Państwo i Społeczeństwo
III: 2003 nr 1

Leszek Korzeniowski

POLITYKA BEZPIECZEŃSTWA INFORMACJI W ZARZĄDZANIU FIRMĄ

Wprowadzenie

W procesie zarządzania od dawna docenia się konieczność zdobywania i zarządzania wiedzą, natomiast nie zwraca się uwagi na problem ochrony informacji przed niepożądaną zmianą lub utratą. Jest to zagadnienie, którym dawniej zajmowali się zazwyczaj specjaliści kontrwywiadu wojskowego lub służby bezpieczeństwa państwa. Po 1989 r. problem ten absorbować musi menedżerów firm komercyjnych; bankructwa będące skutkiem utraconych własnych informacji (lub zlekceważenia możliwości uzyskania niezbędnych informacji) stały się w Polsce codziennością.

Autor podejmuje próbę określenia pojęcia polityki bezpieczeństwa informacji i jej miejsca w zarządzaniu firmą koncentrując się na profilaktyce w trzech dających się wyodrębnić formach: organizacyjnej, prawnej i fizycznej. Nie bez znaczenia jest także aspekt praktyczny związany z wiedzą i umiejętnościami menedżerów, popełniających nagminnie błędy w kształtowaniu polityki bezpieczeństwa w zarządzanych firmach.

1. Bezpieczeństwo informacji

Informacja jest pojęciem złożonym i należy do wielu powszechnie stosowanych pojęć, które nie mają jednoznacznej definicji[1]. Nie wdając się w tym miejscu w analizę problemów definicyjnych należy zauważyć różnorodność cech, które będą miały znaczenie w kształtowaniu bezpieczeństwa. Informacja może być obiektywna lub subiektywna, potencjalna lub aktywna, pierwotna lub wtórna. Spo-

[1] Więcej na temat pojęcia i cech jakościowych informacji w: L. Korzeniowski, *Firma w warunkach ryzyka gospodarczego*, Kraków 2001.

śród wielu różnych informacji niektóre z nich będą bardziej przydatne, poprawne, użyteczne, dające zadowolenie i opłacalne dla użytkowników, niż inne, to znaczy że będą jakościowo lepsze. Przez jakość informacji należy tu rozumieć ogół właściwości informacji wiążący się ze zdolnością zaspokojenia stwierdzonych lub przewidywanych potrzeb użytkownika informacji.

Na jakość informacji składają się wszystkie pożądane cechy informacji; im informacja ma wyższą jakość, tym z większą pewnością menedżerowie mogą na niej polegać podejmując decyzję. Jednakże ze wzrostem jakości wzrasta również zazwyczaj koszt uzyskania informacji. Jeżeli wyższa jakość informacji nie przyczynia się w istotnym stopniu do zdolności podejmowania decyzji, to uzasadnionym jest zrezygnowanie z dodatkowych kosztów.

Polityka zarządzania bezpieczeństwem informacyjnym musi także uwzględniać nowe trendy zarządzania. Konieczność łączenia systemów obsługujących Internet z systemami o krytycznym znaczeniu dla działania przedsiębiorstwa (np. wspomaganie zarządzania, dokonywanie zamówień, współpraca z partnerami, dokonywanie zakupów) osłabiają system ochrony i ułatwiają dostęp włamywaczom.

Wykradanie tajemnic stało się domeną elektronicznych włamywaczy, którzy poznają tajemnice firm na odległość, pozostając anonimowymi i nieuchwytnymi. Ocenia się, że 59% stron internetowych oferujących produkty lub usługi w 1999 r. doświadczyło przynajmniej jednego naruszenia bezpieczeństwa[2]. Zagrożenie jest tym większe, że włamywacze poszukujący zawodowo strzeżonych informacji gospodarczych (w odróżnieniu od nastoletnich hakerów) nie pozostawiają „wizytówek" w postaci zmienionych stron www. Dlatego bardzo trudno jest zauważyć kradzież informacji. W przypadku innych form kradzieży coś fizycznie ginie – informację można ukraść jedynie kopiując ją. Pozornie nie ginie nic – właściciel dalej ma informację, z tym, że już bez żadnej wartości[3].

Lekceważenie identyfikacji zagrożeń i podejmowanie decyzji przez kadrę zarządzającą jest powszechne we wszystkich formach organizacyjno-prawnych przedsiębiorczości[4]. Jest to jedna z przyczyn wzrostu przestępczości gospodarczej – według statystyk policji, liczba przestępstw gospodarczych w Polsce wzrasta. Równocześnie jednak rozmiary tzw. „ciemnej liczby" w przestępczości gospodarczej są ogromne. Niektórzy podają, że tylko jedno na 1000 przestępstw gospodarczych jest ujawniane[5].

Wyniki globalnego raportu Ernst&Young dotyczącego bezpieczeństwa informacyjnego wskazują na alarmujące rozbieżności między deklarowaną przez firmy i organizacje znajomością tematu, a ich faktyczną odpornością na zagrożenia zewnętrzne i wewnętrzne[6]. Wyniki badań wskazują, że choć świadomość potrzeby

---

[2] Z. Zwierzchowski, *Najpierw bezpieczeństwo*, „Rzeczpospolita" 2000 (5 X).

[3] Odwrotnie, gdy celowo przekazuje się komuś informację, np. w celach marketingowych, to właściciel nadal ją posiada, a informacja taka staje się dla niego cenniejsza.

[4] Do najgłośniejszych takich przykładów można zaliczyć bankructwo amerykańskiej firmy Enron, która pociągnęła za sobą upadek największej światowej firmy audytorskiej, Andersen. Sprawcą tego okazał się Dawid Duncan, jeden z najważniejszych menedżerów odpowiedzialnych za badanie ksiąg handlowych Enronu.

[5] S. Kozdrowski, *Wybrane zagadnienia kryminologii*, Słupsk 2000, s. 54.

[6] *Bezpieczeństwo informacyjne*, „Biznes Trendy" 2002 (VI), s. 15.

zapewnienia bezpieczeństwa informacyjnego wzrasta na całym świecie, kroki podejmowane przez firmy w celu zapewnienia tego bezpieczeństwa są niejednolite i często niewystarczające. Badania m.in. wykazały, że:

- przedstawiciele zaledwie 40% organizacji wyrazili przekonanie o możliwości wykrycia ataku na swoje systemy informatyczne,
- 40% organizacji nie bada przypadków naruszenia swojego bezpieczeństwa,
- ponad 75% organizacji doświadczyło niespodziewanego ograniczenia dostępności swoich krytycznych systemów,
- tylko 53% organizacji posiada plany kontynuacji działania,
- mimo powszechnie dostępnych informacji o przewadze zagrożeń wewnętrznych nad zewnętrznymi, zaledwie 41% organizacji obawia się ataków od wewnątrz na swoje systemy,
- poniżej 50% organizacji szkoli swoich pracowników w zakresie bezpieczeństwa informacyjnego.

Znikoma jest wykrywalność i karalność przestępstw na rynku kapitałowym, polegających głównie na manipulowaniu informacjami. Komisja Papierów Wartościowych i Giełd w latach 1991-2002 skierowała do prokuratury 249 zawiadomień o popełnieniu przestępstwa, które zaledwie w 55 przypadkach zostały zmienione w akty oskarżenia[7]. Przyczyną takiego stanu są wysokie koszty i niskie umiejętności prokuratorów, detektywów i specjalistów prowadzących dochodzenia i gromadzących dowody procesowe w sprawach dotyczących przestępstw informacyjnych.

Polityka bezpieczeństwa informacji musi być w przedsiębiorstwie wszechstronna, uwzględniająca nie tylko przeciwdziałanie zagrożeniom utraty informacji lub jej ujawnienia osobom nieuprawnionym, ale także ochronę informacji przed wszelkimi innymi zagrożeniami. Struktura bezpieczeństwa musi odpowiadać konkretnej firmie i rodzajowi prowadzonej przez nią działalności. Szczególny nacisk należy położyć na działania priorytetowe. Technologiczne instytuty badawcze będą kłaść nacisk na tajność danych przy uwzględnieniu ich integralności, podmioty handlowe postawią na dostępność dla odbiorców.

Planując politykę bezpieczeństwa informacji należy uwzględnić:

wartość posiadanych zasobów informacji. Należy przeanalizować, co ma być poddane ochronie: urządzenia, oprogramowanie, baza danych pod kątem ryzyka utraty[8] posiadanych zasobów informacji. Jakie będą konsekwencje przełamania ochrony – utrata przewagi konkurencyjnej, wiarygodności, zagrożenie bezpieczeństwa, konsekwencje odszkodowawcze itp.,

- **źródło agresji.** Należy rozważyć, kto mógłby zagrażać zasobom informacji – obce służby specjalne, wywiad wojskowy, agendy rządowe, terroryści, sabotażyści, konkurenci, złodzieje, nieuprawnieni pracownicy a może przypadkowe osoby ciekawskie? Jaka jest wartość informacji dla potencjalnego agresora,

---

[7] *Przestępcy czują się bezkarni*, „Rzeczpospolita" 2002 (23 II).

[8] Przez utratę informacji rozumiem tu nie tylko pozbycie się informacji przez jej posiadacza, ale także utratę jej wartości przez jej poznanie przez inne podmioty, obniżenie wartości informacji przez jej zniekształcenie itp.

- **poziom możliwości agresora.** Jakimi możliwościami technicznymi, intelektualnymi i organizacyjnymi dysponuje potencjalny agresor? Jakie nakłady finansowe i rzeczowe, byłby w stanie ponieść, ile czasu poświęcić dla uzyskania lub zniszczenia zasobów informacji,
- **poziom ochrony** informacji niejawnych (klauzula tajności) i ilość informacji podlegających ochronie,
- **poziom dostępu** i liczbę uprawnionych osób,
- **wskazania służb ochrony państwa** i innych kompetentnych instytucji.

2. Zabezpieczenia organizacyjne

Każdy przedsiębiorca, działający nawet w najprostszej formie prawno-organizacyjnej, wytwarza tysiące informacji dotyczące realizacji zamówień, wynagrodzeń pracowników, należności podatkowych, rozliczeń z ubezpieczycielami, dokumentacji materiałowych itp. Duże przedsiębiorstwo wytwarza tych informacji miliony. Równocześnie w coraz większym stopniu traktuje się informacje jako kluczowy czynnik, ułatwiający menedżerom reagowanie na złożone i dynamiczne otoczenie. Nic dziwnego, że coraz więcej menedżerów traktuje samą informację jako cenny skarb – taki, którym trzeba uważnie gospodarować i który należy starannie chronić[9].

Zabezpieczenia organizacyjne są często niedoceniane. Obejmują one zarówno właściwe funkcjonowanie firmy, jak i systemu informacyjnego. Tego typy zabezpieczenia są realizowane przez instrukcje, procedury, upoważnienia, dokumentację i normy prawne. Podstawową zaletą zabezpieczeń organizacyjnych są niskie koszty, łatwość ich przyswojenia przez personel, brak ingerencji w zasadniczy proces przetwarzania danych i łatwość kontroli.

Podstawą zabezpieczeń organizacyjnych jest odpowiednia struktura zbioru informacji przedsiębiorstwa, na którą składają się:

- **tajemnica państwowa**, czyli informacja niejawna, której nieuprawnione ujawnienie może spowodować istotne zagrożenie podstawowych interesów Rzeczypospolitej Polskiej, a w szczególności niepodległości lub nienaruszalności terytorium, interesów obronności, bezpieczeństwa państwa i obywateli, albo narazić te interesy na co najmniej znaczną szkodę[10]. Rodzaje informacji, w liczbie 96, będących tajemnicą państwową są ściśle określone[11],
- **tajemnica służbowa**, czyli informacja niejawna nie będąca tajemnicą państwową, uzyskana w związku z czynnościami służbowymi albo wykonywaniem prac zleconych, której nieuprawnione ujawnienie mogłoby narazić na szkodę interes państwa, interes publiczny lub prawnie chroniony interes oby-

---

[9] P. L. Tom, *Managing Information as a Corporate Resource*, Glenview 1987, s. 4 (za: J. A. F. Stoner, *Kierowanie*, Warszawa 1997, s. 589).

[10] Ustawa z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych (Dz.U. nr 11, poz. 95).

[11] Załącznik nr 1 do Ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych (Dz.U. nr 11, poz. 95).

wateli albo jednostki organizacyjnej[12]. Pomimo, iż ustawa odwołuje się do treści wiadomości stanowiących tajemnicę służbową a nie do formalnego jej oznaczenia przez odpowiedni organ jako tajemnicy służbowej, to punktem wyjścia jest jednak fakt, że określona wiadomość jest na mocy kompetentnego organu utrzymywana w tajemnicy[13],

- **informacja chroniona** podlega ochronie prawnej na podstawie ustawy lub przyjętego na siebie zobowiązania, związana z pełnioną funkcją, wykonywaną pracą, działalnością publiczną, społeczną, gospodarczą lub naukową[14]. Do tej kategorii należy także zaliczyć określone odrębnymi ustawami lub umowami pomiędzy stronami, tajemnice: zawodową, skarbową, bankową, lekarską, handlową, statystyczną, przedsiębiorstwa itp. Informacje te ze względu na poziom ochrony są często określane jako informacje służbowe, odróżnia je jednak inna podstawa prawna ochrony oraz brak oznaczeń specjalnymi klauzulami,
- **dane osobowe,** przez które rozumie się każdą informację dotyczącą osoby fizycznej, pozwalającą na określenie tożsamości tej osoby[15],
- **informacje neutralne** z punktu widzenia prawa do ochrony lub obowiązku udostępniania,
- **informacje publiczne,** przez które rozumie się każdą informację o sprawach publicznych, do udostępniania których obowiązane są władze publiczne i inne podmioty wykonujące zadania publiczne[16].

Za ochronę informacji odpowiedzialny jest kierownik jednostki organizacyjnej, w której informacje podlegające ochronie są przetwarzane, przekazywane lub przechowywane. Do takich jednostek organizacyjnych należy także przedsiębiorca ubiegający się o zawarcie lub wykonujący umowę związaną z dostępem do informacji niejawnych, dotyczących zadań opłacanych w całości lub części ze środków publicznych[17].

Organizacja ochrony informacji niejawnych uwzględnia cztery poziomy tajemnicy, którym odpowiadają cztery rodzaje klauzuli tajności:
tajemnica państwowa:
- ściśle tajne,
- tajne.
tajemnica służbowa:
- poufne,
- zastrzeżone.
Informacje niejawne podlegają ochronie:

- oznaczone klauzulą „ściśle tajne" i „tajne" podlegają ochronie przez okres 50 lat, przy czym dane identyfikujące funkcjonariuszy i żołnierzy służb ochrony

[12] Ustawa z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych (Dz.U. nr 11, poz. 95).

[13] Por. L. Gardocki, *Prawo karne*, Warszawa 1998, s. 290.

[14] Zob. Ustawa z dnia 2 czerwca 1997 r., Kodeks karny (Dz.U. nr 88, poz. 553 ze zm.), art. 266, § 1.

[15] Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. nr 133, poz. 883 ze zm.).

[16] Ustawa z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz.U. nr 112, poz. 1198).

[17] W rozumieniu przepisów Ustawy z dnia 10 czerwca 1994 r. o zamówieniach publicznych (Dz.U. nr 119, poz. 773).

państwa wykonujących czynności operacyjno-rozpoznawcze, dane identyfikujące osoby udzielające odpowiednim organom pomocy oraz informacje niejawne uzyskane od innych państw lub organizacji międzynarodowych, jeżeli taki był warunek ich udostępnienia, chronione są bez względu na upływ czasu, natomiast niektóre informacje oznaczone klauzulą „tajne" mogą przestać stanowić tajemnicę państwową po upływie 20 lat,

- oznaczone klauzulą „poufne" podlegają ochronie przez 5 lat,
- oznaczone klauzulą „zastrzeżone" przez 2 lata.

Stanowiska lub rodzaje prac zleconych, z którymi może łączyć się dostęp do informacji niejawnych odrębnie dla każdej klauzuli tajności określa kierownik jednostki organizacyjnej. Dopuszczenie do pracy lub pełnienia służby na stanowisku albo zlecenie pracy, z którą może się łączyć dostęp do informacji niejawnych, może nastąpić po przeprowadzeniu postępowania sprawdzającego oraz po przeszkoleniu danej osoby w zakresie ochrony informacji niejawnych. Materiały i dokumenty zawierające dane i informacje podlegające ograniczeniom w ich ujawnianiu mogą być udostępniane wyłącznie osobom upoważnionym.

Dostęp do informacji niejawnych stanowiących tajemnicę państwową mają osoby, którym służby ochrony państwa[18] po przeprowadzeniu postępowania sprawdzającego i przeszkoleniu wydały poświadczenie bezpieczeństwa. Osoby te mogą zapoznać się z takimi materiałami i dokumentami po zaszeregowaniu do jednej z kategorii o określonym poziomie dostępu. Generalnie obowiązuje zasada, że informacje niejawne mogą być udostępniane wyłącznie osobom dającym rękojmię zachowania tajemnicy i tylko w zakresie niezbędnym do wykonywania przez nią pracy lub pełnienia służby na zajmowanym stanowisku albo innej zleconej pracy. Przez „rękojmię zachowania tajemnicy" rozumie się spełnianie ustawowych wymogów dla zapewnienia ochrony informacji niejawnych przed ich nieuprawnionym ujawnieniem.

System ochrony informacji niejawnych w Polsce tworzą:

- Komitet Ochrony Informacji Niejawnych[19],
- służby ochrony państwa,
- kierownicy jednostek organizacyjnych, w których informacje niejawne są wytwarzane, przetwarzane, przekazywane lub przechowywane,
- pełnomocnicy do spraw informacji niejawnych.

Miejscem przechowywania, wytwarzania, przetwarzania lub przekazywania dokumentów zawierających informacje niejawne jest kancelaria tajna. Stanowi ją wyodrębniona komórka organizacyjna podległa bezpośrednio pełnomocnikowi ochrony, odpowiedzialna za właściwe rejestrowanie, przechowywanie, obieg i wydawanie takich dokumentów uprawnionym osobom.

Kancelaria powinna być zorganizowana w wyodrębnionym pomieszczeniu, odpowiednio usytuowanym i zabezpieczonym, być obsługiwana przez pracowników pionu ochrony. Jej pracami kieruje kierownik, wyznaczony przez kierownika

[18] Agencja Bezpieczeństwa Wewnętrznego i Agencja Wywiadu.

[19] Przepisy Ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych (Dz.U. nr 11, poz. 95 ze zm.) powołujące Komitet Ochrony Informacji Niejawnych zostały uchylone.

jednostki organizacyjnej na wniosek pełnomocnika do spraw ochrony informacji niejawnych.

3. Ochrona prawna

Globalizacja, szybkość przepływu danych, powszechność dostępu do informacji i totalny (wszechogarniający) charakter zasobów informacji zagrażający jednostkom ludzkim i organizacjom przyczynia się do zwiększanie prawnej ochrony danych osobowych i informacji niejawnych. Wyraźnie powiększają się granice obszarów chronionych prawem publicznym, poprzez instytucje i środki publiczno-prawne. Wiedza o przepisach prawa regulującego ochronę i odpowiedzialność za brak lub niewystarczającą ochronę jest niezbędna menedżerom i pracownikom przedsiębiorstw a także działającym w ich otoczeniu agencjom konsultingowym, wywiadowniom gospodarczym i indywidualnym detektywom.

Ochronę prawną informacji wywieść można już z Konstytucji Rzeczypospolitej Polskiej, która w art. 51 zapewnia[20]:

- prawo do nieujawniania informacji dotyczących danej osoby, z wyjątkiem wynikającym z ustaw,
- ograniczenie władz publicznych w prawie do pozyskiwania, gromadzenia i udostępniania informacji o obywatelach do zakresu niezbędnego w demokratycznym państwie prawa,
- prawo każdego do dostępu dotyczących danej osoby urzędowych dokumentów i zbiorów danych z ograniczeniami wynikającymi z ustaw,
- prawo każdego do żądania sprostowania oraz usunięcia informacji nieprawdziwych, niepełnych lub zebranych w sposób sprzeczny z ustawą.

Konstytucyjne ograniczenie do pozyskiwania, gromadzenia i udostępniania informacji o obywatelach (a więc nie o każdym, czyli każdej osobie fizycznej, ale o obywatelach Rzeczypospolitej Polskiej) dotyczy władz publicznych, tzn. podmiotów wykonujących zadania w zakresie władzy ustawodawczej, wykonawczej i sądowniczej (Sejm i Senat, Prezydent RP, Rada Ministrów, sądy i trybunały, samorząd terytorialny i inne jednostki wykonujące władztwo publiczne).

Ustawowe zabezpieczenia prawne informacji wywodzą się z przepisów kodeksów prawa karnego, cywilnego, pracy, spółek handlowych oraz ordynacji podatkowej, ustaw o ochronie informacji niejawnych, zwalczających nieuczciwą konkurencję, prawa bankowego, o statystyce publicznej, o ochronie zdrowia psychicznego, o ochronie danych osobowych i innych przepisów szczegółowych.

Odpowiedzialność karna przewidziana w Kodeksie karnym[21] uregulowana została w rozdziale XXXIII „przestępstwa przeciwko ochronie informacji". Art. 265 określa odpowiedzialność za ujawnienie lub wykorzystanie tajemnicy państwowej. Odpowiedzialność ponosi nie tylko ten, kto wbrew przepisom ustawy

[20] Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz.U. nr 78, poz. 483).

[21] Ustawa z dnia 2 czerwca 1997 r., Kodeks karny (Dz.U. nr 88, poz. 553 z późn. zm.), art. 265 i nast.

ujawnia tajemnicę państwową, ale i ten, kto ją wbrew przepisom ustawy wykorzystuje. Należy zwrócić uwagę na karalność dziennikarzy za publikację dokumentów tajnych. Przepis o ochronie tajemnicy państwowej ma związek z przepisami ustawy o tajemnicy państwowej i służbowej, zgodnie z którą tajemnicę państwową obowiązany jest zachować każdy, do kogo ona dotarła.

Odpowiedzialność za ujawnienie informacji zastrzeżonej dotyczy tajemnicy innej niż państwowa – np. służbowej, zawodowej i innej tajemnicy powierzonej (art. 266). Odpowiedzialność dotyczy ujawnienia zastrzeżonej informacji wbrew ustawie lub przyjętemu zobowiązaniu.

Odpowiedzialność za nieuprawnione uzyskanie informacji (art. 267) dotyczy szeroko rozumianego naruszenia tajemnicy korespondencji, np. otwarcie cudzego pisma, nieprawne podłączenie się do przewodu służącego do przekazywania informacji, naruszenie elektroniczne, magnetyczne albo inne szczególnego zabezpieczenia informacji. Odpowiedzialność ponosi także ten, kto w celu uzyskania informacji, do której nie jest uprawniony, zakłada lub posługuje się urządzeniem podsłuchowym, wizualnym albo innym urządzeniem specjalnym a także ten, kto uzyskaną w ten sposób informację ujawnia innej osobie. Natomiast policja przy wykonywaniu czynności operacyjno-rozpoznawczych, po uzyskaniu zgody Prokuratora Generalnego, może legalnie kontrolować korespondencję i stosować środki techniczne umożliwiające uzyskanie w sposób tajny informacji[22].

Odpowiedzialność za bezprawne „zepsucie" informacji (art. 268 i 269) dotyczy jej zniszczenia, uszkodzenia, usunięcia, utrudnienia osobie uprawnionej zapoznania się z nią – zarówno zapisów tradycyjnych, jak i na komputerowym nośniku informacji.

Oprócz przepisów Kodeksu karnego odpowiedzialność karna została przewidziana w przepisach ustaw regulujących poszczególne dziedziny życia gospodarczego i wiąże się ona z bezprawnymi (to znaczy zabronionymi pod groźbą kary przez ustawę obowiązującą w czasie jego popełnienia) i zawinionymi czynami człowieka.

Odpowiedzialność na podstawie Kodeksu cywilnego[23] wynika ze szkody wyrządzonej przedsiębiorcy czynem niedozwolonym ze swej winy lub z treści umowy łączącej strony. Naprawienie szkody obejmuje straty, które poszkodowany poniósł oraz korzyści, które mógłby osiągnąć, gdyby mu szkody nie wyrządzono. Natomiast odpowiedzialność umowna oparta jest na zasadzie swobody zawierania umów – strony mogą umówić się, że w przypadku nie zapewnienia ochrony informacji przedsiębiorcy zostanie mu zapłacona kara umowna. Wcześniej zawarta umowa powinna jednak określać rodzaje informacji, których zobowiązano się nie ujawniać innym osobom, czas trwania ochrony i wysokość kary umownej w przypadku nienależytej ochrony.

Cywilnoprawna ochrona sfery tajemnicy przedsiębiorcy (tajemnica korespondencji i tajemnica handlowa) skutkuje dopiero wówczas sankcjami, gdy dobra

---

[22] Ustawa z dnia 6 kwietnia 1990 r. o Policji (Dz.U. nr 30, poz. 179 z późn. zm.), art. 19.

[23] Ustawa z dnia 23 kwietnia 1964 r., Kodeks cywilny (Dz.U. nr 16, poz. 93 z późn. zm.), zwłaszcza art. 415, art. 361, art. 483, § 1.

te zostały zagrożone[24]. Niezależnie od winy i subiektywnych celów naruszenia tajemnicy, sam fakt wkroczenia w sferę cudzej prywatności jest traktowany jako naruszenie dobra osobistego. Należy zauważyć, że osoba prawna, wykazując naruszenie tajemnicy przedsiębiorcy na podstawie przepisów art. 448 Kodeksu cywilnego nie musi precyzyjnie określać rozmiaru uszczerbku (jak wymagają tego przepisy o zwalczaniu nieuczciwej konkurencji)[25].

Odpowiedzialność z przepisów Kodeksu pracy[26] dotyczy pracownika wyrządzającego szkodę na skutek niezapewnienia ochrony informacji pracodawcy. Jeżeli na skutek niewykonania lub nienależytego wykonania obowiązków pracowniczych pracownik ze swej winy wyrządził pracodawcy szkodę, ponosi odpowiedzialność materialną. Wina pracownika może być umyślna, to znaczy wtedy, gdy pracownik chce wyrządzić szkodę, jak i wówczas, gdy wyrządzenie szkody przewiduje i z tym się godzi. Wina pracownika może być także nieumyślna, to znaczy gdy pracownik przewiduje możliwość wyrządzenia szkody lecz bezpodstawnie przypuszcza, że tego uniknie, oraz gdy nie przewiduje możliwości wyrządzenia szkody choć mógł i powinien to przewidzieć.

Odpowiedzialność na podstawie przepisów Kodeksu spółek handlowych[27] jest inna dla spółek osobowych, a inna dla spółek kapitałowych. Ochrona informacji w spółkach osobowych (jawna, partnerska, komandytowa, komandytowo-akcyjna) może być wywiedziona z przepisu zobowiązującego wspólników do powstrzymania się od wszelkiej działalności sprzecznej z interesami spółki (art. 56). W spółkach kapitałowych członek zarządu, rady nadzorczej, komisji rewizyjnej oraz osoba biorąca udział w tworzeniu spółki i likwidator odpowiada wobec spółki za szkodę wyrządzoną działaniem lub zaniechaniem, sprzecznym z prawem lub postanowieniami umowy spółki, chyba że nie ponosi winy (art. 293, art. 483), co nie wyłącza dochodzenia naprawienia szkody na zasadach ogólnych. Przestępstwo zagrożone jest karą pozbawienia wolności do lat 5 i grzywną. Tej samej karze podlega ten, kto nakłania do działania na szkodę spółki lub udziela pomocy w popełnieniu tego przestępstwa.

Ordynacja podatkowa[28] zapewnia ochronę tajemnicy skarbowej, przez którą rozumie się indywidualne dane zawarte w deklaracji oraz innych dokumentach składanych przez podatników, płatników lub inkasentów a także informacje podatkowe, akta i dokumentację rachunkową organów podatkowych i informacje uzyskane przez organy podatkowe z banków.

Każdy, kto będąc obowiązanym do zachowania tajemnicy skarbowej (a są nimi pracownicy urzędów i izb skarbowych, wójt, burmistrz, prezydent miasta, starosta, marszałek województwa oraz pracownicy samorządowych służb finanso-

---

[24] A. Bierć, *Ochrona prawna danych osobowych w sferze działalności gospodarczej w Polsce – aspekty cywilnoprawne*, [w:] *Ochrona danych osobowych*, red. M. Wyrzykowski, Warszawa 1999, s. 129.

[25] Ibidem, s. 131.

[26] Ustawa z dnia 26 czerwca 1974 r., Kodeks pracy (Dz.U. nr 24, poz. 141 z późn. zm.), art. 114 i nast.

[27] Ustawa z dnia 15 września 2000 r., Kodeks spółek handlowych (Dz.U. nr 94, poz. 1037). Do 31 grudnia 2000 r. było to Rozporządzenie Prezydenta Rzeczypospolitej z dnia 27 czerwca 1934 r., Kodeks handlowy (Dz.U. nr 57, poz. 502, ze zm.).

[28] Ustawa z dnia 29 sierpnia 1997 r., Ordynacja podatkowa (Dz.U. nr 137, poz. 926 ze zm.).

wych, członkowie i pracownicy biur samorządowych kolegiów odwoławczych, minister właściwy do spraw finansów publicznych i pracownicy oraz praktykanci Ministerstwa Finansów), ujawnia informacje objęte tą tajemnicą, podlega karze pozbawienia wolności do lat 5. Ustawa rozróżnia Skarb Państwa i innych pokrzywdzonych: jeżeli pokrzywdzonym nie jest Skarb Państwa, ściganie przestępstwa ujawnienia tajemnicy skarbowej następuje na wniosek pokrzywdzonego[29]. Jest to wyraźna wada w systemie prawnej ochrony tajemnicy skarbowej, gdyż z samego charakteru informacji wynika, że pokrzywdzony może nie wiedzieć o ujawnianiu dotyczących go danych objętych tajemnicą skarbową, a posiadająca taką wiedzę policja, prokuratura i inne uprawnione instytucje nie mają obowiązku uświadamiać o tym pokrzywdzonego.

Zasady ochrony informacji, które wymagają ochrony przed nieuprawnionym ujawnieniem jako stanowiące tajemnicę państwową lub służbową, określa Ustawa o ochronie informacji niejawnych[30].

Zgodnie z Ustawą o zwalczaniu nieuczciwej konkurencji[31], tajemnica przedsiębiorstwa stanowi dobro chronione prawem. Zgodnie z art. 11 tej ustawy przedmiotem tego prawa są „cudze informacje stanowiące tajemnicę przedsiębiorstwa", a treścią prawa przedsiębiorcy „prawo żądania, aby każda osoba nieuprawniona powstrzymała się od przekazywania, ujawniania lub wykorzystywania cudzych informacji, stanowiących tajemnicę przedsiębiorstwa". Zgodnie z Ustawą, czynem nieuczciwej konkurencji jest przekazanie, ujawnienie lub wykorzystanie cudzych informacji stanowiących tajemnicę przedsiębiorstwa albo ich nabycie od osoby nieuprawnionej, jeżeli zagraża to istotnym interesom przedsiębiorcy. W przypadku zagrożenia lub naruszenia interesów przedsiębiorcy w przypadku czynu nieuczciwej konkurencji, przedsiębiorca może:
- zażądać zaniechania niedozwolonych działań,
- domagać się usunięcia skutków niedozwolonych działań,
- wymagać złożenia oświadczenia odpowiedniej treści i w odpowiedniej formie,
- zażądać naprawienia szkody,
- zażądać wydania bezpodstawnie uzyskanych korzyści.

Tajemnica, podobnie jak nazwa (firma) przedsiębiorstwa, jest prawem o charakterze osobisto-majątkowym[32]. Prawo do tajemnicy przedsiębiorcy jest bowiem związane zarówno z osobą przedsiębiorcy, jak i z przedsiębiorstwem. Punktem odniesienia tajemnicy jest w istocie przedsiębiorca, który tę tajemnicę ustanawia. Jednocześnie jest ona składnikiem przedsiębiorstwa, nieraz o znacznej wartości i może być przedmiotem obrotu.

Naruszenie prawa do tajemnicy przedsiębiorstwa może być uznane za naruszenie prywatności przedsiębiorcy i podlegać ochronie na podstawie przepisów Kodeksu cywilnego o ochronie dóbr osobistych (łącznie z możliwością domagania

[29] Ibidem, art. 306, § 4.

[30] Ustawa z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych (Dz.U. nr 11, poz. 95).

[31] Ustawa z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (Dz.U. nr 47, poz. 211 z późn. zm.).

[32] A. Bierć, op. cit., s. 131.

się zadośćuczynienia pieniężnego), a także może powodować odpowiedzialność cywilną (i karną) określoną w przepisach Ustawy o zwalczaniu nieuczciwej konkurencji.

Przepisy prawa bankowego[33] chronią informacje objęte tajemnicą bankową[34] w tym także przed tzw. osobami trzecimi, do których zalicza się akcjonariuszy, członków banku spółdzielczego, audytorów niebędących pracownikami banku, agencje windykacyjne, agencje marketingowe i inne[35]. W sytuacji szczególnej, gdy osoby trzecie wykonują czynności związane z działalnością banku, podstawą dostępu przez nich do informacji bankowej jest pisemne upoważnienie banku do przekazania określonej informacji wskazanej przez klienta banku konkretnej osobie trzeciej. Za naruszenie tajemnicy bankowej grozi odpowiedzialność karna[36].

Przepisy Ustawy o statystyce publicznej[37] chronią dane jednostkowe osób fizycznych oraz dane indywidualne osób prawnych. Nie mogą być publikowane ani udostępniane informacje statystyczne możliwe do powiązania z konkretną osobą oraz dane indywidualne, charakteryzujące wyniki ekonomiczne przedsiębiorców, zwłaszcza jeśli składają się na nie mniej niż trzy podmioty lub udział jednego podmiotu w określonym zestawieniu jest większy niż trzy czwarte całości. Naruszenie tych zakazów podlega sankcjom karnym, tj. karze pozbawienia wolności lub karze grzywny[38].

Przepisy Ustawy o ochronie zdrowia psychicznego zobowiązują osoby wykonujące czynności wynikające z tej ustawy do zachowania w tajemnicy wszystkiego, o czym powezmą wiadomość w związku z wykonywaniem tych czynności[39].

Przepisy Ustawy o ochronie danych osobowych obejmuje ochroną prawną każdą informację dotyczącą osoby fizycznej, pozwalającą na określenie tożsamości tej osoby, a także wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej[40].

Ustawa ustanawia organ ochrony danych osobowych – Generalnego Inspektora Danych Osobowych, powoływanego i odwoływanego przez Sejm Rzeczypospolitej Polskiej za zgodą Senatu na czteroletnią kadencję. Generalny Inspektor kontroluje zgodność przetwarzania danych z przepisami o ochronie danych osobowych, wydaje decyzje administracyjne, rozpatruje skargi, prowadzi rejestr zbiorów danych, udziela informacji o zarejestrowanych zbiorach, opiniuje projekty ustaw i rozporządzeń, inicjuje i podejmuje przedsięwzięcia oraz uczestniczy w pra-

---

[33] Ustawa z dnia 29 sierpnia 1997 r., Prawo bankowe (Dz.U. nr 140, poz. 939 ze zm.).

[34] Ibidem, art. 105.

[35] Zob. pisma Przewodniczącego Komisji Nadzoru Bankowego z 11 lutego 2000 r. w sprawie przestrzegania tajemnicy bankowej przez banki z udziałem kapitału zagranicznego, nr NB/BI/WA/16/2000; z 21 lipca 2000 r. w sprawie respektowania przepisów o tajemnicy bankowej, nr NB/BPN/I/434/00.

[36] Ustawa z dnia 29 sierpnia 1997 r., Prawo bankowe (Dz.U. nr 140, poz. 939 ze zm.), art. 171.

[37] Ustawa z dnia 29 czerwca 1995 r. o statystyce publicznej (Dz.U. nr 88, poz. 439 z późn. zm.).

[38] Ibidem, art. 54-59.

[39] Ustawa z dnia 19 sierpnia 1994 r. o ochronie zdrowia psychicznego (Dz.U. nr 111, poz. 535 ze zm.), art. 50, ust. 1.

[40] Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. nr 133, poz. 883 ze zm.).

cach międzynarodowych organizacji i instytucji zajmujących się problematyką danych osobowych[41].

Kto przetwarza w zbiorze dane osobowe, choć ich przetwarzanie nie jest dopuszczalne albo do których przetwarzania nie jest uprawniony, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2. Jeżeli dany czyn dotyczy danych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, danych o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym, kara pozbawienia wolności wynosi do 3 lat[42]. Karalne jest również:
- przechowywanie w zbiorze danych niezgodnie z celem,
- udostępnianie danych osobowych lub umożliwianie dostępu do nich osobom nieupoważnionym,
- niedopełnienie obowiązku zabezpieczenia danych osobowych przed zabraniem ich przez osobę nieuprawnioną, uszkodzeniem lub zniszczeniem,
- niezgłaszanie (mimo obowiązku) danych do rejestru zbioru danych,
- niedopełnienie obowiązku poinformowania osoby, której dane dotyczą, o jej prawach lub nie przekazanie tej osobie informacji umożliwiających korzystanie z praw przyznaniem jej w ustawie o ochronie danych osobowych.

4. Ochrona fizyczna

Ochrona fizyczna polega na zapewnieniu bezpieczeństwa fizycznym nośnikom informacji: ich trwałości, integralności i niedostępności dla sił fizycznych lub zjawisk elektromagnetycznych, cieplnych, chemicznych itp.

Do podstawowych środków ochrony fizycznej informacji można zaliczyć[43]:

- wydzielenie w części obiektów „strefy bezpieczeństwa" i poddanie jej szczegółowej kontroli wejść i wyjść oraz kontroli przebywania,
- wydzielenie wokół stref bezpieczeństwa strefy administracyjnej służącej kontroli osób lub pojazdów,
- wprowadzenie systemu przepustek lub innego systemu określającego uprawnienia wejścia, przebywania i wyjścia ze strefy bezpieczeństwa,
- wprowadzenie systemu przechowywania kluczy do pomieszczeń chronionych, szaf pancernych i innych pojemników służących do przechowywania informacji niejawnych,
- zapewnienie kontroli stref bezpieczeństwa i stref administracyjnych przez odpowiednio przeszkolonych pracowników pionu ochrony,
- stosowanie wyposażenia i urządzeń służących ochronie informacji niejawnych, które posiadają odpowiednie certyfikaty i świadectwa kwalifikacyjne.

---

[41] Ibidem, art. 12.

[42] Ibidem, art. 49.

[43] Ustawa z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych (Dz.U. nr 11, poz. 95), art. 57.

Szczególnej ochronie podlegają systemy i sieci teleinformatyczne, służące wytwarzaniu, przechowywaniu, przetwarzaniu i przekazywaniu informacji. Środki bezpieczeństwa tych sieci obejmują środki ochrony[44]:

- **fizycznej**, przez umieszczenie urządzeń systemu lub sieci w strefie bezpieczeństwa oraz instalację środków zabezpieczających pomieszczenie przed nieuprawnionym dostępem, podglądem i podsłuchem,
- **elektromagnetycznej,** przez umieszczenie urządzeń, połączeń i linii w strefach bezpieczeństwa gwarantujących spełnienie wymogów zabezpieczenia elektromagnetycznego lub zastosowanie urządzeń, połączeń i linii o obniżonym poziomie emisji lub ich ekranowanie i filtrowanie zewnętrznych linii zasilających i sygnałowych,
- **kryptograficznej,** polegającej na stosowaniu metod i środków zabezpieczających informacje przez szyfrowanie oraz stosowanie innych mechanizmów kryptograficznych gwarantujących integralność i zabezpieczenie przed nieuprawnionym ujawnieniem tych informacji lub uwierzytelnienie podmiotów lub uwierzytelnienie informacji. Do istotnych czynników zabezpieczenia należą algorytmy i klucze kryptograficzne oraz hasła dostępu,
- **bezpieczeństwa transmisji,**
- **kontroli dostępu** do urządzeń, systemu lub sieci teleinformacyjnej.

Kancelaria tajna powinna być zlokalizowana w strefie bezpieczeństwa, na piętrze, z wyłączeniem poddaszy[45]. Powinna być oddzielona od innych pomieszczeń ścianami i stropami trwałymi, niepalnymi, o dużej wytrzymałości. Drzwi kancelarii powinny być metalowe lub obite blachą stalową o grubości 2 mm, z zabezpieczeniem antywłamaniowym oraz wyposażone w dwa zamki o skomplikowanym mechanizmie. Okna kancelarii powinny być zabezpieczone stalowymi kratami oraz przed obserwacji kancelarii z zewnątrz.

Wyposażenie kancelarii powinny stanowić szafy pancerne z zamkami o skomplikowanym mechanizmie. W kancelarii można zainstalować system nadzoru wizyjnego, wyłącznie w celu kontroli dostępu do pomieszczeń, a także wydzielić pomieszczenie, w którym osoby posiadające poświadczenie bezpieczeństwa mogą zapoznawać się z dokumentami na miejscu.

Trzeba pamiętać, że każde urządzenie lub przewód, przez który płyną dane, generuje promieniowanie elektromagnetyczne o określonej częstotliwości. Sygnał jest emitowany przez monitor, kable, gniazda i porty a nawet do sieci energetycznej, z której komputer jest zasilany. Promieniowanie komputera jest na tyle silne, że za pomocą specjalnego urządzenia można je odebrać z odległości kilkuset metrów. Wykorzystując specjalnie przystosowane anteny, informacje z komputera

---

[44] Rozporządzenie Prezesa Rady Ministrów z dnia 25 lutego 1999 r. w sprawie podstawowych wymagań bezpieczeństwa systemów i sieci teleinformatycznych (Dz.U. nr 18, poz. 162).

[45] Rozporządzenie Rady Ministrów z dnia 9 lutego 1999 r. w sprawie organizacji kancelarii tajnych (Dz.U. nr 18, poz. 156), § 5.

można odczytać także wykorzystując sieć elektryczną, grzewczą, wodną oraz przewody klimatyzacyjne[46].

Zabezpieczenia przed takimi zagrożeniami to:

- kabiny elektromagnetyczne, tzw. klatki Farradaya, w których umieszczane są odpowiedni uziemione urządzenia przetwarzające informacje niejawne,
- wyklejanie ścian pomieszczeń metalowymi foliami, spełniającymi podobną rolę ale o niższych parametrach niż klatki Farradaya,
- metalowe pudełka, w których umieszcza się monitor, drukarkę i komputer a także szyfratory i urządzenia nadawczo-odbiorcze,
- zabezpieczenia komputerów przenośnych według amerykańskich norm TEMPEST[47].

Ochrona informacji przesyłanej, gdy wielokrotnie wzmaga się niebezpieczeństwo przechwycenia i podsłuchania przesyłanych wiadomości, wymaga wyrafinowanych zabezpieczeń technicznych, wspomagających metody organizacyjne i prawne. Urządzenia szyfrujące osłabiają równocześnie czujność osób przekazujących informacje, które wiedząc, że rozmowa jest zabezpieczona technicznymi urządzeniami szyfrującymi, często nie zachowują należytej ostrożności w przekazywaniu informacji.

Wnioski

Zarządzanie informacjami stanowi zagadnienie, które ze względu na swoją złożoność i znaczenie dla realizacji celów firmy, powinno w znacznym stopniu angażować menedżerów. Na politykę bezpieczeństwa informacji składają się działania profilaktyczne w co najmniej trzech uzupełniających się formach: organizacyjnej, prawnej i fizycznej. Takie ujęcie powinno stanowić propozycję dalszych badań ujmujących całościowo problematykę bezpieczeństwa przedsiębiorcy i poszukujących odpowiedzi na pytania o zależność pomiędzy różnymi czynnikami warunkującymi realizację celów zarządzania.

Bibliografia

Bačová M., *Podstata a nevyhnosť existencie bankového dohľadu,* „Acta Oeconomica cassoviensia" N° 4, Košice 2000, s. 7-17.

Bezpieczeństwo informacyjne, „Biznes Trendy. Magazyn INFOR" 2002 (czerwiec), s. 15.

Bierć A., *Ochrona prawna danych osobowych w sferze działalno ści gospodarczej w Polsce – aspekty cywilnoprawne,* [w:] *Ochrona danych osobowych,* red. M. Wyrzykowski, Warszawa 1999, s. 111-153.

[46] K. R. Urbański, *Chroń swój komputer*, „Rzeczpospolita" 2000 (15 V).

[47] *Temporary Emantion and Spurious Transmission.*

Čarnický Š., *Strategická úloha informačných systémov*, „Acta Oeconomica cassoviensia" No 5, Košice 2001, s. 83-92.

Dadak W., *Prawnokarna ochrona tajemnicy handlowej w post ępowaniu w sprawach zamówień publicznych*, „Czasopismo Prawa Karnego i Nauk Penalnych" 2000, z. 1, s. 269-276.

Gardocki L., *Prawo karne*, Warszawa 1998.

Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz.U. nr 78, poz. 483).

Korzeniowski L., *Firma w warunkach ryzyka gospodarczego*, Kraków 2001.

Korzeniowski L., *Redukcja ryzyka działalności banku przez ochron ę fizyczną*, [w:] *Ryzyko w działalności banków komercyjnych*, red. J. Stacharska-Targosz, Poznań 2000, s. 161-174.

Kozdrowski S., *Wybrane zagadnienia kryminologii*, Słupsk 2000.

Ochrona danych osobowych, red. M. Wyrzykowski, Warszawa 1999.

Mesároš M., *Účinne organizovanie, riadenie a manažérske vedenie*, Košice 2001.

Palmer S., Weaver M., *Úloha informací v manažerském rozhodování*, Praha 2000.

Peciak J., *O utajnianiu mowy bez tajemnic*, Warszawa 1980.

Przestępcy czują się bezkarni, „Rzeczpospolita" 2002 (23 II).

Rozporządzenie Prezesa Rady Ministrów z dnia 25 lutego 1999 r. w sprawie podstawowych wymagań bezpieczeństwa systemów i sieci teleinformatycznych, (Dz.U. nr 18, poz. 162).

Rozporządzenie Rady Ministrów z dnia 9 lutego 1999 r. w sprawie organizacji kancelarii tajnych (Dz.U. nr 18, poz. 156).

Stefanowicz B., *Wybrane zagadnienia infologicznej analizy informacji*, Płock 1999.

Stoner J. A. F., Freeman R. E, Gilbert D. R. jr, *Kierowanie*, Warszawa 1997.

Tom P. L., *Managing Information as a Corporate Resource*, Glenview 1987.

Urbański K. R., *Chroń swój komputer*, „Rzeczpospolita" 2000 (15 V).

Ustawa z dnia 23 kwietnia 1964 r., Kodeks cywilny (Dz.U. nr 16, poz. 93 z późn. zm.)

Ustawa z dnia 26 czerwca 1974 r., Kodeks pracy (Dz.U. nr 24, poz. 141, tekst jedn. z późn. zm.).

Ustawa z dnia 6 kwietnia 1990 r. o Policji (Dz.U. nr 30, poz. 179 z późn. zm.).

Ustawa z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (Dz.U. nr 47, poz. 211 z późn. zm.).

Ustawa z dnia 10 czerwca 1994 r. o zamówieniach publicznych (Dz.U. z 1998 r., nr 119, poz. 773).

Ustawa z dnia 19 sierpnia 1994 r. o ochronie zdrowia psychicznego (Dz.U. nr 111, poz. 535 z późn. zm.).

Ustawa z dnia 29 września 1994 r. o rachunkowości (Dz.U. nr 121, poz. 591 z późn. zm.).

Ustawa z dnia 29 czerwca 1995 r. o statystyce publicznej (Dz.U. nr 88, poz.439 z późn. zm.).

Ustawa z dnia 2 czerwca 1997 r., Kodeks karny (Dz.U. nr 88, poz. 553 z późn. zm.).
Ustawa z dnia 22 sierpnia 1997 r. o ochronie osób i mienia (Dz.U. nr 114, poz. 740 z późn. zm.).
Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. nr 133, poz. 883 z późn. zm.).
Ustawa z dnia 29 sierpnia 1997 r., Ordynacja podatkowa (Dz.U. nr 137, poz. 926 z późn. zm.).
Ustawa z dnia 29 sierpnia 1997 r., Prawo bankowe (Dz.U. nr 140, poz. 939 z późn. zm.).
Ustawa z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych (Dz.U. nr 11, poz. 95).
Ustawa z dnia 15 września 2000 r., Kodeks spółek handlowych (Dz.U. nr 94, poz. 1037).
Ustawa z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz.U. nr 112, poz. 1198).
Varcholová T., *Manažérska analýza,* Bratislava 2001.
Zwierzchowski Z., *Najpierw bezpieczeństwo*, „Rzeczpospolita" 2000 (10 V).