ZESZYTY NAUKOWE POLITECHNIKI RZESZOWSKIEJ Nr 272
Zarządzanie i Marketing z. 17 (2/10) 2010

Mirosław WŁODARCZYK[1]

PROBLEMY ZARZĄDZANIA WIEDZĄ W PRZEDSIĘBIORSTWIE

Przedmiotem pracy są praktyczne aspekty zarządzania wiedzą. Przedstawiono podstawowe problemy działalności informacyjnej we współczesnej gospodarce i w ochronie wiedzy poufnej w przedsiębiorstwie. Wskazano główne różnice w działalności pomiędzy wywiadem gospodarczym i szpiegostwem gospodarczym. Poza działaniami techniczno-organizacyjnymi najlepszą ochronę wiedzy poufnej w przedsiębiorstwie zapewniają lojalni pracownicy.

1. ZNACZENIE I ŹRÓDŁA WIEDZY

Zasadniczymi czynnikami rozwoju współczesnej gospodarki są wiedza, kapitał finansowy, kapitał rzeczowy i zasoby ludzkie. Według Petera Druckera wiedza staje się jedynym zasobem ekonomicznym, a pozostałe czynniki są uzupełnieniem sił wytwórczych[2]. Wiedza ma też rzadko spotykaną właściwość, a mianowicie w miarę jej wykorzystywania nie zmniejsza się, lecz rośnie. W ujęciu potocznym terminy „wiedza" i „informacja" używane są zamiennie i traktowane jako synonimy, ale w rzeczywistości wiedza jest pojęciem szerszym. Według Alberta Einsteina do podstawowych elementów wiedzy należy informacja, która tworzy wiedzę razem z doświadczeniem:

wiedza = informacja + doświadczenie.

Dynamicznie rosnąca konkurencyjność w skali lokalnej, regionalnej i globalnej oraz koncentracja kapitału generują coraz większe zapotrzebowanie na informacje, a to sprzyja rozwojowi usług informacyjnych. Usługi informacyjne są przykładem szybko rozwijającego się outsourcingu. Towarzyszą temu bardziej efektywne metody gromadzenia informacji oraz ich przetwarzania. Należy zauważyć, że jednocześnie zwiększa się zainteresowanie nieuprawnionym (nielegalnym) przejęciem informacji jako jednym z bardziej skutecznych, choć nieetycznych, narzędzi walki konkurencyjnej.

Obserwacja otoczenia i zbieranie informacji należą do najstarszych rodzajów aktywności człowieka. Szczególnie duży wzrost zainteresowania informacją, zwłaszcza poufną, nastąpił w ubiegłym wieku w związku z szeroką skalą konfrontacji militarnych i nasileniem się konkurencji w gospodarce. Współcześnie dynamiczny rozwój gospodarki lokalnej, regionalnej i globalnej oraz koncentracja kapitału generują coraz większe zapotrzebowanie na informacje, bowiem pozyskanie informacji i jej przetworzenie mają decydujący wpływ na powodzenie przedsiębiorstwa na rynku. Można przyjąć, że wykorzystanie wiedzy pozwoliło na szybsze opanowanie aktualnej recesji w porównaniu z poprzednimi kryzysami.

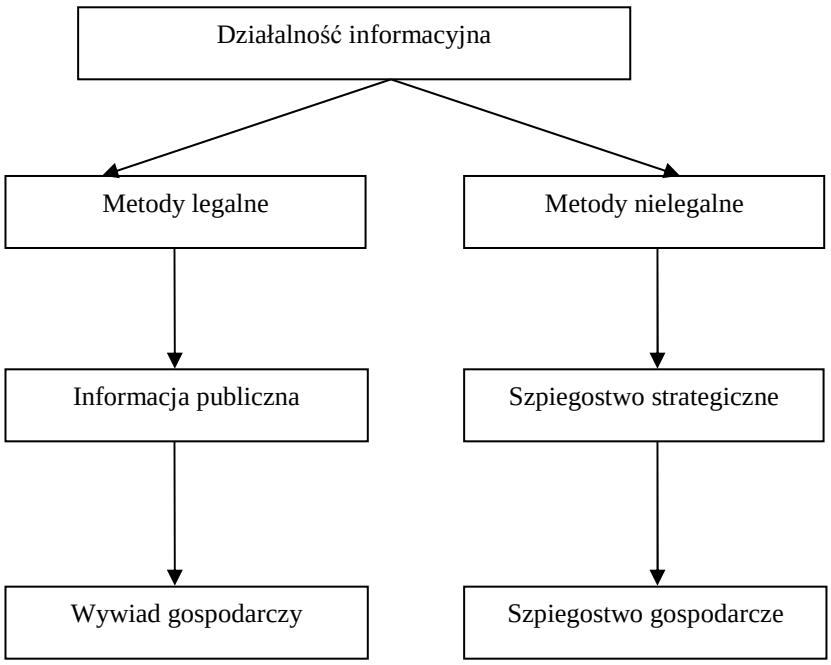
---

[1] prof. dr hab. inż. Mirosław Włodarczyk, Katedra Marketingu, Wydział Zarządzania, Społeczna Wyższa Szkoła Przedsiębiorczości i Zarządzania w Łodzi.

[2] P.F. Drucker, *Praktyka zarządzania*, Nowoczesność–Akademia Ekonomiczna w Krakowie, Kraków 1994, s. 73.

W działalności informacyjnej można wyróżnić:
- organizacje wyższej użyteczności (biblioteki, urzędy i agencje publiczne) wykonujące określoną misję społeczną,
- przedsiębiorstwa pozyskujące informacje na potrzeby własne,
- dostawców usług informacyjnych (ośrodki doradcze, wywiadownie gospodarcze, konsultanci itp.) z pewnego obszaru geograficznego, technicznego czy gospodarczego[3].

W klasyfikacji działalności informacyjnej rozróżniamy metody legalne i nielegalne. Następuje ich szybki rozwój dzięki popytowi na informacje i rozwojowi techniki, zwłaszcza technologii informatycznej i elektroniki. Ogromna liczba informacji jest pozyskiwana za pomocą działań legalnych, będących domeną wywiadu gospodarczego (*business intelligence*), nazywanego „białym wywiadem". Nawet CIA pozyskuje zresztą 80% danych z informacji publicznej. Natomiast metody nielegalne są wykorzystywane przez szpiegostwo gospodarcze (*corporate espionage*), określane jako „czarny wywiad". Są one niezgodne z prawem i nie powinny być akceptowane przez menedżerów. Jednocześnie coraz częściej podejmowane są działania zmierzające do ochrony zasobów wiedzy poufnej przedsiębiorstwa, które są domeną kontrwywiadu (*counter-intelligence*).



Rys. Klasyfikacja metod w działalności informacyjnej
Źródło: opracowanie własne.

[3] S. Forlicz, *Informacja w biznesie*, PWE, Warszawa 2008, s. 61.

Do podstawowych źródeł wywiadu gospodarczego należą:
- publikacje i patenty,
- rejestry sądowe, ewidencja działalności gospodarczej,
- urzędy i agencje publiczne,
- samorządy terytorialne,
- samorządy i stowarzyszenia zawodowe,
- roczniki statystyczne,
- targi i wystawy,
- literatura firmowa konkurentów,
- rozmowy z pracownikami konkurenta bez użycia kamuflażu,
- rozmowy z dostawcami i odbiorcami konkurenta,
- analiza produktów konkurenta.

Metody te nie wymagają dużych nakładów, dzięki czemu przedsiębiorstwa o mniejszych zasobach mogą je wykorzystać we własnym zakresie lub poprzez dostawców usług informacyjnych (np. wywiadownie gospodarcze). Dzięki stałej współpracy i znajomości potrzeb dostawcy mogą dostarczyć informacji bardziej użytecznych, a także uczestniczyć w ich przetwarzaniu. Metody działania szpiegostwa gospodarczego opisano poprzednio[4].

2. WIEDZA W DZIAŁALNOŚCI GOSPODARCZEJ

W działalności gospodarczej można wyróżnić:
- wiedzę materialną,
- wiedzę niematerialną.

Wiedza niematerialna (w pełni dostępna) służy poznaniu świata i zrozumieniu otaczających nas zjawisk. Wiedzę tę zdobywa się w trakcie nauczania oraz z różnych źródeł publikowanych, zarówno w wersji papierowej, jak i elektronicznej. Wiedza niematerialna ma charakter nieodpłatny i stanowi podstawę wszelkiej działalności intelektualnej. Wiedza materialna powstaje w badaniach stosowanych i pracach rozwojowych, posiada zazwyczaj charakter odpłatny i może powodować bezpośrednie konsekwencje gospodarcze. W miarę upływu czasu wiedza materialna traci swoją wartość ze względu na postęp techniczny.

Najważniejszym w działalności gospodarczej kryterium podziału wiedzy jest swoboda korzystania z niej, czyli dostęp do wiedzy. Według tego kryterium Wiesław Kotarba wyróżnia trzy kategorie wiedzy:
– wiedzę w pełni dostępną – wolną,
– wiedzę jawną chronioną,
– wiedzę niedostępną – utajnioną.

Wiedza materialna obejmuje wiedzę jawną chronioną i wiedzę utajnioną (poufną). Wiedzę jawną chronioną stanowi wiedza, która na danym terytorium i w danym czasie podlega ochronie prawnej na korzyść określonego podmiotu. Inne podmioty mogą poznać jej treść, ale nie mogą tego wykorzystać w działalności gospodarczej bez zgody właścicie-

[4] M. Włodarczyk, *Metody działania wywiadu gospodarczego*, [w:] *Zarządzanie przepływem i ochroną informacji*, red. M. Kwieciński, Krakowska Szkoła Wyższa im. Andrzeja Frycza Modrzewskiego, Kraków 2007, s. 111.

la[5]. Do wiedzy w pełni dostępnej zalicza się także tę wiedzę chronioną, której ochrona ustała z różnych przyczyn, na przykład ze względu na wygaśnięcie okresu ochrony prawnej.

Natomiast na wiedzę poufną składają się informacje produkcyjne, handlowe lub organizacyjne, których przedsiębiorstwo nie ujawnia publicznie w obawie przed potencjalną konkurencją. Przedmiotem szczególnego zainteresowania konkurentów jako najbardziej pożądane są:

- wyniki prac rozwojowych i testów nowych produktów,
- planowane porozumienia o współpracy strategicznej,
- szczegóły umów handlowych,
- opisy wynalazków i wzorów użytkowych przed ich zgłoszeniem do urzędu patentowego.

Zakres wiedzy chronionej zależy od uznania, co stanowi istotę przewagi konkurencyjnej przedsiębiorstwa[6]. Przedmiotem ochrony w przedsiębiorstwie wykorzystującym nowoczesną technologię powinna być wiedza poufna, określana zwykle jako *know-how*. Obejmuje ona doświadczenia produkcyjne i specyficzne umiejętności nabyte w realizacji określonych procesów. Ochrona tej wiedzy należy do podstawowych zadań przedsiębiorstwa przemysłowego. Dla przedsiębiorstwa handlowego ważne są warunki współpracy z dostawcami, a zwłaszcza szczegóły finansowe umów. Oprócz *know-how* zainteresowanie konkurentów możliwościami nielegalnego pozyskania informacji dotyczy informacji poufnej typu: *know-who, know-what, know-where, know-when* („wiedzieć kto, co, gdzie, kiedy")[7]. Wprawdzie zachowanie ich poufności i aktualności jest utrudnione w dłuższym okresie czasu, ale nie wyklucza to usilnych starań konkurentów zainteresowanych ich szybkim pozyskaniem.

Drobne informacje ze źródeł legalnych wymagają pogłębienia i wyższych kompetencji, wspomaganych specjalną techniką. Wówczas łatwo jest przekroczyć granice etyczne i przepisy prawne „Ustawy z 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji"[8]. Według przywołanej ustawy „czynem nieuczciwej konkurencji jest przekazanie, ujawnienie lub wykorzystanie cudzych informacji stanowiących tajemnicę przedsiębiorstwa albo ich nabycie od osoby nieuprawnionej, jeżeli zagraża[ją] lub narusza[ją] interes przedsiębiorcy" (art. 11). Tajemnicę przedsiębiorstwa stanowi informacja spełniająca jednocześnie trzy przesłanki:

- nie została przedstawiona do wiadomości publicznej,
- obejmuje dane techniczne, technologiczne, organizacyjne lub inne,
- przedsiębiorstwo podjęło odpowiednie działania w celu zapewnienia poufności informacji.

Informacja poufna przedsiębiorstw jest przedmiotem ciągłego zainteresowania konkurencji i stała się poszukiwanym towarem. Popyt na wiedzę stanowiącą tajemnicę przedsiębiorstw pobudza do działań niezgodnych z prawem, czyli jest stymulatorem rozwoju szpiegostwa gospodarczego[9].

---

[5] W. Kotarba, *Zarządzanie wiedzą chronioną w przedsiębiorstwie*, Instytut Organizacji i Zarządzania w Przemyśle „ORGMASZ", Warszawa 2001, s. 18.

[6] M. Kwieciński, *Mapy zagrożeń w ochronie wiedzy*, [w:] *Zarządzanie przepływem i ochroną informacji*, red. M. Kwieciński, Krakowska Szkoła Wyższa im. Andrzeja Frycza Modrzewskiego, Kraków 2007, s. 177.

[7] C. Evans, *Zarządzanie wiedzą*, PWE, Warszawa 2003.

[8] Ustawa z 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (DzU 1993, nr 47, poz. 211 ze zm.).

[9] B. Martinet, Y.-M. Marti, *Wywiad gospodarczy. Pozyskiwanie i ochrona informacji*, PWE, Warszawa 1999, s. 159.

Jak już zaznaczono wcześniej, metody nielegalne nie powinny być akceptowane przez menedżerów. W praktyce zamawiający deklaruje w umowie zainteresowanie informacją pochodzącą ze źródeł legalnych, co wyłącza jego odpowiedzialność karną w razie dekonspiracji agenta, gdyż zgodnie z kodeksem karę ponosi naruszający prawo. Odpowiedzialność cywilna nabywcy nie jest jednak zupełnie wykluczona, gdyż „sąd może zobowiązać nabywcę do zapłaty stosownego wynagrodzenia za korzystanie…" na mocy art. 11 przywołanej ustawy.

3. OCHRONA WIEDZY POUFNEJ PRZEDSIĘBIORSTWA

Zarządzanie wiedzą staje się szczególnie złożonym procesem ze względu na intensywne i ciągłe zmiany w otoczeniu. Konieczne jest nieustanne dostosowywanie się do turbulentnego otoczenia i wykorzystywanie wiedzy całego personelu, a nie tylko zarządu. Pracownicy są depozytariuszami kompetencji przedsiębiorstwa i każdy system ochrony wiedzy powinien opierać się na ich zaufaniu i lojalności. Z reguły przedsiębiorca uprzedza pracownika o obowiązku zachowania poufności informacji odbierając jednocześnie pisemne zobowiązanie o obowiązku jej zachowania w okresie trwania stosunku pracy i przez okres trzech lat od jego ustania. Czasem zawiera się dodatkowe porozumienie z pracownikiem o zakazie konkurencji, ale warto przy tym poddać analizie opłacalność takiej umowy ze względu na ponoszone koszty i ewentualne straty w przypadku nielojalności pracownika.

Ciągłe i kosztowne inwestowanie przedsiębiorcy w zabezpieczenia systemu informatycznego nie będzie efektywne, jeśli przedsiębiorstwo nie posiada lojalnych pracowników, traktujących ochronę tajemnicy przedsiębiorstwa jak własny interes. Profesjonaliści są zgodni w ocenie, że największym zagrożeniem w ochronie informacji poufnej są pracownicy, niezależnie od zajmowanego stanowiska. Może to wynikać z ich gadulstwa, nieostrożności lub niedostatku wiedzy w zakresie ochrony informacji, ale należy także brać pod uwagę możliwości szantażu i działania z chęci zysku. Ochrona informacji poufnej przedsiębiorstwa należy do podstawowych obowiązków pracowników na każdym szczeblu. W przypadku trudności z zachowaniem pozycji przedsiębiorstwa i wdrożenia programu oszczędnościowego pojawiają się cięcia kosztów osobowych, co powinno być utrwalone w świadomości pracowników.

Poznanie zagrożeń jest pierwszym krokiem do opracowania zasad bezpieczeństwa informacji w przedsiębiorstwie opartych na:

- poufności,
- integralności,
- dostępności informacji[10].

Poufność polega na dostępie do informacji dla ograniczonej liczby pracowników. Integralność informacji polega na jej kompletności i dokładności, a dostępność oznacza otrzymanie informacji przez upoważnionego pracownika w rozsądnym czasie bez jej zatajenia. Realizacja tych zasad w praktyce będzie wymagała podejmowania istotnych decyzji – na przykład, czy uczestnik projektu może uzyskać bezpośredni dostęp do określonego zbioru informacji, czy też pośredni poprzez koordynatora projektu. Decyzja powinna być oparta na analizie ewentualnych zysków i strat, gdyż ograniczenie przepływu

[10] J. Chmielewski, *Czy ochrona informacji firmy to wyłączny interes pracodawcy?*, „Przegląd Organizacji" 2006/2.

informacji poprzez określenie licznych poziomów dostępu może opóźniać realizację zadań, a w krańcowym przypadku obniżać jakość projektu. Działanie kierownictwa powinno skupiać się na zapewnieniu warunków do nieformalnej komunikacji wewnętrznej, gdyż przyczynia się ona do lepszego wykorzystania zasobów przedsiębiorstwa.

Przedmiotem permanentnego zainteresowania konkurentów pozostają warunki współpracy z dostawcami i głównymi odbiorcami produktów, w tym rabaty, warunki płatności, perspektywy wspólnych przedsięwzięć oraz inne informacje, które wpływają na osiągnięcie przewagi na rynku. Aby zapewnić systemową ochronę zasobów, należy przeprowadzić audyt bezpieczeństwa informacji w przedsiębiorstwie. Często zarząd nie przykłada dostatecznej uwagi do tego zagadnienia, uznając istniejącą sytuację za zadowalającą. Warto zwrócić uwagę na rzutkich pracowników, którzy mają dostęp do wielu informacji poufnych, a ich ambicje mogą być niezaspokojone. Dlatego należy zapoznać się z CV pracowników i sprawdzić określone fakty istotne dla ich postaw. Pobieżne sprawdzanie CV jest zazwyczaj formalnością, która w istocie wnosi niewiele do analizy potencjalnych zagrożeń. Tymczasem zatrudnienie profesjonalnego agenta lub własnego pracownika u konkurenta jest jedną z metod nielegalnego pozyskiwania informacji. Inne znane i nielegalne metody opisano poprzednio[11].

Źródła osobowe są i będą ważnym dostawcą informacji, zwłaszcza te wyposażone w łatwy dostęp do systemu informatycznego. System ten może być także atakowany z zewnątrz, co stwarza zagrożenia dla informacji i wiedzy poufnej przedsiębiorstwa. Do nich należą: nieautoryzowany dostęp, modyfikacja lub zniszczenie informacji w wyniku włamania do systemu teleinformatycznego. Wykorzystanie sieci teleinformatycznej w komunikacji z otoczeniem bez skutecznego jej zabezpieczenia przed nieuprawnioną ingerencją powoduje duże szkody dla klientów i przedsiębiorstwa. Wielkość strat powstających z tego tytułu może być trudna do oszacowania z powodu różnicy wartości i przeznaczenia informacji oraz czasu występowania zagrożenia. Z reguły przedsiębiorstwa niechętnie przyznają się do strat w obawie przed ujawnianiem słabości systemu i utraty zaufania klientów.

Poważnym zagrożeniem jest wywiad elektroniczny, który stanowi podstawę systemu nielegalnego pozyskiwania informacji, czyli szpiegostwa. Nielegalne metody obejmują:

- podsłuch systemów teleinformatycznych,
- montaż transmiterów w komputerach,
- analizę promieniowania elektromagnetycznego z urządzeń komputerowych,
- analizę mikrofal łączności satelitarnej,
- szantaż i sabotaż komputerowy[12].

Należy podkreślić, że dostępność niektórych z nich jest ograniczona ze względu na wysokie koszty. Nie dotyczy to podsłuchu systemu teleinformatycznego, który nie wymaga kosztownych urządzeń. Emisję mikrokomputera można zarejestrować nawet z odległości kilku kilometrów. Rozróżniamy podsłuch aktywny lub pasywny. Podsłuch aktywny wiąże się z ingerencją w przesyłane wiadomości, ich zawartość lub kolejność. Natomiast w podsłuchu pasywnym można tylko stwierdzić ruch w sieci lub poznać treść informacji. Przeciwdziałanie podsłuchowi poprzez zmniejszenie mocy emisji nie jest skuteczne, ponieważ znane są przypadki rejestracji informacji w samochodzie osobowym na parkingu przedsiębiorstwa. Jest to znacznie mniej kłopotliwa metoda niż podsłuch

[11] M. Włodarczyk, *op. cit.*, s. 109.

[12] *Ibidem*, s. 113.

telefoniczny, choć niewątpliwie czasochłonna. Włamanie przez bezprzewodową sieć komputerową jest groźniejsze niż z Internetu, gdyż trudniej je wykryć. Po włamaniu z Internetu pozostaje adres intruza, natomiast wykorzystanie sieci bezprzewodowej prawie nie pozostawia śladu. Aby zapobiegać takim zagrożeniom, nie należy używać bezprzewodowych sieci komputerowych w sprawach poufnych. Skuteczną ochronę transmisji informacji poufnych zapewnia kodowanie, ale nie jest często stosowane z różnych względów. Przeciwnicy kodowania i dekodowania informacji zwracają m.in. uwagę na możliwość występowania zakłóceń, co oczywiście może się zdarzać, ale w rzeczywistości nie stanowi większego problemu.

Kolejnym zagrożeniem dla zasobów informacji przedsiębiorstwa jest upowszechnienie telefonów komórkowych z kamerami i aparatami fotograficznymi, gdyż w praktyce nie ma możliwości ciągłego monitorowania wszystkich pracowników. Dlatego zakaz używania aparatów komórkowych na stanowiskach pracy wprowadza coraz większa liczba pracodawców, m.in. Samsung, Volkswagen, Departament Stanu USA. Zagrożeniem dla bezpieczeństwa informacji mogą stać się kontakty ze środkami masowego przekazu, jeśli pracownik nie jest przeszkolony w zakresie ochrony wiedzy poufnej. Prawo do informacji publicznej zapewnia się poprzez powołanie rzecznika prasowego odpowiadającego za oficjalne kontakty zewnętrzne. Komunikaty przekazywane przez rzecznika powinny być wcześniej opracowane w kontekście zachowania bezpieczeństwa informacji. Odpowiednia treść i zwięzłość komunikatu sprzyjają zainteresowaniu uczestników spotkania i zadawaniu dodatkowych pytań, co może stanowić pewną korzyść dla przedsiębiorstwa jako informacja zwrotna.

4. PODSUMOWANIE

Współczesna technika umożliwia nieuprawnione przejmowanie wiedzy poufnej przedsiębiorstw, których zarząd i pracownicy nie są świadomi zagrożeń występujących w otoczeniu. Do podstawowych błędów popełnianych przez zarządzających należy rezygnacja z profesjonalnego audytu bezpieczeństwa informacji w przedsiębiorstwie oraz zbyt mała uwaga skierowana na szkolenie personelu w zakresie ochrony wiedzy. Słabym ogniwem w ochronie wiedzy przedsiębiorstwa pozostają pracownicy niezadowoleni z ich pozycji w przedsiębiorstwie lub zainteresowani uzyskaniem korzyści materialnych w zamian za tajemnice przedsiębiorstwa przekazane konkurentom. Najlepszy system bezpieczeństwa informacji będzie zawodny bez lojalnych pracowników, identyfikujących się z przedsiębiorstwem i dysponujących wiedzą o potencjalnych zagrożeniach. Paradoksem jest teza, że największym zagrożeniem i jednocześnie najlepszym obrońcą poufności tajemnic przedsiębiorstwa pozostaje personel.

LITERATURA

[1] Chmielewski, J., *Czy ochrona informacji firmy to wyłączny interes pracodawcy?*, „Przegląd Organizacji" 2006/2
[2] Drucker, P.F., *Praktyka zarządzania*, Nowoczesność–Akademia Ekonomiczna w Krakowie, Kraków 1994
[3] Evans, C., *Zarządzanie wiedzą*, PWE, Warszawa 2003
[4] Forlicz, S., *Informacja w biznesie*, PWE, Warszawa 2008
[5] Kotarba, W., *Zarządzanie wiedzą chronioną w przedsiębiorstwie*, Instytut Organizacji i Zarządzania w Przemyśle „ORGMASZ", Warszawa 2001

[6] Kwieciński, M., *Mapy zagrożeń w ochronie wiedzy*, [w:] *Zarządzanie przepływem i ochroną informacji*, red. M. Kwieciński, Krakowska Szkoła Wyższa im. Andrzeja Frycza Modrzewskiego, Kraków 2007
[7] Martinet, B.; Marti, Y.-M., *Wywiad gospodarczy. Pozyskiwanie i ochrona informacji*, PWE, Warszawa 1999
[8] Ustawa z 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (DzU 1993, nr 47, poz. 211 ze zm.)
[9] Włodarczyk, M., *Metody działania wywiadu gospodarczego*, [w:] *Zarządzanie przepływem i ochroną informacji*, red. M. Kwieciński, Krakowska Szkoła Wyższa im. Andrzeja Frycza Modrzewskiego, Kraków 2007

METHODICAL PROBLEMS IN MEASUREMENT OF ENTERPRISE COMPETITIVE ADVANTAGE

Current state of discussion on measurement methods of enterprise competitive advantage has been presented. It has been emphasized that extraordinary economic results of enterprise in the sector are not identical with the possession of competitive advantage. Measurement of competitive advantage should be carried out in many stages focusing on the analysis of dependence: resources – main business processes – competitive advantage – success (results) of enterprise. Such methodical approach in competitive advantage quantification would be able to utilize in practice the elements of various theoretical ideas, namely the resource-based-approach (in competence perspective) and the contingency approach.