



## Andrzej Żebrowski

# Walka informacyjna – przedsiębiorstwo – globalizacja

Postępująca rywalizacja to nie tylko współpraca, ale przede wszystkim walka, która sprawia, że otoczenie wewnętrzne i zewnętrzne każdej organizacji nieustannie się zmienia. W procesie tym człowiek stanowi centralne ogniwo wszelkich zmian. Zawsze będzie dążył do zaspokojenia swoich potrzeb. Także żądza posiadania władzy ma wpływ na zachodzące przeobrażenia (zarówno w pozytywnym, jak i negatywnym znaczeniu). Oznacza to, że jedne organizacje osiągają założone cele, inne tylko w określonym zakresie, a pozostałe nie są w stanie tego dokonać.

Na gruncie pogłębiającej się globalizacji oddziaływanie organizacji gospodarczych w sferze ekonomicznej stale wzrasta. Dlatego też można powiedzieć, że przestrzeń bezpieczeństwa ekonomicznego współczesnych przedsiębiorstw (krajowych, międzynarodowych i globalnych) tworzą zbiory stale poszerzających się wartości, które wymagają coraz bardziej wyspecjalizowanej wiedzy, będącej motorem napędzającym wszelkie zmiany.

\*\*\*

Globalizacja to rozwój i zagrożenia, a także coraz większa otwartość na kontakty ze światem zewnętrznym w ramach prowadzonej walki informacyjnej.

„Granice gospodarcze i kulturowe zanikają dużo szybciej niż polityczne, ale i te wyglądają już zupełnie inaczej. Obecnie coraz bardziej wspólne cele ekonomiczne mają nie poszczególne państwa, ale ponadnarodowe grupy interesów. To nie proletariusze wszystkich krajów połączyły się, ale zupełnie inne grupy. One zglobalizowały się najbardziej, pozostawiając innych w tyle. Nie należy, zatem przeciwstawiać państw, lecz konfrontować grupy interesu”<sup>1</sup>.

„Globalizacja polega na tym, że stopniowo zanikają granice i to pod każdym względem. Kiedyś informacja trafiała w czasie rzeczywistym tylko tam, gdzie docierał

<sup>1</sup> W. Kołodko, *Ludzka twarz globalizacji*, „Trybuna”, 18 marca 2000.

głos, teraz dociera wszędzie. Ta rewolucja – o niebywałych konsekwencjach dla funkcjonowania gospodarki – dopiero się zaczyna. I to trzeba umieć wygrać<sup>2</sup>.

Zespół nazywany Grupą Lizbońską<sup>3</sup> zaprezentował problematykę globalizacji w materiale *Granice rywalizacji, globalizacja gospodarki a przyszłość ludzkości*, gdzie postawiono następującą tezę: „W przeciwieństwie do internacjonalizacji – w której ramach państwo narodowe może znaleźć podstawową funkcję swego pochodzenia, globalizacja rozwija tylko proces umiędzynarodowienia; mianowicie – jako kluczowy aktor – dąży, by w gospodarce i społeczeństwie proces ten odgrywał coraz większą rolę, choć wiadomo, że przedsięwzięcie to w coraz większym stopniu zwalnia państwo i jego instytucje z kierowania gospodarką i jej kształtowania<sup>4</sup>”.

Według stanowiska Grupy Lizbońskiej, niektórzy ekonomiści uważają, że należy widzieć trzy koncepcje, z których wynikają konsekwencje polityczne, społeczne, jak i strategiczne, m.in. w gospodarce<sup>5</sup>:

- pierwsza, to internacjonalizacja gospodarki i stowarzyszeń (spółek), która oznacza wymianę surowców, produktów przemysłowych i usług, pieniędzy, idei i ludzi między dwoma państwami lub większą ich liczbą,
- druga, to umiędzynarodowienie gospodarki i stowarzyszeń (spółek), które przejawia się przede wszystkim w ten sposób, że przelewa się lub przenosi resursy, szczególnie kapitały, a w mniejszym zakresie również pracę, z jednej gospodarki do innych,
- trzecia, to globalizacja gospodarki i stowarzyszeń (spółek), które należy rozumieć jako nowe zjawisko, mogące przyjąć rozmaite formy i rozwiązania.

W związku z tym globalizację można przedstawić w następujących, mniej lub bardziej konkretnych formach<sup>6</sup>:

- globalizacja w zakresie finansowym,
- globalizacja rynków i strategii rynkowych, zwłaszcza w zakresie rywalizacji,
- globalizacja technologiczna i związana z nią wiedza (różnorodne badania i wiedza),
- globalizacja form życia, środków komunikacji oraz życia kulturalnego,
- globalizacja w zakresie możliwości sterowania,
- globalizacja jako polityczne współżycie w ramach całego świata,
- globalizacja percepcji i świadomości.

Zatem globalizacja jest zjawiskiem, w którym wydarzenia, rozstrzygnięcia i czynności mające miejsce w jednej części świata wywierają wpływ na funkcjonowanie organizacji gospodarczych w odległych jego częściach. Oznacza to, że globalizacja składa się z dwóch istotnych elementów: pierwszy to rozprzestrzenianie się, a drugi to intensywność.

Aby wygrać szanse i zminimalizować zagrożenia niezbędna jest wspomniana wiedza, która pozwala na dokonywanie wyborów.

Istotnym elementem rozwoju w dalszym ciągu jest jednak globalizacja. Ma ona miejsce nie tylko w gospodarce i handlu między przedsiębiorstwami i państwami, ale

<sup>2</sup> J. Karczmarek, *Globalizacja – rozwój i zagrożenia „Myśl Wojskowa”* 2001, nr 1, s. 99–100.

<sup>3</sup> <http://www.baks.com/4198C.html>.

<sup>4</sup> J. Karczmarek, *Globalizacja...*, s. 103.

<sup>5</sup> *Ibidem*, s. 103.

<sup>6</sup> *Ibidem*, s. 103–104.

także w kulturze, sporcie, polityce, itp. „W ostatnich latach można jednak zauważyć wpływ czysto ekonomicznego myślenia”<sup>7</sup>.

\*\*\*

Konkurencja coraz częściej przyjmuje postać walki, której celem jest nie tylko wykluczenie, ale i zniszczenie rywali. W takim ujęciu nie jest środkiem do celu, lecz raczej ukrytym celem – normą niszczenia przeciwnika (konkurencji).

Rywalizacja w sferze gospodarczej w toczącej się walce informacyjnej nie musi oznaczać bezpośredniego starcia. Konfrontacja ta może przebiegać na płaszczyźnie informacyjnej i psychologicznej, a w skrajnych przypadkach prowadzić do fizycznej destrukcji. Działania te, to ciągła modyfikacja, dostosowywanie się do nowych wyzwań i potrzeb, a ich zakres jest postępujący zarówno w sferze metod i zainteresowań.

„Należy mieć świadomość tego, że na gruncie dalszego pogłębiania się procesu prywatyzacji, rozregulowania i liberalizacji rynków, globalne przedsięwzięcia coraz bardziej wyłączają państwa i ich instancje od kierowania gospodarką światową i jej kształtowania. Wielonarodowe koncerny i tak zwane sieci finansowe są lepiej dostosowane do rozwoju globalnych procesów gospodarczych aniżeli państwa. Pojawia się więc nowa sprzeczność między polityką państwa a gospodarką, gdyż ta ostatnia coraz bardziej wymyka się spod władzy państwa”<sup>8</sup>.

Przeobrażeniom w sferze gospodarczej towarzyszy postęp naukowo-techniczny, który jest również czynnikiem sprawczym rozwoju nowych środków i sposobów prowadzenia walki informacyjnej wspierającej działalność organizacji. Również rozwój technologii teleinformatycznych sprawia, że wspomniana walka informacyjna będzie nabierać coraz większego znaczenia.

Jednym z ważniejszych czynników, które mają wpływ na zwiększenie potencjału (ekonomicznego<sup>9</sup>) organizacji gospodarczej jest automatyzacja systemów wspierających proces decyzyjny. Komputeryzacja tych systemów i integracja z infrastrukturą<sup>10</sup> telekomunikacyjną jest czynnikiem determinującym ich podatność na ataki wewnętrzne i zewnętrzne. Różnorodność elementów walki informacyjnej wpływa na jej zróżnicowaną intensywność.

Pozostałe elementy walki informacyjnej, które mogą stanowić zagrożenie dla bezpieczeństwa procesów decyzyjnych, zasobów informacyjnych, finansowych i osobowych przedstawia rys. 1.

„Na szczególną uwagę zasługuje atak informatyczny, który obejmuje kompleks tzw. zaczepnych operacji informacyjnych, ukierunkowanych na przełamywanie obrony informatycznej systemów i sieci teleinformatycznych przeciwnika (konkurencji), ich obezwładnianie i porażanie oraz aktywne manipulowanie zawartą w nich wiedzą”<sup>11</sup>.

<sup>7</sup> *Ibidem*, s. 106.

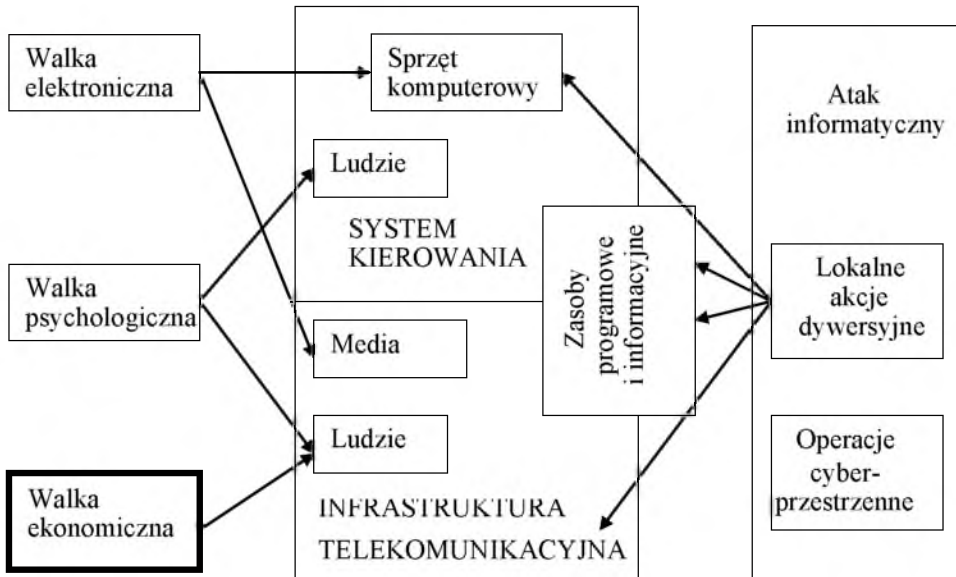
<sup>8</sup> *Ibidem*.

<sup>9</sup> Potencjał ekonomiczny – maksymalna zdolność w zakresie produkcji dóbr i usług, jaką dany naród jest w stanie osiągnąć w pewnym okresie (*Mobilization Preparedness*, Washington 1983, s. 4).

<sup>10</sup> Infrastruktura – obiekty, urządzenia stałe i instytucje usługowe (krajowe i międzynarodowe) niezbędne do należytego funkcjonowania społeczeństw, tzn. produkcyjnych działów gospodarki oraz życia (w tym bezpieczeństwa) ludności (*Słownik terminów z zakresu bezpieczeństwa narodowego*, Warszawa 2002, s. 47).

<sup>11</sup> A. Stokalski, *Informacyjny wymiar działań wojennych*, VII Konferencja Naukowa „Automatyzacja dowodzenia”, Jelenia Góra, 12–15 maja 1999 r.

Przyjmuje się, że do ataków informatycznych zalicza się metody stosowane przez hakerów, a ponadto podsłuch i inwigilację przy użyciu środków technicznych, naruszanie integralności danych komputerowych a także sabotaż, oszustwo, fałszerstwo komputerowe. Może on być również przeprowadzony przy użyciu wirusów komputerowych, które po wprowadzeniu do systemu mogą podejmować działania natychmiast lub pozostawać w ukryciu. Ukryte wirusy aktywizują się po pewnym czasie i docierają do określonych elementów systemu. Mogą one być wprowadzane przez producentów, eksporterów sprzętu komputerowego i oprogramowania. Zakłada się również wprowadzenie do systemów i sieci teleinformatycznych mikroorganizmów, które mogą doprowadzić do ich fizycznego zniszczenia. Takim przykładem jest stosowanie bakterii do utylizacji układów scalonych, które rozkładają arsenek galu.



Rysunek 1. Niesiłowe zagrożenia bezpieczeństwa systemów kierowania

Źródło: J. Czerwieński, *Problemy bezpieczeństwa systemów dochodzenia a walka informacyjna*, „Myśl Wojskowa” 2000, nr 3, s. 95.

W Polsce w 1998 r. zanotowano ponad 900 oficjalnie zgłoszonych wykroczeń (ataki hakerów). Na podstawie kwalifikacji dokonanej przez poszkodowanych charakterystyka tych wykroczeń przedstawia się następująco<sup>12</sup>:

- 11% próby włamania,
- 41% skuteczne włamania,
- 39% bombardowanie internetowych skrzytek pocztowych, niepożądana korespondencja,
- 9% inne.

<sup>12</sup> Materiały z serwera TP S.A., [www.tpnet.pl](http://www.tpnet.pl).

Dodajmy, że niektóre grupy hakerów mają powiązania z obcymi służbami specjalnymi.

Przypadki te pokazują, jak łatwo można dostać się do systemów komputerowych dysponując tylko ogólnie dostępnym sprzętem komputerowym (tzw. podwójnego zastosowania). Natomiast specjaliści mający dostęp do wysokowyspecjalizowanych narzędzi mogą penetrować systemy w sposób, który wyrządza większe szkody i o wiele trudniejszy do ukrycia (działania te można określić jako operacje cyberprzestrzenne).

„Operacje cyberprzestrzenne są o wiele groźniejszą formą walki informacyjnej (...), jako że przede wszystkim są zorganizowanym, zaplanowanym działaniem – tak zwane cyberataki są prowadzone w określonym celu i przeciwko konkretnym osobom lub organizacjom [gospodarczym – przyp. autora]”<sup>13</sup>.

Operacje cyberprzestrzenne są prowadzone tam, gdzie istnieje dostęp do systemów i sieci komputerowych. Stanowi to poważne zagrożenie nie tylko dla organizacji gospodarczych. Są one wymierzone również w infrastrukturę państwa<sup>14</sup>, zwłaszcza w systemy telekomunikacyjne, energetyczne, bankowe, dystrybucji paliw i wody, kierowanie ruchem kolejowym, powietrznym, siłami zbrojnymi, zarządzania państwem itp.

Do pozawojzkowych źródeł walki informacyjnej zalicza się:

- powstanie i rozwój bazy informatycznej o zasięgu ogólnopaństwowym (globalnym),
- powszechna komputeryzacja wielu sfer życia (w tym gospodarczego),
- powszechność systemów łączności elektronicznej,
- istnienie licznych o różnym przeznaczeniu baz danych i powszechne wykorzystywanie komputerów osobistych.

\*\*\*

Istotą aktywności organizacji gospodarczych jest prowadzenie takich działań, które obejmują zarówno kooperacje pozytywne, jak i negatywne. Oznacza to, że w zależności od zmian zachodzących w otoczeniu zewnętrznym (bliższym i dalszym organizacji) i jej interesami w aktywności tej może dominować współpraca bądź walka.

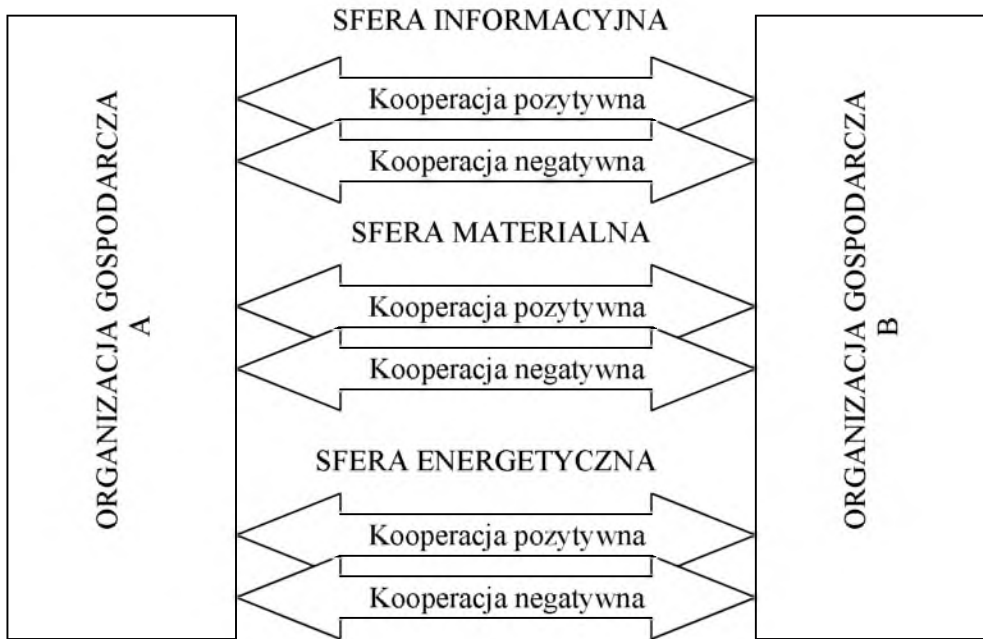
Do czynników kształtujących rozwój organizacji gospodarczych należą materia, energia i informacja<sup>15</sup>, które na siebie wzajemnie oddziałują.

Z punktu widzenia ekonomicznego, gdy oddziaływanie to jest wynikiem celowej aktywności ludzkiej – mogą przybierać formę kooperacji pozytywnej i negatywnej (co przedstawia rys. 2).

<sup>13</sup> J. Czerwieński, *Problemy bezpieczeństwa systemów dowodzenia a walka informacyjna*, „Myśl Wojskowa” 2000, nr 3, s. 97.

<sup>14</sup> Infrastruktura państwa – część instytucji obejmująca obiekty, urzędnicy stałe i instytucje usługowe niezbędne do należytego funkcjonowania produkcyjnych działów gospodarki oraz życia (w tym bezpieczeństwa) ludności kraju (*Słownik z zakresu bezpieczeństwa narodowego*, Warszawa, 2002, s. 48).

<sup>15</sup> M. Mazur, *Jakościowa teoria informacji*, Warszawa 1970, s. 19.



Rysunek 2. Pozytywne i negatywne formy sfer oddziaływań

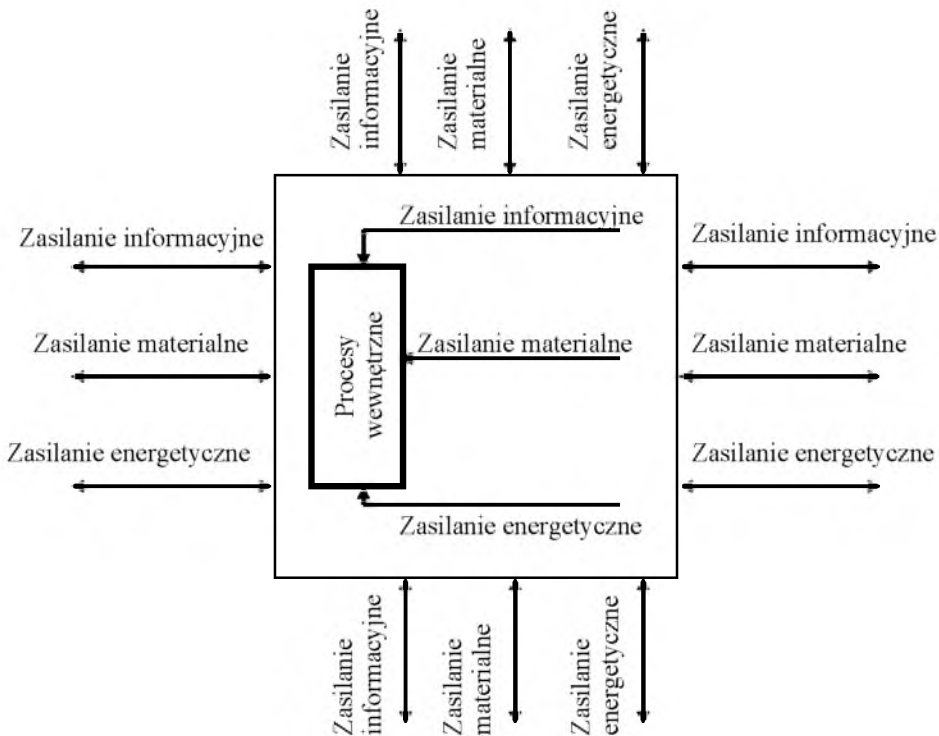
Źródło: opracowano na podstawie R. Szpyra, *Oddziaływanie informacyjne sił powietrznych – kierunki poszukiwań badawczych*, „Myśl Wojskowa” 2002, nr 1, s. 95.

Organizacja gospodarcza charakteryzuje się zarówno aktywnością wewnętrzną, jak i zewnętrzną. Procesy zachodzące w jej otoczeniu i poszczególnych komponentach wymagają zasilania materialnego, energetycznego i informacyjnego (co przedstawia rys. 3).

W tym procesie dominującą rolę odgrywa informacja (zasoby informacyjne organizacji gospodarczej).

„Dzisiaj zasoby informacyjne decydują o tzw. inteligencji instytucji, tj. o sposobie wykorzystania posiadanych przez nią możliwości, zdolnościach dostosowania do nowych sytuacji i programowania swojej przyszłej działalności, a więc o zdolnościach osiągania stałych sukcesów w warunkach ciągłych zmian i traktowania tych zmian nie tylko w kategoriach zagrożeń, lecz jako szans na rozwijanie nowej skutecznej działalności”<sup>16</sup>.

<sup>16</sup> P. F. Drucker, *Innowacja i przedsiębiorczość. Praktyka i zasady*, Warszawa 1992, s. 36–37.



Rysunek 3. Zewnętrzne sfery oddziaływań oraz sfery zasilania procesów wewnętrznych

Źródło: opracowano na podstawie R. Szpyra, *Działania informacyjne sił powietrznych – kierunki poszukiwań badawczych*, „Myśl Wojskowa” 2002, nr 1, s. 96.

\*\*\*

Zmiany zachodzące w organizacjach gospodarczych wymagają innego spojrzenia na system pozyskiwania, przetwarzania i udostępniania informacji, a więc na zarządzanie informacjami w sferze gospodarczej.

Zarządzający przedsiębiorstwem podejmując różne formy aktywności, mogą generować informacje o korzyściach, kosztach i paraliżu. Informacje dotyczące wspomnianych korzyści i kosztów przyczyniają się do podejmowania określonych działań, natomiast te o paraliżu (destrukcji) utrudniają niewątpliwie osiągnięcie przyjętego celu (celów).

Każda organizacja jest zależna od informacji, sposobów jej pozyskiwania, gromadzenia, przetwarzania, ochrony i dystrybucji. Zasoby informacyjne organizacji mają ścisły związek z wymianą danych, jak również z jej rozwojem. Właściwe wykorzystywanie informacji z otoczeniem wewnętrznym i zewnętrznym daje wymierne korzyści. Jeżeli potraktujemy organizację jako system oparty na wiedzy, to jej zaplecze stanowi wspomniana wiedza, umiejętności pracowników, systemy i sieci teleinformatyczne oraz bazy danych. Są one szczególnie narażone na wszelkie negatywne oddziaływanie.

Istotnym problemem funkcjonowania tego systemu jest integracja jego elementów. Ich właściwe skojarzenie (na zasadzie synergii), przekłada się na wzrost efektywności działania, a więc realizacja celów przez organizację gospodarczą.

„Zarówno w ujęciu ogólnym, jak i różnych dziedzin nauki informacje są utożsamiane z wiedzą poszczególnych osób oraz określonych grup ludzi”<sup>17</sup>. Oznacza to, że wiedza jest połączeniem doświadczenia i wybranych informacji, które dla skutecznego działania organizacji będą wykorzystywane przez uprawnionych zarządzających. „W dobie szybko dokonujących się zmian jest ona postrzegana jako zasób dominujący, niewyczerpalny, symultaniczny i nieliniowy”<sup>18</sup>.

W trwającej walce informacyjnej w sferze gospodarczej wiedza jest pozyskiwana zarówno z zewnątrz, jak i wewnątrz organizacji. Może się to odbywać przez<sup>19</sup>:

- nabycie (przejmowanie innych organizacji lub pozyskiwanie najlepszych pracowników),
- ośrodki tworzenia wiedzy (tworzenie własnych ośrodków naukowych),
- łączenie (organizowanie zespołów ludzi z różnym doświadczeniem, wykształceniem i umiejętnościami, którzy pracują wspólnie i kolektywnie wymieniają się wiedzą),
- adaptacja (wiedza powstająca w efekcie reakcji na oddziaływanie otoczenia zewnętrznego),
- tworzenie sieci nieformalnych.

W tym procesie nie można zapominać o wywiadzie gospodarczym (cywilnym i wojskowym – agendy rządowe), komórkach wywiadu gospodarczego przedsiębiorstw konkurencyjnych, wywiadowniach gospodarczych.

Dostęp do wieloźródłowych informacji zwiększa możliwości pozyskiwania danych. Znaczne możliwości w tym zakresie niosą ze sobą nowoczesne technologie teleinformatyczne, sprzęt i oprogramowanie. Istotny jest także proces kształcenia i doskonalenia ludzi, którzy je wykorzystują i pamiętają, że „inteligentna organizacja gospodarcza wymaga inteligentnych ludzi”.

Powszechna komputeryzacja zwiększa możliwości oddziaływania na konkurencję w ramach prowadzonej walki informacyjnej, gdzie obok pozyskiwania informacji i jej ochrony, atak może polegać m.in. na<sup>20</sup>:

- zerwaniu procedur wymiany informacji,
- manipulowaniu informacją,
- korzystaniu z nieautoryzowanego dostępu do zasobów informacyjnych oraz nielegalnym zbieraniu i wykorzystywaniu informacji,
- nielegalnym kopiowaniu danych zawartych w systemach informatycznych,
- masowym niszczeniu oprogramowania.

Atak informacyjny to działania ofensywne, których podstawowym celem jest pozyskiwanie informacji znajdujących się w sferze zainteresowania organizacji gospodarczej. Jest on także wspierany przez przedsięwzięcia o charakterze psychologicznym (manipulacja, dezinformacja, propaganda) i zakłócanie percepcji odbiorczej przeciwnika (konkurencji).

<sup>17</sup> T. Pszczołowski, 1978, *Mała encyklopedia prakseologii i teorii organizacji*, Wrocław-Warszawa-Kraków-Gdańsk, s. 269; zob. też A. S. Reber, *Słownik psychologii*, 2000, s. 823.

<sup>18</sup> A. Strojny, *Zarządzanie wiedzą. Ogólny zarys koncepcji*, „Przegląd Organizacji” 2000, nr 2.

<sup>19</sup> A. Strojny *Zarządzanie wiedzą w organizacjach*, Kraków 1999.

<sup>20</sup> J. L., *Rosyjska koncepcja walki informacyjnej*, „Wojskowy Przegląd Zagraniczny” 1999, nr 1, s. 84.



Dla skuteczności podejmowanych decyzji, zarządzający organizacją powinni zwracać uwagę także na właściwe zabezpieczenie posiadanych zasobów informacyjnych, finansowych i osobowych przed nieuprawnionym dostępem. Dlatego przedsiębiorstwa kontrwywiadowcze, kontrpropagandowe i związane z bezpieczeństwem informacji (fizyczna, techniczna, systemów i sieci teleinformatycznych) są niezbędne do realizacji celów strategicznych.

Bezpieczeństwo każdej organizacji (w tym gospodarczej), to ludzie i właściwie prowadzona polityka personalna przez uprawnionych zarządzających. To na nich spoczywa bezwzględny obowiązek niedopuszczenia do przecieku informacji. Błędna polityka kadrowa to duża fluktuacja personelu, którego wiedza ma wartość zarówno dla własnej organizacji, jak i konkurencji.

Bezpieczeństwo osobowe to przede wszystkim wymiar ludzki. Na terenie organizacji gospodarczej mogą przebywać trzy (różne) podmioty mające wpływ na jej funkcjonowanie bądź jego zakłócanie (co przedstawia rys. 4).

Zalicza się do nich m.in.:

- osoby odpowiedzialne za przyjęcie i wdrożenie procedur bezpieczeństwa i ich przestrzeganie,
- klientów i gości,
- grupy (osoby) tzw. podwyższonego ryzyka (zewnętrzne i wewnętrzne) stanowiące rzeczywiste zagrożenie dla organizacji.

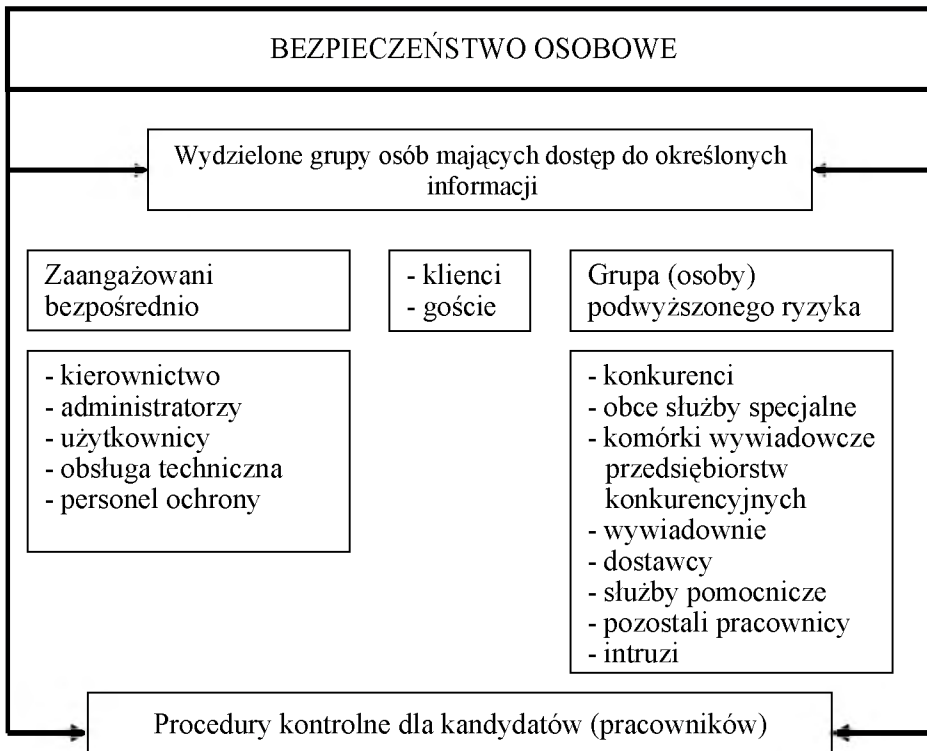
Bezpieczeństwo osobowe to również:<sup>21</sup>

- zakres obowiązków pracowniczych – jako dokument integralny umowy o pracę powinien zawierać zapisy zobowiązujące do określonych zachowań związanych z bezpieczeństwem,
- dobór kadr i ich przegląd (umowy na czas określony, system awansu zawodowego, ewentualnie zwolnień dyscyplinarnych) powinien odbywać się według ściśle określonych procedur,
- powinny zostać opracowane warunki i zasady obowiązujące przy zatrudnianiu pracowników,
- nie należy lekceważyć nawet najdrobniejszych sygnałów o zachowaniach negatywnych.

\*\*\*

Współczesne przedsiębiorstwa to dynamiczna i rozciągnięta w czasie aktywność prowadzona w przestrzeni osobowej i technicznej. Rozwój organizacji gospodarczej oznacza właściwe funkcjonowanie własnego systemu informacyjnego i jego walkę z analogicznym systemem (systemami) przeciwnika (konkurencji). Oznacza to prowadzenie intensywnej walki informacyjnej, na którą składa się: zdobywanie informacji, zakłócanie procesów informacyjnych przeciwnika, obrona własnych systemów informacyjnych.

<sup>21</sup> A. Białas, *Bezpieczeństwo informacji usług w nowoczesnej instytucji*, Warszawa 2006, s. 467–468.



Rysunek 4. Grupy osób, które znajdują się na terenie jednostki organizacyjnej

Źródło: opracowano na podstawie M. Polok, *Ochrona tajemnicy państwowej i tajemnicy służbowej w polskim systemie prawnym*, Warszawa 2006, s. 135.

„Walka informacyjna to kooperacja negatywna wzajemnie realizowana w sferze zdobywania informacji, zakłócania informacyjnego i obrony informacyjnej, gdzie każdemu działaniu jednej strony podporządkowane jest działanie antagonistycznej strony drugiej<sup>22</sup>.

Człowiek i informacja (wyselekcjonowana i wartościowa) to komponenty, które kształtują wizerunek i pozycję organizacji praktycznie w każdym środowisku. Dokonywanie wyboru ostatecznego wariantu przy rozważaniu różnych alternatywnych możliwości działania przy umiejętnym wykorzystywaniu wskazanych zasobów, pozwala na realizację przyjętych celów. Potrzeby informacyjne i bezpieczeństwo (osobowe, finansowe, informacyjne) to atrybuty skutecznego działania każdej organizacji gospodarczej.

<sup>22</sup> L. Ciborowski, *Walka informacyjna*, Toruń 1999, s. 187.

## Bibliografia

- Białas A., *Bezpieczeństwo informacji usług w nowoczesnej instytucji*, Warszawa 2006.
- Ciborowski L., *Walka informacyjna*, Toruń 1999.
- Czerwieński J., *Problemy bezpieczeństwa systemów dowodzenia a walka informacyjna*, „Myśl Wojskowa” 2000, nr 3.
- Drucker P. F., *Innowacja i przedsiębiorczość. Praktyka i zasady*, Warszawa 1992, <http://www.baks.com/4198C.html>.
- J. L., *Rosyjska koncepcja walki informacyjnej*, „Wojskowy Przegląd Zagraniczny” 1999, nr 1.
- Karczmarek J., *Globalizacja – rozwój i zagrożenia*, „Myśl Wojskowa” 2001, nr 1.
- Kołodko W., *Ludzka twarz globalizacji*, „Trybuna”, 18 marca 2000 r.
- Mazur M., *Jakościowa teoria informacji*, Warszawa 1970.
- Mobilization Preparedness*, Defense University, Washington 1983.
- Pszczółowski T., *Mała encyklopedia prakseologii i teorii organizacji*, Wrocław–Warszawa–Kraków–Gdańsk 1978.
- Reber A. S., 2000, *Słownik psychologii. Słownik z zakresu bezpieczeństwa narodowego*, 2002, Warszawa,
- Stokalski A., *Informacyjny wymiar działań wojennych*, VII Konferencja Naukowa „Automatyzacja dowodzenia”, Jelenia Góra, 12–15 maja 1999 r.
- Strojny A., *Zarządzanie wiedzą. Ogólny zarys koncepcji*, „Przegląd Organizacji” 2000, nr 2.
- Strojny A., *Zarządzanie wiedzą w organizacjach*, Kraków 1999.
- [www.tpnet.pl](http://www.tpnet.pl)