Mariusz Zarzycki[1], Adam Pelikant[2]
[1]MCSE, MCSA, MCT, Katedra Informatyki, Wydział Zarządzania, Uniwersytet Łódzki
[2]Wyższa Szkoła Informatyki, Katedra Inżynierskich Zastosowań Informatyki, 93-008 Łódź, ul Rzgowska 17a
email: mzarzycki@uni.lodz.pl,
apelikan@wsinf.edu.pl

POLITYKA BEZPIECZEŃSTWA ZASOBÓW INFORMATYCZNYCH

Streszczenie – Każda organizacja powinna mieć określony, wyraźny cel, misję oraz strategię swojego działania. Z wyraźnie określonych celów i strategii wynika strategia i cele zarządzania bezpieczeństwem informacji i całym systemem IT. Brak jednoznacznie zdefiniowanego systemu zarządzania bezpieczeństwem oraz stworzenia polityki bezpieczeństwa informacji (PBI) powoduje, że systemy IT zarządzane są w oparciu o intuicję służb informatycznych i „rozmyte" zasady. Taki stan rzeczy może prowadzić do nadmiernego rozbudowania zabezpieczeń i nieuzasadnionego wzrostu kosztów utrzymania struktury IT. Co może za sobą pociągnąć zaniedbania systemów i narażenie firmy na straty spowodowane incydentem, do którego można było nie dopuścić. Aby tego uniknąć, niezbędne jest zatem sformułowanie w jednostce polityki bezpieczeństwa zasobów informatycznych, która określa sposób rozumienia bezpieczeństwa, stanowi podstawę do dalszych analiz w celu zaproponowania konkretnych rozwiązań technicznych, ustala odpowiedzialność osób i komórek oraz jasno wyraża intencję kierownictwa jednostki dotyczące wspierania wszelkich działań zmierzających do realizacji tej polityki. Celem pracy jest zaprezentowanie podstawowych informacji związanych z polityką bezpieczeństwa zasobów informatycznych. Autor przedstawia cechy poprawnie zdefiniowanej PBI, poszczególne kroki oraz zasady potrzebne w procesie tworzenia polityki bezpieczeństwa informacji oraz strukturę zarządzania bezpieczeństwem informacji według ENSI.

1 Definicja polityki bezpieczeństwa informacji

Wedle definicji [1], Polityka Bezpieczeństwa Informacji jest zbiorem zasad i procedur obowiązujących przy zbieraniu, przetwarzaniu i wykorzystywaniu informacji w organizacji i dotyczy całego procesu korzystania z informacji, niezależnie od sposobu jej gromadzenia i przetwarzania. Polityka Bezpieczeństwa Informacji określa podstawowe zasady ochrony informacji, niezależnie od systemów ich przetwarzania (informatyczny, papierowy) oraz sposobu ich przetwarzania w tych systemach. Obejmuje bezpieczeństwo fizyczne, logiczne i komunikacji prze-

twarzanych informacji. Swoim zasięgiem obejmuje zarówno sprzęt i oprogramowanie, za pomocą, których informacje są przetwarzane, jak i ludzi, którzy te informacje przetwarzają.

W literaturze istnieje wiele przykładowych formatów polityki bezpieczeństwa informacji [2]. Mogą one stanowić bazę startową do tworzenia specyficznych dla każdej jednostki polityk bezpieczeństwa informacji. Oczywistym jest, iż polityka musi być zaadaptowana do określonych struktur organizacyjnych i informacyjnych danej jednostki gospodarczej, tak, aby zapewnić pełną zgodność z istniejącymi planami i zasadami dotyczącymi biznesowych aspektów funkcjonowania przedsiębiorstw.

2 Zasady tworzenia polityki bezpieczeństwa informacji

Tworzenie polityki musi być realizowane przy udziale zarówno personelu technicznego jak i decydentów. Personel techniczny jest w stanie ocenić skutki różnych wariantów tworzonej polityki oraz możliwości jej implementacji. Decydenci odpowiadają za wprowadzenie polityki w życie. S. J. Gaston przedstawia osiem zasad, niezbędnych do uwzględnienia przy opracowywaniu polityki bezpieczeństwa informacji [2,3]:

Zasada pierwsza mówi, że w jednostce powinna być opracowana i rozpowszechniona ogólna strategia bezpieczeństwa opisująca i wiążąca ze sobą wszystkie plany, standardy i procedury bezpieczeństwa informacji. W świetle drugiej zasady kierownictwo powinno angażować do projektowania i kontrolowania polityki bezpieczeństwa zasobów możliwie najwięcej komórek organizacyjnych, ponieważ ich pełny i aktywny udział w tym procesie jest kwestią zasadniczą dla pomyślnego wdrożenia polityki w jednostce. Zasada trzecia oznacza, że polityka bezpieczeństwa informacji rozpoczyna się od ustanowienia zasad, na których będzie się ona opierać. Czwarta zasada wymaga, aby dokładnie określić wzajemne związki między polityką bezpieczeństwa informacji a innymi planami opracowanymi w jednostce. Według zasady piątej w polityce bezpieczeństwa powinny być przedstawione zakres polityki i jej znacznie, standardy będące podstawą tworzenia polityki, wymagane i zatwierdzone przypadki odstępstw od polityki bezpieczeństwa i standardów. Zasada szósta mówi, że polityka bezpieczeństwa informacji winna jasno określać potrzebę klasyfikacji informacji i systemów po to, aby była możliwa natychmiastowa reakcja na pojawiające się ryzyko zagrożeń. Zasada ta stanowi punkty wyjścia do projektowania środków ochrony zasobów informatycznych. Zasada siódma odnosi się do czynnika ludzkiego i stwierdza się w niej, że należy jasno zdefiniować rolę i odpowiedzialność poszczególnych komórek i pracowników w aspekcie bezpieczeństwa zasobów informacji. Ostatnia, ósma zasada, uwzględnia środowisko mikrokomputerowe i mówi o tym, że konieczne jest opracowanie oddzielnej polityki dla tego środowiska, stanowiącej załącznik do po-

lityki bezpieczeństwa zasobów. Winna ona przydzielać obowiązki i odpowiedzialność tym wszystkim osobom, które wykorzystują mikrokomputery jako stanowiska autonomiczne do przetwarzana danych.

Kluczowym elementem polityki jest zapewnienie, aby każdy uświadomił sobie własną odpowiedzialność za utrzymywanie bezpieczeństwa.

3 Polityka bezpieczeństwa informacji, a realia Polski

Powszechną praktyką w Polsce, w trakcie tworzenia polityki bezpieczeństwa informacji, jest zastosowanie metodyki prezentowanej przez *European Network Security Institute* – TISM [2,3] (ang. *Total Information Security Management*). TISM umożliwia w zorganizowany sposób i z przewidywalnym efektem wprowadzać w firmach program ochrony informacji uwzględniając takie dziedziny jak: analiza ryzyka, konstrukcja dokumentów, polityka audytów i testów, konstrukcja procedur postępowania, kultura ochrony informacji instytucji. Głównym założeniem Polityki Bezpieczeństwa Informacji tworzonej wg metodyki TISM jest określenie:

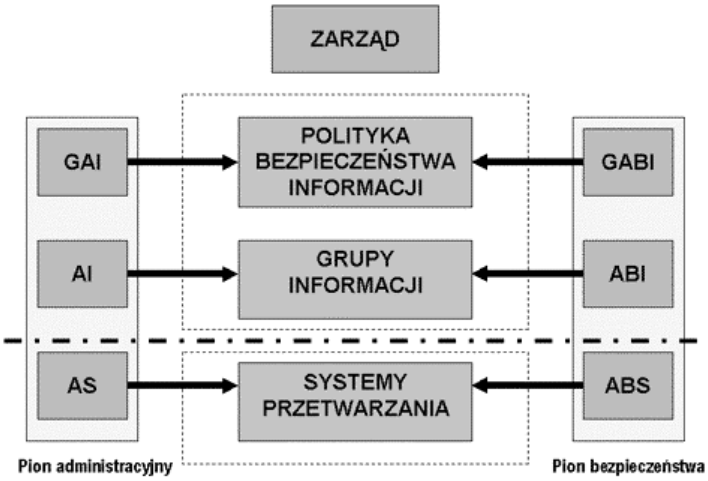
- jakie grupy informacji firma chce chronić,
- w jakich systemach mogą być one przetwarzane,
- kto i na jakich zasadach ma mieć do nich dostęp,
- kto jest odpowiedzialny za zarządzanie informacją,
- kto jest odpowiedzialny za zarządzanie bezpieczeństwem informacji.

Wedle TISM wyróżnia się trzy podstawowe poziomy w hierarchii polityki bezpieczeństwa:

- politykę bezpieczeństwa – dokument główny – na poziomie, którego ustala się podstawowe zasady ochrony informacji w organizacji,
- grupę informacji – poziom, gdzie ustala się specyficzne wymagania ochrony w stosunku do informacji,
- system przetwarzania – poziom na, którym określa się spełnienie wymagań wyższych poziomów, w którym informacje z danej grupy się znajdują.

Polityka, która opiera się na TISM jako wzorcu ma strukturę modułową, polegającą na tworzeniu odrębnych zasad dla poszczególnych grup informacji i ich systemów przetwarzania w oparciu o zasady przyjęte w Polityce Bezpieczeństwa Informacji. Strukturę polityki bezpieczeństwa wg TISM przedstawia rys 1.

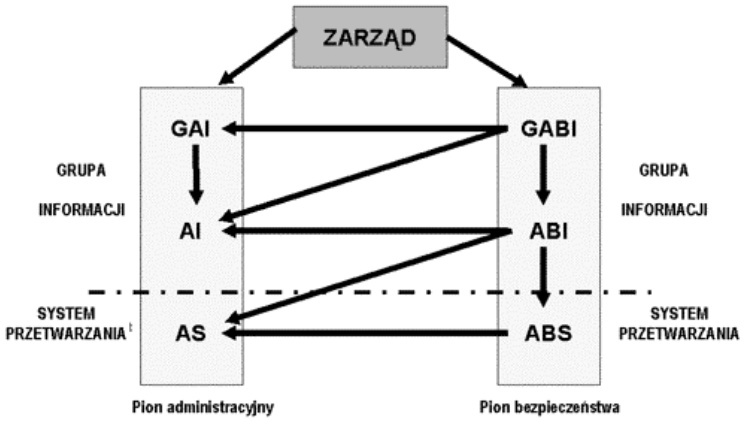
Wg TISM struktura zarządzania informacją oraz bezpieczeństwo informacji ma określoną postać. Polega ona na określeniu odpowiednich ról administratorów, które zgrupowane są w dwóch pionach: administracyjnym i bezpieczeństwa.



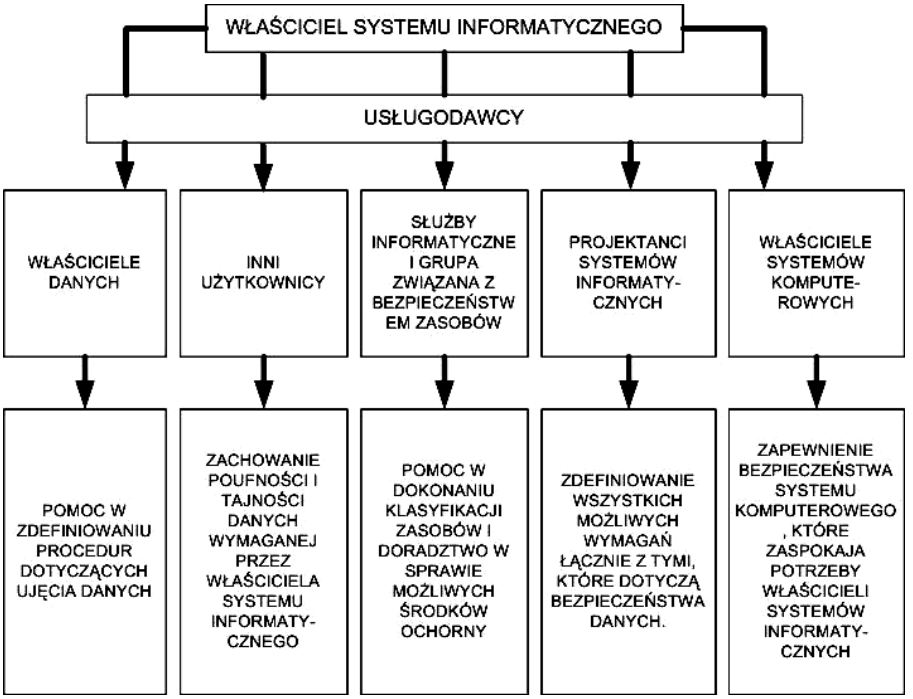
Rys. 1. Modułowa i hierarchiczna struktura polityki bezpieczeństwa wg TISM. Źródło: http://www.ensi.net

Dotyczą one zarówno głównej Polityki Bezpieczeństwa Informacji, grup informacji, jak i systemów przetwarzania (rys. 1). Na poziomie głównej Polityki Bezpieczeństwa Informacji określone są role: Głównego Administratora Informacji (GAI) oraz Głównego Administratora Bezpieczeństwa Informacji (GABI). Na poziomie grupy informacji określone są role: Administratora Grupy Informacji (AI), Administratora Bezpieczeństwa Grupy Informacji (ABI). Na poziomie systemu przetwarzania określone są role: Administratora Systemu (AS) oraz Administratora Bezpieczeństwa Systemu (ABS). Praktyka pokazuje, iż wewnątrz pionów następuje łączenie ról np.: zarząd pełni rolę GAI, gdyż to on określa ważność poszczególnych grup informacji podlegających ochronie. Nie łączy się natomiast ról między pionami, co wynika z przyjętej koncepcji bezpieczeństwa: administrator i administrator bezpieczeństwa (rys 2).

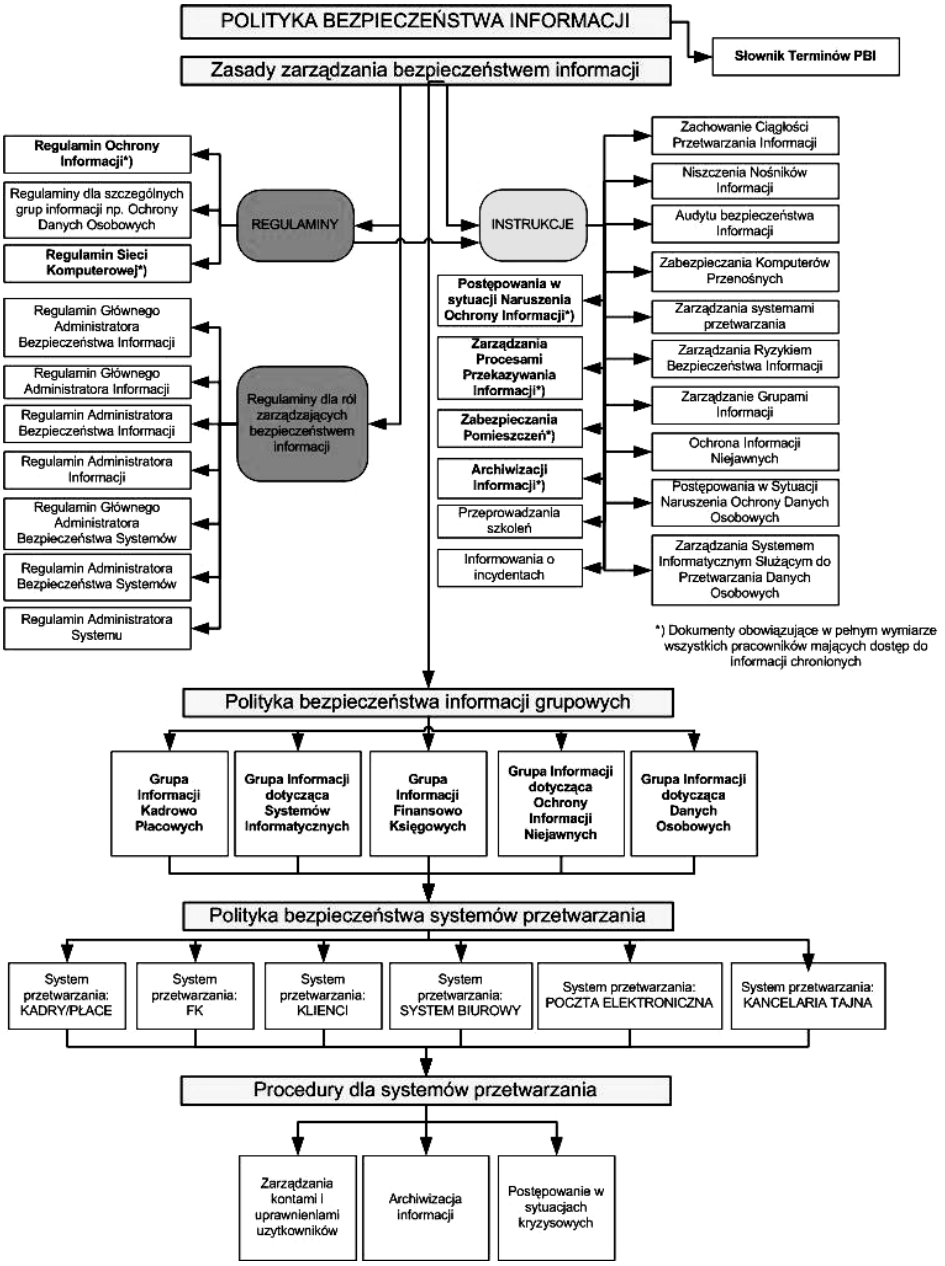
Podczas tworzenia polityki bezpieczeństwa informacji, niezwykle ważną rolę odgrywają właściciele systemów informatycznych. Określają oni wymagania dotyczące bezpieczeństwa informacji dla wszystkich systemów, których są właścicielami. Są oni ponadto koordynatorami współpracy z innymi grupami osób w celu ustalenia wszystkich koniecznych wymogów związanych z bezpieczeństwem zasobów. G. Idzikowska cytując S.J. Gastona przyrównuje ich do dyrygentów orkiestry i przedstawia powiązania między właścicielami a innymi grupami osób, związanymi z systemami informatycznymi (rys 3).



Rys. 2. Struktura zarządzania bezpieczeństwem informacji - zależności. Źródło: http://www.ensi.net



Rys. 3. Współpraca właściciela systemu informatycznego z innymi grupami osób. Źródło: G.Idzikowska. *Wiarygodność danych a bezpieczeństwo zasobów w środowisku informatycznym rachunkowości,* Wydawnictwo UŁ, Łódź 2002 , s. 165 za S. J. Gaston, *Information Security,* The Canadian Institute od Charterem Accountants, Kanada 1996, s.20.



Rys. 4. Mapa dokumentów polityki bezpieczeństwa informacji. Źródło: http://www.ensi.net

Analizując rysunek 3 widać, iż właściciele systemów informatycznych powinni współpracować z właścicielami danych, projektantami systemów oraz specjalistami w zakresie ochrony danych, aby dokonać klasyfikacji

danych i innych zasobów informatycznych oraz dokładnie określić procedury bezpieczeństwa stosownie do tej klasyfikacji [3]. Wynikiem prac związanych z implementacją PBI jest zbiór dokumentów, nazywanych wedle terminologii przyjętej przez ENSI, mapą dokumentów polityki bezpieczeństwa informacji (rys 4).

Ważnym elementem związanym z tematem polityki bezpieczeństwa informacji jest kwestia strategii jej wdrożenia. Problem ten szeroko opisany jest w literaturze, dlatego w pracy zrezygnowano z przedstawiania szczegółowych informacji na ten temat.

4 Podsumowanie

Nieprawdą byłoby stwierdzenie, iż w polskich jednostkach gospodarczych brak jest działań w zakresie tworzenia i implementacji polityki bezpieczeństwa informacji. Kwestia bezpieczeństwa zasobów informacyjnych (w tym informatycznych) stanowi strategiczne działania wielu polskich firm. Głównym problemem jest fakt, iż wykonywane działania nie mają jednak, w większości przypadków, charakteru systematycznego, lecz jedynie są one doraźne i oparte na intuicji często niezbyt kompetentnych osób. Wdrożona w jednostce gospodarczej polityka bezpieczeństwa informacji ma znaczący wpływ na koncepcję przeprowadzania audytu systemów informatycznych. Istnienie PBI, sugeruje audytorowi odnoszenie się w prowadzonym badaniu do procedur, regulaminów i zasad sprecyzowanych w poszczególnych elementach polityki bezpieczeństwa informacji (patrz rys 4). Brak wdrożonej polityki, powoduje, iż audyt, szczególnie IT jest czynnością inicjującą potrzebę posiadania polityki bezpieczeństwa informacji, poprzez identyfikację istniejących przyczyn ryzyka oraz zagrożeń, na jakie narażona jest ogólnie rozumiana informacja. Należy również podkreślić, iż audyt systemów IT w jednostce pozbawionej PBI, wymaga od audytora kompleksowego spojrzenia na zagadnienie bezpieczeństwa zasobów, a co za tymi idzie i informacji.

Literatura

[1] http://www.wnsi.net

[2] Gaston S.J.: *Information Security*, The Canadian Institute of Chartered Accountants, Canada 1999.

[3] Idzikowska G.: *Wiarygodność danych a bezpieczeństwo zasobów w środowisku informatycznym rachunkowości,* Wydawnictwo UŁ, Łódź 2002

[4] http://www.isaca.org

[5] http://www.isaca.org.pl

[6] http://www.ogc.gov.uk

[7] http://www.sei.cmu.edu/cmm/

[8] http://www.iso.org

[9] Górski J.: *Polityka bezpieczeństwa informacji*, Informatyka 1998, nr 9.

[10] Forystek M.: *Audyt informatyczny*, InfoAudit, Warszawa 2005

SECURITY POLITIC FOR COMPUTERS SYSTEMS

Summary – All organizations have to have strictly determined destination and working strategy. From this parts appears destinations and strategy of information and IT system security. Not enough strict definition of security system (policy) carry on to situation that administration based on intuition and fuzzy rules. This state carry on to not reasonable enlarge security system and costs of it implementation and use. It lead firms to danger of data and information lose. Main idea of this paper is presentation of most important information's and features of correctly built security system. The most important steps in the creation of security system due to ENSI norms are pointed.