PRACE NAUKOWE UNIWERSYTETU EKONOMICZNEGO WE WROCŁAWIU
Nr 52 2009
Podejście procesowe w organizacjach

**Sławomir Wawak**
Uniwersytet Ekonomiczny w Krakowie

# PODEJŚCIE PROCESOWE WE WDRAŻANIU SYSTEMÓW ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACJI

## 1. Wstęp

Do połowy lat 80. XX w. problemy bezpieczeństwa informacji były domeną służb dyplomatycznych, agencji wywiadowczych czy wojska. Dopiero znaczne zmiany w funkcjonowaniu gospodarki spowodowane masową informatyzacją wymogły zmianę spojrzenia wśród przedsiębiorstw. Jednym z pierwszych przejawów zidentyfikowania nowych potrzeb było opublikowanie w 1992 r. przez Departament Handlu i Przemysłu Wielkiej Brytanii *A Code of Practice for Information Security Management*. Trzy lata później dokument ten został zaktualizowany, rozszerzony i opublikowany jako brytyjska norma BS 7799.

Główne przyczyny wzrostu popularności systemu zarządzania bezpieczeństwem informacji (SZBI) można podzielić na trzy grupy związane:
– ze wzrostem znaczenia informacji w gospodarce,
– z pogłębianiem współpracy pomiędzy przedsiębiorstwami,
– z rosnącym poziomem trudności zarządzania informacjami.

Do pierwszej grupy można zaliczyć poufność i dostępność informacji, a także konieczność zapewnienia ciągłości działania organizacji. Coraz więcej przedsiębiorców zauważa potrzebę zachowania poufności informacji w organizacji. Gdy weszła w życie ustawa o ochronie danych osobowych, wiele firm traktowało ją jako zbędne prawo, które utrudni pracę. Jednak nagłaśnianie przez prasę przypadków sprzedawania i wykorzystywania danych osobowych zarówno przez legalnie działające firmy, jak i przez organizacje przestępcze, spowodowało zmianę sposobu patrzenia na problem poufności. Współcześnie przedsiębiorcy są w stanie uszeregować informacje wykorzystywane w organizacji według poziomów poufności. Praktycznie nie spotyka się już postawy „nie mam nic do ukrycia". Jednak za tą świadomością często nie idzie wdrażanie zabezpieczeń. Kompleksowym sposobem rozwiązania tego problemu może być system zarządzania bezpieczeństwem informacji.

Dostępność informacji nie jest zwykle postrzegana jako problem organizacyjny. Brak dostępu do danych jest łatwo tłumaczony urlopem, brakiem prądu, wirusem, zgubionym kluczem. Niektórzy przedsiębiorcy lekceważą nawet włamania na stronę internetową firmy, traktując je jako *signum temporis*. Tymczasem, jak pokazały włamania na strony rządowe w kwietniu 2008 r., brak dostępu do informacji może wpływać na wizerunek zarówno całej organizacji, jak i osoby nią zarządzającej. Koszty braku dostępu do informacji mogą być znaczące dla sklepu internetowego, ale również dla przedsiębiorstwa, które będzie zmuszone opóźnić podjęcie ważnej decyzji. Koszty braku lub długiego czasu dostępu do informacji są trudne do zidentyfikowania i dlatego zwykle nie są mierzone.

Dostępność informacji jest jednym z czynników wpływających na zdolność organizacji do utrzymania ciągłości działania. Przerwanie ciągłości może nastąpić w wyniku długotrwałej awarii sieci energetycznej, odcięcia od dostępu do surowców, dostarczenia wadliwych półproduktów przez kooperanta, nieprawidłowego zaplanowania działań, awarii sieci informatycznej, niezachowania płynności finansowej i innych przyczyn. Już pobieżna analiza prasy przynosi wiele przykładów niezachowania ciągłości działania, takich jak choćby: zatrzymanie produkcji w zakładach chemicznych w Policach w wyniku awarii sieci energetycznej w kwietniu 2008 r., ograniczenie produkcji w zakładach produkujących nawozy sztuczne jako efekt ograniczenia dostaw gazu ziemnego z Rosji na początku 2006 r., przerwanie produkcji w zakładach Fiata w wyniku dostarczenia wadliwych części silników w lutym 2008 r. czy coroczne wiadomości o biurach podróży, które z powodów finansowych nie są w stanie zapewnić swoim klientom powrotu z wczasów w Grecji czy Egipcie. Zachwianie ciągłości działania zwykle oznacza duże straty, utratę wizerunku, a nawet konieczność zamknięcia działalności. Może ono być szczególnie niebezpieczne w przypadku stosowania technologii wymagających stałego działania linii produkcyjnej, np. linii odlewania stali, gdzie zatrzymanie oznacza konieczność przeprowadzenia kosztownego i długotrwałego remontu.

Pogłębianie współpracy pomiędzy przedsiębiorstwami związane z wdrażaniem nowoczesnych rozwiązań organizacyjnych, takich jak organizacje sieciowe, outsourcing, budowanie długotrwałych relacji zgodnie z zasadami zarządzania jakością i TQM, wprowadzanie międzyorganizacyjnych systemów informatycznych, powoduje konieczność badania nie tylko własnych zabezpieczeń, ale także bezpieczeństwa udostępnianych partnerom informacji. Przykładem może być niewielkie przedsiębiorstwo, które wykonywało zlecenia dla przemysłu motoryzacyjnego związane z wprowadzeniem nowych modeli samochodów. W związku z tym pracownicy mieli dostęp do poufnej dokumentacji projektowej, a także prototypów samochodów. Tymczasem organizacja nie stosowała żadnych zabezpieczeń, np. stosowano nieszyfrowaną sieć Wi-Fi, a komputery wyposażone w system Windows nie miały zapór.

W przypadku badania zabezpieczeń partnera niemożliwe jest zastosowanie audytu drugiej strony proponowanego w systemach zarządzania jakością, ponieważ samo dopuszczenie do jego przeprowadzenia może świadczyć o niewystarczającym

poziomie zabezpieczeń. Z tego powodu system zabezpieczeń certyfikowanych przez niezależną, akredytowaną organizację może być dobrym rozwiązaniem pozwalającym potwierdzić właściwy poziom bezpieczeństwa informacji u kontrahenta.

Trzecia istotna grupa przyczyn popularności SZBI to wzrost trudności zarządzania informacjami. W większości organizacji występują równolegle co najmniej dwa obiegi dokumentów – papierowy i elektroniczny. Dodatkowo wiele informacji przekazywanych jest ustnie bezpośrednio lub telefonicznie. Istniejące w przedsiębiorstwach służby informatyczne zajmują się wyłącznie bezpieczeństwem i funkcjonowaniem systemów informatycznych. Nadzorują działanie serwerów, funkcjonowanie sieci, instalują programy antywirusowe i zapory na stacjach roboczych. Jednak nie są zainteresowane pozatechnicznymi problemami obiegu informacji. Jeżeli przedsiębiorstwo wdrożyło system zarządzania jakością, to istnieją również służby odpowiedzialne za obieg dokumentów, ich aktualność i dostępność. Jednak zwykle pomijają one np. problemy poufności. Brakuje zatem spójnego podejścia do informacji i ich bezpieczeństwa w organizacji. Kompleksowa koncepcja zarządzania informacjami prezentowana przez SZBI może stanowić rozwiązanie tych problemów.

## 2. Ujęcie wieloaspektowe systemu zarządzania bezpieczeństwem informacji

System zarządzania bezpieczeństwem informacji może być analizowany w ujęciu wieloaspektowym obejmującym aspekty: celowościowy, podmiotowy, strukturalny, funkcjonalny i instrumentalny.

Głównym celem stosowania tego systemu jest zabezpieczenie obiegu informacji. Należy przez to rozumieć zarówno ograniczenie dostępu osób niepowołanych, jak i zapewnienie ciągłości działania, rzetelności i kompletności informacji. Celami pośrednimi są:

- zapewnienie stałej dostępności informacji dla pracowników,
- zapewnienie dostępności informacji dla klientów,
- ograniczenie dostępu do informacji osobom nie mającym uprawnień,
- uniemożliwienie dostępu osobom podejmującym nielegalne próby ich uzyskania,
- zapewnienie ciągłości działania systemu informacyjnego,
- zabezpieczenie przed utratą danych,
- stosowanie rozwiązań zapewniających dostęp do aktualnej, rzetelnej i kompletnej informacji.

Rozpatrując konkretną organizację, można, na podstawie powyższej listy, opracować klasyfikator celów uwzględniający specyfikę działania systemu informacyjnego. Przykładowe cele szczegółowe mogą dotyczyć: zarządzania incydentami związanymi z dostępem do danych, kontroli dostępu do aplikacji, wykrywania nieautoryzowanego przetwarzania informacji.

Cele powinny wynikać ze strategii organizacji, a dokładnie z jej polityki bezpieczeństwa informacji. Osobami odpowiedzialnymi za ich określenie muszą zatem

być najwyższe władze organizacji. Realizacja celów powinna być mierzona przez zestaw mierników oceniających skuteczność i efektywność systemu. Można w tym celu wykorzystać np. strategiczną kartę wyników, wprowadzając do niej nowy arkusz w perspektywie procesów wewnętrznych. Cele powinny być regularnie przeglądane, a ich realizacja monitorowana np. podczas przeglądów zarządzania lub spotkań komitetu bezpieczeństwa informacyjnego.

Podmiotami uczestniczącymi w systemie zarządzania bezpieczeństwem informacji są: dyrektor organizacji, menedżer bezpieczeństwa informacji, administrator systemów informatycznych wraz z informatykami, audytorzy wewnętrzni, kierow-

Tabela 1. Zadania uczestników systemu zarządzania bezpieczeństwem informacji

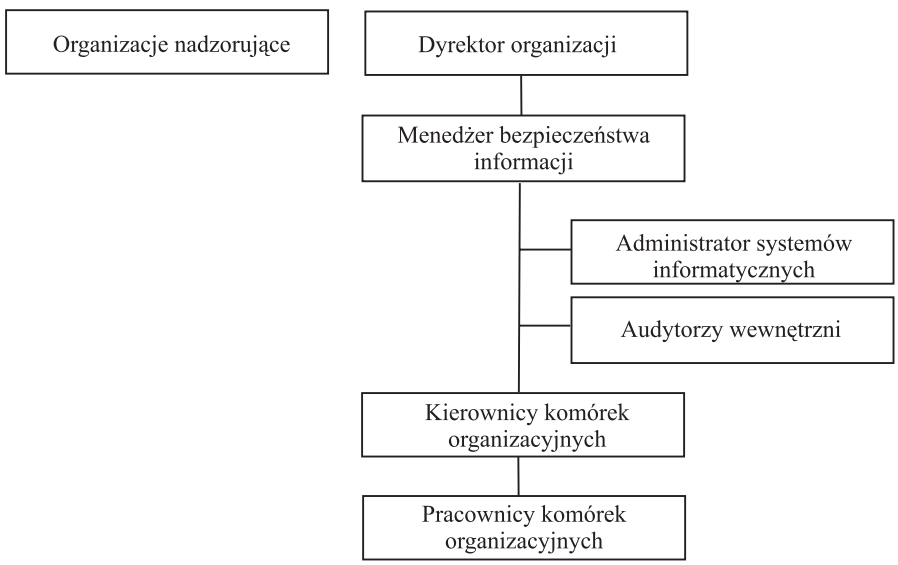
| Stanowisko | Zadania |
|---|---|
| Dyrektor organizacji | – określanie polityki bezpieczeństwa,<br>– wyznaczanie celów systemu,<br>– akceptowanie mierników monitorowania systemu,<br>– organizacja przeglądu zarządzania,<br>– okresowy monitoring działania systemu,<br>– przeprowadzanie kontroli (niezależnie od audytów) |
| Menedżer bezpieczeństwa informacji | – administrowanie systemem,<br>– monitoring działania zabezpieczeń,<br>– organizacja szacowania ryzyka,<br>– nadzorowanie prowadzenia działań korygujących i zapobiegawczych,<br>– szkolenie pracowników,<br>– raportowanie o działaniu całego systemu |
| Administrator systemów informatycznych | – monitoring zabezpieczeń informatycznych,<br>– wdrażanie zabezpieczeń,<br>– szkolenie pracowników (strona techniczna),<br>– raportowanie o stosowaniu zabezpieczeń technicznych |
| Audytor wewnętrzny | – monitoring funkcjonowania systemu,<br>– raportowanie wyników prowadzonych audytów,<br>– proponowanie wprowadzania działań korygujących i zapobiegawczych |
| Kierownik komórki organizacyjnej | – monitoring działania systemu w swojej komórce,<br>– monitoring powiązań pomiędzy komórkami lub organizacjami,<br>– zgłaszanie propozycji zmian w systemie,<br>– identyfikacja czynników ryzyka,<br>– analiza wystarczalności zabezpieczeń,<br>– raportowanie o działaniu systemu w komórce |
| Pracownik | – stosowanie zabezpieczeń,<br>– informowanie o incydentach,<br>– proponowanie zmian w zabezpieczeniach |
| Organizacje nadzorujące | – prowadzenie niezależnego audytu SZBI,<br>– wydawanie certyfikatów potwierdzających zgodność (jednostki certyfikujące),<br>– wskazywanie możliwych kierunków rozwijania systemu,<br>– zalecanie działań doskonalących |

Źródło: opracowanie własne.

nicy komórek organizacyjnych oraz pracownicy. Liczba uczestników może się zmieniać w zależności od liczby osób mających dostęp do aktywów informacyjnych. Szczególnym uczestnikiem mogą być organizacje zewnętrzne, które działają na zlecenie dyrektora organizacji, a ich zadaniem jest niezależne monitorowanie systemu. Zadania poszczególnych uczestników prezentuje tab. 1.

Zakres zadań zaprezentowany w tabeli może się zmieniać, w zależności od specyfiki organizacji oraz poziomu dojrzałości systemu. Wysoka świadomość pracowników może pozwolić bowiem na przekazanie im dodatkowych obowiązków. Kluczowym stanowiskiem ze względu na funkcjonowanie systemu jest menedżer bezpieczeństwa informacji. Musi on jednak mieć pełne poparcie ze strony dyrektora organizacji, bez którego system nie będzie działać prawidłowo. Poparcie to musi być prezentowane przy różnych okazjach pracownikom.

Na rysunku 1 zaprezentowano ramową strukturę systemu zarządzania bezpieczeństwem informacji. Dodatkowymi organami występującymi w systemie mogą być grupy robocze, np. komitet bezpieczeństwa informacji, którego uczestnicy pomagają dyrektorowi organizacji w kreowaniu polityki bezpieczeństwa.




Rys. 1. Ramowa struktura systemu zarządzania bezpieczeństwem informacji w organizacji

Źródło: opracowanie własne.

Głównymi funkcjami systemu zarządzania bezpieczeństwem informacji są: wykrywanie niedoskonałości systemu, wykrywanie incydentów, identyfikacja zagrożeń, wprowadzanie zabezpieczeń, analiza skuteczności zabezpieczeń oraz zwiększanie efektywności działania systemu. Funkcje te są realizowane przez procesy, wśród których należy wyróżnić systemowe, tzn.: szacowanie ryzyka, nadzór nad dokumentami

i zapisami, przegląd systemu, audyt wewnętrzny oraz działania korygujące i zapobiegawcze. Dodatkowo, ze względu na specyfikę organizacji można wyróżnić procesy związane ze stosowanymi grupami zabezpieczeń, np. zarządzanie dostępem do systemów informatycznych, wypożyczanie aktywów czy udzielanie dostępu do obszarów bezpiecznych.

Podstawowymi instrumentami systemu zarządzania bezpieczeństwem informacji są metody szacowania ryzyka, audyt, przegląd zarządzania oraz zabezpieczenia zebrane w dziesięciu grupach (*Norma ISO 27001:2005*..., 2007, s. 20 i n.):

– A.5. Polityka bezpieczeństwa.
– A.6. Organizacja bezpieczeństwa informacji.
– A.7. Zarządzanie aktywami.
– A.8. Bezpieczeństwo zasobów ludzkich.
– A.9. Bezpieczeństwo fizyczne i środowiskowe.
– A.10. Zarządzanie systemami i sieciami.
– A.11. Kontrola dostępu.
– A.12. Pozyskiwanie, rozwój i utrzymanie systemów informacyjnych.
– A.13. Zarządzanie incydentami związanymi z bezpieczeństwem informacji.
– A.14. Zarządzanie ciągłością działania.
– A.15. Zgodność.

Dodatkowo można wskazać narzędzia stanowiące programowe oraz sprzętowe zabezpieczenia. Do pierwszej grupy zaliczyć można zapory, routery, konfigurację sieci, do drugiej zaś zamki, kłódki czy szafy pancerne. Jednak kluczowym zadaniem wymienionych grup zabezpieczeń jest uświadomienie pracowników, jak bowiem wskazuje doświadczenie, człowiek stanowi najsłabsze ogniwo systemu bezpieczeństwa informacyjnego.

## 3. Wdrożenie SZBI jako proces

Procedura przygotowania i wdrożenia systemu zarządzania bezpieczeństwem informacji została opisana w punktach 4.2 i 4.3 normy [*Norma ISO 27001:2005*…, 2007, s. 9]. Składa się ona z następujących kroków:

– określenia zakresu i granic SZBI,
– określenia polityki SZBI,
– określenia podejścia do szacowania ryzyka,
– określenia ryzyka,
– analizy i oceny ryzyka,
– identyfikacji i oceny wariantów postępowania z ryzykiem,
– wybrania zabezpieczeń,
– akceptacji ryzyka szczątkowego,
– uzyskania autoryzacji dla wdrożenia systemu,
– opracowania deklaracji stosowania,
– opracowania planu postępowania z ryzykiem,

– wdrożenia planu postępowania z ryzykiem,
– wdrożenia zabezpieczeń,
– określenia sposobów mierzenia skuteczności zabezpieczeń,
– szkolenia pracowników i współpracowników.

Zakres systemu zarządzania bezpieczeństwem informacji nie może być dowolnie określony, musi bowiem uwzględniać charakter działalności organizacji. Błędem jest podmiotowe lub przedmiotowe ograniczanie systemu, które może spowodować jego niepełną sprawność. Przykładowo wprowadzenie systemu wyłącznie w biurze obsługi klienta lub tylko w zakresie systemu informatycznego z pewnością nie przyniesie oczekiwanych efektów. W przypadku gdy organizacja wdrożyła już system zarządzania jakością, dobrym rozwiązaniem jest jego integracja z SZBI. Działanie takie przyczynia się do skrócenia czasu wdrożenia, a jednocześnie do obniżenia kosztów funkcjonowania.

Między wspomnianymi systemami występuje wiele podobieństw, takich jak choćby struktura dokumentacji, na której szczycie znajduje się polityka SZBI. Jej zadaniem jest określenie głównych kierunków i zasad działania w zakresie zapewnienia bezpieczeństwa informacji. Z punktu widzenia zarządzania strategicznego polityka może być traktowana jako element strategii dotyczący prawidłowego funkcjonowania systemu informacyjnego. Takie spojrzenie pozwala w przypadku zintegrowanego systemu zarządzania na łatwiejsze zarządzanie wieloma rodzajami polityki występującymi w firmie.

Kluczowym etapem projektowania systemu zarządzania bezpieczeństwem informacji jest opracowanie metody szacowania ryzyka. Norma ISO 27001:2005 nie wskazuje konkretnej metody, zostawia w tym względzie pewną dowolność. Takie podejście jest uzasadnione, ponieważ systemy są wdrażane w różnych organizacjach. Propozycję metody zawiera natomiast norma ISO TR 13335-3:1998. Ogranicza się ona wprawdzie do systemów informatycznych, jednak może być z łatwością zaadaptowana do szerszej kategorii, jaką jest system informacyjny[1]. Metoda musi być przygotowana w sposób, który umożliwi wielokrotne jej powtarzanie i zapewni porównywalność wyników. Powinna ona uwzględniać nie tylko wymagania prawne, ale także związane z działalnością organizacji. Metoda musi zawierać kryteria, które pozwolą na zdefiniowanie akceptowalnych poziomów ryzyka, a na tej podstawie na podjęcie decyzji o akceptacji.

Norma ISO 27001:2005 wymaga, aby określenie ryzyka było prowadzone w czterech krokach:
– identyfikacji, jakie aktywa (informacje, sprzęt itp.) znajdują się w organizacji w zakresie wdrażania SZBI oraz kto jest za nie odpowiedzialny,
– identyfikacji, co może stanowić zagrożenie dla tych aktywów,
– identyfikacji podatności, czyli słabych stron aktywów,
– identyfikacji konsekwencji dla aktywów w przypadku wystąpienia zagrożeń.

[1] Częstym błędem popełnianym podczas wdrożenia systemu zarządzania bezpieczeństwem informacji jest pominięcie informacji występujących w formie innej niż elektroniczna (np. dokumentacji papierowej, nagrań, tablic informacyjnych czy rozmów telefonicznych).

Nie zostało w normie wskazane jednoznacznie, że zagrożenia i podatności powinny być zidentyfikowane indywidualnie dla każdego typu aktywów, jednak audytorzy certyfikujący systemy niechętnie odnoszą się do metod, w których podatności zostały określone grupowo[2]. Identyfikacja ryzyka jest działaniem pracochłonnym i wymaga uczestnictwa przedstawicieli wszystkich komórek organizacyjnych. Z tego powodu optymalnym sposobem jego przeprowadzenia jest szkolenie połączone z warsztatami.

Analiza ryzyka jest prowadzona na podstawie wyników identyfikacji. Jej celem jest wskazanie strat, jakie może spowodować naruszenie poufności, dostępności, dokładności lub kompletności (integralności) aktywów[3]. Następnie należy wskazać prawdopodobieństwo wystąpienia incydentów naruszenia bezpieczeństwa oraz strat, uwzględniając przy tym stosowane obecnie zabezpieczenia. Na tej podstawie możliwe jest oszacowanie poziomu ryzyka i podjęcie decyzji, czy jest ono akceptowalne, czy też konieczne jest podjęcie dodatkowych działań zabezpieczających.

Norma proponuje cztery rozwiązania: wprowadzenie zabezpieczeń, świadome zaakceptowanie ryzyka, unikanie ryzyka lub przeniesienie go na inne organizacje, np. ubezpieczycieli. Wybór zabezpieczeń jest ułatwiony dzięki obecności w normie listy ponad 100 propozycji, których wdrożenie należy rozważyć. Lista została opracowana na podstawie zasad zarządzania bezpieczeństwem informacji opublikowanych w *Normie ISO 17799:2005*.

Akceptacja ryzyka szczątkowego (akceptowalnego) przez kierownictwo oraz zgoda na wdrożenie stanowią przejście od fazy projektowania do fazy implementacji systemu zarządzania bezpieczeństwem informacji. Efektem zakończonej fazy projektowania jest deklaracja stosowania SZBI, która zawiera opis wybranych i wdrożonych zabezpieczeń, a także ewentualne uzasadnienia wyłączenia niektórych zabezpieczeń zalecanych przez normę.

Fazę wdrożenia rozpoczyna opracowanie i wdrożenie planu postępowania z ryzykiem. W planie tym należy określić działania, które powinny zostać podjęte, i ich kolejność oraz wskazać stanowiska odpowiedzialne za wprowadzanie zmian. Następnym etapem jest wdrożenie zabezpieczeń przewidzianych w deklaracji stosowania oraz określenie sposobu mierzenia ich skuteczności. Należy zapewnić możliwość porównywania wartości wskaźników w czasie. Końcowym etapem fazy wdrożeniowej jest przeprowadzenie szkoleń. Ich celem jest zaznajomienie pracowników z nowymi sposobami organizacji pracy i wyjaśnienie przyczyn wprowadzanych zmian.

[2] Audytorzy argumentują przy tym, że takie rozwiązanie uniemożliwia uzyskanie powtarzalności metody. Trudno się zgodzić z takim argumentem, patrząc z punktu widzenia organizacji. Należy natomiast zauważyć, że utrudnia to pracę audytora i może znacznie wydłużyć proces audytowania.

[3] Bezpieczeństwo informacji jest rozumiane w normie ISO 27001:2005 jako poufność, dokładność i integralność. Nazwa systemu może zatem być myląca i stać się przyczyną błędów wdrożeniowych. Jednocześnie warto zauważyć, że w literaturze polskiej można znaleźć szersze podejście do problematyki informacji, np. u K. Woźniaka [2005].

## 4. Podsumowanie

Wdrożenie systemu zarządzania bezpieczeństwem informacji jest procesem o wiele bardziej złożonym niż implementacja systemu zarządzania jakością ze względu na dużą liczbę czynników mogących wpłynąć na jego skuteczność. Niezbędne staje się zapewnienie wysoko wykwalifikowanych kadr nie tylko posiadających umiejętności w zakresie informatycznym, ale także dobrze znających zasady wdrażania systemów zarządzania na bazie norm ISO.

Wymagana jest także podwyższona świadomość kierownictwa organizacji. Brak zdecydowania kierownictwa w zakresie wykorzystania technologii, dążenie do stosowania modnych narzędzi informatycznych czy pozorna oszczędność we wprowadzaniu innowacji mogą spowodować, że organizacja stanie się bardziej podatna na zagrożenia.

Podejście procesowe do wdrażania SZBI ułatwia budowę spójnego, logicznego systemu, który zapewni wymagany poziom bezpieczeństwa, a jednocześnie nie sparaliżuje przedsiębiorstwa serią niewłaściwie skonfigurowanych zabezpieczeń.

## Literatura

Krupski R. (red.), *Zarządzanie przedsiębiorstwem w turbulentnym otoczeniu*, PWE, Warszawa 2005.

*Norma ISO 17799:2005 Technika informatyczna – Techniki bezpieczeństwa – Praktyczne zasady zarządzania bezpieczeństwem informacji*, PKN, Warszawa 2007.

*Norma ISO 27001:2005 Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji – Wymagania*, PKN, Warszawa 2007.

*Norma ISO TR 13335-3 Information Technology – Guidelines for the management of IT Security – Part 3: Techniques for the management of IT Security*, ISO, Geneva 1998.

Saint-Germain R., *Information security management best practice based on ISO/IEC 17799*, „The Information Management Journal" July/August 2005.

Woźniak K., *SIM jako instrument wspomagania zarządzania strategicznego w firmie*, praca doktorska, AE, Kraków 2005.

## A PROCESS APPROACH TO IMPLEMENTATION OF INFORMATION SECURITY MANAGEMENT SYSTEMS

### Summary

Information security management systems are applicable in computer and telecommunications services, public administration and self-government administration. Top management of organization, while beginning implementation of ISMS usually covers only technical problems of information security, which can be solved by computer experts. Only a few of managers are aware of organizational problems connected with specificity of products or services. In this article, a process approach to implementation of ISMS was discussed.