PRACE NAUKOWE UNIWERSYTETU EKONOMICZNEGO WE WROCŁAWIU
Nr 49 2009
Zmiana warunkiem sukcesu
Rozwój i zmiany w małych i średnich przedsiębiorstwach

Janina Stankiewicz, Patrycja Łychmus, Hanna Bortnowska
Uniwersytet Zielonogórski

KODEKS ETYCZNY ISTOTNYM INSTRUMENTEM CHRONIĄCYM BEZPIECZEŃSTWO INFORMACJI W MIKRO- LUB MAŁYM PRZEDSIĘBIORSTWIE

1. Potrzeba permanentnego zabezpieczania informacji w organizacji

Menedżerowie, którzy chcą sprawnie zarządzać przedsiębiorstwem we współczesnej gospodarce rynkowej, muszą być nastawieni nie tylko na stałe poprawianie jego konkurencyjności, ale również na przeciwdziałanie niekontrolowanemu „wypływowi" informacji z firmy. Jest to ważne, gdyż informacja stanowi jeden z najważniejszych aktywów przedsiębiorstwa, a o przewadze konkurencyjnej często decyduje dostęp do niej i umiejętne jej wykorzystanie w praktyce. Ważnym zadaniem menedżerów jest zatem zapewnienie ochrony *know-how* organizacji oraz innych niejawnych (poufnych i zastrzeżonych[1]) informacji związanych z funkcjonowaniem, ponieważ błędy w ich przetwarzaniu lub ochronie przechowywania mogą prowadzić m.in. do znacznych strat finansowych, konsekwencji prawnych, utraty reputacji, spadku zaufania nabywców produktów/usług i innych partnerów biznesowych, a nawet likwidacji firmy.

Zapewnienie przedsiębiorstwu bezpieczeństwa informacji, rozumianego jako stan, w którym ryzyko przez nią ponoszone jest akceptowalne lub funkcjonuje ona w warunkach braku zagrożenia [Orzeł 2005], nie jest jedynie wyzwaniem technologicznym, ale również problemem związanym z ludźmi i zarządzaniem [Mitnick 2003, s. 15]. Co więcej, bezbronność systemów bezpieczeństwa rzadko bywa skut-

[1] Zgodnie z *Ustawą z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych*, informacje niejawne zaklasyfikowane jako stanowiące tajemnicę służbową oznacza się klauzulą: 1) „poufne" – w przypadku gdy ich nieuprawnione ujawnienie powodowałoby szkodę dla interesów państwa, interesu publicznego lub prawnie chronionego interesu obywateli oraz 2) „zastrzeżone" – w przypadku gdy ich nieuprawnione ujawnienie mogłoby spowodować szkodę dla prawnie chronionych interesów obywateli albo jednostki organizacyjnej. Natomiast informacje niejawne zaklasyfikowane jako stanowiące tajemnicę państwową oznacza się klauzulą: 1) „ściśle tajne" lub 2) „tajne" [szerzej: *Ustawa*… 1999].

kiem technicznych czy też technologicznych niedoskonałości, częściej – konsekwencją popełnianych błędów podczas korzystania z tych technologii [Ohrimenco 2008]. Potwierdza to m.in. opinia K. Mitnicka [2003, s. 16], amerykańskiego eksperta do spraw bezpieczeństwa systemów komputerowych, jednego z najsłynniejszych hakerów świata: „W miarę wymyślania coraz to nowych technologii zabezpieczających, utrudniających znalezienie technicznych luk w systemie, napastnicy będą zwracać się w stronę ludzkich słabości. Złamanie »ludzkiej« bariery jest o wiele prostsze i często wymaga jedynie inwestycji rzędu kosztu rozmowy telefonicznej, nie mówiąc już o mniejszym ryzyku". Tak więc największym zagrożeniem dla bezpieczeństwa informacji w przedsiębiorstwie, szczególnie w mikro- lub małym, bywają pracownicy, mający fizyczny dostęp do jego zasobów informacyjnych, a także wiedzę na temat stosowanych w nim procedur działania [Schetina i in. 2002; Adamczyk i in. 2005]. W tego rodzaju organizacjach, biorąc pod uwagę, iż zazwyczaj zatrudnieni mają ze sobą bezpośrednie i codzienne kontakty *face to face*, istnieje większe prawdopodobieństwo, w porównaniu z organizacjami średnimi lub dużymi, niekontrolowanego „wypływu" informacji. Wiąże się to m.in. z zacieraniem wśród pracowników granicy tego, które informacje można rozpowszechniać, a które powinny być chronione i nie wynoszone poza firmę, ponieważ „wszyscy mówią sobie niemal o wszystkim".

Z zaprezentowanej perspektywy zagrożeń ważnym zadaniem menedżerów w zakresie bezpieczeństwa informacji w mikro- i małych przedsiębiorstwach jest wdrożenie organizacyjnych i technicznych systemów zabezpieczeń, skonstruowanie takiego systemu informacyjnego, który zapewni poufność informacji, ich nienaruszalność oraz dostępność, ale również poszukiwanie takich metod i środków, które zminimalizują zagrożenie „wypływu" informacji z przedsiębiorstwa, będącego skutkiem nieetycznych[2], celowych lub niezamierzonych działań pracowników na szkodę pracodawcy – kradzieży danych, fałszerstw dokumentacji, ujawniania informacji dotyczących klientów, popełniania błędów podczas wprowadzania danych itp. Tym bardziej że – jak wykazują wyniki badań zawarte w raporcie *Globalny stan bezpieczeństwa informacji 2005*[3], dotyczące sposobów zabezpieczania informacji w przedsiębiorstwach, średnia liczba zdarzeń związanych z naruszeniem bezpieczeństwa sukcesywnie zwiększa się (z 704 w 2004 r. do 862 w 2005 r., co daje wzrost o 22,4%) [Berinato 2005; *Menedżerowie odpowiedzialni za...,* http://www.pwc.com/pl/pol/about/press-rm/2006/06_01_18 grms.html, marzec 2008]. Najczęstszymi sprawcami tych zdarzeń byli hakerzy, którzy w 2005 r. odpowiadali za 63% „ata-

[2] Przez nieetyczne działania pracowników rozumiemy tutaj takie, które wiążą się z nieprzestrzeganiem przez nich zasad bezpieczeństwa informacji, niewyznawanie takich wartości, jak np. uczciwość, rzetelność, odpowiedzialność, dyskrecja, lojalność wobec pracodawcy i klientów.

[3] Badania zostały przeprowadzone przez magazyn CIO i firmę PriceWaterhouseCoopers w marcu i kwietniu 2005 r. Analizie poddano wypowiedzi ponad 8200 respondentów, pełniących różne funkcje w organizacjach: dyrektorów operacyjnych (CEO) i finansowych (CFO), dyrektorów ds. IT (CIO), dyrektorów ds. bezpieczeństwa (CSO) oraz innych osób odpowiedzialnych za bezpieczeństwo informacji z 63 państw.

ków". Kolejne miejsca, jako wspomniani sprawcy, zajęli: obecni pracownicy (33%) i byli pracownicy firmy (20%). Te rezultaty potwierdzają także wyniki innych badań („Globalne badanie wycieków danych 2006"), według których przyczyną „wypływu" danych i informacji z przedsiębiorstwa byli głównie pracownicy. Istotne jest to, że w większości przypadków (77%) były one spowodowane nieświadomym działaniem jednostek, a w 23% − postępowaniem zamierzonym, celowo szkodliwym [Kaspersky Lab, za: Polaczek 2007; http://www.emodus.pl/tresc/ 50/21/25/]. Jeszcze mniejszym optymizmem napawają rezultaty badań przeprowadzonych przez firmę Cyber-Ark Software Inc. wśród 600 osób zatrudnionych w przedsiębiorstwach zlokalizowanych w Wielkiej Brytanii, Holandii i USA i opublikowanych w grudniu 2008 r. Z raportu wynika, że w sytuacji groźby utraty pracy tylko 41% zatrudnionych Brytyjczyków, 42% Amerykanów i 2% Holendrów nie byłoby skłonnych wykraść pracodawcy żadnych cennych informacji. Badani stwierdzili, że ukradliby przede wszystkim: bazy danych o klientach (odpowiednio 25, 53 i 31%), plany i oferty firmy (17, 31 i 16%), loginy i hasła dostępu (13, 35 i 15%) oraz dokumentację produktów przedsiębiorstwa (11, 30 i 15%). Rzadziej, według wyników przytaczanych badań, respondenci deklarowali kradzież informacji z działu personalnego (odpo-wiednio 6, 28 i 8%), a także dokumentów prawnych firmy, np. umów i kontraktów (6, 23 i 4%).

Przeciwdziałając tego rodzaju zagrożeniom, konieczne jest uczenie pracowników, które z posiadanych przez nich informacji mają charakter poufny lub są zastrzeżone i których rozprzestrzenianie będzie działaniem na szkodę przedsiębiorstwa i brakiem lojalności wobec firmy, pracodawcy i współpracowników. Można to uczynić przez dobór formy i stosowną konstrukcję kodeksu etycznego.

Celem artykułu jest odpowiedź na pytanie: jak można poprzez kodeks etyczny obligować członków mikro- i małych przedsiębiorstw do nieujawniania poufnych i zastrzeżonych informacji? By odpowiedzieć na tak postawione pytanie, przeanalizowano literaturę przedmiotu dotyczącą specyfiki zawartości kodeksów ogólnych i deontologicznych.

2. Kodeks ogólny i deontologiczny a bezpieczeństwo informacji w organizacji

Kodeks etyczny firmy określa zakres odpowiedzialności zarządu, rady nadzorczej i pozostałych członków organizacji, wynikający z przyjętych przez przedsiębiorstwo zobowiązań wobec społeczeństwa. Owe zobowiązania polegają zazwyczaj na promocji dobra, praw ludzkich, korzyści i dobrobytu społecznego, zakazywaniu działań i zachowań uważanych za zagrażające wymienionym wartościom [Klimczak 1996, s.72; Rybak 2004, s. 139]. Ponadto ujęte są w nim obowiązki przedsiębiorstwa i jego pracowników wobec innych podmiotów, zwłaszcza interesariuszy. Zawiera także respektowane w przedsiębiorstwie standardy uczciwego działania. Kodeks etyczny określa zatem ramy postępowania członków organizacji, stanowiąc wykaz zachowań dopuszczalnych i bezwzględnie zakazanych [Rybak 2004, s. 139].

Wprowadzanie kodeksu etycznego do codziennej praktyki, po jego akceptacji przez członków organizacji, może się przyczynić do zwiększenia bezpieczeństwa informacji w przedsiębiorstwie, stawia bowiem „tamę" niepożądanym zachowaniom pracowników związanym z ujawnianiem *know-what*, *know-how*, *know-who*, *know--when*, *know-where* i wprowadza za nie sankcje, ustanawia też dyrektywy chroniące zarówno dobra osobiste zatrudnionych, jak i ich dane oraz wiedzę [Rybak 2004, s. 142]. Formalne pisemne zestawienie wartości i norm etycznych, którymi powinni kierować się członkowie organizacji, nie tylko ułatwia menedżerom zarządzanie przedsiębiorstwem, lecz także staje się swoistym „drogowskazem" postępowania dla pracowników. Pomaga też w podejmowaniu decyzji etycznych oraz jest podstawą przy rozwiązywaniu dylematów moralnych. Wpływa pozytywnie na motywację etyczną zatrudnionych [Ford 1994, s. 130]. Kodeks etyczny może zatem stać się istotnym, choć specyficznym w porównaniu z innymi instrumentami, regulatorem (modyfikatorem) zachowań członków organizacji, wspomagając proces zmian behawioralnych w przedsiębiorstwie.

By kodeks etyczny służył skutecznej ochronie informacji w mikro- i małych przedsiębiorstwach, konieczny jest wybór stosownej formy: kodeksu ogólnego będącego odzwierciedleniem filozofii firmy albo kodeksu określającego szczegółowo zasady postępowania (zwanego deontologicznym) [Pratley 1998, s. 243]. Pierwszy, w którym określa się etyczne zasady postępowania pracowników z perspektywy filozofii firmy, zawiera ogólny opis systemu wartości obowiązującego w przedsiębiorstwie. Nie zawiera zazwyczaj szczegółowego opisu pożądanych zachowań pracowników. Obejmuje natomiast założenia filozofii firmy i określa podstawowe zobowiązania zatrudnionych stanowiące fundament kultury organizacyjnej przedsiębiorstwa. Służy jako konstytucja zasad obowiązujących uczestników organizacji w zakresie ich podstawowych moralnych celów i obowiązków. Definiuje system wartości, który jest albo powinien być wyznawany w firmie.

Wadą kodeksu będącego odzwierciedleniem filozofii firmy, z perspektywy zapewnienia ochrony informacji w mikro- i małych przedsiębiorstwach, jest ogólność zawartych w nim zasad. Może to ograniczać zasięg oddziaływania na pracowników – nie wszyscy są w stanie (nie mogą i nie potrafią) odnosić ogólne sformułowania zawarte w takim kodeksie do konkretnych sytuacji zagrażających bezpieczeństwu informacji. Mankament ten może nie mieć znaczenia w średnich lub dużych firmach, w których najczęściej szczegółowe zasady zachowania się (wobec klientów, pracowników innych wydziałów, kontrahentów itp.) są regulowane osobnymi przepisami ujętymi np. w procedurach postępowania. W mikro- i małych przedsiębiorstwach zakres formalnych regulacji sformułowanych przez przedsiębiorstwo jest zazwyczaj mniejszy, co oznacza, że wprowadzając w nich kodeks etyczny, bardziej wskazane byłoby stosowanie takiego, który zawierałby konkretny zbiór zasad służący ochronie informacji, odnoszący się do różnych potencjalnych sytuacji zawodowych. Taki walor posiada kodeks deontologiczny, bowiem drobiazgowo określa obowiązki pracowników względem ich firmy oraz wobec kontrahentów i konsumentów. Trzeba

zaznaczyć, że czasami ta nadmierna szczegółowość bywa postrzegana jako słabość[4], jednak w przypadku ochrony informacji stanowi zaletę, wskazuje bowiem pracownikom konkretne sytuacje mogące stanowić źródło niekontrolowanego „wypływu" informacji, a których w przeciwnym razie nie percypowaliby jako niebezpiecznych. Tym samym uczulają zatrudnionych na potencjalne zagrożenia związane z pełnionymi przez nich funkcjami w organizacji oraz przeciwdziałanie im. Dostarczają członkom organizacji jednoznacznych wskazówek o tym, które zachowania służą ochronie informacji w organizacji, a jakich zachowań należy unikać, bo zagrażają ich bezpieczeństwu. Tym samym likwidują sferę niepewności wśród pracowników w zakresie własnego postępowania i ograniczają liczbę dylematów moralnych. Z tych względów, naszym zdaniem, w mikro- lub małym przedsiębiorstwie większe możliwości kształtowania pożądanych zachowań pracowników wobec informacji ma kodeks deontologiczny.

3. Deontologiczny kodeks etyczny jako instrument obligujący pracowników mikro- i małych przedsiębiorstw do dbania o bezpieczeństwo informacji

Kodeks deontologiczny firmy ma na celu pomaganie pracownikom w etycznym postępowaniu. Zawiera wskazania, w jaki sposób ogólne moralne zasady stosują się do tego, czym zajmuje się przedsiębiorstwo [De George 1995, za: Gasparski 2004, s. 284]. Stanowi on połączenie technicznych, prakseologicznych (tj. dotyczących roztropności) i moralnych imperatywów. Kodeksy tworzone dla organizacji z sektora mikro- i małych przedsiębiorstw powinny różnić się stopniem i sposobem argumentacji wspierającej owe imperatywy. Powinny także jednoznacznie komunikować zachowania pracowników związane z działaniem w imieniu firmy, a także precyzyjnie akcentować zachowania, które są wbrew jej interesom. Trzeba, by zawarte w kodeksie zasady mające na celu ochronę bezpieczeństwa informacji oscylowały wokół drugiego z wymienionych obszarów. Dlatego podczas formułowania zawartych w nim zasad konieczne jest zastosowanie silnych bodźców uczulających pracowników na potencjalne zagrożenia „wypływu" informacji, co nie byłoby możliwe przez zastosowanie form pozytywnych, np. „powinno się", „należy" itp. Stąd można przyjąć za zasadne użycie takich sformułowań, jak: „nie wolno", „trzeba", np.:

1) nie wolno wykorzystywać poufnych i zastrzeżonych informacji, do których ma się dostęp w związku z wykonywaną pracą, a których użycie mogłoby narazić pracodawcę na straty;

2) trzeba informować przełożonych o wszelkich zdarzeniach zagrażających bezpieczeństwu poufnych i zastrzeżonych informacji, o niepokojących telefonach, „atakach" hakerów itp.;

[4] Im bardziej skonkretyzowane są bowiem wytyczne dotyczące postępowania w określonych sytuacjach, tym bardziej, jak zauważa P. Pratley [1998, s. 243], kuszące dla pracowników jest ich naruszenie, szczególnie w sytuacji, kiedy nie są oni w pełni do nich przekonani.

3) nie wolno wykorzystywać posiadanych poufnych i zastrzeżonych informacji celem prowadzenia działalności konkurencyjnej wobec pracodawcy;

4) nie wolno ulegać pokusie „sprzedaży" poufnych i zastrzeżonych informacji przedsiębiorstwa celem uzyskania osobistych korzyści czy zysków;

5) nie wolno fałszować danych przedsiębiorstwa celem osiągnięcia zysku;

6) nie wolno zatrzymywać informacji „na własność", w przypadku gdy są one niezbędne innym pracownikom;

7) nie wolno rozprzestrzeniać poufnych i zastrzeżonych informacji wśród pracowników, którzy nie mają do nich uprawnień;

8) nie wolno prowadzić w miejscach publicznych rozmów, podczas których mogłyby zostać ujawnione osobom postronnym ważne poufne i zastrzeżone informacje przedsiębiorstwa;

9) nie wolno prowadzić rozmów telefonicznych w sytuacji, w której istnieje ryzyko usłyszenia ich przez niepowołane osoby;

10) trzeba chronić dokumenty papierowe lub komputerowe nośniki danych przed nieuprawnionym dostępem osób trzecich;

11) nie wolno udostępniać nieuprawnionym osobom trzecim urządzeń przetwarzających dane przedsiębiorstwa;

12) nie wolno przekazywać osobom nieupoważnionym haseł dostępu do informacji lub służbowych identyfikatorów;

13) nie wolno odchodzić od stanowiska pracy bez uprzedniego zablokowania klawiatury i włączenia wygaszacza ekranu zabezpieczonego hasłem;

14) nie wolno dopuszczać do sytuacji, w której osoby nieupoważnione mogłyby zobaczyć poufne i zastrzeżone informacje na ekranie monitora lub odczytać je z ruchu dłoni na klawiaturze;

15) nie wolno dopuszczać do sytuacji, w której osoby nieupoważnione mogłyby przeczytać dokumenty znajdujące się na biurku.

16) nie wolno wysyłać poufnych lub zastrzeżonych informacji za pomocą poczty elektronicznej bez uprzedniego zabezpieczenia ich hasłem;

17) trzeba szyfrować dyski, pliki i dokumenty zawierające poufne lub zastrzeżone dane/informacje;

18) trzeba przewozić komputery przenośne jako bagaż podręczny i maskować je podczas podróży;

19) nie wolno pozostawiać bez nadzoru dokumentów, nośników danych i sprzętu komputerowego w hotelach ani w samochodzie;

20) nie wolno wynosić poza miejsce pracy dokumentów zawierających poufne i zastrzeżone informacje;

21) nie wolno dopuszczać do sytuacji, w których w wyniku nieprawidłowego obchodzenia się z dokumentami, nośnikami danych lub komputerami poufne i zastrzeżone dane/informacje mogłyby ulec zniszczeniu.

Innym sposobem wskazywania na niestosowność pewnych zachowań jest pobudzanie wnioskowania moralnego osób zastanawiających się nad tym, jak postąpić w

konkretnym przypadku. Można to uczynić np. przez systematyczne publikowanie (bez podawania nazwisk) raportów o prowadzonych postępowaniach dyscyplinarnych wobec pracowników działających niezgodnie z zasadami kodeksu. Istnieje również możliwość umieszczenia w kodeksie pytań i odpowiedzi prezentujących wybrane przypadki, związane z potencjalnymi dylematami moralnymi. Oto przykłady.

Pracownik do przełożonego: „Usłyszałem na korytarzu rozmowę pomiędzy pracownikami Działu Badawczo-Rozwojowego na temat cech i użyteczności nowego produktu, którego wejście na rynek jest planowane w przyszłym roku. Ponieważ jest to produkt, którego docelowym odbiorcą są kobiety, czy mogę podzielić się tą informacją z moją żoną?".

Kierownik: „Nie. Istnieje bowiem ryzyko upowszechnienia tych informacji wśród znajomych żony, co może spowodować dalsze ich rozprzestrzenianie, co będzie działaniem na szkodę firmy".

Chcąc poprawić skuteczność kodeksu deontologicznego w uczeniu pracowników zachowań służących zapewnieniu bezpieczeństwa informacji, można również, poza odpowiedziami na przykładowe pytania, umieścić w nim wskazówki dotyczące postępowania w przypadku wątpliwości natury etycznej [Gasparski 2004, s. 292]. Mogą one mieć postać takich pytań kontrolnych, jak: Czy to jest legalne? Czy to jest uczciwe? Jak bym się czuł, gdybym to zrobił? Czy mógłbym „dobrze spać" po zrobieniu tego? Co pomyśleliby o tym moi bliscy? Czy jest to w zgodzie z wartościami i normami obowiązującymi w przedsiębiorstwie? Czy to zagraża realizacji strategii firmy lub jej planom rozwojowym? W uzupełnieniu tej listy trzeba w kodeksie zalecać zadawanie przez pracownika pytań dopóty, dopóki nie uzyska się pewności, że dane postępowanie jest słuszne. Jeżeli w dalszym ciągu pracownik ma wątpliwości, jak powinien się zachować w danej sytuacji, może się zwrócić np. do przełożonych lub specjalistów z zakresu etyki biznesu.

4. Uwagi końcowe

Zapewnienie bezpieczeństwa informacji w organizacji jest aktualnym problemem, z którym borykają się współcześni menedżerowie. Jego utrzymaniu sprzyja wiedza pracowników na temat znaczenia informacji, zakorzenienie w nich przeświadczenia, że zasoby informacyjne organizacji muszą być należycie chronione. W tym celu przydatne może być prezentowanie członkom organizacji właściwych, etycznych zachowań służących bezpieczeństwu informacji, ponieważ, jak pisze M. Rybak [2004, s. 145], dokonanie właściwego osądu moralnego, a następnie podjęcie stosownej decyzji nie przysparza poważniejszych problemów osobie mającej do tego odpowiednie przygotowanie merytoryczne i moralne (wiedzę i doświadczenie). Dlatego tak ważne jest uczenie pracowników postępowania zgodnego z etyką, a zatem trzeba ich obligować do przestrzegania kodeksu etycznego obowiązującego w przedsiębiorstwie. Jednak skuteczność kodeksu jako regulatora zachowań w organizacji bywa, jak stwierdzają A. Kitson i R. Campbell [1996, za: Rybak 2004, s. 140],

uzależniona od spełnienia co najmniej trzech warunków. Pierwszy to konieczność poprzedzenia opracowania kodeksu długim okresem konsultacji i dyskusji prowadzonych przez wszystkich pracowników. Z niego wynika drugi warunek – kodeks nie może być narzucony przez zarząd, lecz powinien być traktowany jako własność tych, którzy mieli na niego jakikolwiek wpływ. I trzeci – wprowadzenie kodeksu musi być poprzedzone programem szkolenia i rozwoju członków organizacji.

Literatura

Adamczyk A., Renk R., Radziulis J., Hołubowicz W., *Klasyfikacja informacji i danych prawnie chronionych oraz wymagania dotyczące środków informatycznych przeznaczonych do ich przechowywania i przetwarzania*, 2005 http://www.ploug.org.pl/konf_05/materialy/pdf/11.pdf (lipiec 2008).

Berinato S., *Stan światowego bezpieczeństwa informacyjnego*, „CSO" 2005 nr 12.

Cyber-Ark Software Inc., *The Global Recession and Its Effect on Work Ethics*, 2008, http://www.cyber-ark.com/pdf/Ethics-Survey-Results.pdf (grudzień 2008).

De George R.T., *Business Ethics*, Prentice Hall, Englewood Cliffs 1995.

Donaldson J., *Key Issues in Business Ethics*, Academic Press, London 1989.

Engelmann M., *Bezpieczeństwo informacji – bezpieczeństwo fizyczne*, „Boston IT Security Review" 2007 nr 3.

Ford W.D.R., *Ethical decision making: A review of theeEmpirical literature*, „Journal of Business Ethics", marzec 1994.

Gasparski W., *Wykłady z etyki biznesu. Nowa edycja*, Wyższa Szkoła Przedsiębiorczości i Zarządzania im. Leona Koźmińskiego, Warszawa 2004.

http://www.emodus.pl/tresc/50/21/25/ (październik 2008).

Kitson A., Campbell R., *The Ethical Organization: The Ethical Theory and Corporate Behaviour*, Macmillan Press, London 1996.

Klimczak B., *Etyka gospodarcza*, AE, Wrocław 1996.

Mitnick K., *Sztuka podstępu. Łamałem ludzi, nie hasła*, Helion, Gliwice 2003.

Ohrimenco S., *Bezpieczeństwo informacji, problemy kształcenia kadr*, http://www.ase.md/~osa/publ/ru/pubru104/ohrymenco-Poland.pdf (marzec 2008).

Orzeł J., *Stan bezpieczeństwa systemów informatycznych*, 2005, http://209.85.129.104/search?q=cache:rSxem6guuO4J:www.techbox.pl/aktualizacja/data/pliki/95_Stan%2520bezpieczenstwa%2520SI_rap _v1_3.pps+ryzyko+kadrowe+bezpiecze%C5%84stwo+informacji &hl=pl&ct=clnk&cd=2&gl=pl (marzec 2008).

Polaczek T., *Bezpieczeństwo informacji domeną nowoczesnego biznesu*; http://www.sec-info.silesia.pl/T.Polczek%20-%20prezent%20SEC-INFO%202007.pdf (marzec 2008).

Pratley P., *Etyka w biznesie*, Gebethner i Ska, Warszawa 1998.

Rybak M., *Etyka menedżera – społeczna odpowiedzialność przedsiębiorstwa*, Wydawnictwo Naukowe PWN, Warszawa 2004.

Schetina E., Green K., Carlson J., *Bezpieczeństwo w sieci*, Helion, Gliwice 2002.

Ustawa z dnia 22 stycznia 1999 roku o ochronie informacji niejawnych, DzU 1999 nr 11 poz. 95, tekst ujednolicony, http://lkp.org.pl/pdf/prawo/ustawa_tajemnica.htm (marzec 2008).

THE IMPORTANCE OF A CODE OF ETHICS AS AN INSTRUMENT PROTECTING INFORMATION SECURITY IN A MICRO OR SMALL ENTERPRISE

Summary

In a turbulent, changeable environment, the protection of information in an organization is one of the current problems which concerns managers. The biggest danger to data security in a company, especially in a micro or small one, comes from employees. The aim of the article is to answer the question of how to oblige members of micro and small companies not to leak information which is confidential and restricted.