Krzysztofa Głomba, Józefa Orła, Kajetana Wojsyka, Dariusza Woźniaka).

b) Dane bibliograficzne analizowanych aktów prawnych i normatywnych zawarto w załączniku nr 1.

Załącznik nr 1: „Uogólniony materiał analityczny dotyczący aktów prawnych i normatywnych"

Szczegółowy wykaz analizowanych aktów prawnych i normatywnych

Ustawy ogólne i akty wykonawcze do nich:

- NIEJAWNE – Ustawa z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych (Dz.U. 1999 nr 11 poz. 95)
- NIEJAWNE – Rozporządzenie Prezesa Rady Ministrów z dnia 25 sierpnia 2005 r. w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego (Dz.U. 2005 nr 171 poz. 1433)
- NIEJAWNE – Rozporządzenie Prezesa Rady Ministrów z dnia 29 września 2005 r. w sprawie trybu i sposobu przyjmowania, przewożenia, wydawania i ochrony materiałów zawierających informacje niejawne (Dz.U. 2005 nr 200 poz. 1650)
- NIEJAWNE – Rozporządzenie Prezesa Rady Ministrów z dnia 5 października 2005 r. w sprawie sposobu oznaczania materiałów, umieszczania na nich klauzul tajności, a także zmiany klauzuli tajności (Dz.U. 2005 nr 205 poz. 1696)
- NIEJAWNE – Rozporządzenie Rady Ministrów z dnia 18 października 2005 r. w sprawie organizacji i funkcjonowania kancelarii tajnych (Dz.U. 2005 nr 208 poz. 1741).
- OSOBOWE – Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. 1997 nr 133 poz. 883)
- OSOBOWE – Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U. 2004 nr 100 poz. 1024)
- OSOBOWE – Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie wzoru zgłoszenia zbioru danych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych (Dz.U. 2004 nr 100 poz. 1025)
- INFORMATYZACJA – Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U. 2005 nr 64 poz. 565)

- INFORMATYZACJA – Rozporządzenie Rady Ministrów z dnia 27 września 2005 r. w sprawie sposobu, zakresu i trybu udostępniania danych zgromadzonych w rejestrze publicznym (Dz.U. 2005 nr 205 poz. 1692)
- INFORMATYZACJA – Rozporządzenie Rady Ministrów z dnia 11 października 2005 r. w sprawie minimalnych wymagań dla systemów teleinformatycznych (Dz. U. 2005 nr 212 poz. 1766)
- INFORMATYZACJA – Rozporządzenie Rady Ministrów z dnia 11 października 2005 r. w sprawie minimalnych wymagań dla rejestrów publicznych i wymiany informacji w formie elektronicznej (Dz.U. 2005 nr 214 poz. 1781)
- INFORMATYZACJA – Rozporządzenie Ministra Nauki i Informatyzacji z dnia 19 października 2005 r. w sprawie testów akceptacyjnych oraz badania oprogramowania interfejsowego i weryfikacji tego badania (Dz.U. 2005 nr 217 poz. 1836).

Ustawy i akty wykonawcze dla wybranych rejestrów

- PESEL – Ustawa z dnia 10 kwietnia 1974 r. o ewidencji ludności i dowodach osobistych (Dz. U. z 2001 r. nr 87 poz. 960 z późn. zm.)
- PESEL – Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 20 grudnia 2002 r. w sprawie trybu przekazywania danych pomiędzy organami prowadzącymi ewidencję ludności oraz powiadamianie o nadaniu numeru PESEL (Dz. U. z 2002 r. nr 236 poz. 1996)
- KRS – Ustawa z dnia 20 sierpnia 1997 r. o Krajowym Rejestrze Sądowym (Dz. U z 1997 roku, nr 121, poz. 769)
- KRS – Rozporządzenie Ministra Sprawiedliwości z dnia 21 grudnia 2000 r. w sprawie ustroju i organizacji Centralnej Informacji Krajowego Rejestru Sądowego oraz szczegółowych zasad udzielania informacji z Krajowego Rejestru Sądowego (Dz. U. 2000 nr 117 poz. 1238)
- TERYT – Ustawa z dnia 29 czerwca 1995r. o statystyce publicznej (Dz. U. Nr 88 poz. 439)
- TERYT – Rozporządzenie Rady Ministrów z dnia 15 grudnia 1998 r. w sprawie szczegółowych zasad prowadzenia, stosowania i udostępniania krajowego rejestru urzędowego podziału terytorialnego kraju oraz związanych z tym obowiązków organów administracji rządowej i jednostek samorządu terytorialnego (Dz. U. 1998 nr 157 poz. 1031)

Ustawy branżowe i akty wykonawcze do nich

- STATYSTYKA – Ustawa z dnia 29 czerwca 1995r o statystyce publicznej (Dz. U. z 1995 r. Nr 88 poz. 439 z późn. zm.)
- STATYSTYKA – Rozporządzenie Rady Ministrów z dnia 27 lipca 1999 r. w sprawie sposobu i metodologii prowadzenia i aktualizacji rejestru podmiotów gospodarki narodowej, w tym wzorów wniosków, ankiet i zaświadczeń, oraz szczegółowych warunków i trybu współdziałania służb statystyki publicznej z innymi

organami prowadzącymi urzędowe rejestry i systemy informacyjne administracji publicznej (Dz.U. 1999 nr 69 poz. 763)

- BANKOWA – Ustawa z dnia 29 sierpnia 1997 r. Prawo bankowe (Dz. U. z dnia 21 listopada 1997 r.).

Normy międzynarodowe (przyjęte oficjalnie w Polsce) dotyczące problematyki bezpieczeństwa systemów informatycznych

- PN-I-13335-1 – „Technika informatyczna – Wytyczne do zarządzania bezpieczeństwem systemów informatycznych. Pojęcia i modele bezpieczeństwa systemów informatycznych",
- PN-ISO/IEC 17799 – „Technika informatyczna – Praktyczne zasady zarządzania bezpieczeństwem informacji",
- PN-I-07779-2 – „Systemy zarządzania bezpieczeństwem informacji – Część 2: Specyfikacja i wytyczne do stosowania".

Wyniki analizy aktów prawnych pod kątem przetwarzania informacji o różnych klauzulach tajności

Aspekty organizacyjno-prawne

- W regulacjach ogólnych wprowadza się pojęcia:
  - „Informacji niejawnych" – chronionych w podstawowym interesie państwa („tajemnica państwowa") lub w interesie państwa, interesie publicznym lub prawnie chronionym interesie obywateli albo jednostki organizacyjnej („tajemnica służbowa").

[Jak widać, już na poziomie definicji ustawowych granica pomiędzy tajemnicą państwową a tajemnicą służbową jest „rozmyta" – w obu występuje pojęcie „interesu państwa"]

  - „Danych osobowych" – chronionych w interesie obywateli.
- Ustawa o ochronie informacji niejawnych i akty wykonawcze do niej koncentrują się na ochronie dokumentów, tj. cyt.: "każdej utrwalonej informacji niejawnej, (...) również informacji niejawnej utrwalonej na elektronicznych nośnikach danych". Oznacza to, że zapisy tych aktów prawnych dotyczą również informacji/danych niejawnych przetwarzanych w systemach/sieciach teleinformatycznych.
- Podstawowe zapisy dot. klasyfikacji informacji niejawnych:
  - Klasyfikowanie informacji niejawnej oznacza przyznanie tej informacji jednej z klauzul tajności, o których mowa w ustawie o ochronie informacji niejawnych [omówiono je w dalszej części niniejszego punktu].
  - Dokumentom lub ich zbiorom przyznaje się klauzulę tajności co najmniej równą najwyżej zaklasyfikowanej informacji lub najwyższej klauzuli w zbiorze.

[Jest to reguła bardzo istotna z punktu widzenia celów niniejszej publikacji]

- Dopuszczalne jest przyznawanie różnych klauzul tajności częściom dokumentu lub poszczególnym dokumentom w zbiorze dokumentów, pod warunkiem wyraźnego ich oznaczenia i wskazania klauzuli po odłączeniu dokumentu bądź jego części.
- Klauzulę tajności przyznaje osoba, która jest upoważniona do podpisania dokumentu i bez jej zgody albo bez zgody jej przełożonego klauzula nie może być zmieniona lub zniesiona.

[Jest to reguła istotna z punktu widzenia celów niniejszej publikacji]

- Zawyżanie lub zaniżanie klauzuli tajności jest niedopuszczalne.
- Informacje niejawne stanowiące tajemnicę państwową podzielono na:
  a) oznaczone klauzulą „ściśle tajne",
  b) oznaczone klauzulą „tajne".
- Informacje niejawne stanowiące tajemnicę służbową podzielono na:
  a) oznaczone klauzulą „poufne",
  b) oznaczone klauzulą „zastrzeżone".
- Materiały (czyli m.in. dokumenty) otrzymywane z zagranicy oraz wysyłane za granicę oznacza się odpowiednią do ich treści klauzulą tajności określoną w ustawie oraz jej zagranicznym odpowiednikiem.

[W ogólnym przypadku oznaczenie dokumentu zagranicznym odpowiednikiem polskiej klauzuli tajności (lub odwrotnie – polskim odpowiednikiem klauzuli zagranicznej) może nie być oczywiste – co wynika z dwóch przesłanek:

a) po pierwsze, różne mogą być polskie i zagraniczne kryteria stosowane do klasyfikowania informacji,
b) po drugie, czysto techniczny problem powstaje w sytuacji, gdy polski i zagraniczny systemy klasyfikowania mają różne ilości wartości „niejawności"; w polskim systemie zbiór dopuszczalnych wartości ma pięć elementów (ściśle tajne, tajne, poufne, zastrzeżone, jawne).

Z uwagi na pierwszą przesłankę należy porównać polskie i zagraniczne kryteria. W przypadku stwierdzenia niezgodności konieczne wydaje się indywidualne rozpatrywanie przypadku każdego dokumentu.

Można podjąć próbę uniknięcia konieczności takiego podejścia po stwierdzeniu prawdziwości drugiej przesłanki poprzez stworzenie tablicy przejść z polskich na zagraniczne klauzule tajności.]

- Informacje niejawne stanowiące tajemnicę państwową podlegają ochronie w sposób określony niniejszą ustawą przez 50 lat od daty ich wytworzenia.

[Jest to reguła istotna z punktu widzenia kosztów systemu przechowywania]

- Informacje niejawne stanowiące tajemnicę służbową podlegają ochronie w sposób określony niniejszą ustawą przez okres:
  a) 5 lat – oznaczone klauzulą „poufne",
  b) 2 lat – oznaczone klauzulą „zastrzeżone";

Osoba upoważniona może skrócić ten okres albo go wydłużyć na kolejne okresy o tej samej długości, nie dłużej jednak niż na okres 20 lat.

[Jest to reguła istotna z punktu widzenia kosztów systemu przechowywania]

- Podstawowe zapisy dotyczące systemów teleinformatycznych przetwarzających dane/informacje prawnie chronione zawarte w regulacjach ogólnych:
  - Systemy i sieci teleinformatyczne, w których mają być wytwarzane, przetwarzane, przechowywane lub przekazywane **informacje niejawne**, podlegają akredytacji bezpieczeństwa teleinformatycznego przez służby ochrony państwa.

[Jest to reguła istotna z punktu widzenia kosztów budowy i przygotowania do wdrożenia systemu informatycznego]

  - Określono podstawowe warunki bezpieczeństwa teleinformatycznego.
  - Określono warunki techniczne i organizacyjne, jakim powinny odpowiadać systemy informatyczne, służące do przetwarzania danych osobowych.
  - System informatyczny przetwarzający dane osobowe powinien umożliwić odnotowanie i udostępnienie na piśmie, w powszechnie zrozumiałej formie, treści danych o każdej osobie, której dane są przetwarzane, wraz z informacjami następującymi:
    a) data pierwszego wprowadzenia danych tej osoby,
    b) źródło pochodzenia danych,
    c) identyfikator użytkownika wprowadzającego dane,
    d) informacja komu, kiedy i w jakim zakresie dane zostały udostępnione,
    e) sprzeciw wobec przetwarzania danych konkretnej osoby.
  - Na podstawie ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne określono:
    a) minimalne wymagania dla systemów teleinformatycznych, mając na uwadze konieczność zapewnienia:
       i. spójności działania systemów teleinformatycznych używanych do realizacji zadań publicznych poprzez określenie co najmniej specyfikacji formatów danych oraz protokołów komunikacyjnych i szyfrujących, które mają być stosowane w oprogramowaniu interfejsowym
       ii. sprawnej i bezpiecznej wymiany informacji w formie elektronicznej między podmiotami publicznymi oraz między podmiotami publicznymi a organami innych państw lub organizacji międzynarodowych,

z uwzględnieniem Polskich Norm oraz innych dokumentów normalizacyjnych zatwierdzonych przez krajową jednostkę normalizacyjną, zachowując zasadę równego traktowania różnych rozwiązań informatycznych,

    b) minimalne wymagania dla rejestrów publicznych i wymiany informacji w formie elektronicznej, uwzględniając konieczność zachowania spójności prowadzenia rejestrów publicznych i wymiany informacji w formie elektronicznej z podmiotami publicznymi.

- Podstawowe zapisy dotyczące organizacji ochrony danych/informacji prawnie chronione zawarte w regulacjach ogólnych:
  - Za ochronę informacji niejawnych odpowiada kierownik jednostki organizacyjnej, w której takie informacje są wytwarzane, przetwarzane, przekazywane lub przechowywane.
  - Informacje niejawne, którym przyznano określoną klauzulę tajności muszą być wytwarzane, przetwarzane, przekazywane lub przechowywane w warunkach uniemożliwiających ich nieuprawnione ujawnienie, zgodnie z przepisami określającymi wymagania dotyczące kancelarii tajnych, obiegu i środków fizycznej ochrony informacji niejawnych, odpowiednich dla przyznanej im klauzuli tajności.

[Nie określono wyjątków od tej zasady, a więc dotyczy to również informacji/danych niejawnych przetwarzanych w systemach/sieciach teleinformatycznych]

  - Zasady działania kancelarii tajnej:
    a) w kancelarii tajnej dokumenty o różnych klauzulach powinny być fizycznie od siebie oddzielone,
    b) organizacja pracy kancelarii tajnej musi zapewniać możliwość ustalenia w każdych okolicznościach, gdzie znajduje się dokument klasyfikowany pozostający w dyspozycji jednostki organizacyjnej,
    c) dokumenty oznaczone klauzulami „ściśle tajne" i „tajne" mogą być wydawane poza kancelarię tajną jedynie w przypadku, gdy odbiorca zapewnia warunki ochrony takich dokumentów przed nieuprawnionym ujawnieniem. W razie wątpliwości co do zapewnienia warunków ochrony, dokument może być udostępniony wyłącznie w kancelarii tajnej,
    d) fakt zapoznania się przez osobę uprawnioną z dokumentem zawierającym informacje niejawne stanowiące tajemnicę państwową podlega odnotowaniu w karcie zapoznania się z dokumentem.

[Zapisy powyższe, literalnie dotyczące dokumentów przetwarzanych w kancelarii tajnej, są – zdaniem autorów – przesłanką, którą należy uwzględnić w trakcie budowy i eksploatacji SI]

  - W ustawie o ochronie informacji niejawnych i rozporządzeniach wydanych na jej podstawie określono zasady:
    a) uzyskiwania certyfikatu bezpieczeństwa teleinformatycznego dla systemów informatycznych, w których przetwarzane są informacje niejawne
    b) dopuszczania do pracy lub pełnienia służby na stanowisku albo zlecenia pracy, z którymi może się łączyć dostęp do informacji niejawnych
    c) organizacji eksploatacji systemów informatycznych, w których przetwarzane są informacje niejawne
  - W ustawie o ochronie danych osobowych i rozporządzeniach wydanych na jej podstawie określono:
    a) zasady dopuszczania do przetwarzania danych osobowych

b) zasady zgłaszania zbioru danych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych
c) strukturę i zawartość dokumentacji przetwarzania danych osobowych
d) poziomy bezpieczeństwa przetwarzania danych osobowych w systemach informatycznych.

– Na podstawie ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne określono sposób, zakres i tryb udostępniania danych zgromadzonych w rejestrze publicznym.

- W ustawie o informatyzacji działalności podmiotów realizujących zadania publiczne i jej aktach wykonawczych:
  – określono sposób, zakres i tryb udostępniania danych zgromadzonych w rejestrze publicznym,
  – wskazano, iż systemy teleinformatyczne używane przez podmioty publiczne do realizacji zadań publicznych powinny zostać wyposażone w składniki sprzętowe i programowe:
    a) umożliwiające wymianę danych z innymi systemami teleinformatycznymi do realizacji zadań publicznych za pomocą określonych protokołów komunikacyjnych i szyfrujących
    b) zapewniające dostęp do zasobów informacji udostępnianych przez systemy teleinformatyczne używane do realizacji zadań publicznych przy wykorzystaniu określonych formatów danych.,
  – sformułowano wymóg, aby – jeżeli w wymianie informacji w formie elektronicznej, w tym z rejestrami publicznymi, stosuje się cechę informacyjną tożsamą co do treści z wymienioną cechą informacyjną – cechę stosować zgodnie z określoną definicją.
- W ustawach będących podstawą prowadzenia wybranych rejestrów kwestia poufności gromadzonych w nich danych jest określana w sposób zróżnicowany, nie zawsze wprost:
  – Dla rejestru PESEL w ustawie o ewidencji ludności i dowodach osobistych oraz aktach wykonawczych wydanych na jej podstawie:
    a) używa się pojęcia „dane osobowe" dla określenia przedmiotu działania organów prowadzących ewidencję ludności, ale bez jawnego odwołania się do ustawy o ochronie danych osobowych jako podstawy prawnej ochrony tych danych,
    b) nie przypisuje się danym gromadzonym w rejestrze żadnej z klauzul tajności,
    c) ale: określa się obowiązek przesyłania danych w łańcuchu gmina <–> urząd wojewody <–> minister właściwy ds. administracji w sposób „uniemożliwiający dostęp do nich osób nieupoważnionych" a dla podmiotów pozyskujących dane osobowe ze zbiorów meldunkowych, zbioru PESEL drogą teletransmisji sformułowano wymóg posiadania zabezpieczenia technicznego i organizacyjnego „uniemożliwiającego wykorzystanie danych niezgodnie z celem ich uzyskania".

[na dzień dzisiejszy zbiór PESEL ma klauzulę „poufne" – naszym zdaniem niezasadnie, co pokazujemy w rozdz. 10]

- Dla rejestru KRS w ustawie o Krajowym Rejestrze Sądowym jest zapis wskazujący, iż jest to rejestr jawny.
- Dla rejestru TERYT ustawa o statystyce publicznej przesądza, że jest on jawny a informacje zbierane i gromadzone w nim nie podlegają rygorom poufności i tajemnicy statystycznej.

- Inne regulacje dotyczące wybranych rejestrów:
  - Dla rejestru PESEL Ustawa o ewidencji ludności i dowodach osobistych określa wymóg prowadzenia ewidencji ludności na wszystkich poziomach (minister właściwy ds. administracji publicznej, wojewoda, organy gminy) w SI, a jedno z rozporządzeń dopuszcza możliwość prowadzenia ewidencji ludności przez organy gminy w systemie kartotecznym.
  - Dla rejestru PESEL dla podmiotów pozyskujących dane osobowe ze zbiorów meldunkowych oraz zbioru PESEL drogą teletransmisji sformułowano wymóg posiadania urządzeń umożliwiających identyfikację osoby uzyskującej dane w systemie oraz zakresu, daty i celu ich uzyskania.
- W ustawach branżowych wprowadza się pojęcia „tajemnic branżowych"; ich przykłady w przeanalizowanych aktach prawnych to „tajemnica bankowa" i „tajemnica statystyczna"; oczywiście informacje/dane o takich klauzulach są prawnie chronione
- Regulacje branżowe:
  - W prawie bankowym nie ma zapisów określających wymagania na systemy informatyczne w związku z ewentualną poufnością przetwarzanych w nich danych,
  - W ustawie o statystyce publicznej zabroniono gromadzenia w jednym zbiorze lub w jednej bazie danych wszystkich zebranych przez służby statystyki publicznej danych osobowych dotyczących konkretnej osoby fizycznej, pochodzących z różnych badań statystycznych, które w połączeniu mogą służyć do charakterystyki lub oceny osoby
  - Określono maksymalny okres przetwarzania informacji stanowiących tajemnicę bankową w celu oceny zdolności kredytowej i analizy ryzyka kredytowego (5 lat od daty wygaśnięcia zobowiązania).
  - Urzędy statystyczne udostępniają nieodpłatnie organom prowadzącym urzędowe rejestry oraz systemy informacyjne administracji publicznej okresowo wykazy podmiotów wpisanych do rejestru REGON wraz z nadanym im numerem identyfikacyjnym oraz zakodowanym opisem informacji objętych rejestrem.
  - Jednym z zadań GUS związanym z prowadzeniem rejestru podmiotów gospodarki narodowej (REGON) jest ustalenie form wymiany informacji z organami prowadzącymi rejestry i ewidencje lub systemy informacyjne administracji publicznej.

- Służby statystyki publicznej udostępniają nieodpłatnie:
  a) organom prowadzącym inne urzędowe rejestry i systemy informacyjne administracji publicznej wykazy podmiotów wpisanych do rejestru wraz z nadanym im numerem identyfikacyjnym i zakodowanym opisem informacji objętej rejestrem
  b) organom administracji rządowej oraz innym instytucjom rządowym, organom samorządu terytorialnego, Najwyższej Izby Kontroli, Narodowemu Bankowi Polskiemu, Państwowej Inspekcji Pracy oraz Generalnemu Inspektorowi Ochrony Danych Osobowych, na ich pisemny wniosek, wyciągi z rejestru.
- W rozporządzeniu w sprawie sposobu i metodologii prowadzenia i aktualizacji rejestru podmiotów gospodarki narodowej określono zasady okresowego przekazywania przez Prezesa GUS bazy danych rejestru:
  a) do Centralnej Informacji Krajowego Rejestru Sądowego
  b) do centralnej informacji o zastawach rejestrowych
  c) Ministrowi Finansów na potrzeby Krajowej Ewidencji Podatników
  d) Prezesowi ZUS na potrzeby kompleksowego systemu informatycznego ZUS.
- Dodatkowo w ww. rozporządzeniu są zapisy o przekazywaniu Prezesowi GUS informacji przez 3 konkretne podmioty:
  a) Minister Sprawiedliwości przekazuje informacje zgromadzone w Centralnej Informacji KRS o podmiotach wpisanych do KRS
  b) Minister Finansów przekazuje informacje zgromadzone w krajowej ewidencji podatników (KEP) o podmiotach wpisanych do KEP
  c) Prezes ZUS przekazuje informacje o liczbie pracujących dla poszczególnych podmiotów, zgromadzone w rejestrach ZUS.

Aspekty techniczne

- Regulacje ogólne:
  - W ustawie o ochronie informacji niejawnych i rozporządzeniach wydanych na jej podstawie:
    a) określono że urządzenia i narzędzia kryptograficzne wchodzące w skład systemów i sieci teleinformatycznych przetwarzających informacje niejawne stanowiące tajemnicę państwową (klauzule „ściśle tajne" i „tajne") oraz tajemnicę służbową dla klauzuli „poufne" podlegają badaniom i certyfikacji prowadzonym przez służby ochrony państwa,
    b) wskazano sposoby zapewnienia poszczególnych typów ochrony systemów/lub sieci teleinformatycznych (ochrona elektromagnetyczna, ochrona kryptograficzna, niezawodność transmisji).
  - W ustawie o ochronie danych osobowych i rozporządzeniach wydanych na jej podstawie:
    a) zobowiązano administratora danych do zastosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzania danych

osobowych, a w szczególności dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieupoważnioną, przetwarzaniem z naruszeniem ustawy, zmianą, utratą, uszkodzeniem lub zniszczeniem

b) określono wymagane środki bezpieczeństwa dla poszczególnych poziomów bezpieczeństwa danych osobowych.

– W minimalnych wymaganiach dla systemów teleinformatycznych, określonych w rozporządzeniu wykonawczym do ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne wskazano, że systemy teleinformatyczne używane przez podmioty publiczne do realizacji zadań publicznych powinny zostać wyposażone w składniki sprzętowe i programowe zapewniające dostęp do zasobów informacji udostępnianych przez systemy teleinformatyczne używane do realizacji zadań publicznych przy wykorzystaniu określonych formatów danych.

- Regulacje dotyczące wybranych rejestrów:
  – Dla rejestru PESEL:
    a) określono obowiązek przesyłania danych w łańcuchu gmina <–> urząd wojewody <–> minister w sposób „uniemożliwiający dostęp do nich osób nieupoważnionych"
    b) dla podmiotów pozyskujących dane osobowe ze zbiorów meldunkowych oraz zbioru PESEL drogą teletransmisji sformułowano wymóg posiadania urządzeń umożliwiających identyfikację osoby uzyskującej dane w systemie oraz zakresu, daty i celu ich uzyskania a także zabezpieczenia technicznego i organizacyjnego „uniemożliwiającego wykorzystanie danych niezgodnie z celem ich uzyskania".
  – Ponieważ rejestry KRS i TERYT są jawne, więc w zapisach prawnych nie ma zapisów określających wymagania techniczne z tytułu poufności danych w tych rejestrach utrzymywanych.
- W przeanalizowanych regulacjach branżowych brak zapisów nt. wymagań technicznych wynikających z potrzeb przetwarzania informacji poufnych.

Aspekty ekonomiczne

- W przeanalizowanych regulacjach prawnych brak zapisów wprost dotyczących wymagań ekonomicznych związanych z potrzebą przetwarzania informacji poufnych.

Wyniki analizy aktów normatywnych pod kątem przetwarzania informacji o różnych klauzulach tajności

Aspekty organizacyjno-prawne

- Zaleca się klasyfikowanie informacji, tak aby wskazać potrzebę, priorytety i poziom ochrony. Zaleca się wykorzystywanie systemu klasyfikowania informacji do zdefiniowania odpowiedniego zbioru poziomów ochrony i do informowania o potrzebie użycia specjalnych środków postępowania.

- Wybrane wytyczne w zakresie klasyfikacji informacji:
  - Zaleca się aby w klasyfikacjach i związanych z nimi zabezpieczeniach ochrony informacji były uwzględniane **potrzeby współużytkowania** lub zastrzegania informacji oraz skutki dla działalności biznesowej związane z tymi potrzebami, np. nieuprawniony dostęp lub zniszczenie informacji.

[na poziomie różnych SI potrzeba współużytkowania jest synonimem interoperacyjności!]

  - Zaleca się, aby informacje i dane wyjściowe z systemów obsługujących klasyfikowane dane były oznakowane w zależności od ich ważności dla instytucji i **wrażliwości** *[pojęcie „informacje/dane wrażliwe" jest używane tutaj i w dalszym części niniejszego rozdziału w znaczeniu „informacje/dane wymagające ochrony" (zarówno na podstawie ustaw i aktów wykonawczych jak i na podstawie regulacji wewnętrznych instytucji/jednostki organizacyjnej)]*. Może być stosowne także oznakowanie informacji w zależności od ich krytyczności dla organizacji, np. wg kryteriów integralności i dostępności. Zaleca się, aby wytyczne klasyfikacji z góry nie zakładały, że nie jest konieczne, aby klasyfikacja jakiejkolwiek informacji była bezterminowa, ale że może zostać zmieniona zgodnie z ustaloną wcześniej polityką;

[Wskazane aspekty są ważne z punktu widzenia kosztów gromadzenia, przechowywania i przetwarzania informacji]

  - Zaleca się, aby uważać przy interpretacji oznaczeń stosowanych w klasyfikacji dokumentów otrzymanych z innych organizacji, które mogą mieć różne definicje dla tych samych lub podobnie brzmiących oznaczeń.

[Na problem ten autorzy zwrócili już uwagę w komentarzu do ósmego myślnika w ramach trzeciej kropki w punkcie „Aspekty poufności" poprzedniego podrozdziału]

  - Zaleca się, aby obowiązek w zakresie określania klasyfikacji elementu informacji, a także okresowego przeglądania klasyfikacji spoczywał na twórcy lub wyznaczonym **właścicielu informacji**.

[Zwracamy uwagę, że zalecenie to jest uogólnieniem zapisu z ustawy o ochronie informacji niejawnych, gdzie mówi się tylko o twórcy („osoba upoważniona do podpisania dokumentu")]

- Oznaczanie i postępowanie z informacją:
  - Bardzo ważne jest, aby został zdefiniowany odpowiedni zestaw procedur oznaczania i postępowania z informacją, zgodnych z przyjętym w instytucji schematem klasyfikacji. Procedury te powinny dotyczyć aktywów informacji w formie fizycznej i elektronicznej. Zaleca się, aby dla każdej kategorii klasyfikacji były określone procedury postępowania z informacją, odnoszące się do następujących czynności przetwarzania informacji:
    a) kopiowanie,
    b) przechowywanie,
    c) przesyłanie/przekazywanie przy użyciu różnych mediów,
    d) niszczenie.

- Zaleca się, aby zwracać uwagę na ochronę integralności informacji elektronicznej udostępnianej publicznie, w celu zapobieżenia nieupoważnionej modyfikacji, która mogłaby naruszyć dobre imię instytucji. Zaleca się, aby przed publicznym udostępnieniem informacji miał miejsce formalny proces jej zatwierdzania.
- Zaleca się, aby oprogramowanie, dane i inne informacje, udostępniane za pomocą systemu publicznie dostępnego i wymagające wysokiego poziomu integralności było chronione za pomocą odpowiednich mechanizmów, np. podpisów cyfrowych. Zaleca się staranne zabezpieczenie elektronicznych systemów publikacji, w szczególności tych, które pozwalają na odpowiedź i bezpośrednie wprowadzanie informacji, tak aby:
  - informacja była otrzymywana zgodnie z prawem dotyczącym ochrony danych,
  - informacja wprowadzana i przetwarzana przez system publikacji była przetwarzana w całości, dokładnie i w odpowiednim czasie,
  - informacje wrażliwe były chronione podczas procesu ich zbierania i w czasie ich przechowywania,
  - dostęp do systemu publikacji nie pozwalał na niezamierzony dostęp do sieci lokalnych, do których jest on podłączony.
- Zaleca się lokalizację urządzeń do przetwarzania krytycznych lub wrażliwych informacji w obszarach bezpiecznych, chronionych wyznaczonym obwodem zabezpieczającym, z odpowiednimi barierami i kontrolą wstępu.
- Zaleca się opracowanie rutynowych procedur realizacji uzgodnionej strategii sporządzania zapasowych kopii, sporządzania zapasowych kopii danych i próbnego ich przywracania, rejestrowania w dziennikach zdarzeń i błędów.
- Zaleca się stworzenie właściwych procedur operacyjnych dla ochrony dokumentów, nośników komputerowych (taśm, dysków, kaset), danych wejściowych i wyjściowych oraz dokumentacji systemowej przed uszkodzeniem, kradzieżą i nieuprawnionym dostępem.
- Zaleca się opracowanie procedur zarządzania wyjmowalnymi nośnikami komputerowymi, takimi jak taśmy, dyski, kasety oraz drukowanymi raportami. Zaleca się:
  - wymazanie poprzedniej zawartości wszelkich nośników wielokrotnego użytku, które mają być wyniesione z instytucji, o ile nie będzie już potrzebna,
  - zaleca się, aby w przypadku wynoszenia jakichkolwiek nośników z instytucji potrzebne były upoważnienia, a w celu przeprowadzenia późniejszego audytu zaleca się prowadzenie odpowiedniej ewidencji,
  - zaleca się przechowywanie wszystkich nośników w bezpiecznym miejscu, zgodnie z zaleceniami ich producentów.
- W celu ochrony przed nieuprawnionym ujawnieniem lub nadużyciem informacji zaleca się stworzenie procedur postępowania z nimi i ich przechowywania. Zaleca się też opracowanie procedur posługiwania się informacjami, zgodnie z ich klasyfikacją, zawartymi w dokumentach, przetwarzanymi w systemach przetwarzania danych, komputerach przenośnych.

- Zaleca się, aby wymiany danych prowadzić na podstawie umów. Zaleca się tworzenie procedur i standardów ochrony informacji i nośników podczas transportu. Zaleca się rozważenie skutków zarówno dla działalności biznesowej, jak i dla bezpieczeństwa, związanych z elektroniczną wymianą danych oraz wymagań dotyczących zabezpieczeń.
- Zaleca się opracowanie formalnych procedur kontroli przyznawania praw dostępu do systemów i usług informacyjnych. Zaleca się, aby procedury obejmowały wszystkie etapy w „cyklu życia" dostępu użytkownika, od początkowej rejestracji nowych użytkowników do końcowego wyrejestrowania użytkowników, którzy nie wymagają już dostępu do systemów i usług informacyjnych. Zaleca się, aby specjalną uwagę zwrócić, tam gdzie to jest właściwe, na potrzebę kontroli przyznawania uprzywilejowanych praw dostępu, które pozwalają obchodzić systemowe mechanizmy zabezpieczenia.
- Zaleca się, aby przyznawanie i używanie przywilejów (wszelkich funkcji lub urządzeń w wielożytkownikowych SI, które pozwalają użytkownikowi na obejście zabezpieczeń systemu lub aplikacji) ograniczać i kontrolować. W systemach wielożytkownikowych, które wymagają ochrony przed nieuprawnionym dostępem, zaleca się kontrolowanie przydzielania przywilejów za pośrednictwem formalnego procesu autoryzacji.
- Zaleca się ścisłe kontrolowanie środowisk projektowych i wsparcia informatycznego. Zaleca się, aby kierownicy odpowiedzialni za systemy aplikacji byli również odpowiedzialni za zabezpieczenie środowiska, w którym są prowadzone prace rozwojowe i obsługa informatyczna oraz zapewniali, że wszystkie proponowane zmiany w systemach będą podlegać ocenie z punktu widzenia osłabienia bezpieczeństwa, zarówno systemu, jak i środowiska eksploatacyjnego.
- Zaleca się wymuszanie formalnych procedur kontroli zmian. Zaleca się, aby procedury te zapewniały, że bezpieczeństwo i procedury kontrolne nie zostały naruszone, programiści mają dostęp jedynie do części systemu, które są niezbędne do ich pracy, a ponadto wykonywanie jakiejkolwiek zmiany jest poprzedzone uzyskaniem formalnej zgody i upoważnienia.
- Należy zwrócić uwagę na wymagania prawne dotyczące tzw. transgranicznego przepływu danych (informacja jest utworzona w jednym kraju i przysłana do innego kraju) – mogą one być różne w poszczególnych krajach.
- Zabezpieczanie dokumentów instytucji:
  - Zaleca się, aby wszelkie klucze kryptograficzne związane z zaszyfrowanymi archiwami i podpisami elektronicznymi przechowywać w bezpiecznym miejscu i w razie potrzeby udostępniać uprawnionym osobom.
  - Zaleca się uwzględnienie zjawiska starzenia się nośników używanych do przechowywania zapisów. Zaleca się, aby wdrożone procedury przechowywania i postępowania były zgodne z zaleceniami producenta nośnika.
  - W przypadku zastosowania do przechowywania zapisów nośników elektronicznych, zaleca się wprowadzanie procedur zapewniających dostęp do da-

nych (możliwość czytania danego nośnika i formatu) przez cały okres przechowywania, tak aby zabezpieczyć się przed utratą danych, spowodowaną zmianami technologii w przyszłości.

- Zaleca się, aby system przechowywania danych i ich obsługi zapewniał możliwość łatwej identyfikacji zapisu jego ustawowego lub określonego wewnętrznymi przepisami okresu przechowywania, a także odpowiedniego niszczenia zapisów po upłynięciu tego okresu, jeżeli nie są już potrzebne instytucji.

Aspekty techniczne

- Identyfikacja i uwierzytelnianie użytkowników:
  - Trzeba zapewnić, aby wszyscy użytkownicy (w tym personel obsługi technicznej) mieli unikalne identyfikatory użytkownika do swojego osobistego i wyłącznego użytku.
  - Istnieją różne procedury uwierzytelniania, które mogą być użyte, aby potwierdzić tożsamość użytkownika. Stosowanie haseł jest bardzo częstym sposobem zapewnienia identyfikacji i uwierzytelnienia, opartym na tajemnicy znanej tylko użytkownikowi. To samo można osiągnąć, stosując techniki kryptograficzne i protokoły uwierzytelniania.
  - Urządzenia, takie jak tokeny pamięciowe czy karty elektroniczne, które znajdują się w posiadaniu użytkownika, mogą również być użyte w celu identyfikacji i uwierzytelnienia. Uwierzytelnienie tożsamości osoby może być oparte także na biometrycznych technikach wykorzystujących unikalne cechy szczególne lub atrybuty tej osoby. Kombinacja technik i mechanizmów, łączonych w bezpieczny sposób, pozwoli na silniejsze uwierzytelnienie.
- Zaleca się, aby dostęp logiczny do informacji i oprogramowania komputerowego był zastrzeżony wyłącznie dla uprawnionych użytkowników. Trzeba zapewnić, aby systemy aplikacji:
  - Kontrolowały dostęp użytkowników do informacji i funkcji systemu aplikacji, zgodnie ze zdefiniowaną polityką kontroli dostępu uwzględniającą cele działalności biznesowej,
  - Chroniły przed nieuprawnionym dostępem do jakiegokolwiek oprogramowania narzędziowego lub systemowego, które umożliwiałoby obejście zabezpieczeń w systemie lub aplikacji,
  - Uniemożliwiały naruszenie bezpieczeństwa innych systemów, z którymi są współużytkowane zasoby informacyjne,
  - Umożliwiały dostęp do informacji jedynie jej właścicielowi, innym wyznaczonym osobom lub zdefiniowanym grupom użytkowników.
- Zaleca się rozważenie zastosowania niżej podanych zabezpieczeń, tak aby zrealizować wymagania ograniczania dostępu do informacji:
  - Zapewnianie, że dane wyjściowe z systemów aplikacji przetwarzających informacje wrażliwe zawierają jedynie informacje przewidywane do dalszego

użycia oraz, że są one wysyłane tylko do uprawnionych terminali lub miejsc, włączając w to okresowe przeglądy danych wyjściowych, tak aby zapewnić, że nadmiarowe informacje są usuwane.

[Jest to zalecenie do bezpośredniego wykorzystania w systemach informatycznych przetwarzających dane/informacje prawnie chronione].

- Systemy wrażliwe mogą wymagać dedykowanego (izolowanego) środowiska przetwarzania. Trzeba brać pod uwagę niżej podane zagadnienia.
  - Zaleca się, aby właściciel aplikacji jasno określił i udokumentował wrażliwość systemu aplikacji.
  - Jeżeli aplikacja wrażliwa ma być uruchomiona we wspólnym środowisku, to zaleca się określenie i uzgodnienie z jej właścicielem tych systemów aplikacji, z którymi aktywa będą współużytkowane.

[Jest to kolejne zalecenie do bezpośredniego wykorzystania w systemach informatycznych przetwarzających dane/informacje prawnie chronione].

- Zaleca się potwierdzanie ważności danych wyjściowych z systemu aplikacji, tak aby zapewnić, że przetwarzanie przechowywanej informacji jest właściwe i odpowiednie w zdefiniowanych okolicznościach.
- Zaleca się stosowanie systemów i technik kryptograficznych w celu ochrony informacji, dla której istnieje określone ryzyko, a inne zabezpieczenia nie zapewniają wystarczającej ochrony.
- Zabezpieczanie dokumentów instytucji:
  - Zaleca się uwzględnienie zjawiska starzenia się nośników używanych do przechowywania zapisów. Zaleca się, aby wdrożone procedury przechowywania i postępowania były zgodne z zaleceniami producenta nośnika,
  - W przypadku zastosowania do przechowywania zapisów nośników elektronicznych, zaleca się wprowadzanie procedur zapewniających dostęp do danych (możliwość czytania danego nośnika i formatu) przez cały okres przechowywania, tak aby zabezpieczyć się przed utratą danych, spowodowaną zmianami technologii w przyszłości,
  - Zaleca się, aby system przechowywania danych i ich obsługi zapewniał możliwość łatwej identyfikacji zapisu jego ustawowego lub określonego wewnętrznymi przepisami okresu przechowywania, a także odpowiedniego niszczenia zapisów po upłynięciu tego okresu, jeżeli nie są już potrzebne instytucji.
- Istotne dla bezpiecznej wymiany danych drogą elektroniczną są m.in. poniższe zagadnienia.
  - Uwierzytelnianie. Jakiego poziomu zaufania co do tożsamości mają wymagać partnerzy od siebie nawzajem?
  - Autoryzacja. Kto jest uprawniony do wystawiania i podpisywania dokumentów? W jaki sposób dowiaduje się o tym partner?
  - Procedury podpisywania. Jakie są wymagania co do poufności, integralności i dowodów nadania i odbioru najważniejszych dokumentów oraz co do niezaprzeczalności umów?

- Weryfikacja. Jaki stopień weryfikacji jest właściwy dla sprawdzenia dostarczonej przez klienta informacji o płatności?
- Regulowanie zobowiązań. Jaka jest najbardziej odpowiednia forma płatności dla zabezpieczenia przed oszustwami?
- Odpowiedzialność. Kto ponosi ryzyko związane z oszustwami w transakcjach?

- Konieczne jest zapewnienie, że użytkownicy mający dostęp do sieci i usług sieciowych nie naruszają bezpieczeństwa tych usług sieciowych. Zaleca się, aby w tym celu zapewnić:
  - Odpowiednie interfejsy pomiędzy siecią instytucji a sieciami należącymi do innych instytucji lub sieciami publicznymi.
  - Odpowiednie mechanizmy uwierzytelniania użytkowników i urządzeń.
  - Kontrolę dostępu użytkowników do usług informatycznych.

Aspekty ekonomiczne

- W przeanalizowanych regulacjach normatywnych brak zapisów wprost dotyczących wymagań ekonomicznych związanych z potrzebą przetwarzania informacji poufnych.

Załącznik nr 2: „Uogólniony materiał analityczny dotyczący mechanizmów ochrony danych"

W załączniku tym przedstawiono wybrane aspekty bezpieczeństwa danych przechowywanych i przetwarzanych w popularnie stosowanych systemach informatycznych. Przypadki opisane w załączniku są tylko przykładowymi podatnościami, które powinny uzmysłowić czytelnikowi to, iż analizowane systemy informatyczne nie zapewniają należytej ochrony danych, szczególnie w przypadku gdy informacje posiadają rożne klauzule tajności. Oczywiście systemy informatyczne mają dużo więcej podatności, lecz ich dokładne opisywanie wykracza poza zakres tematyczny tej książki.

Jednym z najważniejszych elementów bezpieczeństwa systemu jest odpowiednie uwierzytelnienie użytkowników oraz przyznawanie im na tej podstawie odpowiednich uprawnień, czyli autoryzacja. Nawet w przypadku bardzo mocnych i precyzyjnych mechanizmów kontroli dostępu do danych, cały system przydziału uprawnień jego użytkownikom opiera się na informacjach wprowadzonych w trakcie procesu uwierzytelniania. Jeśli na tym etapie nie zostaną zastosowane silne mechanizmy, cały późniejszy przydział uprawnień traci sens, ponieważ będzie zbudowany na małowiarygodnych informacjach. Bardzo ważne jest więc prawidłowe uwierzytelnienie z zastosowaniem tzw. silnych metod. Aktualnie za silne metody uwierzytelnienia uważane są metody zapewniające możliwość posługiwania się hasłami jednokrotnymi, które nie posiadają typowych słabości charakteryzujących hasła statyczne. System silnego uwierzytelnienia powinien poprawnie współpracować z systemem kontroli dostępu (np. zapora sieciowa) w oparciu o protokół RADIUS oraz z zewnętrzną bazą użytkowników LDAP. Generowanie haseł dynamicznych po stronie użytkownika odbywać się powinno na urządzeniu typu Smart Card obsługiwanym przez odpowiednie oprogramowanie klienckie wyłącznie po podaniu poprawnego kodu dostępu do karty przez użytkownika. Ta sama karta, która w połączeniu z oprogramowaniem klienckim jest generatorem haseł dynamicznych powinna zapewniać możliwości bezpiecznego składowania na niej certyfikatów cyfrowych oraz haseł statycznych. Niestety aktualnie żaden system operacyjny czy bazodanowy w swej standardowej postaci nie oferuje funkcji uwierzytelniania w ten sposób. Z tego też powodu proces uwierzytelniania

i autoryzacji został opisany na przykładzie Windows, gdzie standardowo oprócz logowania lokalnego można wykorzystać, np. protokół Kerberos.

MS Windows 2000

W systemie Windows 2000 identyfikacja użytkowników jest podstawą uzyskania dostępu do zasobów lokalnych i sieciowych. W tym modelu istnieją dwa rodzaje identyfikacji:

- Logowanie interaktywne – użytkownicy identyfikują się na komputerze lokalnym lub używając konta w domenie.
- Identyfikacja sieciowa – system zatwierdza tożsamość użytkownika dla każdej usługi sieciowej, do której użytkownik próbuje uzyskać dostęp. System zabezpieczeń wspiera w tym celu trzy mechanizmy identyfikacji: Kerberos, karty inteligentne oraz NTLM (aby zapewnić kompatybilność ze starszymi wersjami Windows).

Protokół Kerberos służy do ustalenia tożsamości użytkownika oraz usług sieciowych (identyfikacji wzajemnej) wewnątrz domeny. Mechanizm identyfikacji Kerberos wydaje bilet (ticket) nadawania biletów (TGT), który służy do otrzymywania biletów usługi (ST) zapewniających dostęp do usług sieciowych. Bilety te zawierają zaszyfrowane dane, w tym hasło szyfrowe potwierdzające tożsamość użytkownika dla żądanej usługi. Klient przedstawia bilet usługi żądanej usłudze sieciowej. Bilet stanowi dowód tożsamości użytkownika dla usługi oraz dowód tożsamości usługi dla użytkownika.

Protokół NTLM był domyślnym protokołem identyfikacji sieciowej w systemie Windows NT 4.0, opartym na mechanizmie wezwanie/odpowiedź. Jest on zachowany w systemie Windows 2000 w celu zapewnienia kompatybilności z wcześniejszymi klienckimi i serwerowymi wersjami Windows. NTLM jest także stosowaną w Windows 2000 metodą potwierdzania logowania na komputerach autonomicznych.

System Windows 2000 wspiera kilka protokołów identyfikacyjnych umożliwiających dostęp telefoniczny, na przykład MS-CHAP, CHAP i SPAP. System Windows 2000 można skonfigurować tak, aby wspierany był protokół EAP (Extensible Authentication Protocol), który umożliwia identyfikację użytkowników zdalnych za pomocą dodatkowych urządzeń, takich jak karty inteligentne i certyfikaty. Zabezpieczenie warstwy transportu EAP (EAP-TLS) umożliwia identyfikację użytkowników zdalnych przy użyciu kombinacji dowodów tożsamości, na przykład karty inteligentnej i numeru PIN.

Jeśli chodzi o nadawanie uprawnień do usług, to administratorzy mogą nadać określone prawa kontom grup lub pojedynczych użytkowników. Prawa użytkowników różnią się od uprawnień, które są związane z określonymi obiektami (takimi jak drukarki i foldery).

Kolejnym ważnym elementem systemu Windows 2000 dającym możliwość udostępniania wybranych zasobów upoważnionym użytkownikom jest przyznawanie uprawnień do zbiorów danych i plików.

Dzięki zastosowaniu systemu plików NTFS można skorzystać z nadawania kilku typów uprawnień:

- prawa dostępu do plików, katalogów,
- system zarządzania zapisem i odczytem danych (system transakcyjny),
- możliwość szyfrowania danych,
- możliwość kompresji danych,
- możliwość przydzielania przestrzeni dla danych każdemu użytkownikowi osobno.

Mnogość grup, do których użytkownik może przynależeć niesie ze sobą kolejne zagrożenia. Administrator implementujący prawa użytkowników narażony jest na błędne zdefiniowanie uprawnień, tym samym dopuszczenie nieuprawnionych osób do dostępu do krytycznych danych. Poza tym administrator musi posiadać dopuszczenie do najwyższych klauzul tajności jakie posiadają dane przetwarzane w systemie i tutaj powstaje kolejne zagrożenie. Przyznawanie uprawnień powinno być wielopoziomowe, uczestniczyć w nim musi poza administratorem systemu osoba odpowiedzialna za ochronę informacji niejawnych w instytucji.

Unix

W systemie Unix prawa do plików są nadawane dla trzech rodzajów obiektów, tj. właściciela, grupy użytkowników związanych z plikiem (grupa ta jest nazywana właścicielem grupowym lub krócej grupą pliku) oraz całej reszty. Użytkownik będący właścicielem pliku wcale nie musi należeć do grupy pliku, chociaż najczęściej zdarza się, że grupa pliku jest grupą główną (login grupą) właściciela pliku. Każdemu z trzech obiektów można przydzielić poziomy dostępu, symbolicznie reprezentowane przez litery r,w,x, oznaczające prawo do czytania, zapisu (modyfikacji) i wykonywania. Interpretacja uprawnień w odniesieniu do plików zwykłych jest intuicyjna, jednak w przypadku plików specjalnych takich jak katalogi czasami może wydawać się mniej oczywista. I tak prawo „r" do katalogu daje możliwość przeszukiwania jego zawartości (np. wykonanie komendy ls), prawo „w" umożliwia modyfikacje jego zawartości (np. usuwanie plików), zaś „x" pozwala na uczynienie danego katalogu katalogiem bieżącym. Istnieją rozwinięcia standardowych uprawnień dostępu do plików takie jak niżej wymienione:

- prawo dostępu z literą „t" (Stickly bit) powoduje utrzymanie w pamięci binariów programu, nawet jeśli proces, który z nich korzystał już się zakończył. Jest to wprowadzane w celu przyspieszenia działania często wykonywanych programów;
- prawo dostępu z literą „s" (Set UID/Set GID czyli SUID/GUID) dla plików wykonywalnych powoduje, że procesy, które wykonują, mają taki sam dostęp do zasobów systemowych, jak właściciel wykonywanych programów, a nie użytkownik, który uruchamia dany proces.

Najbardziej znanym przykładem pliku mającego ustawiony atrybut SUID jest plik zawierający program do zmiany haseł: /bin/passwd. Program ten musi mieć możliwość modyfikacji pliku /etc/passwd a tylko root ma prawo zapisu w tym pliku. W związ-

ku z tym plik /bin/passwd ma ustawiony atrybut siud. "Zwykły" użytkownik (nie root) wykonujący program zawarty w tym pliku na czas jego wykonywania uzyskuje prawa dostępu takie jak root (ponieważ właścicielem pliku jest root) i może zmodyfikować swoje hasło w pliku haseł.

Prawa, które zostały wymienione jako przykłady bardziej wyrafinowanego przydziału uprawnień stanowią niestety często zagrożenie, ponieważ stosowane w nieświadomy do końca sposób mogą przenieść zbyt wysokie uprawnienia dostępu do zasobów systemu na obiekty, które bezpośrednio nie posiadają takiego poziomu uprawnień. W ten sposób może dojść do naruszeń w zakresie poufności informacji przechowywanej i przetwarzanej w środowisku tych systemów.

Dodatkowo analizując najważniejsze podatności systemów Unix wykorzystywanych w najczęściej spotykanych wersjach i konfiguracjach widać, iż są to systemy, które posiadają wiele luk stanowiących zagrożenie dla poufności, integralności i dostępności informacji w nich przechowywanych i przetwarzanych. Ich przykładami są Network File System (NFS) i Network Information Services (NIS) – dwie ważne usługi wykorzystywane w sieciowych systemach UNIX. NFS to usługa stworzona przez Sun Microsystems, w celu udostępniania plików przez sieć systemom UNIX. NIS to zestaw usług, tworzących bazę danych (składającą się z tzw. map), świadczącą usługi informacyjne innym usługom sieciowym, jak np.: Network File System NFS. Najczęściej mapy to pliki passwd i group, wykorzystywane w charakterze centralnego systemu uwierzytelnienia użytkowników. Problemy bezpieczeństwa obydwu usług stale się pojawiają (przepełnienie bufora, DoS, słabe uwierzytelnienie) i sprawiają, że usługi te są częstym przedmiotem ataków. Słaba konfiguracja NFS i NIS, pozwala na wykorzystanie luk przez zdalnych i lokalnych użytkowników. Słabe uwierzytelnienie w systemie NIS podczas wysyłania zapytań do map NIS można wykorzystać za pomocą aplikacji takich jak ypcat lub getent, które wyświetlają wartości map oraz umożliwiają dostęp do plików z hasłami. Podobny problem jest z NFS, które opiera się na zaufaniu do identyfikatora użytkownika (UID) oraz grupy (GID), przedstawianych serwerowi przez klienta NFS. W zależności od konfiguracji serwera może to pozwolić dowolnemu użytkownikowi na podmontowanie i podgląd zdalnego systemu plików. Prawie wszystkie systemy UNIX i Linux są dystrybuowane z zainstalowanym NFS i NIS – często domyślnie uruchamianych. W przypadku NFS, domyślnie pliki „exports" (pliki te specyfikują katalogi, które mają być współdzielone) są zazwyczaj puste.

Berkeley Internet Name Domain (BIND) jest najczęściej wykorzystywaną implementacją Domain Name System (DNS), krytycznego systemu pozwalającego na konwersję nazw (np. www.sans.org) na zarejestrowany numer IP. Rozpowszechnienie i krytyczność BIND sprawiły, że często stawał się on celem ataków, w szczególności ataków Denial of Service (DoS).

Istnieje szereg przyczyn takiego stanu rzeczy – przede wszystkim jest to brak zainstalowanych łat bezpieczeństwa oraz różne błędy w konfiguracji. W rezultacie może dojść do ataków Denial of Service, przepełnienia bufora bądź zatrucia pamięci pod-

ręcznej serwera DNS (DNS cache poisoning). Wśród najnowszych słabości systemu BIND znajduje się podatność na atak Denial of Service, opisana w zaleceniu CERT CA-2002-15. W tym przypadku atakujący, aby wymusić wewnętrzną kontrolę poprawności, może wysłać odpowiednie pakiety DNS. Kontrola ta jest przeprowadzana błędnie, powodując zamknięcie serwera. Inny przypadek to atak przepełnienia bufora, opisany w zaleceniu CERT Advisory CA-2002-19, w którym atakujący wykorzystuje luki w implementacjach bibliotek rozwiązywania nazw DNS (DNS resolver libraries). Poprzez wysyłanie złośliwych odpowiedzi DNS, atakujący może wykorzystać te luki i wykonać dowolny kod. Może także spowodować atak Denial of Service.

Istnieje również dodatkowe ryzyko związane z wykorzystaniem podatnego serwera BIND do przechowywania na nim nielegalnych materiałów bez wiedzy administratora lub jako odskoczni do dalszych ataków.

Prawie wszystkie wersje systemów UNIX oraz Linux są rozprowadzane z którąś z wersji BIND. BIND jest prawdopodobnie zainstalowany, jeżeli skonfigurowano system jako serwer.

Bazy danych na przykładzie Oracle

Bazy danych to niezwykle skomplikowane aplikacje i często trudno jest je odpowiednio skonfigurować i zabezpieczyć. Bazy danych takie jak MySQL, Postgres i Oracle posiadają wiele wrażliwych cech: konta i hasła użytkowników, systemy audytowe, przywileje i prawa dostępu do obiektów baz danych, wbudowane polecenia, unikalne języki skryptowe i języki programowania, protokoły sieciowe, łaty, rozbudowane systemy zarządzające, itp. Środowisko zajmujące się bezpieczeństwem z reguły ignorowało temat bezpieczeństwa baz danych. Z kolei wielu specjalistów od baz danych nie uważało kwestii bezpieczeństwa za zadania leżące w ich zakresie obowiązków. Większość baz danych posiada wiele cech i możliwości, które mogą zostać wykorzystane do naruszenia integralności, poufności i dostępności danych, które przechowują.

Kolejną przyczyną lżejszego potraktowania zagadnień bezpieczeństwa w przypadku baz danych było, jak to miało miejsce w przypadku produktów Oracle, nieudostępnianie pełnych wersji czasowych swoich produktów. Mało kogo było stać na zakupienie drogich licencji a przez to wąskie było środowisko osób testujących te rozwiązania pod kątem bezpieczeństwa.

Dane w bazie Oracle przechowywane są w tabelach znajdujących się w przestrzeniach tabel (tablespace). Pojedyncza przestrzeń tabel może rozciągać się na wiele plików danych natomiast pojedynczy plik może należeć tylko do jednej przestrzeni. Przestrzeń tabel może logicznie składać się z różnego rodzaju segmentów (zbiorów bloków danych zaalokowanych na rzecz obiektu bazodanowego). Segment jest natomiast grupą extendów, które z kolei są ciągłymi zestawami bloków danych. Bloki są najmniejszą jednostką alokacji przestrzeni. Baza danych Oracle potrafi posługiwać się blokami różnej wielkości.

Najważniejszą przestrzenią tabel dla działania bazy danych jest przestrzeń SYSTEM przechowująca wszelkie słowniki bazy.

Wszystkie nowoczesne relacyjne bazy, również Oracle posiadają możliwość bezpośredniego ich odpytywania za pomocą specjalnych narzędzi, z ominięciem tradycyjnych zabezpieczeń na poziomie systemu operacyjnego. Na przykład dostęp do baz danych Oracle można uzyskać za pośrednictwem portu 1521/TCP. Większość aplikacji baz danych posiada dobrze znane domyślne konta i hasła, które mogą posłużyć do uzyskania dostępu do danych na różnych poziomach.

CERT/CC opublikował zalecenie, CA-2003-05, dotyczące wielu luk w Oracle, które mogłyby wykorzystane do włamania się do bazy danych. Ostatnio, US-CERT wydał zalecenie na temat SQL Injection Vulnerabilities in Oracle E-Business Suite (TA04-160A), które może doprowadzić do naruszenia integralności bazy danych.

Jak się okazuje, przy niewłaściwej dbałości o ochronę bazy Oracle, może dojść do naruszeń związanych z nieuprawnionym dostępem oraz udanych ataków na dostępność zasobów nie tylko bazy danych ale i całego systemu. W 2002 roku Oracle opublikowało ponad 20 informacji o zagrożeniach w swoich produktach. Ponadto standardowe dystrybucje Oracle zawierają w sobie komponenty Open Source np. Apache – które też nie są wolne od błędów.

Głównymi słabymi punktami baz firmy Oracle jest serwis Oracle Listener, oraz moduły serwisu Apache.

Oracle Listener jest komponentem odpowiedzialnym przede wszystkim za komunikację miedzy klientami a serwerem Oracle (również za komunikację międzyserwerową). Jest to komponent każdej instalacji systemu bazodanowego Oracle. Największe słabości tego serwisu prawdopodobnie wynikają ze złych założeń przyjętych w fazie jego projektowania. Standardowo Oracle Listener przyjmuje komendy nie weryfikując ich nadawcy. Dowolny użytkownik lub proces łączący się na port 1521/TCP może prowadzić dialog z tym serwisem, który w najlepszym przypadku prowadzi do przekazania intruzowi wielu istotnych informacji, zaś w najgorszym może zniszczyć pliki z danymi bazy, pliki konfiguracyjne czy też same binaria Oracle.

Bardzo poważnym w swych konsekwencjach atakiem może być wykorzystanie Listenera do nadpisania już istniejącego pliku. Jest to możliwe, ponieważ serwis ten w żaden sposób nie weryfikuje zmiany położenia pliku logów. Podając mu nazwę i ścieżkę istniejącego pliku można dokonać jego nadpisania. Oczywiście pod warunkiem posiadania przez proces Listenera odpowiednich praw dostępu. Niestety np. w systemach Microsoftu proces ten działa jako Local_System, co daje mu bardzo duże uprawnienia.

W systemach Unix przekierowanie logów do pliku /home/oracle/.rhosts i odpowiednio spreparowane zapisy (Oracle w wypadku wystąpienia błędu wysyła do pliku logów komunikat zawierający oryginalną komendę, która wywołała problem) mogą umożliwić zdalne zalogowanie się do systemu na konto, które intruz założył wykorzystując serwis Listener.

Komunikując się z wykorzystaniem protokołu TNS (Transparent Network Substrate) z serwisem Oracle Listener można pozyskać wiele cennych informacji na temat

systemu bazodanowego a w skrajnych przypadkach doprowadzić do zniszczenia plików z danymi bazy, plików konfiguracyjnych lub binariów Oracle.

Zaprezentowane przykładowe luki systemów Oracle, mogą prowadzić do utraty poufności, integralności i dostępności informacji w nich przechowywanych. Są one błędami popełnionymi w fazie projektowania produktu. Jeden z nich umożliwia ujawnienie informacji przekazywanej w poprzednim połączeniu innego użytkownika z usługą Listener. Błąd programisty polega prawdopodobnie na tym, że bufor do którego są przyjmowane komunikaty nie jest każdorazowo czyszczony. W rezultacie ustawiając w odpowiednim parametrze większą niż w rzeczywistości długość wydawanej komendy TNS można odczytać cześć komendy wydanej przez poprzedniego użytkownika.

Aktualne informacje na temat wykrytych luk w systemach Oracle publikowane są na stronie: http://otn.oracle.com/deploy/security/alerts.htm.

Systemy portalowe

Integracja baz danych z serwisami WWW oraz stosowanie dynamicznych metod generowania stron dają praktycznie nieograniczone możliwości prezentowania danych poprzez strony WWW. Niewłaściwe stosowanie tej technologii może wprowadzić znaczne zagrożenia dla udostępnianych danych a nawet dla całości infrastruktury IT.

Prezentowane przykłady są zaczerpnięte z powszechnie dostępnych materiałów na temat bezpieczeństwa aplikacji WWW: http://www.owasp.org/guide/, http://quiz.ngsec.biz:8080/, http://www.owasp.org/webgoat/.

Jednym z typów zagrożenia jest brak inicjowania wartości zmiennych i brak sprawdzania ilości pobieranych parametrów. W niektórych językach szablonowych, działających po stronie serwera aplikacji (np. PHP) zmienne pobierane od użytkownika są automatycznie rejestrowane jako zmienne globalne. Jeżeli intruz dopisze do zlecenia kolejny parametr i jeśli zmienna o takiej samej nazwie jest używana wewnętrznie przez daną procedurę, to może to spowodować zmianę logiki działania procedury. Wyjaśniono to na poniższym przykładzie:

Za uwierzytelnienie użytkownika odpowiada następujący kod: (pseudokod ilustrujący algorytm)

```
if (sprawdz_uzytkownika_w_bazie($login, $password)) {
$state="OK"; } ... if ($state=="OK") {
UWIERZYTELNIENIE OK } else { BŁĄD ! }
```

Jak widać za pomyślne uwierzytelnienie odpowiada ostatecznie wartość flagi „state". Flaga ta jest wcześniej ustawiana przez procedurę wyszukującą dane logowania w bazie. Jeśli zmienna „state" nie jest inicjowana przed użyciem, to jest możliwe arbitralne ustawienie jej wartości w zleceniu przesyłanym przez klienta:

```
http://serwer_aplikacji/login.php?login=admin&password=xxx&state=OK
```

Niezależnie od wartości zmiennych login i password, intruz zostanie pomyślnie uwierzytelniony.

Oczywiście zastosowanie tej metody nie ogranicza się tylko do procedur uwierzytelniających.

Równie skutecznie można atakować aplikacje manipulując parametrami przekazywanymi w cookies. Zdarza się, że w cookies są przechowywane bardzo istotne dane. Tak jak parametry GET/POST mogą być one modyfikowane przez użytkownika.

Przykład:

Po uwierzytelnieniu, aplikacja ustawia w cookie użytkownika określony parametr, np: „authorized=yes". Jeśli aplikacja podejmuje decyzje o autoryzacji do danego zasobu tylko i wyłącznie na podstawie tej flagi, to jest możliwy trywialny atak polegający na ustawieniu tego parametru zgodnie z wymaganiami uwierzytelnionego użytkownika.

lang=en-us; AUTHORIZED=yes; y=1 ; time=12:30GMT;

Warto zauważyć że niezależnie od tego czy cookie jest przesyłane przez SSL, czy też normalne, daje się je modyfikować w momencie przesyłania przez przeglądarkę, przy pomocy programów typu proxy.

Zdarza się, że aplikacja webowa wykorzystuje funkcje systemu operacyjnego do konstruowania stron HTML. Funkcje te są uruchamiane po stronie serwera. Często aplikacja przekazuje do tych funkcji czy poleceń systemowych parametry pobierane od użytkownika. Jeśli parametry te nie są szczegółowo sprawdzane, to może to prowadzić do manipulacji funkcjami i komendami systemu operacyjnego.

Przykład:

Aplikacja pobiera od użytkownika nazwę katalogu, a następnie wyświetla jego zawartość. Parametr pobrany od użytkownika jest doklejany do komendy:

cmd.exe /c dir /b .....

Jeżeli intruz dopisze do parametru znak & to będzie mógł wykonać dowolną komendę systemową. Znak & dla Windows2000 (tak jak znak ; dla Unixów) oddziela komendy systemowe.

Innym sposobem nieuprawnionego dostępu do danych przekazywanych pomiędzy przeglądarką internetową i systemem portalowym jest **przejęcie sesji**. Protokół HTTP odpowiadający za komunikację przeglądarki z aplikacją internetową, nie zna pojęcia sesji (jest protokołem bezstanowym). Każde odwołanie jest traktowane jako osobna sesja HTTP. Aplikacja internetowa musi operować pojęciem sesji, gdyż jej interakcja z użytkownikiem składa się z wielu odwołań HTTP. W związku z tym, to aplikacja musi implementować kontrolę sesji. Na początku sesji użytkownika (po uwierzytelnieniu się do aplikacji, lub przy pierwszym odwołaniu) jest tworzony identyfikator sesji (token), który jest przekazywany do klienta. Później ten identyfikator jest przedstawiany przez klienta dla serwera za każdym razem. W ten sposób serwer wie że dane odwołanie należy do określonej sesji. Najczęściej wykorzystywaną metodą jest przekazywanie tokena sesji w cookie, ale spotyka się również przekazywanie tokena jako parametr GET w URL czy też metodą POST, w ukrytym polu formularza. Niezależnie od wykorzystywanej metody przekazywania, należy pamiętać o tym, że identyfikator sesji jest jednym z parametrów przekazywanym przez użytkownika. W związku z tym jest on narażony na różne ataki, np:

- manipulacje identyfikatorem przez klienta,
- podsłuch,
- podszywanie się przy użyciu podsłuchanego lub przewidywalnego identyfikatora sesji.

Identyfikator sesji ściśle określa użytkownika w aplikacji. W związku z tym podsłuchanie lub odgadnięcie tego identyfikatora może prowadzić do ominięcia mechanizmów uwierzytelniających lub przechwycenia danych w ramach sesji użytkownika.

MS Internet Information Services (IIS) używa mechanizmu tzw. ISAPI do kojarzenia pewnych rozszerzeń z bibliotekami DLL (zwanymi filtrami ISAPI). Preprocesory takie jak ColdFusion czy PHP także używają ISAPI, a IIS zawiera wiele filtrów ISAPI, realizujących między innymi funkcje Active Server Pages (ASP), usługi sieciowe .Net oraz współdzielenia drukarek w sieci. Wiele filtrów ISAPI instalowanych domyślnie wraz z IIS nie jest niezbędnych do poprawnej pracy w większości instalacji. Wiele z nich jest natomiast podatnych na ataki. Przykładami wykorzystania luk w IIS jako mechanizmu propagacji złośliwego kodu są robaki Code Red i Code Red 2. W celu usunięcia tych podatności należy włączyć jedynie te rozszerzenia ISAPI, które muszą być wykorzystywane przez serwer. Zaleca się także ograniczenie opcji HTTP możliwych do użycia z każdym z rozszerzeń.

Większość serwerów WWW zawiera przykładowe strony i aplikacje, których celem jest demonstracja funkcjonalności serwera. Nie zostały one zaprojektowane do bezpiecznego działania w środowisku produkcyjnym. Niektóre przykładowe aplikacje serwera IIS pozwalały na zdalne przeglądanie i nadpisywanie wybranych plików, a także zdalny dostęp do niektórych wrażliwych informacji o serwerze – w tym do hasła administratora. Należy usunąć takie aplikacje przed umieszczeniem serwera w środowisku produkcyjnym.

Instalacja IIS pozbawiona regularnego dozoru będzie także zawierać luki, które wykryto od momentu publikacji oprogramowania. Przykładem mogą być luki w PCT i SSL, których dotyczy poprawka MS04-011, a które pozwalały na zablokowanie działania serwera lub przejęcie przez atakującego pełnej kontroli nad nim. Z tych powodów instalacja dostępnych poprawek w jak najkrótszym czasie, w szczególności na publicznie dostępnych serwerach WWW, jest sprawą krytyczną.

Dodatki firm trzecich, takie jak ColdFusion czy PHP, mogą wprowadzić do systemu z serwerem IIS kolejne podatności. Mogą one być efektem zarówno nieprawidłowej konfiguracji, jak i luk w samym produkcie.

Problem może dotyczyć każdego systemu z zainstalowanym serwerem WWW. W szczególności (lecz nie wyłącznie) dotyczy to:

- Microsoft IIS: Windows NT 4.0 i nowsze, w tym Windows XP Professional
- Serwer HTTP Apache: wspierany na Windows NT 4.0 SP3 i nowszych; może działać także na Windows 95/98
- Sun Java System/Sun One/iPlanet Web Server: Windows NT 4.0 SP6 i nowsze

Windows 2000 Server zawiera w domyślnej instalacji serwer IIS. Wielu administratorów przekonało się o tym w następstwie niesławnych epidemii Code Red i Nim-

dy. Ponadto, wiele aplikacji wymaga funkcjonalności dostarczanej przez IIS, co może skutkować instalacją tego serwera wraz z taką aplikacją, być może bez świadomości administratora. Nie należy nigdy zakładać, że opisane problemy nie dotyczą danej sieci jedynie dlatego, że nie został w niej świadomie zainstalowany żaden ze wspomnianych serwerów.

Może się wydawać, iż w przypadku wielu naruszeń i w związku z tym uzyskaniem nieuprawnionego dostępu do poufnych danych antidotum stanowić może szyfrowanie transmisji. Jak się okazuje, również mechanizmy i aplikacje szyfrujące dane nie są w 100 procentach wolne od błędów implementacyjnych. Przykładem takim jest popularny pakiet OpenSSL. Wykorzystywany jest on jako wzbogacenie aplikacji komunikujących się przez sieć o kryptograficzne mechanizmy bezpieczeństwa. Jest szeroko wykorzystywaną implementacją SSL/TLS, stosowaną przez wielu producentów. Najbardziej znaną aplikacją korzystającą z tej biblioteki jest serwer WWW Apache (do bezpiecznych połączeń http). Serwery POP, IMAP, SMTP i LDAP także mają swoje OpenSSL'owe odpowiedniki.

Zazwyczaj OpenSSL jest wykorzystywany jako zestaw narzędzi, które inne aplikacje wykorzystują do zapewnienia kryptograficznej ochrony dla połączeń sieciowych. Zamiast atakowania OpenSSL bezpośrednio, exploity są skierowane na aplikacje wykorzystujące OpenSSL. Kilka znany exploit'ów atakuje serwery Apache korzystające z OpenSSL. Tak więc fakt, że wykorzystywany jest serwer Apache z OpenSSL nie gwarantuje, że dane są poprawnie chronione. Odpowiednio zmodyfikowany exploit może zostać wykorzystany do zaatakowania Sendmail, openldap, CUPS lub innego programu wykorzystującego OpenSSL.

Znaleziono wiele luk w OpenSSL, z których najbardziej poważne to pięć opisanych w CAN-2002-0655, CAN-2002-0656, CAN-2002-0557, CAN-2002-0659 oraz CAN-2003-0545. Umożliwiają one zdalne wykonanie dowolnego kodu z przywilejami użytkownika korzystającego z bibliotek OpenSSL (w niektórych przypadkach, takich jak 'sendmail', jest to root).

Każdy system UNIX i Linux z OpenSSL 0.9.7 lub wcześniejszymi wersjami posida wymienione podatności. Należy zwrócić uwagę, że OpenSSL jest często instalowane jako wsparcie dla innego komponentu. Na przykład na systemie RedHat Linux 9.0 pakiety takie jak Apache, CUPS, Curl, OpenLDAP, Stunnel i Sendmail (między innymi) wykorzystują biblioteki OpenSSL do zabezpieczania połączeń.

Na koniec trzeba jeszcze wspomnieć o problemie współdzielenia informacji w przypadku wielodostępu. Problem ten występuje we wszystkich wielodostępnych systemach informatycznych m.in. w procesie przetwarzania danych oraz udostępniania informacji. Jest to szczególnie istotne przy dużym nacisku kładzionym na zapewnienie odpowiedniego poziomu interoperacyjności systemu przy jednoczesnym zachowaniu wymaganego poziomu bezpieczeństwa udostępnianej informacji.

Mechanizmy ochrony systemów operacyjnych i bazodanowych realizują politykę sterowanego współdzielenia i niezawodności. Można wyróżnić kilka poziomów dzielenia zasobów:

- całkowita izolacja (brak dzielenia zasobów);
- dzielenie kopii obiektów danych;
- dzielenie oryginalnych obiektów danych;
- dzielenie programów.

Każdy poziom dzielenia nakłada dodatkowe wymagania dotyczące mechanizmów ochrony systemu. Dzielenie danych wprowadza problem nieufności, w którym właściciel obiektu danych może nie mieć zaufania do innego podmiotu, z którym dzieli dostęp do tego obiektu. Na przykład może się obawiać, że przekaże uzyskane prawa dostępu jeszcze innemu podmiotowi. Poza tym właściciel obiektu może się po prostu obawiać nadużycia przekazanych innym podmiotom przywilejów.

Większość systemów dysponuje możliwościami dzielenia oryginałów programów lub danych. Wielodostępne, bezpośrednie systemy baz danych często umożliwiają różnym użytkownikom jednoczesny dostęp do wspólnej bazy danych. Większość systemów operacyjnych dopuszcza, aby procesy współbieżne wykonywały ten sam kod i uzyskiwały dostęp do globalnych tablic systemu lub katalogów plików.

Istnieje wiele przyczyn dzielenia oryginalnych danych zamiast ich kopii. Główną ich przyczyną jest chęć zaoszczędzenia pamięci. Inną przyczyną jest oszczędność czasu, który byłby potrzebny na tworzenie kopii lub przesyłanie zmian do głównej kopii. Trzecia przyczyna wynika z konieczności zapewnienia, aby każdy z podmiotów dysponował spójnym i aktualnym stanem danych.

Ochrona oryginalnych danych nakłada dodatkowe wymagania co do mechanizmów ochrony, ponieważ podmiot z prawem pisania mógłby zniszczyć te dane. Współbieżne dostępy do danych muszą być synchronizowane, aby ochronić podmioty piszące przed wzajemnymi zakłóceniami działania.

Mechanizmy ochrony są tak samo potrzebne do zachowania niezawodności jak do wcześniej omówionego dzielenia zasobów. Zapobiegają one błędnemu działaniu programów polegającemu np. na zapisywaniu danych do segmentów pamięci należących do programu nadzorczego lub innych programów. Zapobiegają również uszkodzeniom systemu powodowanymi przez oprogramowanie wcześniej nie przetestowane. Chronią programy użytkowe przed bezpośrednim zapisem na dysk, co mogłoby doprowadzić do zniszczenia plików i katalogów. Dostarczają awaryjnych kopii plików w razie wystąpienia błędów sprzętu bądź nieumyślnego zniszczenia. Aby ograniczyć skutki awarii spowodowanych przez błędne działanie programów, mechanizmy ochrony zapewniają izolację błędów i narzędzia odtwarzania poprawnego stanu.

Jeszcze jednym zagadnieniem, na które należy zwrócić uwagę przy okazji omawiania kontroli dostępu do zbioru przechowującego dane o rożnych klauzulach tajności jest problem wykonywania kopii bezpieczeństwa. Szczególnie, że dane wędrujące na nośniki backup-owe bardzo często zmieniają system plików, w strukturach którego są zapisywane i jednocześnie tracą przypisane do nich atrybuty kontroli dostępu – związane z listami upoważnień. Powstaje więc pytanie: kto, i w jaki sposób (jakimi narzędziami) ma wykonywać backup, tak aby niemożliwym było jego późniejsze odtworzenie w innym miejscu, z pominięciem kontroli dostępu do jego zawartości, oraz

jaką klauzulę nadać tak stworzonej kopii bezpieczeństwa? Standardowe systemy operacyjne nie rozwiązują problemów tworzenia kopii bezpieczeństwa w tak specyficznych warunkach, jak te, które rozpatrywane są w ramach tej książki.

Polskie Towarzystwo Informatyczne

Oddział Górnośląski

ul. Raciborska 3, 40-074 Katowice
tel./fax: +48 32 2519811
www.pti.katowice.pl
Katowice@pti.org.pl