PRACE NAUKOWE AKADEMII EKONOMICZNEJ WE WROCŁAWIU
Nr 1144 — 2006
Informatyka Ekonomiczna 9

Adam Nowicki, Artur Rot

ROLA KULTURY ORGANIZACYJNEJ W ZARZĄDZANIU BEZPIECZEŃSTWEM SYSTEMU INFORMACYJNEGO PRZEDSIĘBIORSTWA

1. Wstęp

Globalizacja gospodarki powoduje, iż dotychczasowe warunki, w których funkcjonowały organizacje, diametralnie się zmieniają. Otoczenie, w którym działa współczesne przedsiębiorstwo, jest nie tylko zmienne, ale często wręcz nieprzewidywalne. Według R. Krupskiego „wysoka turbulencja otoczenia, nieciągłość zdarzeń oraz globalizacja procesów i struktur to podstawowe cechy współczesnego świata gospodarczego" [Krupski 2003]. Współczesne zarządzanie w warunkach nowej globalnej ekonomii, jak nigdy jeszcze dotąd, uzależnione jest od informacji i sprawnie działających systemów informacyjnych (SI). Technologia informacyjna pozwala osiągnąć organizacjom nową jakość funkcjonowania, a jednocześnie rośnie stopień zależności sprawnego zarządzania od nowoczesnych, lecz bezpiecznych rozwiązań teleinformatycznych. W miarę postępu technologicznego, a szczególnie gwałtownego rozwoju Internetu, a także wzrostu znaczenia informacji dla funkcjonowania organizacji, zagrożenia systemu informacyjnego stają się coraz bardziej powszechne i przybierają różnorodne formy. Systemy informacyjne wykreowały nowe rodzaje ryzyka, a ich bezpieczeństwo nabrało wymiaru globalnego i przyczyniło się do coraz szerszego zakresu systemów informatycznych.

We współczesnych systemach informacyjnych same zabezpieczenia technologiczne nie są już wystarczające. Zapewnienie bezpieczeństwa systemu informacyjnego powinno być sumą rozwiązań organizacyjnych i technicznych. Ponieważ obecnie systemy informacyjne są często bardzo złożone, heterogeniczne i mają charakter dynamiczny, pojedyncze rozwiązania nie mogą zapewnić pełnej ochrony przed wszystkimi możliwymi zagrożeniami. Dlatego warto nakładać warstwy odpowiednich rozwiązań, które chronią przed jak największą ich liczbą.

Zarządzanie bezpieczeństwem systemu informacyjnego jest ciągłym, dynamicznym i skomplikowanym procesem, wymagającym stałego nadzoru i przystosowywania się do zmiennych warunków otoczenia. Musi być ono rozpatrywane nie tylko w aspekcie technologicznym, ale również społecznym, organizacyjnym, ekonomicznym oraz prawnym. Dlatego też istnieje konieczność podjęcia rozważań

dotyczących nie tylko technologicznej sfery zarządzania bezpieczeństwem SI, ale przede wszystkim zagadnień natury organizacyjnej, w szczególnie tych związanych z kulturą organizacyjną w firmie.

Niniejszy artykuł jest próbą prezentacji istoty i znaczenia zarządzania bezpieczeństwem SI. Jego celem jest również wskazanie znaczenia kultury organizacyjnej dla bezpieczeństwa SI, a także podkreślenie, iż proces zarządzania bezpieczeństwem jest ściśle powiązany z zarządzaniem organizacją oraz powinien być elementem zarówno strategii biznesu, jak i strategii IT.

2. Zarządzanie organizacją a zarządzanie bezpieczeństwem

Współczesne koncepcje zarządzania przedsiębiorstwem wymagają coraz większego zasilania w informację i wiedzę. Informacja staje się, w coraz większym stopniu podstawowym zasobem przedsiębiorstw, zwłaszcza przedsiębiorstw działających na mocno konkurencyjnych rynkach. Stąd też zagadnienia związane z bezpieczeństwem SI stanowią integralną część ogólnego planu zarządzania organizacją. Problematyka ta jest również powiązana z wymogami prawnymi. Nie bez znaczenia są również uwarunkowania kulturowe i środowiskowe. Omówienia i analizy zagadnień związanych z zarządzaniem bezpieczeństwem SI nie można zatem przeprowadzać w oderwaniu od teorii organizacji i zarządzania.

Współczesne metody zarządzania znacznie różnią się od metod klasycznych, proponowanych przez takich teoretyków organizacji i zarządzania, jak F. Taylor, K. Adamiecki, H. Fayol czy M. Weber. Podobnie jest z organizacjami, które funkcjonują w zupełnie innych warunkach społecznych i ekonomicznych.

W warunkach gospodarki globalnej, obok niewątpliwie najważniejszego dla organizacji zasobu, który stanowią ludzie, coraz większego znaczenia nabierają zasoby informacyjne oraz związana z nimi technologia informacyjna. Obecnie wyróżnia się trzy zasadnicze podejścia do teorii organizacji i zarządzania, których znaczenie może wzrastać, a mianowicie: kierunek systemowy, kierunek sytuacyjny i tzw. kierunek dynamicznego zaangażowania.

Kierunek systemowy pozwala na postrzeganie organizacji jako całości i jako części większego środowiska zewnętrznego. Systemowa teoria organizacji obejmuje analizę organizacji jako systemu społecznego złożonego z takich elementów, jak: role społeczne, cele, wartości, układy informacyjno-decyzyjne, a także metody i techniki zarządzania. Podstawowym narzędziem badawczym w ujęciach systemowych jest model [Krupski 2005, s. 245]. Z kolei **Kierunek sytuacyjny** koncentruje się na współzależnościach wielu czynników występujących w sytuacji kierowniczej. **Kierunek dynamicznego zaangażowania** zaś stanowi wyzwanie dla sposobu myślenia o zarządzaniu i organizacjach w XXI w. Zwolennicy tego kierunku coraz częściej nakłaniają kierowników do przemyślenia tradycyjnych struktur organizacyjnych. M. Hammer i J. Champy, twórcy koncepcji reinżynieringu, zachę-

cają do zastępowania pewnych procesów nowymi, które zwiększą sprawność organizacyjną. Reinżynieringoznacza bowiem „radykalne przemyślenie i przeprojektowanie procesów, za pośrednictwem których stwarzamy wartość (dla klientów) i wykonujemy pracę" [Hammer, Champy 1995].

Zarządzanie bezpieczeństwem SI jest złożonym przedsięwzięciem, mającym duże znaczenie dla organizacji, dlatego trzeba do niego podchodzić w sposób systemowy. **Podejście systemowe** jest czołowym paradygmatem w nauce drugiej połowy XX w. Szereg nauk, w tym nauki o organizacji i zarządzaniu, przyjęło ten paradygmat, podkreślający, że całość to więcej niż suma jej części, a więc istnieje konieczność badania poszczególnych elementów nie w oderwaniu od siebie, ale z uwzględnieniem relacji o określonych właściwościach zachodzących między nimi [Krupski 2005, s. 240-241].

Według J. Skalika, cechą charakterystyczną podejścia systemowego jest uwzględnienie otoczenia, celów, elementów i relacji między nimi, traktowanych jako system [Skalik 1998, s. 147]. Wzmożone zainteresowanie tym nurtem sprawiła m.in. publikacja P.M. Sengego [1998], w której autor udowodnił wielką użyteczność badania dynamiki systemów społecznych. Odnosząc to do problematyki zarządzania bezpieczeństwem SI, należy pamiętać, iż największym zasobem SI są ludzie. Są oni jednak również przyczyną największych zagrożeń dla jego bezpieczeństwa. Ważne są więc odpowiednie motywowanie i kontrola zachowań pracowników, podnoszenie poziomu ich świadomości i umiejętne edukowanie. Ujęcie systemowe koncentruje się także na oddziaływaniach między elementami systemu, opiera się na spojrzeniu ogólnym, całościowym oraz prowadzi do działania „kierunkowego" nastawionego na cel. Senge określił je jako „dyscyplinę widzenia całości".

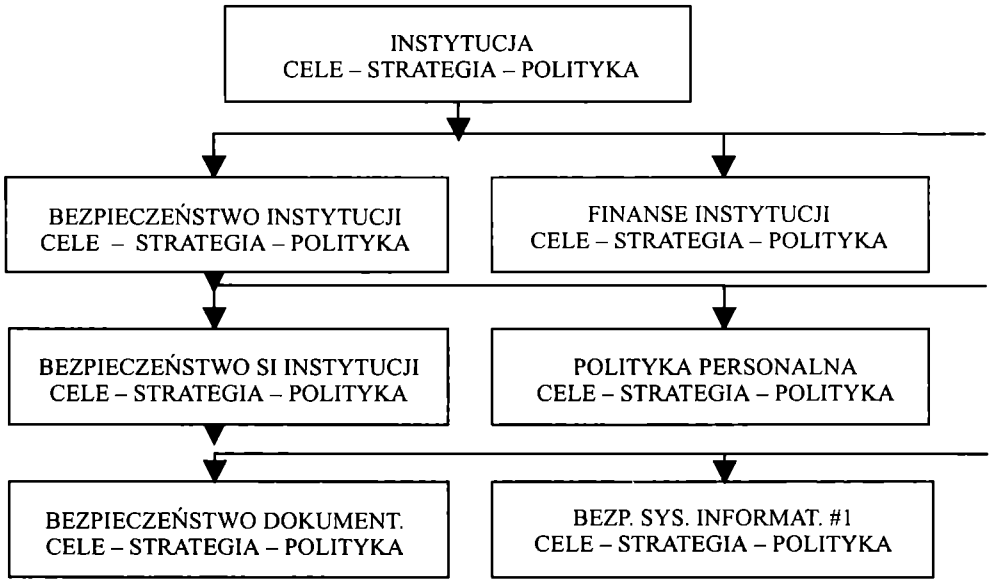
Zarządzanie bezpieczeństwem systemu informacyjnego będzie zatem dotyczyć m.in.:

- wyznaczania osób odpowiedzialnych za proces na wszystkich jego poziomach,
- określania celów i ustalenia generalnej strategii w zakresie bezpieczeństwa SI,
- koordynowania ludźmi oraz zasobami organizacji w celu zapewnienia odpowiedniego poziomu dostępności, poufności, integralności, autentyczności i niezawodności zasobów systemu informacyjnego,
- określenia zadań do wykonania oraz ustalenia, kto je wykona, jak je grupować i gdzie ma się podejmować decyzje w zakresie bezpieczeństwa SI,
- kierowania ludźmi, czyli motywowania załogi organizacji do pracy w interesie organizacji, w sposób zapewniający bezpieczeństwo SI,
- podnoszenia umiejętności i świadomości pracowników w zakresie zastosowania technologii informacyjnych i ich bezpieczeństwa,
- kontrolowania działań, porównywania ich z celami i korygowania znacznych odchyleń, co pozwoli na osiągnięcie ustalonych celów w zakresie bezpieczeństwa,
- monitorowania i oceny wyników zarządzania.

Klasyczne funkcje zarządzania: planowanie, organizowanie, motywowanie (odnoszone do ludzi) i kontrola występujące w różnych sekwencjach są nierozerwalnie złączone z wymienionymi działaniami w obszarze bezpieczeństwa systemów informacyjnych przedsiębiorstwa. Ponadto, zarządzanie bezpieczeństwem SI to proces oparty na wskazaniu [Biała 2000, s. 281-282]:

- **celów** – określenie, co ma być osiągnięte,
- **strategii** – określenie, jak osiągnąć wytyczone cele,
- **polityki** – określenie, co ma być wykonane dla osiągnięcia celów.

Odzwierciedla to hierarchiczny model organizacji, która ma wytyczony globalny cel, misję związaną z tym, do czego została dana instytucja powołana. Globalne cele, strategia i polityka organizacji są uwarunkowane szeregiem czynników i elementów, takich jak bezpieczeństwo instytucji, jej finanse, technologia, rynek itp., położonych niżej w podstawowej hierarchii (zob. rys. 1).

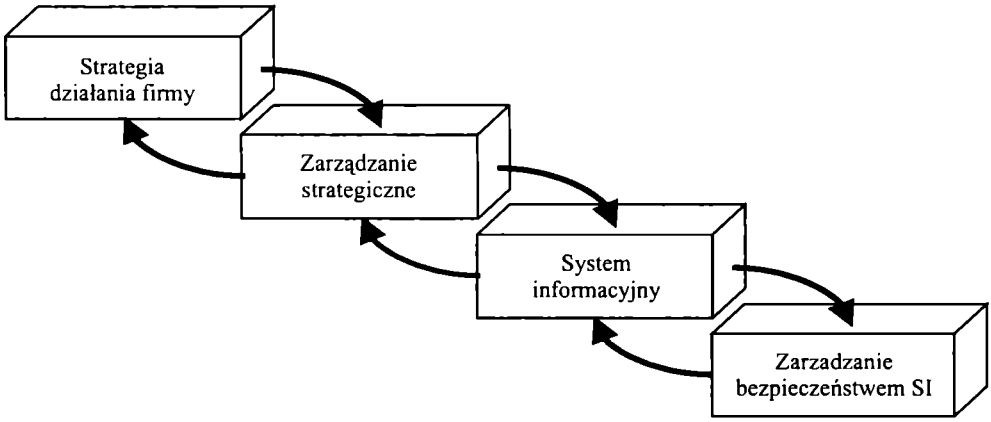


Rys. 1. Hierarchia celów, strategii oraz polityki w instytucji

Źródło: [Białas 2000, s. 282].

W znacznej części pozycji literaturowych rozważania dotyczące bezpieczeństwa systemów informacyjnych prowadzono w pewnym oderwaniu od środowiska, w którym zarządzanie bezpieczeństwem jest realizowane, czyli od instytucji. Problematykę zarządzania bezpieczeństwem systemu informacyjnego w przedsiębiorstwie należy bowiem rozważać w aspektach zarządzania strategicznego, gdyż musi ono zostać wpisane w strategię firmy. Powinno ono być elementem zarówno strategii biznesu, jak i strategii IT. Problematyce zarządzania strategicznego poświęcona została praca [Krupski 2003]. W publikacji tej zarządzanie strategiczne

zostało zdefiniowane jako „proces definiowania i redefiniowania strategii w reakcji na zmiany otoczenia lub wyprzedzający te zmiany, a nawet je wywołujący, oraz sprzężony z nim proces implementacji, w którym zasoby i umiejętności są tak dysponowane, by realizować przyjęte długofalowe cele rozwoju, a także by zabezpieczyć istnienie organizacji w potencjalnych sytuacjach nieciągłości". Z kolei Z. Drążek i B. Niemczynowicz definiują je jako „trudną sztukę kierowania rozwojem organizacji w długim okresie oraz umiejętność wykorzystywania szans i unikania zagrożeń w jej otoczeniu" (Drążek, Niemczynowicz 2003, s. 13).

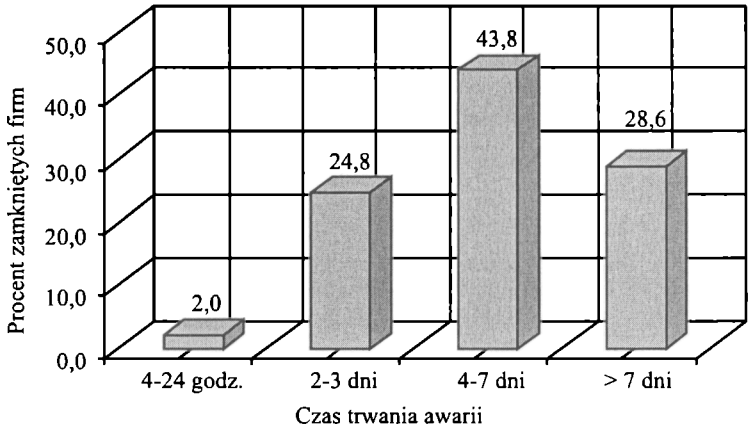


Rys. 2. Relacje pomiędzy strategią firmy a zarządzaniem bezpieczeństwem systemu informacyjnego
Źródło: opracowanie własne.

Powyższe definicje zwracają uwagę na kwestię unikania zagrożeń oraz zapewnienia ciągłości funkcjonowania organizacji. Realizacja tych zadań uzależniona jest bezpośrednio od sprawnego zarządzania bezpieczeństwem SI. Na rysunku 3. zobrazowano zależność pomiędzy awarią systemu informacyjnego a ryzykiem upadłości przedsiębiorstwa. Awaria systemu informatycznego może wywołać bardzo poważne konsekwencje dla przedsiębiorstwa. Według badań firmy Debis Systemhaus GmbH awarii trwającej 2-3 dni nie jest w stanie przetrwać co czwarta firma, jednak gdy awaria jest dłuższa, ryzyko upadłości jest już znaczne [*Bezpieczeństwo systemów...*, s. 68].

Badania przeprowadzonych w 2002 r. w 1300 firmach na terenie USA i Kanady dały następujące wyniki i spostrzeżenia (Grzywacz 2003, s. 15):

- 54 firm poniosło straty w wyniku ataków i włamań,
- 78 firm poniosło straty wskutek działalności wprowadzonych wirusów,
- 42 firm zanotowało ataki z zewnątrz,
- 25 firm straciło w wyniku włamań ponad 250 tys. dol.,
- 15 firm straciło w wyniku włamań ponad 1 mln dol.,
- większość firm nie potrafiła podać wielkości strat.



Rys. 3. Czas awarii a ryzyko upadłości przedsiębiorstwa

Źródło: [*Bezpieczeństwo systemów...*, s. 68].

Z powyższych danych wynika niezaprzeczalnie konieczność uwzględnienia celów bezpieczeństwa systemu informacyjnego w strategii firmy. Ponadto w pracy [Krupski 2003] stwierdza się, iż podstawą formułowania i realizacji zarządzania strategicznego jest informacja. Dlatego też strategia organizacji, osiąganie celów przedsiębiorstwa, a więc i zarządzanie strategiczne, uzależnione są od sprawnie funkcjonującego (również bezpiecznego) systemu informacyjnego.

3. Istota, cele i przesłanki zarządzania bezpieczeństwem SI

Jak już podkreślano w artykule, sprawne funkcjonowanie współczesnych przedsiębiorstw nie jest obecnie możliwe bez zastosowania nowoczesnych technologii informacyjnych. Rozwój technologii informacyjnych i e-gospodarki oprócz ogromnych korzyści niesie ze sobą także zagrożenia. Są to nowe rodzaje niebezpieczeństw, często niezrozumiane i niedoceniane przez kierownictwo organizacji. Według firmy Ernst & Young największą przeszkodą w osiągnięciu potrzebnego poziomu bezpieczeństwa jest zbyt duże tempo zmian i wzrost stopnia zaawansowania zagrożeń (tak uważa 70% respondentów wspomnianych już badań przeprowadzonych przez Ernst & Young w 2004 r.) [Ernst & Young 2004]. Ponad połowa menedżerów uważa, że ich pracownicy nie posiadają wystarczających możliwości, aby sprostać rosnącym zagrożeniom.

W miarę rozwoju systemów informacyjnych zmienia się technologia zabezpieczeń, jednak dziś same zabezpieczenia już nie wystarczają – należy je optymalnie dobierać, właściwie stosować i odpowiednio nimi zarządzać [Białas 2001]. Aby zapewnić prawidłowe funkcjonowanie systemów informatycznych firmy, należy sprawnie i efektywnie zarządzać bezpieczeństwem. Nowoczesne przedsiębiorstwo musi stosować cały zestaw uzupełniających się metod, narzędzi, syste-

mów politycznych oraz procedur, aby chronić się przed zagrożeniami, stąd konieczność podejścia do problematyki bezpieczeństwa SI w sposób systemowy. Podejście systemowe jest to element konieczny dla właściwego funkcjonowania systemu bezpieczeństwa, a co za tym idzie – rozwoju przedsiębiorstwa [Wajda 2002, s. 829-831].

W większości krajowych opracowań dotyczących problematyki zarządzania bezpieczeństwem przyjmuje się definicję przytoczoną w normie PN-I-02000 – *Technika informatyczna – Zabezpieczenia w systemach informatycznych – Terminologia*. Do definicji tej można mieć jednak pewne zastrzeżenia. Po pierwsze, wyszczególnione w niej etapy i elementy procesu zarządzania bezpieczeństwem nie wydają się być kompletne i spójne. Ponadto w definicji opracowanej poniżej zwrócono uwagę na cykliczność i powtarzalność procesów zarządzania bezpieczeństwem SI, które są zasadniczym elementem w dynamicznie zmieniającym się otoczeniu funkcjonowania systemów informacyjnych. Dlatego też zbiór działań i procesów wchodzących w skład zarządzania bezpieczeństwem można uzupełnić o procesy doskonalenia systemu zabezpieczeń. Na te aspekty pierwotna definicja nie zwracała uwagi. Poniższa definicja porusza ponadto aspekt ekonomiczny, który w definicji przytoczonej przez Polski Komitet Normalizacyjny został całkowicie pominięty. Zarządzanie bezpieczeństwem musi wiązać się z racjonalnym finansowaniem i umiejętnym gospodarowaniem przeznaczonymi na ten cel środkami finansowymi [Wawrzyniak 2002].

Zarządzanie bezpieczeństwem systemu informacyjnego to ciągły, cykliczny, złożony i racjonalnie finansowany proces, umożliwiający bezpieczną realizację misji, do której instytucję powołano. Zarządzanie bezpieczeństwem systemu informacyjnego obejmuje zespół złożonych powtarzalnych procesów zmierzających do osiągnięcia i utrzymywania oczekiwanego poziomu bezpieczeństwa systemu informacyjnego, tzn. poziomu poufności, integralności, dostępności, autentyczności i niezawodności. Jego realizacja obejmuje działania, takie jak:

- określenie celów, strategii i polityk bezpieczeństwa SI instytucji,
- określenie potrzeb bezpieczeństwa systemu informacyjnego instytucji,
- identyfikowanie i analizowanie zagrożeń dla zasobów systemu informacyjnego przedsiębiorstwa,
- identyfikowanie i analizowanie ryzyka naruszenia zasobów SI,
- planowanie i projektowanie adekwatnych zabezpieczeń (metod, środków fizycznych, technologicznych, organizacyjnych, kadrowych itp.)
- monitorowanie i ocena wdrożenia oraz eksploatacji zabezpieczeń w celu racjonalnego zabezpieczenia systemu informacyjnego przedsiębiorstwa,
- opracowanie i wdrożenie programu szkoleniowo-uświadamiającego,
- ciągłe doskonalenie systemu zabezpieczeń.

Aby możliwe było pełne spełnienie tych funkcji, zarządzanie bezpieczeństwem systemu informacyjnego powinno stanowić integralną cześć ogólnego planu zarządzania przedsiębiorstwem. Jedno jest pewne: zapewnienie odpo-

wiedniego stanu bezpieczeństwa systemu informacyjnego wymaga kompleksowego podejścia. Rozwiązania techniczne oraz odpowiedni poziom inwestycji są istotne, ale równie ważnymi elementami są zasoby ludzkie oraz kwestie organizacyjne, a szczególnie poziom kultury organizacyjnej [Bryl 2005].

Zarządzanie bezpieczeństwem ma charakter złożony. Rozważania w tym zakresie mogą dotyczyć [Jelonek 2005]:

- istoty informacji i jej specyficznej postaci, często niezrozumiałej dla wielu osób (pracownicy nie znając wagi informacji, często nie są świadomi, że nastąpiło nadużycie),
- systemów, w których informacja jest przetwarzana, gromadzona i rozpowszechniana,
- środowiska, w którym te systemy działają (np. pomieszczenia),
- personelu, który korzysta z tych systemów i który często bywa nieprzewidywalny, łamiąc zasady bezpiecznego użytkowania systemów informatycznych,
- całego otoczenia prawnego.

Dodając do tego, że wszystko wokół jest zmienne i słabo określone, zapewnienie bezpieczeństwa złożonego systemu nie jest sprawą trywialną, wymaga wzorowej organizacji, dyscypliny, wiedzy i sprawnego zarządzania. Zatem zarządzanie bezpieczeństwem SI to nie tylko stosowanie zabezpieczeń technologicznych, ale przede wszystkim procesy związane z czynnikiem ludzkim, polegające na właściwym ich doborze, przeszkoleniu, motywowaniu. Odpowiednia rola kierownictwa przedsiębiorstwa w procesach zarządzania bezpieczeństwem, właściwy dobór pracowników, stworzenie stanowiska inspektora bezpieczeństwa i dobór na nie odpowiedniej osoby, dbałość o personel, szkolenia użytkowników systemów informatycznych oraz odpowiednia polityka w zakresie kontaktów z kontrahentami są elementami koniecznymi do utrzymania właściwego poziomu bezpieczeństwa systemu informacyjnego w obiekcie gospodarczym.

Najpewniejszą ochronę zasobów przedsiębiorstwa zapewnimy poprzez wdrożenie pełnego systemu zarządzania bezpieczeństwem. Korzyści z wdrożenia takiego systemu i podejścia do omawianych zagadnień w sposób systemowy to m.in. [Niemiec 2002]:

- zgodność z wymaganiami prawnymi,
- ochrona interesów firmy,
- poprawa wydajności pracowników osiągana poprzez odpowiednie szkolenia,
- lepsza organizacja pracy,
- oszczędności finansowe,
- poprawa wizerunku organizacji.

Konsekwencja w zabezpieczaniu zasobów, monitorowaniu bezpieczeństwa, wykrywaniu i ściganiu nadużyć pozwala na bieżąco sprawować pełną kontrolę nad posiadanymi informacjami, co w dłuższej perspektywie w połączeniu z otwartą polityką informacyjną umożliwi zwiększenie zaufania do firmy przez jej klientów i partnerów [Szafrański 2001]. Tymczasem wiele przedsiębiorstw inwestuje w pro-

dukty związane z bezpieczeństwem dopiero wtedy, gdy zostaną ujawnione słabości i trzeba przedsięwziąć jakieś kroki, nie stosuje natomiast ciągłej analizy i eliminacji zagrożeń. Bagatelizując problem zarządzania bezpieczeństwem SI, narażamy przedsiębiorstwo na skutki, do których zaliczyć można przede wszystkim:

- straty materialne (przeciek ważnych informacji do konkurencji, gorsze warunki kontraktu, utratę prestiżu i wiarygodności, stratę klientów i kontrahentów),
- sankcje prawne,
- bałagan organizacyjny,
- ucieczkę wykwalifikowanej kadry,
- niewłaściwe decyzje.

Prawidłowo wdrożony i utrzymywany system zarządzania bezpieczeństwem SI pomaga każdej organizacji w codziennym funkcjonowaniu, dbałości o interesy właścicieli i klientów, spełnianiu misji i celów organizacji oraz pozostawaniu w zgodzie z wymaganiami prawa. Należy również podkreślić, że w szybko zmieniającym się świecie biznesu, sprawne zarządzanie bezpieczeństwem systemu informacyjnego staje się zadaniem krytycznym, od którego mogą zależeć losy organizacji, jej funkcjonowanie oraz wiarygodność.

4. Główna rola kultury organizacyjnej i sposobu zarządzania

Określone wzory myślenia i zachowania członków organizacji utrwalają się w postaci **kultury organizacyjnej**. Zainteresowanie kulturą organizacyjną pojawiło się w nauce o zarządzaniu już od czasu rozwoju kierunku *human relations*, podkreślającego znaczenie sposobów współdziałania ludzi dla sprawnego funkcjonowania organizacji. Znaczenie pojęcia kultury organizacyjnej wciąż jednak jest przedmiotem sporów i kontrowersji. E. Hall, znany badacz kultury, pisze o niej jako o systemie komunikacji międzyludzkiej (Hall 1987). Inny słynny badacz kultury, Edgar Schein przedstawia ją jako wielopoziomowy układ, podobny do góry lodowej. Niektóre „poziomy" są widoczne, można je zobaczyć gołym okiem, inne są głęboko zanurzone „w oceanie", trudno je zaobserwować i zrozumieć. J. Skalik pisze, iż w teorii organizacji i zarządzania kultura organizacyjna jest takim systemem wartości i norm, który wpływa na racjonalność działań [Krupski 2003, s. 399]. Rola kultury organizacyjnej polega na określeniu rodzajów powiązań między ludźmi w firmie, zdefiniowaniu ich ról i zobowiązań, ustanowieniu standardów postępowania, norm i wartości, popartych wiarygodnością kierownictwa. Kształt kultury organizacyjnej jest wynikiem m.in. stosunku pracowników do siebie, do przełożonych, do rozwiązań organizacyjno-technicznych czy też otoczenia instytucji. Do czynników wpływających na kulturę organizacyjną zalicza się m.in. [Krupski 2005, s. 274]:

- doświadczenia przeszłości kształtujące nawyki postępowania,
- obserwacje zachowania bezpośredniego zwierzchnika, styl przywódcy,

- przekonania, wartości, założenia i sposoby postępowania dyrekcji i zarządu organizacji,
- dominujący styl zarządzania,
- wartości, wierzenia i wzory zachowania składające się na kulturę narodową,
- konwencje, tradycje i praktyki związane z typem działalności organizacji,
- wartości przestrzegane i deklarowane przez jednostki oraz ich cechy osobowościowe.

Biorąc pod uwagę te elementy, można stwierdzić, iż kultura organizacyjna i sposób zarządzania przedsiębiorstwem w zasadniczy sposób wpływają na działanie organizacji, determinują jej członków, którzy dążą do osiągania zamierzonych efektów, są czynnikami, bez których nie mogłaby prawidłowo funkcjonować żadna organizacja, dlatego też odgrywają istotną rolę w procesach zarządzania bezpieczeństwem SI.

Poważnymi zagrożeniami dla systemu informacyjnego są świadome, szkodliwe działania wewnątrz organizacji, niedopatrzenia, błędy pracowników oraz powszechnie akceptowana kultura przedsiębiorstwa, dopuszczająca naruszanie istniejących rodzajów polityki, procedur, zasad i wartości związanych z bezpieczeństwem. Aby wyeliminować większość tych problemów, bezpieczeństwo systemu informacyjnego musi dla pracowników wyższego szczebla stać się integralnym elementem procesu zarządzania organizacją oraz podstawą kultury organizacyjnej. Zarząd i kierownictwo obiektu gospodarczego muszą postrzegać zarządzanie bezpieczeństwem SI jako jedno z podstawowych zadań. Takie podejście wyznacza i kreuje zachowania jednostek w organizacji, a tym samym zwiększa odporność firmy na zagrożenia. Duża część organizacji nie podejmuje jednak właściwych działań w celu zapewnienia bezpieczeństwa SI. Wynika to zarówno z błędnych inwestycji, jak i z błędów w egzekwowaniu wprowadzonych zasad działania. Ze wspomnianych już badań Ernst & Young z 2004 r. wynika, że jedynie niespełna 20% respondentów postrzega bezpieczeństwo systemów informacyjnych jako kwestię priorytetową na poziomie kierownictwa najwyższego szczebla (Ernst & Young 2004).

Żadne rozwiązanie techniczne nie zredukuje zagrożeń wynikających z cech ludzkiej osobowości, a każda strategia, która nie dostrzega tej zależności, jest skazana na porażkę. Właściwie przeszkoleni pracownicy mogą stać się najskuteczniejszym elementem strategii zarządzania bezpieczeństwem. Dlatego też pierwszym krokiem powinno być zapewnienie, że funkcjonują oni w odpowiedniej kulturze organizacyjnej, świadomej kwestii związanych z bezpieczeństwem. Największy wpływ na kierunek działań w zakresie bezpieczeństwa może wywierać kierownictwo wyższego szczebla, określając odpowiedzialność swoją oraz kierownictwa średniego szczebla. Dla różnych działów przedsiębiorstwa należy zdefiniować odpowiednie zakresy odpowiedzialności za zarządzanie bezpieczeństwem SI. Znane jest powiedzenie angielskie: If it is everybody's job, then it is nobody job (jeśli wszyscy za to odpowiadają, to nie odpowiada za to nikt) [Martinet, Marti 1999,

s. 257]. Brak widocznego zaangażowania ze strony kierownictwa wyższego szczebla uniemożliwia wykształcenie odpowiednich postaw wśród pracowników i zbudowanie odpowiedniej kultury organizacyjnej. Dzięki zaangażowaniu kierownictwa podejmowane działania obierają właściwy cel i kierunek, tym samym wzmacniając siłę organizacji [Ernst & Young 2004]. Wytworzenie kultury, w której ceni się bezpieczeństwo, opierającej się na świadomości każdej jednostki oraz poczuciu odpowiedzialności za własne poczynania, należy do zarządu przedsiębiorstwa [Scarlett 2002].

Tworzenie takiej kultury organizacyjnej stanowi wyzwanie i może zostać zrealizowane, jeśli kierownictwo wyższego szczebla będzie postępować zgodnie z tym, co samo głosi. Zdecydowany wpływ na kształtowanie wzorów kultury danej organizacji ma zatem kadra kierownicza, która ma za zadanie opracować politykę i strategię działania oraz procedury zarządzania. Kultura organizacyjna staje się narzędziem w ręku kadry menedżerskiej, która przez politykę personalną ma sposobność oddziaływania na uczestników organizacji w taki sposób, aby osiągnięte zostały cele organizacji – w tym przypadku cele związane z bezpieczeństwem jej systemu informacyjnego. Stosując odpowiednią politykę personalną, organizacja dobiera ludzi o określonych cechach. Z kolei działania i wypowiedzi menedżerów kształtują obraz organizacji w świadomości podwładnych, a to wpływa na ich zachowania i działania powiązane z bezpieczeństwem systemu informacyjnego.

O tym, jak ważnym czynnikiem w pomyślnej realizacji strategii firmy jest kultura organizacyjna, świadczą doświadczenia znanych światowych firm, które preferują silną kulturę zbiorową, a jednocześnie eksponują w niej szczególnie bliskie sobie wartości. W firmie Du Pont najważniejsze jest bezpieczeństwo i obowiązuje tam zasada, że raport na temat incydentu, wypadku musi znaleźć się na biurku szefa najpóźniej w ciągu 24 godzin [Krupski 2005, s. 412]. Podkreślić jednak należy, iż szybko zmieniające się warunki funkcjonowania przedsiębiorstw wymuszają konieczność tworzenia programów ciągłej zmiany kultury organizacyjnej, co oznacza kształtowanie kultury organizacyjnej inicjującej zmiany – kształtowanie kultury innowacyjnej, elastycznej, adaptacyjnej i efektywnej [Skalik 1997, s. 10-11]. W takiej sytuacji nabierają znaczenia znajomość technik nowoczesnego zarządzania, zorganizowane działania, a także zorganizowanie sprawnej funkcji personalnej.

Powyższą problematykę rozważać można w kontekście teorii katastrof, czyli nauki o ryzyku. Dostarcza ona metod analitycznych, które można zastosować w celu określenia wrażliwości organizacji na działania pracowników. W ramach tej teorii badane są niedobory organizacyjne mogące generować zagrożenia. Niedobory te, związane ze złą kulturą organizacyjną, mogą wiązać się z nadmiernym poczuciem przewagi nad konkurencją, czyli brakiem samokrytyki, zbytnią pewnością, niedostrzeganiem konsekwencji pewnych zagrożeń itp. Niedobory te wynikają ze złej kultury organizacyjnej, nieodpowiedniego sposobu zarządzania przedsiębiorstwem, braku wiedzy menedżerskiej. Można je podzielić na trzy zasadnicze kategorie:

- **kulturowe,**
- **organizacyjne,**
- **menedżerskie** [Martinet, Marti 1999, s. 211-213].

W tabeli 1 przedstawiono koncepcję M. Kervena, zaadaptowaną na potrzeby problematyki zarządzania bezpieczeństwem systemu informacyjnego.

Tworzenie kultury wyczulonej na ochronę prywatności, zachęcającej pracowników do etycznych postępowań i zniechęcającej ich do moralnie dwuznacznych sposobów wykorzystywania informacji, jest znakomitym działaniem profilaktycz-

Tabela 1. Niedobory kulturowe, organizacyjne i menedżerskie w aspekcie problematyki zarządzania bezpieczeństwem systemu informacyjnego

Określenie	Klasyczne symptomy
Niedobory kulturowe	
Kultura niezniszczalności	Nam porażka nie grozi. Nasi konkurenci nigdy nas nie prześcigną. Cokolwiek o nas wiedzą, jakiekolwiek informacje posiadają, nie może nam to zaszkodzić
Kultura prostoty	Zarządzanie bezpieczeństwem SI nie jest niczym trudnym. Wystarczy niewielka wiedza i kilka rozwiązań technicznych
Kultura braku komunikacji	Zawsze tak było i nie ma podstaw, aby to kwestionować. O sprawach technicznych nie ma co dyskutować. Między różnymi działami przedsiębiorstwa nie ma płynnej i sprawnej komunikacji
Kultura „w czubek własnego nosa"?	Dział X sprzeciwia się temu tylko dlatego, że propozycję zgłosił dział Y
Niedobory organizacyjne	
Podporządkowanie problematyki zarządzania bezpieczeństwem innym obszarom funkcjonowania przedsiębiorstwa (np. marketing).	Osoby odpowiedzialne za bezpieczeństwo SI i jego zarządzanie są służbowo podporządkowane kierownikom funkcjonalnym. Dla bezpieczeństwa SI nie tworzy się oddzielnych służb
Rozmywanie odpowiedzialności	Nikt nie określa funkcji i zadań związanych z zarządzaniem bezpieczeństwem systemu informacyjnego. Nie ma wyznaczonych osób za to odpowiedzialnych. Uważa się powszechnie, że ludzie są odpowiedzialni i znają swoje obowiązki zawodowe
Niedobory menedżerskie	
Brak systemu uczenia się z wykorzystaniem doświadczenia	Kontynuowanie praktyk innych przedsiębiorstw uważane jest za niepotrzebne. Nieprzywiązywanie wagi do sygnałów wcześniej pojawiających się w tej samej branży
Brak metod zabezpieczania SI	Brak odpowiednich podręczników, procedur, instrukcji, regulaminów, polityki
Brak programów kształcenia w zakresie bezpieczeństwa	Ludzie nieposiadający wystarczającej wiedzy popełniają niebezpieczne w skutkach błędy
Brak przewidywania sytuacji kryzysowych	W przypadku naruszenia poufności zasobów SI, ludzie wpadają w panikę i popełniają kolejne błędy

Źródło: [Martinet, Marti 1999, s. 211-212].

nym. Wspomniana kultura w połączeniu z rygorystycznym planem zapewniania bezpieczeństwa utrudni pracownikom podejmowanie działań niezgodnych z przyjętymi zasadami, pozostawiając przy tym kierownictwu dość dużą swobodę w egzekwowaniu tych zasad. Zawsze łatwiej pozwolić od czasu do czasu na wyjątek od twardej polityki niż na gwałt wdrażać rygorystyczne procedury w środowisku nie nastawionym na przestrzeganie wymogów [Ernst & Young 2004]. Budowanie zabezpieczeń na podstawie zasad etycznych, zrozumiałych i łatwych do zastosowania przez wszystkich pracowników świadczyć może o znakomitym podejściu menedżerskim [Holtzman 2003].

5. Zakończenie

Dokonując podsumowania rozważań zawartych w niniejszym artykule, stwierdzić można, iż bezpieczeństwo systemu informacyjnego powinno być przedmiotem sprawnego zarządzania. Istotne jest również systemowe myślenie o zarządzaniu bezpieczeństwem oraz zaangażowanie wszystkich pracowników, a szczególnie znajomość tej problematyki przez ścisłą kadrę kierowniczą. Wiąże się to bezpośrednio z koniecznością kształtowania kultury organizacyjnej nastawionej na ochronę poufnych zasobów informacyjnych przedsiębiorstwa. W artykule podkreślono, iż żadne rozwiązania techniczne i technologiczne nie zredukują zagrożeń wynikających z cech ludzkiej osobowości, a każda strategia, która nie dostrzega tej zależności, jest skazana na porażkę. Dlatego należy pamiętać, iż przeszkoleni pracownicy mogą stać się najskuteczniejszym elementem strategii zarządzania bezpieczeństwem. W związku z tym należy zapewnić, aby pracowali oni w odpowiedniej kulturze organizacyjnej, świadomej kwestii związanych z bezpieczeństwem systemu informacyjnego przedsiębiorstwa.

Literatura

Bezpieczeństwo systemów – SecurITy, „PC World Komputer Pro" 2003 nr 2, s. 68.

Białas A., *Zarządzanie bezpieczeństwem informacji*, [w:] *Bezpieczeństwo systemów komputerowych*, red. A. Grzywak, Wydawnictwo Pracowni Komputerowej Jacka Skalmierskiego, Gliwice 2000.

Białas A., *Zarządzanie bezpieczeństwem informacji*, „Networld" 01.03.2001.

Bryl J., *Bezpieczeństwo systemów e-Commerce*, „Gazeta IT" nr 3(33) z dn. 14 marca 2005.

Drążek Z., Niemczynowicz B., *Zarządzanie strategiczne przedsiębiorstwem*, Polskie Wydawnictwo Ekonomiczne, Warszawa 2003.

Ernst & Young – *Światowe badanie dotyczące Bezpieczeństwa Informacji 2004 – wyniki światowe*, http://www.ey.com/GLOBAL/content.nsf/Poland/TSRS_-_Library_-_GISS_2004.

Ernst & Young – *Światowe Badanie dotyczące Bezpieczeństwa Informacji 2004 – wyniki dotyczące Polski*, http://www.ey.com/GLOBAL/content.nsf/Poland/TSRS_-_Library_-_GISS_2004.

Grzywacz J. (red.), *Bezpieczeństwo systemów informatycznych w bankach w Polsce*, Oficyna Wydawnicza SGH w Warszawie, Warszawa 2003.

Hall E., *Bezgłośny język*, Państwowy Instytut Wydawniczy, Warszawa 1987.

Hammer M., Champy J., *Reengineering the Corporation*, Nicholas Brealey Publishing, London 1995.

Holtzman D.A., *Bezpiecznie, bo etycznie*, CXO – Magazyn kadry zarządzającej z dn. 03.03.2003.
Jelonek D., *Wybrane aspekty polityki bezpieczeństwa informacji w e-przedsiębiorstwie*, www.it-investment.pl/upload/plik-42.doc.
Krupski R. (red.), *Zarządzanie przedsiębiorstwem w turbulentnym otoczeniu*, Polskie Wydawnictwo Ekonomiczne, Warszawa 2005.
Krupski R. (red.), *Zarządzanie strategiczne. Koncepcje – metody*, AE, Wrocław 2003.
Martinet B., Marti Y.B., *Wywiad gospodarczy. Pozyskiwanie i ochrona informacji*, Polskie Wydawnictwo Ekonomiczne, Warszawa 1999.
Niemiec A., *Zarządzanie bezpieczeństwem informacji w świetle norm ISO*, http://www.prim.com.pl/referaty/wdrazanie_iso17799.htm (08-12-2003).
Scarlett S.D., *Biosfera niepewności*, CXO – Magazyn kadry zarządzającej z dn. 02.09.2002.
Senge P.M., *Piąta dyscyplina. Teoria i praktyka organizacji uczących się*, Dom Wydawniczy ABC, Warszawa 1998.
Skalik J. (red.), *Projektowanie organizacji instytucji*, AE, Wrocław 1998.
Skalik J., *Współczesne kierunki i formy zmian w organizacjach dynamicznych*, Prace Naukowe Akademii Ekonomicznej nr 779, AE, Wrocław 1997.
Szafrański M., *Zmowa milczenia*, Raport Computerworld – *Bezpieczeństwo* z dn. 9 kwietnia 2001 r.
Wajda K., *Wpływ systemów informacyjnych na rozwój przedsiębiorstwa*, [w:] *Zarządzanie firmą w społeczeństwie informacyjnym*, red. A. Stabryła, AE, Kraków 2002.
Wawrzyniak D., *Zarządzanie bezpieczeństwem systemów informatycznych w bankowości*, AE, Wrocław 2002.

THE ROLE OF ORGANIZATIONAL CULTURE IN THE MANAGEMENT OF INFORMATION SYSTEM SECURITY OF ENTERPRISE

Summary

The rapid progress in the area of information technology brings new threats of information disclosure. The subject of IS/IT security has become very significant. Every organization has to apply adequate methods, tools and organizational requirements to protect its information resources.

The technical safeguard is not any more enough protection. It is necessary to choose different tools and methods of protection and finally to manage them in a proper way. The information system security management has to be examined not only in technological aspects, but also in social, organizational, economical and legal. It should be undertaken by interdisciplinary team of specialists. So it is necessary to take into consideration not only technological area of IS security management, but also organizational problems, especially connected with organizational culture in the enterprise.

The article presents the essence and the importance of the information system security management. Its aim is also to show the meaning of the organizational culture and its role for information system security. The authors pointed out in the paper that the process of IS security management is closely connected with the organization management and that it should be the element of business and IT strategy.

Adam Nowicki – prof. dr hab., kierownik Katedry Inżynierii Systemów Informatycznych Zarządzania Akademii Ekonomicznej we Wrocławiu.

Artur Rot – dr, asystent w Katedrze Inżynierii Systemów Informatycznych Zarządzania Akademii Ekonomicznej we Wrocławiu.