

**Mirosław KWIECIŃSKI**

Krakowska Akademia im. Andrzeja F. Modrzewskiego

## **KONCEPCJA WYKORZYSTANIA WYWIADU I KONTRWYWIADU GOSPODARCZEGO W ZACHOWANIU BEZPIECZEŃSTWA INTELEKTUALNEGO**

### **Wstęp**

Globalizacja wywołana zasadniczo przez dynamiczny rozwój Informacyjnej Technologii zdecydowanie zdynamizowała ekspansywność przedsiębiorstw oraz rywalizację o klienta na rynku. Eksplozja rywalizacji w gospodarce spowodowała rozszerzenie współzawodnictwa o prymat również na systemy państw i społeczeństw. Rozwój nowych form rywalizacji, wywołany fundamentalną rolą informacji uświadomił menadżerom, jak wielkie znaczenie w prowadzeniu działań ofensywnych ma zachowanie bezpieczeństwa przedsiębiorstw. Fundamentalne miejsce zajmuje tu bezpieczeństwo intelektualne. Ponieważ zarówno w teorii, jak i praktyce zarządzania organizacjami zauważa się zarówno podejście procesowe, jak i produktowe, problem zachowania bezpieczeństwa w ekspansywnej działalności przedsiębiorstw należy także zwrócić uwagę z obu punktów widzenia.

Cykl życia organizacji wskazuje wyraźnie, jak podstawową rolę wyznacza się fazie wzrostu i (w konsekwencji) dojrzałości. Ale zarządzania organizacją to w konsekwencji permanentne zarządzanie kryzysowe. Każdej bowiem fazie, a szczególnie fazie rozwoju, towarzyszą kryzysy. Ich przełamywanie stanowi esencją umiejętności i doświadczeń menedżerów. Wśród centralnych zagadnień związanych z rosnącą ekspansją działalności przedsiębiorstw znajduje się troska o zachowanie bezpieczeństwa organizacji. Łatwo bowiem odsunąć, w niezwykle dynamicznych staraniach o poszerzenie udziału w rynku i wzrost liczby klientów, niejako na plan drugi, problem zachowania bezpieczeństwa w nowej już sytuacji przedsiębiorstwa. W tym zakresie menadżerowie powinni z dużą uwagą obserwować zmiany w strukturze zasobów i zachowań pracowników przedsiębiorstwa. Służyć to ma dążeniu do zachowania równowagi w relacjach pomiędzy organizacją a jej otoczeniem, a także zachowaniu niezbędnej dla dalszej pomyślnej ekspansji, właściwej struktury zasobów przedsiębiorstwa. Konieczność podjęcia bez zbędnej zwłoki niezbędnych zmian uchroni przedsiębiorstwo od sytuacji przełamywania pojawiających się w przyszłości barier, a także stanowić będzie o dalszych dobrych podstawach wyjściowych do prowadzenia działań ekspansywnych. Jest to zatem obszar permanentnej restrukturyzacji zasobów w sytuacji dynamicznego rozwoju przedsiębiorstwa.

Zgodnie z klasyczną teorią zarządzania firmy powinny wykorzystać posiadaną wiedzę czy zasoby w nowych obszarach działalności i czerpać z tego korzyści. Trudno jednak stwierdzić, który z zasobów - relacje z klientami, produkt, czy też inne kompetencje - należy rozwijać. Trudno jest także znaleźć równowagę między wymaganiami związanymi z bieżącym prowadzeniem firmy a rozwijaniem działalności w nowych obszarach. Na szybko zmieniającym się rynku trzeba wprowadzać innowacje i dywersyfikować działalność, aby utrzymać osiągniętą pozycję, ale pamiętając, że zawsze istnieje ryzyko nadmiernej dywersyfikacji. Jest to zaledwie

tylko jeden z przejawów zagrożeń i element starań o zachowanie niezbędnego poziomu bezpieczeństwa.

### **Wywiad gospodarczy – współczesne narzędzie ekspansji przedsiębiorstw**

Współczesny biznes prowadzony w ramach różnorodnych organizacji gospodarczych pełen jest różnorodnych zagrożeń, wynikających zasadniczo z gwałtownych zmian w otoczeniu. Istnieje co prawda efektywne narzędzie identyfikacji zagrożeń w postaci wywiadu gospodarczego, pozwalające na zrozumienie istoty, kierunku i tempa zmian w biznesie prowadzonym w otoczeniu przedsiębiorstwa, ale uprawianie samego wywiadu gospodarczego nie eliminuje wszelkich zagrożeń. Centralnym zatem problemem, tkwiącym przed menadżerami każdego przedsiębiorstwa jest zapewnienie niezbędnego minimum bezpieczeństwa.

Spójrzmy jednakże na możliwości, jakie stwarza **wywiad gospodarczy**. Zrozumienie koncepcji wywiadu gospodarczego napotyka na wiele trudności. Zasadniczym elementem sporu jest sam termin „wywiad”. Powszechnie utożsamiany jest on ze szpiegostwem czy w ogóle z nielegalnym pozyskaniem niedostępnych innymi sposobami informacji oraz działaniem przy zachowaniu całkowitej tajności.<sup>1</sup> Także traktowanie wywiadu gospodarczego jako zespołu działań o ukształtowanej sekwencji: pozyskiwanie – gromadzenie – przetwarzanie – rozpowszechnianie w celu gospodarczego wykorzystania wydaje się być zbyt ogólne i nieprecyzyjne.<sup>2</sup> Pojawia się także określenie wywiadu gospodarczego jako „przeanalizowana informacja”.<sup>3</sup> Wydaje się, że kluczem do zrozumienia terminu „wywiad gospodarczy” może być właściwe polskie tłumaczenie terminu *intelligence*, ma on bowiem wielorakie znaczenie. Przede wszystkim termin *intelligence* odnosi się bardziej do procesu i zdolności uczenia się przedsiębiorstwa, jak uporać się z nową lub skomplikowaną sytuacją, do zdolności nabywania wiedzy o otoczeniu własnym i konkurentów, jak myśleć kwintesencjonalnie. To także analityczny proces (oraz jego finalny produkt) przekształceń informacji w zastosowaną w praktyce wiedzę o możliwościach (potencjale), zamiarach (intencjach), osiągnięciach i pozycji przede wszystkim uczestników rywalizacji konkurencyjnej.<sup>4</sup>

*Competitive Intelligence (CI)* należy zatem traktować jako zbiór idei, metod i procesów wspomagających podejmowanie decyzji biznesowych w drodze planowanego i świadomego przetwarzania informacji z różnych źródeł, wykorzystywanie zgromadzonego w przedsiębiorstwie doświadczenia i wiedzy dla właściwego rozumienia i przewidywania dynamiki biznesu. Takie podejście do rozumienia wywiadu gospodarczego uprawnia do traktowania go także jako specyficznego i niepowtarzalnego systemu informacji strategicznej (SIS).<sup>5</sup>

<sup>1</sup> zob. np. *Encyklopedia szpiegostwa*. Warszawa 1995, s. 281; podaję za: K. Materska: *Wywiad gospodarczy z perspektywy informacji naukowej*. W: R. Borowiecki, M. Kwieciński (red.): *Zarządzanie zasobami informacji w przedsiębiorstwie. Ku przedsiębiorstwu przyszłości*. Warszawa 2001, s. 326

<sup>2</sup> zob. B. Martinet, Y. Marti: *Wywiad gospodarczy. Pozyskiwanie i ochrona informacji*. Warszawa 1999, s. 12

<sup>3</sup> zob. M. Kaliski, P. Mroziak: *Tworzenie efektywnego systemu wywiadu gospodarczego*. W: R. Borowiecki, M. Kwieciński (red.): *Informacja w zarządzaniu przedsiębiorstwem. Pozyskiwanie, wykorzystanie i ochrona*. Kraków 2003, s. 380

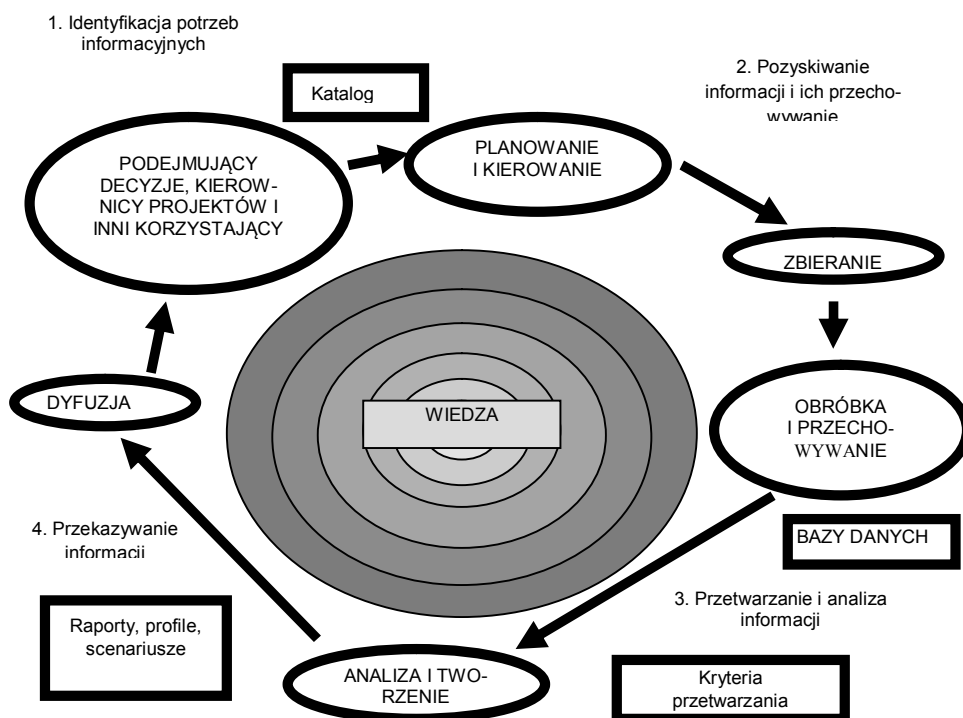
<sup>4</sup> zob. K. Materska, op. cit., s. 326

<sup>5</sup> Ibidem

Tak specyficzny i złożony system przetwarzania informacji wymaga swego rodzaju oprzyrządowania, wyznaczonego strukturą działań. Jego istotą jest koncentrowanie się na takich działaniach, które można nazwać „inteligencją na bazie informacji”. Wymagają one sekwencyjnego ujęcia (rys.1).

Niewątpliwie wywiad gospodarczy wiąże się z funkcjonowaniem przedsiębiorstwa. Poprzez uporządkowanie wiedzy o jego otoczeniu, nadaje on wszelki sens działaniu, wyznacza kierunki rozwoju. W tej dziedzinie zatem konieczne jest zachowanie następujących działań:

- permanentne zdobywanie (i gromadzenie) wiedzy o otoczeniu;
- ukierunkowanie (selekcja, filtrowanie) pozyskiwania informacji i sygnałów, przy wykorzystaniu różnorodnych metod oraz zachowaniu niezbędnej szybkości;
- mądre (otwarte), pozbawione schematycznych podejść, analizowanie (przetwarzanie) materiału informacyjnego, stawiające na uzyskanie konkretnej wartości (dodanej) dla użytkownika, a pozwalające przy tym wykorzystać cały zasób wiedzy zgromadzonej dotychczas w przedsiębiorstwie oraz istniejące struktury zarządzania wiedzą;
- przekazanie (dostarczenie) informacji określonej odbiorcy z grona kadry menedżerskiej, dostosowane do jego osobistej jak najlepszej recepcji i percepcji.



**Rysunek nr 1.** Sekwencyjne ujęcie struktury działań wywiadu gospodarczego w przedsiębiorstwie

Źródło: opracowanie własne na podstawie M. Kaliski, P. Mrozik: *Tworzenie...*, op. cit., s. 384

Efektem działań wywiadu gospodarczego jest stale powiększany zasób wiedzy o otoczeniu przedsiębiorstwa. Jest to możliwe wskutek generowania różnorodnych produktów wewnętrznych wywiadu. Przykładowy zestaw takich produktów przedstawia poniższa tabela.

<i>Nazwa produktu</i>	<i>Kryterium podziału</i>	<i>Treść</i>
<b>bazy danych</b>	przedmiotowe	Profile konkurentów i ich historia, profile osobowe menedżerów konkurencji, opisy techniczne zakładów konkurencji
	geograficzne	Jak wyżej według województw, krajów, kontynentów, mapy regionów działania konkurencji
<b>raport</b> (wymaga skupienia natychmiastowej uwagi)	częstotliwość	Regularne: cotygodniowy, comiesięczny Nieregularne: np. Flash Raports (raporty alarmowe)
	odbiorcy	Członkowie zarządu, twórcy projektów
	stopień szczegółowości	Cała branża, konkretna firma, wybrane zdarzenie
<b>scenariusz</b> (wymaga dystansu, dłuższej refleksji)		Scenariusze na przyszłość, przeglądy trendów

**Tabela nr 1.** Przykładowy zestaw produktów wewnętrznych wywiadu gospodarczego  
Źródło: opracowanie własne na podstawie M. Kaliski, P. Mroziak: *Tworzenie...*, op. cit. oraz K. Materska: *Wywiad...*, op. cit.

Przedstawione przykłady produktów wywiadu gospodarczego zwykle charakteryzują się ewolucją zgodnie z potrzebami wynikającymi ze zmieniającego się otoczenia. Doskonaleniu podlega także sposób dostarczania poszczególnym odbiorcom potrzebnych informacji.

Jak już wspomniano, wszelką podstawę budowania przewag konkurencyjnych przedsiębiorstwa stanowi informacja. Wartość poszczególnych informacji nie jest jednak jednakowa, stąd kryterium, które należy tu zastosować, to uznanie danej informacji za informację strategiczną, mogącą mieć szczególną wartość, zasadniczo dla konkurentów, ale także dla klientów, dostawców lub banków. Przez informację strategiczną można najogólniej rzecz biorąc uznać każdą informację, której rozpowszechnianie lub ujawnianie może spowodować utratę przewagi konkurencyjnej. Przy tej okazji mogą ujawnić się pewne związki przyczynowo-skutkowe, które mogą mieć charakter:

- bezpośredni (np. ujawnienie terminu wprowadzenia nowego produktu na rynek);
- pośredni (rzucenie fałszywej pogłoski, która może spowodować popsucie dobrego klimatu współpracy między przedsiębiorstwami).

Prowadzenie zadań wywiadowczych w ramach realizowanego cyklu prowadzi zwykle do uzyskania wielu cennych informacji o prowadzonym przez konkurentów procesie obserwacji i identyfikacji działań „naszego” przedsiębiorstwa. Stwarza to okazję do wykształcenia narzędzia kontrwywiadu gospodarczego.

### **Kontrwywiad gospodarczy – skuteczne narzędzie ochrony przewagi konkurencyjnej**

Zakres ważnych informacji, wyrażających charakter przewagi konkurencyjnej będzie zmieniać się w zależności od uznania, co stanowi treść owej przewagi. Do przykładów tego stanu rzeczy można zaliczyć:

- istotę (właściwość) działalności przedsiębiorstwa, co wiąże się z określeniem wszelkich zagrożeń ciążących nad jego działalnością. Trudno tu zatem wskazać na uniwersalne informacje pod względem ważności, ponieważ dla przedsiębiorstwa przemysłowego stosującego nowoczesne technologie przewagą konkurencyjną będzie wyłączność procesu produkcji, z kolei dla dystrybutora będą to specyficzne warunki umów handlowych z dostawcami lub spedytorami;
- strategię przedsiębiorstwa, która ulega przewartościowaniu w zależności od fazy rozwoju, co skutkuje zmianami w skali wartości informacji. I tak na przykład informacja o zatrudnieniu menedżera wyspecjalizowanego w innej niż dotychczas realizowana specyfika działalności danego przedsiębiorstwa staje się informacją ważną, chociaż wiąże się ze zwykłym anonsem prasowym o poszukiwaniu pracownika (specjalisty);
- czynnik czasu, który odgrywa istotną rolę w procesie wywiadu gospodarczego, szczególnie w warstwie wartości samych informacji, a także ich poufności. O wartości informacji decyduje moment czasowy, dla którego posiada ona szczególne znaczenie – informacja spóźniona staje się bezużyteczna.

Oprócz informacji ważnych dla całego przedsiębiorstwa ze względów strategicznych, istnieją informacje istotne dla jego działów, które mogą stać się obiektem przecieków lub specyficznych działań wywiadu gospodarczego. Do takich komórek należą przede wszystkim dział badań i rozwoju, który jest narażony jako obiekt ataku z powodu rodzaju prowadzonych tam działań i sposobu funkcjonowania, a także dział produkcji (wydział produkcji). Ten z kolei powinien być chroniony poprzez utrudnioną łączność (komunikację) z zewnątrz, ścisłą kontrolę wstępu na teren wydziałów produkcyjnych oraz informowaniu przełożonych o każdej próbie udzielenia wywiadu (np. w postaci pozwolenia na zwiedzanie, lub zrobienia raportu). Także wszelki ruch personelu przedsiębiorstwa związany ze zwolnieniami, odejściem na emeryturę, zatrudnieniem stażystów, pracowników na czas ściśle określony musi podlegać ścisłym rygorom ochrony informacji. Chodzi tu zwłaszcza o przeciwdziałanie wydostawaniu się ważnych dokumentów poza teren przedsiębiorstwa.

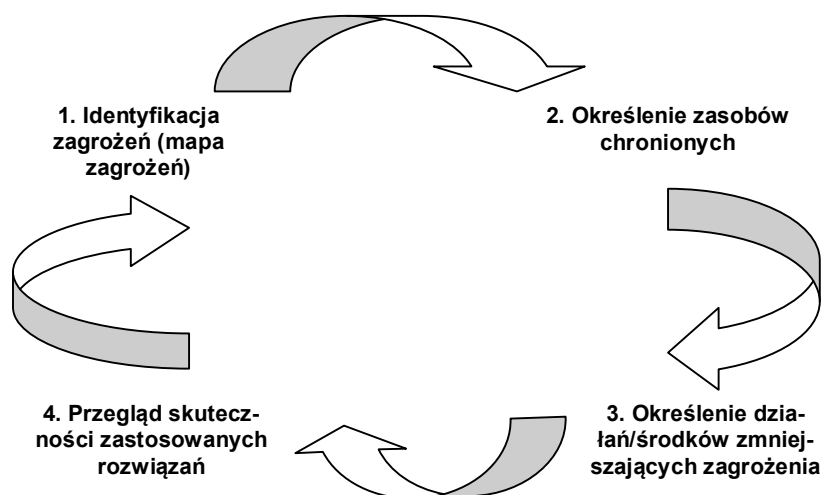
Cały system bezpieczeństwa informacyjnego powinien być należycie zorganizowany, na podstawie podejścia, które można określić jako działowe. Oznacza to, że bezpieczeństwo pomieszczeń zapewnione powinno być przez firmę ochroniarzkie (wsparte np. przez systemy kamer telewizyjnych), składanie i ochrona patentów – przez dział badań i rozwoju, bezpieczeństwo komputerowe – przez dział informatyki, itd. Taki system zabezpieczeń (kontrwywiadu) powinien być centralnie koordynowany i kontrolowany, co może pozwolić mu na lepszą ochronę informacji, w przeciwieństwie do struktury rozproszonej, która jest źródłem przecieków i utraty informacji. Zadanie takie można powierzyć osobie centralnie odpowiedzialnej za:

- wprowadzenie i utrzymywanie skutecznego systemu ochrony informacji;

- zbieranie, klasyfikowanie i wykorzystywanie sporządzonych przez ogół różnego rodzaju działów raportów dotyczących incydentów związanych z wtargnięciem w system informacyjny przedsiębiorstwa.

Oczywiście w celu zwiększenia efektywności centralizacji działań w tym zakresie potrzebne jest przeszkolenie pracowników w dziedzinie ochrony informacji, jej znaczenia dla przedsiębiorstwa, a także metod postępowania. Organizacja ochrony informacji może także w przedsiębiorstwie przyjąć formę sieci odpowiedników w różnych działach, które funkcjonowałyby według precyzyjnych ustalonych procedur (np. raporty dotyczące incydentów związanych z wtargnięciem, okresowe szkolenia itp.). Wszelkie informacje wydostające się na zewnątrz powinny prowadzić zawsze przez ten sam kanał, na przykład przez dział rzecznika prasowego. Komórka ochrony informacji, która także musiałaby powstać jako odrębny dział byłaby naturalną kontynuacją działań komórki wywiadu gospodarczego, obie jednak będą związane stałą współpracą.

Sprawność działania systemu bezpieczeństwa organizacji wynika z przestrzegania reguł wynikających z cyklu zarządzania bezpieczeństwem. Katalog zagrożeń traktowany jako identyfikacja zagrożeń uruchamia cykl zarządzania bezpieczeństwem (rysunek 2).



**Rysunek nr 2.** Cykl zarządzania bezpieczeństwem organizacji

Źródło: J. Grzechowiak: *Mapa zagrożeń*. „CSO Magazyn Zarządzających Bezpieczeństwem” 2005, nr 1, s. 11

Sporządzenie katalogu zagrożeń wymaga zebrania wielu ważnych informacji, pozwalających menedżerom ds. bezpieczeństwa scharakteryzować podatność organizacji na wszelkie niebezpieczeństwa. Analiza zebranego materiału informacyjnego powinna pozwolić udzielić odpowiedzi na następujące pytania:

- jak przedstawia się ocena poziomu zagrożeń formułowana przez odpowiedzialne za bezpieczeństwo instytucje i służby państwowe, media, instytucje analityczne, firmy ochrony i towarzystwa ubezpieczeniowe;

- czy chronione zasoby przedstawiają istotną wartość dla zainteresowań środowisk przestępczych;
- czy zasoby chronione podatne są na zniszczenie lub dewastację w wyniku działań innych czynników (np. oddziaływanie sił natury, katastrofy techniczne);
- jak przekłada się charakterystyka sąsiedztwa na poziom bezpieczeństwa;
- jakie rekomendacje w zakresie pożądanego poziomu bezpieczeństwa pojawiły się ze strony właścicieli, udziałowców, zarządu, *stakeholdersu*.

Wysoka jakość informacji, pochodzących z wiarygodnych źródeł, decyduje o kolejnych etapach cyklu zarządzania bezpieczeństwem. Jakość i wartość katalogu zagrożeń przesądza zatem o jakości całego systemu bezpieczeństwa. Ważnym elementem budowy katalogu zagrożeń jest podzielenie chronionych zasobów na kategorie, którym przyporządkowane zostaną odpowiednio – w zależności od potrzeb – priorytety. Na ogół podział zasobów dotyczy:

- ludzi (personel, klientów, podwykonawców);
- zasoby rzeczowe (maszyny, urządzenia, półprodukty, sprzęt komputerowy);
- informacje;
- procesy (dostawa, produkcja, magazynowanie, pakowanie i wysyłka).

Zasadniczy priorytet ochrony obejmuje zasoby ludzkie, w tym wiedza pracowników, a także wszelkie kontakty formalne i nieformalne. Zachowanie wymienionych priorytetów decyduje o poziomie bezpieczeństwa intelektualnego w przedsiębiorstwie.

### **Ochrona informacji w organizacji chaotycznej – dylematy polityki bezpieczeństwa intelektualnego**

W dobie organizacji szeroko przetwarzających różnorodne informacje aplikacyjność idei teorii chaosu znajduje szerokie możliwości zastosowań. Wydaje się, że jednym z najistotniejszych z tej perspektywy rozpatrywania jest kontekst kreatywności ludzi w organizacji. Staje się ona istotnym czynnikiem warunkującym elastyczność organizacji. Chaos może oznaczać: otwartą komunikację, partnerską współpracę, celową sieć powiązań, wielorakość mocnych stron.<sup>6</sup> Ograniczenie ludziom w organizacji pola dla kreatywności, ogranicza jednocześnie samej organizacji możliwość adaptacji. Zakres wolności jednostek nie może być jednakże ani zbyt rozległy, ani zbyt wąski. Uznaje się, że relacja między stopniem kreatywności dla działania a stopniem formalizacji dla struktury ma charakter odwrotnie proporcjonalny.<sup>7</sup>

Turbulentne otoczenie doprowadziło do wykształcenia specyficznej postaci chaotycznej organizacji, jako organizacji w ruchu, i wykorzystywanej przez nią – chaotycznej informacji. Transfer informacji w organizacji chaotycznej charakteryzuje się brakiem linearności, co w zasadzie podtrzymuje jej istnienie. Do specyfiki transferu informacji w organizacji chaotycznej należy zaliczyć:

- zdecydowanie nieformalny przepływ informacji;
- traktowanie w sposób równoważny tradycyjnych i nowoczesnych nośników informacji;

<sup>6</sup> U.R. Müller: *Zmiana warty w zarządzaniu*. Warszawa 2000, s.199

<sup>7</sup> R. Krupski: *Teoria chaosu a zarządzanie*. „Organizacja i Kierowanie” 1999, nr 2 (96)

- zacieranie się granic pomiędzy informacją ważną a nieistotną;
- spontaniczne generowaniem informacji;
- brak rozeznania w zakresie ośrodków nadawania i odbioru informacji;
- ciągłą, nieformalną reinterpretacją informacji, traktowaną jako istota jej transferu;
- posiadanie przez informację dużej mocy decyzyjnej oraz podtrzymywanie przez to chaotycznych procesów zachowań, działań i decyzji.<sup>8</sup>

Największe pole dla realizacji koncepcji informacji chaotycznej przewiduje się na poziomach strategicznym i taktycznym zarządzania. Tutaj winno się preferować tzw. twórczy chaos oraz akceptować szумы informacyjne. Wynika to z całkowicie nowej roli informacji w analizowanej koncepcji organizacji chaotycznej, dla której przewiduje się:

- traktowanie informacji jako najbardziej poszukiwanego towaru;
- celowe zniekształcania obrazu przedsiębiorstwa;
- wyrównywanie potencjałów energetycznych firmy i jej otoczenia;
- traktowanie zasobów rzeczowych, finansowych i ludzkich jako nośników informacji.<sup>9</sup>

Zmiana roli informacji pociąga za sobą także przewartościowania w podejściu do niej przez decydentów, preferujących szумы, zniekształcenia oraz niejednoznaczność informacji. Rosnącą turbulencją stwarza także ogromne problemy dla określenia zestawu działań i podejść dla realizacji celów zachowania bezpieczeństwa informacji w organizacji. Wydaje się, że zasadniczym poziomem zarządzania, na którym powinny koncentrować się wysiłki i rozstrzygnięcia na rzecz zachowania integralności informacji, to poziom operacyjny. Poziom ten traktowany jest bowiem jako miejsce, na którym ustrukturyzowane kanały przepływu informacji są konieczne i do pewnego stopnia sprawdzają się. Może on zatem posłużyć jako baza do odniesień i działań w dziedzinie zachowania określonego poziomu bezpieczeństwa informacji w organizacji.

Obserwacja możliwości zachowania bezpieczeństwa informacji w organizacji chaotycznej budzi potrzebę zmiany przewartościowań w dotychczas obowiązującym imperatywie. Trudno bowiem będzie w pełni zachować poufność, integralność i dostępność informacji, głównie ze względu na naturę działań w obrębie kreatywności ludzi w organizacji. Jak już bowiem wspomniano ograniczanie kreatywności ludzi obniża zdolności adaptacyjne organizacji w turbulentnym otoczeniu. Z kolei charakter informacji przetwarzanej w organizacji chaotycznej trudno poddaje się dotychczasowym rygorom ochrony.

Kluczowym zatem zasobem ochrony informacji stają się, co już wielokrotnie podkreślano, ludzie. Charakter ich działań w organizacji chaotycznej wymyka się spod kontroli przewidzianej szczegółowymi procedurami. Zwłaszcza, że wykorzystują oni przetwarzane informacje dla tworzenia coraz to nowych projektów. Stąd głównym ośrodkiem tworzenia staje się ludzki mózg, a ściślej jego zdolności do zapamiętywania kontekstów informacji, szcążkowej ich postaci, zdolności do wyłowienia z szumów tej informacji, która zdecydowanie otworzy drogę do rozwinięcia projektu o niezwykle oryginalnym kształcie i treści. Takie podejście rodzi myśl kon-

<sup>8</sup> A. Binsztok, K. Perechuda: *Nowe funkcje informacji we współczesnych koncepcjach zarządzania*. W: R. Borowiecki, M. Kwieciński (red. nauk.): *Informacja w zarządzaniu przedsiębiorstwem. Pozyskiwanie, wykorzystanie i ochrona (wybrane problemy teorii i praktyki)*. Kraków 2003, s. 38

<sup>9</sup> Ibidem, s. 39

trolowania wszystkiego tego, co pojawia się w ludzkiej wyobraźni. Wszelkie wycieki, chociażby śladowo zaznaczonych przejawów nowatorstwa, mogą być zagospodarowane przez inne mózgi, bez żadnej gwarancji, że nie zostaną wykorzystane w innych konkurencyjnych projektach, nad którymi w tym samym czasie pracuje się.

Dotychczasowe procedury ochrony informacji w organizacji nie przewidują ochrony tej zawartości, która rodzi się i konstytuuje w ludzkich mózgach. Nie można bowiem kontrolować tego, co zamierza powstawać i realnie powstaje w ludzkim mózgu, a nie zostało jeszcze zmaterializowane chociażby w zwykłych notatkach-szkicach, luźnych uwagach na piśmie, czy pliku w komputerze, a co wraz z szybkim upływem czasu może przekształcić się w konkretną całość. Najgroźniejszym zatem dla zachowania bezpieczeństwa informacji w organizacji chaotycznej jest brak możliwości daleko zaawansowanej kontroli nad ludzką twórczością, jej możliwościami, a wynikającej z koniecznej kreatywności w działaniu.

Co zatem pozostaje w tej sytuacji szczeblowi operacyjnemu zarządzania? Najszybszym rozwiązaniem, dającym pewne przesłanki kontroli nad zachowaniem bezpieczeństwa informacji pozostaje wdrożenie systemu wykorzystującego technologię mikroprocesorów. W taki mikroprocesor wyposażony byłby każdy pracownik - mózg organizacji chaotycznej w momencie podpisania umowy o pracę (dzieło). Wszczepienie mikroprocesora stwarzałoby możliwości szerokiej kontroli pracy uczestnika organizacji, łącznie z rejestracją wszelkich rozmów, czy to w zespole, czy przy pomocy wszelkich komunikatorów. Ponadto mikroprocesory stwarzałyby okazję do:

- kontroli zachowań i rozmów pracowników-mózgów poza pomieszczeniami tworzenia projektów;
- rejestracji wszelkich zmian w pracy organizmu pracownika, które mogłyby posłużyć wykrywaniu przypadków braku lojalności, na przykład z wykorzystaniem wariografu;
- bezpośredniego indywidualnego komunikowania się z pracownikiem, które pozwalałoby na uprzedzanie sytuacji zagrożeń wycieku informacji przetwarzanych w trakcie tworzenia projektów;
- budowy i wykorzystywania programów poddających pod kontrolę zachowanie lojalności pracownika;
- ogromną pomoc w tworzeniu profilu kreatywności, jak i map zagrożeń, wynikających z odniesienia udziału każdego pracownika w zespołach tworzących projekty.

Wszelkie te przedsięwzięcia pozwalałyby na zachowanie bezpieczeństwa informacji przetwarzanych w trakcie tworzenia projektów, zanim znajdą one postać „zmaterializowaną”. Jest rzeczą oczywistą, że bezpieczeństwo informacji jako najważniejszy imperatyw, stałoby się najważniejszą przesłanką do wyrażenia zgody przez pracownika na ograniczenie własnej wolności z tytułu udziału w podejmowanych pracach. Zmiana miejsca pracy wiązałaby się z koniecznym przestrzeganiem rygorów o podobnym profilu w innych konkurencyjnych zespołach.

Wydaje się zatem, że w przypadku organizacji chaotycznych może nadejść era Wielkiego Brata, jako odpowiedź na zagrożenia bezpieczeństwa informacji. Opisywana koncepcja zmian stanowić może nieco skomplikowane, aczkolwiek łatwo przyswajalne przez menedżerów rozwiązanie, za którym przynajmniej mogą oni spodziewać się obiecujących wyników. Ramy prawne nowych rozwiązań

z pewnością uwzględnią będą konieczność zachowania bezpieczeństwa informacji w organizacji jako najważniejszego imperatywu jej działania.

### **Zakończenie**

Można przyjąć, że zastosowanie koncepcji wywiadu i kontrwywiadu gospodarczego w realizacji zadań przedsiębiorstwa może odegrać ogromną rolę. Zespoły pracownicze, jako depozytariusze wiedzy winny być stale analizowane, zwłaszcza w obszarze łączących ich relacji. Relacje międzyludzkie w przedsiębiorstwie, podobnie jak komórki nerwowe ludzkiego mózgu, bywają określane inteligencją organizacji. W kontrwywiadzie gospodarczym natomiast zasadniczym czynnikiem sukcesu jest zapewnienie możliwości skutecznej wymiany informacji między ludźmi. Ma to szczególne znaczenie w tworzeniu sieci kontaktów interpersonalnych, zarówno wewnętrznych, jak i zewnętrznych.

Ochrona informacji w organizacji chaotycznej może w pełni zagospodarować technologię mikroprocesorów. Miniaturyzacja chipów, postępy nanotechnologii zdecydowanie wspomogą ideę podejmowanych rozwiązań. W efekcie uczestnicy organizacji chaotycznej staną się w pełni „przeźroczyści”.

Powyzsza tendencja znajduje swoje potwierdzenie w obserwacji gwałtownych zmian w projektach i technologiach związanych z zachowaniem bezpieczeństwa po zamachach na WTC. Wprowadzenie nowych metod kontroli spowodowało podjęcie przez amerykańskie utajnione Biuro Świadomości Informacyjnej (Information Awareness Office) zaawansowanych prac nad stworzeniem systemu integrującego wiedzę z publicznych i prywatnych baz danych – firm ubezpieczeniowych, biur turystycznych, banków i łączącego ją z danymi biometrycznymi – cyfrowym zapisem linii papilarnych, wzorca tęczy oka oraz ... profilem DNA. Do pracy w Biurze Świadomości zaangażowano także psychologów, którzy starają się przetworzyć na język cyfrowy schematy ludzkich zachowań i gestów. Jednocześnie informatycy opracowują tzw. siatki neuronalne, czyli superszybkie programy komputerowe, które porządkują ową gigantyczną bazę danych i wyławiają z niej najistotniejsze informacje. Dzięki nim będzie można błyskawicznie zidentyfikować człowieka, odtworzyć ze szczegółami jego przeszłość i przewidzieć przyszłe zachowania.<sup>10</sup>

Nie jest to jeszcze świat matriksu, ale stąd niedaleko już do ogromnej kontroli nad ludzką wyobraźnią, a to stanowi przecież podstawę działań w organizacji chaotycznej.

---

<sup>10</sup> K. Pytko: *Szpiegom nie dorównasz*. „Focus” 2007, nr 8