ZESZYTY NAUKOWE UNIWERSYTETU SZCZECIŃSKIEGO

NR 476 STUDIA INFORMATICA NR 21 2007

MAREK MAZUR

POLITYKA BEZPIECZEŃSTWA SYSTEMÓW INFORMATYCZNYCH

Wstęp

Wraz z rozwojem zastosowań informatyki wzrasta zainteresowanie bezpieczeństwem systemów informatycznych, które stały się istotnym atutem w działaniu współczesnych organizacji, ale jednocześnie muszą być traktowane jako czynnik ryzyka. Problematyka bezpieczeństwa ma tu charakter interdyscyplinarny. Wiąże się z identyfikacją czynników zagrażających systemom informatycznym i oceną ich oddziaływania na organizacje. Zapewnienie bezpieczeństwa zależy od wielu przedsięwzięć podejmowanych przez różne jednostki organizacyjne i szczeble kierowania oraz podmiotów działających w otoczeniu. Coraz częściej osiągnięcie celów przez poszczególne organizacje będzie uzależniona od opracowania i realizacji założeń polityki bezpieczeństwa, czyli w wymiarze technicznym, kosztowym, finansowym, prawnym, społecznym, zatem wręcz w wymiarze cywilizacyjnym.

Celem artukułu jest wskazanie, jak ważne miejsce zajmują zagadnienia związane ze środowiskiem technicznym, informatyczną infrastrukturą, systemem zarządzania, finansami, ekonomiką przedsiębiorstwa, otoczeniem prawnym i społecznym, zapewniające skuteczne i racjonalne włącznie problematyki bezpieczeństwa do systemu zarządzania. Dobór i przygotowanie metod i środków powinny być w znacznej mierze ukierunkowane na kadrę, która realizuje różne zadania związane z polityką bezpieczeństwa, a tym samym może budzić zainteresowanie pomiotów atakujących systemy informatyczne. Punktem wyjścia jest ustalenie istoty polityki bezpieczeństwa systemów informatycznych i jej miejsca w systemie zarządzania.

1. Istota polityki bezpieczeństwa systemów informatycznych

Polityka jest pojęciem wieloznacznym. Pojawia się w różnych kontekstach związanych z kierowaniem organizacjami. W ogólnym znaczeniu dotyczy stosowania metod i zasad prowadzących do osiągnięcia określonych celów organizacji. W aspekcie podmiotowym ma zastosowanie w działalności wielkich organizacji, ale również przedsiębiorstw i instytucji. Oczywiście, nie można pominąć struktur tworzonych z różnych organizacji osiągających wspólne cele, czyli grup organizacji. Termin polityka jest stosowany również w aspekcie rodzaju działalności, a za przykład może posłużyć polityka rachunkowości lub polityka finansowa. Wspólną cechą różnych określeń, w których użyto terminu polityka, jest długookresowy charakter i związek ze strategią działania. Pojęcie polityka występuje zarówno w nazwach dyscyplin naukowych, jak i w obszarze praktyki społecznej.

W skali makro przykładem zastosowania omawianego terminu może być polityka ekonomiczna państwa, a w skali mikro znaczenie tej problematyki dobrze ilustruje polityka rachunkowości podmiotu gospodarczego. Przykładem zastosowania o charakterze pośrednim są natomiast opracowywane przypadki zasad realizacji celów przez różne organizacje terytorialne, społeczne lub skupiające grupy organizacji.

Przykładem dyscypliny naukowej jest nauka polityki ekonomicznej (lub teorii polityki ekonomicznej) zajmująca się badaniem celów, form, narzędzi i sposobów oddziaływania państwa na proces gospodarczy[1]. Nie rozważając złożonej problematyki polityki ekonomicznej państwa w gospodarce rynkowej, należy podkreślić, że od polityki w znacznym stopniu zależą warunki i możliwości działania podmiotów gospodarczych, których podstawowym celem jest zapewnienie sobie egzystencji i wzrostu wartości rynkowej firmy[2]. Nauka polityki ekonomicznej bada oddziaływanie organów kierowniczych, tutaj państwowych, na określony obszar działalności, w tym przypadku, gospodarkę narodową. Tworzy podstawy do przygotowania strategii, planów i sterowania procesami gospodarczymi i oceny realizacji przyjętych celów. Uprawiana jest w złożonych warunkach cywilizacyjno-rozwojowych, wyzwań rozwojowych, przed którymi stoją

[1] *Polityka gospodarcza*. Red. B. Winiarski. PWN, Warszawa 1999, s. 19.

[2] K. Sawicki: *Polityka bilansowa jako narzędzie zarządzania firmą*. W: *Polityka bilansowa i analiza finansowa. Nowoczesne instrumenty zarządzania firmą*. Red. *idem*. Ekspert, Wrocław 2001, s. 17.

współczesne społeczeństwa gospodarujące[3]. Aby polityka ekonomiczna osiągnęła cele, musi być dostosowana do istniejących realiów. Jest ważnym instrumentem realizacji szerokiego zakresu celów zorganizowanego społeczeństwa.

Aby oddziaływanie państwa w gospodarce było skuteczne, musi się opierać na wykorzystywaniu pewnych praw, wskazaniu zasad doboru środków właściwych do osiągania zamierzonych celów i metod posługiwania się tymi środkami pod kątem przyjętych celów[4].

Odpowiednikiem polityki ekonomicznej państwa na szczeblu mikroekonomicznym jest polityka przedsiębiorstwa. Polega ona na ustalaniu celów podmiotu gospodarującego i sposobów jego osiągnięcia. Polityka przedsiębiorstwa ma odzwierciedlenie we wdrażanej strategii. Tym samym osiągnięcie długookresowych celów jest uzależnione od odpowiedniego opracowania planów, przygotowania sposobów ich realizacji, koordynacji i oceny z zastosowaniem dostępnych instrumentów i metod, a także od powołania organów sprawujących nadzór.

W uzupełnieniu należy zwrócić uwagę na wiele przedsięwzięć podejmowanych przez instytucje międzynarodowe, które realizują liczne zadania zaliczane do polityki ekonomicznej. Wyznaczane są tu określone cele ekonomiczne i społeczne, dobierane środki ich realizacji, opracowywane systemy koordynacji i kontroli. We współczesnym świecie warunki działania organizacji zależą nie tylko od uwarunkowań wewnętrznych, najbliższego otoczenia, ale również od założeń przyjętych przez organa państwa, instytucje międzynarodowe i organizacje ponadnarodowe.

Przedstawione niektóre właściwości długookresowego regulowania zasad realizacji celów przez prowadzenie odpowiedniej polityki w danej dziedzinie mogą być zaadaptowane do potrzeb właściwego i pełniejszego omówienia zagadnień polityki bezpieczeństwa systemów informatycznych.

Polityka bezpieczeństwa systemów informatycznych to ważna część szeroko rozumianej polityki w zakresie informatyki, którą w skrócie można nazwać polityką informatyki. Przez politykę informatyki należy rozumieć sferę działalności różnych organizacji międzynarodowych, krajowych, w tym organów państwowych i organizacji społeczno-zawodowych oraz organów kierowniczych poszczególnych organizacji, polegającą na opracowaniu zasad korzystania z dóbr informatycznych oraz inicjowaniu i realizowaniu przedsięwzięć zmierzających do włączenia sfery informatycznej w proces rozwoju społeczno-gospodarczego

[3] J. Stacewicz: *Polityka gospodarcza*. SGH, Warszawa 1998, s. 5.

[4] *Polityka gospodarcza*..., s. 20.

i cywilizacyjnego. Polityka informatyki wiąże się z przygotowywaniem wielu norm, standardów i rozwiązań w prawie międzynarodowym i systemach prawnych poszczególnych krajów. W pojedynczych organizacjach, na przykład przedsiębiorstwach lub instytucjach, jest połączona ze sferą strategiczną. Zagadnienia te są wyzwaniem dla wszystkich form organizacji społeczeństwa. Widoczny jest związek bezpieczeństwa systemów informatycznych poszczególnych organizacji z działalnością ogromnej liczby podmiotów.

J. Kisielnicki i H. Sroka twierdzą, że jeśli system informacyjny zarządzania jest po to, aby organizacja mogła osiągać określone cele, to system musi spełniać wiele kryteriów, a do podstawowych zalicza się bezpieczeństwo[5]. Bezpieczeństwo systemów informatycznych odgrywa coraz większą rolę wraz z rozwojem zastosowań informatyki i postępującą globalizacją.

Bezpieczeństwo systemów informatycznych jest determinowane przez ogół środków, metod, warunków, przedsięwzięć i rozwiązań przeznaczonych do rozpoznawania zagrożeń, eliminowania ich oraz usuwania lub minimalizowania skutków związanych z negatywnym oddziaływaniem na składniki, procesy i rozwój systemów informatycznych, realizację celów organizacji i podmiotów działających w jej otoczeniu. Ma być realną gwarancją właściwej realizacji celów wobec ryzyka występowania różnych niekorzystnych zjawisk wywierających wpływ na systemy informatyczne. Realizacja zależy od sprawności zarządzania, rozwiązań organizacyjnych, technicznych, prawnych i instytucjonalnych. Zakres oddziaływania wiąże się z ryzykiem, które zależy między innymi od oddziaływania organizacji, warunków wewnętrznych i zewnętrznych, dostępnych technologii, atrakcyjności zasobów informacyjnych i wiedzy zgromadzonych w systemie informatycznym.

Na bezpieczeństwo ogromny wpływ ma globalizacja i czynniki, które jej sprzyjają.

Najczęściej się uważa, że dążenie do globalizacji ułatwione zostało przez: trzy czynniki:

- zaawansowana sieć telekomunikacyjna, a zwłaszcza Internet,
- regionalne porozumienia o wolnym handlu,

[5] J. Kisielnicki, H. Sroka: *Systemy informacyjne biznesu. Informatyka dla zarządzania*. Placet, Warszawa 2005.

– zniesienie lub ograniczenie barier handlowych uzasadnionych względami politycznymi, co pozwoliło na stosunkowo swobodny przepływ towarów, produktów i usług na całym świecie[6].

Na skutek globalizacji systemów informatycznych, a w szczególności z powodu rozwoju sieci komputerowych, można prowadzić działalność praktycznie z dowolnego miejsca. Stale rosnąca liczba użytkowników Internetu, upowszechnienie zastosowań informatyki i ich oddziaływanie na wszystkie sfery życia społeczeństwa to kolejne przesłanki wzrostu zainteresowania bezpieczeństwem systemów informatycznych.

Problematykę bezpieczeństwa i polityki bezpieczeństwa wobec systemów informacyjnych czy węższym zakresie – systemów informatycznych, najczęściej się rozpatruje z punktu widzenia wybranych aspektów. Niewątpliwie wpływ na to ma podejście do zakresu zarządzania systemem informacyjnym.

P. Beynon-Davies za M. Earlrem wyróżnia, trzy poziomy zarządzania odnoszące się do systemów informacyjnych: zarządzanie systemami informacyjnymi, technologią informacyjną, zarządzanie informacją[7]. Priorytet ma zarządzanie informacją, za które ma odpowiadać przede wszystkim kierownictwo strategiczne. Zarządzanie to jest wiązane z całościowym rozwojem organizacji, a w którym duży udział mają planowanie i koordynacja. Chodzi tu o przypisywanie w systemach informacyjnych, oczywiście również wspomaganych komputerowo, kluczowej roli informacji, będącej głównym efektem działania tego typu systemów.

2. Polityka bezpieczeństwa informacji

Sposób formułowania podstawowych zagadnień w ramach polityki bezpieczeństwa informacji może posłużyć do ogólnej charakterystyki dotychczasowego podejścia do polityki bezpieczeństwa systemów informatycznego i wskazania pełniejszego obrazu tych zagadnień.

D.L. Pipkin słusznie stwierdza, że instytucje powinny wprowadzić efektywne środki bezpieczeństwa, które zapewnia ochronę informacji posiadanej przez firmę, ciągłą dostępność systemów podtrzymujących krytyczne funkcje oraz odpowiednie mechanizmy zabezpieczenia informacji przed jej rozmyślnym

[6] *Zarządzanie wartością przedsiębiorstwa a alokacja kapitału*. Red. J. Bielinski. CeDeWu, Warszawa 2004, s. 291.

[7] P. Beynon-Davies: *Inżynieria systemów informacyjnych*. WNT, Warszawa 1999, s. 59.

lub przypadkowym ujawnieniem, manipulacją, modyfikacją, zniszczeniem lub skopiowaniem[8].

We współczesnym przedsiębiorstwie zarządzanie informacją jest odpowiedzią na dynamiczne zmiany w otoczeniu i ogromnej roli informacji. Według P. Sienkiewicza, do najważniejszych zagadnień zarządzania informacjami w firmie należy zaliczyć:

a) opracowanie i wdrażanie racjonalnych strategii informacyjnych jako określonej polityki informacyjnej firmy;
b) sterowanie przepływem informacji w sieci komunikacyjnej firmy;
c) zapewnienie efektywnej eksploatacji systemów informatycznych;
d) zarządzanie jakością informacji, czyli tworzenie warunków do maksymalizacji pełności (kompletności), wiarygodności (niezawodności) i aktualności (terminowości) informacji wykorzystywanych przez kierownictwo firmy;
e) stworzenie bezpieczeństwa informacyjnego firmy (ochrony zasobów informacyjnych);
f) konserwację systemów informacyjnych;
g) rozwój systemów informacyjnych, czyli racjonalne planowanie środków inwestycyjnych na projektowanie i wdrażanie środków informatyki;
h) zapewnienie pożądanego rozwoju kadr informacyjnych i użytkowników systemów informacyjnych;
i) tworzenie warunków do zapewnienie efektywnych związków firmy z rynkiem informacyjnym;
j) zapewnienie integracji systemów informacyjnych wykorzystywanych na różnych szczeblach zarządzania i w różnych podsystemach funkcjonalnych.

Zaprezentowany wykaz zagadnienia jest rozbudowany w aspekcie tematycznym, uwzględnia działania ukierunkowane nie tylko na sam podmiot gospodarczy, ale również na jego otoczenie. Ważne miejsce zajmuje w nim sprawa bezpieczeństwa informacyjnego. Główną rolę przypisano ochronie zasobów informacyjnych, które mogą być dobrem pozyskiwanym nawet niedozwolonymi metodami. Informacja jest traktowana jako największe dobro organizacji, wymagające właściwego zarządzania, w tym ochrony.

[8] D.L. Pipkin: *Bezpieczeństwo informacji. Ochrona globalnego przedsiębiorstwa*. WNT, Warszawa 2002, s. 13.

Systemy informatyczne są środowiskiem w którym to dobro jest gromadzone, utrzymywane i udostępniane użytkownikom. Realizacja celów organizacji zależy więc od struktury, funkcjonowania i rozwoju systemów o bardzo złożonej strukturze, wykonujących swoje zadania z dużą szybkością i wymagających coraz większych nakładów finansowych. Konieczność korzystania w coraz większym stopniu z komunikacji przez sieci telekomunikacyjne i komputerowe sprawia, że organizacje przygotowują kanały połączeń z otoczeniem. W ten sposób systemy informatyczne stają się środowiskiem poważnie zagrożonym atakami, co może niekorzystnie oddziaływać na całą organizację.

3. Wybrane propozycje w zakresie polityki bezpieczeństwa systemów informatycznych

Bezpieczeństwo systemów informatycznych zależące od wielu czynników, powinno być jednym z najważniejszych zadań dla kierownictwa organizacji.

T. Kifner na przykład stwierdza, że system bezpieczeństwa i ochrony informacji w przedsiębiorstwie to zestaw praw i reguł opisanych w formie zaleceń i procedur określających, w jaki sposób „wrażliwa" informacja jest zarządzana, zabezpieczana w przedsiębiorstwie, dystrybuowana między jednostkami przedsiębiorstwami i innymi kontrahentami. Wraz z ze wzrostem złożoności warunków działania należy tę problematykę przygotować pod kątem metodycznym. Wymagane jest wieloaspektowe podejście i odwołanie się do różnych dyscyplin.

Polityka jest przemyślanym sposobem postępowania, zbiorem praw, reguł i wskazówek opisujących sposób działania organizacji i kierowania[9]. Od polityki zależą warunki działania i szanse realizacji celów. Odnosi się to również do przygotowania warunków do bezpiecznej realizacji celów systemów informatycznych. Takie podejście wymaga określenia:

a) miejsca bezpieczeństwa systemów informatycznych w informatyce, zakresu integracji z innymi dziedzinami, na przykład z prawem i systemem prawa,
b) aspektów organizacyjnych,
c) miejsca w polityce organizacji i kierowaniu organizacjami, a zwłaszcza w zarządzaniu przedsiębiorstwem,
d) koncepcji zasad, narzędzi i metod.

[9] Por. T. Kifner: *Polityka bezpieczeństwa i ochrony informacji*. Wyd. Helion, Gliwice 1999, s. 18.

Polityka bezpieczeństwa jest ważną częścią szeroko rozumianej polityki wobec informatyki, którą w skrócie można nazwać polityką informatyki. Politykę tę należy włączyć do problemów badawczych informatyki. Jest to uzasadnione tym, że w obszarze badawczym powinny być realizowane podstawowe funkcje:

- opisowa (empiryczna),
- wyjaśniająca (eksplikacyjna),
- prognostyczna (przewidująca).

Polityka zajmuje się obserwacją zjawisk, ustalaniem (poszukiwaniem) prawidłowości, formułowaniem wskazań praktycznych i określeniem środków ich realizacji. W ten sposób oprócz teorii informatyki (informatyki teoretycznej) i informatyki stosowanej pojawi się jeszcze jeden obszar dociekań naukowych i działalności praktycznej, który podobnie jak w innych dyscyplinach ma szansę się przekształcić w określonych warunkach w osobną dziedzinę. Teoria informatyki i informatyka stosowana odgrywają ważną rolę w ustalaniu zasad i metod realizacji polityki w różnych obszarach, w tym także w polityce bezpieczeństwa systemów informatycznych. Szczególnym jej przejawem są liczne krajowe i międzynarodowe regulacje prawne dotyczące badań i zastosowań z zakresu informatyki. Przygotowywane są różnego rodzaju standardy w obszarze informatyki i telekomunikacji, zasady ochrony praw autorskich, zasobów informacyjnych, na przykład danych osobowych, integralności danych, baz danych, działania komputerów, wykrywania i zwalczania przestępczości komputerowej itd.

Polityka zajmuje się obserwacją zjawisk, ustalaniem (poszukiwaniem) prawidłowości, formułowaniem wskazań praktycznych i określeniem środków ich realizacji. Polityka bezpieczeństwa systemów informatycznych wymaga uwzględnienia aspektów strukturalnych, funkcjonalnych i rozwoju systemu informatycznego. Umożliwia to ochronę poszczególnych składników systemu, procesów realizowanych w nim i wspomaganych przez system informatyczny. Oczekiwanych korzyści nie osiągnie się wówczas, gdy zagadnienia te nie będą rozpatrywane w dłuższym okresie i z uwzględnieniem roli, jaką odgrywa system w rozwoju całej organizacji. W ten sposób można zapewnić ochronę zgromadzonym zasobom, procesom informacyjnym, pracy komputerów, a także zwiększyć skuteczność działania całej organizacji.

Wraz ze wzrostem złożoności środowiska działania organizacji będą one coraz bardziej zainteresowane przygotowaniem zasad zapewniających bezpieczeństwo systemom informatycznym w ramach ich ogólnej polityki i włączenia w obszar kierowania organizacjami, a zwłaszcza z uwzględnieniem w zarządza-

niu przedsiębiorstwem lub instytucjami. Wymagają tego ogólne zasady działania podmiotów społeczno-gospodarczych zainteresowanych efektywnością, zmniejszaniem niepewności i ograniczaniem ryzyka. Efektywność i ryzyko są obecnie głównymi kryteriami decyzji inwestycyjnych. Przygotowanie rozwiązań zapewniających bezpieczną eksploatację informatycznej infrastruktury to ważne zadanie organów kierowniczych w państwie. Uzasadnione jest też oczekiwanie odpowiednich rozwiązań w strukturach terenowych, w tym w organach samorządowych. Wraz z rozszerzaniem zakresu komunikacji między obywatelami naszego państwa a licznymi jednostkami administracji problem ten nabiera ogromnej wagi. Nie można go ograniczać jedynie do wdrożenia systemu podpisu elektronicznego. W praktyce dobrze można zidentyfikować i realizować zadania budowy systemu bezpieczeństwa w przedsiębiorstwach, które są zdane na własne siły i ponoszą ryzyko na własny rachunek. Oczywiście, ponoszą też odpowiedzialność za oddziaływanie własnych systemów informatycznych na inne podmioty.

Koncepcje zasad, narzędzi i metod zależą od typu organizacji przygotowującej i prowadzącej politykę bezpieczeństwa systemów informatycznych. W zależności od typu organizacji będą dobierane środki, metody, zakres oddziaływania, zasięg czasowy, podmioty podlegające regulacjom.

Głównymi formami oddziaływania stosowanymi przez organizacje międzynarodowe jest opracowywanie norm prawnych, standardów, przygotowywanie zaleceń, systemów kontroli, powoływanie instytucji prowadzących kontrolę i propagujących właściwe korzystanie z informatycznej infrastruktury. Ważna jest budowa systemu ścigania przestępstw komputerowych. Działalność ma tu zasięg światowy, jest bowiem w dużej mierze nastawiona na inspirowanie działań organów poszczególnych państw. Światowy zasięg mają także różne jednostki zwalczające piractwo komputerowe.

Organa państwowe mają znacznie większy bezpośredni udział, przygotowują bowiem odpowiednie rozwiązania w systemie prawa, powołują instytucje bezpośrednio lub pośrednio stające na straży bezpieczeństwa zastosowań informatyki. Przykładem jest Generalny Inspektor Ochrony Danych Osobowych, instytucja, która włącza problematykę ochrony systemów informatycznych, w tym dóbr w nich zgromadzonych, w wymiar sprawiedliwości.

Polityka bezpieczeństwa systemów informatycznych, o czym już wspomniano, jest integralną częścią problematyki zarządzania poszczególnych organizacji. Ma decydujący wpływ na warunki funkcjonowania przedsiębiorstw i instytucji. Oddziałuje na warunki podejmowania decyzji, ryzyko działalności,

a w konsekwencji na sytuację ekonomiczno-finansową, pozycję na rynku, i to w długich okresach.

Polityka bezpieczeństwa ma ścisły związek z działalnością osób, które w licznych przypadkach przez sieci komputerowe, zwłaszcza przez Internet, kontaktują się z handlowcami, administracją publiczną, bankami, instytucjami kulturalnymi i wieloma innymi podmiotami. Jako użytkownicy systemów informatycznych są zainteresowani bezpiecznym załatwieniem swoich spraw. Przez administratorów systemów, których są użytkownikami, są jednak postrzegani jako potencjalne źródło świadomego lub nieświadomego zagrożenia.

4. Ogólne założenia polityki bezpieczeństwa systemu informatycznego w organizacji

Na podstawie metod i teorii opracowanych przez różne dyscypliny poszczególne organizacje uzyskują wsparcie w tworzeniu warunków do zapewnienia bezpieczeństwa systemom informacyjnym. Poszczególne podmioty zawsze będą brać pod uwagę warunki, w których działają. Dla obecnej fazy rozwoju społeczeństwa charakterystyczne jest to, że megatrendy cywilizacyjne mają charakter globalny[10]. Opracowanie założeń i prowadzenie polityki bezpieczeństwa systemów informatycznych jest więc problematyką bardzo złożoną.

Do podstawowych zagadnień polityki bezpieczeństwa systemów informatycznych w organizacjach należy zaliczyć:

a) badanie roli organizacji w kształtowaniu polityki bezpieczeństwa systemów informatycznych, identyfikacje głównych obszarów, ustalenie podmiotów oddziałujących na działanie tych systemów;
b) włączanie strategii bezpieczeństwa systemów informatycznych do strategii organizacji, analizowanie oddziaływania zastosowań informatyki na rozwój organizacji, jej sytuację w otoczeniu, a w przypadku przedsiębiorstw – na pozycję na rynku, ryzyko działalności i sytuację ekonomiczno-finansową, warunki pracy, stosunki międzyludzkie itp.;
c) przygotowywanie koncepcji, metod i narzędzi zapewniających bezpieczeństwo systemom informatycznym;
d) wdrażanie metod i środków umożliwiających identyfikację zagrożeń, analizę ryzyka i przeciwdziałanie tym zagrożeniom;

[10] J. Stacewicz: *op.cit.*, s. 5.

e) śledzenie warunków formułowanych w systemie prawa, przygotowywanie i wdrażanie odpowiednich zmian w systemach informatycznych i ich otoczeniu;
f) wdrażanie standardów wpływających na jakość systemów informatycznych;
g) zapewnienie racjonalności w sferze bezpieczeństwa, między innymi przez dobór metod, środków i działań stosownie do skali zagrożeń;
h) opracowanie zasad zarządzania jakością zasobów gromadzonych i udostępnianych przez systemy informatyczne, a także realizowanych przez nie procesów;
i) przygotowywanie odpowiednich rozwiązań w systemie zarządzania w ramach planowania, kontroli, organizacji, motywacji do przestrzegania przyjętych zasad przez poszczególnych pracowników, między innymi przez właściwe sprawowanie funkcji koordynacyjno-przywódczej przez kierownictwo.

Efekty uzyskiwane dzięki systemom komputerowym zależą od zapewnienia stabilnej pracy urządzeń technicznych, postawy kadry, skutecznej ochrony zasobów informacyjnych, w szczególności danych i oprogramowania, poziomu bezpieczeństwa procesów informacyjnych, stopnia zorganizowania systemu informacyjnego i sprawności systemu zarządzania systemem informatycznym.

Każda firma powinna opracować własną politykę, która pomoże uczestnikom organizacji w realizowaniu wybranej strategii[11]. Strategia bezpieczeństwa systemów informatycznych organizacji w aspekcie czasowym wiąże bieżącą działalność ze stanami oczekiwanymi w przyszłości wyznaczonymi przez kierunki rozwoju. Problematykę tę należy widzieć w połączeniu z ogólną strategią przedsiębiorstwa lub instytucji. Znaczenie polityki bezpieczeństwa systemów informatycznych zależy od skali zastosowania informatyki oraz jej wpływu na działalność organizacji i różnorodności zagrażających im czynników. Współcześnie systemom informatycznym zagraża wiele czynników. Aby je zidentyfikować, należy przygotować zasady pogrupowania. W podziałach zagrożeń najczęściej bierze się pod uwagę następujące kryteria:

a) źródła pochodzenia czynników – spoza systemu lub związane z systemem;

[11] *Zarządzanie. Teoria i praktyka*. Red. A. Koźmiński, W. Piotrowski. PWN, Warszawa 1999, s. 169.

b) przyczyny powstania – wynik celowej działalności ludzi lub przypadkowej zjawiska (losowe);
c) rodzaje składników systemu informacyjnego narażonych na czynniki destrukcyjne – dane, programy i informacja o organizacji systemu;
d) rodzaj czynników, będących zagrożeniem dla danych i systemów informacyjnych – techniczne, programowe, kadrowe;
e) skala zagrożenia – niewielka, prawie niezauważalna, istotna, wyraźne zakłócenie działania systemów komputerowych ze skutkami odczuwalnymi w systemie informacyjnym i działalności podmiotu wspomaganego informatycznie, a nawet zagrażającymi jego żywotnym interesom społeczno-gospodarczym[12].

Z powodu ogromnego zróżnicowania czynników zagrażających danym, samym systemom komputerowym i wspomaganym komputerowo systemom informacyjnym należy podjąć przeciwdziałanie przez dobór i zastosowanie środków oraz metod zgodnie z charakterem tych czynników. Doskonaleniem metod ochrony systemów informatycznych zajmuje się wielu instytucji badawczych i organizacji prowadzących różne zadania w praktyce społecznej i informatyzacji. Praktyka i badania naukowe kształtowania informatyzacji we współczesnej organizacji wyróżniają cztery istotne kwestie: środowisko, proces, forma i treść oraz efekty strategii informacji[13].

Polityka bezpieczeństwa systemów informatycznych powinna obejmować różne metody, dostosowane do rozdziału systemów, podatności na zakłócenia działania w danym środowisku i atrakcyjności zgromadzonych w nich zasobów. Swoboda podejmowania przedsięwzięć jest uzależniona od dostępności środków finansowych. Brak środków jest zbyt często używanym argumentem za nieprowadzeniem polityki bezpieczeństwa. Ochronę zapewniają między innymi środki techniczne i organizacyjno-administracyjne ściśle związane z zarządzaniem, szyfrowaniem oraz programowaniem. Ogromne znaczenie mają także rozwiązania przyjęte w prawie krajowym i międzynarodowym.

W polityce bezpieczeństwa systemów informatycznych trzeba podjąć próbę ustalenia podstawowych zasad, a wśród nich między innymi:

a) włączania polityki bezpieczeństwa do ogółu zagadnień zarządzania organizacją, ustalania celów i zadań priorytetowych, opracowywania od-

[12] M. Mazur: *Bezpieczeństwo danych i systemów*. W: *Wstęp do informatyki w zarządzaniu*. Red. E. Kolbusz, I. Rejer. Uniwersytet Szczeciński, Szczecin 2006, s. 288.

[13] M. Pańkowska: *Zarządzanie zasobami informatycznymi*. Difin, Warszawa 2001, s. 37.

powiednich planów, właściwego podziału obowiązków, systematycznej kontroli;
b) ciągłości uaktualniania i realizacji;
c) adekwatności zakresu polityki i nakładów do ryzyka;
d) różnorodności różnych sposobów i metod;
e) dokumentowanie założeń polityki i zjawisk, które występują w trakcie jej realizacji (na przykład prób włamań i włamań do systemów informatycznych);
f) dążenia do zapewnienia najwyższej jakości funkcjonowania, struktury, rozwoju i efektów działania systemów informatycznych, a w szczególności danych, informacji i wiedzy;
g) legalności stosowanych rozwiązań;
h) integracji rozwiązań technicznych, technologicznych, szyfrowania, metod programowych, zarządczych;
i) stosowania podejścia wyprzedzającego ewentualne pojawienie się zagrożeń (antycypacyjna rola polityki).

Zaproponowana lista zasad nie jest wyczerpująca, jednak wskazuje na wiele istotnych zagadnień. Konieczne są badania tej problematyki. Stosownie do zagrożeń w organizacjach powinna nawiązywać współpraca między różnymi jednostkami i komórkami organizacyjnymi. Wiele zamierzeń powinno być ukierunkowanych na kadrę, jej wiedzę, umiejętności, odporność na szpiegostwo przemysłowe i wywiad gospodarczy.

Zakończenie

Systemy informatyczne mogą być poważnym źródłem zagrożenia dla każdej organizacji. Przeciwdziałanie im i usuwanie ich skutków wymaga prowadzenia odpowiedniej polityki bezpieczeństwa przez wiele podmiotów. Ma ona swój wymiar międzynarodowy z powodu coraz liczniejszych uregulowań prawnych i standardów technologicznych. Pod względem tematycznym polityka bezpieczeństwa skupia się na wypracowywaniu zasad, ustalaniu czynników, które należy neutralizować, doborze metod zapewniających bezpieczne funkcjonowanie i rozwój zastosowań informatycznych. Ogół przedstawionych zagadnień ma praktyczny wymiar, ale również badawczy, który należy uwzględnić w różnych dziedzinach, na przykład w zarządzaniu, informatyce, prawie, nauce o przedsię-

biorstwie. Jest to dziedzina badań wymagająca integracji i znacznych środków, co wpływa na sytuację ekonomiczno-finansową każdego użytkownika systemów informatycznych.

THE SAFETY POLICY OF INFORMATION SYSTEMS

Summary

The information systems can be the most important source of danger for every organization. The safety policy concentrates on development of rules, finding factors, which have to be overcome, and on the methods, which ensure the safety running and development of computer application.

Translated by Marek Mazur